



**Politecnico
di Torino**

Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Gestionale

**Evoluzione del mercato della cybersecurity e ruolo
strategico dei Managed Security Service Provider
nell'era dell'intelligenza artificiale**

Relatrice:

Francesca Montagna

Candidato:

Marco Mercuri

Anno Accademico 2025-2026

Sommario

Abstract	4
Introduzione.....	5
1. Evidenze empiriche sull'evoluzione del settore cybersecurity.....	6
1.1 Evoluzione dell'interesse accademico.....	6
1.2 Evoluzione dell'interesse industriale	9
1.3 Pressioni di mercato e driver di domanda.....	12
2. Modello lineare dell'innovazione Cybersecurity.....	14
2.1 Ricerca di Base	14
2.2 Ricerca Applicata	21
2.3 Fase precompetitiva	23
3. La fase competitiva nella cybersecurity.....	27
3.1 Cyber Solutions – Le varie tecnologie nel mondo della cybersecurity.....	29
3.2 Managed Security Services – Da tecnologia a servizio gestito.....	40
3.3 Limiti strutturali delle soluzioni frammentate.....	45
3.4 Platformization	47
3.4 Principali vendor nell'era delle piattaforme multi-dominio	49
3.5 Analisi delle forze di Porter: soluzioni frammentate e piattaforme multi-dominio	56
3.6 Curve ad S – Traiettorie evolutive e confronto di performance tecniche	59
3.7 Piattaforme multi-dominio e l'evoluzione del ruolo degli MSSP	63
3.8 Analisi della domanda di cybersecurity e implicazioni per i modelli MSSP	64
3.9 Sintesi interpretativa e implicazioni strategiche per gli MSSP.....	69
4. Ruolo strategico di un MSSP nell'era dell'AI - Caso Nais	70
4.1 Posizionamento competitivo e problema strategico	70
4.2 Definizione delle leve strategiche.....	72
4.3 Strategia di implementazione dell'AI nei processi SOC.....	75
4.4 Evidenze preliminari e segnali quantitativi	81
5. Conclusioni	84
5.1 Limiti dello studio e sviluppi futuri	84
5.2 Sintesi dei risultati.....	85
Appendice	86
Bibliografia	87
Sitografia	89

Abstract

Il presente lavoro di tesi analizza l'evoluzione del mercato della cybersecurity alla luce dell'aumento della complessità delle superfici d'attacco, della crescente pressione normativa e dell'adozione di nuove tecnologie quali l'intelligenza artificiale, nonché della progressiva dipendenza dei processi di business da dati e servizi digitali. In questo contesto, il settore sta attraversando una fase di trasformazione strutturale caratterizzata dal passaggio da soluzioni verticali a piattaforme multi-dominio integrate, data-driven e fortemente automatizzate. La ricerca affronta la domanda su come un *Managed Security Service Provider* possa evolvere la propria architettura di servizi e il proprio modello operativo per costruire un posizionamento competitivo sostenibile in un mercato in rapida espansione e continuo cambiamento. Attraverso un'analisi del modello lineare dell'innovazione e delle dinamiche competitive di mercato, integrata da un caso studio sul modello di *Augmented SOC* sviluppato da Nais, la tesi individua un insieme di best practice per l'evoluzione strategica degli MSSP e per la progettazione di servizi SOC-as-a-Service scalabili ed economicamente sostenibili, supportati da capacità di automazione intelligente.

I risultati mostrano come la sostenibilità competitiva degli MSSP, con particolare evidenza nel segmento mid-market, richieda una riconfigurazione integrata del modello di servizio, in cui tecnologia, intelligenza artificiale, organizzazione e relazioni di filiera concorrono alla definizione di un assetto strategico scalabile e coerente. Tali evidenze forniscono indicazioni operative per il percorso evolutivo di Nais e delineano principi di replicabilità applicabili ad altri MSSP che intendano strutturare modelli di servizio sostenibili nel lungo periodo.

Introduzione

Negli ultimi anni la cybersecurity ha assunto un ruolo di priorità strategica per imprese e istituzioni, guidata dalla crescente dipendenza dei processi di business e servizi digitali e dalla sofisticazione e frequenza degli attacchi informatici. Questo contesto ha trasformato la sicurezza informatica da funzione tecnica di supporto a priorità strategica trasversale per molte imprese, con implicazioni dirette sulla continuità operativa, governance aziendale e conformità normativa. Le organizzazioni, quindi, non devono più scegliere se investire in sicurezza, ma comprendere come farlo in modo sostenibile, misurabile e coerente con una minaccia in continua evoluzione.

Dal lato dell'offerta, il settore sta attraversando una trasformazione di paradigma altrettanto profonda. Le soluzioni verticali specializzate che hanno dominato il mercato della cybersecurity per anni, hanno presentato nel tempo limiti strutturali sempre più impattanti nell'adozione per le organizzazioni. Questi vincoli hanno accelerato la convergenza verso piattaforme multi-dominio integrate e fortemente automatizzate, ridisegnando i confini di competizione tra gli attori della filiera. In questo scenario, i fornitori di servizi di sicurezza gestiti si trovano a dover ridefinire la propria proposta di valore per non rischiare di essere percepiti come semplici *system integrator* e non portare valore aggiunto per il cliente nel nuovo ecosistema.

Il presente lavoro si colloca in questo perimetro, guidato dalla domanda su come un *Managed Security Service Provider* possa costruire un posizionamento competitivo e sostenibile nell'era dell'intelligenza artificiale, affrontandola attraverso due livelli di analisi complementari. Il primo è teorico e competitivo: traccia l'evoluzione del mercato dalla ricerca di base alla fase competitiva e analizza le dinamiche tra i paradigmi in competizione per identificare le implicazioni per i modelli MSSP. Il secondo è empirico e applicativo: grazie alla collaborazione con l'azienda *Nais*, fornitore di servizi di sicurezza gestiti operante nel mercato italiano, traduce le evidenze teoriche in un caso studio concreto per la definizione delle leve strategiche competitive e di una strategia di implementazione dell'intelligenza artificiale nei processi operativi a supporto della scalabilità e sostenibilità nell'ecosistema emergente degli MSSP. Il lavoro si articola in cinque capitoli. Il primo fornisce un inquadramento empirico dell'evoluzione dell'interesse accademico e industriale nel settore, attraverso un'analisi bibliometrica, brevettuale e dei principali driver di domanda. Nel secondo capitolo viene interpretata questa evoluzione attraverso il modello lineare dell'innovazione, tracciando la traiettoria dalla ricerca di base alla fase precompetitiva. Il terzo capitolo analizza le dinamiche competitive del mercato, confrontando i due paradigmi attraverso l'applicazione di strumenti analitici e identificando le implicazioni per i *Managed Security Service Provider*. Il quarto capitolo traduce le evidenze teoriche nel caso *Nais*, sviluppando le leve strategiche per un MSSP in evoluzione, la strategia di implementazione dell'AI a supporto della scalabilità e sostenibilità dei servizi e mostrando le prime evidenze quantitative dei risultati ottenuti. Il quinto capitolo discute i risultati complessivi della ricerca, evidenziandone i principali limiti metodologici e definendo alcuni spunti di approfondimento per sviluppi futuri.

1. Evidenze empiriche sull'evoluzione del settore cybersecurity

Il presente capitolo ha l'obiettivo di fornire un inquadramento empirico dell'evoluzione del settore della cybersecurity attraverso l'analisi di indicatori quantitativi riconducibili alla produzione scientifica e all'attività brevettuale. L'esame congiunto della dinamica bibliometrica e brevettuale consente di osservare l'andamento dell'interesse accademico e industriale nel tempo, offrendo una prima rappresentazione oggettiva delle traiettorie di sviluppo del dominio tecnologico considerato.

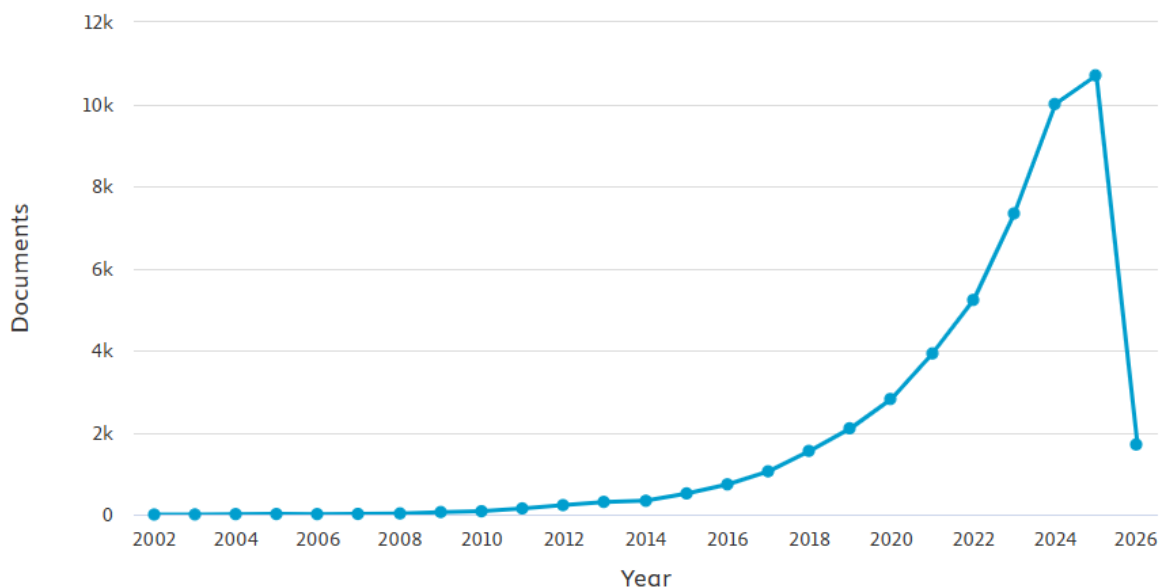
In particolare, l'analisi della produzione scientifica permette di valutare l'intensità e la progressiva articolazione della ricerca nel campo della cybersecurity e della sua integrazione con l'intelligenza artificiale, mentre l'analisi brevettuale fornisce un'indicazione dell'attività di ricerca e sviluppo applicata da parte degli attori industriali.

L'obiettivo non è quello di misurare la qualità dell'innovazione, bensì di individuare segnali quantitativi della maturazione e della crescente centralità del settore. Tali evidenze costituiscono la base per l'inquadramento teorico successivo, volto a interpretare l'evoluzione osservata alla luce dei modelli di innovazione tecnologica.

1.1 Evoluzione dell'interesse accademico

Per comprendere a pieno la rilevanza e l'impatto della materia della sicurezza informatica è stata condotta un'analisi quantitativa e bibliometrica sull'argomento della cybersecurity per individuare l'evoluzione dell'interesse accademico attraverso il trend di crescita dei report accademici nel corso degli anni. La ricerca è stata condotta sulla piattaforma Scopus interrogando i campi titolo, abstract e parole chiave (TITLE-ABS-KEY) attraverso due query principali ed escludendo le aree disciplinari non pertinenti (ad esempio neuroscienze, medicina, agraria e discipline umanistiche) al fine di circoscrivere l'analisi al dominio tecnologico di interesse.

Documents by year

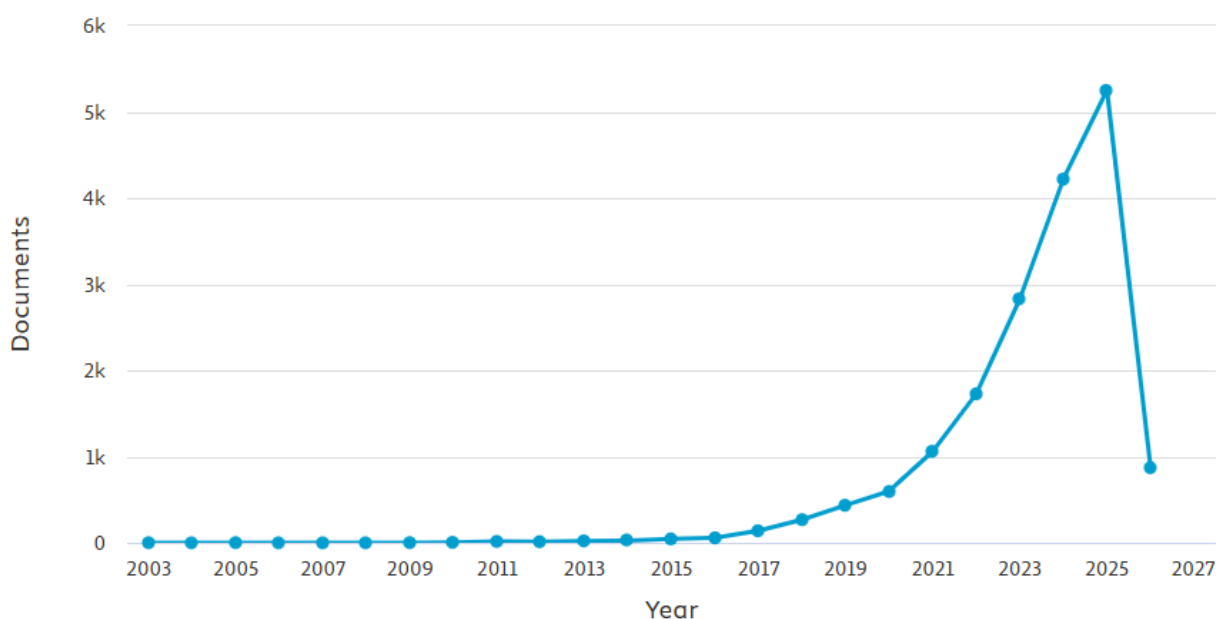


Fonte: Elsevier. (2026). Scopus database. Retrieved from <https://www.scopus.com>

Figura 1.1: Serie temporale delle pubblicazioni scientifiche in cybersecurity; query di ricerca accorciata: cybersecurity AND (cyber attack* OR malware)

L'evoluzione della produzione scientifica in ambito cybersecurity risulta osservabile già a livello bibliometrico. La literature review condotta sulla piattaforma Scopus evidenzia, a partire dal 2002, un totale di 48.270 contributi scientifici riconducibili al dominio della sicurezza informatica. La curva ha avuto un flesso di crescita incrementale a partire approssimativamente dal 2019, coerentemente con il fenomeno della pandemia e la digitalizzazione dei processi di business. Il numero di pubblicazioni raggiunge un massimo nel 2025, con 10.547 documenti indicizzati. Seppur con un range temporale ridotto, la produzione delle pubblicazioni sull'argomento continua nel 2026 con un totale di 1708 documenti a fine febbraio.

Documents by year



Fonte: Elsevier. (2026). Scopus database. Retrieved from <https://www.scopus.com>

Figura 1.2: Serie temporale delle pubblicazioni scientifiche in cybersecurity e AI; query di ricerca accorciata: cybersecurity AND ("artificial intelligence" OR AI OR "machine learning" OR "deep learning" OR "large language model*" OR LLM* OR "generative AI")

L'analisi è stata estesa alla produzione scientifica relativa ai temi congiunti di cybersecurity e intelligenza artificiale, al fine di osservare l'evoluzione del sottodominio tecnologico emergente. La literature review condotta su Scopus evidenzia un totale di 17.590 contributi scientifici a partire dal 2003. Il numero di pubblicazioni mostra una crescita progressiva dal 2016 e un'accelerazione più marcata a partire dal 2020.

L'andamento risulta coerente, in termini proporzionali, con la curva complessiva della cybersecurity, suggerendo una progressiva integrazione delle tecnologie di intelligenza artificiale nel settore della sicurezza informatica. Il numero massimo di pubblicazioni è stato registrato nel 2025, con 5.248 articoli indicizzati.

Nel complesso, l'evidenza bibliometrica indica un crescente interesse accademico verso l'intersezione tra cybersecurity e AI, confermandone la rilevanza nell'evoluzione tecnologica del settore.

1.2 Evoluzione dell'interesse industriale

L'analisi dell'evoluzione del settore della cybersecurity non può limitarsi alla dimensione accademica, ma richiede l'osservazione dell'attività di ricerca e sviluppo in ambito industriale. In tale prospettiva, l'attività brevettuale rappresenta un indicatore quantitativo rilevante, in quanto consente di cogliere l'intensità degli investimenti tecnologici e la formalizzazione della conoscenza in applicazioni potenzialmente trasferibili al mercato. Il seguente approfondimento è stato condotto tramite la piattaforma Patent Inspiration per individuare l'evoluzione e la crescita della proprietà intellettuale nella cybersecurity.

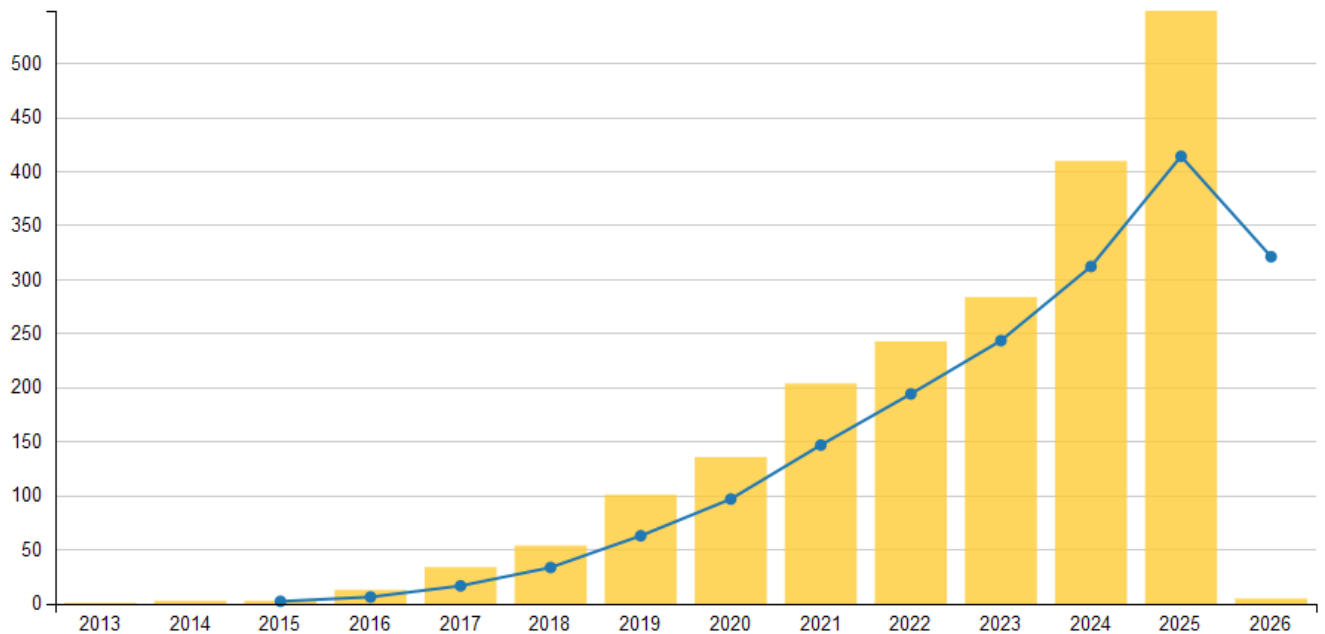


Figura 1.3: Evoluzione annuale dei depositi brevettuali nel dominio della cybersecurity; Patent Inspiration

L'andamento dell'evoluzione annuale dei depositi brevettuale è coerente con quello delle produzioni scientifiche, con una crescita sostenuta a partire dal 2019 e un picco massimo che supera i 500 depositi nel 2025.



Figura 1.4: Distribuzione geografica delle famiglie brevettuali in cybersecurity; Patent Inspiration

La Figura 1.4, mostra come la distribuzione geografica della proprietà intellettuale del settore sia concentrata particolarmente in alcuni Paesi:

- **United States: 1431**
- Israel: 97
- United Kingdom: 78
- Republic of Korea: 62
- Canada: 58

Questa mappatura suggerisce la centralità di specifici ecosistemi tecnologici nell'evoluzione del settore.

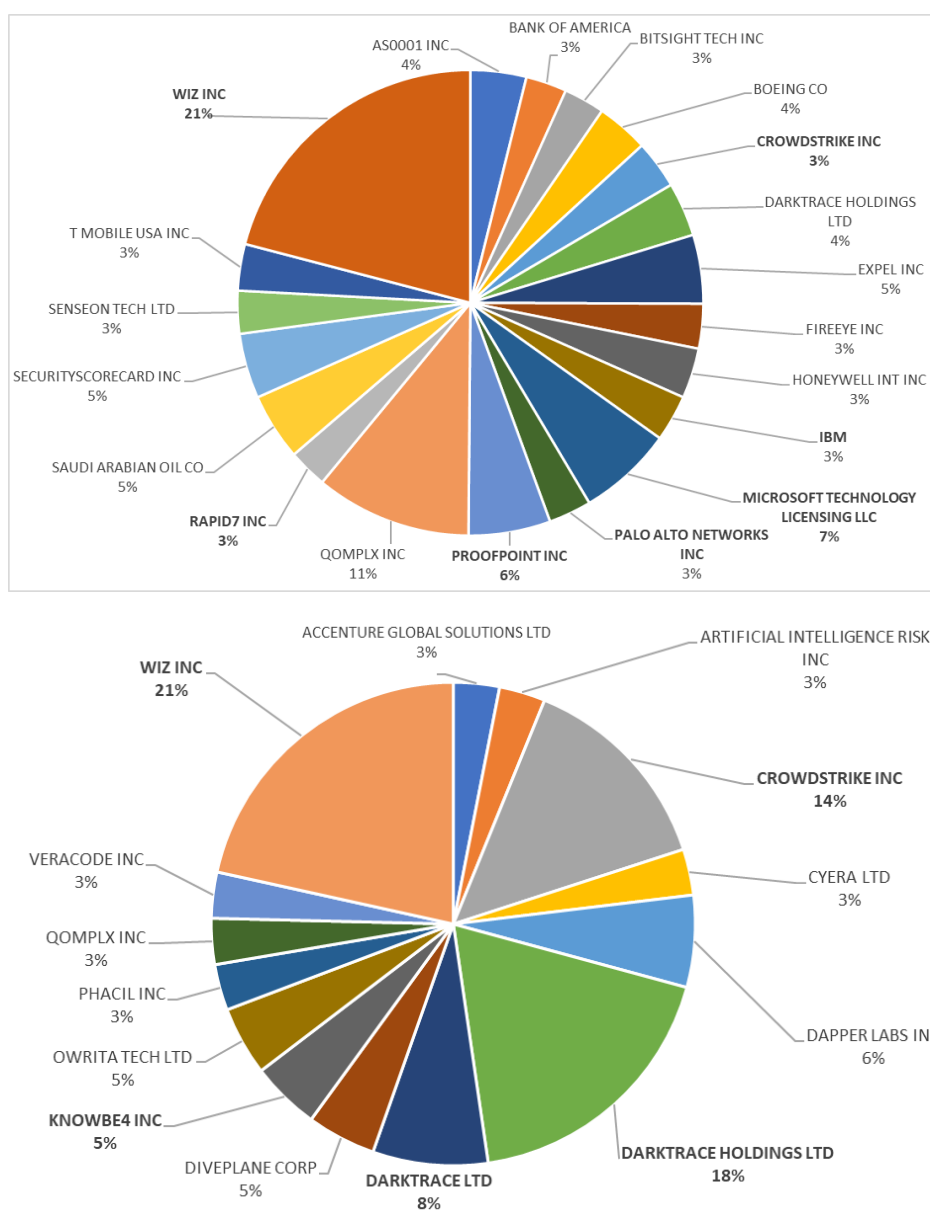


Figura 1.5: Distribuzione percentuale delle famiglie brevettuali in cybersecurity per azienda (in alto) vs. percentuale delle famiglie brevettuali in cybersecurity e AI per azienda (in basso).

L'analisi della distribuzione brevettuale per azienda presente in Figura 1.5, mostra inoltre che alcuni attori detengono quote rilevanti dell'attività di deposito nel dominio della cybersecurity (grafico in alto). Il confronto con il sottodominio che integra cybersecurity e intelligenza artificiale (grafico in basso) evidenzia come parte di questi operatori mantenga una posizione significativa anche nel perimetro AI-driven, indicando una continuità nelle strategie di ricerca e sviluppo.

Questa analisi preliminare del settore permette di avere un inquadramento delle dinamiche evolutive del settore e di quella che si può definire come una progressiva integrazione delle tecnologie come l'intelligenza artificiale nelle traiettorie di innovazione della cybersecurity.

1.3 Pressioni di mercato e driver di domanda

L'evoluzione della cybersecurity non può e non deve essere interpretata esclusivamente tramite indicatori accademici o brevettuali, ma deve riflettere le trasformazioni strutturali che hanno interessato il contesto economico e tecnologico globale e l'accelerazione della domanda riconducibile a fattori organizzativi e normativi.

Uno dei primi elementi di discontinuità rilevante è stato rappresentato dalla pandemia da COVID-19, che ha inevitabilmente accelerato i processi di digitalizzazione e trasformato radicalmente i modelli organizzativi. La diffusione del lavoro da remoto, l'adozione massiva di servizi cloud, la virtualizzazione dei processi aziendali e l'assenza di politiche di governance del rischio informatico e di gestione degli eventi hanno ampliato la superficie di attacco e facilitato il lavoro degli hacker. Questo contesto ha profondamente cambiato il posizionamento della sicurezza informatica nei diversi settori, passando da funzione di supporto tecnico a priorità essenziale per la continuità operativa e resilienza aziendale.

Come appena citato, un altro fattore impattante è riconducibile all'aumento della frequenza e della sofisticazione degli attacchi informatici, che ha ampliato in modo significativo per organizzazioni private e pubbliche l'esposizione al rischio. Report di mercato come *Cost of a Data Breach 2025* di IBM e *Data Breach Investigation Report 2025* di Verizon mostrano come nell'ultimo anno, il costo medio globale di un data breach, ossia la divulgazione o perdita di dati sensibili o riservati, sia stato di circa 4.44 milioni di dollari con crescenti violazioni correlate all'uso e alla governance dell'intelligenza artificiale (IBM, 2025b; Verizon, 2025b). Oltre a questi dati viene riportata l'evoluzione degli attacchi ransomware, eventi malevoli che bloccano i sistemi informatici di un'organizzazione con richiesta di riscatto per il ripristino delle informazioni, e tecniche sofisticate come il furto di credenziali e la compromissione della supply chain. Questi dati evidenziano come la progressiva integrazione di nuove tecnologie non abbia solo un beneficio di miglioramento ma abbia un impatto bidirezionale, permettendo l'utilizzo ad attori ostili per migliorare l'efficacia dei propri attacchi.

Parallelamente all'evoluzione degli attacchi informatici e alla digitalizzazione del business, il rafforzamento del quadro regolatorio, in particolare in Europa, sta contribuendo a consolidare la centralità del tema e definire un livello minimo di resilienza per tutte le realtà aziendali indipendentemente dalla dimensione. Negli ultimi anni la *Direttiva (UE) 2022/2555 NIS2* e il *Regolamento (UE) 2022/2554 DORA* stanno introducendo obblighi più stringenti in materia di gestione del rischio, governance e responsabilità del management. Questi sono solo alcuni esempi di come la pressione normativa stia sensibilizzando le diverse organizzazioni e abilitando i servizi di sicurezza informatica in diversi settori. Un'analisi più dettagliata dell'impatto delle normative sui principali settori economici sarà sviluppata nel Capitolo 3, nell'ambito dell'esame della domanda e delle sue determinanti settoriali.

Le previsioni di mercato confermano inoltre una crescita sostenuta della spesa globale in cybersecurity, con tassi di incremento superiori a quelli medi dell'IT. In particolare, il report Gartner (2024), società internazionale di consulenza e ricerca specializzata nell'analisi dei mercati tecnologici e nelle previsioni di spesa IT, riporta una previsione di spesa per la fine del 2025 di 212 miliardi di dollari nella cybersecurity, con un tasso di crescita del 15.1% rispetto al 2024 (Gartner,

2024). Le previsioni della spesa globale in cybersecurity risultano coerenti con quanto emerge da numerose indagini campionarie rivolte ad executive di livello C. Ad esempio report provenienti da aziende di consulenza strategica internazionali come PwC Global Digital Trust Insights 2026 documentano come il 60% dei 3887 business e tech executives intervistati hanno come principale obiettivo di investimento strategico prioritario quello del rischio cyber (PwC, 2025). Inoltre, il report Deloitte Global's Future of Cyber survey evidenzia come la figura del *Chief Information Security Officer (CISO)* stia assumendo sempre più responsabilità ed influenza nelle decisioni strategiche aziendali per la pianificazione dell'adozione di soluzioni di sicurezza informatica con particolare interesse per l'implementazione dell'intelligenza artificiale nei programmi di cybersecurity (Deloitte, 2024). Questi dati sono evidenti segnali di un cambio di direzione verso la prioritizzazione dell'argomento della sicurezza informatica nelle organizzazioni e del conseguente impatto sull'evoluzione del mercato.

Le presenti dinamiche verranno approfondite nei successivi capitoli, ma costituiscono una base fondamentale per comprendere le evoluzioni tecnologiche e competitive del settore.

2. Modello lineare dell'innovazione Cybersecurity

Il modello lineare dell'innovazione descrive il processo innovativo come una sequenza progressiva di fasi che si sviluppano a partire dalla ricerca di base, originata da una scoperta scientifica, per poi evolvere nella ricerca applicata, nello sviluppo tecnologico e infine nella diffusione sul mercato di prodotti e servizi. Nelle prime fasi, quali ricerca di base e applicata, assume un ruolo centrale il sistema accademico, che opera in un contesto caratterizzato da elevata incertezza scientifica e tecnologica. Le università, a differenza delle aziende, possono permettersi di assumere il rischio di studiare fenomeni innovativi che potrebbero fallire sul mercato e diminuirne la percentuale tramite l'alto livello di competenze specialistiche a disposizione. In tale ambito vengono esplorate molteplici traiettorie di ricerca, delle quali solo una parte si traduce successivamente in applicazioni industriali. L'adozione di questo modello nel presente lavoro consente di fornire una lettura strutturale dell'evoluzione della cybersecurity, offrendo una chiave interpretativa per collegare le evidenze empiriche alle dinamiche competitive e tecnologiche del settore.

2.1 Ricerca di Base

2.1.1 Teoria dell'informazione e segretezza perfetta (Shannon, 1949)

Claude Shannon, nato a Petoskey nel Michigan il 30 aprile 1916, è stato un celebre matematico e ingegnere statunitense che grazie ai suoi studi è stato definito "*il padre della teoria dell'informazione*". Dopo la laurea nel 1936 in matematica e in ingegneria elettronica all'università del Michigan, si trasferì per un master al MIT (Massachusetts Institute of Technology) sull'utilizzo dell'algebra Boole per l'analisi e l'ottimizzazione dei circuiti di comunicazione a relè. Nel 1941 prese il ruolo di ricercatore matematico presso la Bell Telephone dove nel 1948 pubblicò il saggio "*A mathematical theory of communication*", uno dei pilastri della moderna teoria dell'informazione e dell'informatica. Grazie ai suoi lavori dedicati alla teoria dell'informazione, all'affidabilità dei circuiti, al problema della sicurezza della comunicazione e alla crittografia, Shannon ha profondamente cambiato la teoria e la pratica della comunicazione. Nel 1949 Shannon pubblicò *Communication Theory of Secrecy Systems*, gettando le basi verso la moderna crittografia, dove vengono descritti i criteri generali che un sistema di cifratura deve rispettare per considerarsi affidabile. La crittografia a *scrittura segreta* ha come scopo quello di nascondere, di rendere incomprensibile, all'interesse di terzi, i messaggi che si scambiano due interlocutori.

Grazie a Shannon, per la prima volta i responsabili militari potevano misurare la sicurezza dei propri sistemi su base matematica introducendo alcuni concetti come:

- Entropia, misura matematica dell'incertezza di una chiave o messaggio;

- Perfect Secrecy, sicurezza perfetta, conoscere il cifrato non riduce l'incertezza sul messaggio;
- Unicity distance, la quantità di testo cifrato necessario per determinare univocamente la chiave e aprire la 'resistenza' dei cifrari a traffico lungo;
- Confusion and diffusion, principi che rendono un cifrario resistente all'analisi statistica.

Shannon aprì le porte al mondo della sicurezza informatica e ne fece capire l'importanza, permettendo evoluzioni successive come la crittografia a chiave pubblica (Diffie-Hellman, RSA) negli anni '70. Oggi soluzioni come le *Public Key Infrastructure (PKI)*, framework di sicurezza che gestisce i certificati digitali e chiavi crittografiche per autenticare le identità e cifrare i dati di rete, sono possibili solo perché Shannon ha formalizzato il significato della sicurezza di una chiave (Shannon, 1948).

2.1.2 Modello Shannon-Weaver

Warren Weaver, nato nel 1894 a Reedsburg, Wisconsin, era uno scienziato, matematico e direttore della *Division of Natural Sciences* della Fondazione Rockefeller dal 1932 fino al 1955. Il suo contributo nella propagazione della teoria di Shannon fu di fondamentale importanza, mentre Shannon si focalizzava su aspetti prettamente ingegneristici e matematici per l'ottimizzazione delle telecomunicazioni, Weaver si propose come collaboratore e facilitatore per rendere il lavoro accessibile ad un pubblico non tecnico e contribuendo sulla parte comunicativa della teoria. La loro collaborazione culminò nella pubblicazione congiunta della teoria, dividendo in due parti il libro: la sezione tecnica di Shannon e l'introduzione interpretativa di Weaver senza alcuna alterazione dei fondamenti matematici. Weaver si concentrò sul problema della comunicazione creando una tassonomia a tre livelli:

- Livello A – Tecnico, accuratezza di trasmissione dei simboli;
- Livello B – Semantico, precisione del significato per far coincidere l'informazione con l'interpretazione;
- Livello C – Efficacia, l'impatto del messaggio sul destinatario.

L'impatto di Weaver non si limita alla comprensione effettiva della teoria ma trasforma la catena definita da Shannon per le telecomunicazioni, in uno schema generale e fondamentale della comunicazione umana e artificiale.

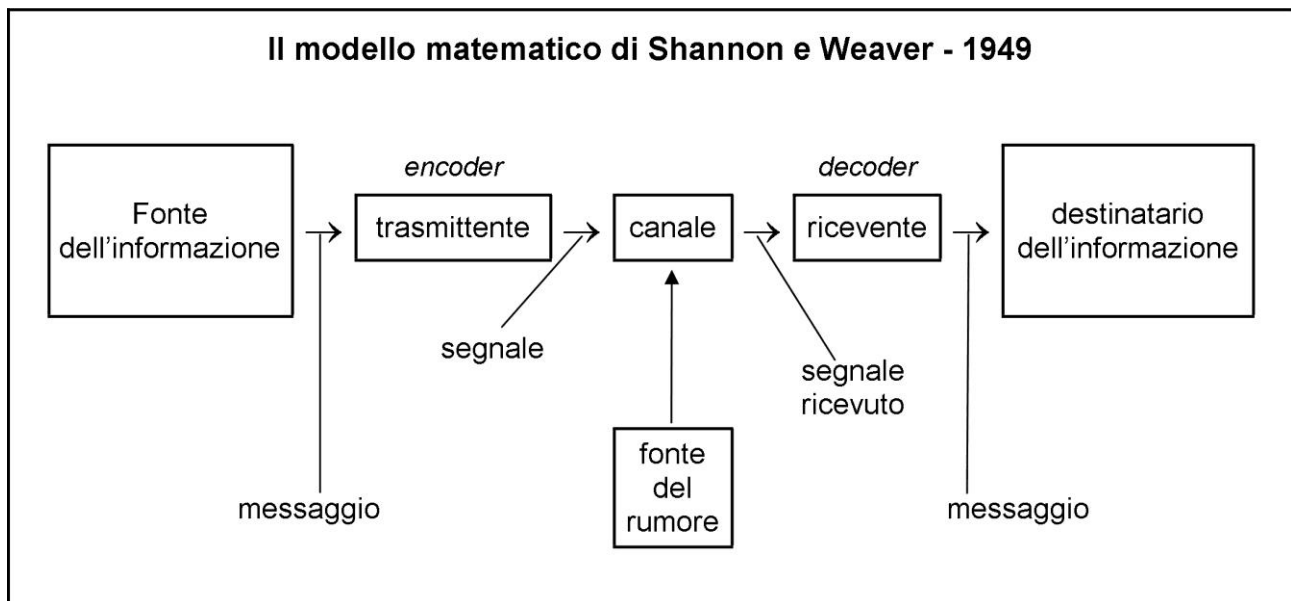


Figura 2.1: Il modello matematico di Shannon e Weaver -1949

Fonte: https://it.wikipedia.org/wiki/Teoria_dell'informazione#Modello_di_Shannon-Weaver

Il modello di Shannon-Weaver suddivide la comunicazione in sette componenti principali:

- Fonte dell'informazione, genera il messaggio iniziale non ancora codificato;
- Trasmettitore, codifica il messaggio in un segnale adatto alla trasmissione;
- Canale, permette di passare il segnale direttamente al ricevente con una capacità limitata definita da Shannon;
- Fonte del rumore, sono i tipi di interferenze che alterano il segnale definiti da Weaver;
- Ricevente, decodifica il segnale ricevuto per ricostruire il messaggio;
- Destinatario dell'informazione, riceve e interpreta il messaggio decodificato.

Questo è un modello lineare semplice pilastro della teoria della comunicazione, ma che presenta allo stesso tempo due limiti importanti. Il primo è proprio la linearità del modello e l'assenza di feedback, il flusso unidirezionale non rappresenta la conversazione reale dove il destinatario risponde, corregge o influenza il mittente. Il secondo è la definizione del rumore come interferenza centrale e non come possibilità di errore di chi codifica e di chi decodifica (Shor, 1994).

2.1.3 Diffie–Hellman e RSA: fondamenti della sicurezza scalabile nelle reti moderne

Whitfield Diffie e Martin Hellman, due ricercatori di Stanford, nel 1976 pubblicarono il celebre articolo *New Directions in Cryptography*. Questa pubblicazione cambiò profondamente il concetto di sicurezza informatica introducendo due idee rivoluzionarie: lo scambio di chiavi a canale insicuro e il concetto di crittografia a chiave pubblica. Fu un'innovazione radicale dove due soggetti a distanza potevano stabilire un segreto comune comunicando apertamente. Il *Diffie-Hellman Key Exchange*, meccanismo matematico alla base del concetto rivoluzionario, sfrutta il problema del logaritmo discreto considerato computazionalmente difficile. L'idea è che ogni attore coinvolto nella comunicazione scegliesse un segreto privato, calcolasse una trasformazione matematica basata su un numero primo e una base pubblica e inviasse il risultato al secondo interlocutore coinvolto. Una volta scambiati i valori, ambe le parti possono calcolare la stessa chiave segreta condivisa che resta sconosciuta a parti terze e rendendo impossibile l'estrazione delle chiavi originali. Questo schema permise di risolvere il problema della distribuzione delle chiavi senza fornire però veri e propri meccanismi per cifrare o firmare messaggi in modo diretto, rimanendo vulnerabile ad attacchi di tipo *man-in-the-middle* se non integrato con forme di autenticazione. Questa lacuna fu colmata nel 1978 da Ronald Rivest, Adi Shamir e Leonard Adleman, studenti del MIT, che pubblicarono il primo schema pratico di crittografia a chiave pubblica soprannominato "RSA". L'obiettivo era quello di separare i ruoli di chi crea la sicurezza (chiave privata) e di chi la utilizza (chiave pubblica) senza scambiare informazioni in una fase preliminare. Il processo per la realizzazione dell'algoritmo RSA sfrutta la difficoltà della fattorizzazione di grandi numeri primi come fondamento di sicurezza, estendendo il framework della crittografia a chiave pubblica fornendo un sistema completo per la crittografia e firma digitale. La combinazione di questi due studi ha avuto un impatto fondamentale sulla sicurezza della comunicazione e sull'evoluzione della cybersecurity, rendendo possibile la nascita della *Public Key Infrastructure*. La PKI è un sistema organizzato di certificati digitali e autorità di certificazione che consente di associare chiavi pubbliche a utenti, server e dispositivi, permettendo a milioni di utenti di autenticarsi e scambiare dati in sicurezza senza dover condividere manualmente chiavi segrete. Fino ad oggi il calcolo della fattorizzazione dei numeri primi ha rappresentato uno dei più grandi problemi della computazione classica, ma con l'avvento dei computer quantici e della loro potenza di calcolo questa strategia di cifratura risulta poco robusta. Il paradigma non è più descritto dalla classica algebra booleana ma da qubit che possono rappresentare più stati (Diffie & Hellman, 1976).

2.1.4 Dorothy E. Denning: modello Intrusion Detection System

Dorothy E. Denning è una ricercatrice statunitense di sicurezza informatica, riconosciuta principalmente per gli studi sul controllo degli accessi basato su reticolo (LBAC) e i sistemi di rilevamento delle intrusioni (IDS). In particolare, nel 1987 Denning pubblica su IEE Transactions on Software Engineering “*An Intrusion Detection Model*” che rappresenta uno dei primi passi verso i moderni sistemi di rilevamento delle intrusioni (IDS) (Denning, 1987). Questo modello nasce dall’esigenza di colmare il divario tra controlli preventivi e realtà dei sistemi multiutente e in rete. L’obiettivo della ricercatrice era quello di normalizzare il problema della rilevazione delle minacce, attribuire un’architettura generale, riutilizzabile e indipendente della piattaforma. Il modello proposto si basa:

- Sullo sviluppo di una struttura che monitora in tempo reale i registri di audit di un sistema (eventi di log in, accessi a file, comandi) per rilevare violazioni di sicurezza, identificando nel comportamento degli utenti pattern anomali utilizzando i log come strumento di inferenza sul rischio in tempo reale;
- Sulla costruzione di profili per soggetto e finestra temporale, combinando profili statistici e regole di abuso con una base di conoscenza aggiornabile e un ciclo integrato di allerta-risposta;
- Sull’indipendenza dell’ambiente applicativo, fornendo un framework flessibile per la costruzione di IDS generici.

Denning diede un contributo fondamentale al mondo della sicurezza informatica modificando quella che era una gestione idiosincratica della registrazione degli eventi e della definizione di un comportamento ‘anomalo’, in una gestione chiara, univoca e replicabile. Questo ha portato al possibile sviluppo di nuove implementazioni di sicurezza come:

- Endpoint Detection & Response (EDR);
- Extended Detection & Response (XDR).

permettendo di aumentare il perimetro dell’individuazione di nuove minacce.

2.1.5 MPEG come infrastruttura di protezione dei contenuti

La cifratura dei dati non è l'unico livello di protezione dei contenuti digitali, ma l'insieme di scelte architettoniche che permettono di proteggere e preservare anche i contenuti multimediali. In questa sezione parleremo di come un innovatore italiano, Leonardo Chiariglione, abbia rivoluzionato il mondo dei contenuti multimediali tramite il gruppo MPEG. Leonardo Chiariglione ha conseguito la laurea magistrale in ingegneria elettronica presso il Politecnico di Torino e un Ph.D. presso l'università di Tokyo nel 1973. In quel periodo, a partire dal 1972, iniziò a lavorare presso il CSELT (Centro Studi e Laboratori Telecomunicazioni), un importante centro di ricerca e sviluppo di telecomunicazioni torinese. Durante la permanenza nel CSELT ha fondato, insieme a Hiroshi Yasuda nel 1988, il comitato MPEG (Moving Pictures Experts Group), un team internazionale di esperti che ha realizzato standard rivoluzionari per rendere interoperabile ed efficiente la gestione dei media digitali. Tra gli standard sviluppati dal gruppo MPEG, i principali sono:

- MPEG-1, primo standard MPEG progettato per la compressione di video e audio per formati Video CD;
- MPEG-2, evoluzione di MPEG-1 per la televisione digitale, DVD, trasmissioni satellitari e HDTV;
- MPEG-4, standard per applicazioni di streaming, multimedialità web e Digital Rights Management (DRM);
- MPEG-7, standard per la ricerca efficiente dei contenuti multimediali attraverso metadati;
- MPEG-21, standard per la gestione e la distribuzione dei contenuti digitali.

L'obiettivo del gruppo MPEG non era quello di creare nuovi formati multimediali, ma di rendere i media digitali una commodity a larga scala. Avere un linguaggio comune ha abbattuto pesantemente i costi di distribuzione dei contenuti multimediali, generato enormi effetti di rete e reso scalabile la diffusione di un contenuto conforme agli standard stabiliti. Lo standard MPEG-1 Audio Layer III è un caso esemplare che ha permesso la diffusione del formato MP3, usato tutt'oggi per i contenuti musicali, dimostrando come la sinergia tra governance degli standard e ricerca proprietaria abiliti l'adozione globale di un'innovazione.

Di conseguenza però la diffusione è stata un catalizzatore per il mondo della pirateria digitale, sfruttando proprio il principio di interoperabilità degli standard. Il susseguirsi di questi eventi ha dato impulso all'adozione di sistemi DRM, infrastrutture tecnologiche che regolano accesso, copia, modifica e diffusione d'autore. Grazie al supporto di Chiariglione, il DRM moderno è un sistema che gestisce licenze, modalità di consumo, pay-per-view, controllo sulle autorizzazioni e accessi, stabilendo delle barriere di protezione per il mondo dei contenuti digitali. Alcuni esempi d'uso del DRM:

- Apple iTunes, tramite l'app store utilizza il DRM per limitare il numero di dispositivi associabili al singolo account per l'ascolto dei brani;
- Spotify, sfrutta tecnologie blockchain per il pagamento agli artisti;
- Microsoft software, sfrutta "PlayReady" tecnologia DRM che garantisce la distribuzione dei contenuti su una rete e gestisce le autorizzazioni per l'uso del software;
- Documenti sensibili, tenere traccia di chi visualizza i file a livello aziendale.

2.1.6 Minaccia quantistica e cornice teorica di sicurezza (Shor, Grover)

Fino agli inizi degli anni '90, la crittografia a chiave pubblica (RSA e Diffie-Hellman) ha rappresentato lo standard di protezione basandosi sull'assunzione che fattorizzare un intero grande o risolvere il logaritmo discreto in un gruppo finito richiedesse tempo super-polinomiale a un avversario classico. Questa base teorica venne capovolta da Peter Williston Shor, nel 1994 mentre lavorava ai Bell Laboratories, tramite la sua invenzione nota oggi come *Algoritmo di fattorizzazione di Shor*. Proposto nel suo articolo "*Algorithms for Quantum Computation: Discrete Logarithms and Factoring*", l'algoritmo dimostra che, su un calcolatore quantistico fault-tolerant, i problemi di fattorizzazione di numeri interi grandi e risoluzione del logaritmo discreto si risolvono in tempo polinomiale. Dal punto di vista teorico, si costruisce una funzione periodica $f(x) = a \cdot x \bmod N$ e si chiede di stimarne il periodo r . L'algoritmo sfrutta la trasformata quantistica di Fourier (QFT), stimabile attraverso computer quantistici, per stimare il periodo r e recuperando i fattori N , riducendo il tempo di fattorizzazione da esponenziale a polinomiale. Lo stesso algoritmo è replicabile per il logaritmo discreto, facendo crollare i principi alla base della sicurezza informatica. Attualmente non esistono macchine di questa scala a livello commerciale; tuttavia, la minaccia è intertemporale e algoritmi di questo tipo permettono di prevenire potenziali attacchi in un futuro prossimo (Shor, 1994). A supporto della teoria di Shor, Lov Grover nel 1996 sviluppò un algoritmo per la ricerca non strutturata in un database di N elementi che dimostra come un computer quantistico possa accelerare questo tipo di ricerca da $O(N)$ a $O(\sqrt{N})$. A differenza dell'algoritmo di Shor, che compromette direttamente la crittografia a chiave pubblica, l'algoritmo di Grover spiega come tramite computer con potenza di calcolo maggiore aumenti la rapidità di attacchi brute-force, minacciando la crittografia a chiave simmetrica (Grover, 1996). L'Advance Encryption Standard (AES), standard di crittografia a chiave simmetrica utilizzato a livello mondiale, risulta vulnerabile all'algoritmo di Grover. Un modo efficace per contrastarlo è raddoppiare la dimensione della chiave per mantenere un livello di sicurezza quantistica pari a quello attuale passando da *AES-128* ad *AES-256*. Questi due algoritmi dimostrano come l'ascesa dell'informatica quantistica richieda un approccio proattivo alla cybersecurity, mettendo le aziende e i governi in una posizione di progresso e preparazione per la difesa da minacce di questa portata.

2.2 Ricerca Applicata

La ricerca applicata traduce le astrazioni della crittografia, dei modelli di attacco e della teoria dell'informazione in protocolli e processi scalabili e misurabili. In questa sezione verranno trattati alcuni fenomeni di applicazione della ricerca di base per definirne la fase dell'innovazione.

2.2.1 EDR & XDR - learning at scale

I sistemi *EDR* e *XDR* sono l'evoluzione moderna del modello proposto da Denning. *L'Endpoint Detection and Response (EDR)* è una tecnologia della cybersecurity progettata per monitorare e proteggere in modo continuo i singoli dispositivi come workstation, tablet, smartphone e server. Questi strumenti permettono ai diversi team di sicurezza di rilevare, analizzare e rispondere rapidamente alle minacce informatiche a livello di endpoint. *L'Extended Detection and Response (XDR)* è l'evoluzione dell'EDR, cioè una piattaforma unificata che permette di monitorare tutta l'infrastruttura digitale di un'organizzazione. Questi sistemi tramite l'integrazione con l'intelligenza artificiale e il modello di apprendimento a larga scala migliorano incredibilmente la loro efficienza, rendendo il processo di rilevamento delle minacce scalabile. Ad esempio, la combinazione di EDR con l'intelligenza artificiale permette di esaminare migliaia di endpoint rimanendo sensibile e robusto, riducendo il numero di falsi positivi e aumentando l'efficacia nell'analisi delle vere minacce. Il *learning at scale* impatta profondamente sull'architettura del sistema permettendo di:

- evitare la centralizzazione di dati grezzi e i conseguenti costi di rete e storage;
- alleggerire gli host da modelli che gravano su CPU e RAM.

Nel contesto del XDR, guardiamo uno spazio più vasto che tiene sotto controllo tutto lo stack di sicurezza aziendale e non soltanto gli endpoint dei singoli dispositivi. Più dati vengono gestiti, più il tempo di risposta diminuisce e migliora il processo di apprendimento durante la produzione. Il secondo valore aggiunto del *learning at scale* rispetto l'utilizzo di questi dispositivi è la capacità di correlare eventi rilevati in domini diversi e apparentemente separati ma in realtà comunicanti evitando la duplicazione e la corretta ricostruzione dell'incidente. Il risultato pratico è che migliaia di notifiche slegate si comprimono in pochi incidenti ben strutturati, con priorità e azioni suggerite.

2.2.2 SOAR e automazione della risposta

Il modello di Denning ha formalizzato il processo di rilevazione e notifica di un incidente di sicurezza, senza estendere il ragionamento sulla risposta. Sulla base di questo modello sono state introdotte diverse tecnologie che implementano la risposta, una delle più importanti è il *SOAR* (*Security Orchestration, Automation and Response*), cioè un sistema progettato per integrare e orchestrare strumenti di sicurezza separati, automatizzare attività operative ripetitive e coordinare le risposte agli incidenti tramite regole predefinite e strutturate all'interno di un *Security Operation Center*. L'automazione di queste piattaforme è abilitata dalle *playbook*, sequenze strutturate di azioni e decisioni che, sotto determinate condizioni, definiscono il flusso operativo e standardizzano le procedure di risposta. Il problema architetturale di questo sistema però è dato dalla staticità delle regole che governano le *playbook*, che permettono di eseguire azioni predefinite indipendentemente dal contesto. Per superare questi limiti diversi contributi in letteratura propongono modelli di risposta cost-aware, dove i parametri dello strumento vengono aggiornati iterativamente a partire dai casi storici chiusi e dalla revisione post-incidente tramite una funzione di costo associata alle azioni di mitigazione da compiere. Questo permette di evolvere il motore decisionale che Denning descriveva come regole statiche, in criteri dinamici di decisione su come intervenire, con che intensità e quale grado di autonomia rispetto alla supervisione umana.

2.2.2 PQC – Migration at scale

Abbiamo parlato dell'impatto degli algoritmi post-quantum nella basic research, soffermandoci sulla potenza di calcolo e il cambio di paradigma a livello di difesa e standardizzazione nel mondo della cybersecurity. Il passaggio dalla teoria alla pratica richiede l'affrontare una serie di sfide che non emergono nel contesto della ricerca teorica. La migrazione PQC deve confrontarsi con la complessità delle infrastrutture reali, caratterizzate da eterogeneità tecnologica, vincoli legacy, requisiti di performance e necessità di continuità operativa. Il primo problema sostanziale da affrontare sono le caratteristiche significativamente diverse tra gli algoritmi PQC e i suoi predecessori, che impattano profondamente nelle infrastrutture di sistema e nell'adozione a larga scala. Pertanto, un pilastro fondamentale per la ricerca applicata sulla migrazione PQC è il concetto di crypto-agility, ovvero la capacità di un sistema di adattarsi a cambiamenti negli algoritmi crittografici senza richiedere modifiche architetturali sostanziali. Questo concetto viene sviluppato in parallelo con gli schemi ibridi che rappresentano una strategia di transizione promettente. L'obiettivo è quello di combinare algoritmi crittografici classici e post-quantum, garantendo un doppio livello di sicurezza e di 'paracadute' nel caso uno dei due algoritmi non bastasse o non fosse supportato. In questo modo, con la presenza di un attaccante, bisognerebbe rompere entrambi gli algoritmi per compromettere la comunicazione cifrata. L'esempio più comune di schema ibrido è la chiave crittografica classica di Diffie-Hellman *X25519*, in combinazione con l'algoritmo di crittografia post-quantum *Kyber*. L'adozione degli algoritmi post-quantum è velocizzata dal *National Institute of Standards and Technology (NIST)* degli Stati Uniti, tramite la pubblicazione nel 2024 di tre algoritmi di crittografia progettati per proteggere i sistemi attuali contro gli attacchi futuri con tecnologie quantistiche. Proprio per questo nello stesso anno, Google ha prima implementato il supporto sperimentale per TLS con *Kyber* ibrido, per poi passare a *ML-KEM* introdotto dal NIST come uno dei tre algoritmi per la protezione.

2.3 Fase precompetitiva

In questo paragrafo tratteremo la fase precompetitiva del nostro modello lineare dell'innovazione concentrandoci su come la ricerca applicata, la sperimentazione e la validazione tecnologica diventino fondamentali per trasformare l'elaborazione di prototipi in soluzioni trasferibili al mercato. Inoltre, parleremo di alcune delle startup più interessanti nel contesto di mercato della cybersecurity e per la nostra analisi.

2.3.1 Mondo militare nella cybersecurity

Il settore militare è uno dei principali incubatori della ricerca per il mondo della cybersecurity. Fin dalla Seconda guerra mondiale, le competenze sviluppate per la segretezza strategica in ambito militare sono state la scintilla per l'evoluzione informatica e la sua difesa. Proprio per questa presenza fondamentale della sicurezza informatica nei centri di difesa, sono nati ambienti, laboratori e programmi in cui la ricerca non è orientata al business ma all'applicazione e al trasferimento tecnologico. Prendendo come esempio gli Stati Uniti, agenzie come DARPA (*Defense Advanced Research Projects Agency*) sono il motore dell'evoluzione cyber. La DARPA è un'agenzia governativa del dipartimento della difesa degli Stati Uniti d'America incaricata dello sviluppo di nuove tecnologie per uso militare. Finanzia programmi su software verification, supply chain security, attacchi simulati e programmi di resilienza di rete che vengono poi trasferiti a spin-off o startup attraverso partnership con università o gare. Una delle scoperte più interessanti fu ARPANET, nonché la prima rete a commutazione di pacchetto su scala geografica e predecessore dell'attuale Internet. In Europa la NATO (*North Atlantic Treaty Organization*) ha istituito il NATO Industry Cyber Partnership, per collaborare con aziende del settore cybersecurity con l'obiettivo di trovare soluzioni innovative nel cyberspazio, aumentare la consapevolezza delle minacce informatiche per la NATO e i suoi partner e rafforzare la resilienza e capacità di protezione delle informazioni. Fortinet, leader globale di soluzioni e servizi di cybersecurity, partecipa a questa iniziativa dal 2016 dimostrando come il mondo istituzionale e quello aziendale collaborino per il progresso tecnologico. Un esempio emblematico e più maturo di continuità tra ricerca militare e mondo commerciale in questo ambito è Israele, che con le unità cyber dell'IDF alimenta il flusso costante verso startup e centri accademici. Infatti, molte delle start up e realtà oggi leader del mercato sono state fondate da ex membri dell'IDF, e alcune di queste verranno trattate più approfonditamente di seguito.

2.3.2 Prompt Security

Prompt Security è una start up fondata nel 2023 da Itamar Golan e Lior Drihem, entrambi con un background nell'Israel Defense Forces, Check Point e Orca Security, che si è fin da subito posizionata come pioniera nella protezione runtime delle applicazioni basate su modelli di linguaggio (LLM) e IA generativa (GenAI) nelle aziende; argomenti centrali nel mondo della cybersecurity. Il loro obiettivo è chiaro e mirato, le aziende integrano, attraverso team di sviluppo, modelli linguistici di grandi dimensioni senza misure di sicurezza, esponendo dati sensibili e aumentando i rischi per la sicurezza. L'offerta proposta da Prompt Security è una piattaforma all-in-one che protegge le aziende dall'utilizzo e dallo sviluppo di app tramite intelligenza artificiale nei diversi settori, avendo una visione completa ed in tempo reale dell'organizzazione e dei punti di contatto. *"L'intelligenza artificiale generativa si sta rapidamente infiltrando nelle aziende e questo comporta un mondo di nuovi rischi ad alto valore"*, ha dichiarato Itamar Golan, CEO e co-fondatore di Prompt Security. *"I dipendenti sono fortemente incentivati a condividere i dati aziendali con gli strumenti di intelligenza artificiale di generazione, che spesso vengono addestrati sui dati e possono farli trapelare in seguito. Allo stesso modo, quando le organizzazioni integrano l'intelligenza artificiale nei loro prodotti, si espongono a una serie di sfide per la sicurezza, tra cui modelli manipolati da malintenzionati e contenuti generati non sicuri o che violano il copyright. Eppure, nonostante tutti i rischi, l'intelligenza artificiale genera un valore immenso e adottarla non è una questione di scelta, ma è la chiave per la sopravvivenza del business"* (Prompt Security, 2024).

L'offerta di Prompt Security è completa:

- Sicurezza, attraverso l'ispezione delle risposte dell'AI, dei dati sistematici e la loro estrazione;
- Governance, controllo di tutti gli strumenti AI nell'azienda e delle policy applicate;
- Privacy, rileva e nasconde i dati sensibili.

Nel 2024 ha ricevuto un round di investimento di \$5M guidato da Hetz Ventures con la partecipazione di Four Rivers e altri CISO di aziende come Elastic e Dolby. Un'altra importante milestone significativa è l'acquisizione da parte di SentinelOne annunciata il 5 agosto 2025, prevista per il Q3 2026 (Prompt Security, 2024). Questa è una mossa strategica da parte di SentinelOne che estende la sicurezza IA-native ad endpoint e cloud. Prompt Security non è interessante solo per l'idea e la realizzazione rapida e concreta, ma dimostra come startup innovative accelerino la scalabilità dell'AI nella cybersecurity.

2.3.3 Pentera

Pentera nasce nel 2015, sotto il nome di Pcysys, da un'idea di due ricercatori Arik Liberzon e Arik Faingold; ed è stata resa scalabile all'arrivo del CEO Amitai Ratzon nel 2017. Il loro obiettivo è quello di individuare e validare percorsi critici a livello di sicurezza aziendale. Nel 2021 cambia il nome in *Pentera* e introduce *Ransomware Ready* un modulo che permette di replicare in ambienti di produzione le stesse sequenze operative dei ceppi di ransomware più distruttivi per verificare come un attaccante riuscirebbe a muoversi tra gli asset critici delle aziende cliente, comportamento noto anche come *lateral movement*. Questa esigenza nasce dalla crisi ransomware che in quel periodo storico ha colpito numerose aziende, in particolare negli Stati Uniti. Pentera è nota per aver costruito le categorie *Automated Security Validation (ASV)* ed *Exposure Management*, tramite una piattaforma che simula attacchi reali in ambienti on-premise, cloud ed ibridi, identificando i divari di sicurezza e riducendo l'esposizione ad attacchi cyber tramite test continuativi. Fino a quel momento, le analisi erano affidate a società di consulenza, tramite hacker etici, che misuravano il rischio al momento del controllo e non in maniera costante e continuativa. Questo approccio proattivo all'analisi e al controllo è diventato ad oggi il marchio di fabbrica dell'azienda e ha portato un interesse costante da parte di numerosi investitori. Dal cambio di rotta Pentera ha raccolto \$210M, \$150M in un round di Serie C nel 2022 e \$60M in un round di Serie D nel 2025, da fondi come K1 Investment Management, Awz Ventures e Blackstone (Pentera, 2022; 2025). Inoltre, nel 2025 Pentera ha acquisito DevOcean per circa \$30M, startup israeliana specializzata in AI-powered remediation su larga scala, potenziando la propria piattaforma con la remediation automatica (Calcalist Tech, 2025).

2.3.4 PQShield

PQShield è una spin-out dell'Università di Oxford fondata nel 2018 da Ali El Kaafaarani (CEO), rappresenta la crescente transizione da paper accademici a soluzioni commerciabili, rappresentando applicazioni sul post quantum scalabili in ecosistemi enterprise. La startup di Oxford si posiziona come leader nel post-quantum cryptography, fornendo un framework ibrido che integra standard consolidati a livello di crittografia con algoritmi quantum-safe. Il loro obiettivo è quello di evitare migrazioni disruptive per settori ad alta esposizione come security, automotive, IoT e finanza. PQShield ha sviluppato il primo chip di test al silicio per crittografia *PQC* completamente funzionale, migliorano la conformità del settore ai nuovi standard NIST. Nel comunicato stampa viene dichiarato: "*PQShield ha progettato e costruito il primo chip di test al silicio per crittografia post-quantistica completamente funzionante per supportare la conformità ai nuovi standard NIST PQC. Secondo il comunicato, il chip di test fornisce ai fornitori di semiconduttori gli strumenti necessari per implementare soluzioni PQC sicure mentre il settore passa dalla preparazione al rispetto dei requisiti di conformità. Ciò consente una valutazione dettagliata del consumo energetico, delle prestazioni e delle contromisure dell'analisi del canale laterale (SCA), il tutto in un ambiente reale.*" (Stubbs, 2024; The Quantum Insider, 2024). L'offerta dell'azienda è ampia ed include un set di prodotti diversificato:

- UltraPQ Suite, gamma completa di prodotti per l'implementazione di crittografia post-quantum;

- PQPlatform-TrustSys, Root-of-Trust quantum-resilience;
- PQCryptoLib-Embedded, soluzione post-quantum per firmware.

Complessivamente, PQShield ha raccolto circa \$64M in tre round di finanziamento fino al 2025:

- Round seed da \$7M nel 2020, da investitori come Kindred Capital e Oxford Sciences Innovation (Jarvis, 2024).
- Round di serie A da \$20M nel luglio 2024, con la partecipazione di investitori già presenti come Oxford Science Enterprise (PQShield, 2022);
- Round di serie B da \$37M, guidato dalla società di venture capital Addition e nuovi investitori come Braavos Capital, Legal & General e Chevron Technology Ventures (PQShield, 2024c).

2.3.5 Cylock

Cylock è una startup italiana fondata nel 2021 a Roma da un team di hacker etici altamente specializzati, specializzata in *vulnerability assesment* accessibile anche alle PMI. La loro mission è garantire alle aziende un ambiente digitale sicuro, aiutandole a proteggere i dati sensibili e mantenere la fiducia dei clienti. Hanno brevettato il software EVA per individuare in maniera accurata le vulnerabilità dei sistemi aziendali. Integrano nel loro software funzioni di intelligenza artificiale, sviluppate interamente dal loro team specializzato, per permettere di simulare migliaia di attacchi mirati per testare sistemi IT, reti, siti web, end point, app ed email aziendali mantenendo un costo contenuto del servizio. Il cliente quindi non si deve appoggiare ad un team specializzato che si occupa di penetration test, ma tramite il software “click & play” e l’uso dell’AI può adoperare in autonomia l’attività di vulnerability assessment. Infatti, il sistema utilizza algoritmi per l’autoconfigurazione e la riproduzione di attacchi in modo non invasivo e sicuro, generando report certificati validi standard come ISO 27001, NIS2 e GDPR; in maniera automatica tramite l’integrazione di modelli LLM. Ha ricevuto in totale 818k€ di investimenti con un Pre Seed Round di 318 k€ da parte di 5 investitori e un seed round di 500 k€ con *Scientifica Venture Capital* come lead investor (Crunchbase, 2025). Le prospettive di crescita della startup sono notevoli, è stata inserita tra le top 5 startup di cybersecurity agli Italian Security Awards 2025; il premio promosso da *SecurityOpenLab* per valorizzare le realtà nel panorama nazionale più innovative ed affidabile. Inoltre, è stata premiata dal Governo britannico con il prestigioso premio “UKPA 2024” come migliore startup cybersecurity del 2024 (Cylock, 2025). Cylock è un ottimo esempio della scalabilità dell’AI nel mondo della cybersecurity fondata nel nostro territorio.

3. La fase competitiva nella cybersecurity

Questo capitolo analizza la fase competitiva del mercato della cybersecurity, con l'obiettivo di costruire una cornice coerente per interpretare le dinamiche evolutive del settore e, successivamente, derivarne implicazioni concrete per un *Managed Security Service Provider* che opera prevalentemente nel segmento PMI e mid-market, come Nais.

Il mercato della cybersecurity è un settore in grande crescita globale, alimentata da tre driver strutturali citati nel Capitolo 1:

- Continua evoluzione della digitalizzazione dei dati e conseguente dipendenza da infrastrutture cloud;
- Evoluzione delle minacce;
- Fattori esogeni come le normative internazionali ed europee che trasformano la sicurezza da scelta discrezionale a requisito di governance e resilienza.

In questa sezione si farà riferimento alle stime di mercato di Statista Market Insights per descrivere l'ordine di grandezza del settore e la ripartizione per segmenti. In particolare, secondo tale fonte, i ricavi stimati per il mercato globale della cybersecurity sono pari a 196.51 miliardi di dollari nel 2025, con un tasso di crescita annuale composto del 5,94% nel periodo 2025–2030 e un valore previsto di 265.17 miliardi di dollari nel 2030 (Statista Market Insights, 2025a).

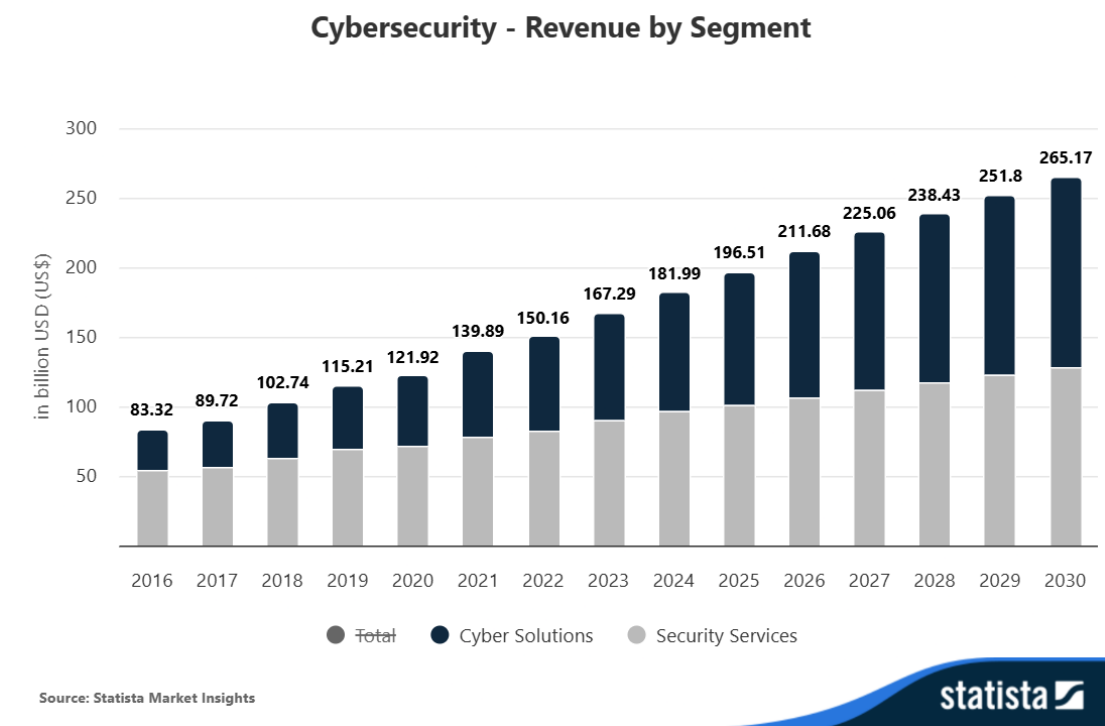


Figura 3.1: [Cybersecurity – Revenue by Segment, Statista Market Insight](#)

Per coerenza espositiva, il capitolo adotta una segmentazione macro in due aree, coerente con le tassonomie più diffuse nelle analisi di settore:

- Cyber Solutions: Cloud Security, Network Security, Data Security, Endpoint Security, Identity & User Security;
- Managed Security Services.

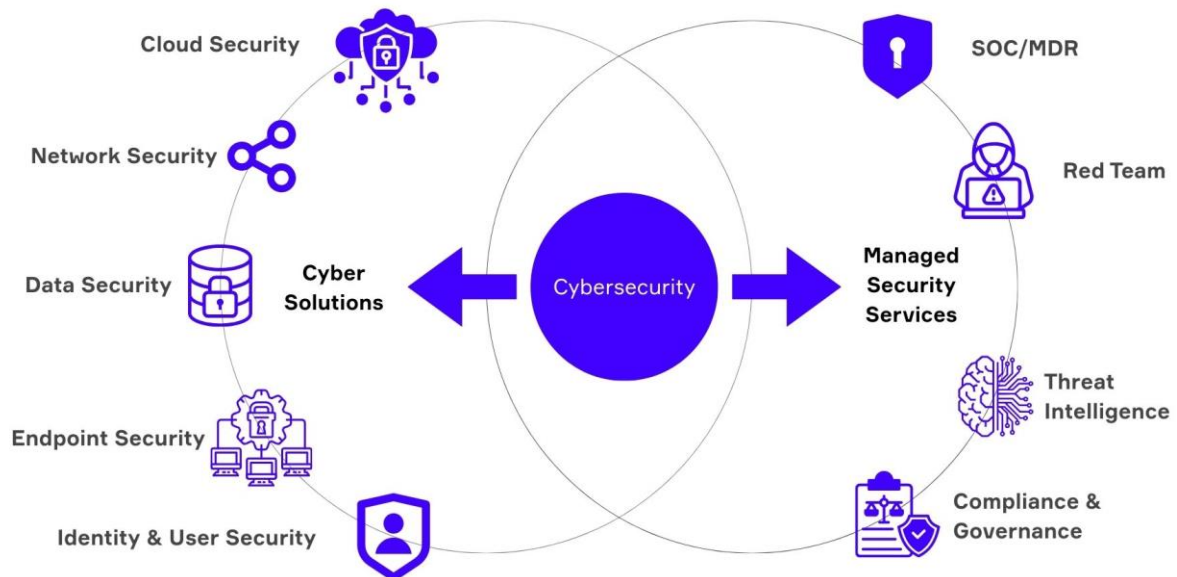


Figura 3.2 – Ecosistema della cybersecurity

Sulla base di questa cornice, nel capitolo verranno inizialmente analizzate le principali tecnologie del paradigma delle soluzioni frammentate, definiti i *Managed Security Services* e affrontati i principali vincoli e limiti strutturali del paradigma. Nella seconda parte del capitolo, invece, verrà analizzato l'emergere del nuovo paradigma delle piattaforme multi-dominio e applicati framework come l'analisi delle cinque forze di Porter e curve ad S per il confronto evolutivo dell'ecosistema cyber. Infine, verranno analizzate le implicazioni dirette per un *Managed Security Service Provider* e definiti il perimetro e la domanda di mercato di riferimento.

3.1 Cyber Solutions – Le varie tecnologie nel mondo della cybersecurity

3.1.1 Cloud Security

La migrazione verso servizi cloud ha ridefinito il perimetro della cybersecurity: applicazioni, identità, dati e carichi di lavoro si spostano in ambienti dinamici e distribuiti, aumentando la superficie d'attacco e incrementando la probabilità di errori di configurazione e nei controlli. In questo scenario, la cloud security è rappresentata dall'insieme di controlli e processi necessari a governare in modo continuo configurazioni, identità, workload e dati in ambienti IaaS/PaaS/SaaS, secondo il modello di responsabilità condivisa tra fornitore e cliente. Un elemento caratterizzante del contesto competitivo è la forte concentrazione del mercato cloud infrastrutturale: i tre hyperscaler principali (Amazon Web Services, Microsoft Azure e Google Cloud) pesano congiuntamente su una quota maggioritaria della spesa enterprise, con effetti diretti su standard tecnologici, API, telemetrie disponibili e modelli di controllo.

Ci sono diversi tipi di servizi cloud infrastrutturale:

- Software-as-a-Service (SaaS), eroga applicazioni interamente ospitate ed eseguite sui server dei provider (es. Google Workspace, Slack, Microsoft 365);
- Platform-as-a-service (PaaS), mette a disposizione un ambiente gestito su cui il cliente può sviluppare ed eseguire le proprie applicazioni senza gestire l'infrastruttura sottostante (es. Azure App Service, Google App Engine);
- Infrastructure-as-a-Service (IaaS), fornisce ai clienti l'hardware e le infrastrutture di connettività remota necessari per carichi di lavoro e sistemi informatici (es. Microsoft Azure, Google Compute Engine, Amazon Web Services).

La progressiva migrazione verso questi modelli ha reso necessario lo sviluppo della *cloud security*, una disciplina della cybersecurity dedicata alla protezione degli ambienti cloud computing. Essa comprende l'insieme di tecnologie, protocolli e pratiche consolidate volte a proteggere dati, applicazioni e infrastrutture cloud. Questo dominio permette inoltre di mitigare i rischi connessi a configurazioni errate delle infrastrutture, evoluzione e distribuzione degli attacchi informatici e violazioni di conformità normativa.

Le tecnologie del dominio sono diverse e le più importanti includono:

- Cloud Security Posture Management (CSPM), automatizza e unifica l'identificazione e la correzione di configurazioni errate negli ambienti cloud, garantendo monitoraggio continuo della postura di sicurezza;
- Cloud Workload Protection Platform (CWPP), soluzione di sicurezza progettata per proteggere i workload in esecuzione nel cloud;
- Cloud Access Security Broker (CASB), controllano e governano l'uso delle applicazioni Software-as-a-Service tramite l'introduzione di policy tra utenti e servizi cloud;
- Secure Service Edge (SSE), architettura che permette di convergere funzionalità di sicurezza erogate interamente via cloud per applicare policy di sicurezza uniformi;
- Secure Access Service Edge (SASE), è un'architettura che estende SSE con funzionalità di rete su larga scala. Infatti, si colloca all'intersezione tra il cloud e la network security.

Diverse analisi di mercato stimano come questo sia un settore in forte crescita con una dimensione che si colloca intorno ai 40 miliardi di dollari, con un tasso di crescita annuo stimato del 10-13% fino al 2030 (Mordor Intelligence, 2025; MarketsandMarkets, 2025a).

Cloud-Native Application Protection Platform

Negli ultimi anni, il modello di cloud security si sta evolvendo verso piattaforme unificate di protezione cloud-native, note come *Cloud-Native Application Protection Platform* (CNAPP), che integrano le principali capability elencate in precedenza, tipicamente *CSPM*, *CWPP*, *CIEM*, spesso arricchite da funzionalità di scansioni di immagini e container e prioritizzazione del rischio. Il valore competitivo di questa convergenza risiede nella riduzione del numero di tecnologie utilizzate per la protezione e nella correlazione di segnali eterogenei per produrre priorità operative e workflow di remediation più rapidi. La *Market Guide for Cloud-Native Application Protection Platforms 2025* di Gartner evidenzia come queste soluzioni stiano sempre di più integrando l'intelligenza artificiale generativa, *machine learning* e *large language model* (LLM) per ridurre l'overhead di gestione, offrire raccomandazioni di policy e migliorare l'analisi dei pattern per il rilevamento e la risposta alle minacce nell'ordine di ridurre significativamente il *Mean Time To Response* (MTTR). La spesa per le CNAPP, secondo Gartner, attingerà fondi da diversi segmenti della cyber security con una *market size* stimata nel 2024 di 11.33 miliardi di dollari (Gartner, 2025a).

I principali provider di soluzioni CNAPP elencati nella Tabella A.1 in *Appendice*, sono per la maggior parte leader in diversi settori della cyber security. Questo posizionamento riflette una tendenza strutturale del mercato verso la *platformization* delle soluzioni tecnologiche e dell'erogazione di servizi gestiti di cybersecurity.

3.1.2 Network Security

La *network security* comprende l'insieme delle misure volte a proteggere l'infrastruttura di rete da accessi non autorizzati, usi impropri o violazioni, garantendo i principi della triade CIA (*Confidentiality, Integrity, Availability*). Essa permette di garantire un'infrastruttura sicura affinché dispositivi, applicazioni e utenti possano operare in modo protetto.

L'accelerazione digitale ha portato ad un ampliamento della superficie d'attacco, dalle reti locali e geografiche fino ad arrivare all'Internet of Things (IoT) e al cloud computing. Ogni nuova implementazione tecnologica introduce inevitabilmente una potenziale vulnerabilità aggiuntiva, evidenziando la necessità di framework di sicurezza di rete strutturati e aggiornati. Stime del mercato della network security mostrano come il settore nel 2024 ha generato ricavi pari a 24.61 miliardi di dollari, con una previsione di 27.19 miliardi di dollari per il 2025. Le proiezioni di mercato (Figura 3.3) mostrano una crescita incrementale, con un tasso di crescita annuo composto previsto dell'8,02% tra il 2025 e il 2030 (Statista Market Insight, 2025b).

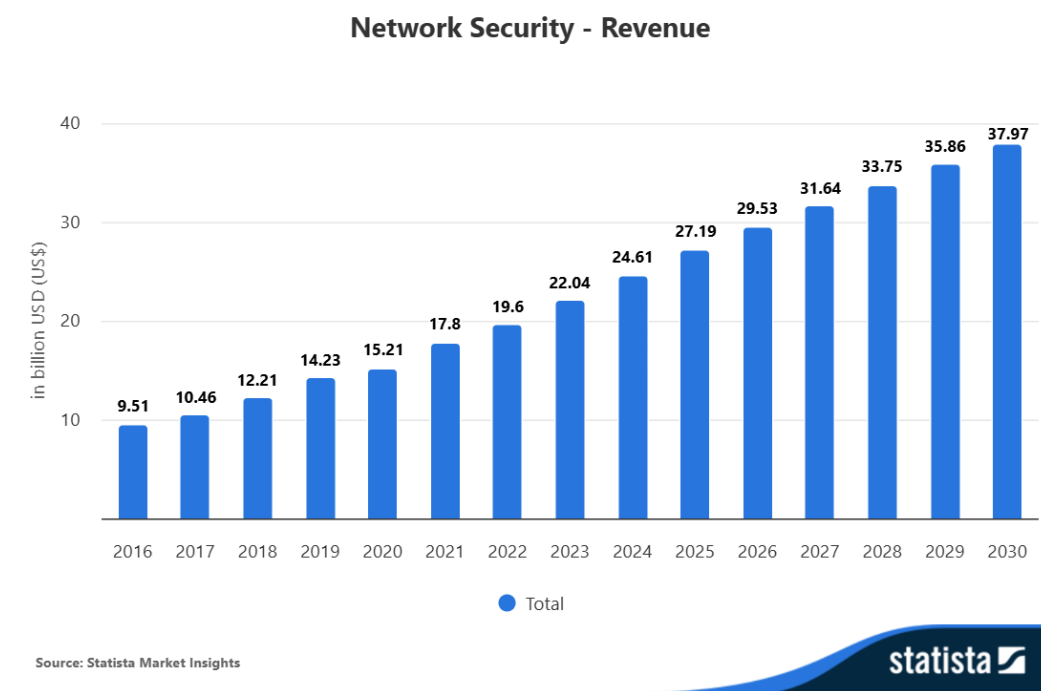


Figura 3.3: [Network Security – Revenue, Statista Market Insights](#)

Le principali tecnologie della *network security* sono:

- Next-Generation Firewalls (NGFW), firewall *stateful* di nuova generazione che eseguono ispezione profonda del traffico (*Deep Packet Inspection*), riconoscono le applicazioni e integrano funzioni come IPS, URL filtering e SSL inspection in un'unica piattaforma;
- Secure Access Service Edge (SASE), architettura cloud-delivered che converge connettività e sicurezza di rete in un unico servizio distribuito a livello globale;
- Zero Trust Network Access (ZTNA), modello di accesso basato su identità e contesto che stabilisce connessioni a livello di singola applicazione, applicando il principio del

“*never trust, always verify*” sostituendo l’accesso da remoto con una Virtual Private Network (VPN) tradizionale offrendo un accesso più sicuro, granulare e scalabile, in linea con i modelli di lavoro ibrido e le esigenze di sicurezza moderne;

- Intrusion Detection/Prevention Systems (IDS/IPS), sonde di rete che analizzano il traffico tramite firme e analisi comportamentale per rilevare (IDS) e, se in linea, bloccare (IPS) tentativi di attacco o traffico malevolo;
- Network Detection and Response (NDR), piattaforme che effettuano ispezione profonda del traffico e usano analisi avanzata e *machine learning* per individuare anomalie e movimenti laterali, generando allarmi e *playbook* di risposta.

Al fine di identificare le dinamiche competitive del dominio e i principali operatori di mercato, ricorreremo ad un benchmark di settore basato sulle tecnologie *Hybrid Mesh Firewall* (Figura 3.4) e *SASE Platform* (Figura 3.5), con l’ausilio dei quadranti di Gartner.



Figura 3.4: Magic Quadrant for Hybrid Mesh Firewall , Gartner 2025



Figura 3.5: Magic Quadrant for SASE Platforms, Gartner 2025

Dall'analisi dei due quadranti emergono come leader di mercato ricorrenti Palo Alto Networks e Fortinet mentre Check Point si posiziona diversamente in base al servizio erogato. Cisco si posiziona come azienda in forte crescita nel settore della network security, pur essendo un player storico del segmento. Altri due player che meritano di essere citati sono:

- Zscaler, con la sua soluzione *Zero Trust Exchange* per SASE, con un focus particolare sul cloud;
- CrowdStrike, con la sua soluzione *Falcon* per NDR, AI-native con una forte componente verso la scalabilità.

Rispetto all'impatto dell'intelligenza artificiale nel dominio, il tasso di adozione è in forte crescita perché permette di passare da un approccio reattivo ad uno proattivo favorendo la gestione di volumi esponenziali di dati senza un aumento lineare del numero di risorse umane. Tra i principali vantaggi dell'integrazione troviamo:

- Rilevamento e risposta alle minacce in tempo reale, gli algoritmi di intelligenza artificiale possono analizzare i dati e rilevare anomalie quasi istantaneamente;
- Analisi comportamentale attraverso algoritmi che acquisiscono dati e comprendono approfonditamente il normale comportamento della rete;
- Analisi predittiva e intelligence sulle minacce, modelli che si integrano con database di comportamenti dannosi noti;
- Scalabilità ed efficienza;
- Integrazione con le piattaforme SIEM, per stabilire la priorità degli avvisi e selezionare le criticità più rapidamente, e SOAR per prendere soluzioni dettagliate sulla risposta agli incidenti.

3.1.3 Data Security

La *data security* è la disciplina che protegge i dati lungo tutto il loro ciclo di vita, indipendentemente dalla loro posizione e il contesto in cui risiedono. Con la digitalizzazione dei processi di business è diventato necessario garantire che le informazioni aziendali rimangano protette e disponibili, come condizione abilitante per la continuità operativa in diversi settori. Secondo Statista Market Insights, il mercato globale della *data security* ha ricavi pari a 14.7 miliardi di dollari nel 2025 (Statista Market Insights, 2025c).

Le principali categorie tecnologiche del segmento includono:

- Data Encryption, sfrutta algoritmi crittografici per proteggere dati a riposo e in transizione, mantenendo illeggibili le informazioni senza accesso autorizzato;
- Data Loss Prevention (DLP), una delle soluzioni più importanti che permette di prevenire l'esfiltrazione di dati sensibili tramite monitoraggio continuo di endpoint, reti, sistemi di posta elettronica e ambienti cloud;
- Data Security Posture Management (DSPM), piattaforme che monitorano continuamente gli ambienti di lavoro per analizzare permessi, configurazioni e livello di esposizione di rischio dei dataset aziendali;
- Data Classification, categorizzazione dei dati per sensibilità e priorità;
- Backup and Recovery, soluzioni di backup per il ripristino dei dati dopo gli incidenti.

3.1.4 Endpoint Security

L'Endpoint Security comprende l'insieme di soluzioni, tecnologie e processi che proteggono i dispositivi collegati all'ambiente di rete aziendale (anche detti endpoint) come workstation, server, dispositivi mobili e in alcuni contesti asset OT. L'obiettivo è quello di prevenire, rilevare e bloccare malware, ransomware e attività anomale sui dispositivi di estremità, prima che l'attacco possa propagarsi sul resto dell'infrastruttura. Le stime di Statista Market Insights per il mercato dell'Endpoint Security riportano ricavi pari a 15.41 miliardi di dollari nel 2025 con tasso di crescita annuale del 7,17% fino al 2030 (Statista Market Insights, 2025d).

Le principali tecnologie dell'Endpoint Security sono:

- Endpoint Protection Platform, è una soluzione di sicurezza integrata progettata per proteggere gli endpoint, concentrandosi sulla prevenzione delle minacce piuttosto che sulla risposta agli incidenti. La piattaforma unifica diverse tecnologie come gli antivirus di nuova generazione (NGAV), strumenti di prevenzione della perdita di dati (DLP), sistemi di prevenzione delle intrusioni, firewall e funzionalità di gestione di vulnerabilità e patch
- Endpoint Detection and Response (EDR), è il cuore operativo per i servizi MDR. Permette di raccogliere costantemente dati da tutti gli endpoint, analizzarli e può rispondere automaticamente per prevenire o ridurre al minimo i danni causati dalle minacce individuate.
- Extended Detection and Response (XDR), raccoglie, normalizza e correla i dati su una varietà di livelli di sicurezza (endpoint, firewall, e-mail, server, carichi di lavoro cloud e rete generale)

L'importanza della combinazione di queste tre tecnologie sta nella copertura di tre livelli complementari: prevenzione, rilevamento/risposta e correlazione. Per l'evoluzione della cybersecurity, fino ad arrivare ai moderni SOC e MDR, queste tre tecnologie permettono di avere una visione a 360 gradi degli endpoint di un'azienda. Siamo passati dal tradizionale antivirus installato in locale a un confronto di file 24/7 che capisce il comportamento dell'endpoint nel suo insieme. Il prossimo step di questo segmento è segnato dall'utilizzo di piattaforme cloud e dall'intelligenza artificiale. Il cloud permette di raccogliere un'enorme mole di dati su processi, file e pattern di attacco che vengono usati per addestrare e aggiornare continuamente i modelli di machine learning. Inoltre, lo spazio cloud permette a queste tecnologie di spostare il peso computazionale al di fuori dell'endpoint rendendo più veloci le analisi complesse senza gravare sulla CPU e rendendo più semplice l'erogazione del servizio al cliente da parte del distributore. In particolare, una tecnologia come l'XDR riceve un consolidamento della telemetria e correlazione cross-dominio, con limite: dipende dalla qualità di integrazioni e data layer con la combinazione di ambienti cloud e intelligenza artificiale, permettendo di monitorare e correlare in modo efficiente i log dai diversi sistemi aziendali con una risposta immediata e accurata. La potenza dell'intelligenza artificiale permette di avere un numero limitato di incidenti, già correlati, con arricchimento di informazioni che facilitano enormemente l'analisi di un esperto per la risposta al rischio o addirittura compiono azioni di isolamento e blocco del dispositivo automatiche.

Per guidare l'analisi sui principali player nel settore utilizzeremo il Magic Quadrant di Gartner sul Endpoint Protection Platforms, che rappresenta l'unità di misura per la leadership nel segmento dell'endpoint security.



Figura 3.6: Magic Quadrant for EPP – Fonte: Gartner, 2025

Di seguito l'analisi dei principali leaders del segmento:

Vendor / Piattaforma	Approccio e AI	Feature principali (EPP/EDR/XDR)	Weakness tipiche
CrowdStrike – Falcon Platform	Soluzione cloud native con motori di machine learning e analisi comportamentale su grande volume di telemetria endpoint	Unifica antivirus di nuova generazione, EDR, threat hunting e threat intelligence in un agente leggero con console centralizzata	Prezzo percepito come elevato per realtà piccole, piattaforma ricca ma complessa da padroneggiare, alcuni falsi positivi e forte dipendenza dal backend cloud
Microsoft – Defender for Endpoint	Piattaforma EPP EDR XDR integrata nell'ecosistema Microsoft con uso estensivo di modelli di machine learning nel cloud	Integrazione nativa con Windows e Microsoft 365, combinazione di prevenzione e rilevamento con risposta automatizzata e forte rapporto qualità prezzo se inclusa nelle suite	Portali e interfacce non sempre omogenei, necessita di tuning per ridurre il rumore di alert, gestione più complessa in ambienti misti non Microsoft
SentinelOne – Singularity	Piattaforma endpoint con intelligenza artificiale sia lato agente sia nel backend cloud orientata a prevenzione e risposta autonoma	EPP più EDR più XDR con forte automazione nella risposta, funzioni di rollback, isolamento macchina e ricostruzione automatica della sequenza di attacco	La console e le funzionalità avanzate possono risultare complesse inizialmente, richiede lavoro di tuning sugli alert, alcune aree funzionali percepite meno mature da parte di alcuni utenti
Palo Alto Networks – Cortex XDR (endpoint)	EPP EDR XDR integrato con firewall e soluzioni cloud Palo Alto con motore analitico basato su algoritmi avanzati di correlazione	Agente endpoint con antivirus avanzato e rilevamento comportamentale, forte integrazione con infrastruttura di rete e cloud del vendor, supporto a servizi MDR	Deployment e integrazione più complessi se non si usa già lo stack Palo Alto, segnalazioni di falsi positivi e necessita di configurazione accurata, alcune limitazioni dell'agente su piattaforme specifiche
Trend Micro – Apex One	Piattaforma single agent che combina EPP ed EDR con algoritmi di machine learning e analisi comportamentale	Protezione contro malware exploit e ransomware, virtual patching tramite integrazione con gestione delle vulnerabilità, opzioni SaaS e on premise con console centralizzata	Consumo di risorse percepito elevato quando tutti i moduli sono attivi, curva di apprendimento su console e policy, storico di vulnerabilità critiche sulla componente di management che richiede attenzione al patching
Sophos – Intercept X	Piattaforma EPP con motore di deep learning e tecnologie specifiche contro ransomware e exploit	Difesa multilivello con moduli anti exploit anti ransomware e controllo applicazioni, funzioni di rollback dei file cifrati, gestione via Sophos Central e possibilità di servizio MDR	Impatto sulle prestazioni su endpoint meno recenti durante scansioni e aggiornamenti, configurazione delle esclusioni delicata, alcune funzionalità avanzate disponibili solo nelle edizioni di licenza più costose

3.1.5 Identity & User Security

Per Identity & User Security include l'insieme di controlli che riducono il rischio legato all'uso delle identità digitali e ai canali di interazione dell'utente (in particolare posta elettronica e strumenti di collaborazione). Il micro-obiettivo di proteggere il singolo utente si riflette nella tutela di tutta l'azienda, con più livelli di sicurezza per impedire che una minaccia passi dall'essere localizzata a diffusa nell'ambiente lavorativo. In particolare, in questo contesto parliamo di *Identity and Access Management (IAM)* per identificare la disciplina che si occupa di fornire e proteggere le identità digitali e autorizzazione di accesso degli utenti in un sistema IT. Gli strumenti IAM consentono alle organizzazioni di creare ed eliminare in modo sicuro identità digitali, politiche di controllo degli accessi, verifiche degli utenti e monitoraggio delle attività. La stima del mercato di questo segmento è di 22 miliardi di dollari nel 2025 con crescita dei ricavi annua di circa il 10% fino al 2030 (MarketsandMarkets, 2025b). I componenti e le funzioni principali delle soluzioni di gestione delle identità e degli accessi includono:

- Servizi di directory, memorizzazione e gestione dei dati sulle identità, credenziali e autorizzazione degli accessi per gli utenti tramite directory centralizzate o esterne (es. Microsoft Active Directory, Google Workspace);
- Strumenti di autenticazione, Multi-Factor Authentication (MFA) per l'autenticazione a più fattori, Single Sign-On per l'accesso a più app e servizi con un unico set di credenziali e l'autenticazione adattiva con schemi di AI e machine learning;
- Controllo degli accessi, tramite gli strumenti di gestione del privilegio di accesso (PAM) per supervisionare la sicurezza degli account e il controllo degli accessi per account con privilegi elevati come gli amministratori di sistema;
- Gestione delle credenziali.

Inoltre, ci sono tecnologie come:

- Mail Security, protegge il canale delle mail per il phishing, business email compromise e distribuzione di malware e ransomware;
- Security Awareness Training (AST), formazione continua degli utenti per ridurre il rischio legato al comportamento e azioni 'scorrette' del singolo sul web.

L'intelligenza artificiale, in questo contesto, sta modificando il paradigma facendo passare da un ambiente statico a uno dinamico attraverso l'automatizzazione dei processi di autenticazione e di controllo. Per fare ciò si usano degli agenti AI autonomi, che diventano veri e propri utenti non umani spesso bersagli di attacchi informatici. Da un lato abbiamo un'autenticazione e gestione degli accessi umani più efficiente e scalabile, dall'altro nuovi utenti non umani scarsamente protetti e rischiosi per l'azienda. La direzione del mercato si dovrà sempre di più spostare verso la protezione di questi sistemi che permettono di migliorare i processi di controllo. Il fenomeno di adversarial ML è uno dei più comuni, dove gli attaccanti manipolano l'input del codice per bypassare la detection, permettendo alla minaccia di agire indisturbata. Inoltre, l'AI permette di migliorare la detection in e-mail e AST. La criticità nell'uso dell'intelligenza artificiale per mail e AST si ripercuote nell'ambito della privacy e compliance, data la vasta richiesta di dati utente esposti a violazioni e leaks.

Per identificare i player e le tendenze del segmento, è possibile fare riferimento alle analisi di settore (ad esempio Magic Quadrant per Access Management ed Email Security) come indicatori comparativi.



Figura 3.7: Magic Quadrant for AM – Fonte: Gartner

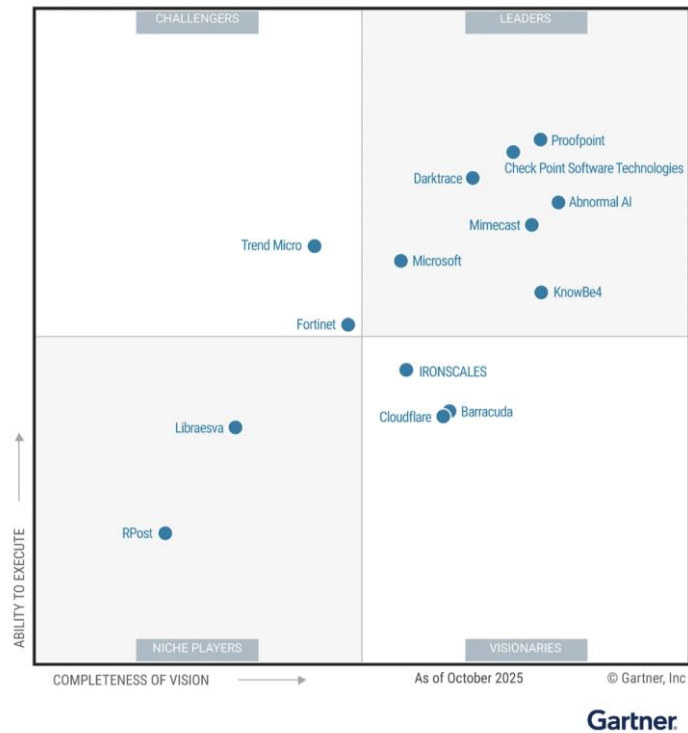


Figura 3.8: Magic Quadrant for Email Security– Fonte: Gartner

Da questi due grafici viene messo in risalto la presenza di Microsoft come leader con ruolo centrale in entrambe le categorie. La centralità strategica attribuita da Microsoft per il dominio dell'Identity & User Security è dovuta all'importanza che ricopre nei contesti cloud e SaaS, rappresentando il principale punto di controllo per applicare policy, privilegi e gestione del rischio in ottica Zero Trust. Inoltre, è un dominio che non protegge più soltanto gli utenti umani ma anche *non-human identities* e agenti AI in forte espansione nelle aziende. Inoltre, il *Microsoft Digital Defense Report 2025* descrive un aumento del 32% degli attacchi *identity-based* nella prima metà del 2025, diventando una superficie d'attacco scalabile sia per i malintenzionati che per il segmento di sicurezza (Microsoft, 2025a).

3.2 Managed Security Services – Da tecnologia a servizio gestito

Nei paragrafi precedenti sono state trattate le principali famiglie tecnologiche concentrando l'analisi sui prodotti e i principali vendor. La sicurezza informatica però non rappresenta solo un insieme di soluzioni efficaci, ma soprattutto la capacità di renderle operative e governabili. In questa sezione verranno quindi analizzati in modo sintetico i principali *Managed Security Services* che permettono di identificare alcuni dei servizi storicamente erogati da un *Managed Security Service Provider*.

3.2.1 SOC – Security Operations Center

Il Security Operations Center (SOC) è un centro operativo centralizzato, fisico o virtuale, che assicura, in modo continuativo, la capacità di un'organizzazione di rilevare, analizzare e gestire gli incidenti cyber, trasformando flussi eterogenei di telemetria in decisioni e azioni di risposta. È un modello operativo che combina personale tecnico, processi e piattaforme tecnologiche per mantenere una sorveglianza costante su endpoint, rete, identità, cloud applicazioni, dati e tutto il perimetro digitale. Questo modello operativo garantisce copertura continua e riduzione del:

- *Lifecycle Incident*, il tempo complessivo di un incidente che intercorre dall'individuazione alla risoluzione;
- Danno economico e operativo derivante da violazioni informatiche;
- Incertezza e complessità della gestione delle soluzioni di sicurezza informatica.

Questa funzione diventa di fondamentale importanza per la postura di sicurezza informatica, in quanto garantisce capacità sistemica di gestione per rilevare segnali, correlare eventi, stabilire priorità di rischio e applicare azioni di contenimento e ripristino in tempi compatibili con la continuità operativa.

I modelli più diffusi di erogazione del SOC includono:

- SOC tradizionale, generalmente interno all'azienda;
- SOC-as-a-Service, esterno e gestito da un MSSP.

Il SOC tradizionale è un progetto di lunga durata, che richiede tempo, spese infrastrutturali e competenze che molto spesso le aziende e in particolare le PMI non hanno o non possono sostenere. Generalmente sono soluzioni utilizzati in ambienti con particolari esigenze di riservatezza o tecnologici molto specifici. La soluzione del SOC-as-a-Service permette di delegare il compito della gestione degli allarmi ad un MSSP, esternalizzando la sicurezza informatica e definendo un modo più efficiente e scalabile per la gestione del servizio. La soluzione permette di ottenere l'accesso a team esperti attivi 24/7 per tutto l'anno con tecnologie aggiornate e capacità di risposta rapide, senza la necessità per il cliente di ricorrere ad alcuna infrastruttura fisica. Questo rapporto è sancito con un contratto che definisce il tempo di durata di gestione, KPI da monitorare come *Service Level Agreement* (SLA), *Mean Time to Detect* (MTTD) e *Mean Time to Response* (MTTR) e soprattutto le responsabilità in caso di incidente informatico. Questa soluzione è adatta a realtà che vogliono concentrarsi sul proprio business avendo garantita la sicurezza operativa e non dover integrare ulteriori competenze specifiche a livello di risorse aziendali. Esistono anche soluzioni *co-managed* dove le responsabilità e le attività operative sono ripartite tra cliente e provider. Questa

configurazione consente di mantenere il controllo su compliance e governance lato cliente, affidando le attività di monitoraggio continuo, threat hunting e gestione degli incidenti a fornitori esterni. Sul piano normativo, l'industrializzazione di questo modello risponde a requisiti sempre più stringenti di gestione e tracciabilità degli incidenti richiesti. La normativa NIS2 richiede misure di gestione del rischio che includono la capacità di gestione degli incidenti e continuità operativa, con annessa documentazione delle misure intraprese per diversi settori. Analogamente, il regolamento riferito alle entità del settore finanziario chiamato DORA impone la capacità di gestione degli incidenti ICT e di reporting.

Dal punto di vista tecnologico, ci sono due strumenti principali che aiutano a rendere il SOC un servizio scalabile e gestito in maniera efficiente e sono:

- *Security Information and Event Management (SIEM)*;
- *Security Orchestration, Automation and Response (SOAR)*.

Il SIEM è una tecnologia che permette di raccogliere log e telemetrie da tutti gli stack di sicurezza collegati, costruendo regole di correlazione e casi d'uso. Tramite la memorizzazione dei log e la correlazione permette al SOC di tenere sotto controllo ogni evento ed eventualmente ricostruire una storia d'attacco tramite la visibilità fornita dal SIEM. Il SOAR invece è l'orchestratore per eccellenza e, tramite l'ausilio di *playbook*, permette ai team di integrare e coordinare strumenti di sicurezza separati, automatizzare le attività ripetitive e semplificare i workflow di risposta agli incidenti e alle minacce. Ciò che differenzia un SOC efficace non è la presenza nominale di questi strumenti, ma la capacità di convertirli in un modello operativo ripetibile: casi d'uso prioritizzati, regole mantenute e misurate, riduzione del rumore, tempi di triage prevedibili, escalation disciplinata e produzione di evidenze. In questa cornice, l'automazione e l'uso di intelligenza artificiale diventano abilitatori di scalabilità, ma solo se inseriti in processi governati (validazione, gestione dei falsi positivi, controlli sulla qualità dei dati e tracciabilità delle azioni). Anche per questo, i SOC di nuova generazione tendono ad evolvere verso modelli *augmented*, in cui un livello di orchestrazione intelligenze e assistenza all'analista riduce l'overhead operativo e rende più sostenibile l'erogazione multi-tenant tipica degli MSSP, senza sacrificare *governance* e *accountability*. Queste esigenze motivano l'emergere di piattaforme *Augmented SOC* e di modelli SOC-as-a-service orientati agli outcome operativi e alla scalabilità di gestione per il cliente.

3.2.2 Red Teaming

Il *red teaming* è un processo di verifica dell'efficacia delle misure di sicurezza informatica in cui il *Red Team*, personale specializzato sicurezza informatica, conduce attacchi simulati e non distruttivi contro i sistemi dell'organizzazione. Questo processo permette di individuare le vulnerabilità reali prima che possano essere sfruttate da attori malevoli e ad apportare miglioramenti mirati alle operazioni di sicurezza. Aiuta le organizzazioni a:

- Individuare e valutare vulnerabilità presenti nell'infrastruttura e nei processi di sicurezza;
- Valutare l'efficacia degli investimenti sulla sicurezza informatica;
- Prepararsi a potenziali attacchi reali;
- Stabilire priorità di investimento per il miglioramento dei sistemi di sicurezza.

Il *red team* opera congiuntamente con il *blue team*, responsabile della gestione della difesa nel SOC, per proporre strategie di mitigazione per il miglioramento costante della sicurezza informatica dell'organizzazione, costituendo quello che viene chiamato *purple team*. Nel contesto dell'erogazione dei servizi gestiti, queste pratiche permettono al fornitore di dimostrare in modo oggettivo e verificabile le vulnerabilità presenti nello stack di sicurezza del cliente e proporre azioni di mitigazione mirate. Tali attività, inoltre, costituiscono una prova misurabile della gestione della sicurezza informatica richiesta dalle normative del settore, in particolare NIS2 e DORA, e del valore operativo del servizio gestito.

3.2.3 Threat Intelligence

La *threat intelligence*, denominata anche *cyber threat intelligence* (CTI), consiste nell'insieme delle informazioni dettagliate e fruibili relative alle minacce alla sicurezza informatica. Supporta i team che si occupano di sicurezza nell'adottare un approccio proattivo alla rilevazione, mitigazione e prevenzione di attacchi informatici. Si distinguono tre livelli di CTI:

- Tattica, fornisce indicatori tecnici di compromissione e informazioni sulle tecniche di attacco in uso, permettendo di anticipare attacchi futuri della stessa tipologia;
- Operativa, aiuta ad identificare gli attori delle minacce che potrebbero prendere di mira una determinata organizzazione o settore;
- Strategica, intelligence di alto livello che destinata ai responsabili delle decisioni aziendali, come i CEO e altri dirigenti non tecnici, che fornisce una visione delle minacce globali e verticali al settore target.

Per un'azienda, quindi, la CTI è uno strumento essenziale per comprendere quali minacce sono più probabili nel proprio contesto operativo, quali siano prevalenti nel settore di appartenenza e quelle di maggiore frequenza nella propria organizzazione. Per un MSSP la dimensione è ancora più critica in quanto deve essere integrata nel modello di servizio per allineare i casi d'uso alle minacce reali del portafoglio clienti e dimostrare la capacità di rispondere alle *Tactics, Techniques and Procedures* (TTP) effettivamente impiegate dagli attaccanti. Possiamo vedere la CTI come un radar esterno che, tramite una funzione centralizzata dedicata, svolge tre ruoli complementari:

- Osserva il perimetro delle minacce e le dinamiche emergenti del settore;

- Produce report settoriali e indicatori di rischio a supporto dell'decisione strategiche ed operative;
- Aiuta il SOC nella gestione della sicurezza del cliente.

3.2.4 Governance & Compliance

La Governance & Compliance nella cybersecurity si riferisce alla definizione e implementazione di politiche, procedure e controlli per garantire che un'organizzazione rispetti normative, standard e regolamenti in materia di sicurezza informatica. Include la gestione del rischio, la supervisione strategica e la verifica della conformità a framework come ISO/IEC 27001, GDPR, NIS2, DORA e TISAX. Queste dimensioni rappresentano il fondamento strategico della cybersecurity aziendale, garantendo che la sicurezza sia integrata nei processi di business e che l'organizzazione mantenga una postura di sicurezza adeguata. È essenziale per evitare sanzioni regolamentari, proteggere la reputazione aziendale e dimostrare la *due diligence* nei confronti degli *stakeholder*. Le principali attività includono:

- Gestione del rischio e supervisione strategica;
- Risk assessment, audit interni e monitoraggio continuo;
- Reporting verso il management e gli organi di controllo;
- Sviluppo di programmi di governance e metriche di sicurezza aziendali.

Per un'organizzazione è importante essere in linea con gli standard normativi e poter dimostrare di avere una politica di sicurezza approvata, processo di gestione degli incidenti strutturato, investimenti documentati nell'ambito della sicurezza informatica e la nomina di ruoli di responsabilità formalmente definita nell'ambito come quello del *Chief Information Security Officer* (CISO). Per un MSSP ha una duplice importanza:

- Garantire al cliente di soddisfare i requisiti normativi applicabili al proprio settore;
- Supportare il cliente nel percorso di adeguamento verso tali standard.

Inoltre, è strategicamente rilevante per un MSSP individuare quali normative si applicano ai settori rappresentati nel proprio portafoglio clienti per offrire soluzioni verticali e utili ai fini della conformità.

Il quadro normativo di riferimento ha subito un'accelerazione significativa a partire dal 2022, con l'entrata in vigore e l'aggiornamento dei seguenti framework:

- NIS2, direttiva europea in vigore dal 2023, che estende il perimetro applicativo della NIS1 introducendo requisiti espliciti su *governance*, gestione del rischio, *incident reporting* e *supply chain*;
- DORA (*Digital Operational Resilience Act*), regolamento per il settore finanziario applicabile dal 17 gennaio 2025, che impone alle organizzazioni di riferimento un framework strutturato di gestione del rischio ICT, *incident reporting*, test di resilienza operativa, controllo sui fornitori terzi;

- NIST CSF 2.0, aggiornamento del *Cybersecurity Framework del National Institute of Standards and Technology*, rafforza la parte di *governance* del rischio cyber;
- ISO/IEC 27001:2022, revisione dell'impianto del *Sistema di Gestione della Sicurezza delle Informazioni* (ISMS), include sicurezza delle informazioni e protezione della *privacy*.

Un recente ed importante tema di compliance è quello che riguarda il referente la figura del Referente CSIRT. Nel quadro NIS2 e del D.lgs. 138/2024, è un presidio tecnico-organizzativo centrale nella governance della sicurezza e nell'adempimento degli obblighi di *incident reporting* verso istituti di conformità come l'*Agenzia per la Cybersicurezza Nazionale* (ACN). È il punto di collegamento operativo tra l'organizzazione e il sistema nazionale di cybersicurezza (ACN e CSIRT Italia), inserito nella struttura di cyber-governance prevista dal decreto NIS. Il referente garantisce l'adempimento puntuale degli obblighi di notifica degli incidenti significativi (tempistiche di 24 ore, aggiornamenti successivi, report finale) secondo artt. 25–26 D.lgs. 138/2024 e linee guida ACN. Un MSSP, oltre ad aiutare con i servizi di sicurezza gestita, può essere incaricato dall'azienda interessata per designare una figura di riferimento all'interno dell'organizzazione e svolgere le funzioni operativamente associate al ruolo.

Un altro esempio di come la sicurezza diventi requisito abilitante per l'operatività del business è rappresentato dalla TISAX (*Trusted Information Security Assessment Exchange*). Si tratta di uno schema di valutazione e condivisione dei risultati di sicurezza delle informazioni specifico per il settore automotive, gestito da ENX Association sulla base dei requisiti ISO/IEC 27001. Questo rappresenta uno standard del settore dove i principali costruttori *Original Equipment Manufacturer* (OEM) e i loro fornitori richiedono la certificazione TISAX come condizione per la gestione di dati sensibili del costruttore, dati di prototipazione, informazioni di sviluppo e dati personali. In questo contesto, un MSSP aiuta le organizzazioni soggette a questo requisito per:

- La costruzione dell'impianto documentale ISO 27001/TISAX (policy, risk assessment, registri, procedure di incident response, ruoli);
- Erogazione di servizi gestiti a copertura dei controlli su monitoraggio, *logging*, gestione incidenti, *hardening* di rete ed endpoint;
- La produzione di report e indicatori periodici che costituiscono evidenza durante l'*assessment* TISAX.

3.3 Limiti strutturali delle soluzioni frammentate

Nel contesto dell'ecosistema frammentato della cybersecurity, l'approccio best of breed, fondato sulla selezione delle tecnologie tecnicamente superiori per ciascun dominio, ha dominato fino ad oggi le strategie di acquisto delle organizzazioni. Sebbene a livello di singola funzione il risultato sia rilevante, la frammentazione di queste soluzioni puntuali genera un'inefficacia operativa in termini di criticità di natura tecnica, organizzativa ed economica sempre più impattante con l'evoluzione degli attacchi informatici. In questa sezione verrà effettuata un'analisi su quelli che sono i principali limiti strutturali di questo tipo di approccio e dei bisogni conseguentemente generati.

I primi due limiti, e anche i più immediati, sono rappresentati dall'eterogeneità tecnologica degli stack di sicurezza e dalla sua complessità di gestione. I segnali preliminari di questi limiti erano stati resi noti già nel 2019 durante il *RSA Conference*, dal *Chief Security Officer of Public Cloud di Palo Alto Networks*, *Matthew Chiodi* affermando che in media le piccole organizzazioni possiedono dai 15 ai 20 strumenti, quelle di medie dimensioni dai 50 ai 60 e le large enterprise arrivano a superare i 130 strumenti (Matthew Chiodi, 2019). Nonostante questi numeri, nell'articolo *Simplify to Survive: How Organizations Can Navigate Cyber-Risk* del 2023 di Richard Watson, consulting leader di Ernst & Young, viene specificato come gran parte delle organizzazioni utilizza realmente solo il 10-20% delle tecnologie possedute (Watson, 2023). Questa molteplicità di strumenti, sviluppati da diversi vendor e con protocolli di comunicazioni, prioritizzazione e formati di log differenti genera il fenomeno dei data silos, dove ogni strumento possiede esclusivamente il proprio sottoinsieme di dati, privo di capacità native di condivisione e correlazione con soluzioni eterogenee. Queste caratteristiche generano profonda complessità nella gestione degli eventi da parte degli esperti che, in caso di attacco informatico, devono correlare, normalizzare e integrare i dati provenienti dalle diverse soluzioni, prima di rispondere all'attacco. Inoltre, l'assenza di integrazione nativa genera possibili vulnerabilità tra uno strumento e un altro che gli attori malevoli, grazie all'uso di nuove tecnologie come l'intelligenza artificiale, posso facilmente sfruttare come vettori d'attacco. Ogni soluzione puntuale genera indipendentemente una moltitudine di alert indipendenti con tassi di falsi positivi significativi, che impattano profondamente sulla gestione dei reali eventi informatici. In un'analisi condotta nel 2023 a 900 analisti di cybersecurity dall'azienda Tines, il 63% dei rispondenti si dichiara esausto dal carico di lavoro dovuto alla gestione degli alert su base giornaliera (Tines, 2023). Infine, la necessità di triage manuale estende significativamente le metriche operative di riferimento quali il *Mean Time to Detect* e il *Mean Time to Respond*, che impattano direttamente sul tempo di vita di un evento malevolo.

Un altro limite riguarda il lato economico-organizzativo del modello. Il *Total Cost of Ownership* di un ecosistema frammentato è sistematicamente sottostimato in fase di decisione d'acquisto, poiché le organizzazioni tendono a considerare esclusivamente i costi di licenza, trascurando il peso delle voci di costo indirette come la manutenzione continuativa, il costo del personale specialistico necessario per l'operatività di ciascuno strumento e i costi di formazione. Inoltre, la complessità genera delle diseconomie di scala dove i costi marginali di gestione e coordinamento eccedono i benefici marginali di sicurezza all'aggiunta di uno strumento verticale. Tale dinamica trova fondamento nella *Transaction Cost Theory* (Williamson, 1985), secondo cui al crescere della complessità relazionale tra unità indipendenti i costi di coordinamento aumentano in misura più che proporzionale rispetto ai benefici marginali ottenibili, rendendo la governance integrata

strutturalmente preferibile alla governance frammentata. Questo fenomeno genera una curva di rendimento non lineare dell'investimento di sicurezza:

- Nelle fasi iniziali, ogni nuova soluzione porta contributo marginale elevato;
- Progressivamente il costo marginale di coordinamento supera i benefici marginali erodendo completamente il ritorno dell'investimento;
- Il punto di incontro delle due curve rappresenta la soglia oltre la quale il paradigma *best of breed* diventa economicamente irrazionale.

I limiti appena descritti hanno generato un bisogno di cambiamento strutturale che si è manifestato attraverso il fenomeno della “*Platformization*”, le cui dinamiche e l'impatto sull'ambiente competitivo verranno analizzate nel dettaglio nelle sezioni successive.

3.4 Platformization

I limiti strutturali appena descritti attivano i vendor di prodotto che in risposta a questi bisogni danno vita al paradigma della *platformization*, ossia la progressiva trasformazione della cybersecurity da insieme di prodotti e servizi disaggregati a ecosistemi integrati costruiti attorno a una piattaforma tecnologica centrale. In questa sessione faremo riferimento ad uno studio di IBM e Palo Alto Networks sul fenomeno della platformization e su come questo sistema cambi profondamente la logica e i ruoli nel mercato competitivo della cybersecurity. Secondo lo studio, le organizzazioni possiedono in media 83 diverse soluzioni di sicurezza da più di 29 diversi fornitori, più strumenti equivalgono a più minacce e ogni integrazione è un potenziale punto di ingresso per gli hacker. Seguendo l'analisi, una piattaforma unificata rafforza la sicurezza e riduce i costi impiegando 72 giorni in meno per rilevare un incidente di sicurezza (MTTD) e 84 giorni in meno per contenerlo (MTTR). Ottengono inoltre un *Return of Investment* (ROI) medio del 101%, rispetto al 28% di coloro che non hanno ancora adottato la piattaforma (IBM Institute for Business Value, 2024). Le piattaforme di sicurezza offrono una visibilità senza pari, difese rafforzate, costi migliorati ed efficienza, il tutto con tangibili vantaggi aziendali. Una piattaforma di sicurezza solida e integrata può essere lo scudo che protegge la reputazione, la fiducia dei clienti e i profitti dell'organizzazione.

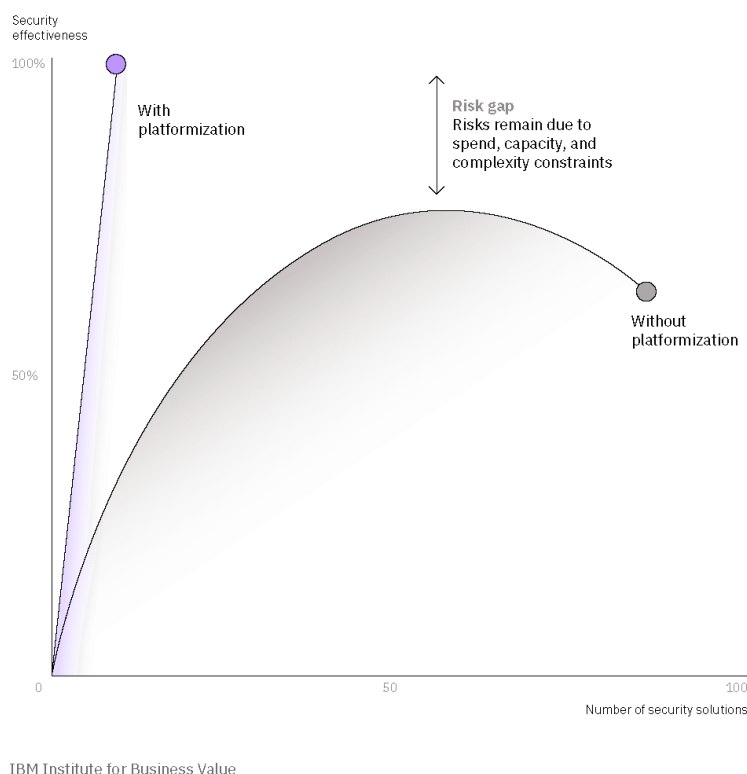


Figura 3.9: Efficacia della sicurezza con e senza platformizzazione. Adattato da "[Capturing the cybersecurity dividend](#)" di IBM Institute for Business Value (2024). IBM.

Nello studio, l'*IBM Institute for Business Value* ha collaborato con *Palo Alto Networks* per intervistare 1000 dirigenti del segmento della sicurezza in 21 settori e 18 Paesi differenti. Il 52% dei dirigenti afferma che la complessità rappresenta il principale ostacolo alle proprie attività di sicurezza informatica. Il costo medio della complessità della sicurezza informatica è superiore al

5% del fatturato totale annuo. Attraverso questi bisogni è emersa la necessità di creare un ambiente unico di controllo, che garantisca una protezione a 360 gradi dell'ambiente informatico delle aziende (IBM Institute for Business Value, 2024). L'intelligenza artificiale ricopre un ruolo fondamentale in questo salto innovativo, consentendo di analizzare dati in modo più efficace, migliorare le strategie di difesa e ottimizzare la risposta agli incidenti. Allo stesso tempo la *platformization* facilita l'adozione di tecnologie AI avanzate, tra cui l'agent AI, migliorando la governance e la gestione del rischio. È chiaro, dunque, che il mondo della sicurezza informatica e dell'intelligenza artificiale si intersechino sempre di più favorendo però l'evoluzione degli attacchi informatici. La società di analisi del settore *Enterprise Strategy Group* ha recentemente pubblicato un rapporto su come l'intelligenza artificiale generativa influisce sugli sforzi di sicurezza informatica delle organizzazioni. Questo rapporto sottolinea che il 76% delle organizzazioni ritiene che gli aggressori informatici otterranno il vantaggio maggiore dall'intelligenza artificiale generativa, rispetto solo al 24% che ritiene che i difensori della sicurezza avranno il sopravvento (Enterprise Strategy Group, 2024). Tuttavia, nonostante le preoccupazioni delle organizzazioni sul fatto che gli hacker abbiano inizialmente acquisito un vantaggio con la tecnologia, gli analisti *ESG* hanno scritto: *“L'intelligenza artificiale generativa potrebbe aiutare a migliorare la produttività del team di sicurezza, accelerare il rilevamento delle minacce, automatizzare le azioni di riparazione e guidare la risposta agli incidenti.”* (Enterprise Strategy Group, 2024).

Le piattaforme sono fondamentali per sfruttare tutto ciò che l'intelligenza artificiale ha da offrire, come:

- Identificare e prevenire minacce dovute proprio dall'uso dell'intelligenza artificiale, come un codice generato dall'AI per il furto d'identità e accesso;
- Garantire una protezione dei dati e della privacy in modo più completo ed efficiente.

Inoltre, la *platformization* permette di avere tutti i dati necessari per l'allenamento dell'intelligenza artificiale memorizzati e definiti, velocizzando il processo di machine learning e di miglioramento continuo.

3.4 Principali vendor nell'era delle piattaforme multi-dominio

In questa sezione verranno analizzati i principali vendor che stanno utilizzando un approccio a piattaforma multi-dominio nel mercato competitivo della cybersecurity. In particolare, verranno analizzate l'evoluzione della proposta di valore nel corso degli anni, le soluzioni proposte e i relativi domini coperti e, infine, gli investimenti e le acquisizioni strategiche in corso per rafforzare il proprio posizionamento nel nuovo paradigma emergente.

3.4.1 Palo Alto Networks

Palo Alto Networks nasce nel 2005 come azienda di *network security* in California e cresce fino a trasformarsi in un player multi-dominio con un portafoglio che oggi ruota tipicamente intorno a tre famiglie: *Strata* per la sicurezza di rete, *Prisma* per cloud e SASE, *Cortex* per SecOps (XDR, automazione/SOAR, “next-gen SIEM”). L'azienda eroga servizi a più di 70000 organizzazioni in 150 stati, includendo 85 organizzazioni nelle Fortune 100 (Palo Alto Networks, s.d.-a). Questa realtà non si concentra su un'unica piattaforma di sicurezza ma su tre diverse per ogni segmento della cybersecurity. L'azienda non ha introdotto il concetto di *platformization*, ma è stata tra i primi grandi vendor a cristallizzarla come strategia esplicita (dal 2024) e promuovendolo in modo sistematico come risposta al *tool sprawl* e integrandolo strettamente con l'intelligenza artificiale e risultati operativi come elemento differenziante. Sulla propria pagina istituzionale, l'azienda dichiara come le proprie piattaforme siano state sviluppate al 94% tramite AI generativa e come le operazioni di sicurezza vengano anch'esse gestite dall'intelligenza artificiale (Palo Alto Networks, s.d.-a). Gli investimenti fatti nel 2025 confermano una spinta strategica verticale verso l'intelligenza artificiale, il 22 luglio 2025 completa l'acquisizione di Protect AI, un leader innovativo nella protezione di applicazioni e modelli di AI e nel Red Teaming automatizzato. L'integrazione della tecnologia di Protect AI verrà integrata nella piattaforma Prisma AIRS con l'obiettivo di offrire una sicurezza completa dell'intelligenza artificiale end-to-end, andando ad analizzare la sicurezza degli agenti e dei diversi modelli di intelligenza artificiale (Palo alto Networks, 2025c). Sempre nel 2025 fa una mossa strategica significativa di riposizionamento architetturale, la piattaforma Prisma Cloud viene integrata all'impianto Cortex/SecOps in modo da unire la sicurezza cloud e le capacità del SOC in un'unica piattaforma chiamata Cortex Cloud (poi Cortex Cloud 2.0). Infine, il 30 luglio 2025 annuncia l'acquisizione di CyberArk , leader globale per *l'identity security*, per 25 miliardi di dollari con l'obiettivo di integrare capacità tecniche e architetturali del dominio sicurezza dell'identità (Palo Alto Networks, 2025b).

I principali indicatori economici del *Fiscal Year 2025* sono riportati nella Tabella 2.1 di seguito (valori espressi in milioni di USD):

	2024	2025	YoY%
Total revenue	8.027,5	9.221,5	+15%
Total cost of revenue	2.059,2	2.451,6	+19%
Operating expenses (R&D, S&M, G&A)	5.284,4	5.527,0	+5%
R&D	1.809,4	1.984,1	+9.6%

Fonte: [Fiscal Year 2025 - Palo Alto Networks](#)

3.4.2 CrowdStrike

CrowdStrike è una multinazionale statunitense fondata nel 2011 a Sunnyvale (California) da George Kurtz (ex-CTO di McAfee), Dmitri Alperovitch (ex-McAfee executive) e Gregg Martson (CFO), con l'obiettivo iniziale di rivoluzionare il dominio dell'*endpoint protection* attraverso un approccio cloud-native, contrastando i modelli tradizionali basati su *signature* che dominavano il mercato. La *platformization* di CrowdStrike si è affacciata in modo strutturato nel 2013 con il lancio della piattaforma *Falcon* come soluzione cloud-first per *endpoint protection*, evolvendo da un modello product-centric (es. antivirus isolati) ad ecosistemi unificati che consolidano l'eterogeneità delle tecnologie. CrowdStrike offre un'unica piattaforma proprietaria che comprende i seguenti moduli:

- Sicurezza degli endpoint;
- Next-Gen Identity Security;
- Threat intelligence e Threat hunting;
- Next-Gen SIEM;
- Sicurezza agentica;
- Exposure Management;
- Sicurezza del cloud;
- Protezione dei dati;
- Sicurezza SaaS;
- IT Automation;
- Automazione del workflow (SOAR);
- Sicurezza XIoT.

La logica di CrowdStrike è completamente diversa da quella di Palo Alto Networks, offre un'unica piattaforma, un unico agente Falcon, unico data layer cloud, unica threat intelligence ed unica AI.

Nel 2025 ha annunciato l'Agentic Security Platform, un Security Operations Center AI-powered che fornisce velocità, portata e intelligenza richieste per rispondere ai moderni attacchi informatici. L'innovazione di CrowdStrike si basa su due pilastri fondamentali:

- Enterprise Graph, un data layer progettato per essere "AI-ready", che unifica in un unico modello connesso la telemetria proveniente da endpoint, identità, cloud, ambienti SaaS, infrastrutture XIoT e fonti di terze parti;
- Charlotte AI AgentWorks, evolve da assistente conversazionale a infrastruttura per l'orchestrazione di agenti. È la prima piattaforma no-code del settore che offre ad ogni team la possibilità di creare, testare, distribuire e orchestrare agenti di sicurezza affidabili.

Nel 2025 ha fatto importanti investimenti per la piattaforma proprietaria:

- Acquisizione di Pangea, il 16 settembre 2025 CrowdStrike annuncia l'acquisizione di una dei leader nel settore dell'AI security. Le cifre dell'operazione sono di 260 milioni di dollari per l'acquisizione (WSJ, 2025);
- Acquisizione Onum, il 27 agosto 2025 CrowdStrike annuncia l'accordo per acquisire l'azienda pionieristica per la gestione delle pipeline di telemetria in tempo reale.

L'obiettivo è proprio quello di supportare l'evoluzione del SOC attraverso Falcon Next-Gen SIEM. Le stime parlano di un investimento di 290 milioni di dollari (Fortune, 2025).

I principali indicatori economici del *Fiscal Year 2025* sono riportati nella Tabella 2.1 di seguito (valori espressi in milioni di USD):

	2024	2025	YoY%
Total revenue	3.055,6	3.953,6	+29%
Total cost of revenue	755,7	991,5	+31%
Operating expenses (R&D, S&M, G&A)	2.301,8	3.082,6	+34%
R&D	768,5	1.076,9	+40%

Fonte: [Fiscal Year 2025 - CrowdStrike](#)

3.4.3 Microsoft

Microsoft è una multinazionale statunitense fondata nel 1975 ad Albuquerque, New Mexico, da Bill Gates e Paul Allen, inizialmente focalizzata su software operativo e produttività (es. Windows e Office), ma con un progressivo orientamento verso cybersecurity dal 2010 attraverso l'espansione di Azure come piattaforma cloud. La *platformization* di Microsoft si è affacciata in modo strutturato intorno al 2015 con l'evoluzione di Azure Active Directory (ora Entra) come core IAM cloud-native, accelerando nel 2019-2022 con il lancio di Microsoft Threat Protection (ora Defender suite) e l'integrazione di Microsoft Sentinel come SIEM unificato.

Microsoft divide le soluzioni disponibili in quattro suite principali:

- Microsoft Defender Suite, una soluzione XDR completa che offre protezione dalle minacce a più livelli, sicurezza dei dati, conformità, gestione e governance delle identità;
- Microsoft Entra Suite, fornisce soluzioni di sicurezza dell'accesso alla rete, protezione dell'identità, governance e verifica dell'identità;
- Microsoft Intune Suite, una soluzione unificata che riunisce controlli dei privilegi utente, assistenza remota, PKI cloud, intelligenza artificiale, analisi e funzionalità di patching delle app aziendali;
- Microsoft Purview Suite, unifica la sicurezza e la conformità dei dati e aiutare l'organizzazione a prevenire la perdita di dati e gestire i rischi.

Attraverso Microsoft Security Copilot, permette di integrare l'intelligenza artificiale generativa nei diversi stack di sicurezza amplificando le capacità operative.

Nel FY2025 Report, Microsoft non divide i ricavi derivanti dal mondo cybersecurity ma li possiamo stimare partendo da quelli totali e pensando all'evoluzione che sta avendo la società verso questo segmento di mercato. I ricavi totali ammontano a 281,724 miliardi di dollari nel 2025 con una crescita del 15% rispetto all'anno precedente. Le spese per ricerca e sviluppo ammontano a 32,488 miliardi di dollari con una crescita del 10% rispetto al 2024 (Microsoft, 2025b). Nel 2023, attraverso un comunicato ufficiale, Microsoft aveva comunicato il raggiungimento dei 20 miliardi di dollari di ricavi provenienti dal mondo della cybersecurity (Microsoft, 2023). Secondo analisi di mercato, i ricavi derivanti dalla cybersecurity nel 2025 sono stimati a 37 miliardi di dollari, pari al 14% dei ricavi totali (Investing.com, 2025).

3.4.4 Zscaler

Zscaler è una multinazionale statunitense fondata nel 2007 a San Jose (California) da Jay Chaudhry, con l'obiettivo iniziale di rivoluzionare la security network attraverso un approccio cloud-native, contrastando i modelli tradizionali basati su hardware on-prem. Criticamente, da startup focalizzata su secure web gateways è diventata un leader nel zero-trust security. La platformization di Zscaler si è affacciata in modo strutturato intorno al 2016 con il lancio della Zero Trust Exchange (ZTE) come piattaforma cloud-first per secure access, accelerando nel 2019-2022 con espansioni a full SASE (es. integrazione di ZIA, ZPA e ZDX nel 2020).

Le funzioni principali della piattaforma:

- Zero-trust Access Control, verifica ogni utente dispositivo e connessione per un accesso sicuro;
- Threat Protection e Inspection, ispeziona traffico encrypted bloccando malware, phishing e ransomware;
- DLP e Compliance, previene fughe di dati e supporta la compliance;
- User Experience e Performance Optimization, con Zscaler Internet Access e Private Access, ottimizza l'accesso diretto ad internet ed app senza VPN latency .

Nella piattaforma è integrata la Zscaler AI che, oltre ad offrire i principali vantaggi di automazione e scalabilità operativa, garantisce una protezione per l'uso dell'intelligenza artificiale pubblica e per i dati sensibili esposti dall'uso dell'AI privata. Per rafforzare il livello di MSS come transizione alla platformization, nel 2025 ha completato importanti acquisizioni:

- Acquisizione Red Canary, completata 1 agosto 2025 l'acquisizione strategica permette di integrare le competenze dell'azienda per le funzionalità SecOps attraverso le avanzate capacità del Security Operations Center. L'obiettivo è quello di integrare la tecnologia di intelligenza artificiale agente di Red Canary con il proprio Data fabric for Security per offrire una delle soluzioni SOC più complete del settore. Le stime sul costo dell'operazione parlano di cifre intorno ai 650 milioni di dollari (Zscaler, 2025c).
- Acquisizione SPLX, annunciata il 3 novembre 2025 l'acquisizione rappresenta un punto di svolta per il mondo della protezione AI permettendo di acquisire competenze in AI asset discovery e risk assessment, AI red teaming e remediation, AI runtime Guardrail e prompt hardening e AI governance e Compliance. Le stime sul costo dell'operazione parlano di cifre intorno ai 40,65 milioni di dollari (Zscaler, 2025b).

Inoltre, è stato recentemente pubblicato il report del *Fiscal Year 2025* con le principali voci di interesse per la nostra analisi nella Tabella 2.3 di seguito (valori espressi in milioni di USD)

	2024	2025	YoY%
Total revenue	2.167,8	2.673,1	+23%
Total cost of revenue	477,1	618,2	+30%
Operating expenses (R&D, S&M, G&A)	1.812,1	2.183,4	+21%
R&D	499,8	672,5	+35%

Fonte: [Fiscal Year 2025 - Zscaler](#)

3.4.5 Cisco

Cisco System Inc. è una multinazionale statunitense fondata nel 1984 a San Jose in California. È storicamente conosciuta per la fornitura di infrastrutture di rete, che le hanno permesso di sviluppare competenze sempre più trasversali e orientate al mondo della sicurezza informatica tramite acquisizioni ed investimenti. In particolare, nel 2015 ha acquisito OpenDns per la visibilità sul traffico DNS, nella rilevazione delle minacce ed integrare capacità di *threat intelligence* per estendere la sicurezza dell’infrastruttura di rete agli ambienti cloud (Cisco, 2015). Inoltre, nel 2018 ha acquisito Duo Security per integrare competenze nel dominio dell’*identity security* come la *multi-factor authentication* (Cisco, 2018). La direzione verso la *platformization* di Cisco era chiara, ma viene ulteriormente consolidata con due eventi principali:

- Al convegno RSA 2022, presenta la piattaforma unificata end-to-end per ambienti ibridi e multi-cloud denominata *Cisco Security Cloud* (Cisco,2022);
- Il 18 marzo 2024 completa l’acquisizione di *Splunk*, soluzione per la gestione delle informazioni e degli eventi di sicurezza e per la correlazione dei dati cross-dominio (Cisco, 2024a).

Sul fronte dell’intelligenza artificiale, Cisco sta introducendo soluzione per la difesa predittiva per le minacce amplificate dall’AI e un modulo di assistenza per le operazioni del *Security Operation Center*.

Inoltre, è stato recentemente pubblicato il report del *Fiscal Year 2025* con le principali voci di interesse per la nostra analisi nella Tabella 2.4 di seguito (valori espressi in milioni di USD):

	2024	2025	YoY%
Total revenue Security	5.075	8.094	+ 59%
Total R&D	7.983	9.300	+ 16%
R&D Security	≈1.553	≈ 1.809	+17%

Fonte: [Fiscal Year 2025 - Cisco](#)

*per la voce *R&D Security* è stata usata un'approssimazione proporzionata ai Ricavi

3.4.6 Fortinet

Fortinet è stata fondata nel 2000 a Sunnyvale, California, dai fratelli Ken Xie (ex-NetScreen) e Michael Xie, con l'obiettivo di rivoluzionare la network security integrando multiple funzioni in un singolo appliance. Il primo prodotto, FortiGate (lanciato nel 2002), era un firewall fisico con ASIC custom per performance elevate, combinando firewall, VPN, antivirus e intrusion prevention in un'unica soluzione UTM. Criticamente, questo approccio innovativo ha permesso una rapida adozione tra PMI ed enterprise, ma ha esposto Fortinet a rischi di obsolescenza hardware in un'era cloud-first, spingendola verso acquisizioni per espandere il portfolio. Fortinet sta proponendo una piattaforma multi-dominio chiamata *Fortinet Security Fabric*, fondata su tre pilastri principali: *Secure Networking*, *Unified SASE* e *Security Operations*. L'intelligenza artificiale è sempre più integrata nella piattaforma proprietaria, come dichiarato in un report del 2025, in tre modi:

- FortiAI Protect, protegge le organizzazioni con real-time intelligenza che blocca le nuove minacce risk assessment con risposte critiche prioritizzate, riducendo al minimo i falsi positivi;
- FortiAI Assist, automatizza le attività di sicurezza, dagli aggiornamenti dei criteri alle correzioni della configurazione. Ottimizza le operazioni di rete, risolvendo in modo proattivo e autonomo i problemi prima che abbiano un impatto sugli utenti;
- FortiAI SecureAI, garantisce una sicurezza completa dell'intelligenza artificiale, dall'infrastruttura ai dati, salvaguardando la proprietà intellettuale e mantenendo la conformità.

Tra gli investimenti più importanti che hanno aiutato il passaggio alla piattaforma troviamo:

- Acquisizione Next DLP, annunciata il 6 agosto 2024 l'acquisizione ha l'obiettivo di integrare le competenze per la prevenzione della perdita di dati aziendali e rafforzare la leadership nel segmento di mercato. Le cifre dell'operazione si stimano attorno ai 105 milioni di dollari (Fortinet, 2024);
- Acquisizione Perception Point, annunciata l'11 dicembre 2024 l'acquisizione ha l'obiettivo di integrare nella piattaforma proprietaria le funzionalità basate sull'intelligenza artificiale di Perception Point per la protezione della posta elettronica e piattaforme di collaborazione. Le cifre dell'operazione si stimano attorno ai 33,7 milioni di dollari (Fortinet, 2025b).

Inoltre, è stato recentemente pubblicato il report del *Fiscal Year 2025 (a nove mesi fino al 30 settembre)* con le principali voci di interesse per la nostra analisi nella Tabella 2.5 di seguito (valori espressi in milioni di USD):

	2024	2025	YoY%
Total revenue	4.295,7	4.894,6	+14%
Total cost of revenue	843,1	939,7	+12%
Operating expenses (R&D, S&M, G&A)	2.223,3	2.495,8	+13%
R&D	525,7	610,5	+16%

Fonte: [Fiscal Year 2025 - Fortinet](#)

3.5 Analisi delle forze di Porter: soluzioni frammentate e piattaforme multi-dominio

3.5.1 Premessa Metodologica

Per analizzare la struttura competitiva del settore, verrà applicato il modello delle cinque forze competitive di Michael E. Porter. L'ipotesi fondante del framework è che la struttura del settore eserciti un'influenza determinante sulle dinamiche competitive e sulla distribuzione del valore, analizzabile attraverso le seguenti forze:

- Rivalità nel settore;
- Minaccia di nuovi entranti;
- Potere contrattuale dei clienti;
- Potere contrattuale dei fornitori;
- Minaccia di beni sostituti.

Ai fini della presente tesi il modello verrà utilizzato come strumento di lettura sistemica delle trasformazioni competitive nel mercato della cybersecurity per identificare i principali cambiamenti delle forze a seguito dell'avvento del paradigma emergente, e fornire delle basi analitiche per la valutazione del posizionamento strategico degli MSSP nell'evoluzione del mercato.

Date queste premesse, per il contesto analizzato l'applicazione del modello richiede un adattamento interpretativo. Le soluzioni frammentate e le piattaforme multi-dominio non costituiscono settori industriali distinti da analizzare separatamente, ma due assetti competitivi che coesistono lungo una transizione strutturale del paradigma dove i due modelli competono per affermarsi come standard dominante. L'applicazione del framework verrà utilizzato in modo comparativo e differenziale concentrandosi sulle forze che presentano una rilevante discontinuità strutturale nel passaggio tra un paradigma e un altro, escludendo tutte quelle componenti che sono caratteristiche e variano per intensità dei singoli domini precedentemente analizzati. In particolare, le forze della rivalità nel settore, minaccia di nuovi entranti e potere contrattuale dei clienti presentano dinamiche direttamente rilevanti per le implicazioni strategiche degli MSSP. Pertanto, le rispettive forze del potere contrattuale dei fornitori e la minaccia di beni sostituti verranno trattate in forma più sintetica. L'obiettivo è quello di non restituire un'analisi statica del settore, ma identificare le forze che subiscono una trasformazione qualitativa e strutturale nel passaggio tra i due paradigmi.

3.5.2 Rivalità nel settore

Come visto nelle sezioni precedenti nelle soluzioni frammentate la rivalità viene definita principalmente all'interno dei singoli domini dell'ecosistema della sicurezza informatica. Le tecnologie differenziano principalmente per performance tecniche e caratteristiche intrinseche al singolo prodotto del vendor, che permettono di generare valore percepito dal cliente attraverso la qualità della soluzione. Questa dinamica, con la maturazione tecnologica dei singoli domini, tende a spostare la pressione competitiva progressivamente sulle condizioni economiche e sul prezzo delle singole soluzioni. Nel nuovo paradigma questa percezione cambia parallelamente con il valore generato: le piattaforme multi-dominio si concentrano sulla capacità di controllare lo stack di sicurezza del cliente nei diversi domini, acquisendo dati e vantaggio informativo e relazionale. La concentrazione di mercato, soprattutto in questa prima fase, con poche organizzazioni che offrono soluzioni avviate di piattaforme multi-dominio favoriscono i fenomeni di *land-and-expand*, controllo dei domini di sicurezza del cliente, e una domanda di mercato distribuita tra i player.

3.5.3 Minaccia di nuovi entranti

Nel paradigma delle soluzioni frammentate le barriere all'ingresso sono moderate e favoriscono la possibilità di entrata a nuovi vendor per dominio. L'innovazione verticale su un singolo dominio è un percorso praticabile e viene dimostrato dalla storia recente del settore, uno degli esempi più importanti è quello dell'azienda Wiz che dalla fondazione nel 2020 è diventata una dei principali vendor del dominio della Cloud Security (in particolare per le soluzioni CNAPP). Secondo quanto dichiarato dalla società stessa, Wiz ha raggiunto 100 milioni di dollari di *Annual Recurring Revenue* nei primi 18 mesi di attività (Wiz, 2022).

Nel paradigma delle piattaforme multi-dominio l'ingresso come piattaforma end-to-end risulta strutturalmente limitato da barriere tecnologiche, scala di dati per addestrare modelli AI, costi d'integrazione ed economie di scala nell'automazione. Questi fattori abbassano notevolmente le possibilità di entrata nel nuovo paradigma rispetto al precedente. Questa barriera ha generato un nuovo approccio strategico d'entrata nell'ecosistema: i nuovi entrati vengono costruiti con l'obiettivo di essere acquisiti dai grandi vendor piattaforma per integrare specifiche capabilities e rafforza l'ecosistema. Le acquisizioni effettuate dai vendor di piattaforma in sicurezza dell'intelligenza artificiale analizzate nelle sezioni precedenti mostrano un esempio pratico di questo approccio.

3.5.4 Potere contrattuale dei clienti

Questa forza è una delle più rilevanti in termini di trasformazione nel passaggio del paradigma dovuta alla natura dei prodotti. Mentre nelle soluzioni frammentate l'organizzazione dispone di un potere contrattuale medio-alto dovuto alla sostituibilità degli strumenti, la forte disponibilità di alternative comparabili all'interno del singolo dominio e la possibilità di rinegoziare ogni singola tecnologia integrata, nelle piattaforme multi-dominio la rotta si inverte. Nel nuovo paradigma parliamo di ecosistemi integrati che generano degli switching cost significativi: oltre ai costi diretti della sostituzione tecnologica, bisogna considerare la mole di dati gestita e conservata nelle piattaforme e accumulata nei modelli AI per la correlazione dei diversi domini. Il rischio di questo modello è quello della generazione di una dipendenza univoca dal vendor che genera appunto il fenomeno del vendor lock-in. Le valutazioni strategiche dei CISO e CEO devono basarsi sul trade-off della diminuzione della complessità di gestione rispetto alla dipendenza e i rischi commerciali derivati dall'adozione di una soluzione unica dipendente dal singolo vendor.

Questa tensione tra efficienza sistemica e autonomia decisionale costituisce uno dei driver principali della domanda di servizi degli MSSP, mantenendo un approccio agnostico alla tecnologia e rispetto al vendor di piattaforma.

3.5.5 Potere contrattuale dei fornitori

Nel paradigma delle piattaforme multi-dominio, la forte dipendenza da ambienti cloud e componenti per l'integrazione dell'intelligenza artificiale intensifica il potere contrattuale dei fornitori. La differenza sostanziale con il paradigma delle soluzioni frammentate è dovuta proprio alla natura delle piattaforme multi-dominio che richiedono forte dipendenza ad infrastrutture cloud e componenti per integrare l'intelligenza artificiale in un contesto con pochi fornitori che detengono una significativa quota di mercato e un elevato potere contrattuale.

3.5.6 Minaccia di beni sostituiti

Questa forza cambia significativamente di intensità nei due paradigmi. Nelle soluzioni frammentate la minaccia di sostituzione è intrinseca nella natura dei prodotti, dove la varietà di scelta di differenti soluzioni e provider in ogni dominio impatta profondamente la scelta di ogni singolo cliente. Nelle piattaforme multi-dominio la scelta invece è influenzata profondamente dai costi di sostituzione (*switching-cost*): il cambio tecnologico non influenza un singolo dominio della sicurezza, ma tutti quelli coinvolti dalla soluzione adottata. Questo fenomeno presenta problemi significativi anche a livello di rischio che prende il nome di *single point of failure*, dove un incidente che coinvolge direttamente il vendor piattaforma può propagarsi al cliente per l'intero stack di sicurezza.

L'applicazione del framework permette di avere una lettura complessiva delle cinque forze, dove il passaggio di paradigma sposta il potere competitivo in modo asimmetrico verso i player dominanti e riduce progressivamente la libertà di scelta delle organizzazioni acquirenti. Gli effetti di efficienza architetturali però generano inevitabilmente delle criticità significative come il vendor lock-in e il single point of failure. Queste tensioni definiscono uno spazio strategico dove i *Managed Security Service Provider* possono operare per portare valore al cliente, in particolare in organizzazioni di piccole e medie dimensioni.

3.6 Curve ad S – Traiettoria evolutiva e confronto di performance tecniche

3.6.1 Fondamento teorico

Le curve ad S, chiamate così per il loro andamento, sono traiettorie tecnologiche che rappresentano il progredire delle performance di una tecnologia valutate dal mercato rispetto a variabili come la cumulata degli investimenti in R&D del settore, cumulata delle vendite del settore e infine il tempo. Introdotto da Foster (1986) e formalizzato dalla letteratura sull'innovazione tecnologica a partire dal modello di Abernathy e Utterback (1978), questo modello definisce generalmente 3 fasi:

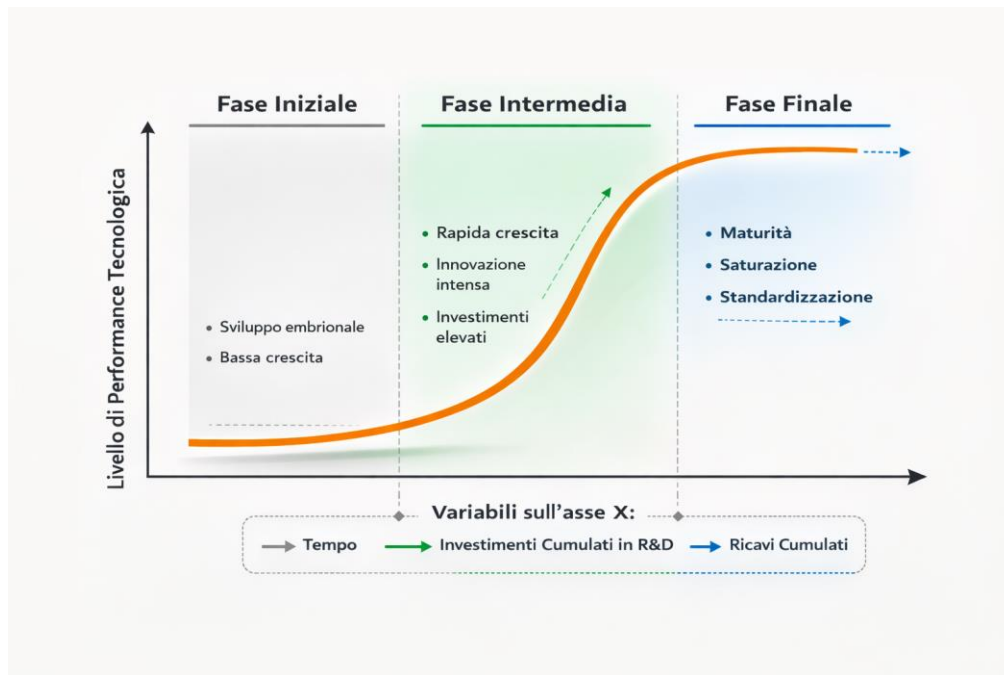


Figura 3.10 - Rappresentazione teorica di una curva ad S

- Fase Iniziale, embrionale dove la tecnologia ha generalmente una crescita contenuta delle performance;
- Fase Intermedia, la tecnologia inizia ad essere adottata dal mercato ed aumentano gli investimenti in R&D. Ne deriva un conseguente aumento di performance, fino al punto di superare il livello della tecnologia precedente e raggiungere la diffusione;
- Fase Finale, rappresenta la fase di maturità della tecnologia e del limite tecnologico che può derivare da motivi tecnici o di esigenze del mercato.

Ai fini della presente analisi, le curve ad S vengono utilizzate per confrontare le traiettorie di performance operative del paradigma delle soluzioni frammentate con quello delle piattaforme multi-dominio AI-driven, con l'obiettivo di verificare se i dati osservabili siano coerenti con una transizione di paradigma.

3.7.2 Costruzione della variabile di performance

Nel settore della cybersecurity i dati puntuali e metriche pubbliche relative alle performance tecnologiche, come tasso di correlazione e numero di falsi positivi, percepite dal mercato sono pressoché assenti. Questo limite per il confronto dei due paradigmi è stato superato formulando un'approssimazione per misurare il ciclo di vita di un incidente informatico, anche detto *incident lifecycle time*. Sono stati estrapolati i dati da uno dei dataset più autorevoli del settore, il report annuale *Cost of a Data Breach di IBM*, che conduce con continuità dal 2019 indagini su diverse organizzazioni di 17 settori industriali per analizzare l'impatto dell'esfiltrazione dei dati a livello di sicurezza informatica.

Da ogni report sono stati estrapolati i dati relativi al *Mean Time to Detect (MTTD)* e il *Mean Time to Response (MTTR)* la cui somma costruisce il ***incident lifecycle time***, cioè il tempo di vita di un incidente di sicurezza:

$$Performance(t) = \frac{1}{MTTD(t) + MTTR(t)} \left[\frac{1}{days} \right]$$

La performance è stata costruita come l'inverso del tempo totale di vita di un incidente, per costruire correttamente le curve: un valore più basso dei dati rappresenta una crescita in termini di performance e di efficienza. Il dataset distingue tre categorie principali per l'analisi in base all'uso dell'intelligenza artificiale nei sistemi di sicurezza delle organizzazioni: *extensive use of AI*, *moderate use of AI* e *no use*. L'approssimazione è stata condotta come segue:

- L'elevata adozione di intelligenza artificiale rappresentata dalla categoria *extensive use of AI* è stata associata alle piattaforme multi-dominio AI driven;
- L'uso moderato di intelligenza artificiale rappresentata dalla categoria *moderate use of AI* è stato associato alle soluzioni frammentate, coerentemente con le caratteristiche dei prodotti.

Queste assunzioni rappresentano i principali limiti delle analisi che vanno interpretate come indicazioni di tendenza di performance di mercato, lasciando spazio a future misurazioni dirette con l'aumentare della disponibilità dei dati pubblici.

3.7.3 Risultati e interpretazione

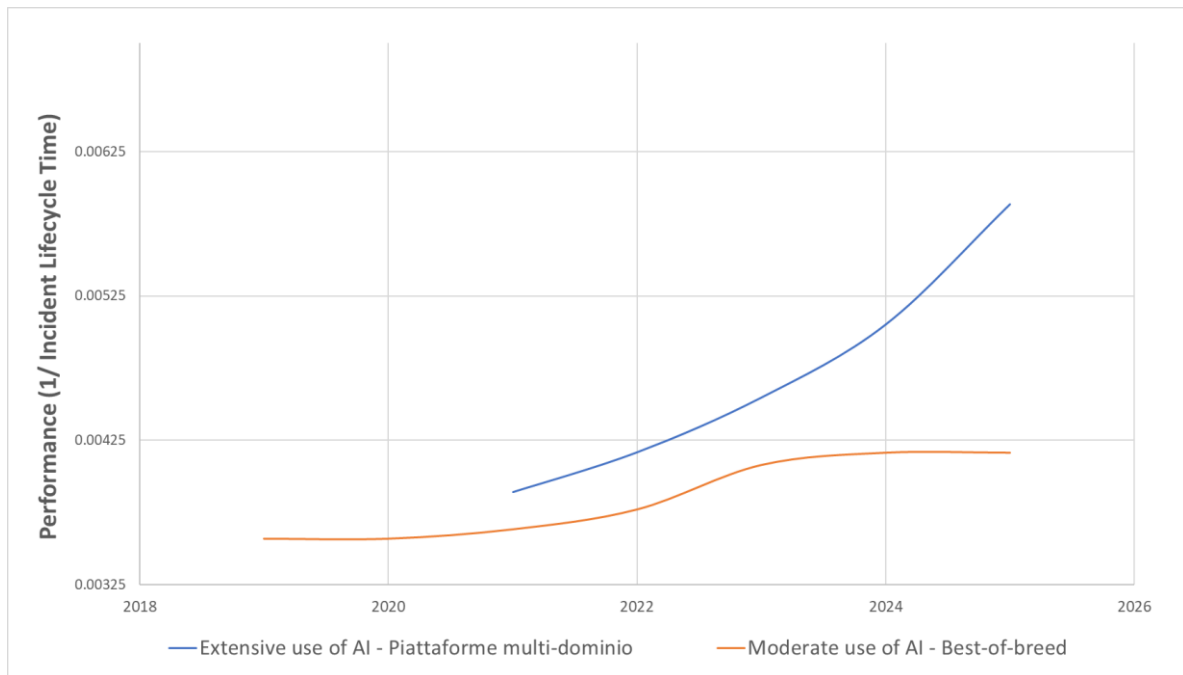


Figura 3.11 - Evoluzione della performance operativa in funzione del livello di adozione dell'AI

Nella Figura 3.11 vengono riportate le due curve risultanti dei paradigmi modellizzate, con una struttura complessiva coerente con il modello teorico delle curve ad S. La curva relativa alle soluzioni best-of-breed del paradigma attuale mostra una crescita di performance contenuta e, a partire dal 2023, emergono i primi segnali di maturazione tecnologica con un progressivo appiattimento della curva. La curva del paradigma delle piattaforme multi-dominio, associata ad un uso intensivo dell'intelligenza artificiale, risulta nella piena fase intermedia con una crescita accentuata a partire dal 2022, coerentemente con la relativa crescita di investimenti in R&D nelle piattaforme multi-dominio. Contrariamente con le evidenze teoriche, la curva delle piattaforme multi-dominio presenta un livello di performance iniziale superiore della curva delle soluzioni frammentate. Questo dato è probabilmente collegato alla crescita delle performance dell'intelligenza artificiale in altri settori, permettendo un'evoluzione rapida a livello di prestazioni e trasferibile al mercato della sicurezza informatica.

3.7.4 Limitazioni dell'analisi

Questa analisi presenta tre limitazioni importanti per una corretta interpretazione delle dinamiche del mercato:

- Limitata estensione temporale delle curve dovuta alla recente affermazione delle piattaforme multi-dominio;
- L'approssimazione non tiene conto di tutte le variabili che incidono nei paradigmi;
- Mancanza di dati pubblici direttamente imputabili ai due paradigmi.

Nonostante queste limitazioni, l'approccio adottato permette di individuare i primi segnali di evoluzione e di cambio di paradigma nel mercato della cybersecurity.

3.7 Piattaforme multi-dominio e l'evoluzione del ruolo degli MSSP

Le piattaforme multi-dominio stanno cambiando profondamente il perimetro competitivo e il valore percepito della sicurezza informatica, ma in maniera differente tra grandi organizzazioni e quelle di piccole e medie dimensioni. Le piattaforme multi-dominio nascono da una esigenza delle organizzazioni di grandi dimensioni per superare i limiti strutturali delle soluzioni frammentate e ridurre il numero di vendor da cui dipendere. Queste organizzazioni sono caratterizzate generalmente da elevata maturità IT, SOC interni e disponibilità di competenze specialistiche dove le piattaforme rappresentano un abilitatore di efficienza in risposta ai limiti strutturali delle soluzioni *best-of-breed*. Le dinamiche cambiano profondamente per organizzazioni di piccole e medie dimensioni che, pur essendo i principali bersagli di attacchi informatici e con un quadro normativo stringente, hanno una limitata disponibilità di risorse specialistiche per la sicurezza informatica e per la gestione di strumenti complessi. Queste realtà necessitano di continuità operativa, ma non percepiscono il valore di un investimento rilevante nelle piattaforme multi-dominio. In questo contesto, il valore percepito si sposta nella continuità operativa, nell'interpretazione del rischio nel contesto specifico, definizione di priorità in base all'impatto sul business, gestione completa di un incidente e dei termini normativi. Un vendor piattaforma fornisce l'infrastruttura tecnologica e gestisce alcune funzioni, lasciando in capo al cliente la responsabilità di tutto il quadro descritto. In questo perimetro i fornitori di servizi di sicurezza gestiti assumono un ruolo fondamentale e, tramite i loro servizi, rispondono esaustivamente alle esigenze del cliente. Il *Security Operation Center* diventa quindi essenziale per un MSSP per posizionarsi in questo mercato e sfruttare i gap operativi dei vendor. L'elemento distintivo risiede nella gestione completa della postura di sicurezza del cliente, definendo priorità di rischio e garantendo la continuità operativa e adeguamento normativo. In questo perimetro, l'integrazione dell'intelligenza artificiale nei processi operativi permette di rendere scalabile il servizio senza perdere la qualità garantita.

Le differenze sostanziali tra mercato enterprise e mid-market, e i bisogni differenti delle organizzazioni nei rispettivi segmenti, mostrano come viene percepito il valore di un MSSP in base al contesto. L'affermazione di un fornitore di servizi di sicurezza gestiti nel mid-market non si basa sulla disponibilità della tecnologia, ma sulla solidità del modello operativo, capacità di assumere responsabilità e sulla credibilità nel gestire a 360 gradi la sicurezza del cliente.

3.8 Analisi della domanda di cybersecurity e implicazioni per i modelli MSSP

Nelle sezioni precedenti è stato analizzato il mercato lato offerta, valutando le dinamiche competitive del settore. In questa sezione analizzeremo la domanda di mercato, differenziandola per grandi e piccole organizzazioni, alla luce delle pressioni individuate nel Capitolo 1. Concentreremo l'attenzione sulle condizioni che influenzano l'adozione della cybersecurity e le implicazioni per i modelli di servizio.

3.8.1 Overview – uno sguardo globale al mercato

A livello globale, la cybersecurity presenta una distribuzione di domanda frammentata per area geografica e per settore. La Figura 3.12 rappresenta la distribuzione dei ricavi nel mercato della cybersecurity per area geografica dove viene evidenziata una forte presenza degli Stati Uniti, seguita dalla forte digitalizzazione dell'Asia Pacifica e in particolare la Cina (Statista Market Insights, 2025a).

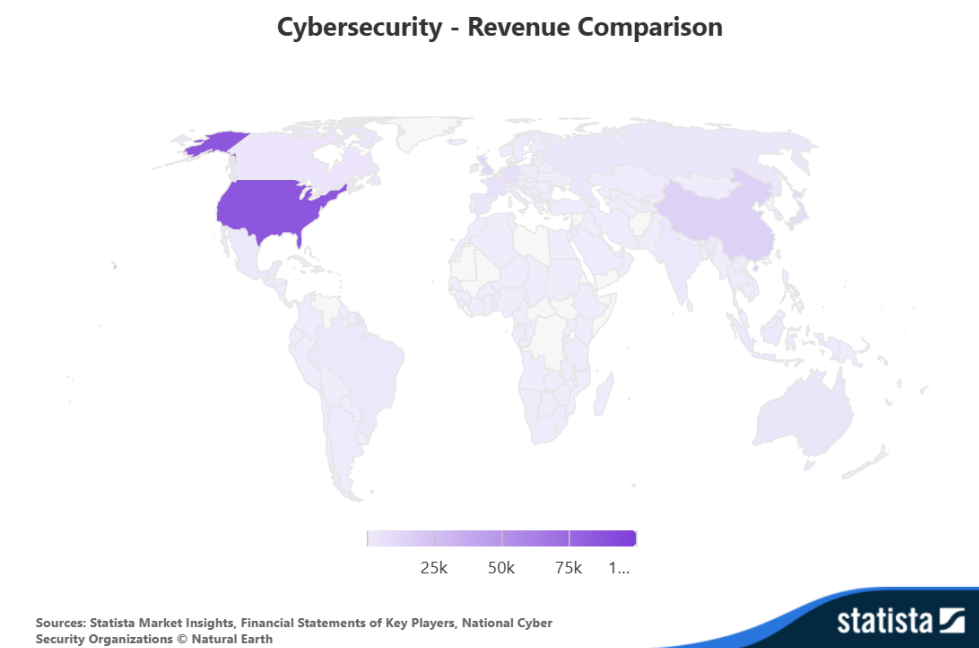


Figura 3.12 - [Revenue Comparison - Statista Market Insights, Financial Statements of Key Players, National Cyber Security Organizations](#)

Nella figura 3.13 sono distribuiti i ricavi per settore industriale con una significativa quota relativa alle entità finanziarie, come banche e assicurazioni, e nell'ambiente governativo (Statista Market Insights, 2025a).

Cybersecurity - Revenue industry share

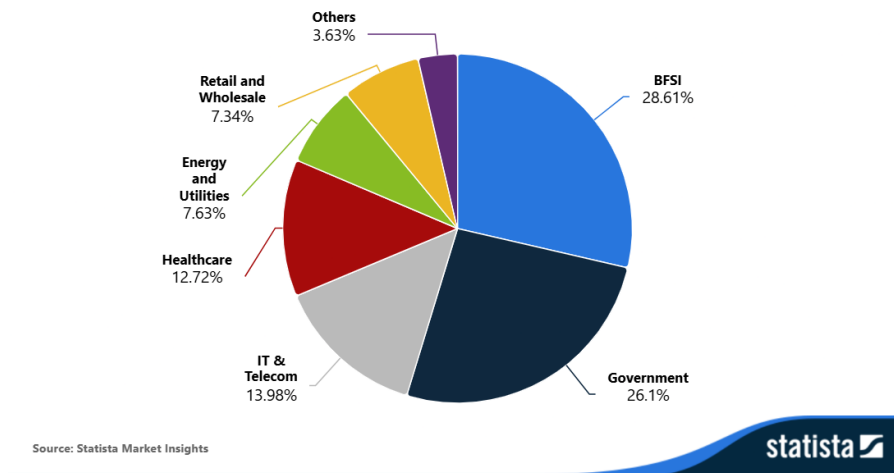


Figura 3.13: [Revenue industry share – Statista Market Insight](#)

La distribuzione degli attacchi informatici rappresenta caratteristiche eterogenee, con un forte coinvolgimento del settore delle industrie manifatturiere e delle organizzazioni finanziarie e assicurative (IBM, 2025b).

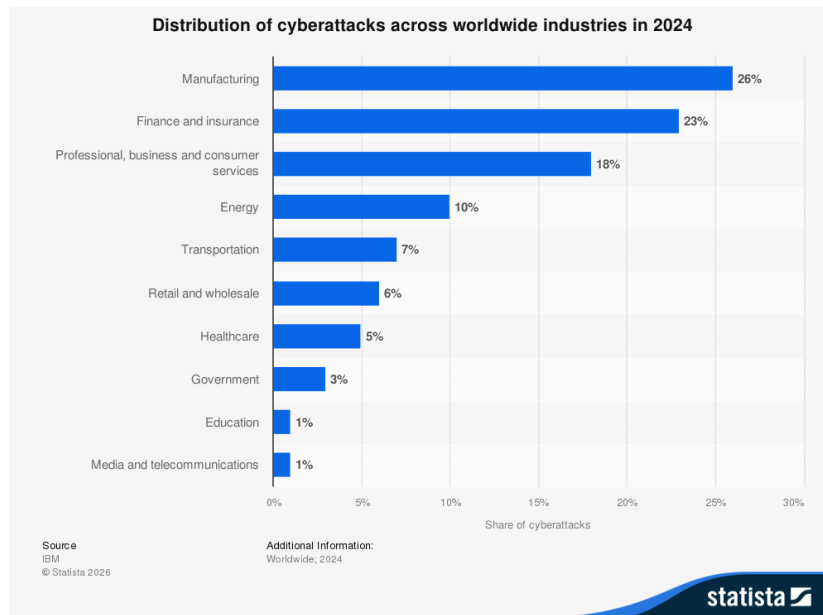


Figura 3.14 - [IBM, Distribution of cyberattacks across worldwide industries in 2024 - Statista](#)

Questo quadro permette di definire i principali settori da analizzare:

- Banking, Financial Services and Insurance;
- Government;
- Industrial & Manufacturing.

3.8.2 Banking, Financial Services and Insurance

Questo settore rappresenta la principale fonte di ricavi del mercato della cybersecurity dovuto a delle esigenze strutturali che lo contraddistinguono come la forte digitalizzazione di dati sensibili, una tolleranza operativa alle interruzioni molto bassa e un perimetro regolatorio stringente. In particolare, nel contesto europeo è emerso nelle sezioni precedenti come le normative giochino un ruolo fondamentale per l'adozione delle soluzioni di sicurezza informatica. In questo settore il regolamento europeo *Digital Operational Resilience Act (DORA)* impone vincoli specifici sulla gestione del rischio ICT delle organizzazioni e della catena di fornitori terzi, che si traduce in una crescita della domanda per tutti quei servizi di sicurezza informatica che garantiscano l'adeguamento alla norma. Inoltre, il settore è uno dei principali bersagli degli attacchi informatici a causa dell'elevato valore dei dati reperibili e delle misure di sicurezza adottate spesso insufficienti.

Nella lettura del report *Verizon Data Breach Investigation Report 2024* nella sezione *Financial and Insurance* system intrusion e social engineering costituiscono una quota rilevante degli incidenti e delle violazioni analizzate, coerentemente con la natura degli asset in gioco nel settore. Un'ulteriore evidenza arriva a livello europeo su phishing e frodi online come componente rilevante di rischio, insieme a malware ed estorsioni, nel *Threat Landscape di ENISA* dedicata al settore finance (Verizon, 2024; ENISA 2024a). Sempre nel report viene fatto riferimento alle minacce alla disponibilità, in particolare DDoS, che assumono rilievo anche in relazione a contesti geopolitici e attività di hacktivism.

In Italia il settore presenta un'attenzione crescente e i segnali arrivano direttamente dalle organizzazioni. Banca d'Italia pubblica negli ultimi anni un report denominato *Framework segnaletico di Vigilanza degli incidenti operativi o di sicurezza*, dove descrive le condizioni operative di sicurezza per valutare trend e nuove minacce comuni nel mercato finanziario italiano. In particolare, nell'analisi del 2024 viene evidenziata una crescita significativa di segnalazioni di incidenti rispetto agli anni precedenti (+58 segnalazioni rispetto al 2023), confermando la necessità di gestione e mitigazione del rischio cyber (Banca d'Italia, 2024).

Queste condizioni richiedono competenze specialistiche di gestione della sicurezza che difficilmente le entità finanziarie internalizzano e che frequentemente vengono affidati a fornitori di servizi di sicurezza gestiti per l'adeguamento alle normative e la protezione della continuità operativa.

3.8.3 Government

Nel demand market della cybersecurity, il settore Government si caratterizza per una domanda strutturale determinata da ampiezza e frammentazione del perimetro digitale da proteggere, criticità dei servizi erogati e pressione regolatoria che vede la pubblica amministrazione come settore ad alta criticità. ENISA sottolinea nel Sectoral Threat Landscape che la pubblica amministrazione in Europa svolge un ruolo critico nell'erogazione di servizi essenziali ai cittadini europei ed è considerata un settore ad alta criticità nel quadro regolatorio europeo (Enisa, 2024b).

A livello globale, la domanda di cybersecurity nel comparto governativo è inoltre alimentata dal fatto che le amministrazioni pubbliche sono un obiettivo privilegiato sia per attori criminali sia per attori legati a dinamiche geopolitiche. Da un lato, la pubblica amministrazione gestisce grandi volumi di dati personali e informazioni sensibili; dall'altro, rappresenta un target ad alto valore per attività di cyber spionaggio, interferenza e “hybrid threats”. In questa direzione, il Microsoft Digital Defense Report 2025 colloca il Government tra i primi settori più colpiti a livello mondiale da attacchi russi (25% dei target settoriali) e riporta che i paesi più frequentemente colpiti includono stati Uniti (20%), Regno Unito (12%) e Ucraina (11%), evidenziando la centralità dei target legati all'area NATO e al contesto geopolitico corrente (Microsoft, 2025b).

Mentre nel contesto operativo, il report *Cybersecurity Considerations 2025: Government & Public Sector* di KPMG, mette in luce come la figura del Chief Information Security Officer (CISO) nelle organizzazioni governative e del settore pubblico si trova ad affrontare una complessa rete di sfide che includono (KPMG, 2025):

- Aumento degli attacchi informatici negli ultimi cinque anni;
- Miglioramento della resilienza e riduzione dei rischi associati alle infrastrutture IT legacy;
- Rapido ritmo delle tecnologie emergenti come AI, blockchain e quantum computing
- Allineamento normativo con GDPR, DORA, NIS2 e eIDAS;

Data la natura degli attacchi informatici del settore, le organizzazioni tendono a richiedere soluzioni per la protezione degli accessi e dell'identità, come *Multi-Factor Authentication* e accessi privilegiati, e la salvaguardia della continuità operativa.

3.8.4 Industrial & Manufacturing

Nel demand market della cybersecurity, il settore *Industrial & Manufacturing* rappresenta un caso ad alta criticità non tanto per la natura dei dati trattati come nei due settori precedenti, quanto per l'impatto economico diretto che un incidente può produrre sulla continuità operativa. La trasformazione digitale legata all'Industry 4.0, l'integrazione crescente tra ambienti IT e OT e la dipendenza da supply chain aumentano in modo significativo la superficie d'attacco: la manifattura moderna combina sistemi gestionali e cloud con impianti, PLC, reti industriali e accessi remoti per manutenzione e teleassistenza. In questo contesto, la cybersecurity non è solo una funzione di protezione informativa, ma diventa una componente abilitante della produzione stessa: ridurre *down time*, prevenire blocchi di linea, proteggere proprietà intellettuale e garantire qualità e sicurezza del processo. Questa centralità si riflette anche nei principali threat report aggiornati al 2025. Secondo l'*IBM X-Force 2025 Threat Intelligence Index*, la manifattura è il settore più colpito per il quarto anno consecutivo; gli impatti più frequenti includono estorsione (29%) e data theft (24%), con obiettivi che spesso combinano monetizzazione e furto di know-how. IBM evidenzia inoltre che, "contro" il trend di riduzione del malware, nel 2024 la manifattura registra il maggior numero di casi ransomware, anche perché molti contesti industriali rimangono vincolati a tecnologie legacy difficili da aggiornare e segmentare rapidamente (IBM, 2025b). Sul perimetro europeo, l'*ENISA Threat Landscape 2025* conferma che, per il manufacturing, il cybercrime è la minaccia primaria sia per livello di attività sia per impatto (59,3%). La minaccia che sostiene la domanda nel manufacturing è dominata dal rischio di system intrusion e ransomware con impatto sulla disponibilità (ENISA, 2025). Da un punto di vista di domanda, questo profilo di rischio genera priorità di adozione abbastanza coerenti tra geografie, ma con intensità diverse tra grandi gruppi e PMI. Le large enterprise industriali tendono a investire su architetture integrate che uniscono identità, endpoint, rete e cloud, affiancate da capacità specifiche per OT (visibilità degli asset, segmentazione, monitoraggio passivo, controllo degli accessi remoti e procedure di incident response compatibili con vincoli di produzione). Le PMI manifatturiere, invece, spesso partono da requisiti minimi di resilienza (backup immutabili e recovery testato, hardening e MFA, gestione vulnerabilità e patching "realistico" per OT, monitoraggio continuo e risposta rapida), perché la prima metrica economica è la riduzione del rischio di fermo impianto e di fermo logistica, più che l'ottimizzazione di un portafoglio best-of-breed. In particolare, per le PMI risultano di essenziale importanza le figure degli MSSP che permettono di erogare servizi per i temi compliance che forzano investimenti cyber nel manufacturing con costi elevati e insostenibili per il piccolo e medio mercato. Inoltre, il valore degli MSSP deriva da una lacuna in competenze di security nel mondo dell'Industry & Manufacturing dovute alla natura del settore e priorità di investimenti passati disallineati con l'attuale evoluzione dell'ambiente lavorativo. Tra le normative più importanti e driver del settore troviamo la NIS2, Cyber resilience Act e la Machinery Regulation (per AI nei macchinari). Coerentemente con questi driver, le soluzioni maggiormente adottate nel settore non si concentrano su un singolo dominio, ma su una combinazione di controlli che massimizzano riduzione del rischio e continuità.

3.9 Sintesi interpretativa e implicazioni strategiche per gli MSSP

L'analisi sviluppata in questo capitolo ha mostrato come la transizione del paradigma dalle soluzioni frammentate "best-of-breed" a quello delle piattaforme multi-dominio AI-driven avvenga tramite una ricomposizione strutturale del mercato della cybersecurity, oltre che da un cambiamento ed evoluzione tecnologica. I limiti strutturali dell'ecosistema delle soluzioni tradizionali, pur essendo significativamente valide e specializzate all'interno dei singoli domini, quali complessità ed eterogeneità architetturale e modello economico organizzativo, hanno generato dei bisogni crescenti nelle organizzazioni per l'evoluzione del mercato della cybersecurity. Le evidenze emerse attraverso l'analisi del settore con l'applicazione dei framework teorici, indicano che il valore competitivo non risiede più nella sola performance della singola tecnologia, ma nelle capacità di orchestrare ed integrare funzionalità eterogenee, efficientare il processo operativo e tradurre le tecnologie in risultati misurabili in termini di riduzione di rischio e resilienza operativa. L'uso di piattaforme però non è facilmente internalizzabile per tutte le organizzazioni, in particolare per quelle del segmento mid-market dove il gap di competenze specialistiche, la crescente pressione normativa e l'evoluzione della tipologia di attacchi rendono complicato il passaggio da disponibilità di strumenti di sicurezza informatica alla reale gestione del rischio. In questo scenario, il ruolo dei *Managed Security Service Provider* diventa fondamentale a patto che il modello di business vada oltre alla semplice integrazione di soluzioni frammentate e diventi un layer di governance, orchestrazione e contestualizzazione delle piattaforme stesse, in grado di seguire tutto il ciclo di vita della sicurezza informatica del cliente ed erogare un servizio continuativo orientato ai risultati per il cliente come riduzione del rischio, continuità operativa e conformità normativa.

Alla luce di queste dinamiche, diventa determinante comprendere a pieno come un fornitore di servizi di sicurezza gestiti possa strutturare la propria architettura operativa e il proprio modello di servizio per seguire questa trasformazione e migliorare la propria competitività, mantenendo al contempo scalabilità, efficienza e coerenza strategica. Il Capitolo 4 approfondisce queste implicazioni attraverso lo studio condotto in collaborazione con l'azienda Nais, fornitore di servizi di sicurezza italiano con piattaforma di orchestrazione proprietaria, offrendo un osservatorio privilegiato sulle scelte e leve strategiche, integrazione dell'intelligenza artificiale nei processi e sulle possibili traiettorie replicabili da altri operatori nel settore.

4. Ruolo strategico di un MSSP nell'era dell'AI - Caso Nais

Nel capitolo precedente è stata analizzata l'evoluzione e le dinamiche competitive del mercato della cybersecurity, individuando le implicazioni dirette per un Managed Security Service Provider. Il presente capitolo applica le evidenze teoriche attraverso l'analisi delle scelte strategiche di Nais, fornitore di servizi di sicurezza gestiti operante nel mercato italiano, con particolare focus sul segmento mid-market. L'analisi si fonda sul tirocinio curricolare svolto presso l'azienda (settembre – dicembre 2025), con l'obiettivo di identificare quelle che sono le leve strategiche per un MSSP per rimanere competitivo nell'evoluzione del mercato e in particolare quella relativa all'integrazione dell'intelligenza artificiale nei processi operativi del *Security Operation Center*. Il caso Nais risulta particolarmente rilevante per tre motivi principali. Il primo è relativo al modello operativo di *Augmented SOC* sviluppato dall'azienda fondato tramite componenti proprietarie di automazione e orchestrazione. In secondo luogo, la rappresentatività del contesto mid-market italiano, caratterizzato da forte pressione normativa, crescita accelerata della domanda e limitata disponibilità di competenze specialistiche interne delle organizzazioni operanti. Infine, il percorso di sviluppo aziendale è fondato su un programma di crescita orientato all'innovazione tecnologica e organizzativa, con iniziative strategiche, come l'integrazione dell'intelligenza artificiale nei processi operativi, osservabili in modo diretto grazie alla collaborazione con l'azienda. La seguente analisi si propone quindi di individuare e valutare le leve strategiche attraverso cui un MSSP può evolvere il proprio modello di servizio nell'era dell'intelligenza artificiale.

4.1 Posizionamento competitivo e problema strategico

Nais, fondata nel 2015, è un *Managed Security Service Provider* italiano specializzato nell'erogazione di servizi di sicurezza gestita per organizzazioni di diversi settori, con focus prevalente sul segmento mid-market in Italia e nel sud Europa. Il portafoglio clienti di Nais si distribuisce prevalentemente nei settori del comparto industriale, dei servizi e della pubblica amministrazione. L'offerta dell'azienda si articola principalmente attorno a servizi di SOC-as-a-Service, monitoraggio continuo dello stack di sicurezza del cliente con attività di detection & response, attività di prevenzione e predizione delle minacce attraverso strumenti e team specializzati e, infine, supporto alla compliance normativa. Nel 2024 l'azienda ha avviato un percorso di evoluzione organizzativa e tecnologica, caratterizzato dallo sviluppo della piattaforma proprietaria *Fluxstorm* concepita come ambiente centralizzato di orchestrazione e gestione dei servizi di sicurezza erogati, che unisce tecnologia e gestione operativa in unico punto di controllo (*Single point of Governance*). Parallelamente, è stata rafforzata la struttura commerciale con un approccio *business-oriented*, al fine di sostenere il percorso di crescita e strutturare in modo scalabile l'offerta di servizi.

Questa continua evoluzione ha determinato una crescita significativa della base clienti e del volume di eventi di sicurezza gestiti, con un conseguente aumento del carico operativo del *Security Operation Center*:

- Crescita di circa il 70% della base clienti nel 2025 rispetto al 2024;
- Numero medio di ticket mensili gestiti dal SOC nel 2025 pari a 35 mila;
- Il numero di ticket mensili gestiti dal singolo operatore è risultato circa 9 volte superiore rispetto al 2024.

La crescita è stata in parte assorbita dal modello operativo di *Augmented SOC*, dove le attività di monitoraggio, triage e gestione degli eventi di sicurezza sono supportate da componenti di automazione avanzata volte a ridurre il rumore generato dai falsi positivi e gestire autonomamente attività con basse criticità. Questo ha permesso di automatizzare gran parte del lavoro a criticità ridotta e definire quelli che sono i ticket “*full automated*” completamente gestiti con automazioni, che rappresentano circa l’80% del carico operativo complessivo. Il workload effettivo degli operatori è allocato principalmente sulle attività parzialmente automatizzate denominate “*semi-automated*” e da quelle che non hanno nessun principio di automazione e richiedono il completo intervento umano chiamate “*not automated*”. Queste sono tipicamente attività con criticità più elevate, ma caratterizzate da una quota non trascurabile di falsi positivi che impattano direttamente sul tempo di lavoro degli analisti e sul carico totale del SOC. Queste condizioni hanno reso necessario la strutturazione in modo sistematico dell’implementazione dell’intelligenza artificiale nei processi operativi, con l’obiettivo di incrementare l’efficienza nella gestione operativa del carico di lavoro, mantenendo invariata la qualità dei servizi di sicurezza erogati al cliente.

In questo contesto si colloca la collaborazione oggetto del presente capitolo, focalizzata sulla gestione strategica della crescita aziendale attraverso due attività principali:

- Attività 1, definizione delle leve strategiche per un MSSP in evoluzione nel mercato della cybersecurity;
- Attività 2, definizione della strategia di implementazione dell’intelligenza artificiale nei processi operativi del SOC;

Nelle sezioni successive verrà effettuata un’analisi dettagliata delle attività svolte, con particolare attenzione ai risultati ottenuti e sulle implicazioni per i modelli MSSP in un contesto di mercato in rapida evoluzione.

4.2 Definizione delle leve strategiche

Nel capitolo precedente l'analisi delle dinamiche competitive del mercato della cybersecurity ha permesso di definire il perimetro operativo per gli MSSP, con particolare attenzione al segmento mid-market. Dati i risultati ampiamente trattati in precedenza, è di fondamentale importanza individuare quelle che sono le leve strategiche che consentono ad un MSSP, nel caso specifico Nais, di governare in modo coerente la transizione del modello di servizio nell'era dell'intelligenza artificiale. La combinazione del contesto competitivo e l'osservazione diretta dei processi operativi e commerciali aziendali hanno permesso di identificare 5 principali leve strategiche per l'evoluzione di un MSSP.

4.2.1 Scalabilità operativa del SOC

La prima leva consiste nella capacità di gestire un volume crescente di eventi e ticket mantenendo il medesimo livello di servizio e sostenibilità economica. L'impatto della crescita non può essere mitigato attraverso un aumento proporzionale e lineare delle risorse umane, perché questo rifletterebbe una relazione diretta con la crescita dei costi e una riduzione del margine. In particolare modo nel segmento mid-market, dove la domanda è in aumento ma la disponibilità a pagare è ridotta, la scalabilità deve derivare da una evoluzione del modello operativo. Nel caso di Nais, una crescita dei clienti impatta profondamente l'operatività del *Security Operation Center*, dove c'è la necessità di ridistribuire il carico di lavoro degli analisti alle componenti di automazione, permettendo di assorbire la crescita senza compromettere gli SLA (*Service Level Agreement*). Questa leva è strettamente connessa alla strategia di implementazione dell'intelligenza artificiale che verrà quindi approfondita nel paragrafo successivo.

4.2.2 Orchestrazione multi-vendor e neutralità tecnologica

Nell'ecosistema della cybersecurity analizzato, l'orchestrazione e un approccio agnostico alle tecnologie consentono ad un MSSP di posizionarsi come figura di riferimento per i clienti. In assenza di tale capacità il fornitore di servizi di sicurezza gestiti rischia di essere identificato come semplice rivenditore di tecnologie e come *system integrator*, perdendo la reale capacità di rispondere ed adattarsi alle esigenze del cliente e di seguirlo in modo completo. Questa è una leva importantissima anche nei confronti dei vendor piattaforma, che in contesti come quelli del mid-market non hanno la capacità di soddisfare le reali esigenze del mercato che vanno oltre alla diminuzione della complessità tecnologica e di controllo. L'orchestrazione consente agli MSSP di adattare le diverse tecnologie alle caratteristiche specifiche dei clienti permettendo di correlare e prioritizzare i dati, mitigare il rischio di vendor lock-in generato dalle piattaforme multi-dominio e mantenere un approccio agnostico volto a garantire la migliore soluzione per i bisogni del cliente. La capacità di rendere completamente personalizzabile l'esperienza del cliente in base alle necessità è un punto di forza estremamente significativo per la competitività nel settore e la differenziazione. Nais ha implementato questa leva strategica attraverso la piattaforma proprietaria *Fluxstorm*, che funge da *single point of governance* per l'intero stack di soluzioni di sicurezza del cliente, garantendo visibilità end-to-end e correlazione cross-dominio.

4.2.3 Standardizzazione dell'offerta

Nel contesto del mid-market è importante rispondere ai vincoli economici e organizzativi attraverso la formalizzazione di bundle di servizi replicabili. La standardizzazione consente di ridurre i costi di prevendita e delivery, semplificare i processi di *onboarding* dei clienti, facilitare l'industrializzazione dei processi SOC e supportare il modello commerciale con pacchetti distinti e chiari in base alla fascia di mercato di riferimento. I bundle di offerta devono rispondere alla reale domanda di mercato, sfruttando le opportunità derivanti da fattori esterni come, ad esempio, i temi della compliance. La capacità di reagire prontamente alle esigenze con modelli di offerta replicabili è una condizione abilitante per la scalabilità operativa.

4.2.4 Integrazione di servizi complementari e partnership

La quarta leva strategica è costituita dall'integrazione di servizi complementari e partnership strutturate. Molti MSSP concentrano la loro proposta di valore nel facilitare l'integrazione di tecnologie e diminuirne la complessità percepita, lasciando un terreno scoperto in tutti quei servizi che permettono di posizionarsi come partner dei clienti. Il valore non risiede soltanto nelle performance delle tecnologie, ma quanto il cliente riesca a percepire la necessità e l'utilità della sicurezza informatica. Nel mid-market, le organizzazioni richiedono un interlocutore unico capace di affrontare la complessità del rischio cyber, e di seguire tutto l'intero ciclo di gestione del rischio con servizi come quelli relativi all'adeguamento normativo e la fase di recovery dopo un incidente. I servizi complementari svolgono un ruolo di amplificatore della proposta di valore: la consulenza compliance diventa un prerequisito per abilitare i servizi cyber, individuando le lacune in termini di gestione del rischio e definendo un piano strutturato di messa a norma attraverso l'integrazione di monitoraggio e controllo richiesti per legge. L'accesso a polizze assicurative cyber è spesso complicato dovuto ad una serie di requisiti minimi stringenti che devono essere implementati da parte del cliente, inoltre la sottoscrizione si basa su un'analisi statica fondata sulle risposte a lunghi questionari che non quantificano realmente in termini di rischi e costi la vera postura di sicurezza del contraente.

Un MSSP deve utilizzare questi canali come opportunità per seguire i clienti con una percezione del valore della sicurezza informatica superiore a quella della mera integrazione e gestione tecnologica. In questo contesto, le partnership con assicuratori e consulenti legali risultano significativamente importanti per accedere a competenze specialistiche senza internalizzarle, preservando flessibilità finanziaria e organizzativa in un contesto in rapida crescita.

4.2.5 Governance dell'innovazione tecnologica (AI)

Per governance dell'innovazione tecnologica si intende la capacità dell'organizzazione di introdurre ed integrare progressivamente nuove tecnologie nel modello operativo e nei servizi erogati. Nell'era dell'intelligenza artificiale, un MSSP deve adottare questa tecnologia come componente che modifica processi, ruoli e responsabilità all'interno di un SOC. Per fare questo, dunque, bisogna definire priorità di adozione, strategia e criteri di valutazione che verranno ampiamente discussi nella sezione successiva.

Le cinque leve individuate costituiscono un framework di riferimento strategico per l'evoluzione di un MSSP, in particolare nel segmento mid-market. Nella prossima sezione verranno approfondite le leve relative della “*Scalabilità del SOC*” e “*Governance dell'innovazione tecnologica (AI)*”, applicandole alla strategia di implementazione dell'intelligenza artificiale, sviluppata nel tirocinio curricolare con Nais, per rispondere alla crescita della domanda e alla complessità del nuovo scenario competitivo.

4.3 Strategia di implementazione dell'AI nei processi SOC

4.3.1 Approccio metodologico utilizzato

Fase 1 – Analisi del processo SOC end-to-end

La base di partenza è stata quella di mappare l'intero processo operativo del *Security Operation Center*, per comprendere e valutare le diverse fasi di gestione degli eventi di sicurezza, dalla generazione dell'alert fino alla chiusura del ticket. Il processo viene supportato da delle *playbook*, uno strumento dinamico che permette di definire procedure standardizzate per classificare e applicare azioni di contenimento agli eventi, che riducono il rumore in entrata generato dalla maggior parte dei falsi positivi. Il principale collo di bottiglia è stato individuato nella presa in carico dei ticket da parte degli operatori che non seguiva delle linee guida standardizzate e causava problematiche nella definizione del *tempo reale di gestione di un alert*, dovuto a dinamiche come la possibilità di prendere in carico più ticket in parallelo. Queste analisi hanno permesso di studiare il processo e ridefinirlo coerentemente con le logiche della piattaforma e le policy desiderate, strutturando un ambiente operativo abilitante all'integrazione dell'intelligenza artificiale. Le dinamiche relative all'assegnazione dei ticket sono state il primo ostacolo da affrontare, in quanto non rappresentava solo una caratteristica tecnica ma un metodo lavorativo consolidato dagli analisti del SOC. La fase di modifica delle procedure è stata quindi introdotta gradualmente per permettere il corretto funzionamento della piattaforma e il relativo apprendimento da parte degli operatori. Questa prima fase ha permesso quindi di definire correttamente il *tempo medio di analisi e di gestione di un alert* utile ai fini del reale valore dei KPI operativi per permettere una prima valutazione sulle tempistiche in relazione al carico di lavoro e, inoltre, ha abilitato un processo standardizzato univoco di gestione degli eventi per tutti gli analisti.

Fase 2 - Classificazione del workload per grado di automazione

Successivamente è stata effettuata un'analisi per classificare il carico di lavoro attraverso tre categorie principali:

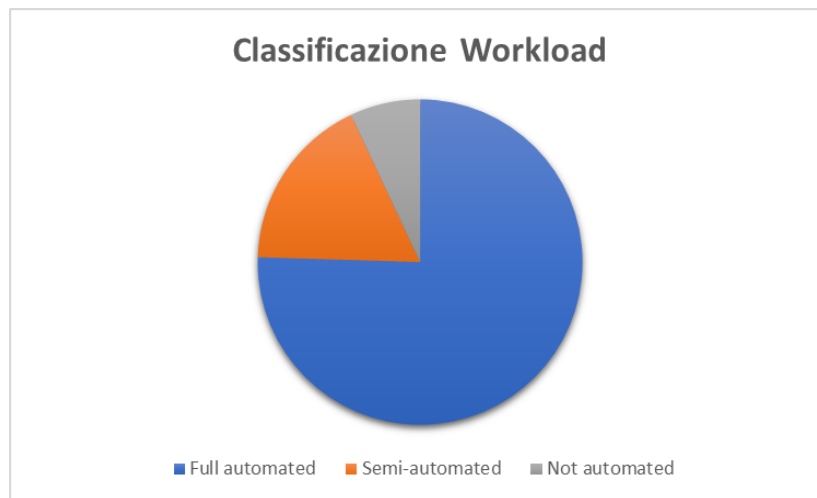


Figura 4.1 — Distribuzione workload per grado di automazione

- *Full automated*, rappresenta circa l'80% del volume totale dei ticket, sono gestiti ed automatizzati dalle *playbook* presenti nella piattaforma. Il tempo medio di gestione è vicino allo zero, determinato dal fatto che ci sono regole predefinite che permettono di individuare tutti quei ticket che non richiedono un intervento umano perché falsi positivi o con richiesta di chiusura automatica concordata col cliente;
- *Semi-automated*, rappresenta circa il 15% del volume totale dei ticket, sono caratterizzati da priorità *bassa e media* di rischio e presentano un elevato numero di falsi positivi che devono essere verificati. Il *tempo medio di analisi stimato*, comprensiva di gestione dell'operatore e *idle time*, è di 30 minuti;
- *Not automated*, rappresenta circa il 5% del volume totale dei ticket, sono caratterizzati da priorità *alta e critica* e richiedono un forte intervento umano perché potrebbero rappresentare un vero e proprio incidente informatico. Il *tempo medio di analisi stimato* è di 45 minuti.

Questa classificazione ha permesso di individuare il principale collo di bottiglia nei ticket *semi-automated* che, nel periodo di analisi, aumentano pesantemente il carico operativo degli analisti.

Fase 3 – Raccolta di evidenze qualitative dagli analisti

Nel periodo precedente alla collaborazione con l'azienda, era stato sviluppato un primo tentativo di implementazione dell'intelligenza artificiale nei processi ma che ha ottenuto scarsi risultati. L'obiettivo è stato quello di ricavare delle evidenze qualitative tramite interviste e questionari sottoposti agli analisti del SOC per comprendere lo scarso utilizzo della soluzione e le principali lacune percepite.

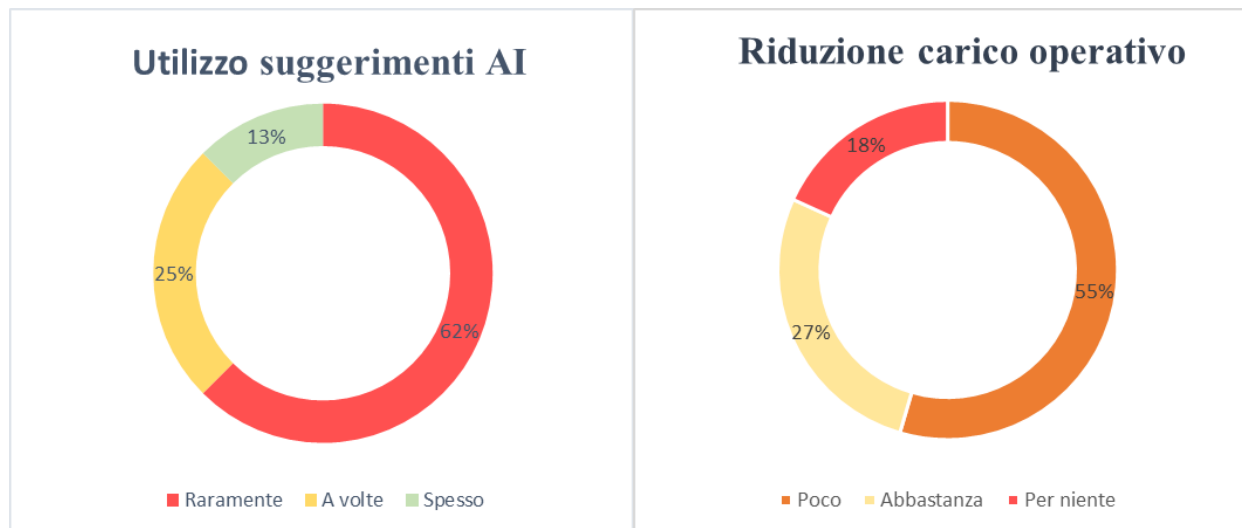


Figura 4.2 - Utilizzo dei suggerimenti AI dagli analisti

Figura 4.3 - Riduzione del carico operativo grazie all'AI

Le Figure 4.2 e 4.3 rappresentano i risultati relativi alle domande del questionario inerenti all'utilizzo effettivo dei suggerimenti delle analisi svolte dall'intelligenza artificiale e dalla relativa riduzione del carico operativo. I dati evidenziano uno scarso utilizzo delle analisi e una bassa percezione della riduzione del carico del lavoro. Le motivazioni principali sono emerse tramite le interviste singole sottoposte ad ogni analista:

- L'AI genera contesto sull'evento ma non ha funzionalità di correlazione sulle attività dei ticket;
- Risposte spesso inutilizzabili a causa di allucinazioni;
- Processo di feedback lungo che grava sul carico operativo.

La prima implementazione dell'intelligenza artificiale è stata pensata come un unico agente che supporta la fase di analisi, ma che richiede troppo effort nelle valutazioni e non restituisce i benefici attesi di automazione e riduzione del carico operativo. Il modello utilizzato era pensato per ricevere le informazioni disponibili dalle *playbook* in modo statico e restituire un'analisi coi dati disponibili, che molto spesso non erano sufficienti per formulare una risposta completa e generava dunque delle allucinazioni.

Fase 4 – Analisi dei trade-off strategici

In questa fase sono state valutate diverse modalità di adozione dell'intelligenza artificiale nei processi del *Security Operation Center*, con l'obiettivo di valutare in che modo le differenti configurazioni tecnologiche e organizzative potessero influenzare la scalabilità operativa, la qualità delle analisi e il livello di controllo degli operatori umani.

La prima dimensione valutata è stata quella del grado di automazione dei processi operativi. Dalle analisi svolte nella fase 1 e 2 è risultato evidente come gli elementi di interesse riguardassero principalmente i ticket *semi-automated* e *not automated*. Di fronte questo scenario sono state valutate due soluzioni di automazione: modelli orientati all'automazione completa e modelli *"Human in the loop"*.

I modelli orientati all'automazione completa sono rappresentati da sistemi AI che gestiscono in modo indipendente l'intero ciclo di vita di un incidente di sicurezza, dalla ricezione dell'evento alla risposta e chiusura del ticket, senza alcuna supervisione umana nel flusso operativo. Questi modelli possono processare volumi illimitati di alert senza incremento proporzionale di personale, eliminando la varianza decisionale di un analista umano e definendo risposte standardizzate alle policy dell'azienda. In un contesto con grandi volumi di ticket come quello di Nais, questo modello potrebbe idealmente permettere di mitigare a pieno la crescita della base clienti senza aumentare linearmente i costi fissi di personale. Questo modello però ha delle controindicazioni che limitano fortemente l'adozione, in particolare nelle fasi iniziali di implementazione. La struttura richiede una maturità di utilizzo della soluzione e un'accuratezza delle risposte generate significativa, che non può essere applicata nelle prime fasi di adozione dove il rischio di falsi positivi e risposte automatizzate errate diventa inaccettabile.

I modelli *"Human in the loop"* o *"AI-Augmented SOC"* sono caratterizzati dall'applicazione dell'intelligenza artificiale a supporto dell'analista umano. L'AI gestisce autonomamente i task a bassa complessità e alta ripetibilità come correlazione di log, classificazione degli alert e arricchimento contestuale del ticket, lasciando le fasi di risposta, comunicazione col cliente ed eventuali escalation all'analista umano. Questo modello, in particolare per un MSSP con focus sul mid-market, permette di integrare progressivamente l'intelligenza artificiale e gestire il grado di automazione, mantenendo una supervisione umana che fornisce garanzia di accountability e interlocuzione professionale per i clienti in caso di incidente reale. La limitazione di questo modello risiede nella scalabilità non lineare, in quanto il *throughput* complessivo è vincolato dalla capacità degli analisti di gestire le escalation e le validazioni; quindi, la crescita del numero dei clienti richiede comunque un aumento del personale anche se non lineare. Questo vincolo però è mitigabile tramite un graduale aumento di automazione nel tempo, permettendo di far accumulare dati storici all'intelligenza artificiale sufficienti a raggiungere soglie di affidabilità accettabili.

La seconda dimensione invece riguarda il tipo di architettura da adottare: soluzione AI monolitica e architettura multi-agente.

L'approccio del singolo agente AI prevede la gestione unificata delle funzioni del SOC tramite correlazione degli alert, *enrichment*, triage, generazione di raccomandazioni e produzione di report. Seppur questa soluzione permette di avere un sistema unico che mantiene una visione olistica e continua di tutti gli eventi in corso, presenta una rigidità funzionale dovuta alla riduzione delle performance in presenza di contesti atipici o non sufficientemente affrontati nella fase di allenamento. Inoltre, il malfunzionamento di un singolo agente con capacità trasversali

significherebbe bloccare l'intero sistema di automazione e di gestione degli eventi con ripercussioni disastrose per l'erogazione di un servizio continuativo come quello del SOC.

L'architettura multi-agente prevede la decomposizione delle funzioni in diversi agenti specializzati autonomi, dove ognuno è ottimizzato in una singola funzione: un agente per l'analisi, uno per l'*enrichment*, uno per il triage, uno per il controllo del comportamento dei precedenti e tutte le soluzioni possibili desiderate. Questi agenti operano in modo coordinato, passandosi informazioni sequenziali o parallele, con un orchestratore centrale che gestisce l'intero flusso. I vantaggi di questo approccio sono significativi, in particolare la possibilità di avere specializzazione funzionale del singolo agente con un modello ottimizzato all'azione da compiere. Inoltre, la modularità evolutiva permette di aggiornare, sostituire o aggiungere singoli agenti senza impatti sull'intera architettura, ideale per una condizione di implementazione incrementale. Le criticità relative al seguente modello sono dovute alla difficoltà di allenare diversi agenti nell'eseguire correttamente le attività assegnate e di mitigare le possibilità di errori nelle valutazioni.

L'analisi condotta e combinata di queste dimensioni ha evidenziato che, nel contesto operativo analizzato, il modello più coerente è rappresentato da un approccio ibrido di *Augmented SOC* supportato da architettura multi-agent per l'automazione. Gli sviluppi della strategia verranno analizzati nella fase successiva.

Fase 5 – Adozione strategica dell'AI nei processi operativi

Per concludere l'analisi condotta, è stata definita una roadmap di implementazione dell'intelligenza artificiale coerentemente con le evidenze raccolte nelle fasi precedenti.

Step 1 – Tool Augmented Agent (6 mesi)

Il primo stadio nasce dall'esigenza di affrontare la criticità strutturale più rilevante emersa dall'analisi preliminari sul processo del SOC, ovvero ridurre l'elevato tasso di falsi positivi nella categoria dei ticket *semi-automated* e abilitare il reale utilizzo dell'intelligenza artificiale da parte degli operatori. La risposta architetturale è la decomposizione del primo modello in due agenti specifici: un *Analysis Agent* responsabile dell'attività di analisi delle informazioni ricevute dall'*Enrichment Agent*, responsabile di fornire contesto informativo strutturato interrogando le *playbook* disponibili e, in caso di informazioni insufficienti, comunicare con la piattaforma per estrapolare i dati mancanti. Questo processo è circoscritto alla categoria *semi-automated* e viene svolto in parallelo con le attività di revisione delle *playbook*. Il piano abilita la produzione di risposte direttamente utilizzabili dagli analisti, che ricevono una scheda precompilata con le informazioni raccolte e le raccomandazioni proposte, e l'automazione della chiusura dei falsi positivi attraverso la funzione *similarity*. Il sistema attraverso le informazioni ricavate calcola il grado di somiglianza tra il ticket in analisi e i casi storici già risolti, e procede alla chiusura automatica senza intervento umano al superamento di una soglia di confidenza predefinita conservativa in fase iniziale. Questa soglia permette di ridurre al minimo gli errori ed evitare che un potenziale attaccante possa eludere il sistema con un incidente reale simile ad un falso positivo, verrà revisionata periodicamente con la parallela crescita del grado di confidenza.

Step 2 – Multi-agent Collaborative System (mesi 6 – 18)

Una volta consolidato il primo step, l'obiettivo è quello di aumentare il numero di agenti con competenze di dominio profondamente diverse per la transizione verso una vera e propria architettura multi-agente. In questa fase alcune attività standardizzabili vengono gestite direttamente dagli agenti di intelligenza artificiale, con intervento umano limitato a casi complessi o a maggiore criticità. Questo passaggio ha quindi l'obiettivo di rendere completamente automatizzati i ticket della categoria *semi-automated*, con supervisione degli operatori ai casi con insufficiente confidenza dei modelli, e lasciare il carico operativo degli analisti sui ticket *not automated*. La fase avrà un primo momento di verifica e controllo delle analisi generate dal modello, in modo da seguire l'incrementale evoluzione del processo. Inoltre, la fase di controllo e introduzione permette di prevenire le complessità di coordinamento come latenza decisionale, conflitti di output, opacità diagnostica e overhead operativo che si possono generare con l'introduzione di nuovi agenti nel sistema ed erodere i benefici marginali attesi.

Step 3 – Advanced Decision Support (mesi 18+)

Una volta consolidato il processo e l'automazione dei ticket *semi-automated*, l'obiettivo è quello di ridurre ulteriormente il carico operativo estendendo l'automazione sulla categoria *not automated*. I ticket in questa classificazione hanno caratteristiche profondamente diverse dovute alla complessità, ambiguità contestuale e scarsa rappresentazione nei dataset storici. Questo step ha quindi l'obiettivo di estendere il sistema multi-agente come supporto decisionale per gli analisti e riclassificare progressivamente le sottocategorie di *not automated* in *semi-automated*. La prima dinamica è un'estensione naturale del processo di implementazione dove, una volta consolidata e automatizzata la gestione dei *semi-automated*, il modello deve ampliare le proprie capacità di *enrichment* e correlazione a supporto delle analisi più complesse per gli analisti. La seconda invece ha l'obiettivo di ridurre la quantità di *not automated* tramite il miglioramento continuo di *playbook* alimentato dalle evidenze e meccanismi raccolti negli step precedenti, accumulo di casistica storica e affinamento di capacità di arricchimento dati del sistema multi-agente.

Questo introduce nella roadmap un meccanismo di feedback strutturale in continuo miglioramento, dove ogni ticket *not automated*, analizzato tramite il supporto AI, genera un data point che nel tempo contribuisce a costruire le condizioni per la standardizzazione futura. L'autonomia operativa completa sui ticket residui è valutabile solo quando il processo di miglioramento e riclassificazione avrà ridotto i ticket non automatizzabili ad una quantità minima accettabile.

4.4 Evidenze preliminari e segnali quantitativi

Premessa metodologica

I dati presentati in questo paragrafo si riferiscono al periodo novembre 2025-febbraio 2026, corrispondente alla fase precedente all'implementazione della strategia (novembre 2025-dicembre 2025) e alla fase di avvio dell'implementazione presso il SOC di Nais (gennaio 2026-febbraio 2026). La finestra temporale osservata è limitata e non consente conclusioni statisticamente definitive: l'obiettivo è quello di identificare i primi segnali quantitativi che confermano o sfidano le assunzioni della strategia. In particolare, andremo ad analizzare l'andamento del tasso di falsi positivi e la distribuzione volumetrica dei ticket per categoria con attenzione su quelli gestiti dall'intelligenza artificiale. La base di dati è stata estratta direttamente dalla piattaforma SOC di Nais e non hanno subito elaborazioni successive.

4.4.1 Espansione della copertura AI: distribuzione volumetrica dei ticket

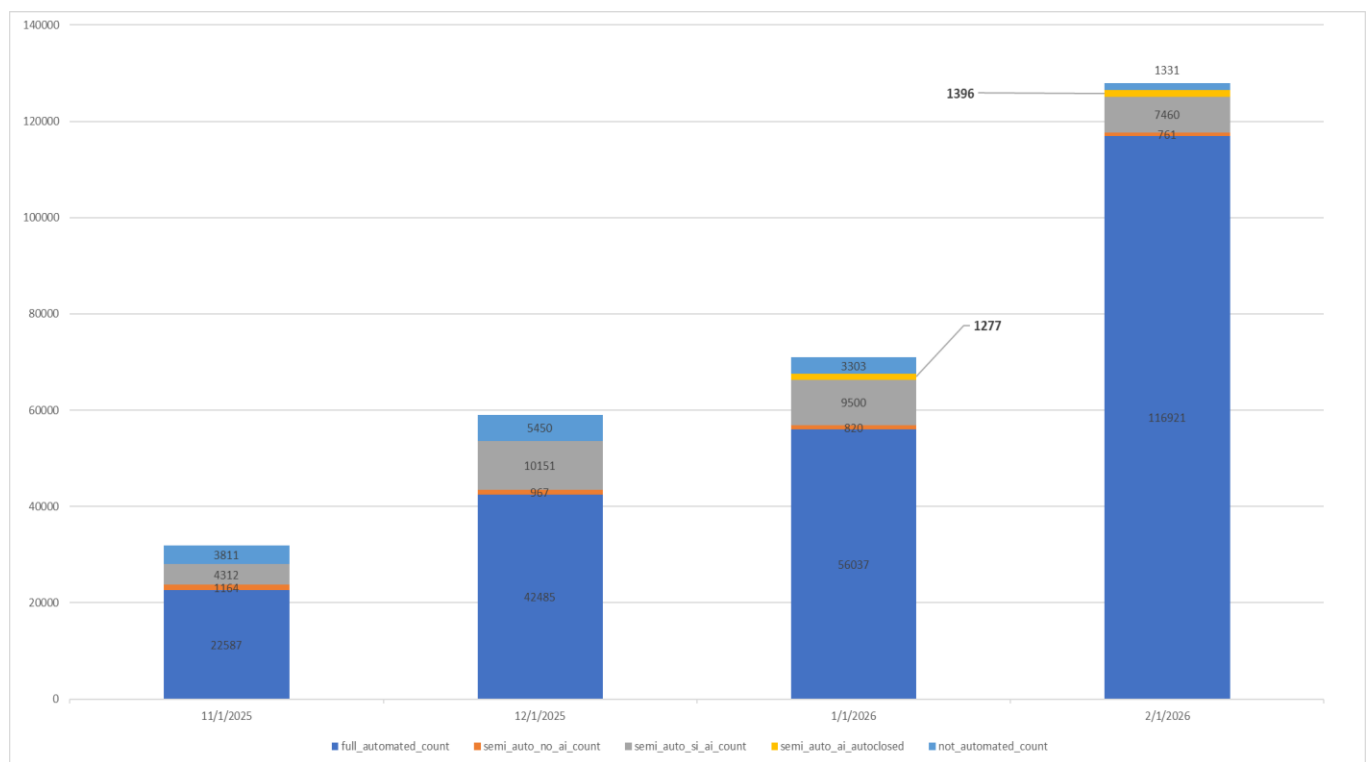


Figura 4.4 - Distribuzione mensile dei ticket per categoria di gestione (nov. 2025 – feb. 2026)

Il primo elemento di evidenza riguarda l'evoluzione della distribuzione dei ticket per categoria di gestione nel periodo osservato. I ticket *full automated* hanno registrato una crescita significativa da novembre 2025 a febbraio 2026, traiettoria che non riflette esclusivamente la crescita dei clienti ma il progressivo allargamento del dominio di copertura automatica su tipologie di ticket precedentemente gestiti con un intervento umano. Questo segnale è direttamente proporzionale alle attività di miglioramento *playbook* svolto in parallelo con l'implementazione dell'intelligenza artificiale. L'elemento più rilevante riguarda il numero di ticket chiusi e gestiti dall'intelligenza artificiale:

Tabella 4.1 — Confronto tra modello AI monolitico e Tool-Augmented Agent sui ticket semi-automated

Categoria	AI Monolitica (Nov-Dic 2025)	Tool-Augmented Agent (Gen_Feb 2026)
<i>semi_automated_ai</i>	14,463	16,960
<i>semi_automated_ai_autoclosed</i>	0	2673

Nei mesi di Novembre e Dicembre 2025 era ancora attivo il modello precedentemente utilizzato di un unico agente AI, i risultati mostrano come ci fosse una totale assenza di chiusure automatiche. Con l’implementazione della strategia e, in particolare, con la funzione di *similarity* (precedentemente descritta nello Step 1) sono iniziati ad emergere i primi segnali di chiusura automatica certificata per somiglianza con casistica storica validata. La crescita del tasso di chiusura automatica è ancora moderata rispetto al numero totale di ticket della categoria, coerentemente con una fase iniziale di implementazione e con una fase di espansione attiva del perimetro di automazione.

Inoltre, nella Figura 4.4 sono presenti segnali di diminuzione del numero di ticket *not automated*. Attualmente questa metrica non è direttamente imputabile alla riclassificazione progressiva descritta nello Step 3 della strategia di implementazione, in quanto il periodo di osservazione è temporalmente limitato.

4.4.2 Riduzione del tasso di falsi positivi e contributo dell’AI

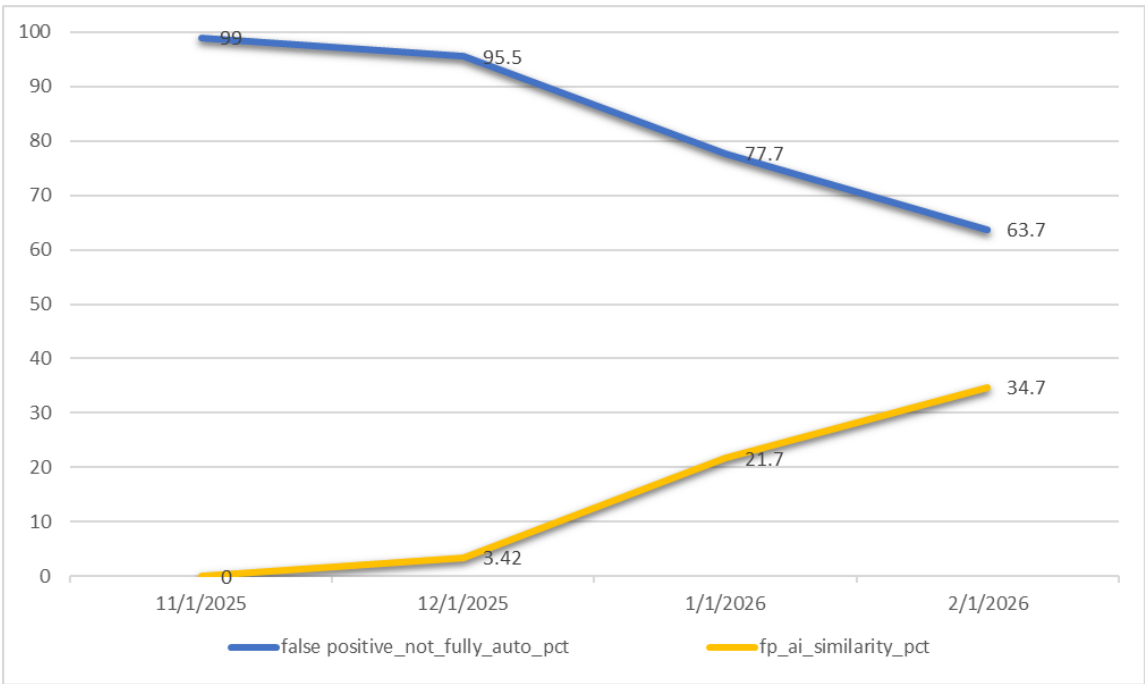


Figura 4.5 - Andamento del tasso di falsi positivi e contributo dell’AI

Il secondo elemento di evidenza riguarda l’andamento del tasso di falsi positivi nella categoria *semi-automated* nel periodo osservato, misurato attraverso due indicatori complementari presenti nella Figura 4.5.

I dati mostrano una riduzione sistematica della percentuale di falsi positivi sul totale della categoria considerata, pari a 35.3 punti percentuali nell’arco del periodo osservato. La riduzione accelera nei mesi di Gennaio e Febbraio 2026 con l’implementazione del *Tool Augmented Agent*, suggerisce un contributo specifico e incrementale della nuova architettura e del miglioramento delle *playbook*.

Il dato più interessante è legato alla chiusura automatica dei falsi positivi per *similarity*, rappresentato dalla curva gialla, raggiungendo il 34.7 % a Febbraio 2026 indicando che oltre un terzo dei falsi positivi gestiti dall’AI nella categoria viene chiuso in automatico.

Tabella 4.1 — Andamento degli indicatori di qualità AI sui ticket semi-automated

Metrica	Nov 2025 (monolitico)	Dic 2025 (monolitico)	Gen 2026 (Tool- Augmented)	Feb 2026 (Tool- Augmented)
False positive rate (%)	99.00	95.50	77.70	63.70
Chiusi da AI similarity (%)	0.00	3.42	21.70	34.70
Riduzione FP vs mese precedente (pp)	-	-3.50	-17.80	-14.00

4.4.3 Interpretazione complessiva e limiti dell’evidenza

I dati preliminari evidenziano una traiettoria coerente con le ipotesi teoriche del framework proposto. La crescita della copertura dell’intelligenza artificiale e i segnali di chiusura automatica per *similarity* configurano la prima evidenza empirica di un sistema che si comporta come previsto. Tuttavia, la finestra temporale è insufficiente per definire un comportamento continuo e validare le ipotesi elaborate. Queste considerazioni non indicano la validità delle evidenze raccolte, ma determinano la natura preliminare delle evidenze quantitative di una prima fase su un percorso destinato ad evolvere nei prossimi anni.

5. Conclusioni

In questa sezione verranno discussi i principali limiti dello studio condotto e alcuni spunti per eventuali sviluppi futuri, successivamente saranno presentate le conclusioni tratte dall'analisi svolta.

5.1 Limiti dello studio e sviluppi futuri

Lo studio condotto presenta tre limiti metodologici che è necessario esplicitare per una corretta interpretazione dei risultati.

Il principale limite di questo studio è dovuto alla scarsa disponibilità di dati pubblici a supporto dell'analisi competitiva. Nel Capitolo 3, è stata condotta una valutazione comparativa delle performance tecnologiche tra i paradigmi delle soluzioni frammentate e delle piattaforme multi-dominio con lo sviluppo della relativa traiettoria tecnologica. Questa analisi si è scontrata con due ostacoli strutturali: da un lato, la ridotta disponibilità di dati pubblici relativi alle performance direttamente riconducibili alle soluzioni, dovuta alla mancata divulgazione da parte dei vendor; dall'altro, la recente introduzione del paradigma delle piattaforme multi-dominio che non dispone di una base di dati sufficiente per condurre uno studio approfondito sulle dinamiche del settore e valutare l'emergere di un *dominant* design attraverso il modello di Abernathy-Utterback. I dati ricavati sono proxy estrapolate da report del settore che, data la natura metodologica, non permettono un'analisi completa per il confronto in quanto riflettono stime di analisti piuttosto che misurazioni dirette delle performance. Con la maturazione del mercato e la disponibilità crescente di dati longitudinali, una ricerca futura potrebbe contribuire a definire con precisione il grado di consolidamento competitivo del settore. Il secondo limite riguarda l'analisi empirica fondata su un singolo caso aziendale operante in un contesto specifico condotto nel Capitolo 4. I principi di replicabilità identificati hanno natura indicativa e richiedono contestualizzazione per essere applicati a condizioni differenti da quelle osservate. Un'estensione naturale del presente lavoro di tesi sarebbe uno studio comparativo su un campione eterogeneo di MSSP per contesto operante, con l'obiettivo di verificare la validità del framework delle leve strategiche identificate. Infine, la certificazione della strategia di implementazione dell'intelligenza artificiale richiede un arco temporale valutativo completo per stabilire gli effettivi benefici generati, la replicabilità e il ritorno dell'investimento previsto. La verifica complessiva del piano di implementazione proposto rimane aperta ad integrazioni delle evidenze preliminari presentate con dati operativi ed economici osservati nel lungo periodo.

5.2 Sintesi dei risultati

Il presente lavoro si è preposto di rispondere ad una domanda di ricerca di natura strategica di come un *Managed Security Service Provider* debba evolvere la propria architettura di servizi e il proprio modello operativo per costruire un posizionamento competitivo sostenibile in un mercato in rapida espansione e continuo cambiamento. Le analisi preliminari hanno permesso di comprendere come l'interesse nel settore della cybersecurity sia in continua crescita, sia nel contesto accademico che in quello industriale, e che le pressioni ed esigenze di mercato enfatizzano questa traiettoria. L'analisi dell'evoluzione strutturale del settore ha mostrato come la cybersecurity sia in una fase di transizione di paradigma che ridisegna i confini di competizione tra gli attori nel mercato. I limiti strutturali delle soluzioni frammentate come l'eterogeneità delle tecnologie, complessità di gestione e il lato economico-organizzativo, hanno portato all'emergere del paradigma delle piattaforme multi-dominio che superano queste criticità tramite funzionalità abilitate dall'integrazione dell'intelligenza artificiale. Tuttavia, queste piattaforme non sono in grado di sostituire il valore che un MSSP genera attraverso la gestione continuativa del servizio: la governance della postura di sicurezza del cliente, la personalizzazione contestuale dei processi di rilevamento e risposta e il supporto all'adeguamento normativo. In questo perimetro, un fornitore di servizi di sicurezza gestiti deve andare oltre al ruolo di *system integrator* e posizionarsi come partner strategico della gestione del rischio cyber, governando le implicazioni operative e organizzative per il cliente nel tempo. In particolare, il segmento mid-market presenta condizioni di domanda strutturalmente favorevoli a questo posizionamento, ma impone vincoli economici e organizzativi che rendono insostenibili i modelli operativi tradizionali basati sulla crescita lineare delle risorse umane. Per rispondere a questi vincoli, lo studio ha permesso di definire le leve strategiche che un MSSP deve attivare per evolvere il proprio modello operativo, tra cui la progressiva integrazione dell'intelligenza artificiale nei processi del *Security Operation Center* come condizione abilitante per la scalabilità e la sostenibilità del servizio nel contesto di crescita della domanda. Il caso Nais ha dimostrato come questa integrazione richieda un percorso evolutivo strutturato, dato dallo studio del contesto operativo e dalla definizione di un framework strategico di implementazione dell'automazione progressivo e graduale. Il vantaggio competitivo sostenibile di un MSSP si fonda sulla capacità di combinare orchestrazione tecnologica, automazione intelligente, servizi complementari a supporto del ciclo del rischio cyber e relazioni di ecosistema strutturate. Questi elementi combinati permettono di costruire una posizione competitiva solida, dove il valore percepito dal cliente risiede nella coerenza e unione di queste dinamiche. Infatti, queste dimensioni si rafforzano reciprocamente: servizi complementari e partnership ampliano la base clienti e permettono di distribuire i costi fissi dell'infrastruttura tecnologica, mentre la scalabilità operativa abilitata dall'intelligenza artificiale sostiene la crescita senza erodere il margine. In sintesi, la sostenibilità competitiva di un MSSP nell'era dell'intelligenza artificiale richiede una riconfigurazione integrata del modello di servizio dove tecnologia, AI, organizzazione e relazioni di ecosistema non sono variabili indipendenti, ma componenti di un sistema da ottimizzare insieme.

Appendice

Tabella 1.A: Principali CNAPP Vendor & Solution (Gartner, 2024)

Vendor	Solution
Aqua Security	Aqua CNAPP
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale CNAPP
Datadog	Datadog CNAPP
Data Theorem	Cloud Secure
Fortinet (Lacework)	Lacework FortiCNAPP
Google Cloud*	Security Command Center
IBM	IBM Security and Compliance Center
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca CNAPP Platform
Palo Alto Networks	Prisma Cloud
Qualys	Qualys TotalCloud
Rapid7	InsightCloudSec
SentinelOne	Singularity Cloud Security
Sophos	Sophos Cloud Native Security
Sysdig	Sysdig Secure
Tenable	Tenable Cloud Security
Trend Micro	Trend Vision One Cloud Security
Uptycs	Uptycs CNAPP
Upwind	Upwind CNAPP
Wiz*	Wiz CNAPP

Bibliografia

- Banca d'Italia. (2024). Framework segnaletico di vigilanza degli incidenti operativi o di sicurezza: Analisi orizzontale 2024. <https://www.bancaditalia.it/compiti/vigilanza/analisi-sistema/approfondimenti-banche-int/Framework-segnaletico-di-Vigilanza-degli-incidenti-operativi-o-di-sicurezza-Analisi-orizzontale-2024.pdf>
- Cisco. (2025) *Cisco cybersecurity readiness index* 2025. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index.pdf
- Commissione Europea. (2022). *Direttiva NIS2*. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- Deloitte. (2024). The Global Future of Cyber Survey, 4th Edition: The promise of cyber. <https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/deloitte-global-future-of-cyber-survey-4th-edition-the-promise-of-cyber.pdf>
- Denning, D. E. (1987). *An intrusion detection model*. *IEEE Transactions on Software Engineering*, 13(2), 222–232. <https://www.cs.colostate.edu/~cs656/reading/ieee-se-13-2.pdf>
- Diffie, W., & Hellman, M. E. (1976). *New directions in cryptography*. *IEEE Transactions on Information Theory*, 22(6), 644–654. <https://doi.org/10.1109/TIT.1976.1055638>
- EIOPA. (2022). *Digital Operational Resilience Act (DORA)*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- Elsevier. (2026). Scopus database. Retrieved from <https://www.scopus.com>
- ENISA. (2024a). *ENISA threat landscape: Finance sector*. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf
- ENISA. (2024b). *ENISA sectoral threat landscape: Public administration*. <https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Public%20Administration%20TL%202024.pdf>
- ENISA. (s.d.). *Cybersecurity market analysis framework*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Cybersecurity%20Market%20Analysis%20Framework%20%28ECSMAF%29_Updated.pdf
- ENISA. (s.d.). *Cybersecurity of critical sectors: Health*. <https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health>
- Enterprise Strategy Group. (2024, aprile). *Generative AI for cybersecurity: An optimistic but uncertain future*. <https://research.esg-global.com/reportaction/515201778/Marketing>
- European Banking Authority. (2020). *Guidelines on ICT and security risk management*. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf
- European Union Agency for Cybersecurity (ENISA). (2025, settembre 30). ENISA Threat Landscape 2025. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- Gartner. (2024, agosto). *Gartner forecasts global information security spending to grow 15% in 2025*. <https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025>

- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, 212–219.
<https://doi.org/10.1145/237814.237866>
- IBM Security. (2025a). *Cost of a Data Breach Report 2025*. https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf
- IBM Security. (2025b). *X-Force Threat Intelligence Index 2025*. <https://www.ibm.com/reports/threat-intelligence>
- IBM Institute for Business Value. (2024). *Capturing the cybersecurity dividend: How unified cybersecurity platforms add business value*. IBM. <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform>
- KPMG. (2025). *Cybersecurity considerations 2025: Government and public sector*. <https://kpmg.com/uk/en/insights/technology/cybersecurity-considerations-government-and-public-sector.html>
- Microsoft. (2024). *Microsoft Digital Defense Report 2024*. <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024>
- Microsoft. (2025a). *Microsoft Digital Defense Report 2025*. <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf>
- National Institute of Standards and Technology. (2023). *Migration to post-quantum cryptography* (NIST SP 1800-38B). <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>
- Patent Inspiration. (2026). *Patent analytics database*. Retrieved from <https://www.patentinspiration.com>
- PwC. (2025). *2026 Global Digital Trust Insights: New world, new rules — Cybersecurity in an era of uncertainty*. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html>
- Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, 27(3), 379–423. <https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>
- Shor, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring*. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*, 124–134.
<https://doi.org/10.1109/SFCS.1994.365700>
- U.S. International Trade Administration. (s.d.). *Italy cybersecurity*. <https://www.trade.gov/country-commercial-guides/italy-cybersecurity>
- Verizon. (2025a). *Data Breach Investigations Report 2025 — Finance snapshot*. <https://www.verizon.com/business/resources/infographics/2025-dbir-finance-snapshot.pdf>
- Verizon. (2025b). *Data Breach Investigations Report 2025 — Manufacturing snapshot*. <https://www.verizon.com/business/resources/infographics/2025-dbir-manufacturing-snapshot.pdf>
- Williamson, O. E. (1985). *The economic institutions of capitalism: Firms, markets, relational contracting*. Free Press.

Sitografia

- Agenzia per la Cybersicurezza Nazionale. (2025). *Cybersicurezza: obiettivi PNRR centrati*. <https://www.acn.gov.it/portale/w/cybersicurezza-obiettivi-pnrr-centrati.-italia-promossa-dall-europa>
- Apple. (2022, maggio). *Apple, Google, and Microsoft commit to expanded support for FIDO standard*. <https://www.apple.com/newsroom/2022/05/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard/>
- Calcalist Tech. (2025). *Cyber unicorn Pentera raises \$60M at over \$1B valuation as ARR approaches \$100M*. <https://www.calcalistech.com/ctechnews/article/ryvxvby21x>
- Chiariglione, L. (s.d.). *Biography*. <https://leonardo.chiariglione.org/communications/biography/>
- Cisco. (2015, August 27). *Cisco completes acquisition of OpenDNS*. Cisco Newsroom. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2015/m08/cisco-completes-acquisition-of-opendns.html>
- Cisco. (2018, October 1). *Cisco completes acquisition of Duo Security*. Cisco Newsroom. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2018/m10/cisco-announces-placeholder.html>
- Cisco. (2022). *Cisco unveils innovations driving new Security Cloud strategy*. <https://investor.cisco.com/news/news-details/2022/Cisco-Unveils-Innovations-Driving-New-Security-Cloud-Strategy/default.aspx>
- Cisco. (2024a). *Cisco completes acquisition of Splunk*. <https://investor.cisco.com/news/news-details/2024/Cisco-Completes-Acquisition-of-Splunk/default.aspx>
- Cisco. (2024b). *Cisco is delivering on platform strategy with rapid innovation across Cisco Security Cloud*. <https://investor.cisco.com/news/news-details/2024/Cisco-is-Delivering-on-Platform-Strategy-with-Rapid-Innovation-Across-Cisco-Security-Cloud/default.aspx>
- Cisco. (2025). *Annual report 2025*. https://www.cisco.com/c/dam/en_us/about/annual-report/2025-cisco-full-annual-report.pdf
- Cisco. (2025, gennaio). *Cisco unveils AI Defense*. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m01/cisco-unveils-ai-defense-to-secure-the-ai-transformation-of-enterprises.html>
- Cloudflare. (2024). *The state of the post-quantum Internet*. <https://blog.cloudflare.com/pq-2024/>
- CrowdStrike. (2025). *CrowdStrike agrees to acquire Onum*. <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-agrees-acquire-onum-supercharge-falcon-next-gen-siem>
- CrowdStrike. (2025). *CrowdStrike to acquire Pangea*. <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-acquire-pangea-secure-every-layer-enterprise-ai>
- CrowdStrike. (2025). *Fourth quarter and fiscal year 2025 financial results*. <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2025>
- CrowdStrike. (s.d.). *The CrowdStrike platform*. <https://www.crowdstrike.com/en-us/platform/>

Crunchbase. (2025). CyLock – Crunchbase company profile & funding. Crunchbase. Recuperato il 15 dicembre 2025, da <https://www.crunchbase.com/organization/cylock>

CyberSecurityUP. (s.d.). *Google Chrome adotta ML-KEM: pronto per la sfida dei computer quantistici*. <https://www.cybersecurityup.it/component/content/article/2-news-cyber-security/869-google-chrome-adotta-ml-kem-pronto-per-la-sfida-dei-computer-quantistici>

Cybersecurity360. (s.d.). *Cyber crisi nel settore manifatturiero in Italia*. <https://www.cybersecurity360.it/news/cyber-crisi-manifatturiero-italiano/>

Cybersecurity360. (s.d.). *Endpoint Protection Platform*. <https://www.cybersecurity360.it/soluzioni-aziendali/software-endpoint-security/>

CyLock. (2025, settembre). *CyLock tra le TOP 5 startup di cybersecurity agli Italian Security Awards 2025*. <https://www.cylock.tech/2025/09/11/cylock-tra-le-top-5-startup-di-sybersecurity-agli-italian-security-awards-2025/>

DataManager. (2025). *In Italia il 90% delle organizzazioni industriali sono state vittime di cyber attacchi nell'ultimo anno*. <https://www.datamanager.it/2025/07/in-italia-il-90-delle-organizzazioni-industriali-sono-state-vittime-di-cyber-attacchi-nellultimo-anno/>

Defense Advanced Research Projects Agency. (s.d.). *About DARPA*. <https://www.darpa.mil/about>

Fortinet. (2024). *Fortinet acquires Next DLP*. <https://www.fortinet.com/it/corporate/about-us/newsroom/press-releases/2024/fortinet-strengthens-top-tier-unified-sase-solution-with-acquisition-of-next-dlp>

Fortinet. (2025). *Fiscal year 2025 results* [SEC filing]. <https://www.sec.gov/Archives/edgar/data/1262039/000126203925000039/ftnt-20250930.htm>

Fortinet. (2025a). *Fortinet acquires Perception Point*. <https://www.fortinet.com/it/blog/business-and-technology/fortinet-acquires-perception-point>

Fortinet. (2025b). *Fortinet expands FortiAI*. <https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-expands-fortiai-across-its-security-fabric-platform>

Fortinet. (s.d.). *About us*. <https://www.fortinet.com/corporate/about-us/about-us>

Fortinet. (s.d.). *Che cos'è XDR?* <https://www.fortinet.com/it/resources/cyberglossary/what-is-XDR>

Fortinet. (s.d.). *La lunga partnership NATO rafforza le nostre difese cibernetiche collettive*. <https://www.fortinet.com/blog>

Fortinet. (s.d.). *What is network security?* <https://www.fortinet.com/resources/cyberglossary/what-is-network-security>

Gartner. (2025). *Market guide for endpoint protection platforms*. <https://www.gartner.com/reviews/market/endpoint-protection-platforms>

Gartner. (2025a). *Market guide* [reprints]. <https://www.gartner.com/doc/reprints?id=1-2LLXZ344&ct=250805&st=sb>

Gartner. (2025). *Magic Quadrant for Hybrid Mesh Firewall*.

Gartner. (2025). *Magic Quadrant for Single-Vendor SASE*.

Gartner. (2025). *Magic Quadrant for EPP*.

Gartner. (2025). *Magic Quadrant for Email Security*.

Gartner. (2025). *Magic Quadrant for AM*.

Governo Italiano. (s.d.). *Piano Nazionale di Ripresa e Resilienza: Misure cloud*. <https://cloud.italia.it/strategia-cloud-pa/le-misure-del-piano-nazionale-di-ripresa-e-resilienza>

IBM. (s.d.). *Che cos'è il rilevamento e risposta degli endpoint (EDR)?* <https://www.ibm.com/it-it/think/topics/edr>

IBM. (s.d.). *Che cos'è il red teaming?* <https://www.ibm.com/it-it/think/topics/red-teaming>

IBM. (s.d.). *Che cos'è il SOAR?* <https://www.ibm.com/it-it/think/topics/security-orchestration-automation-response>

IBM. (s.d.). *Che cos'è l'identity and access management?* <https://www.ibm.com/it-it/think/topics/identity-access-management>

IBM. (s.d.). *Cloud security*. <https://www.ibm.com/it-it/think/topics/cloud-security>

IBM. (s.d.). *Threat intelligence*. <https://www.ibm.com/it-it/think/topics/threat-intelligence>

InfoSecurity Europe. (s.d.). *Why platformization is reshaping cybersecurity*. <https://www.infosecurityeurope.com/en-gb/blog/future-thinking/why-platformization-reshaping-cybersecurity.html>

Innovation Post. (s.d.). *Gestire la cyber security degli asset industriali nell'era delle fabbriche intelligenti*. <https://www.innovationpost.it/tecnologie/industrial-security/gestire-la-cyber-security-degli-asset-industriali-nellera-delle-fabbriche-intelligenti/>

Investing.com. (2025, August 25). *Microsoft: Why its security business rivals CrowdStrike and Palo Alto*. <https://www.investing.com/analysis/microsoft-why-its-security-business-rivals-crowdstrike-and-palo-alto-200665840>

Jarvis, A. (2024). *PQShield pitch deck to raise \$7M seed round*. Alexander Jarvis. <https://www.alexanderjarvis.com/pqshield-pitch-deck-to-raise-7m-seed-round/>

Keepit. (2023). *Tool sprawl in cybersecurity*. <https://www.keepit.com/blog/tool-sprawl/>

Kurtz, G. (2025, August 26). *CrowdStrike CEO on \$290 million Onum acquisition*. Fortune. <https://fortune.com/2025/08/27/crowdstrike-ceo-george-kurtz-interview-290m-onum-acquisition-ai-security/>

MarketsandMarkets. (2025a). *Cloud security market*. <https://www.marketsandmarkets.com/Market-Reports/cloud-security-market-100018098.html>

MarketsandMarkets. (2025b). *Identity and access management market*. <https://www.marketsandmarkets.com/Market-Reports/identity-access-management-iam-market-1168.html>

MarketsandMarkets. (2025c). *Managed security services market*. <https://www.marketsandmarkets.com/Market-Reports/managed-security-services-market-5918403.html>

Microsoft. (2023, gennaio). *Microsoft security reaches another milestone*. <https://www.microsoft.com/en-us/security/blog/2023/01/25/microsoft-security-reaches-another-milestone-comprehensive-customer-centric-solutions-drive-results/>

Microsoft. (2025b). *Annual report 2025*. <https://www.microsoft.com/investor/reports/ar25/index.html>

Microsoft. (2025c). *Microsoft named a leader in the 2025 Gartner Magic Quadrant for email security*. <https://www.microsoft.com/en-us/security/blog/2025/12/05/microsoft-named-a-leader-in-the-2025-gartner-magic-quadrant-for-email-security/>

Microsoft. (2025d, novembre). *Security Copilot with Microsoft 365 E5*. <https://www.microsoft.com/en-us/security/blog/2025/11/18/agents-built-into-your-workflow-get-security-copilot-with-microsoft-365-e5/>

Microsoft. (s.d.). *Che cos'è EDR?* <https://www.microsoft.com/it-it/security/business/security-101/what-is-edr-endpoint-detection-response>

Microsoft. (s.d.). *Microsoft Entra ID*. <https://www.microsoft.com/it-it/security/business/identity-access/microsoft-entra-id>

Microsoft. (s.d.). *Microsoft security suites pricing*. <https://www.microsoft.com/en-us/security/pricing/enterprise/security-suites>

Microsoft. (s.d.). *Windows Resiliency Initiative*. <https://www.microsoft.com/en-us/windows/business/windows-resiliency-initiative>

Mordor Intelligence. (2025). *Cloud security software market*. <https://www.mordorintelligence.com/industry-reports/global-cloud-security-software-market-industry>

Mordor Intelligence. (2025). *Data security market size*. <https://www.mordorintelligence.com/industry-reports/data-security-market>

MSSP Alert. (2024). *Platform trend drives MSSP/MSP market growth*. <https://www.msspalert.com/news/platform-trend-drives-mssp-msp-market-growth>

NATO NCIA. (s.d.). *NATO Industry Cyber Partnership*. <https://www.ncia.nato.int>

Palo Alto Networks. (2025a). *Fiscal fourth quarter and fiscal year 2025 financial results*. <https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-reports-fiscal-fourth-quarter-and-fiscal-year-2025-financial-results>

Palo Alto Networks. (2025b). *Palo Alto Networks announces agreement to acquire CyberArk*. <https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-announces-agreement-to-acquire-cyberark--the-identity-security-leader>

Palo Alto Networks. (2025c). *Palo Alto Networks completes acquisition of Protect AI*. <https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-completes-acquisition-of-protect-ai>

Palo Alto Networks. (2025d). *Prisma AIRS 2.0*. <https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-secures-the-ai-agent-revolution-with-the-launch-of-prisma-airs-2-0>

Palo Alto Networks. (s.d.-a). *About us*. <https://www.paloaltonetworks.it/about-us>

Palo Alto Networks. (s.d.-b). *AI risks and benefits in cybersecurity*. <https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity>

Palo Alto Networks. (2025e). *Understanding and leveraging the role of platformization in AI-first cybersecurity*. <https://www.paloaltonetworks.com/perspectives/understanding-and-leveraging-the-role-of-platformization-in-ai-first-cybersecurity/>

Pentera. (s.d.). *About us*. <https://pentera.io/it/about-us/>

Pentera. (2022, January 11). Pentera announces \$150M Series C at \$1 billion valuation. Business Wire. <https://www.businesswire.com/news/home/20220111006106/en/>

Pentera. (2025, March 12). Pentera secures \$60M to lead security validation market consolidation and drive next phase of growth. PR Newswire. <https://www.prnewswire.com/news-releases/pentera-secures-60m-to-lead-security-validation-market-consolidation>

PQShield. (2022). *PQShield raises \$20 million Series A to fuel global growth*. <https://pqshield.com/pqshield-raises-20-million-series-a-to-fuel-global-growth/>

PQShield. (2024a). *PQShield: At the heart of the PQC conversation*. <https://pqshield.com/pqshield-at-the-heart-of-the-pqc-conversation/>

PQShield. (2024b). *PQShield launches first post-quantum cryptography silicon test chip for NIST compliance*. The Quantum Insider. <https://thequantuminsider.com/2024/09/04/pqshield-launches-first-post-quantum-cryptography-silicon-test-chip-for-nist-compliance/>

PQShield. (2024c). *PQShield raises \$37M in Series B funding*. <https://pqshield.com/pqshield-raises-37m-in-series-b-funding/>

Prompt Security. (2024). *Prompt Security emerges from stealth with \$5M seed to be enterprises' one-stop for generative AI security*. <https://www.prompt.security/press/prompt-security-emerges-from-stealth-with-5m-seed-to-be-enterprises-one-stop-for-generative-ai-security>

Prompt Security. (s.d.). *About us*. <https://www.prompt.security/about-us>

Reuters. (2025, novembre). *Amazon, Google named by EU among 'critical' tech providers for finance industry*. <https://www.reuters.com/sustainability/boards-policy-regulation/amazon-google-named-by-eu-among-critical-tech-providers-finance-industry-2025-11-18/>

SGS. (2024, maggio). *ISO/IEC 27001 transition: What you should know*. <https://www.sgs.com/en-it/news/2024/05/iso-iec-27001-transition-what-you-should-know>

Sophos. (s.d.). *Security Operations Center (SOC)*. <https://www.sophos.com/it-it/cybersecurity-explained/about-soc-security-operations-center>

SRG Research. (2025). *Cloud market share trends: Big three together hold 63%*. <https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher>

Statista Market Insights. (2025a). *Cybersecurity market size worldwide*. <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

Statista Market Insights. (2025b). *Network security market size worldwide*. <https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/network-security/worldwide?currency=USD>

Statista Market Insights. (2025c). *Data security market size worldwide*. <https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/data-security/worldwide>

Statista Market Insights. (2025d). *Endpoint security market size worldwide*. <https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/endpoint-security/worldwide>

Stubbs, M. (2024, 30 agosto). *PQShield builds NIST-ready PQC in silicon*. PQShield. <https://pqshield.com/pqshield-builds-nist-ready-pqc-in-silicon/>

The Wall Street Journal. (2025, September 16). CrowdStrike to buy AI security company Pangea. <https://www.wsj.com/articles/crowdstrike-to-buy-ai-security-company-pangea-a82946e9>

Tines. (2023). *Voice of the SOC 2023*. <https://www.tines.com/reports/voice-of-the-soc-2023/>

Treccani. (s.d.). *Shannon*. Enciclopedia della Matematica. [https://www.treccani.it/enciclopedia/shannon_\(Enciclopedia-della-Matematica\)/](https://www.treccani.it/enciclopedia/shannon_(Enciclopedia-della-Matematica)/)

Watson, R. (2023). *Simplify to survive: How organizations can navigate cyber risk*. Dark Reading. <https://www.darkreading.com/cyber-risk/simplify-to-survive-how-organizations-can-navigate-cyber-risk>

Wikipedia. (2024). *2024 CrowdStrike-related IT outages*. https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages

Wikipedia. (s.d.). *Leonardo Chiariglione*. https://it.wikipedia.org/wiki/Leonardo_Chiariglione

Wikipedia. (s.d.). *Peter Shor*. https://it.wikipedia.org/wiki/Peter_Shor

Wikipedia. (s.d.). *Pentera (azienda)*. [https://it.wikipedia.org/wiki/Pentera_\(azienda\)](https://it.wikipedia.org/wiki/Pentera_(azienda))

Wikipedia. (s.d.). *Teoria dell'informazione — Modello di Shannon-Weaver*. https://it.wikipedia.org/wiki/Teoria_dell%27informazione#Modello_di_Shannon-Weaver

Wiz. (2022). *\$100M ARR in 18 months: Wiz becomes the fastest-growing software company ever*. <https://www.wiz.io/blog/100m-arr-in-18-months-wiz-becomes-the-fastest-growing-software-company-ever>

Zscaler. (2025a). *Fourth quarter and fiscal year 2025 financial results*. <https://ir.zscaler.com/news-releases/news-release-details/zscaler-reports-fourth-quarter-and-fiscal-2025-financial-results>

Zscaler. (2025b). *Zscaler acquires SPLX*. <https://www.zscaler.com/it/press/zscaler-secures-enterprise-ai-lifecycle-acquisition-innovative-ai-security-pioneer-splx>

Zscaler. (2025c). *Zscaler completes acquisition of Red Canary*. <https://www.zscaler.com/press/zscaler-completes-acquisition-red-canary-accelerate-innovations-agentic-ai-driven-security>

Zscaler. (s.d.). *AI solutions*. <https://www.zscaler.com/it/products-and-solutions/zscaler-ai>

Zscaler. (s.d.). *Zero Trust Exchange*. <https://www.zscaler.com/it/products-and-solutions/secure-your-users>