I cinque livelli della sicurezza informatica

A cura di Allianz Global Investors

I crimini informatici sono sempre più numerosi e complessi. Aziende e persone devono esserne consapevoli e intervenire in misura crescente per farvi fronte. Allo stesso tempo, anche gli investimenti nel settore offrono opportunità di grande interesse.

L'approccio a più livelli si è rivelato il più efficace, dato che ai criminali informatici può bastare avere successo una volta sola, ma ai professionisti della sicurezza – e alle organizzazioni che proteggono – occorre creare condizioni di sicurezza in ogni occasione.

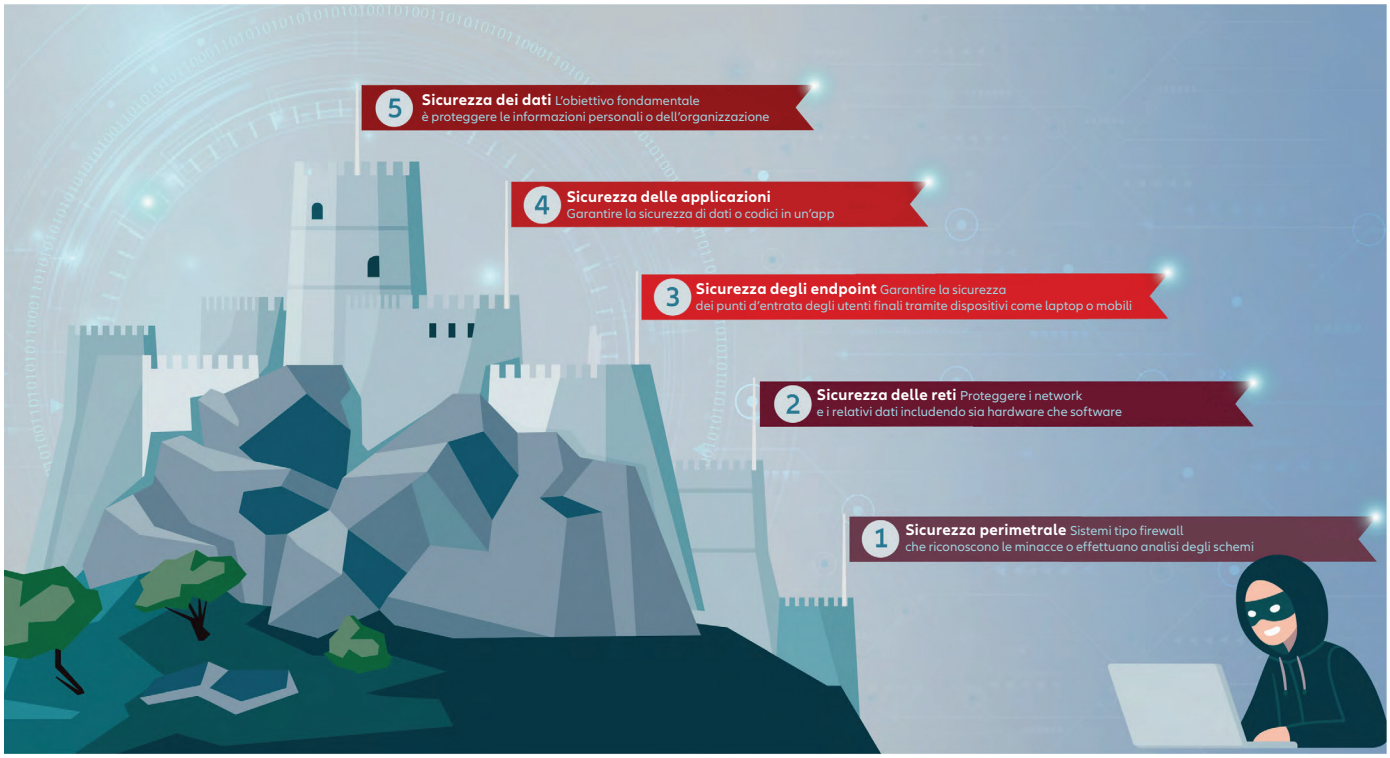
Dato il numero sempre maggiore di dispositivi, automobili, case e, non da ultimo, di processi produttivi e manifatturieri connessi a Internet, le aziende e le persone sono sempre più esposte al rischio di attacchi informatici. Da qui una crescente esigenza di protezione, che richiede approcci sempre più sofisticati alla sicurezza informatica. Una situazione che, peraltro, offre agli investitori interessanti opportunità di partecipare alle prospettive di crescita delle società più all'avanguardia in questi sviluppi. L'approccio a più livelli, di cui si parla in questo articolo (vedi figura 1), si è rivelato il più efficace, dato che ai criminali informatici può bastare avere successo una volta sola, ma ai professionisti della sicurezza – e alle organizzazioni che proteggono – occorre creare condizioni di sicurezza in ogni occasione.

Finora, la prima linea di difesa era rappresentata da una sicurezza perimetrale, tradizionalmente sinonimo di firewall, che puntava ad assicurare la protezione di dati e sistemi filtrando il traffico potenzialmente pericoloso o sconosciuto. Con la crescente ubiquità del cloud e dell'accesso remoto, tali soluzioni, un tempo progettate per gestire e proteggere le reti locali, devono ora adattarsi a questo nuovo e più complesso panorama.

La trasformazione della difesa della sicurezza di rete

La sicurezza di rete comprende sia le tecnologie hardware e software, sia i processi e i dispositivi che proteggono una rete e i suoi dati. Anche in questo caso, l'espansione del cloud e del lavoro da casa (o da ovunque) stanno cambiando radicalmente il contesto; le reti ora includono anche le connessioni al cloud e le infrastrutture ibride che possono essere costituite da data

Figura 1 - **I cinque livelli della sicurezza informatica**



Fonte: Allianz Global Investors

Una violazione della cyber security può rappresentare un grave problema per i privati e addirittura mettere a rischio l'esistenza di un'azienda.

center proprietari, cloud pubblico-privati e applicazioni di software-as-a-service (SaaS).
Con l'aumento dell'uso e l'integrazione delle tecnologie cloud nei processi aziendali e con la creazione di modelli di lavoro flessibili (on-site, remoti e ibridi), molte organizzazioni si trovano, dunque, ad affrontare problemi di vulnerabilità della rete e dei dati. Gli innovatori di questo settore stanno quindi ripensando i concetti di sicurezza consolidati e ideando nuovi modelli. Per esempio, Zscaler e CrowdStrike hanno sviluppato una soluzione basata sull'idea di "zero trust", in cui l'identità dell'utente, le credenziali di sicurezza del dispositivo e i criteri di accesso sono utilizzati per concedere o negare i diritti di accesso. Queste soluzioni di accessibilità condizionata basate sul rischio aiutano a gestire una moltitudine di requisiti di ingresso individuali da parte degli utenti, rilevando in tempo reale le possibili minacce che possono sorgere quando le identità non corrispondono ai relativi diritti di accesso. Questo, a sua volta, protegge da violazioni gli ambienti IT complessi e quindi più vulnerabili alle violazioni.

Sicurezza degli endpoint: dove inizia la sicurezza di una rete

Il crescente utilizzo del cloud sta portando anche a profondi cambiamenti nel modo in cui gli endpoint – ovvero tutti i dispositivi che sono connessi alla rete e in grado di comunicare in entrambe le direzioni – debbano essere

protetti dagli attacchi informatici. Infatti, i malintenzionati ora puntano spesso alla vulnerabilità dei dispositivi endpoint per accedere a una rete, mentre fino a poco tempo fa miravano a violare la sicurezza perimetrale. Data la crescente proliferazione di dispositivi connessi alle reti delle organizzazioni, la crescita dell'"Internet delle cose" (IoT) e i rischi associati al "bring your own device", ossia all'autorizzazione aziendale all'utilizzo di dispositivi personali, la sicurezza degli endpoint è destinata a rappresentare un'area di crescita particolarmente forte nel prossimo futuro. Secondo alcune stime, infatti, il mercato della sicurezza degli endpoint crescerà a un tasso annuo di crescita composto (CAGR) dell'8,3% entro il 2028, raggiungendo un valore di 24,58 miliardi di dollari[1].

Sicurezza delle applicazioni: difendere app e utenti

La sicurezza delle applicazioni è multiforme come le applicazioni stesse. Non comprende solo le procedure utilizzate per siti web e le applicazioni durante l'utilizzo, ma anche quelle utilizzate durante lo sviluppo e la progettazione. Anche in questo caso, l'ascesa del cloud sta cambiando le carte in tavola. Con un numero sempre maggiore di organizzazioni che ospitano risorse in questo modo, la sicurezza delle applicazioni sta diventando sempre più complessa. Una recente ricerca suggerisce che il mercato globale della sicurezza delle applicazioni registrerà un CAGR del 18,3% entro il 2028, raggiungendo un valore di 22,54 miliardi di dollari, rispetto a 6,95 miliardi di dollari nel 2021[2].

1 https://www.globenewswire.com/news-release/2023/01/20/2592453/0/en/endpoint-security-market-size-worth-usd-24-58-billion-by-2028-report-by-fortune-business-insights.html.

2 https://www.vantagemarketresearch.com/industry-report/application-security-market-1406.

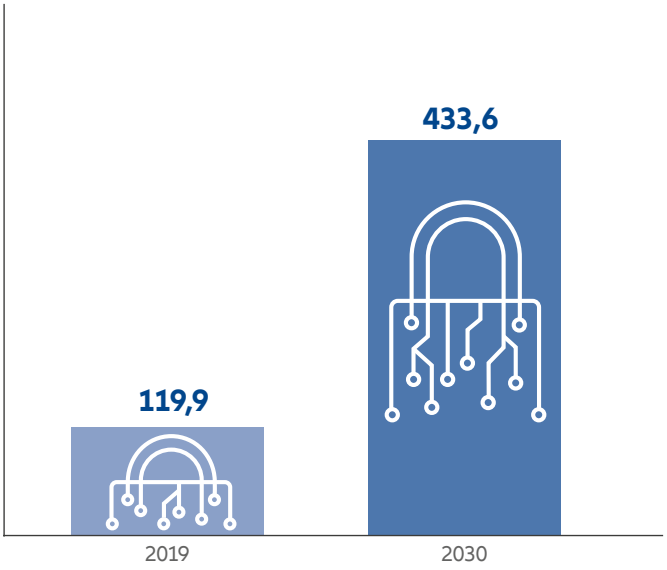
Sicurezza degli endpoint e delle applicazioni

Fondata nel 2011, CrowdStrike ha sviluppato un'offerta per la sicurezza degli endpoint che comprende una serie di moduli unificati per prevenire le violazioni. La sua piattaforma Falcon raccoglie dati sulla sicurezza informatica – elaborando oltre 6 trilioni di eventi alla settimana – e sfrutta l'intelligenza artificiale per migliorare costantemente le sue prestazioni e fornire uno dei più alti tassi di rilevamento ed efficacia del settore. Il fatturato ricorrente annuale dell'azienda è cresciuto del 48% rispetto all'anno precedente, superando i 2,5 miliardi al 31 gennaio 2023[3].
Uno dei leader in una serie di aree e discipline della cyber security è Zscaler, la cui soluzione "Private Access" (ZPA) applica i principi della "fiducia zero" e della segmentazione per offrire agli utenti una connettività diretta e sicura alle applicazioni, eliminando al contempo gli accessi non autorizzati attraverso lo "zero trust network access" (ZTNA). ZPA è attualmente la piattaforma ZTNA più diffusa al mondo e si prevede che questo modello diventerà dominante nei prossimi anni. Gartner prevede che, entro il 2025, oltre il 70% delle implementazioni di accesso remoto utilizzerà ZTNA[4].

3 https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2023/.

4 https://www.datacenterknowledge.com/security/gartner-zero-trust-will-replace-your-vpn-2025 , as of October 2022

Figura 2 - **Un'opportunità di investimento importante**
Il mercato della cyber security è previsto crescere a un tasso annuo del 12,6% da qui al 2030 (dati in miliardi di dollari)[6]



Il mercato della sicurezza degli endpoint è previsto crescere con un tasso (CAGR) del 9,4% entro il 2026, raggiungendo un valore di 22 miliardi di dollari[5].

Sicurezza dei dati: il cuore della protezione

La protezione dei dati attraverso le piattaforme e le applicazioni collegate alla rete di un'organizzazione è spesso considerata la disciplina più importante della sicurezza informatica. La salvaguardia dei dati è di vitale importanza per ogni azienda, dato che molte di loro basano i loro processi e modelli di business sull'archiviazione, la trasmissione e, non da ultimo, sulla monetizzazione dei dati raccolti all'interno e all'esterno. In effetti, le conseguenze delle violazioni a questo riguardo rappresentano uno dei maggiori rischi per le società e le altre organizzazioni in termini di potenziale responsabilità e danni alla reputazione.
Secondo Cowen Research e Boston Consulting Group, "l'elemento umano" è responsabile di almeno tre quarti delle violazioni informatiche. I problemi sono, ad esempio, il mancato rispetto dei protocolli di sicurezza da parte degli utenti o l'eventualità di restare vittime di comunicazioni ingannevoli o di altre forme di social engineering. Per questo motivo, la formazione sulla sicurezza e le tecnologie che identificano e rilevano le minacce in modo più efficace, restano fondamentali per limitare tali violazioni.
Microsoft, per esempio, offre una serie di soluzioni di sicurezza che aiutano i clienti a mantenere i dati al sicuro. Una delle nuove soluzioni dell'azienda è Copilot, che consente ai team di sicurezza di rilevare schemi nascosti e di rispondere più rapidamente agli

5 https://www.prnewswire.com/news-releases/endpoint-security-global-market-report-2022-sector-to-reach-22-billion-by-2026-at-a-cagrof-9-4-301712341.html, as of March 2023

6 https://www.businesswire.com/news/home/20201119005835/en/Global-Cyber-Security-Market-2020-to-2030---by-Component-Security-Type-Deployment-Enterprise-Use-Case-and-Industry---ResearchAndMarkets.comases/endpoint-security-global-market-report-2022-sector-to-reach-22-billion-by-2026-at-a-cagrof-9-4-301712341.html, as of March 2023

Cyber Security: investire nella "protezione" della vita di tutti i giorni

Allianz Cyber Security investe sui mercati azionari globali con focus sia sulle società esposte al tema della cyber security sia su quelle in grado di trarne vantaggio in ottica futura. L'universo della cyber security è ampio e comprende molteplici ambiti, dalla sicurezza informatica al disaster recovery sino alla formazione degli utenti finali.

Le nostre vite sono sempre più digitalizzate. I computer sono già parte integrante della vita lavorativa e gli smartphone si sono trasformati in dispositivi essenziali nel quotidiano. Il prossimo passo sarà l'ascesa dell'Internet of Things (IoT), un ambito in cui rientrano, tra gli altri, auto a guida autonoma, servizi sanitari e assistenza digitali, e smart home. Tali innovazioni renderanno le nostre vite più facili, ma ci esporranno anche a maggiori rischi.

Una violazione della cyber security può rappresentare un grave problema per i privati e addirittura mettere a rischio l'esistenza di un'azienda. Ad esempio, nel 2022 il costo medio di un trasferimento non autorizzato di dati (*data leak*) è stato di 4,34 milioni di dollari e occorrono in media 212 giorni per rilevare un data leak.

Per un'azienda, le conseguenze possono essere molto gravi: un grave danno reputazionale; la possibile perdita di investitori; pesanti sanzioni per protezione inadeguata di dati personali in seguito all'introduzione negli ultimi anni di normative molto più stringenti. In definitiva, alle aziende rimane solo un'opzione: investire nella cyber security. A sua volta, questo crea opportunità interessanti per chi investe nel mercato azionario, per diversi importanti motivi:

Un trend in forte crescita. La cyber security ha numerosi driver di crescita di breve e lungo termine. Il megatrend della "digitalizzazione" accresce la nostra vulnerabilità e quindi la necessità di dotarci di sistemi di cyber security. Esigenza che è stata accentuata dalla pandemia di COVID-19, poiché l'importanza della digitalizzazione è aumentata a una velocità molto superiore rispetto a quanto originariamente previsto.

Un investimento in società fortemente impegnate nella cyber security. Il fondo ha l'obiettivo di individuare i vincitori in un'ottica di lungo periodo, vale a dire le società che beneficiano dei driver di crescita strutturale. Investe in circa 30-60 titoli, in prevalenza di aziende di media dimensione *pure play* (ossia, con almeno il 50% del fatturato derivante dal settore della cyber security), così da offrire un portafoglio "high conviction" molto concentrato.

Un track record tra i più lunghi nell'universo della cyber security. Il team di gestione di Allianz Global Investors vanta un'esperienza pari a 20 anni, con un track record tra i più lunghi nel settore della cyber security.

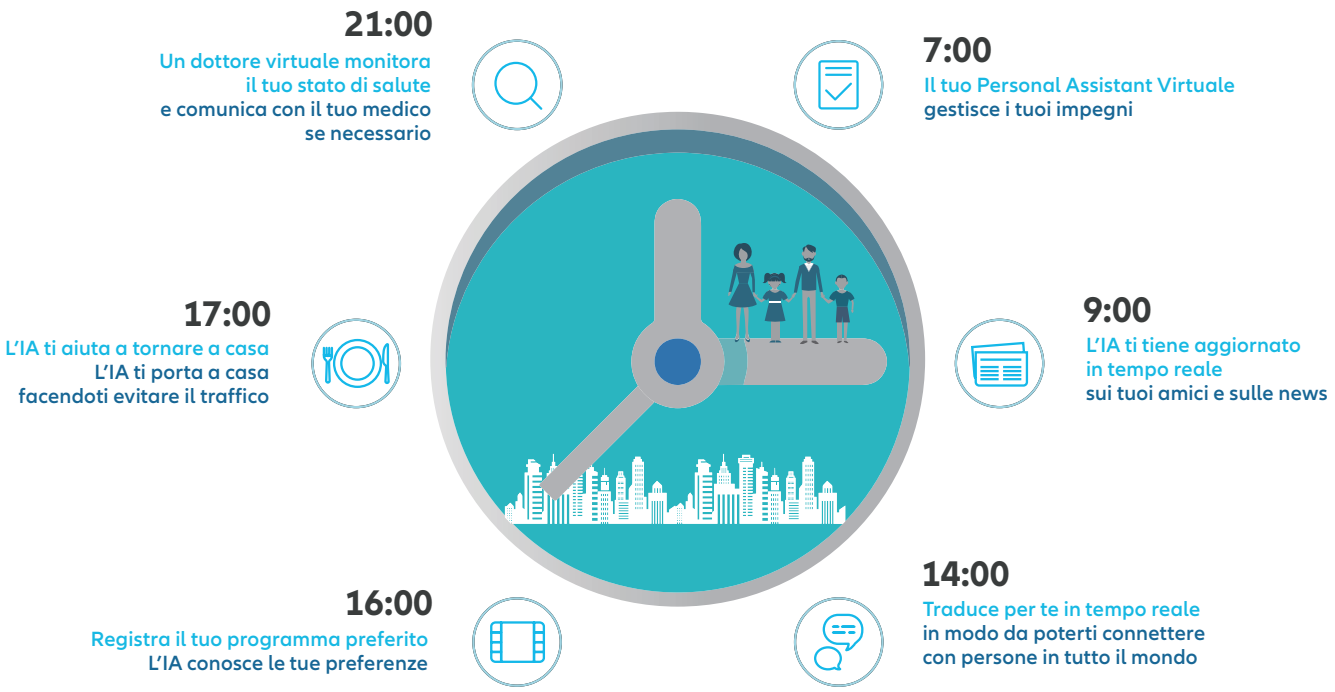
Sicurezza delle applicazioni: il CAGR del mercato è previsto pari a oltre il 18% da qui al 2028, raggiungendo un valore di 22,54 miliardi di dollari.

Allianz Global Artificial Intelligence: potenziale di disruption in ogni settore

L'intelligenza artificiale è destinata a guidare l'ondata di innovazione e automazione per i prossimi decenni e i potenziali benefici che ne derivano hanno convinto molti osservatori a equiparare il suo progresso a quello della prossima rivoluzione industriale, trasformazioni che impatteranno numerosi settori ed aree quali: trasporti, finanza, sanità, industria manifatturiera e altri ancora.
Il potere creativo della *disruption* ha il potenziale per cambiare il nostro modo di vivere e di lavorare (vedi figura 3). L'intelligenza artificiale non riguarda solo i robot: le tecnologie innovative stanno alimentando progressi come gli assistenti intelligenti, le auto a guida autonoma e la diagnostica medica, solo per citarne alcuni. Gran parte di ciò che l'intelligenza artificiale di oggi sta realizzando è, però, ancora nascosto: siamo solo all'inizio del viaggio.
Allianz Global Artificial Intelligence è una strategia di investimento azionaria focalizzata sulle tecnologie di intelligenza artificiale, che seleziona a livello globale le società che sviluppano la sua implementazione in tutte le sue possibili applicazioni: dai big data alle infrastrutture informatiche, dall'automazione sanitaria alle auto a guida autonoma, fino all'internet delle cose. L'obiettivo di Allianz Global Artificial Intelligence è quello di navigare tra i cambiamenti portati da questa tecnologia rivoluzionaria con la convinzione che le società che alimentano l'ecosistema dell'intelligenza artificiale o che sfruttano l'IA per innovare la propria attività saranno meglio posizionate per conquistare il mercato e offrire rendimenti interessanti agli investitori.

Perché investire:
Pioniere nel campo dell'intelligenza artificiale. Allianz Global Artificial Intelligence è stato uno dei primi fondi incentrati su questo megatrend, lanciato con l'obiettivo di individuare la moltitudine delle tecnologie e dei beneficiari dell'IA. L'Intelligenza Artificiale ha il potenziale per rivoluzionare e rinnovare tutti i settori industriali, non solo quelli tecnologici, nei prossimi decenni.
Gestione attiva e approccio disciplinato. Nel fondo si utilizzano l'analisi fondamentale e l'analisi dei trend tematici per identificare le società innovative che sviluppano o sfruttano la tecnologia
IA e che sono meglio posizionate per crescere. La gestione attiva, grazie ad un approccio disciplinato, è focalizzata sulle opportunità di investimento nell'Intelligenza Artificiale senza vincoli settoriali, geografici e di capitalizzazione.
Un team esperto e "sempre connesso". Il team di gestione può contare su decenni di esperienza nel settore e importanti relazioni nella Silicon Valley. Il team è sempre a stretto contatto con le aziende posizionate nei trend in crescita ed è supportato da analisti di ricerca.

Figura 3 - **L'Intelligenza Artificiale nella nostra vita quotidiana**



incidenti grazie all'intelligenza artificiale generativa. Microsoft è leader nella sicurezza informatica e continua a sviluppare soluzioni innovative per proteggere i dati critici. Riteniamo che questo segmento rappresenti un importante motore per la crescita a lungo termine dell'azienda.

Allianz Global Investors identifica i primi attori nella cyber-sicurezza

Quando si parla di sicurezza informatica, è fondamentale che le aziende siano sempre un passo avanti rispetto ai malintenzionati. Il crimine informatico è e continuerà a essere un rischio difficile da valutare. Le aziende leader che forniscono soluzioni in questo settore sono quindi in grado di trarre vantaggio dalla crescente necessità di approcci olistici alla sicurezza informatica, un'esigenza che diventerà sempre più pertinente e complessa da affrontare nei prossimi anni. Allianz Global Investors individua gli innovatori e i primi a muoversi nel campo della cybersicurezza, in particolare quelli che forniscono soluzioni innovative per proteggere applicazioni, organizzazioni e utenti in ambienti cloud complessi.