INTESA SANPAOLO
INNOVATION CENTER

REPORT SULLE TENDENZE DEL SETTORE

INDUSTRIAL & MECHANICS SECURITY OF THINGS

FROST & SULLIVAN

I dati e i commenti riportati nella presente pubblicazione sono stati elaborati e forniti in massima parte da Frost & Sullivan. L'elaborazione è basata su informazioni proprietarie e su una serie di fonti terze, incluse le aziende, le organizzazioni e le istituzioni accademiche citate nel testo.

INDICE

EXECUTIVE SUMMARY

Nel 2022, i dispositivi IoT connessi erano 35,37 miliardi a livello globale, e si stima che questo numero raggiungerà i 73,79 miliardi entro il 2027, con un tasso di crescita annuo composto del 17,3%. I dispositivi IoT sono in grado di misurare dati, assegnare identità, creare interconnessioni e generare informazioni e comprendono sia applicazioni *consumer* che *industrial*, con una forte espansione della comunicazione machine-to-machine in tutti i settori.

Se da un lato l'IoT industriale (IIoT) comporta molti vantaggi, la proliferazione di dispositivi connessi espone inevitabilmente gli asset delle aziende ad attacchi informatici malevoli.

Le organizzazioni devono affrontare un numero crescente di sfide e vulnerabilità in termini di sicurezza: basti pensare che i soli attacchi malware sono aumentati da 60 milioni a livello globale nel 2021 a 112 milioni nel 2022. Colonial Pipeline, Tesla e Abbot Healthcare sono alcune delle vittime delle recenti falle nella sicurezza IoT di alto profilo in tutti i settori. Questi e altri incidenti aumentano l'attenzione degli operatori del mercato e di terze parti sulla necessità di rafforzare la sicurezza informatica nel contesto dell'IoT industriale.

In tutti i **settori industriali**, la convergenza delle tecnologie informatiche e operative (IT/OT) ha creato una "superficie di attacco" più ampia, mettendo a rischio le aziende. Parallelamente, la necessità di rispettare le normative esistenti ed emergenti sta causando uno spostamento degli aspetti di sicurezza informatica dalla fabbrica alla sala riunioni, dopo che, in seguito alla pandemia e al suo impatto persistente, molti dipendenti hanno ottenuto e continuano a godere dell'accesso remoto a risorse OT critiche.

In Italia, da un'indagine di Frost & Sullivan del 2022 è emerso che negli ultimi due anni l'85% delle aziende industriali ha subito gli effetti negativi di un attacco informatico, e il 21% degli intervistati ha indicato le vulnerabilità dei sistemi come la loro principale preoccupazione.

Di conseguenza, gli operatori del mercato industriale di tutti i Paesi e le regioni stanno adottando strategie di sicurezza informatica per proteggere i dispositivi IoT dalle minacce. Nel concreto, gli operatori stanno spostando l'attenzione dalla protezione al rilevamento, attraverso l'implementazione di efficaci sistemi di gestione degli allarmi OT per ridurre il rischio di falsi positivi; tale misura, abbinata all'utilizzo di query attive per scoprire dispositivi IoT dormienti in tutti gli ambienti, svolge un ruolo fondamentale.

I primi ad adottare questi e altri approcci sono i settori delle infrastrutture critiche, mentre l'adozione nei processi generali e nella produzione discreta è a un livello molto meno avanzato.

In questo e in altri ambiti, gli operatori industriali collaborano con terze parti per offrire soluzioni completamente integrate che contribuiscano a ridurre il rischio, mentre i fornitori di sistemi di cybersecurity IT e OT, a loro volta, stanno cominciando ad accedere gli uni negli spazi degli altri per ampliare i portafogli e fornire offerte scalabili.

Tra le aziende da monitorare vi sono Claroty (Stati Uniti), che offre una soluzione completa per proteggere i dispositivi IoT nei siti industriali, Dragos (Stati Uniti), che punta sulla visibilità delle risorse, e Nozomi (Stati Uniti), che ha lanciato Vantage, la prima piattaforma Software as a Service per gestire le minacce OT/IT nella produzione. Altri importanti attori europei includono Applied Risk (Paesi Bassi), Darktrace (Regno Unito) e ICSEC (Polonia), cui si aggiunge Radiflow (Israele).

In futuro, i fornitori di soluzioni di cybersecurity guarderanno all'intelligenza artificiale per rilevare minacce avanzate o sconosciute, oltre che per distinguersi.

Nel settore **sanitario**, la minaccia di un attacco informatico è particolarmente elevata, in uno scenario in cui il 90% dei dati è gestito tramite dispositivi medici e l'Internet of Medical Things (IoMT).

Una maggiore connettività comporta un aumento della frequenza e della gravità delle minacce, mentre proliferano le truffe online, gli attacchi informatici e gli incidenti causati da insider negligenti. Allo stesso tempo, attualmente il tempo impiegato dagli operatori sanitari per individuare i rischi informaci è del 150% superiore a quello di altri settori, il che si traduce in costi sproporzionatamente più alti.

Gli operatori del mercato, pertanto, stanno aumentando gli investimenti per la modernizzazione delle infrastrutture e delle reti, la protezione delle piattaforme cloud-native, la protezione dei dispositivi medici e degli abilitatori IoMT e la salvaguardia delle applicazioni di terzi da comuni agenti di minaccia informatica come ransomware, phishing, raccolta delle credenziali e attacchi di social engineering.

La protezione delle interfacce di programmazione delle applicazioni da violazioni evitabili diventerà la prima linea dell'attività di cybersecurity nel medio e lungo termine, e nell'universo healthcare globale entreranno molti degli stessi fornitori che già occupano il più ampio settore industriale, oltre che operatori che pronti a contendersi un posto in un segmento appetibile.

Anche l'industria **automobilistica**, come il settore dell'assistenza sanitaria, è particolarmente vulnerabile: si stima che entro il 2026 il 95% delle autovetture utilizzerà la telematica integrata.

Individuare tutte le possibili vulnerabilità di un veicolo *connesso*, pertanto, sta diventando un prerequisito fondamentale per definire e gestire qualunque scenario, partendo dall'esempio di violazioni recenti come attacchi informatici a veicoli e server, oltre a fughe di dati.

In questo contesto, molti produttori automobilistici si sono accorti che costi elevati e competenze limitate possono compromettere la loro capacità di sviluppare efficaci piani d'azione per la sicurezza. Finora la maggior parte di loro ha risposto sviluppando le capacità interne e/o collaborando con fornitori di servizi IT esterni per ridurre il rischio informatico. Tuttavia, l'introduzione della normativa WP.29, che impone ai produttori di automobili l'onere di gestire le minacce lungo la filiera, cambia le regole del gioco.

Di conseguenza, le case automobilistiche di fascia alta sono alla ricerca di partner per servizi di consulenza, mentre i produttori del mercato di massa prediligono soluzioni di sicurezza end-to-end. Cybellum (Israele), ad esempio, offre una piattaforma di digital twin per la valutazione delle minacce, mentre Upstream (Stati Uniti) offre una soluzione cloud per rispondere a tutti i requisiti della normativa WP.29.

In futuro, il quadro della sicurezza informatica nel settore automotive diventerà ancora più complesso, considerando che presto i veicoli *a guida autonoma* rappresenteranno un'opportunità di mercato da oltre 100 miliardi di dollari. In questo contesto, lo scenario dei possibili attacchi è molto vario ed è ancora in fase di definizione. Considerato il numero di moduli di deep learning che saranno integrati nei veicoli *a guida autonoma*, sarà fondamentale gestire le minacce basate sull'intelligenza artificiale.

Questo report esamina il panorama in evoluzione delle minacce legate all'IIoT connesso e la risposta emergente per salvaguardare al meglio la *"security of things"* nei settori industriale, sanitario e automobilistico. Il report tiene inoltre conto delle strategie di lungo termine e delle misure di breve termine messe in atto dagli operatori del mercato diretti e da fornitori terzi per gestire la minaccia degli attacchi informatici.

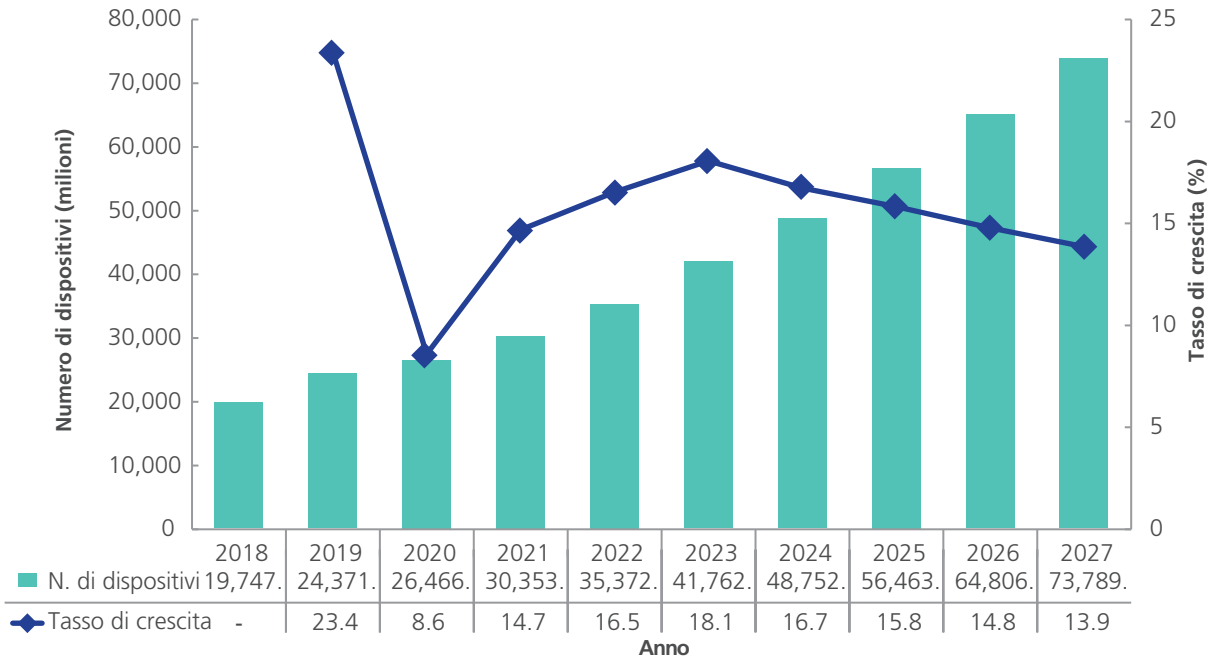
INTRODUZIONE

Nel 2022, i dispositivi IoT connessi erano 35,37 miliardi a livello globale, e si stima che questo numero raggiungerà i 73,79 miliardi entro il 2027, con un tasso di crescita composto annuo (CAGR) del 17,3%.
I dispositivi IoT sono in grado di misurare dati, assegnare identità, creare interconnessioni e generare informazioni

Per qualificarsi come dispositivo IoT, un componente, un prodotto, un'applicazione o un servizio deve far parte di una soluzione più ampia che comprende uno o più di questi quattro elementi.

Nel 2021, il mercato complessivo dell'IoT, che comprende servizi professionali e gestiti, hardware, piattaforme e servizi software e di connettività, ha generato ricavi per 190,26 miliardi di dollari.

DISPOSITIVI IOT CONNESSI, A LIVELLO GLOBALE, 2018-2027



	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027
N. di dispositivi	19,747.	24,371.	26,466.	30,353.	35,372.	41,762.	48,752.	56,463.	64,806.	73,789.
Tasso di crescita	-	23.4	8.6	14.7	16.5	18.1	16.7	15.8	14.8	13.9

Fonte: Frost & Sullivan

Comprendono applicazioni *sia consumer che industrial*, con comunicazioni machine-to-machine in forte espansione in tutti i settori

I servizi IoT per i *consumatori* includono dispositivi indossabili e gadget di monitoraggio personale, come smartwatch o fitness tracker, oltre a elettrodomestici e dispositivi per la casa connessi a internet, come assistenti personali basati su cloud e altoparlanti intelligenti.

I servizi IoT *industriali* (IIoT) puntano a sfruttare la comunicazione machine-to-machine (M2M) e il controllo di qualità per aumentare la produttività e l'efficienza dei sistemi industriali in siti come fabbriche o basi di produzione.

Questi includono i sistemi di riscaldamento, ventilazione e climatizzazione dell'aria (HVAC), di controllo di supervisione e acquisizione dati (SCADA) e monitoraggio industriale basati sulla comunicazione M2M.

Concretamente, secondo la definizione di Frost & Sullivan, il mercato IIoT comprende dispositivi per il tracciamento di beni portatili, la telematica commerciale e di flotte di terzi, il prestito di veicoli, le reti intelligenti, le case intelligenti, l'automazione industriale e di fabbrica, i distributori automatici, i terminali per punti vendita (POS) e transazioni, le applicazioni mediche e sanitarie, l'elettronica di consumo, la telematica per produttori di apparecchiature originali (OEM) (l'"automobile connessa"), l'assicurazione basata sull'utilizzo, la telematica di infotainment e post-vendita, l'automazione degli edifici, la sorveglianza e la sicurezza, il monitoraggio degli asset, la segnaletica digitale e le applicazioni per il benessere, tra gli altri.

Se da un lato l'IoT industriale comporta molti vantaggi, la proliferazione di dispositivi connessi espone inevitabilmente gli asset delle aziende ad attacchi informatici malevoli

La domanda di soluzioni di sicurezza informatica nel settore industriale è trainata dall'aumento della digitalizzazione e della connettività. La convergenza delle *tecnologie informatiche e operative* (IT/OT) espone le organizzazioni e le infrastrutture a un maggiore rischio di attacchi informatici.

Nonostante ciò, molte aziende industriali non dispongono ancora di adeguate misure di sicurezza informatica. I proprietari e gli operatori delle infrastrutture devono salvaguardare sempre più l'ambiente in cui operano, garantire la completa visibilità delle proprie risorse, individuare le vulnerabilità nei loro sistemi e implementare soluzioni che individuino e gestiscano potenziali minacce, riducendo allo stesso tempo il divario di conoscenze tra IT/OT.

Fonte: Frost & Sullivan

PRINCIPALI
ABBREVIAZIONI

IA	*Intelligenza artificiale*
APAC	*Asia Pacifico*
API	*Application Programming Interface - Interfaccia di programmazione dell'applicazione*
Mrd	*Miliardi*
CAGR	*Tasso di crescita composto annuo*
CAN	*Control Area Network - Rete dell'area di controllo*
DDoS	*Distributed Denial of Service*
E2E	*End to End*
ECU	*Electronic Control Unit - Unità di controllo elettronico*
EV	*Electric Vehicle - Veicolo elettrico*
F&B	*Food & Beverage - Alimenti e bevande*
PIL	*Prodotto interno lordo*
HIT	*Healthcare IT - Informatica sanitaria*
HVAC	*Heating, Ventilation and Air Conditioning - Riscaldamento, ventilazione e climatizzazione dell'aria*
IaaS	*Infrastructure as a Service*

UTI	*Unità di terapia intensiva*
IIoT	*Industrial Internet of Things*
IoMT	*Internet of Medical Things*
IoT	*Internet of Things*
ICS	*Industrial Control System - Sistema di controllo industriale*
ISOS	*Integrated Security Operating System - Sistema di Gestione Sicurezza Integrato*
IT	*Information Technology - Informatica*
IVI	*In-vehicle Infotainment - Infotainment a bordo veicolo*
KPI	*Key Performance Indicator - Indicatore chiave di prestazione*
Mio	*Milioni*
M&A	*Mergers and Acquisitions - Fusioni e Acquisizioni*
M2M	*Machine to Machine*
ML	*Machine Learning - Apprendimento automatico*
MSSP	*Managed Security Service Provider - Fornitore di servizi di sicurezza gestiti*
MTTR	*Mean Time to Recovery - Tempo medio di recupero*

Fonte: Frost & Sullivan

O&G	*Oil & Gas - Petrolio e Gas*
OBD	*On-board Diagnostic - Diagnostica di bordo*
OEM	*Original Equipment Manufacturer - Produttore di apparecchiature originali*
OS	*Operating System - Sistema operativo*
OT	*Operational Technology - Tecnologia operativa*
OTA	*Over The Air*
PaaS	*Platform as a Service*
POS	*Point of Sale - Punto vendita*
RoT	*Root of Trust*
SaaS	*Software as a Service*
SCADA	*Supervisory Control and Data Acquisition - Controllo di supervisione e acquisizione dati*
SOAR	*Security Orchestration, Automation and Response - Orchestrazione, automazione e risposta per la sicurezza*
SOC	*Security Operation Center - Centro operativo di sicurezza*
SSL	*Secure Socket Layer*
TA	*Trusted Application - Applicazione attendibile*
TCU	*Telematics Control Unit - Unità di controllo telematico*
TEE	*Trusted Execution Environment - Ambiente di esecuzione affidabile*
TLS	*Transport Layer Security*
TPM	*Tire Pressure Monitoring - Monitoraggio della pressione degli pneumatici*
UEM	*Unified Endpoint Security Management - Gestione unificata della sicurezza degli endpoint*
USA	*Stati Uniti*
V2I	*Vehicle to Infrastructure - Da veicolo a infrastruttura*
V2V	*Vehicle to Vehicle - Da veicolo a veicolo*
V2X	*Vehicle to Everything - Da veicolo a qualsiasi entità*
VPN	*Virtual Private Network - Rete privata virtuale*
WAN	*Wide Area Network - Rete geografica*

Fonte: Frost & Sullivan

INTESA SANPAOLO INNOVATION CENTER:

Intesa Sanpaolo Innovation Center è la società del Gruppo Intesa Sanpaolo dedicata all'innovazione che esplora e studia nuovi modelli di business e di ricerca e agisce da stimolo e motore per la new economy in Italia. La società investe in progetti di ricerca applicata e start-up ad alto potenziale, per favorire la competitività del Gruppo e dei suoi clienti e accelerare lo sviluppo dell'economia circolare in Italia.

Con sede nel grattacielo di Torino progettato da Renzo Piano e un network nazionale e internazionale di hub e laboratori, l'Innovation Center è un abilitatore di relazioni con gli altri stakeholder dell'ecosistema dell'innovazione - come imprese tech, start-up, incubatori, centri di ricerca e università - e promotore di nuove forme di imprenditorialità nell'accesso ai capitali di rischio. Le attività principali su cui si concentra il lavoro di Intesa Sanpaolo Innovation Center sono l'economia circolare, lo sviluppo delle start-up più promettenti, gli investimenti in capitale di rischio della società di gestione Neva SGR e la ricerca applicata.

Per ulteriori informazioni sui prodotti e i servizi di Intesa Sanpaolo Innovation Center, contattare

businessdevelopment@intesasanpaoloinnovationcenter.com

FROST & SULLIVAN:

Con oltre cinquant'anni di esperienza, Frost & Sullivan è conosciuta in tutto il mondo per i suoi servizi dedicati a investitori, dirigenti d'azienda e autorità pubbliche, aiutandoli a orientarsi nei cambiamenti economici e a riconoscere tecnologie rivoluzionarie, macrotendenze, nuovi modelli di business e aziende promettenti, creando ininterrottamente opportunità di crescita per un futuro di successi.

Per ulteriori dettagli sull'ambito di attività e sui servizi offerti da Frost & Sullivan, contattare

LIVIO VANINETTI

Direttore Operativo Frost & Sullivan per l'Italia

livio.vaninetti@frost.com

Data di pubblicazione: febbraio 2024