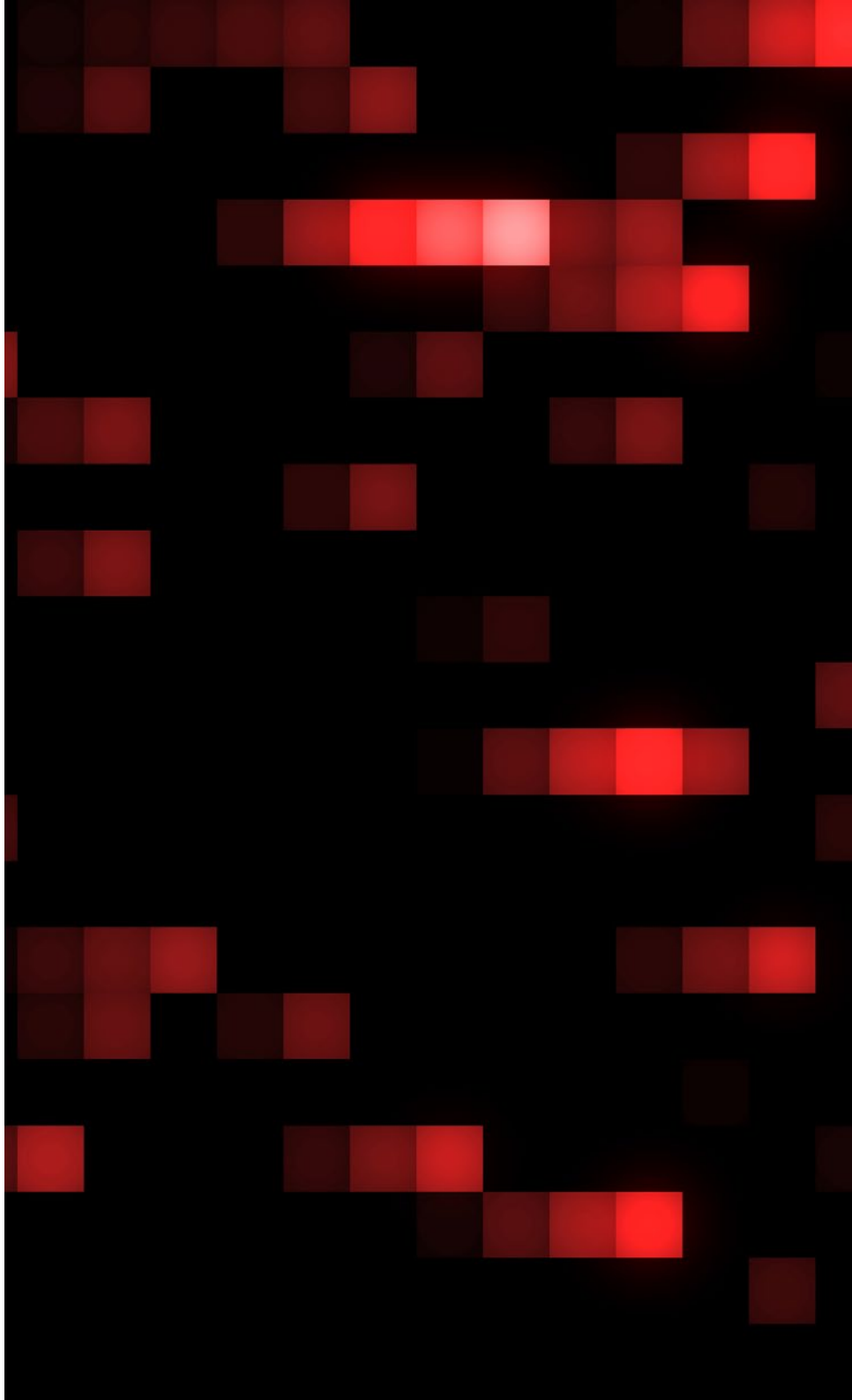
WATCHGUARD THREATSYNC®

Alla scoperta del mondo XDR

Una guida su come sfruttare il potenziale della sicurezza unificata

WatchGuard®

SOMMARIO



01 Le principali sfide di oggi per la sicurezza informatica

Poiché il panorama della sicurezza informatica è sempre più complesso e insidioso, le aziende di tutte le dimensioni faticano a tenere il passo. Gli autori delle minacce non danno la caccia solo alle grandi aziende: prendono di mira in modo aggressivo anche le piccole e medie imprese con sofisticati attacchi informatici.

Le aziende non possono permettersi di nascondere la testa sotto la sabbia e non aggiornarsi in termini di sicurezza. Gli autori delle minacce e le loro tecniche si evolvono rapidamente, per cui è necessario rispondere con la stessa moneta per proteggere gli ambienti, i dispositivi, gli utenti e i dati. Pertanto, è necessario adottare soluzioni di sicurezza in grado di adattarsi e crescere di pari passo con l'azienda e la sua superficie di attacco in espansione.

F12.net™

"La sicurezza informatica non è una destinazione ma un viaggio, semplicemente perché è in continua evoluzione"

Calvin Engen
Chief Technology Officer di F12.net

Quali sono oggi le principali sfide per la sicurezza informatica?

Soluzioni per la sicurezza disconnesse

I team della sicurezza hanno il compito di gestire e contrastare un numero quanto mai crescente di vettori di minacce che minano le reti aziendali, gli endpoint e le identità. Con così tante diverse vulnerabilità in gioco e una gamma così ampia di potenziali attacchi informatici da rilevare e mitigare, ha senso adottare una varietà di soluzioni di sicurezza. Tuttavia, un ampio arsenale di strumenti può essere un'arma a doppio taglio se ogni soluzione funziona in modo indipendente dal resto. Più prodotti di sicurezza non significa più sicurezza.[1]

Un ampio arsenale di strumenti può essere un'arma a doppio taglio se ogni soluzione funziona in modo indipendente dal resto.

[1] Panaseer 2022 Security Leaders Peer Report

19%

Il numero di strumenti di sicurezza utilizzati dalle aziende è aumentato del 19% negli ultimi due anni

36%

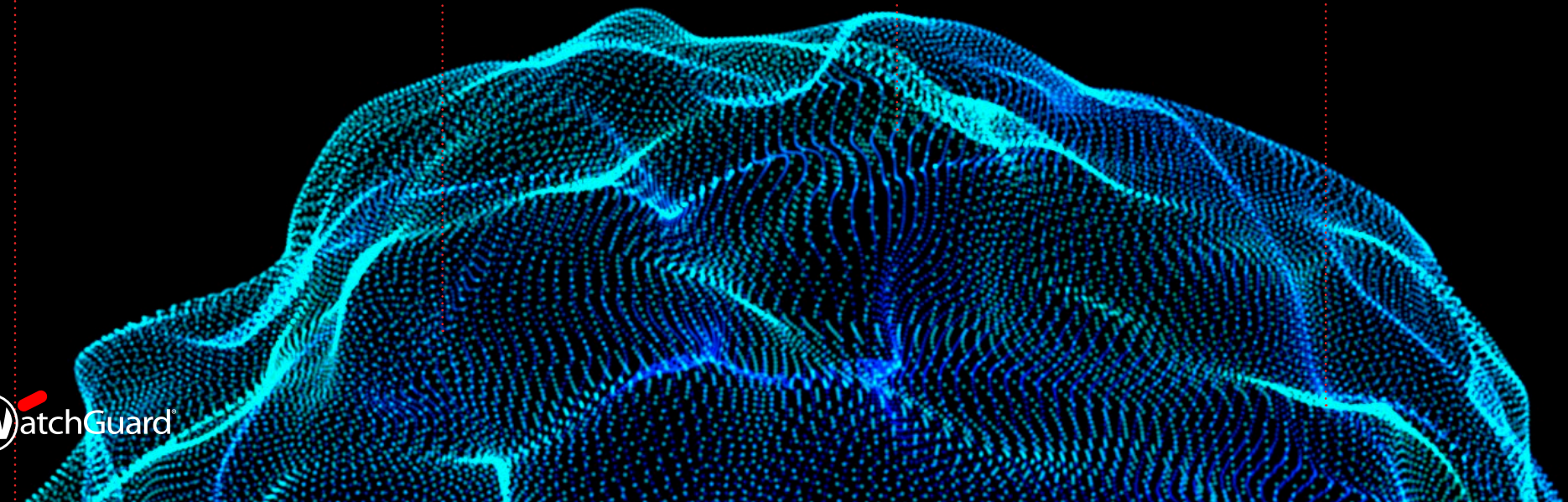
Solo il 36% delle aziende afferma di essere "molto fiducioso" in termini di garantire che i controlli funzionino come previsto

64 - 76

Il numero di strumenti di sicurezza utilizzati dalle grandi aziende è aumentato in media da 64 a 76 applicazioni

82%

Inoltre, l'82% afferma di essere stato sorpreso da incidenti di sicurezza che hanno eluso gli strumenti esistenti



WatchGuard®

Lacune nella visibilità

Tutti questi strumenti separati rendono più difficile avere un'idea completa della protezione. Ogni strumento fornisce solo una visione limitata nella propria area di specializzazione. Presi insieme, il risultato è solo un insieme di tessere di un puzzle che è necessario classificare manualmente e tentare di mettere insieme per comporre un quadro completo.

Come aggravante, il tentativo di mettere insieme i pezzi del puzzle spreca tempo cruciale nel caso di un attacco informatico attivo. Se gli amministratori della sicurezza devono accedere a più console e destreggiarsi tra una mezza dozzina di strumenti diversi solo per determinare cosa potrebbe accadere, i malintenzionati hanno già un notevole vantaggio nell'esecuzione dell'attacco.

> Gli amministratori della sicurezza devono abbattere i compartimenti stagni della sicurezza per smettere di perdere tempo e riuscire a stare al passo con la grande velocità degli attacchi informatici.

Tuttavia, a meno che questi strumenti non siano implementati dallo stesso fornitore, le soluzioni focalizzate su aree di sicurezza diverse raramente forniranno l'interoperabilità necessaria per una protezione efficace.

Difficoltà di correlazione e dati contestuali

Tutti i prodotti di sicurezza, ad esempio le soluzioni di rete, i firewall, la sicurezza degli endpoint o gli strumenti di identità, dispongono di modalità diverse per la presentazione di registri, telemetria e avvisi, ognuna con un formato e una frequenza univoci.

Allo stesso tempo, cercare di interpretare l'immenso volume di dati sulla sicurezza raccolti da questi prodotti è un lavoro immane se svolto manualmente, in quanto i dati sono complessi da combinare e analizzare. È facile perdersi importanti indicatori di minaccia o impantanarsi in falsi positivi quando si affoga nei dati generati da più prodotti disparati. Ciò porta, in ultima analisi, a trascurare minacce che mettono a rischio l'intera organizzazione.

L'integrazione di più prodotti di sicurezza di diversi fornitori può essere complicata e richiedere molto tempo, oltre che conoscenze e competenze specialistiche. Anche se integrati con cura, la gestione di questi prodotti può comunque rivelarsi difficile, principalmente quando si tratta di ambienti IT complessi e diversificati.

Mancanza di automazione della sicurezza

I tuoi utenti si affidano a te per proteggere i loro dati preziosi e salvaguardare le risorse aziendali. Senza automazione, il rilevamento e la risposta in caso di incidenti di sicurezza possono essere operazioni lente e inefficaci e aumentare il rischio di compromettere reti, endpoint e utenti, nonché comportare ulteriori costi e danni per la reputazione conseguenti alla violazione di dati.

1. **Tempi di rilevamento lenti e lunghi**
   Senza rilevamento automatico, i team di sicurezza devono fare affidamento su processi manuali che influiscono in modo significativo sul tempo medio di rilevamento (MTTD), possono impedire la rilevazione di minacce, innescano falsi positivi e ritardano i tempi di risposta agli incidenti. Il ritardo nel rilevare le minacce alla sicurezza può far sì che gli amministratori della sicurezza non vedano le minacce critiche e conducano indagini inutili sugli avvisi di basso livello, portando ad un aumento dei costi e lasciando la porta aperta a potenziali violazioni.

2. **Mancanza di chiarezza sulle azioni di risposta appropriate**
   Come fanno gli amministratori della sicurezza a sapere quale azione di risposta dovrebbero intraprendere per prima? Quando si subisce un incidente di sicurezza, la velocità e l'accuratezza della risposta possono fare la differenza in termini di impatto e portata dell'attacco. Tuttavia, senza capacità di risposta automatizzate, può essere difficile capire quale azione di risposta risolverà la minaccia e ridurrà il tempo medio di risposta (MTTR).

Il tempo è denaro. Tempi di rilevamento lenti e azioni di risposta imprecise possono aiutare gli autori delle minacce a propagare l'attacco in tutta l'azienda e spesso possono comportare tempi di inattività prolungati e perdita di dati. L'automazione della sicurezza mette a tua disposizione servizi di sicurezza coerenti ed efficaci su larga scala.

L'automazione può aiutarti a fornire servizi di sicurezza uniformi ed efficaci su più client e a mantenere un livello standard di sicurezza per tutti.

Complessità della sicurezza e team di sicurezza IT sovraccarichi

Man mano che la tecnologia avanza, gli ambienti IT diventano più complessi, con numerosi sistemi, applicazioni e dispositivi che richiedono un monitoraggio e una manutenzione costanti per garantirne la sicurezza. Inoltre, le minacce sofisticate continuano ad emergere rapidamente, accelerando la pressione a tenere il passo.

Le aziende alla ricerca di nuovi livelli di aggregazione, correlazione e analisi dei dati telemetrici di sicurezza aggiungono ulteriore peso ai già enormi carichi di lavoro del personale addetto alla sicurezza. Gli amministratori devono affrontare un diluvio costante e crescente di avvisi e proteggere una superficie di attacco sempre più diversificata, in cui le minacce sono diventate più complesse da rilevare.

1 **Carenza di professionisti della sicurezza informatica esperti**
Reclutare e trattenere personale qualificato e competente sta diventando sempre più difficile a causa della crescente domanda di professionisti qualificati nel campo, che sono tuttavia estremamente scarsi. Alla luce di questo scenario, ci si può ritrovare a gestire con fatica una vasta gamma di soluzioni di sicurezza specializzate e a non riuscire a trovare il tempo necessario per identificare e mitigare le minacce.

2 **Affaticamento da avvisi**
In media la maggior parte dei professionisti della sicurezza deve affrontare migliaia di avvisi settimanali dovuti ai malware, di cui solo il 19% è considerato effettivo e solo il 4% viene davvero approfondito. Inoltre, alcune soluzioni di sicurezza tradizionali, lungi dal risolvere casi d'uso specifici, creano maggiore stress e aumentano i carichi di lavoro delegando la responsabilità della gestione degli avvisi e costringendo a classificare manualmente le minacce.

Reclutare e trattenere personale qualificato e competente sta diventando sempre più difficile a causa della crescente domanda di professionisti qualificati nel campo, che sono tuttavia estremamente scarsi.

Uno sguardo ravvicinato alle insidie degli approcci alla sicurezza dei prodotti specifici

Le soluzioni di rilevamento e risposta degli endpoint (EDR, Endpoint Detection and Response) e di sicurezza di rete sono due componenti cruciali di una moderna strategia di sicurezza informatica. Questi strumenti aiutano a identificare, rilevare e rispondere alle minacce avanzate contro domini critici.

Sebbene le soluzioni giuste per la sicurezza di rete e l'EDR siano molto efficaci quando si tratta di rilevare e rispondere a minacce sofisticate, offrono visibilità solo su aree specifiche dell'infrastruttura IT. Gli strumenti di sicurezza della rete, come i firewall e i sistemi di rilevamento delle intrusioni, operano su un modello perimetrale della rete e semplicemente non forniscono una visibilità sufficiente degli endpoint. Si concentrano sulla protezione dei punti di entrata e di uscita della rete e sul monitoraggio del traffico ai margini della rete. Tuttavia, con l'avvento del modello di lavoro ibrido, il perimetro della rete è diventato sempre più poroso, rendendo più difficile mantenere una sicurezza efficace.

Allo stesso modo, le soluzioni EDR sono diventate strumenti essenziali nello sforzo di rilevamento e risposta alle minacce per gli endpoint, ma da sole non possono fornire visibilità sulle minacce che si verificano all'interno dei vari ambienti di rete aziendali.

Di conseguenza, molte aziende sono spesso costrette a utilizzare un patchwork di prodotti per rilevare le minacce su più livelli di sicurezza. Poiché le varie soluzioni di sicurezza operano indipendentemente l'una dall'altra, questo approccio frammentato crea punti ciechi, limita la visibilità, i risultati contestuali e l'efficacia del rilevamento e della risposta e, in ultima analisi, rende impossibile la protezione completa end-to-end.

Probabilmente hai già molta familiarità con queste sfide. Gli amministratori della sicurezza le affrontano da troppo tempo. La verità è che la maggior parte di questi ostacoli è semplicemente il sottoprodotto di approcci obsoleti alla sicurezza. Superarli richiede l'impegno a modificare la propria linea d'azione e intraprendere un nuovo percorso per la sicurezza.

02 XDR: la tua porta d'accesso per la sicurezza moderna

Per vincere queste sfide, è necessario adottare un approccio integrato che fornisca correlazione dei dati di contesto e telemetrici su più livelli di sicurezza e domini IT.

> Con soluzioni di sicurezza più strettamente integrate, è possibile ottenere una visione completa del proprio stato di sicurezza.

Un approccio moderno e integrato alla sicurezza informatica dovrebbe includere funzionalità XDR (Extended Detection and Response, rilevamento e risposta estesi) con tecnologie di automazione e intelligenza artificiale, che possono migliorare notevolmente l'efficacia della sicurezza rispetto alle minacce avanzate, semplificando al contempo le operazioni di sicurezza.

Come funziona l'XDR?

Viviamo in una realtà in cui gli attacchi informatici sono la regola più che l'eccezione, e nulla causa più scompiglio di quando queste minacce si materializzano. Mentre gli esperti sono chiamati a lottare con attacchi persistenti e in continua evoluzione e a destreggiarsi fra molteplici sistemi e strumenti, è il momento giusto per adottare una soluzione completa di rilevamento e risposta alle minacce che porti gli MSP in un nuovo mondo di opportunità. L'XDR è la soluzione.

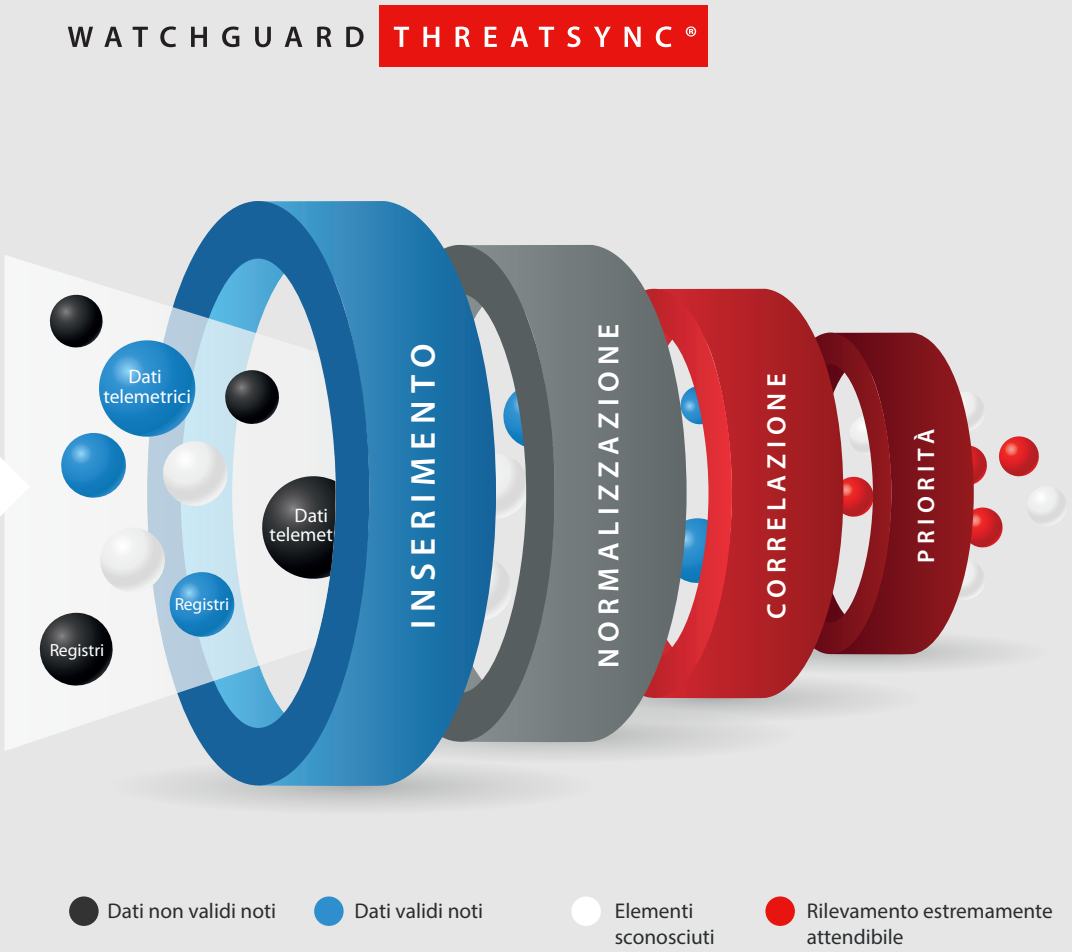
L'XDR offre notevoli vantaggi rispetto agli strumenti di sicurezza disconnessi. Fornisce il contesto e la visibilità necessari per identificare e risolvere gli attacchi informatici con un più alto grado di velocità ed efficacia. L'XDR offre un approccio completo alla sicurezza che sfrutta le tecnologie di automazione e intelligenza artificiale per rilevare e rispondere alle minacce su firewall, server, workstation e dispositivi.

> Una soluzione XDR integrata può semplificare le operazioni di sicurezza, ridurre rallentamenti operativi e costi e può aiutare a raggiungere una maggiore protezione in generale.

Sicurezza degli endpoint

XDR

Sicurezza di rete



03 Accedi al mondo XDR e dai il via libera alla sicurezza unificata

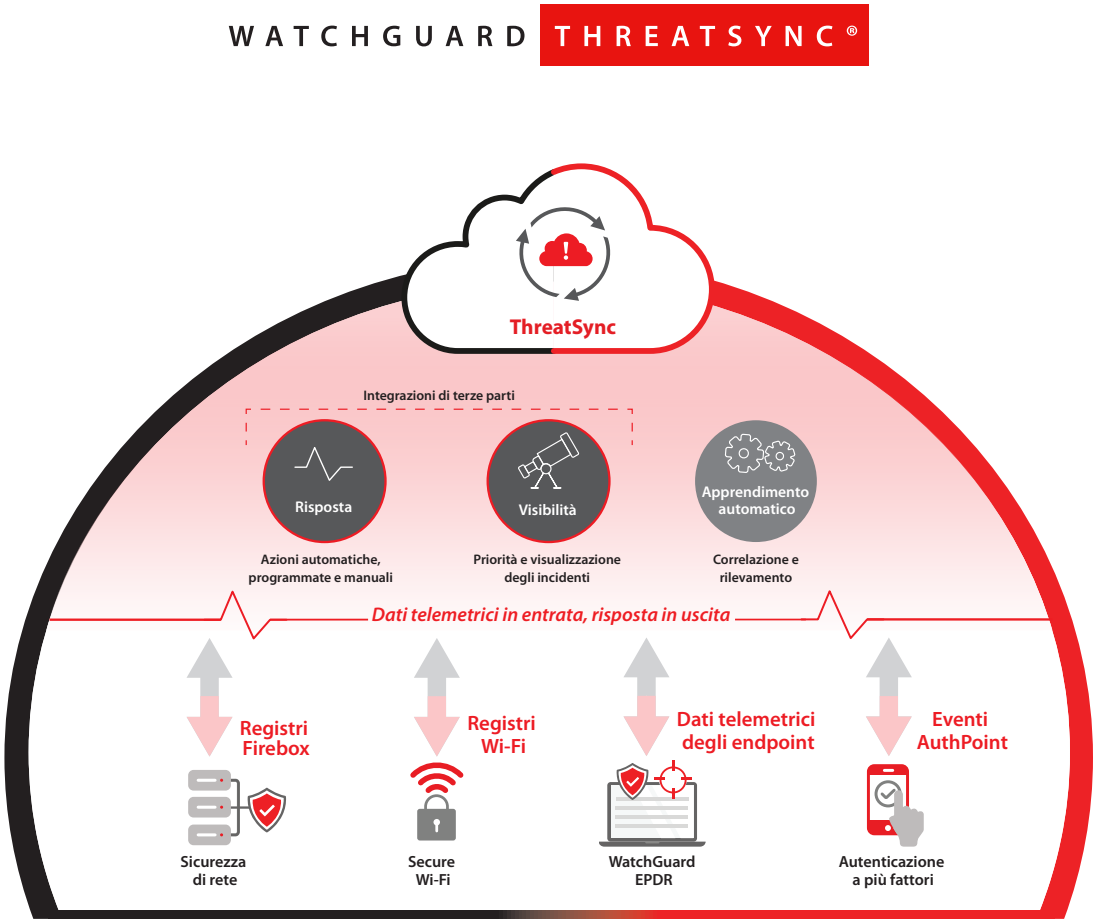
Con ThreatSync offriamo una soluzione XDR completa e semplice da usare, un livello centrale all'interno dell'architettura Unified Security Platform® di WatchGuard. Questo ci consente di unificare i rilevamenti di più prodotti e accelera la risposta alle minacce da un'unica interfaccia.

Estendere, rilevare e rispondere con ThreatSync

1 Estendere
Implementiamo XDR con le integrazioni ottimizzate e la telemetria dei dati di più domini offerte dalle tecnologie di ultima generazione di WatchGuard. Ampliando la gamma di feed di dati per includere intelligence sulle minacce per reti, endpoint e utenti, estendiamo la visibilità e la protezione.

2 Rilevare
Addio ai vecchi approcci alla sicurezza a compartimenti stagni che rallentano i tempi di rilevamento e si dimostrano inefficienti nella prevenzione di alcuni attacchi. Con le capacità di intelligenza artificiale e apprendimento automatico di ThreatSync, identifichiamo le potenziali minacce in tempo reale in diversi domini, per ridurre i tempi di rilevamento e procedere a un rapido contenimento.

3 Rispondere
L'XDR velocizza i tempi di risposta e migliora la sicurezza della tua azienda. Con ThreatSync orchestriamo azioni di risposta automatiche per neutralizzare le minacce contro la tua azienda in modo semplice, rapido e accurato.



* Secure Wi-Fi e AuthPoint saranno presto disponibili, integrati in ThreatSync.

XDR, potente ma semplice

Rilevamento delle minacce multipiattaforma

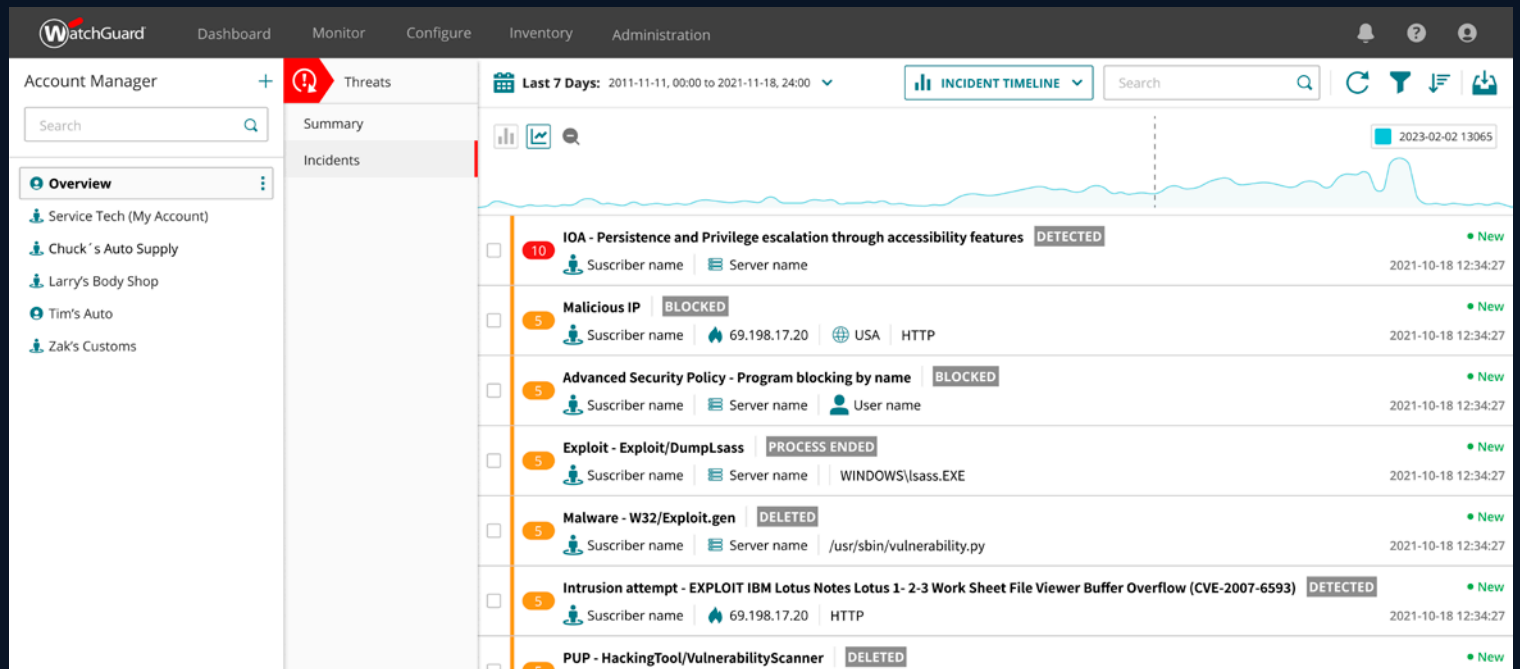
ThreatSync fornisce ampie funzionalità di rilevamento utilizzando gli indicatori di compromissione (IoC) provenienti da tutti i prodotti di sicurezza WatchGuard e mettendo tali indicatori in relazione tra loro. Tale correlazione e tale contesto multidominio consentono alla soluzione di rilevare e classificare le attività potenzialmente dannose relative a specifici ambienti, utenti e dispositivi per ridurre l'MTTD, migliorare l'accuratezza e, infine, permettere una più rapida risoluzione.

Orchestrazione della sicurezza unificata e risposta alle minacce

XDR fornisce una visione olistica della superficie esposta alle minacce, facilitando l'identificazione dei problemi, il triage e la risposta sicura e rapida. ThreatSync aumenta l'efficacia e l'efficienza grazie a una classificazione degli avvisi intelligente, a policy di correzione automatizzate e a opzioni per l'intervento manuale se necessario. Questo livello di orchestrazione della risposta alle minacce aumenta sia la portata sia la precisione.

Semplice da implementare e gestire

Grazie alle sue intuitive funzionalità di gestione e automazione basate su cloud, ThreatSync facilita l'adozione dell'approccio XDR. Fornendo solide funzionalità XDR all'architettura Unified Security Platform di WatchGuard, ThreatSync integra l'intelligence tra i vari prodotti per ridurre i costi e gli oneri di gestione legati all'implementazione di più soluzioni specifiche per il rilevamento e la risposta alle minacce.

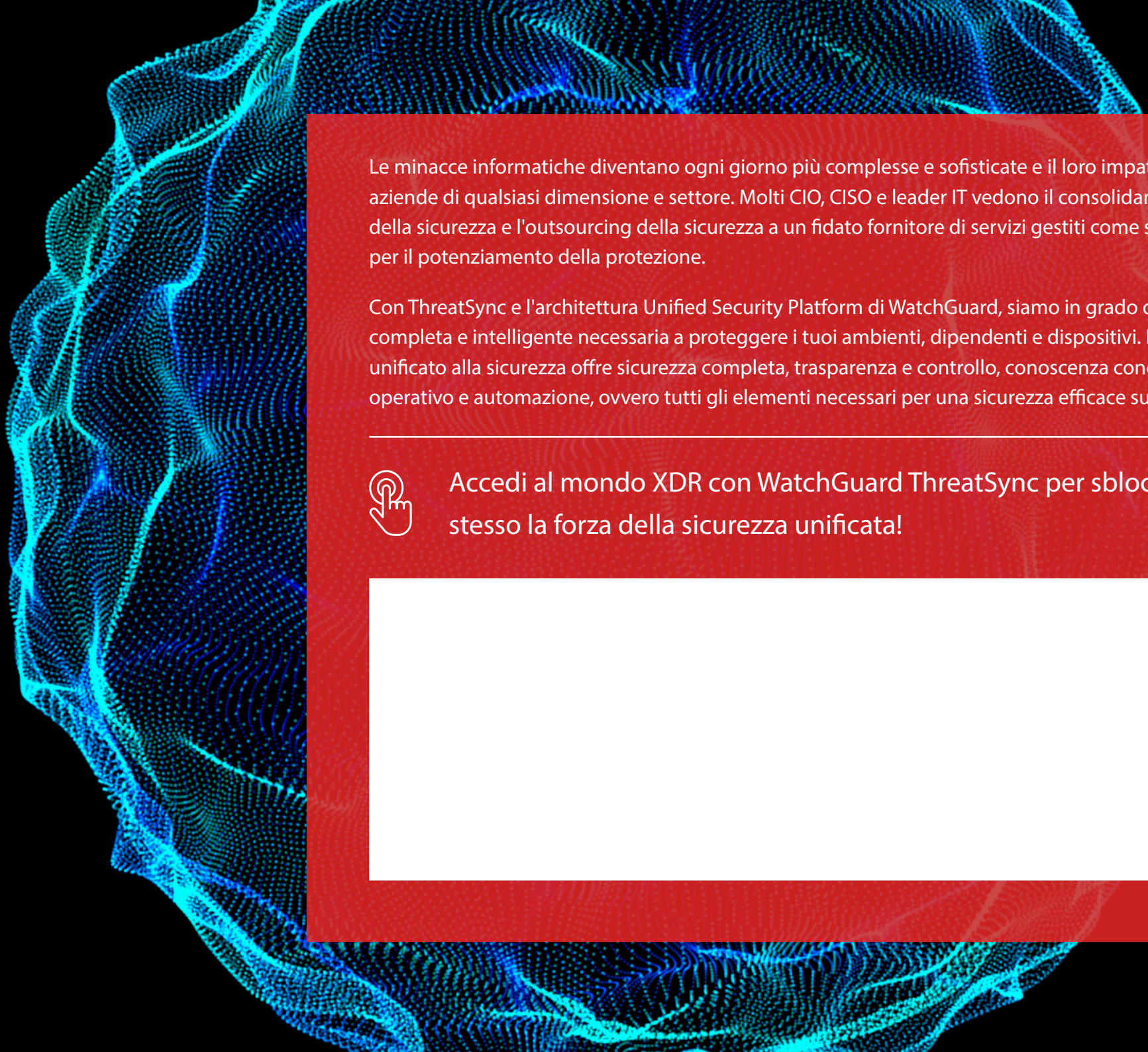


Maggiore visibilità sull'attività di rete e degli endpoint, utile per identificare minacce che altrimenti potrebbero passare inosservate

Sicurezza completa mediante l'unificazione di dati e avvisi in un'unica piattaforma in cui le soluzioni possono collaborare per definire le priorità e rispondere alle minacce

Alleggerimento del carico del team di sicurezza automatizzando il processo di rilevamento e risposta e liberando tempo e risorse per altre attività importanti

Semplificazione del processo di risposta grazie a risposte coordinate e automatizzate alle minacce rilevate



Le minacce informatiche diventano ogni giorno più complesse e sofisticate e il loro impatto colpisce le aziende di qualsiasi dimensione e settore. Molti CIO, CISO e leader IT vedono il consolidamento dei fornitori della sicurezza e l'outsourcing della sicurezza a un fidato fornitore di servizi gestiti come soluzioni convenienti per il potenziamento della protezione.

Con ThreatSync e l'architettura Unified Security Platform di WatchGuard, siamo in grado di fornire la protezione completa e intelligente necessaria a proteggere i tuoi ambienti, dipendenti e dispositivi. Il nostro approccio unificato alla sicurezza offre sicurezza completa, trasparenza e controllo, conoscenza condivisa, allineamento operativo e automazione, ovvero tutti gli elementi necessari per una sicurezza efficace su larga scala.

Accedi al mondo XDR con WatchGuard ThreatSync per sbloccare oggi stesso la forza della sicurezza unificata!

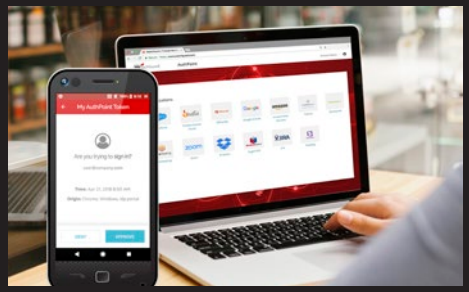
Portafoglio prodotti WatchGuard

Sicurezza di rete

Le soluzioni per la sicurezza di rete di WatchGuard sono totalmente progettate per garantire facilità di implementazione, uso e gestione, oltre a fornire la massima sicurezza possibile. Il nostro esclusivo approccio alla sicurezza di rete è incentrato sull'offerta di una sicurezza all'avanguardia di livello enterprise a qualunque tipo di azienda, a prescindere dalle dimensioni o dalle competenze tecniche.

Secure Wi-Fi

Le soluzioni Secure Wi-Fi di WatchGuard, rivoluzionarie per il mercato di oggi, sono progettate per fornire sicurezza e protezione per gli ambienti Wi-Fi, eliminando al contempo le lungaggini amministrative e riducendo notevolmente i costi. Grazie all'ampia gamma di strumenti di coinvolgimento e alla visibilità dell'analisi aziendale, offrono alle aziende il vantaggio competitivo di cui hanno bisogno per avere successo.



Autenticazione a più fattori

WatchGuard AuthPoint® è la soluzione ideale per gestire le lacune della sicurezza basata su password grazie all'autenticazione a più fattori tramite una piattaforma cloud facile da usare. L'approccio esclusivo di WatchGuard aggiunge il "DNA del cellulare" come fattore di identificazione, per garantire che solo gli utenti autorizzati possano accedere a reti sensibili e applicazioni cloud.

Sicurezza degli endpoint

WatchGuard Endpoint Security è un portafoglio di avanzate soluzioni native per il cloud ideato per la sicurezza degli endpoint che protegge qualsiasi tipo di azienda di da attacchi informatici attuali e futuri. WatchGuard EPDR, la sua soluzione principale basata sull'intelligenza artificiale, migliora immediatamente la protezione delle organizzazioni. Combina funzionalità di protezione degli endpoint (EPP) e di rilevamento e risposta degli endpoint (EDR) con un'applicazione Zero Trust e servizi di ricerca delle minacce.

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella sicurezza informatica unificata. Il nostro approccio Unified Security Platform® è concepito unicamente per i fornitori di servizi gestiti che offrono sicurezza di alto livello per aumentare la scalabilità e la velocità di crescita della propria azienda, migliorandone al contempo l'efficienza operativa. Scelti da oltre 17.000 rivenditori e fornitori di servizi, che provvedono alla sicurezza di più di 250.000 clienti, i pluripremiati prodotti e servizi della nostra azienda coprono l'intelligence e la sicurezza di rete, la protezione avanzata degli endpoint, l'autenticazione a più fattori e la protezione Wi-Fi. Tutto questo offre i cinque elementi essenziali di una piattaforma di sicurezza: sicurezza completa, conoscenza condivisa, trasparenza e controllo, allineamento operativo e automazione. La sede centrale di WatchGuard si trova a Seattle (Washington, Stati Uniti), con uffici dislocati in Nord America, Europa, Asia e America Latina. Per saperne di più, visita WatchGuard.com/it.

NUMERO VERDE ITALIA: **800.911.938** UFFICIO COMMERCIALE INTERNAZIONALE **1.206.613.0895** WEB **www.watchguard.com/it**