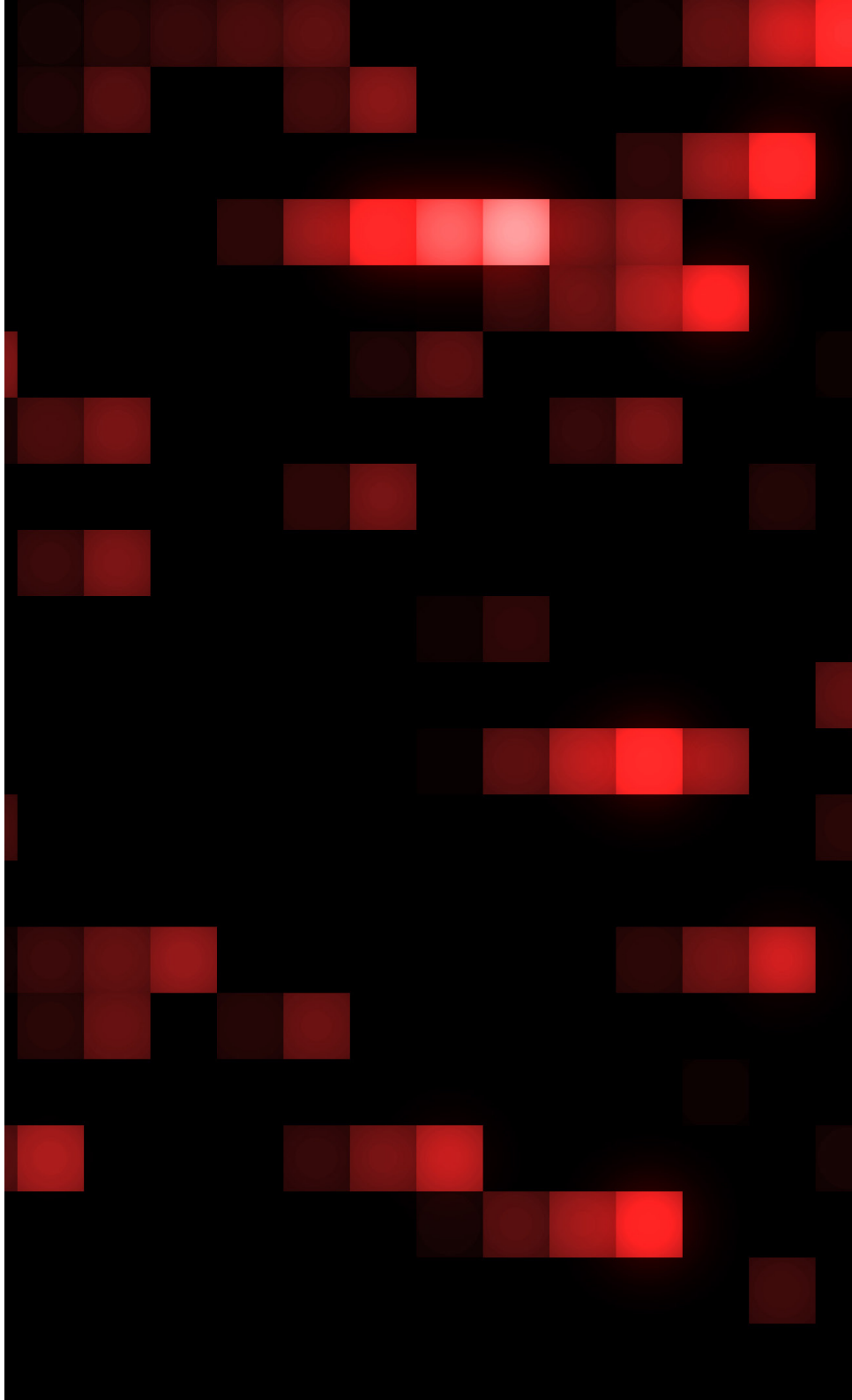
WATCHGUARD THREATSYNC®

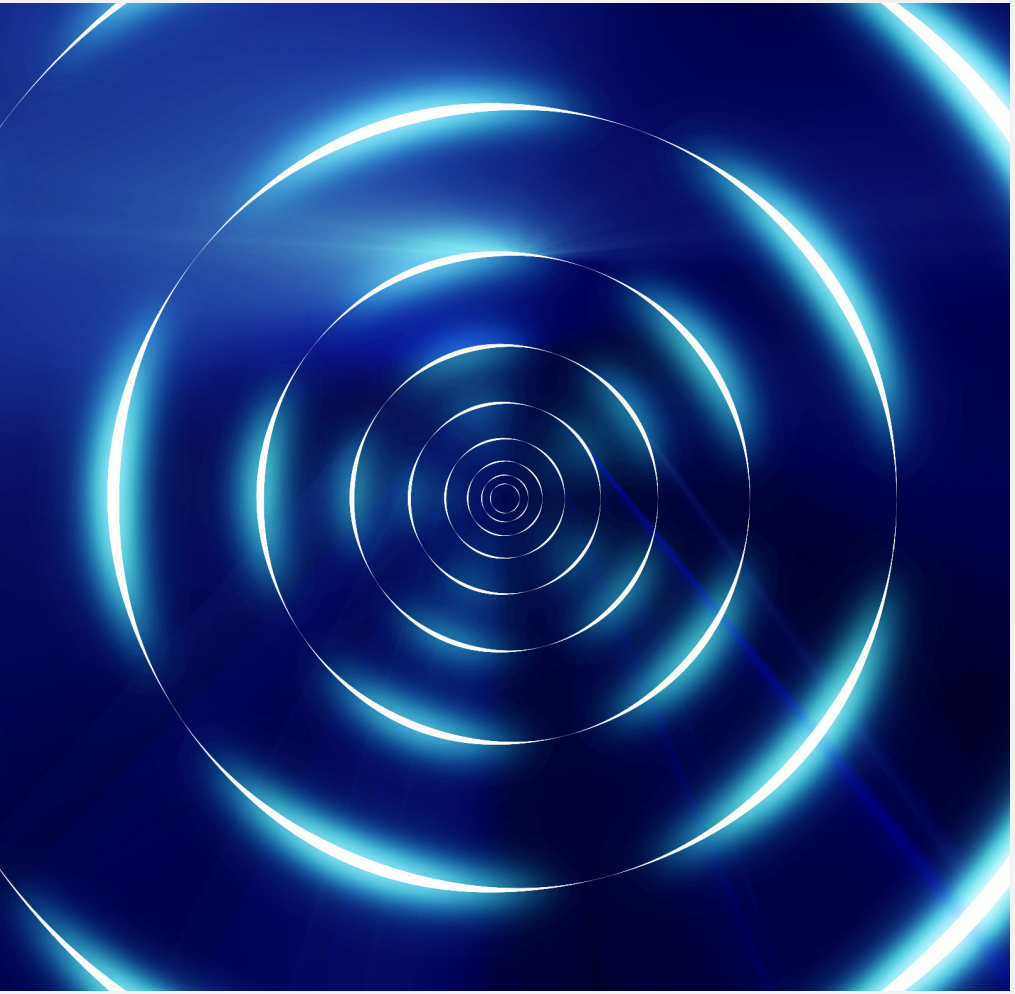
# Alla scoperta del mondo XDR

## Una guida per gli MSP su come sfruttare il potenziale della sicurezza unificata

# 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 (nonché i loro partner commerciali) 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. Le aziende e i loro fidati fornitori di servizi gestiti (MSP) devono rispondere con la stessa moneta per proteggere i propri ambienti, dispositivi, utenti e dati. Pertanto, è necessario adottare soluzioni di sicurezza in grado di adattarsi e crescere di pari passo con l'azienda e l'odierna superficie di attacco in continua 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 in termini di sicurezza informatica per gli MSP?

### Soluzioni per la sicurezza disconnesse

I fornitori di soluzioni di 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 dei propri clienti. 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%

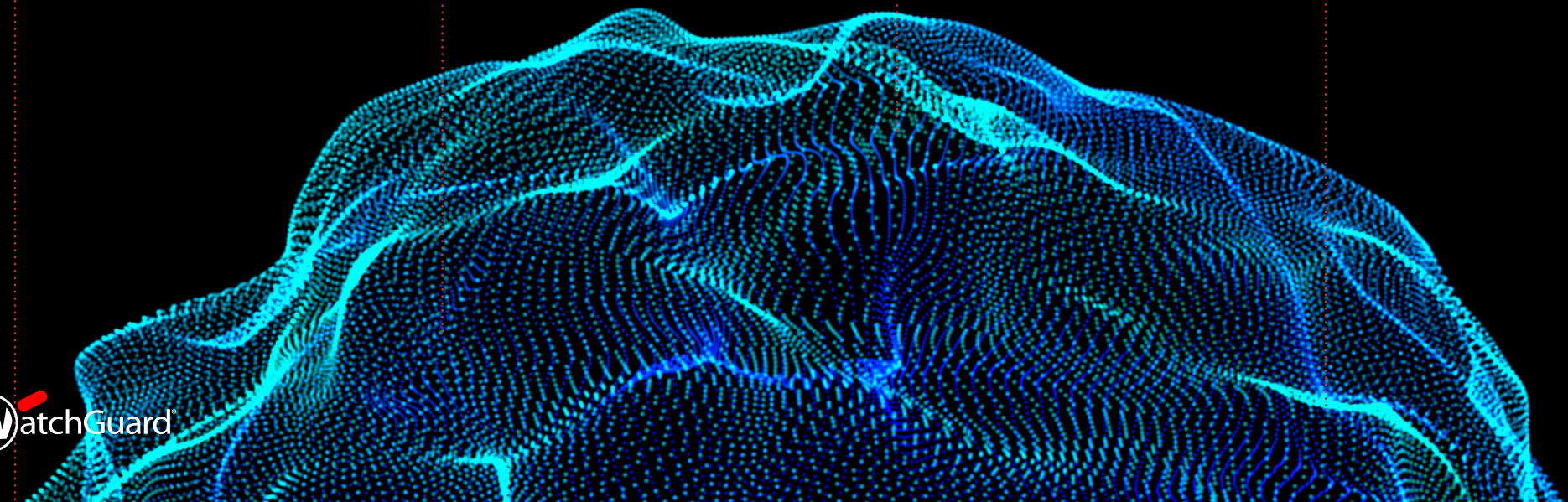
Solo il 36% delle aziende afferma di essere "molto fiducioso" in termini di garantire che i controlli funzionino come previsto

# 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 difficile per gli MSP costruire una visione d'insieme dello stato di protezione di un cliente. 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 MSP 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 immenso 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, infine, a trascurare minacce che mettono a rischio i clienti.

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

Come MSP, i tuoi clienti si affidano a te per proteggere i loro dati preziosi e assicurarsi che la loro attività rimanga integra. Senza automazione, rilevare e rispondere agli incidenti di sicurezza può essere un'operazione lenta e inefficace, che mette i clienti a rischio di costose violazioni dei dati e danni per la reputazione.

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 il tuo team non veda le minacce critiche e conduca 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 un'azienda 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 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

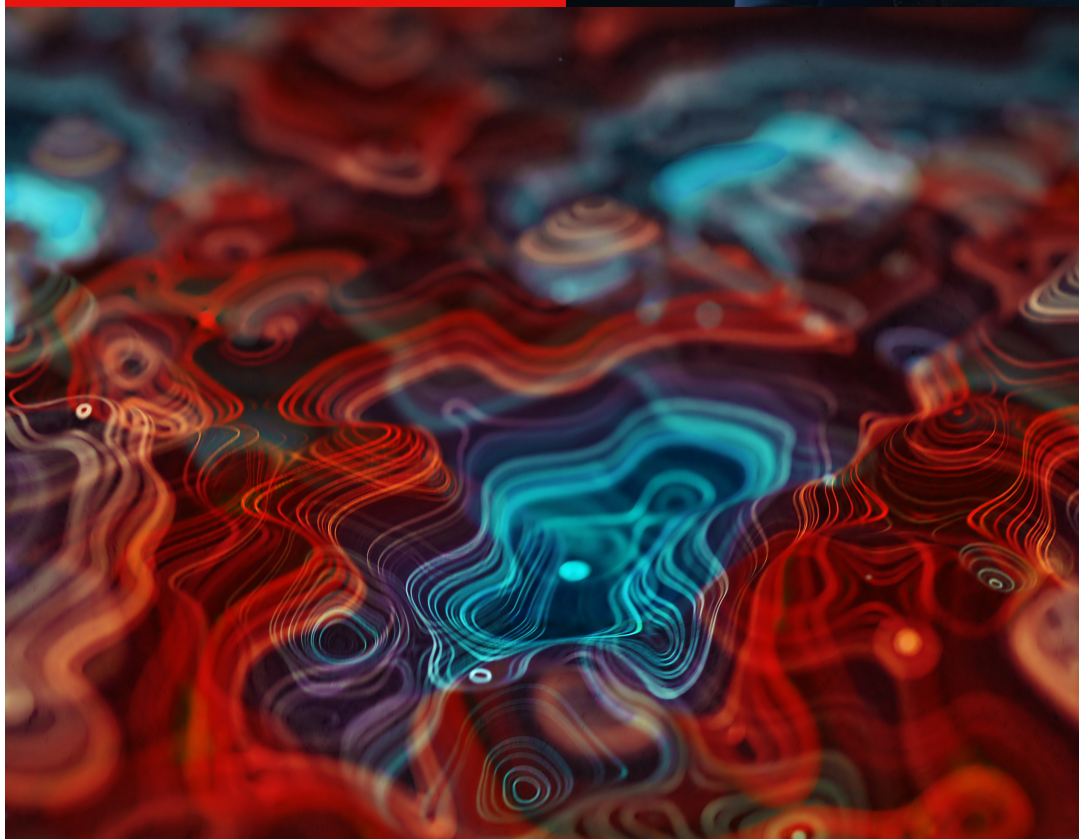
Man mano che la tecnologia avanza, gli ambienti IT diventano più complessi, con numerosi sistemi, applicazioni e dispositivi che richiedono un monitoraggio e una manutenzione costanti per garantirne la sicurezza. Inoltre, continuano a emergere rapidamente minacce sofisticate che esercitano un'enorme pressione sui team degli MSP, obbligati a tenere il passo.

Gli MSP 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, gli MSP con personale ridotto faticano a gestire una vasta gamma di soluzioni di sicurezza specializzate e a trovare il tempo necessario per identificare e mitigare le minacce.

2 **Affaticamento da avvisi**
In media, la maggior parte delle aziende 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 dei fornitori di servizi delegando la responsabilità della gestione degli avvisi e costringendoli a classificare

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

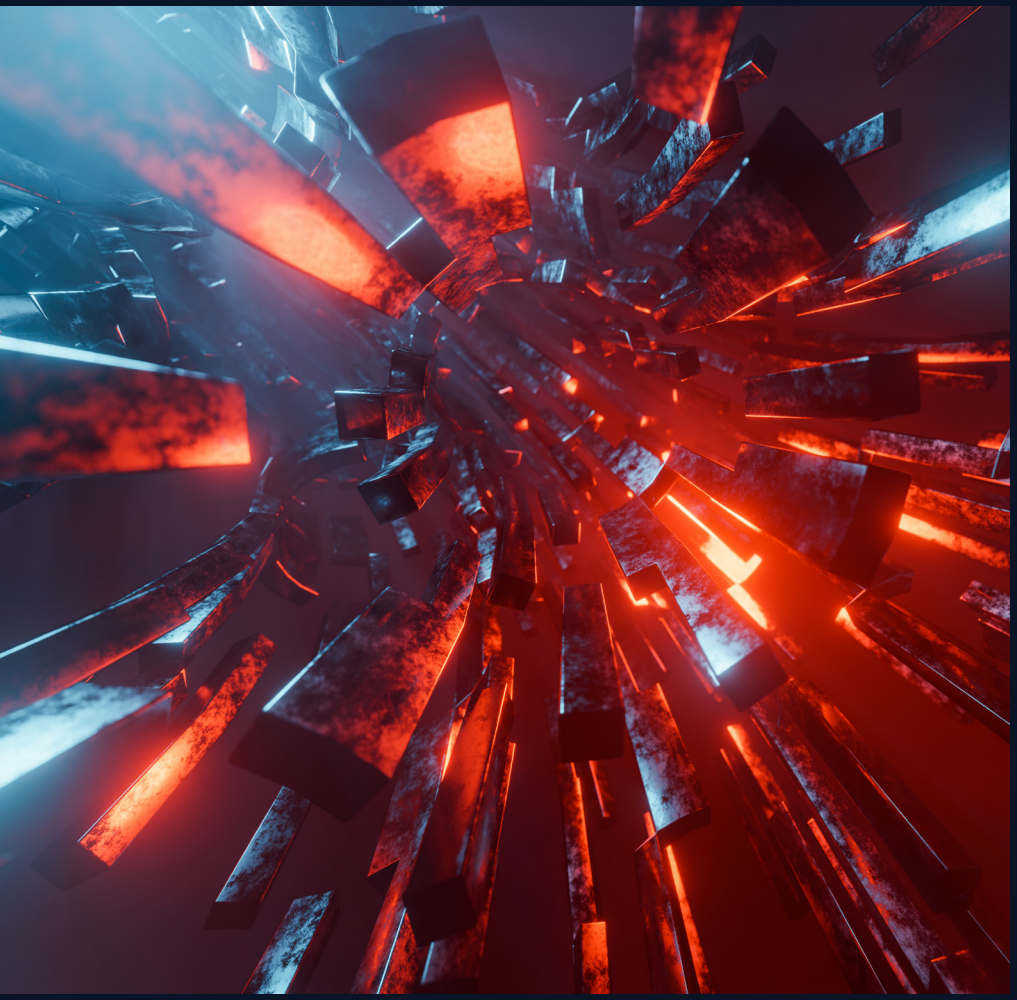
Le soluzioni di rilevamento e risposta degli endpoint (EDR, Endpoint Detection and Response) e di sicurezza di rete sono due componenti cruciali di una moderna strategia di sicurezza informatica. Questi strumenti consentono alle aziende di identificare, rilevare e rispondere a minacce avanzate contro 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 agli MSP 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 per gli MSP che lavorano per rilevare e rispondere alle minacce per gli endpoint, ma da sole non possono fornire visibilità sulle minacce che si verificano all'interno dei vari ambienti di rete dei clienti.

Di conseguenza, gli MSP sono spesso costretti a utilizzare un patchwork di prodotti per rilevare le minacce su più livelli di sicurezza. Questo approccio frammentato, in cui le soluzioni di sicurezza operano indipendentemente l'una dall'altra, crea punti ciechi. Limita la visibilità, i risultati contestuali e l'efficacia del rilevamento e della risposta, rendendo quasi impossibile fornire una protezione completa e end-to-end per i clienti.

Probabilmente hai già molta familiarità con queste sfide. Gli MSP 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, gli MSP devono adottare un approccio integrato che fornisca correlazione dei dati di contesto e telemetria su più livelli nei complessi ambienti IT di oggi. È necessario implementare soluzioni di sicurezza strettamente integrate per ottenere una visione completa dello stato di sicurezza dei clienti.

> Adottando un approccio integrato alla sicurezza informatica che includa funzionalità XDR (Extended Detection and Response, rilevamento e risposta estesi) con tecnologie di automazione e intelligenza artificiale, è possibile migliorare notevolmente l'efficacia della sicurezza rispetto alle minacce avanzate, semplificando al contempo le operazioni di sicurezza.

## Come funziona 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 alle prese con attacchi persistenti e in continua evoluzione e con più sistemi e strumenti di cui occuparsi, ora è il momento giusto per una soluzione completa di rilevamento e risposta alle minacce che porti gli MSP in un nuovo mondo di opportunità. XDR è la soluzione.

XDR offre agli MSP 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.

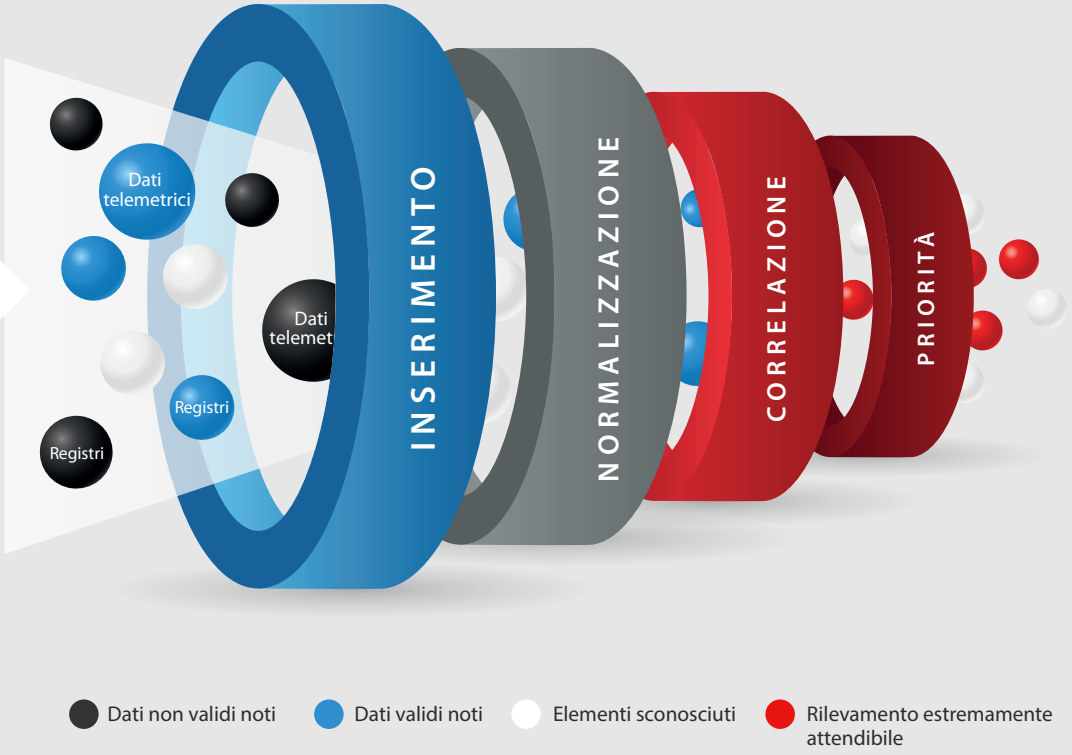
> L'adozione di una soluzione XDR integrata può aiutarti a semplificare le operazioni di sicurezza, ridurre i costi operativi e aiutare i clienti a ottenere un livello di protezione più efficace e completo.

XDR offre notevoli vantaggi rispetto agli strumenti di sicurezza disconnessi. Con XDR, hai il contesto e la visibilità necessari per identificare e risolvere gli attacchi informatici con un più alto grado di velocità ed efficacia. Se vuoi fornire ai tuoi clienti un approccio semplificato e più efficace, l'adozione di una soluzione XDR è la strada da percorrere.

**Sicurezza degli endpoint**

XDR

**Sicurezza di rete**



# XDR a livello di gestione della sicurezza

## Classificazione delle minacce e assegnazione delle priorità

XDR mette in correlazione e riunisce i dati delle attività a diversi livelli di sicurezza e offre una visione prioritaria delle minacce più rilevanti

## Sicurezza semplificata e consolidata

L'intelligence sulle minacce integrata proveniente da ambienti, utenti e dispositivi elimina la necessità di molteplici soluzioni specifiche e semplifica le operazioni di sicurezza.

## Velocità e certezza

XDR offre funzionalità avanzate che consentono rilevamenti precoci, risposte più rapide e maggiormente attendibili e una sicurezza rafforzata.

## Intelligence sulle minacce contestuale

Presi insieme, molti singoli eventi possono essere indicatori di un incidente. XDR consente una contestualizzazione più significativa dei dati e tra domini per accelerare il rilevamento delle minacce.

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

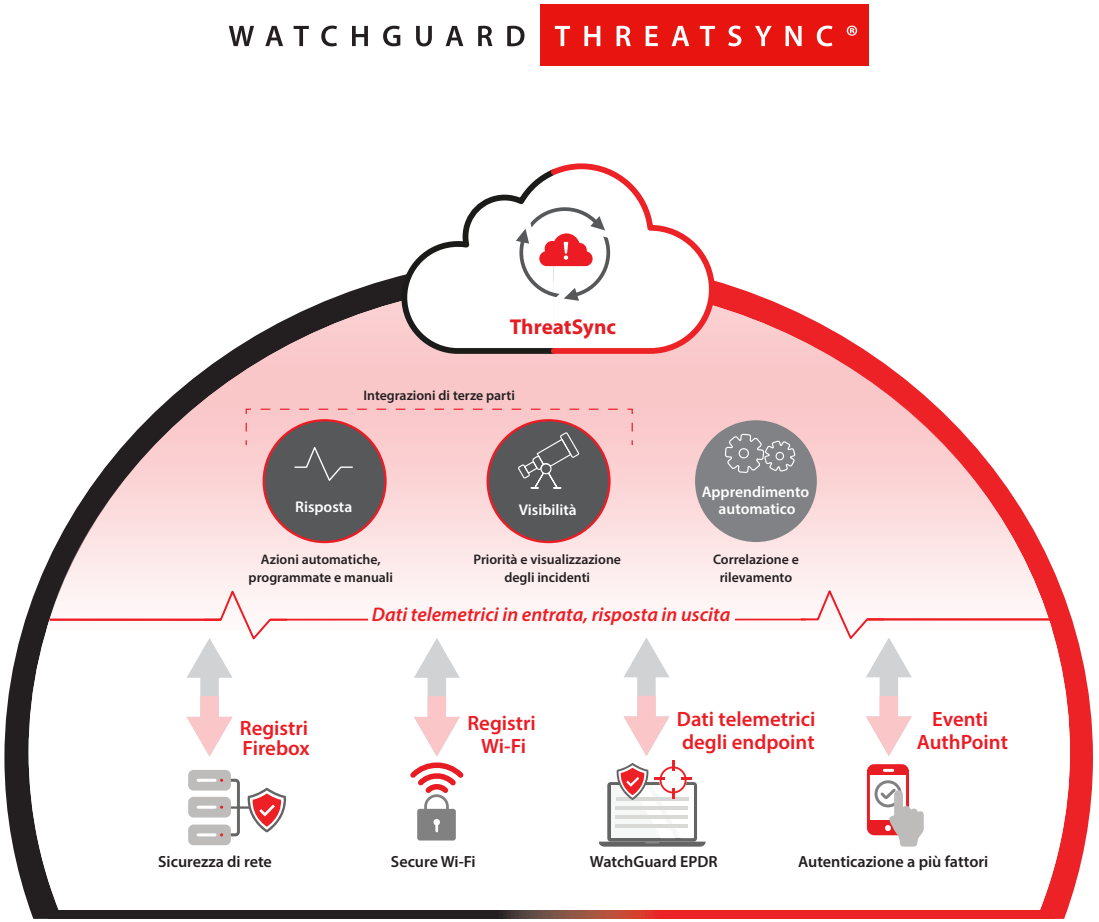
ThreatSync è una soluzione XDR completa e semplice da usare, inclusa nell'architettura Unified Security Platform® di WatchGuard, che unifica i rilevamenti di più prodotti e accelera la risposta alle minacce da un unico pannello di controllo.

## Estendere, rilevare e rispondere con ThreatSync

1 **Estendere**
Sviluppa la tua strategia 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 dal tuo stack di sicurezza in crescita, otterrai una visibilità molto maggiore e una protezione più solida.

2 **Rilevare**
Abbandona il vecchio approccio alla sicurezza a compartimenti stagni e gli strumenti reattivi, scegli il rilevamento basato sull'intelligence sulle minacce derivante da più fonti interconnesse. ThreatSync utilizza l'intelligenza artificiale e l'apprendimento automatico per identificare potenziali minacce in tempo reale tra domini per ridurre i tempi di rilevamento e contenere rapidamente la gravità e la portata dell'attacco.

3 **Rispondere**
Affidati a XDR per rispondere alle minacce in un lampo. ThreatSync consente l'orchestrazione di azioni di risposta automatizzate per neutralizzare le minacce in tutta l'azienda, da un unico pannello di controllo in un processo più semplice e veloce, riducendo i rischi e offrendo una maggiore precisione.




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

# XDR, potente ma semplice

### Rilevamento delle minacce multipiattaforma

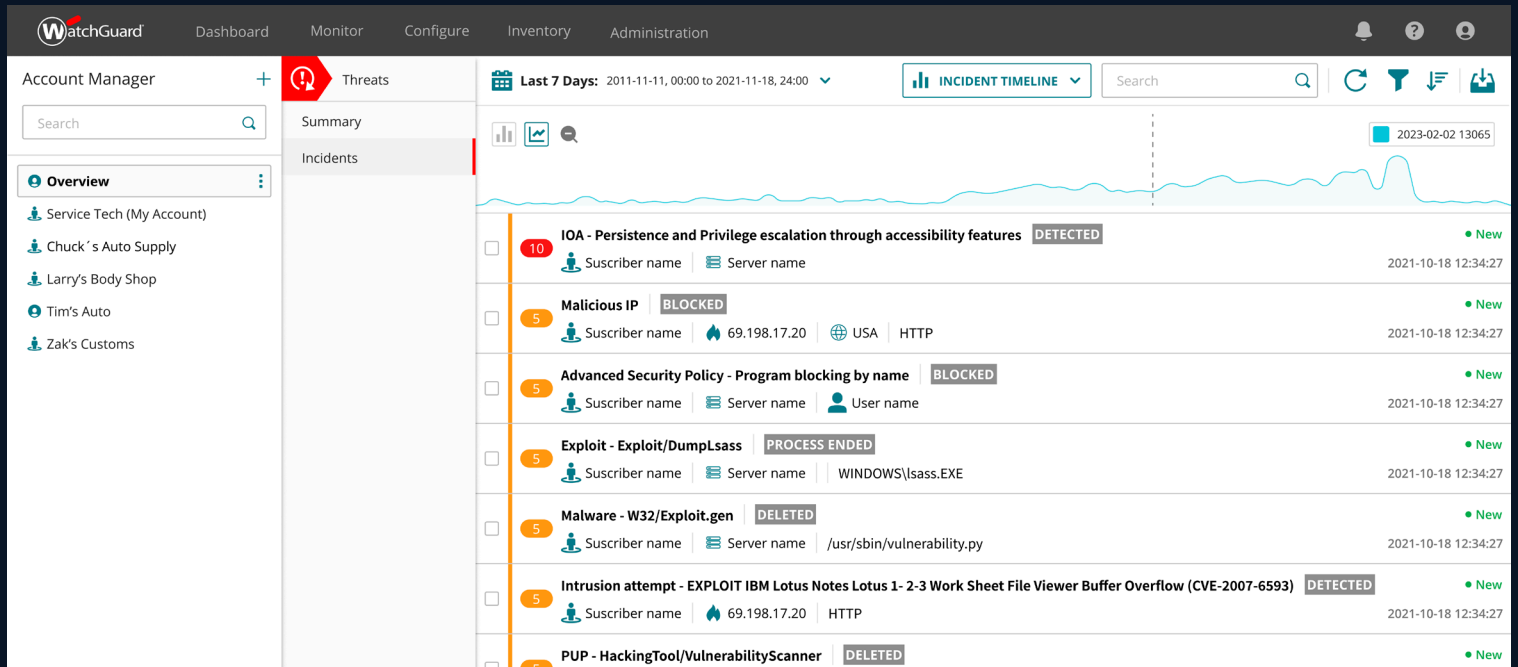
ThreatSync fornisce ampie funzionalità di rilevamento utilizzando gli indicatori di compromissione (IoC) provenienti da tutti i prodotti di sicurezza WatchGuard e mettendo tali indicatori in relazione tra loro. Tale correlazione e tale contesto multidominio consentono alla soluzione di rilevare e classificare 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

Quando gli amministratori della sicurezza e dell'IT hanno una visione olistica della loro superficie esposta alle minacce, riescono facilmente a eseguire il triage e rispondere in modo certo e rapido. ThreatSync consente di lavorare in modo più efficiente con una classificazione degli avvisi intelligente, policy di correzione automatizzate e opzioni per l'intervento manuale se necessario. Questo livello di orchestrazione della risposta alle minacce aumenta sia la portata sia la precisione per i team di sicurezza.

### Semplice da implementare e gestire

Grazie alle sue intuitive funzionalità di gestione e automazione basate su cloud, WatchGuard ThreatSync facilita l'adozione dell'approccio XDR, specialmente in quei contesti dove il tempo e le competenze scarseggiano. 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

**Nessun costo aggiuntivo per l'uso di XDR:** XDR è un principio essenziale della moderna sicurezza informatica che dovrebbe essere alla portata di tutte le aziende. Ecco perché WatchGuard include ThreatSync senza alcun costo aggiuntivo

# 04 ThreatSync e l'approccio della Unified Security Platform di WatchGuard

ThreatSync è un livello di importanza cruciale all'interno dell'architettura Unified Security Platform di WatchGuard, un'unica piattaforma per semplificare e rafforzare ogni aspetto dell'utilizzo, della fornitura e della gestione della sicurezza.

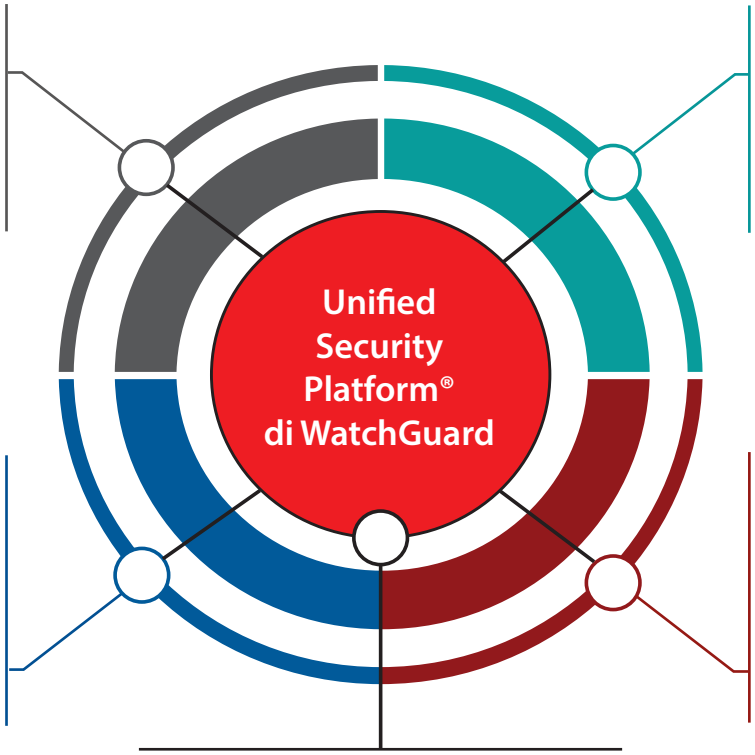
Il nostro approccio unificato alla sicurezza offre sicurezza completa, trasparenza e controllo, conoscenza condivisa, allineamento operativo e automazione, ovvero tutti gli elementi necessari per far crescere e scalare le tue prassi di sicurezza.

### SICUREZZA COMPLETA

Un portafoglio completo di **sicurezza per endpoint, autenticazione a più fattori e prodotti e servizi per la sicurezza della rete** pensati per proteggere ambienti, utenti e dispositivi.

### TRASPARENZA E CONTROLLO

Amministrazione della sicurezza centralizzata, visibilità e generazione avanzata di report grazie a **WatchGuard Cloud.**




### ALLINEAMENTO OPERATIVO

Operazioni aziendali semplificate grazie all'accesso diretto all'API, a un ecosistema ricco di **integrazioni** pronte all'uso e al supporto di tutti i modelli di pagamento e consumo tramite **FlexPay.**

### CONOSCENZA CONDIVISA

Una piattaforma completamente integrata per l'adozione di un modello di sicurezza zero-trust mediante il **Framework di identità** di WatchGuard e l'impiego di un approccio basato su XDR per il rilevamento e la correzione delle minacce tramite **ThreatSync®**.

### AUTOMAZIONE

**Automation Core® di WatchGuard** porta la semplificazione e la scalabilità in ogni aspetto del consumo, della fornitura e della gestione della sicurezza.

## Una piattaforma appositamente costruita per gli MSP

In qualità di MSP, devi assicurarti che le soluzioni del tuo fornitore di sicurezza siano innovative, strettamente integrate e in grado di soddisfare le variabili esigenze dei clienti, in particolare di coloro che dispongono di reti distribuite in tutto il mondo e che applicano politiche per il lavoro ibrido o da remoto. Inoltre, il fornitore dovrebbe disporre di solide capacità di supporto e garantire agli MSP di poter risolvere rapidamente eventuali problemi che si verificano durante l'erogazione del servizio.

Non solo WatchGuard mette l'XDR a portata di mano con ThreatSync, ma fornisce anche un'ampia gamma di servizi di sicurezza e funzionalità incentrate sugli MSP che possono aiutarti a semplificare e rafforzare le tue pratiche di sicurezza, ridurre i costi di gestione e aumentare la crescita dei ricavi.

### Scalabilità

WatchGuard offre un framework scalabile per supportare la crescita dei clienti e l'adozione del portafoglio.

### Usabilità

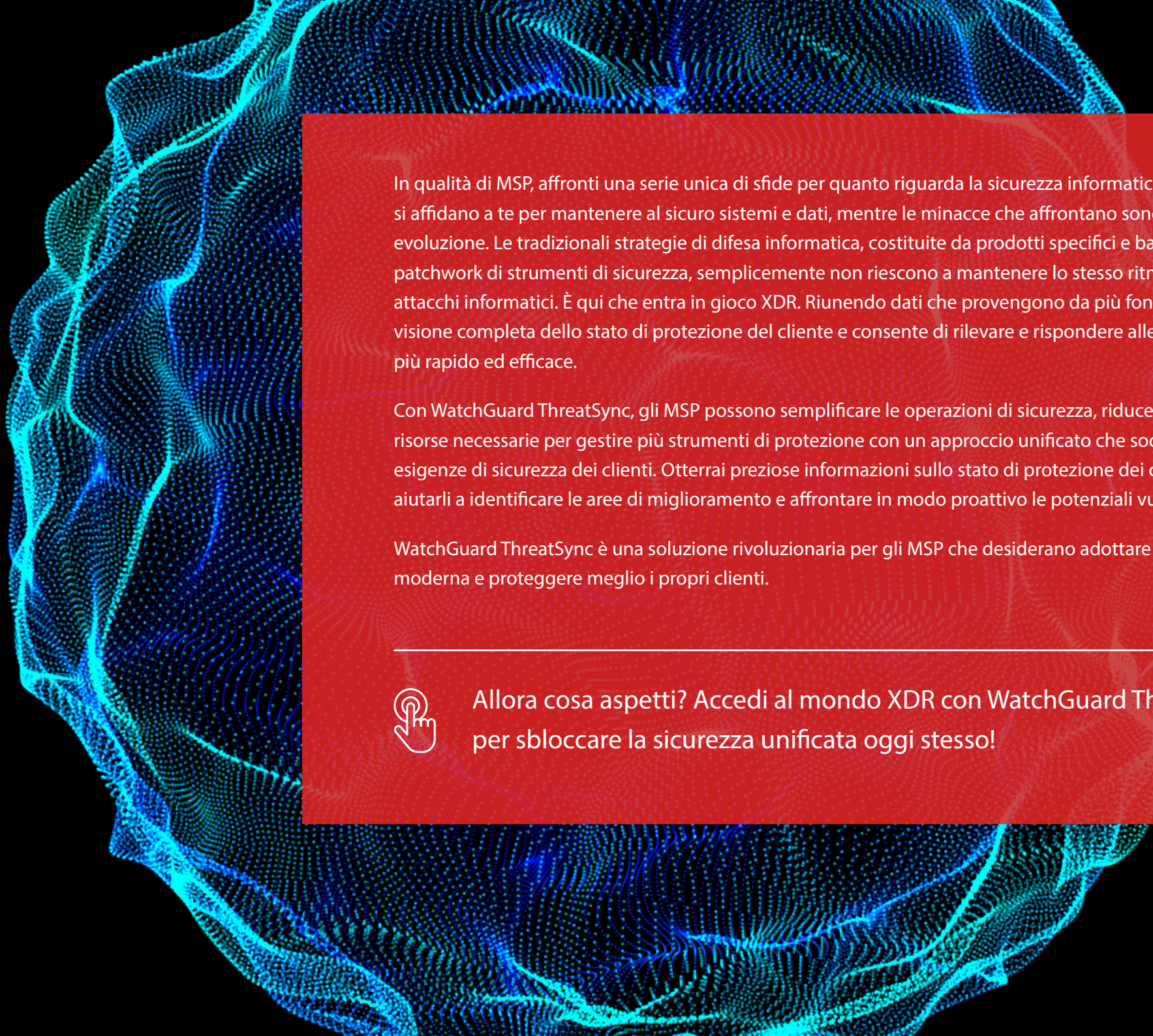
WatchGuard Cloud è facile da usare e gestire, con un'interfaccia intuitiva e dashboard chiari. ThreatSync fornisce i mezzi per identificare e rispondere alle minacce con rapidità.

### Integrazione

WatchGuard garantisce strette integrazioni in tutto lo stack di sicurezza. WatchGuard Cloud è facile da implementare e non interrompe i flussi di lavoro esistenti.

### Supporto

WatchGuard fornisce agli MSP un supporto e un servizio clienti di livello eccellente, con risposte tempestive alle richieste, nonché formazione e training continui sulle ultime tendenze e best practice in materia di sicurezza.



In qualità di MSP, affronti una serie unica di sfide per quanto riguarda la sicurezza informatica. I tuoi clienti si affidano a te per mantenere al sicuro sistemi e dati, mentre le minacce che affrontano sono in continua evoluzione. Le tradizionali strategie di difesa informatica, costituite da prodotti specifici e basate su un patchwork di strumenti di sicurezza, semplicemente non riescono a mantenere lo stesso ritmo dei moderni attacchi informatici. È qui che entra in gioco XDR. Riunendo dati che provengono da più fonti, XDR fornisce una visione completa dello stato di protezione del cliente e consente di rilevare e rispondere alle minacce in modo più rapido ed efficace.

Con WatchGuard ThreatSync, gli MSP possono semplificare le operazioni di sicurezza, riducendo il tempo e le risorse necessarie per gestire più strumenti di protezione con un approccio unificato che soddisfa meglio le esigenze di sicurezza dei clienti. Otterrai preziose informazioni sullo stato di protezione dei clienti, così potrai aiutarli a identificare le aree di miglioramento e affrontare in modo proattivo le potenziali vulnerabilità.

WatchGuard ThreatSync è una soluzione rivoluzionaria per gli MSP che desiderano adottare la sicurezza moderna e proteggere meglio i propri clienti.

---

Allora cosa aspetti? Accedi al mondo XDR con WatchGuard ThreatSync per sbloccare la sicurezza unificata oggi stesso!

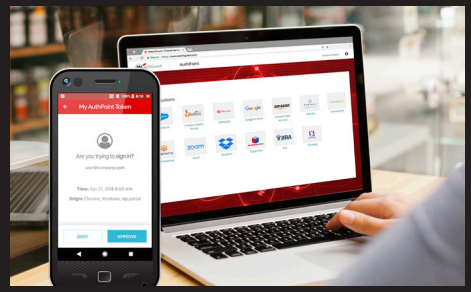
# Portafoglio prodotti WatchGuard

### 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, la nostra soluzione offre il vantaggio competitivo di cui le aziende hanno bisogno per il 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 le aziende di qualsiasi tipo di attacco informatico attuale e futuro. 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 **VENDITE INTERNAZIONALI** 1.206.613.0895 **WEB** www.watchguard.com/it