



# Sicurezza degli endpoint di WatchGuard

Protezione estendibile per prevenire, rilevare e rispondere alle minacce avanzate

L'endpoint è un obiettivo particolarmente apprezzato dai criminali informatici poiché offre numerose vulnerabilità da sfruttare e versioni software che sono spesso obsolete. Questi dispositivi sono frequentemente utilizzati in Internet senza la protezione offerta dalla sicurezza perimetrale aziendale e, peggio ancora, diventano il veicolo attraverso il quale i dipendenti possono inconsapevolmente consentire agli hacker di accedere a endpoint e reti aziendali. È passato il tempo in cui le aziende di tutte le dimensioni dovevano implementare una sicurezza degli endpoint potente che includesse la protezione degli endpoint (EPP) integrata con tecnologie avanzate di rilevamento e risposta degli endpoint (EDR).

La piattaforma WatchGuard Endpoint Security offre massima protezione e complessità minima, per una sicurezza degli endpoint impeccabile. I nostri prodotti e servizi di sicurezza incentrati sull'utente offrono approcci EPP e EDR avanzati con una suite completa di strumenti operativi e di sicurezza per proteggere le persone, i dispositivi e le reti a cui si connettono da siti web dannosi, malware, spam e altri attacchi mirati. Attraverso un'esclusiva combinazione di processi automatizzati e basati sull'IA e servizi di indagine condotti da analisti della sicurezza, i nostri prodotti WatchGuard EPDR e WatchGuard EDR forniscono funzionalità di ricerca delle minacce e classificazione di tutte le applicazioni, certificando la legittimità e la sicurezza di tutte le applicazioni in esecuzione, un'esigenza critica per qualsiasi azienda che implementi un modello di sicurezza Zero Trust.

## Buono o cattivo? Puoi scoprirlo con un margine di sicurezza del 100%

La maggior parte dei prodotti per la sicurezza degli endpoint blocca ciò che è noto come dannoso, indaga su ciò che è sospetto e consente ciò che non è noto, permettendo al malware che cambia rapidamente forma di eludere le difese con altro traffico sconosciuto. I prodotti WatchGuard EDR e WatchGuard EPDR, invece, sono dotati di un servizio applicativo Zero Trust che classifica il 100% degli eseguibili analizzando tutte applicazioni e i processi sospetti e sconosciuti tramite speciali algoritmi di apprendimento automatico nella nostra piattaforma cloud e persino effettuando una verifica con i nostri tecnici di laboratorio, quando necessario. Di conseguenza, tutti gli eseguibili vengono classificati in goodware o malware, affinché i clienti ricevano solo alert confermati e ricevano la massima protezione che deriva dalla posizione di negazione per impostazione predefinita di un modello Zero Trust.

## Trova le minacce nascoste senza aggiungere altro personale

La ricerca delle minacce di solito richiede una risorsa altamente qualificata e numerose ore di esecuzione prima che rilevi le minacce e restituisca le informazioni su come risolverle. Le nostre soluzioni EDR avanzate offrono un servizio di ricerca delle minacce nell'ambito del quale gli analisti della sicurezza effettuano il monitoraggio dell'ambiente degli endpoint del cliente e forniscono informazioni su potenziali attacchi in corso, tra cui analisi delle cause principali, anomalie rilevate, informazioni IT pertinenti e piani di riduzione delle potenziali superfici di attacco. Si tratta di una funzione standard che viene fornita con i nostri prodotti WatchGuard EDR e WatchGuard EPDR e che consente alle aziende di non dover allocare tempo e risorse del personale IT alle indagini sugli endpoint infetti.

## Gestione basata su cloud intuitiva

WatchGuard Cloud è una piattaforma particolarmente vantaggiosa per quelle aziende con personale IT limitato e poca competenza tecnica, proprio per la sua facilità di implementazione, configurazione e gestione dei prodotti per la sicurezza degli endpoint. Fornisce protezione e comunicazione con gli endpoint in tempo reale, inclusi il nostro motore di sicurezza e le firme, e funzionalità di filtro per URL che permettono agli utenti di inviare task e configurazioni a migliaia di computer in pochi secondi. Inoltre, WatchGuard Cloud permette di gestire l'intera gamma di servizi da un unico pannello di controllo, riducendo i costi dell'infrastruttura e il tempo dedicato alla creazione dei report e alle attività operative.

## Estensione delle funzionalità relative a sicurezza, visibilità e operazioni

Sono disponibili dei moduli opzionali con tutti i prodotti di sicurezza EPP ed EDR: Patch Management, per la gestione centralizzata di aggiornamenti e patch per sistemi operativi, applicazioni di terze parti e programmi software non supportati (EOL); Full Encryption, per crittografare e decrittografare le informazioni degli endpoint; Advanced Reporting Tool, per generare una security intelligence e identificare attacchi e comportamenti insoliti; Data Control, per individuare, classificare, verificare e monitorare dati personali non strutturati archiviati negli endpoint; SIEM Feeder, per creare una nuova fonte di informazioni preziose che monitora tutti i processi eseguiti nei dispositivi; infine, il nostro strumento RMM Systems Management per la gestione, il monitoraggio e la manutenzione dell'intera infrastruttura IT.

# Un pacchetto completo con opzioni flessibili per soddisfare ogni esigenza

## WatchGuard EDR e WatchGuard EPDR

- Fornisce una potente protezione di rilevamento e risposta degli endpoint (EDR) da attacchi zero day, ransomware, criptojacking e altri attacchi mirati avanzati che utilizzano modelli di intelligenza artificiale basati sull'apprendimento automatico e sul deep learning.
- Scegli tra le opzioni solo EDR (WatchGuard EDR) ed EPP + EDR (WatchGuard EPDR).

Ottieni una classificazione del 100% con il servizio applicativo Zero Trust, creando il tipo di risposta necessaria per l'implementazione di un modello Zero Trust.

Aumenta l'utilizzo e l'efficienza del personale con le informazioni fornite dal servizio di ricerca delle minacce.

- Implementa un approccio Defense-in-Depth nella sicurezza degli endpoint con WatchGuard EPDR, che include tutti i vantaggi della nostra soluzione WatchGuard per il rilevamento e la risposta degli endpoint e del prodotto Endpoint Protection in un unico pacchetto.

## WatchGuard EPP

- Protegge gli endpoint da virus, malware, spyware e phishing con firme, cache locale e persino i nostri feed di intelligence proprietari ottenuti dal malware precedentemente rilevato da WatchGuard EDR e WatchGuard EPDR.
- WatchGuard è pensato per le organizzazioni che devono gestire numerosi dispositivi di vario genere. WatchGuard EPP centralizza gli antivirus di nuova generazione di tutti i desktop, laptop e server per Windows, macOS e Linux, in aggiunta ai principali sistemi di virtualizzazione e ai dispositivi Android & iOS. La nostra soluzione ti consente di gestire a livello centrale la sicurezza e la riservatezza dei dati memorizzati su smartphone e tablet Android & iOS degli utenti.
- Trova gli exploit zero day utilizzando l'euristica comportamentale e gli indicatori noti degli attacchi come "regole contestuali".

## Moduli di sicurezza aggiuntivi

Aggiungi i moduli opzionali disponibili con tutti i prodotti di sicurezza EPP ed EDR:

### WatchGuard Patch Management

WatchGuard Patch Management è una soluzione per la gestione centralizzata di aggiornamenti e patch per sistemi operativi e per centinaia di applicazioni di terze parti e programmi software non supportati (EOL).

### WatchGuard Full Encryption

WatchGuard Full Encryption sfrutta la tecnologia BitLocker di Microsoft per crittografare e decrittografare le informazioni degli endpoint con una gestione centralizzata delle chiavi di ripristino fornite dalla nostra piattaforma di gestione basata su cloud.

**Estendi con altri moduli opzionali disponibili solo con i prodotti WatchGuard EPDR ed WatchGuard EDR:**

### WatchGuard Advanced Reporting Tool

WatchGuard Advanced Reporting Tool genera automaticamente la security intelligence oltre a fornire strumenti utili per identificare attacchi e comportamenti insoliti e per rilevare l'utilizzo interno inappropriato della rete aziendale.

### WatchGuard Data Control\*

WatchGuard Data Control\* rileva, classifica, verifica e monitora dati personali non strutturati memorizzati in endpoint e server nel corso del tuo intero ciclo di vita.

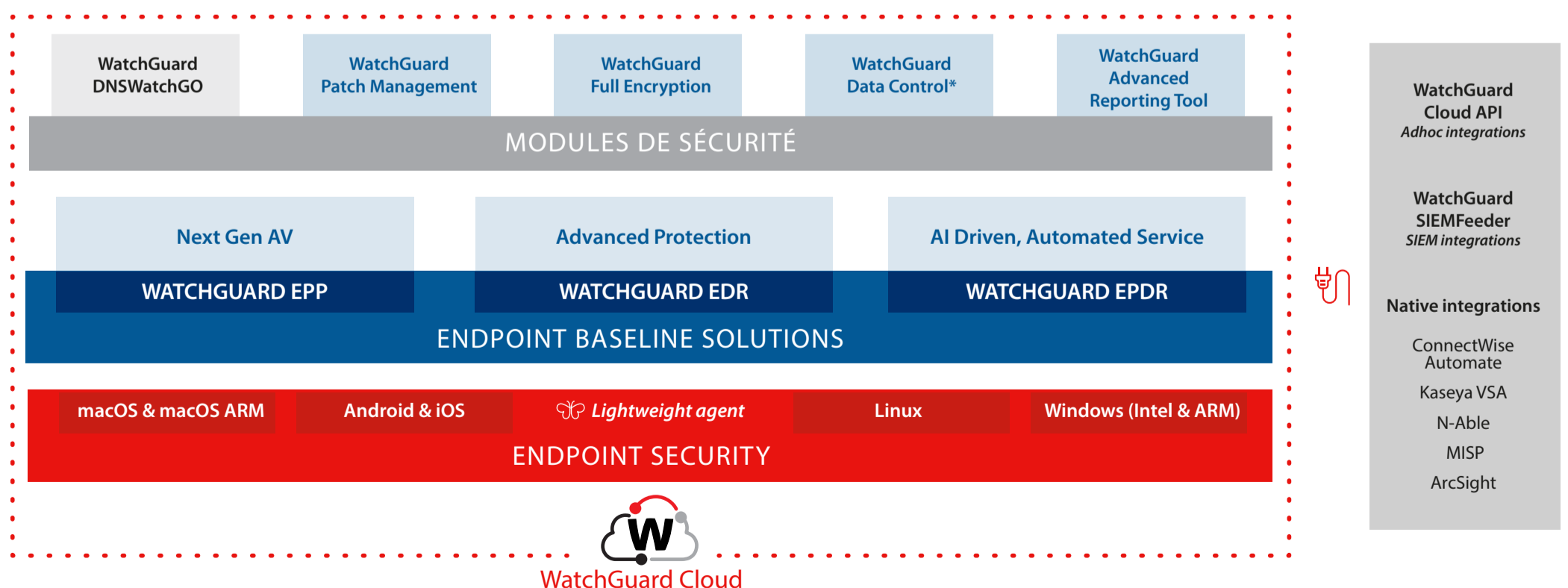
*\*Data Control è disponibile nei paesi seguenti: Spagna, Germania, Regno Unito, Svezia, Francia, Italia, Portogallo, Paesi Bassi, Finlandia, Danimarca, Svizzera, Norvegia, Austria, Belgio, Ungheria e Irlanda.*

### WatchGuard SIEMFeeder

WatchGuard SIEMFeeder integra una nuova fonte di informazioni preziose nella security intelligence di tutti i processi eseguiti nei dispositivi mentre vengono sottoposti a monitoraggio continuo.

### WatchGuard DNSWatchGO

WatchGuard DNSWatchGO fornisce protezione a livello di DNS e filtraggio dei contenuti per proteggere le aziende da phishing, ransomware e altri attacchi, anche quando gli utenti si trovano al di fuori della rete, senza richiedere una VPN.



## Motivi per aggiornare la sicurezza

### 1. Aggiunta di protezione per una forza lavoro distribuita man mano che l'azienda amplia le proprie policy per il telelavoro.

WatchGuard Passport include WatchGuard EPDR, WatchGuard DNSWatchGO e WatchGuard AuthPoint per l'autenticazione a più fattori. Queste soluzioni si combinano per proteggere gli utenti dalla più ampia gamma di minacce e, oltre a fornire sicurezza degli endpoint, proteggono le risorse aziendali dall'infiltrazione dovuta a perdita o furto delle credenziali dei dipendenti, un vettore di attacco utilizzato in alcuni dei più grandi casi di violazione resi note dalla stampa.



★ Soluzione consigliata: **WatchGuard Passport**

### 2. Esecuzione del ripristino dopo un attacco o dopo la scoperta di malware latente su endpoint o reti aziendali quando il malware ha avuto origine su un endpoint.

Le aziende che si trovano in questa posizione fanno due cose: innanzitutto, che sono certamente un obiettivo interessante per i criminali informatici e, in secondo luogo, che il loro attuale livello di protezione non è adeguato. Con l'evoluzione della protezione avanzata di WatchGuard EPDR rappresentata dal servizio applicativo Zero Trust e il servizio di ricerca delle minacce, il numero di attacchi basati su malware che il nostro team di supporto ha sottoposto a indagine/corretto ha avuto una tendenza quasi pari a zero e ciò significa che i nostri clienti non li stanno subendo. Se a questo si aggiungono gli strumenti di visibilità e di gestione che aumentano la produttività di un team IT operante di lavoro, si ottiene tutto ciò che serve per impedire attacchi ripetuti e costose correzioni.

★ Soluzione consigliata: **WatchGuard EPDR**

### 3. Aggiunta di EDR a una soluzione AV esistente come investimento di sicurezza pianificato.

Queste aziende comprendono i rischi per la sicurezza degli endpoint e hanno implementato un prodotto AV, ma si rendono conto di aver bisogno di una soluzione EDR per avere un margine di vantaggio sugli hacker. Non occorre attendere il rinnovo del contratto AV: la nostra soluzione WatchGuard EDR si aggiunge a un'implementazione AV esistente, in modo che i clienti possano usufruire rapidamente del nostro approccio avanzato e differenziato.

★ Soluzione consigliata: **WatchGuard EDR**

### 4. Aggiornamento da un prodotto AV per gli endpoint gratuito o di livello consumer.

A volte le piccole aziende o quelle con pochi dispositivi che attraversano il perimetro della rete puntano su un profilo di rischio ridotto e quindi rimandano gli investimenti in sicurezza. Tuttavia, il mondo sta cambiando e, man mano che le aziende diventano sempre più esposte e devono soddisfare normative più severe sulla sicurezza dei dati e sulla privacy, passano a una soluzione di livello aziendale come il prodotto WatchGuard EPP. Grazie alla solida prevenzione basata sulle firme, incluse le firme malware rilevate nella nostra base installata, nonché all'analisi comportamentale e al filtro dei contenuti web, WatchGuard EPP è una scelta intelligente a prova di futuro, poiché offre una piattaforma scalabile in base alla crescita del business.

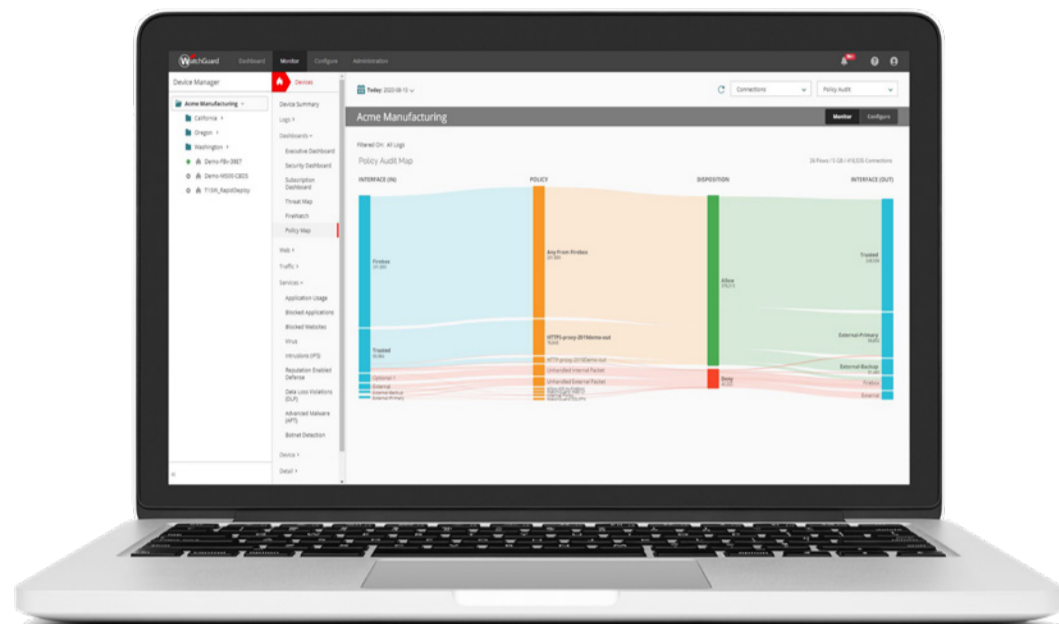
★ Soluzione consigliata: **WatchGuard EPP**



## WatchGuard Cloud



- Connettiti in tempo reale per implementare le attività in migliaia di dispositivi in pochi secondi
- Gestisci tutti i prodotti WatchGuard da una singola console
- Visualizza i dispositivi nelle varie piattaforme di endpoint tra cui Windows, Linux, macOS, iOS e Android



## PORTAFOGLIO WATCHGUARD



### Sicurezza di rete

Le soluzioni per la sicurezza di rete di WatchGuard sono progettate da zero per offrire 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 di livello enterprise e all'avanguardia a qualunque tipo di organizzazione, a prescindere dalle dimensioni o dalle competenze tecniche.



### Autenticazione a più fattori

WatchGuard AuthPoint® è la soluzione giusta per gestire le lacune della sicurezza basata su password con l'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 le persone autorizzate possano accedere a reti sensibili e applicazioni cloud.



### Secure Wi-Fi Cloud

La soluzione Secure Wi-Fi di WatchGuard, rivoluzionaria per il mercato di oggi, è progettata 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 soluzione offre il vantaggio competitivo di cui le aziende hanno bisogno per avere successo.



### Sicurezza degli endpoint

WatchGuard Endpoint Security è un portafoglio di avanzate soluzioni native per il cloud ideato per la sicurezza degli endpoint e 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.

## Scopri di più

Per maggiori dettagli, contatta un rivenditore WatchGuard autorizzato o visita il sito <https://www.watchguard.com/it>.

## Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella fornitura di servizi relativi a sicurezza di rete, sicurezza degli endpoint, Wi-Fi protetto, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi della nostra azienda hanno ottenuto la fiducia di oltre 18.000 rivenditori e fornitori di servizi che provvedono alla sicurezza di più di 250.000 clienti. WatchGuard persegue la missione di rendere la sicurezza accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, diventando in tal modo la soluzione ideale per le aziende del midmarket e distribuite. La sede centrale di WatchGuard si trova a Seattle (Washington, Stati Uniti); l'azienda dispone di uffici dislocati in Nord America, Europa, Asia e America Latina. Per saperne di più, visita [WatchGuard.com](https://www.watchguard.com).