DATASHEET

WATCHGUARD EDR

Endpoint Detection and Response

DIFESA INFORMATICA DALLE MINACCE AVANZATE

Gli attacchi informatici più all'avanguardia sono progettati per aggirare la protezione fornita dalle soluzioni di sicurezza tradizionali. Sono sempre più frequenti e sofisticati per via delle competenze professionali acquisite nel tempo dagli hacker e sono anche il risultato di una mancata correzione delle vulnerabilità di sicurezza nei sistemi.

Alla luce di questa situazione, le piattaforme di protezione tradizionali (EPP) non forniscono una visibilità abbastanza dettagliata dei processi e delle applicazioni in esecuzione nelle reti aziendali. Inoltre, invece di risolvere i problemi alcune soluzioni EDR creano ulteriore stress e aumentano il carico di lavoro degli amministratori della sicurezza, trasferendo su di essi la responsabilità di gestire gli alert e obbligandoli a classificare manualmente le minacce.

EDR AUTOMATIZZATO PER UNA SICUREZZA ANCORA MAGGIORE

WatchGuard EDR è una soluzione innovativa per la sicurezza informatica pensata per computer, laptop e server basata su cloud che automatizza la prevenzione, il rilevamento, il contenimento e la risposta a qualsiasi minaccia avanzata, dal malware zero day al ransomware, fino ai tentativi di phishing e agli exploit in memoria, compresi gli attacchi malwareless, sia attuali che futuri e sia all'interno che all'esterno della rete.

WatchGuard EDR è stato studiato per fornire una visibilità completa degli endpoint tramite il monitoraggio e il rilevamento delle attività malevole che eludono le soluzioni di protezione tradizionali. Viene installato in aggiunta alle soluzioni antivirus esistenti per completarle con un'intera serie di funzionalità EDR automatizzate, tra cui:

- **Servizio Zero Trust Application: Classificazione al 100% delle applicazioni**
- **Servizio di ricerca delle minacce: rilevamento di hacker e utenti interni malevoli**

WatchGuard EDR fornisce i mezzi per combattere efficacemente le minacce e rispondere agli attacchi malevoli grazie alle seguenti tecnologie di sicurezza avanzate:

- Monitoraggio continuo degli endpoint con EDR
- Apprendimento automatico basato su cloud che classifica il 100% dei processi (APT, ransomware, rootkit, ecc.)
- Sandboxing in ambienti reali
- Protezione anti-exploit
- Funzionalità di ricerca delle minacce, incluse analisi comportamentale e rilevamento degli IOA (indicatori di attacco) per individuare gli attacchi di tipo "living-off-the-land" (LotL)
- Indicatori di attacco mappati nel framework MITRE ATT&CK
- Rilevamento e prevenzione degli attacchi RDP
- Capacità di contenimento e correzione come isolamento dei computer e blocco del programma tramite hash o nome
- Recupero dei file crittografati mediante le copie shadow

VANTAGGI

Semplifica e riduce al minimo i costi per la sicurezza

- I servizi gestiti riducono i costi del personale esperto. Non sono presenti falsi alert da gestire e non viene delegata alcuna responsabilità.
- Consente di gestire gli endpoint multipiattaforma da un unico pannello di controllo.
- L'agente leggero e l'architettura nativa per il cloud non influiscono negativamente sulle prestazioni degli endpoint.

Automatizza e riduce il tempo di rilevamento

- Le applicazioni che rappresentano un rischio per la sicurezza possono essere bloccate (tramite hash o nome).
- Blocca l'esecuzione di minacce, malware di tipo zero day, attacchi fileless/malwareless, ransomware e tentativi di phishing.
- Rileva e blocca tecniche, tattiche e procedure di intrusione.

Automatizza e riduce il tempo di risposta e indagine

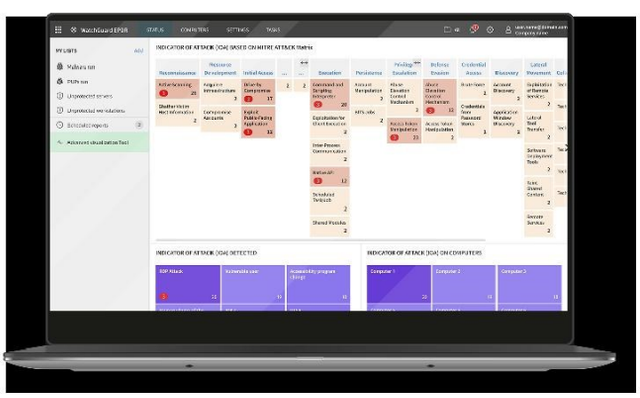
- Risoluzione e risposta: analisi forense per indagare a fondo su ogni tentativo di attacco e strumenti per mitigarne gli effetti (disinfezione).
- Tracciabilità di tutte le azioni: visibilità pratica dell'aggressore e delle sue attività. Indagini avanzate degli indicatori di attacco (IoA).
- Miglioramenti e correzioni delle policy di sicurezza a seguito delle conclusioni dell'analisi forense.

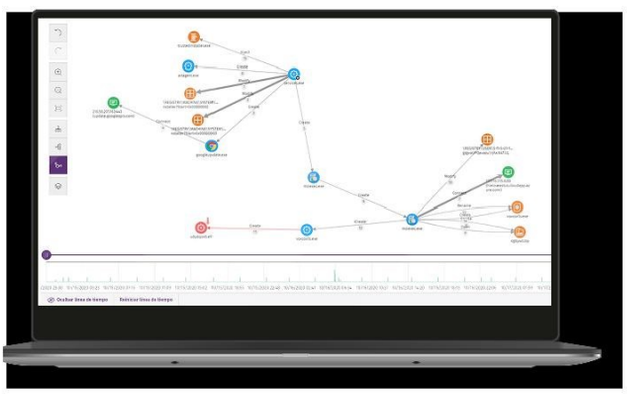
SERVIZIO DI RICERCA DELLE MINACCE E ZERO TRUST

La piattaforma per la sicurezza degli endpoint di WatchGuard non si basa su una sola tecnologia, ma ne implementa diverse per ridurre le possibilità di successo degli autori di minacce. Queste tecnologie lavorano in sinergia e utilizzano le risorse dell'endpoint per minimizzare il rischio di violazione.

Il **servizio Zero Trust Application** classifica il 100% dei processi, monitora l'attività degli endpoint e blocca l'esecuzione delle applicazioni e dei processi malevoli. Ogni esecuzione viene classificata in tempo reale come malevola o legittima senza incertezze e senza delegare la decisione al client ed evitando i processi manuali, grazie alla capacità, alla velocità, all'adattabilità e alla scalabilità dell'intelligenza artificiale e dell'elaborazione cloud.

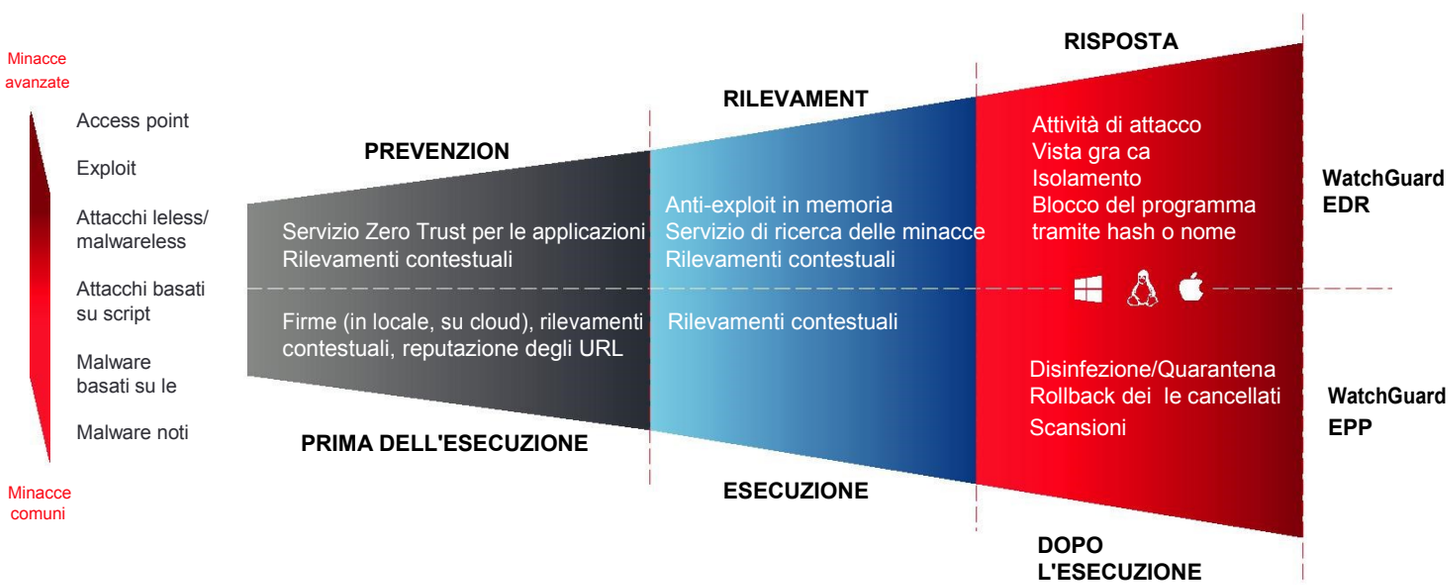
Il servizio integra le tecnologie dei big data e le tecniche di apprendimento automatico multilivello, compreso il deep learning, i risultati della supervisione continua e l'automazione dell'esperienza e delle conoscenze accumulate dal team addetto alle minacce di WatchGuard.





Il **servizio di ricerca delle minacce** si basa su una serie di regole create da esperti di sicurezza informatica che vengono eseguite automaticamente a fronte di tutti i dati raccolti dalla telemetria, attivando indicatori di attacco estremamente attendibili e con un basso indice di falsi positivi, in modo da ridurre al minimo i tempi medi di rilevamento e risposta (Mean Time To Detect, MTTD e Mean Time To Respond, MTTR).

Gli indicatori di attacco sono il risultato di un processo continuo volto a identificare gli autori delle minacce grazie all'analisi avanzata dei dati, alla nostra tecnologia proprietaria di intelligence sulle minacce e alla competenza dei nostri analisti. Gli addetti alla ricerca delle minacce di WatchGuard lavorano partendo dal presupposto che le aziende siano costantemente compromesse.



Piattaforme supportate e requisiti di sistema di WatchGuard EDR

Sistemi operativi supportati: Windows (Intel e ARM), macOS (Intel e ARM) e Linux.

Supporto per sistemi legacy a partire da Windows XP SP3 e Server 2003.

Le funzionalità EDR sono disponibili in Windows, macOS e Linux; Windows è la piattaforma che ne garantisce la piena operatività.

Elenco dei browser compatibili: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

Per informazioni contatta SOPHIANET SRL – commerciale@sophia