DATASHEET

WATCHGUARD EPP

Potente piattaforma di protezione degli endpoint

SFIDE DELLA SICUREZZA INFORMATICA

Nella continua battaglia per la difesa della tua organizzazione, l'endpoint è uno dei bersagli preferiti dei criminali informatici. Questo significa che è più importante che mai proteggere e monitorare tutti gli endpoint che gestiscono informazioni sensibili e si connettono a sistemi sia all'interno che all'esterno della rete aziendale.

Di fatto, lo scorso anno sono stati registrati più di 350.000 nuovi programmi dannosi al giorno. Gli hacker prendono di mira gli endpoint vulnerabili, in cui le aziende archiviano le loro risorse più preziose. Il motivo? Il ritorno economico, naturalmente. Il malware e il ransomware sono le minacce più frequenti, per quanto, paradossalmente, il problema principale non sia costituito dai costi diretti ma piuttosto dal tempo di inattività causato da tali minacce. Questa situazione obbliga le aziende ad adottare misure di rafforzamento della protezione.

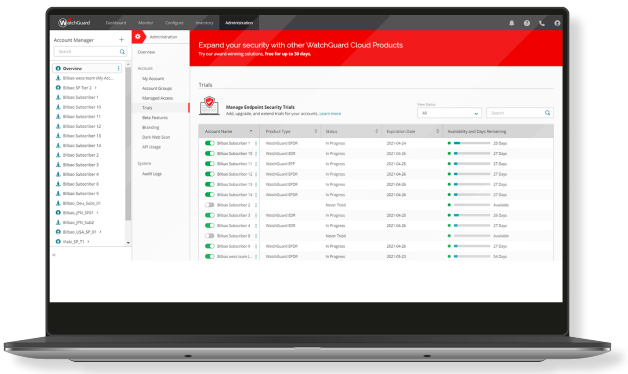
PROTEZIONE DELL'AZIENDA DA MALWARE E RANSOMWARE

La crescente esposizione delle aziende a nuovi tipi di malware e minacce ne compromette i livelli di protezione e richiede nuovi approcci per ridurre l'impatto dei possibili attacchi.

WatchGuard EPP è un'efficace soluzione di sicurezza nativa per il cloud che centralizza l'antivirus di nuova generazione per tutti i desktop, laptop e server per Windows, macOS e Linux, in aggiunta ai principali sistemi di virtualizzazione e dispositivi Android. Questa protezione completa copre tutti i vettori: rete (firewall), e-mail, Web e dispositivi esterni,

e include una serie di tecnologie EPP per prevenire malware, ransomware e le minacce più recenti. Una di queste tecnologie consulta in tempo reale l'intelligence sulle minacce di WatchGuard, un enorme repository basato sui più recenti algoritmi di apprendimento automatico, per rilevare più rapidamente gli attacchi dannosi.

Inoltre, non richiede hardware e software. Il suo agente a basso impatto non incide sulle prestazioni degli endpoint, semplifica la gestione della sicurezza e aumenta l'efficienza operativa.



VANTAGGI

Sicurezza multipiattaforma

- Sicurezza rispetto a minacce avanzate sconosciute: rilevamento e blocco di malware, trojan, phishing e ransomware.
- Sicurezza per tutti i vettori di attacco: browser, e-mail, file system e dispositivi esterni collegati agli endpoint.
- Analisi e disinfezione automatiche dei computer.
- Analisi del comportamento per rilevare malware noto e sconosciuto.
- Sicurezza tra piattaforme: sistemi Windows, Linux, macOS, Android e ambienti virtuali (VMware, Virtual PC, MS Hyper-V, Citrix). Gestione di licenze appartenenti a infrastrutture di virtualizzazione (VDI) sia persistenti che non persistenti.

Gestione semplificata

- Facilità di gestione: non è necessaria alcuna infrastruttura specifica per l'hosting della soluzione; il reparto IT può concentrarsi su attività più importanti.
- Facilità di protezione degli utenti remoti: ogni computer protetto con WatchGuard EPP comunica con il cloud. Gli uffici e gli utenti remoti vengono protetti rapidamente e con facilità, senza installazioni aggiuntive.
- Facilità di distribuzione: più metodi di distribuzione, con programmi di disinstallazione automatici per i prodotti della concorrenza allo scopo di facilitare la migrazione da soluzioni di altri fornitori.
- Curva di apprendimento agevole: l'interfaccia di gestione basata sul Web è semplice e intuitiva, con opzioni di uso frequente attivabili con un solo clic.

Basso impatto sulle prestazioni

- L'agente richiede un utilizzo minimo di rete, memoria e CPU, poiché tutte le operazioni vengono eseguite sul cloud.
- WatchGuard EPP non richiede installazione, gestione o manutenzione di nuove risorse hardware nell'infrastruttura dell'organizzazione.

SICUREZZA CENTRALIZZATA DEI DISPOSITIVI

Gestione centralizzata della sicurezza e degli aggiornamenti del prodotto per tutte le workstation e i server della rete aziendale. È possibile gestire la protezione dei dispositivi con Windows, Linux, macOS e Android da un'unica console di amministrazione basata sul Web.

PROTEZIONE DA MALWARE E RANSOMWARE

WatchGuard EPP analizza i comportamenti e le tecniche di intrusione per rilevare e bloccare malware noto e sconosciuto, nonché ransomware, trojan e phishing.

DISINFEZIONE AVANZATA

Nell'eventualità di una violazione della sicurezza, WatchGuard EPP consente alle aziende di ripristinare lo stato precedente all'aggressione per i computer interessati con strumenti avanzati di disinfezione e con la quarantena, dove vengono archiviati gli elementi sospetti e quelli eliminati.

Consente inoltre agli amministratori di riavviare da remoto le workstation e i server per assicurarsi che vi siano installati gli aggiornamenti più recenti.

MONITORAGGIO IN TEMPO REALE E REPORT

I dashboard completi e alcuni grafici intuitivi assicurano un monitoraggio dettagliato della sicurezza in tempo reale.

I report generati automaticamente segnalano lo stato della protezione, i rilevamenti eseguiti e l'uso scorretto dei dispositivi.

CONFIGURAZIONE DETTAGLIATA DEI PROFILI

È possibile assegnare specifiche policy di protezione in base a profili utente, garantendo a ogni gruppo di utenti l'applicazione della policy più appropriata.

CONTROLLO CENTRALIZZATO DEI DISPOSITIVI

È possibile fermare il malware e la fuga di informazioni bloccando intere categorie di dispositivi (unità flash, modem USB, webcam, DVD/CD, ecc.), inserendo i dispositivi consentiti in appositi elenchi o configurando autorizzazioni di accesso in sola lettura, sola scrittura e lettura-scrittura.

INSTALLAZIONE VELOCE E FLESSIBILE

La distribuzione della protezione può avvenire via e-mail tramite un URL per il download oppure automaticamente in endpoint selezionati tramite lo strumento di distribuzione della soluzione. Il programma di installazione MSI è compatibile con strumenti di altri fornitori (Active Directory, Tivoli, SMS e così via)

MALWARE FREEZER

Malware Freezer mette in quarantena per sette giorni il malware rilevato e, nell'eventualità di un falso positivo, ripristina automaticamente il file interessato nel sistema.

CONFORMITÀ ISO 27001 E SAS 70 GARANTITA 24/7

La soluzione risiede su WatchGuard Cloud con protezione dei dati completa garantita. I nostri data center sono dotati di certificazione ISO 27001 e SAS 70, pertanto i clienti non subiscono costose interruzioni del servizio e infezioni da malware.

Piattaforme supportate e requisiti di sistema di WatchGuard EPP

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

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

WATCHGUARD UNIFIED SECURITY PLATFORM™


Sicurezza di rete


Wi-Fi protetto


Autenticazione a più fattori


Sicurezza degli endpoint

Per saperne di più, contatta il tuo rivenditore WatchGuard autorizzato o visita il sito **www.watchguard.it**

Numero verde Italia: 800.911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 WEB: www.watchguard.com/it/ WatchGuard Technologies, Inc.

Cod. articolo WGCE67474_051121