DATASHEET

HOST SENSOR

Complemento del Threat Detection and Response per il monitoraggio e la correzione degli endpoint

Con il progressivo evolversi delle minacce, diventa sempre più importante proteggere ogni vettore di attacco, dalla rete fino all'endpoint. Threat Detection and Response (TDR), incluso nella Total Security Suite di WatchGuard, correla gli eventi di sicurezza della rete e degli endpoint con l'intelligence sulle minacce per individuare, classificare e consentire un'azione immediata con cui fermare gli attacchi malware. La visibilità sulla rete viene fornita dall'appliance WatchGuard Firebox®, mentre i dati sugli eventi degli endpoint vengono acquisiti attraverso WatchGuard Host Sensor.

WatchGuard Host Sensor rileva costantemente le minacce sull'endpoint, ricevendo ed eseguendo i comandi di risposta. Host Ransomware Prevention (HRP), una funzione di WatchGuard Host Sensor, in abbinamento alla protezione dal malware avanzato fornita da APT Blocker, consente di ottenere una prevenzione leader di settore contro gli attacchi mediante ransomware. Host Ransomware Prevention blocca l'esecuzione del ransomware prima che venga eseguita la crittografia dei file sull'endpoint, mitigando l'attacco ransomware prima che si verifichino danni.

ESTENDERE LA VISIBILITÀ AGLI ENDPOINT

Il componente a basso impatto WatchGuard Host Sensor monitora e rileva le attività delle minacce sui dispositivi utilizzando l'euristica e le analisi comportamentali. Host Sensor invia continuamente questi eventi a ThreatSync di TDR per consentirne la correlazione agli eventi registrati dall'appliance Firebox, permettendo di definire le priorità in base alla gravità complessiva delle minacce.

CORREZIONE AUTOMATICA DELLE MINACCE

WatchGuard Host Sensor consente agli utenti di automatizzare la correzione delle minacce mediante la creazione di policy. In base al punteggio globale delle minacce generato da ThreatSync, le policy definite in precedenza determinano le tattiche di risposta da attivare, compresa la terminazione del processo, la messa in quarantena del file e l'eliminazione del valore del registro di sistema. La correzione automatica delle minacce non solo è in grado di diminuire il tempo necessario alla correzione del problema, ma permette anche di ridurre al minimo l'utilizzo di risorse preziose.

PREVENZIONE AVANZATA DEL RANSOMWARE

Host Ransomware Prevention è un modulo specifico per il ransomware all'interno di WatchGuard Host Sensor. HRP sfrutta un motore di analisi comportamentale e un honeypot di directory esca per monitorare una vasta gamma di caratteristiche che determinano se una data azione è associata o meno a un attacco ransomware. Se la minaccia è potenzialmente dannosa, HRP può impedire automaticamente un attacco ransomware prima che venga effettuata la crittografia dei file.

TRIAGE DELLE MINACCE AVANZATE CON APT BLOCKER

Il malware è in costante evoluzione e alcuni indicatori sospetti possono rappresentare un segno premonitore dell'arrivo di malware ancora non identificato. Ora, grazie alla perfetta integrazione con WatchGuard APT Blocker, WatchGuard Host Sensor può inviare automaticamente i file sospetti a una sandbox di prossima generazione nel cloud per un'analisi approfondita e la riassegnazione del punteggio.

CARATTERISTICHE E VANTAGGI

- Monitoraggio e rilevamento continui degli eventi relativi alle minacce sugli endpoint
- Riduzione dei tempi di rilevamento e correzione grazie all'automazione
- Miglioramento della prevenzione degli attacchi con malware avanzato, compreso il ransomware
- Le policy definite preventivamente vengono eseguite in automatico per terminare il processo, mettere in quarantena i file o eliminare il valore del registro di sistema
- Il software agent a basso impatto utilizza una quantità minima di risorse di elaborazione
- Funziona in abbinamento ad altre soluzioni antivirus già installate

Licenze di Host Sensor

Con un abbonamento a Total Security Suite, ogni appliance comprende un numero fisso di Host Sensor. Gli Host Sensor vengono gestiti e distribuiti all'interno di Threat Detection and Response, dove vengono aggregati per l'uso nell'intero account. Per soddisfare le esigenze aziendali, sono disponibili Host Sensor aggiuntivi attraverso l'offerta di opzioni aggiuntive.

Firebox Model	Included Host Sensors
T15	5
T35	20
T55	35
T70 / M200	60
M370	150
M470	200
M440 / M570 / 670/M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	150
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

Host Sensor Add-On Options
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors
1000 Host Sensors
2500 Host Sensors
5000 Host Sensors

SPECIFICHE DI HOST SENSOR:

Sistemi operativi compatibili

- Windows 7, 8, 8.1, 10
- Windows Server 2003, 2008, 2012
- Linux RedHat/CentOS 6, 7

Compatibile con appliance Firebox T Series, M Series e XTMv.

Servizi di sicurezza WatchGuard

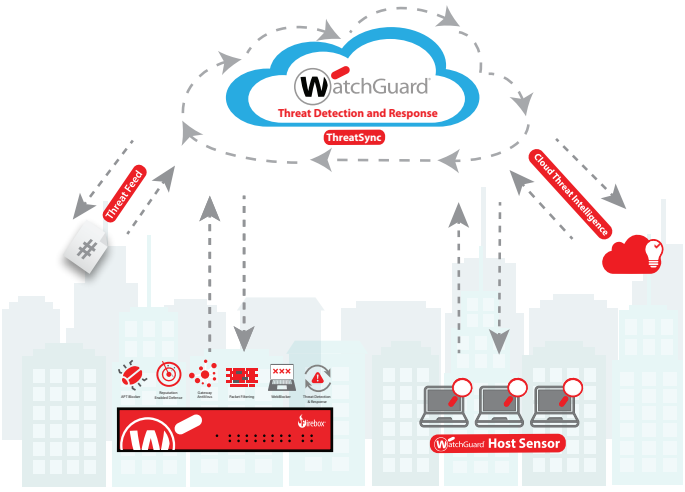
Una sola appliance, un solo pacchetto, sicurezza totale

I clienti traggono il massimo beneficio da difese di sicurezza che funzionano in modo abbinato, offrendo la protezione più efficace, la massima efficienza e prestazioni estremamente elevate. La Total Security Suite di WatchGuard fornisce ai clienti servizi di sicurezza di rete di tipo tradizionale, affiancati da soluzioni di sicurezza avanzate che comprendono APT Blocker, Data Loss Prevention e Threat Detection and Response (TDR).

TDR porta questa filosofia su un piano più elevato, correlando i dati sugli eventi provenienti dai feed della rete, degli endpoint e dell'intelligence sulle minacce per assegnare un punteggio completo alle minacce e classificarle. ThreatSync, il nostro motore di correlazione e classificazione delle minacce, acquisisce gli input dal servizio di sicurezza di rete avanzata, comprendente WebBlocker, APT Blocker, Gateway Antivirus e spamBlocker. Effettua quindi la correlazione di questi dati di rete con i dati sugli eventi degli endpoint acquisiti mediante WatchGuard Host Sensor per generare un punteggio e una classificazione delle minacce in base alla loro gravità.

Con WatchGuard Total Security Suite, le organizzazioni possono usufruire di una sicurezza di rete avanzata, di solide funzioni di visibilità e correzione sugli endpoint e di intelligence sulle minacce di livello enterprise attraverso un'unica soluzione completa.

Funzioni e servizi	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway Antivirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
Access Portal	✓	
Dimension Command	✓	
Supporto	Gold (24x7)	Standard (24x7)



WatchGuard dispone della rete di rivenditori e fornitori di servizi a valore aggiunto più estesa del settore. Consulta la nostra rete di partner certificati su **findpartner.watchguard.com.Ulteriori informazioni su Threat Detection and Response con WatchGuard Host Sensor sono disponibili su watchguard.com/TDR.**

Numero Verde Italia: 800.911.938 EMAIL: italy@watchguard.com

www.watchguard.it