DATASHEET

# THREAT DETECTION & RESPONSE

*Bloccate il malware avanzato con la sicurezza correlata*

Il malware progettato dagli hacker sta diventando sempre più sofisticato. Attraverso tecniche come la creazione di pacchetti, la crittografia e il polimorfismo, i criminali informatici sono in grado di celare i loro attacchi per eludere il rilevamento. Gli attacchi zero-day e il malware avanzato sfuggono facilmente alle soluzioni antivirus, troppo lente per rispondere al flusso costante di minacce emergenti. Organizzazioni di tutte le dimensioni sono alla ricerca di una soluzione che sfrutti un approccio olistico alla sicurezza, a partire dalla rete fino ad arrivare agli endpoint. WatchGuard Threat Detection and Response (TDR) è una potente suite di strumenti di difesa dal malware avanzato che esegue la correlazione degli indicatori delle minacce generati dalle appliance Firebox e dagli Host Sensors per bloccare le minacce malware note, sconosciute ed elusive.

*"Le funzioni di rilevamento correlato e risposta automatica aggiungono un livello mancante alla nostra struttura di sicurezza e ci permettono di rilevare immediatamente le infezioni, impedendo loro di diffondersi nella rete."*

*~ Andre Bromes, SVP e CIO/CISO di Goodwill New York / New Jersey*

## CORRELAZIONE E ASSEGNAZIONE DI PRIORITÀ

ThreatSync è un motore di correlazione basato su cloud che analizza i dati sugli eventi provenienti dagli Host Sensor e dalle appliance Firebox per identificare i comportamenti dannosi.
Le minacce vengono classificate in base alla gravità per gestire le azioni di correzione.

## VISIBILITÀ DELLE MINACCE NELL'ENDOPOINT

L'Host Sensor a basso impatto di WatchGuard estende la visibilità e la gestione delle minacce fino all'endpoint. Invia continuamente dati euristici e comportamentali dall'endpoint a ThreatSync per eseguire correlazione e classificazione. Gli Host Sensor sono gestiti centralmente dal cloud, agevolando agli MSSP (fornitori di servizi di sicurezza gestiti) e agli amministratori IT le operazioni di implementazione, aggiornamento e gestione degli Host Sensor in tutto il mondo.

## RISPOSTA AUTOMATICA

TDR offre una potente protezione contro le minacce malware avanzate e può intervenire automaticamente sui file in quarantena, interrompere processi ed eliminare le chiavi di registro. Mitigate le minacce non appena le individuate con un semplice clic o definendo delle policy per la risposta automatica in base al punteggio assegnato alla minaccia.

## EMAIL DI AVVISI E NOTIFICHE CON THREATSYNC

WatchGuard ThreatSync ora consente di configurare notifiche email personalizzate su indicatori di minacce, incidenti e rimedi che si verificano sulla rete e sugli endpoint. Senza dover accedere al dashboard, puoi restare sempre aggiornato sulla sicurezza dei tuoi sistemi, ovunque ti trovi.

## PREVENZIONE RANSOMWARE CON HRP

Host Ransomware Prevention (HRP) è un modulo specifico per il ransomware all'interno di TDR che utilizza analisi comportamentali e honeypot per individuare segni di ransomware. Se viene rilevato del malware, HRP interviene automaticamente per bloccare il ransomware prima che i file vengano danneggiati definitivamente.

## 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, i file sospetti possono essere inviati a una sandbox di prossima generazione nel cloud per un'analisi approfondita e la riassegnazione del punteggio.

## INTELLIGENCE SULLE MINACCE DI LIVELLO ENTERPRISE

In passato, l'intelligence sulle minacce era un privilegio riservato alle grandi aziende dotate di ampi budget e team di sicurezza molto estesi. Con Threat Detection and Response, WatchGuard aggrega e analizza i feed dell'intelligence sulle minacce, fornendo ai propri clienti i benefici in termini di sicurezza ed evitando la complessità e i costi associati.

DATASHEET

# Rilevamento più intelligente grazie alla correlazione

Gli attacchi con malware avanzato sono complessi e agiscono su più livelli. In genere, gli endpoint si infettano quando un utente cade vittima di una campagna di phishing o fa clic su un collegamento dannoso che dà inizio al processo di infezione. Una volta scatenatosi l'attacco, il malware può tentare di raggiungere un server di controllo e comando per ricevere ulteriori istruzioni. Il malware può anche cercare di diffondersi in altri punti dell'organizzazione attraverso la rete.

Anche se può sembrare che il malware in se stesso abbia caratteristiche assolutamente peculiari, i comportamenti che facilitano il diffondersi dell'attacco attraverso la rete seguono schemi comuni e prevedibili. Se le soluzioni di sicurezza lavorano "in silos", la rete non potrà in alcun modo sapere cosa accade nell'endpoint e viceversa e questo crea un'enorme vulnerabilità a questa pericolosa minaccia. Per questo motivo, l'analisi congiunta dei comportamenti in rete e negli endpoint rappresenta un potente strumento per identificare e bloccare tipi di malware sconosciuti. Con Threat Detection and Response tutto questo è possibile.

I dati sugli eventi provenienti dai servizi di sicurezza sulle appliance Firebox di WatchGuard, come APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus e WebBlocker, vengono inviati a ThreatSync, che li associa ai dati degli endpoint raccolti da Host Sensor. ThreatSync quindi analizza questi dati sulle minacce per assegnare un punteggio dettagliato alle minacce e classificarle in base alla gravità complessiva. Gli eventi identificati sia sulla rete che sull'endpoint ricevono automaticamente il punteggio più elevato (10) per una minaccia.

Con le policy attivate, ThreatSync ordina automaticamente a Firebox di impedire al malware di contattare il server dannoso e disporre la quarantena dei file, l'interruzione di processi o l'eliminazione della persistenza nei valori di registro di sistema a livello di endpoint. Queste operazioni possono essere eseguite anche manualmente grazie alla nostra procedura di correzione guidata in un clic.

| 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 |

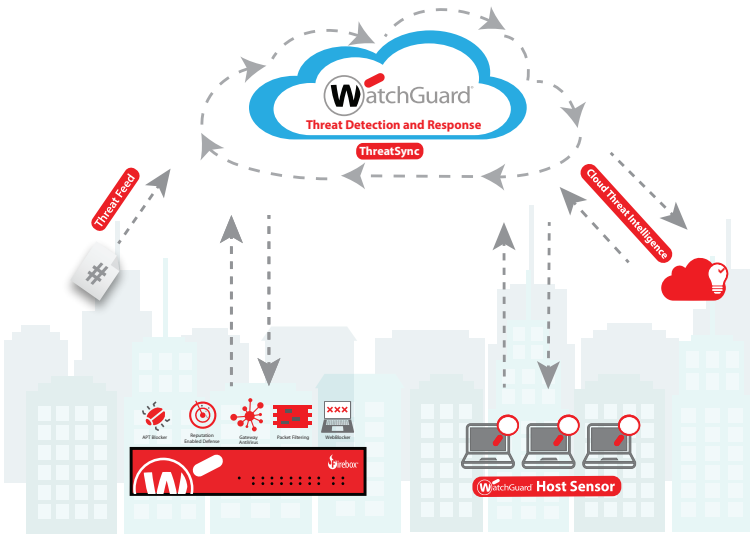
## SPECIFICHE DI HOST SENSOR:

### Sistemi operativi compatibili

- Windows 7, 8, 8.1, 10
- Windows Server 2008, 2012, 2016
- Linux RedHat/CentOS 6, 7

Compatibile con Firebox T Series, M Series, Firebox Cloud e FireboxV.

| 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 | ✓ | |
| DNSWatch | ✓ | |
| 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 nella pagina **watchguard.com/TDR.**

Numero verde Italia: 800-911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 WEB: www.watchguard.it