Threat Detection & Response

Correlare. Classificare. Reagire.

I criminali informatici sferrano attacchi sempre più complessi e sofisticati, utilizzando sistemi coordinati per accedere alla tua rete da ogni tipo di connessione. Le misure di sicurezza devono tenere il passo aggiungendo funzionalità di rilevamento su reti ed endpoint e correlando questa attività sugli eventi traducendola in azioni mirate. Il servizio Threat Detection and Response (TDR, rilevamento e risposta alle minacce) di WatchGuard correla gli eventi di sicurezza della rete e degli endpoint con intelligence sulle minacce per individuare, classificare e consentire un'azione immediata con cui fermare gli attacchi malware. TDR consente alle piccole e medie imprese e agli MSSP che le supportano di porre rimedio in tutta sicurezza agli attacchi con malware avanzato prima che i dati business-critical o la produttività organizzativa risultino compromessi.

Correlazione degli eventi della rete e degli endpoint

ThreatSync è il nuovo motore WatchGuard basato su cloud per la correlazione e la classificazione delle minacce; consente di migliorare la consapevolezza in merito alla sicurezza e la reazione in tutta la rete fino agli endpoint. ThreatSync acquisisce i dati sugli eventi provenienti da WatchGuard Firebox, da WatchGuard Host Sensor e dai feed di intelligence sulle minacce basati su cloud, e correla questi dati per generare un punteggio globale delle minacce su cui basare le azioni di correzione.

Estendere la visibilità agli endpoint

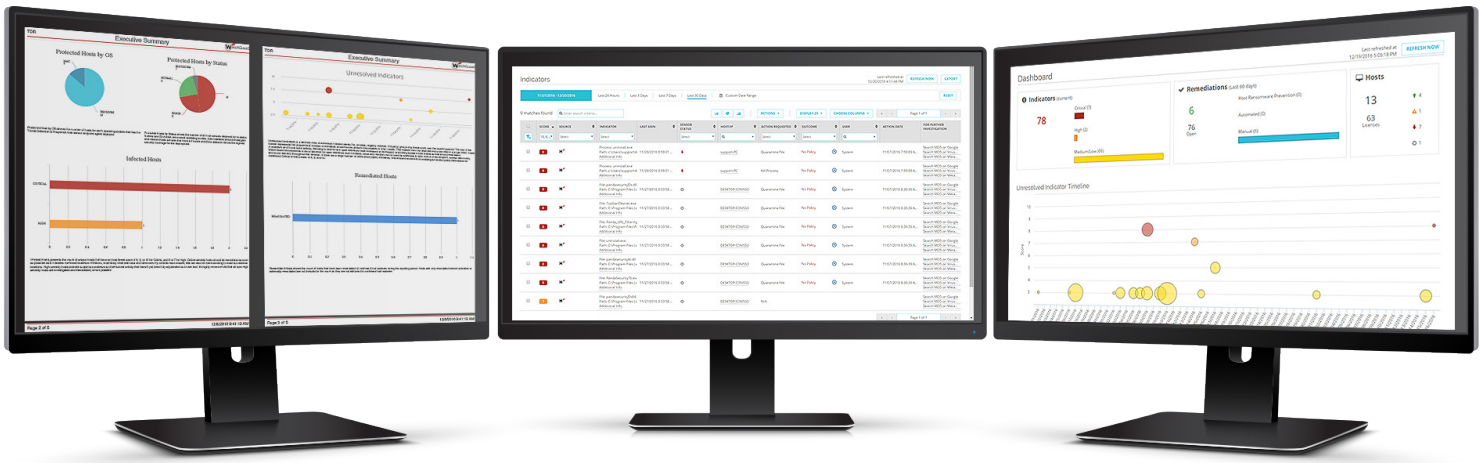
Il WatchGuard Host Sensor a basso impatto monitora e rileva le attività delle minacce sui dispositivi. L'Host Sensor invia continuamente questi eventi a ThreatSync per la correlazione e la classificazione, ricevendo ed eseguendo le istruzioni per la correzione tattica. Gli Host Sensor sono gestiti centralmente dal cloud, agevolando agli MSSP e agli amministratori IT le operazioni di implementazione, aggiornamento e gestione degli Host Sensor in tutto il mondo.

Intelligence sulle minacce di livello enterprise

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

Prevenzione avanzata dal ransomware

Host Ransomware Prevention (HRP) 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 sull'endpoint.



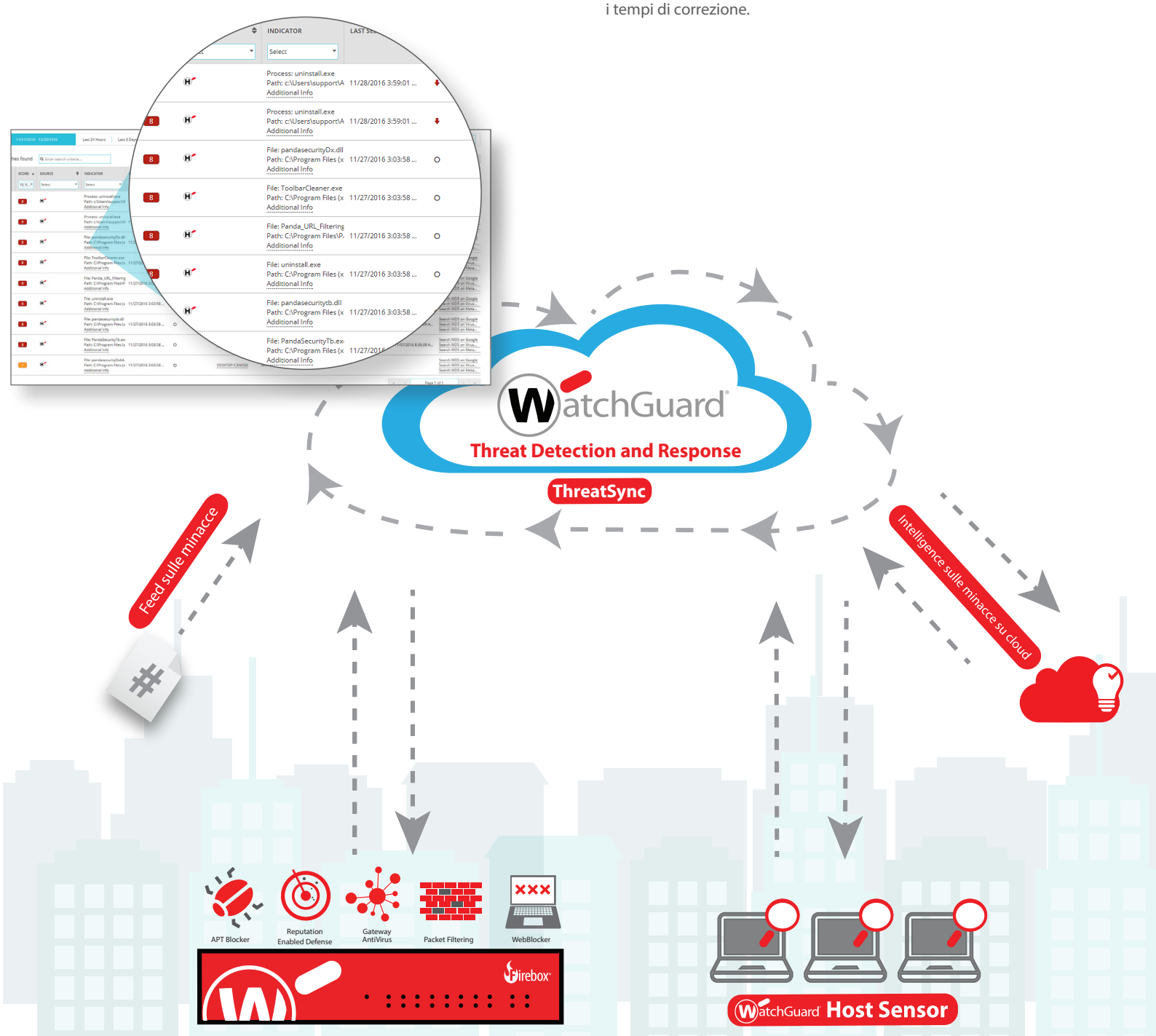
Sicurezza migliorata grazie alla correlazione

ThreatSync, il motore basato su cloud per la correlazione e la classificazione delle minacce di TDR, consente di migliorare la consapevolezza in merito alla sicurezza e la reazione in tutta la rete fino agli endpoint.

ThreatSync è in grado di raccogliere i dati degli eventi di rete da diversi altri servizi di sicurezza presenti sul dispositivo Firebox, tra cui APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus e WebBlocker. Tali eventi vengono correlati alle attività di minaccia rilevate attraverso WatchGuard Host Sensor e l'intelligence sulle minacce di livello enterprise.

ThreatSync quindi analizza questi dati sulle minacce per assegnare un punteggio dettagliato alle minacce e classificarle in base alla gravità complessiva. Vengono ritrasmesse a Host Sensor azioni di risposta specifiche, comprendenti l'inserimento di file in quarantena, la terminazione di processi o l'eliminazione di valori del registro di sistema.

Questa tecnologia proprietaria non solo diminuisce il tempo di rilevamento migliorando la visibilità sulle minacce sia nella rete sia negli endpoint, ma in ultima analisi permette di approntare con sicurezza le reazioni generando un punteggio globale delle minacce, così da migliorare i tempi di correzione.



Una sola appliance, un solo pacchetto, sicurezza totale

Threat Detection and Response è disponibile attraverso WatchGuard Total Security Suite, che include anche soluzioni di sicurezza avanzate come APT Blocker, WebBlocker, Gateway AntiVirus, Intrusion Prevention Service e Reputation Enabled Defense.

Anche se ciascuna di queste soluzioni di sicurezza può fornire protezione dalle minacce avanzate, gli utenti traggono il massimo beneficio quando le difese di sicurezza funzionano in modo integrato, fornendo la protezione più efficace e la massima efficienza senza compromettere le prestazioni dell'unità Firebox.

Prodotto	Supporto	TOTAL SECURITY	Basic Security
Stateful Firewall	✓	✓	✓
Mobile VPN	✓	✓	✓
Branch Office VPN	✓	✓	✓
Proxy Applicativi	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
App Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway Antivirus		✓	✓
Reputation Enabled Defense (RED)		✓	
Network Discovery		✓	✓
APT Blocker		✓	
Data Loss Protection (DLP)		✓	
Dimension Command		✓	
Threat Detection & Response		✓	
Supporto	Standard (24x7)	**Gold (24x7)**	Standard (24x7)

Modello Firebox	Host Sensor inclusi
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
XTMv S	20
XTMv M	50
XTMv L	150
XTMv DC	250

Servono ulteriori Host Sensor?

Threat Detection and Response comprende un numero fisso di Host Sensor disponibili in base all'appliance in uso (Firebox M Series, Firebox T Series o XTMv). Sono disponibili Host Sensor aggiuntivi attraverso un'offerta di aggiornamento disponibile secondo necessità.

Opzioni aggiuntive per Host Sensor
10 Host Sensor
25 Host Sensor
50 Host Sensor
100 Host Sensor
250 Host Sensor
500 Host Sensor

Il servizio Threat Detection and Response comprende un numero fisso di Host Sensor che dipende dal modello dell'appliance. Sono disponibili per l'acquisto ulteriori Host Sensor, che si aggiungono alla quantità complessiva di Host Sensor disponibile per l'account.

Sicurezza facilmente gestibile e scalabile

Threat Detection and Response consente agli utenti di scalare e gestire la sicurezza con grande semplicità. Il servizio basato su cloud permette agli amministratori e agli operatori di implementare rapidamente gli Host Sensor nell'intera organizzazione, creare policy ed eseguire la correzione con un solo clic.

TDR è facilmente scalabile così da poter crescere con la propria azienda. Benché ogni istanza di TDR includa un numero fisso di Host Sensor basati su un'appliance esistente, i pacchetti di aggiornamento permettono di aggiungere facilmente ulteriori Host Sensor per soddisfare le proprie esigenze organizzative.

Se la gestione dei servizi di sicurezza non è il modo migliore di impiegare il tempo e le risorse preziose della propria organizzazione, una vasta rete di partner fornitori di servizi di sicurezza gestiti (MSSP) permette di sfruttare i vantaggi di Threat Detection and Response prendendosi cura delle operazioni quotidiane.

Ulteriori informazioni su Threat Detection and Response. Per ulteriori informazioni sul più recente servizio di sicurezza di WatchGuard, visitare il nostro sito web all'indirizzo **www.watchguard.com/TDR**.

Come iniziare

WatchGuard dispone della rete di rivenditori e fornitori di servizi a valore aggiunto più estesa del settore. Per iniziare visita il nostro sito web, dove potrai trovare il miglior partner per la tua azienda, oppure contattaci direttamente per ottenere risposte a qualsiasi domanda tu possa avere, così da iniziare a collaborare con il partner perfetto per le tue esigenze.

- Visita la nostra pagina "Trova un rivenditore" per trovare un partner nella tua zona: **http://www.watchguard.com/it/wgrd-international/find-a-reseller**
- Parla con uno specialista di sicurezza di WatchGuard: **www.watchguard.com/wgrd-sales/emailus**

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nei prodotti e servizi per la sicurezza di rete, il Wi-Fi protetto e l'intelligence di rete con più di 75.000 clienti in tutto il mondo. La missione della società è di rendere la sicurezza di grado enterprise accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, facendo di WatchGuard la soluzione ideale per le aziende distribuite e le piccole e medie imprese. La sede centrale di WatchGuard si trova a Seattle (stato di Washington, negli Stati Uniti) e dispone di uffici dislocati in Nord America, Europa, Asia Pacifico e America Latina. Per saperne di più, visita WatchGuard.com.