DATASHEET

HOST SENSOR

Threat Detection and Response agent for endpoint monitoring and remediation

As threats continue to evolve, it becomes increasingly important to protect every attack vector from the network to the endpoint. Part of WatchGuard's Total Security Suite, Threat Detection and Response (TDR) correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. Visibility into the network is provided through WatchGuard Firebox® appliance, while endpoint event data is collected through the WatchGuard Host Sensor.

The WatchGuard Host Sensor continuously detects threats on the endpoint, receiving and executing response commands. Host Ransomware Prevention (HRP), a feature of the WatchGuard Host Sensor, along with the advanced malware protection provided through APT Blocker, enables industry-leading prevention against ransomware attacks. Host Ransomware Prevention blocks the execution of ransomware before file encryption on the endpoint takes place, mitigating the ransomware attack before any damage is done.

EXTEND VISIBILITY TO THE ENDPOINT

The lightweight WatchGuard Host Sensor monitors and detects threat activity on devices using heuristics and behavioral analytics. The Host Sensor continuously sends these events to TDR's ThreatSync to be correlated with events from the Firebox appliance, developing a comprehensive threat score prioritization.

AUTOMATED THREAT REMEDIATION

The WatchGuard Host Sensor enables users to automate threat remediation through the creation of policies. Based on the comprehensive threat score generated by ThreatSync, these pre-defined policies determine the response tactics triggered – including kill the process, quarantine file, or delete the registry value. Automated threat remediation can not only decrease the time it takes to remedy the problem, but also helps to minimize the demand on scarce resources.

ADVANCED RANSOMWARE PREVENTION

Host Ransomware Prevention is a ransomware-specific module within the WatchGuard Host Sensor. HRP leverages a behavioral analytics engine and a decoy directory honeypot to monitor a wide array of characteristics that determine if a given action is associated with a ransomware attack or not. If the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption takes place.

ADVANCED THREAT TRIAGE WITH APT BLOCKER

Malware is constantly evolving and suspicious indicators could be early warning signs of yet to be identified malware. Now, thanks to tight integration with WatchGuard APT Blocker, WatchGuard Host Sensors can automatically send suspicious files for deep analysis and re-scoring in a next-generation cloud-sandbox.

FEATURES & BENEFITS

- Continuously monitors and detects endpoint threat events
- Decreases time to detection and remediation through automation
- Improves prevention of advanced malware attacks, including ransomware
- Pre-defined policies run automatically to kill the process, quarantine files, or delete the registry value
- The lightweight software agent consumes minimal processing resources
- Works alongside existing antivirus solutions already deployed

DATASHEET

Host Sensor Licensing

With a subscription for Total Security Suite, each appliance includes a set number of Host Sensors. These Host Sensors are managed and distributed within Threat Detection and Response, where they are aggregated for use throughout the account. To meet organizational needs, additional Host Sensors are available through an add-on offering.

Firebox Model	Included Host Sensors
T15	5
T35	20
T55	30
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

HOST SENSOR SPECIFICATIONS:

Compatible operating systems –

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

Compatible with Firebox T Series, M Series, Firebox Cloud, and FireboxV appliances.

WatchGuard Security Services

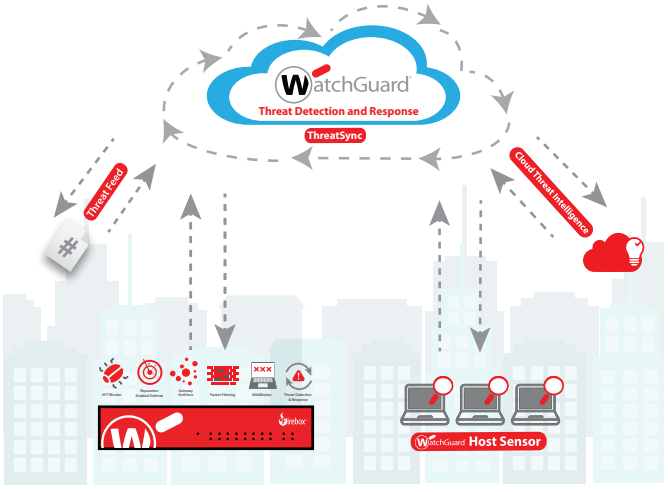
One Appliance, One Package, Total Security

Customers benefit most when security defenses work in tandem, providing the strongest protection, maximum efficiency and lightning-fast performance. WatchGuard's Total Security Suite provides customers traditional network security services, as well as advanced security offerings including APT Blocker, Data Loss Prevention and Threat Detection and Response (TDR).

TDR takes this philosophy a step further, by correlating event data from the network, endpoint and threat intelligence feeds to create a comprehensive threat score and rank. Our threat correlation and scoring engine, ThreatSync, collects input from advanced network security service, including WebBlocker, APT Blocker, Gateway AntiVirus and spamBlocker. It then correlates this network data with endpoint event data collected via the WatchGuard Host Sensor to generate a threat score and rank based on severity.

With WatchGuard Total Security Suite, organizations can benefit from advanced network security, robust endpoint visibility and remediation, as well as enterprise-grade threat intelligence through one complete offering.

Features & Services	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	✓	
Support	Gold (24x7)	Standard (24x7)



WatchGuard has the industry's largest network of value-added resellers and service providers. Browse our network of certified partners at **findpartner.watchguard.com. Learn more about Threat Detection and Response with WatchGuard Host Sensor at watchguard.com/TDR.**

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com