DATASHEET

THREAT DETECTION & RESPONSE

Stop Advanced Malware with Correlated Security

Hackers are designing malware to be more sophisticated than ever. Through packing, encryption, and polymorphism, cyber criminals are able to disguise their attacks to avoid detection. Zero day attacks and advanced malware easily slip by antivirus solutions that are simply too slow to respond to the constant stream of emerging threats. Organizations of all sizes need a solution that leverages a holistic approach to security from the network to the endpoint. WatchGuard Threat Detection and Response (TDR) is a powerful collection of advanced malware defense tools that correlate threat indicators from Fireboxes and Host Sensors to stop known, unknown and evasive malware threats.

"The correlated detection and automated response features adds a missing layer to our security stack and have enabled us to immediately detect infections, and prevent them from spreading within our network."

~ Andre Bromes, SVP and CIO/CISO of Goodwill New York / New Jersey

CORRELATION AND THREAT SCORING

ThreatSync is a cloud-based correlation engine that analyzes event data from Host Sensors and Fireboxes to identify malicious behavior. Threats are scored based on severity to guide remediation.

THREAT VISIBILITY ON THE ENDPOINT

The lightweight WatchGuard Host Sensor extends threat visibility and management to the endpoint. The WatchGuard Host Sensor continuously sends heuristic and behavioral data from the endpoint up to ThreatSync for correlation and scoring. Host Sensors are centrally managed from the cloud, making it easy for IT admins and Managed Security Service Providers (MSSPs) to deploy, update and manage sensors anywhere in the world.

AUTOMATED RESPONSE

TDR provides powerful protection against advanced malware threats and can automatically intervene to quarantine files, kill the processes, and delete registry keys. Mitigate threats as you see them with one-click, or by establishing policies for automated response based on the threat score.

RANSOMWARE PREVENTION WITH HRP

Host Ransomware Prevention (HRP) is a ransomware-specific module within TDR that uses behavioral analysis and honeypots to look for signs of ransomware. If malware is detected, HRP automatically intervenes to stop the ransomware before files are lost.

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, suspicious files can be sent for deep analysis and re-scoring in a next-generation cloudsandbox.

ENTERPRISE-GRADE THREAT INTELLIGENCE

Threat Intelligence was previously only a benefit available to enterprise organizations with big budgets and even bigger security teams. With Threat Detection and Response, WatchGuard aggregates and analyzes threat intelligence feeds - delivering the security benefits without passing on the associated complexities or cost.

DATASHEET

Smarter Detection through Correlation

Advanced malware attacks are complex and multi-staged. Endpoints typically become infected when a user falls for a phishing campaign or clicks on a malicious link to begin the infection process. Once the attack is initiated, the malware may attempt to reach out to command and control servers for further instruction. The malware may also attempt to spread to other points in your organization via your network.

While the malware itself may look entirely unique, the network behaviors needed to facilitate the attack follow common and predictable patterns. If your security solutions are operating in silos, there would be no way for the network to know what's happening on the endpoint and vice versa, which could leave you vulnerable to this dangerous threat. For this reason, analyzing network and endpoint behaviors in tandem provides a powerful means of identifying and stopping never-before-seen malware. Threat Detection and Response makes this possible.

Event data from security services on WatchGuard Fireboxes, including APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus and WebBlocker, is sent to ThreatSync to be matched with endpoint data collected from the Host Sensor. ThreatSync then analyzes this threat data to provide a comprehensive threat score and rank overall severity. Events that are captured on both the network and endpoint automatically receive the most severe threat score of 10.

With policies enabled, ThreatSync will automatically instruct the Firebox to block the malware from calling out to the malicious server and will either quarantine the file, kill the process, or delete the registry key persistence on the endpoint. The same actions can also be performed manually through our one-click, manual remediation.

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

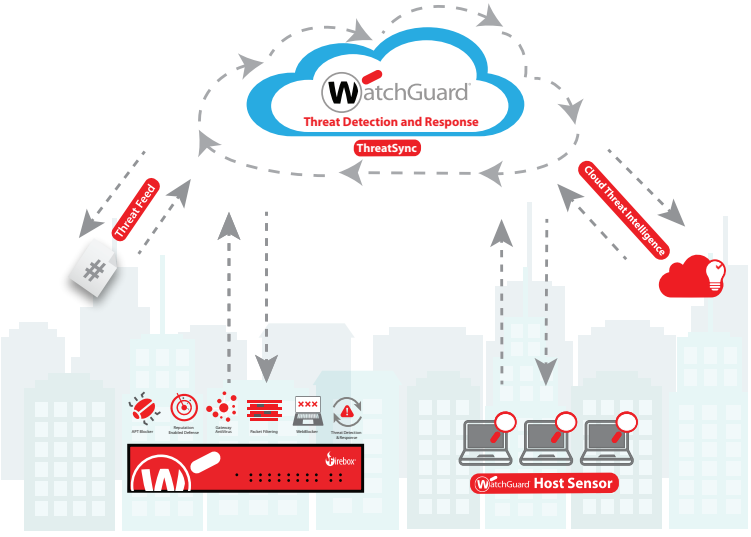
HOST SENSOR SPECIFICATIONS:

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.

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 at **watchguard.com/TDR.**

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