WatchGuard®

THREAT DETECTION & RESPONSE

Threat Detection & Response

Correlate. Prioritize. Respond.

Cyber criminals are mounting attacks with increasing complexity and sophistication, using coordinated means to gain access to your network from any and every connection. Security measures must keep pace by adding detection capabilities across networks and endpoints, as well as the ability to correlate this event activity into targeted action. WatchGuard's Threat Detection and Response (TDR) service correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. TDR enables small and midsize businesses and the Managed Security Service Providers (MSSPs) that support them to confidently remediate advanced malware attacks before business-critical data or organizational productivity is compromised.

Network and Endpoint Event Correlation

ThreatSync is WatchGuard's new cloud-based correlation and threat scoring engine, improving security awareness and response across the network to the endpoint. ThreatSync collects event data from the WatchGuard Firebox, WatchGuard Host Sensor and cloud threat intelligence feeds, and correlates this data to generate a comprehensive threat score to guide remediation.

Extend Visibility to the Endpoint

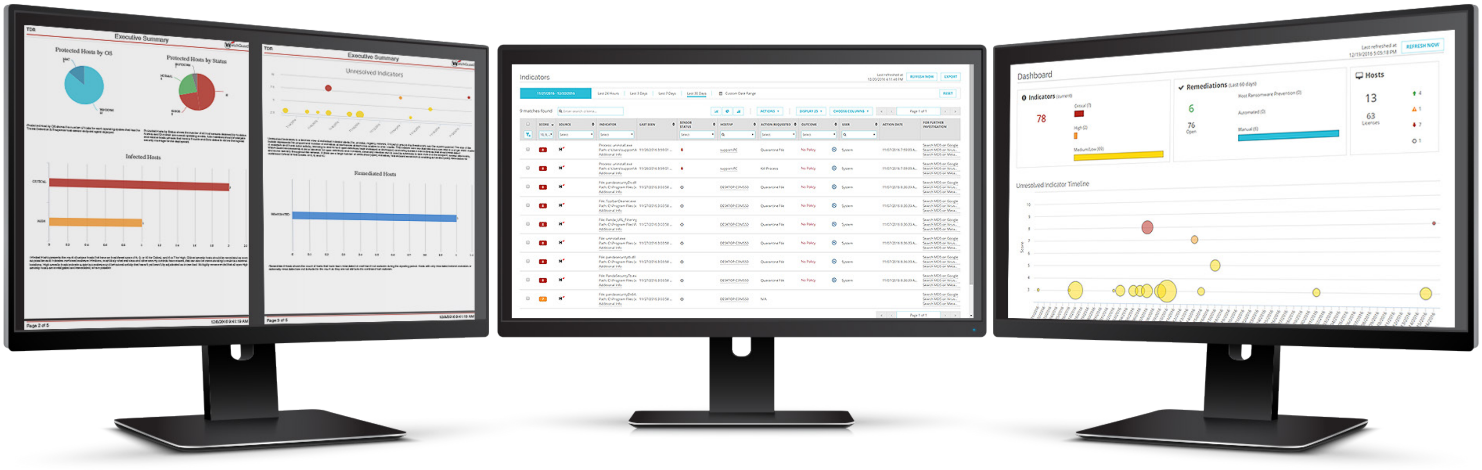
The lightweight WatchGuard Host Sensor monitors and detects threat activity on your devices. The Host Sensor continuously sends these events to ThreatSync for correlation and scoring, receiving and executing the instructions for tactical remediation. Host Sensors are centrally managed from the cloud, making it easy for MSSPs and IT admins to deploy, update and manage host sensors anywhere in the world.

Enterprise-grade Threat Intelligence

Threat Intelligence gathered from third-party vendors was previously only a benefit available to enterprise organizations with big budgets and even bigger security teams. With Threat Detection and Response, WatchGuard consumes and analyzes threat intelligence – delivering the security benefits without passing down the associated complexities or cost.

Advanced Ransomware Prevention

Host Ransomware Prevention (HRP) 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 on the endpoint takes place.



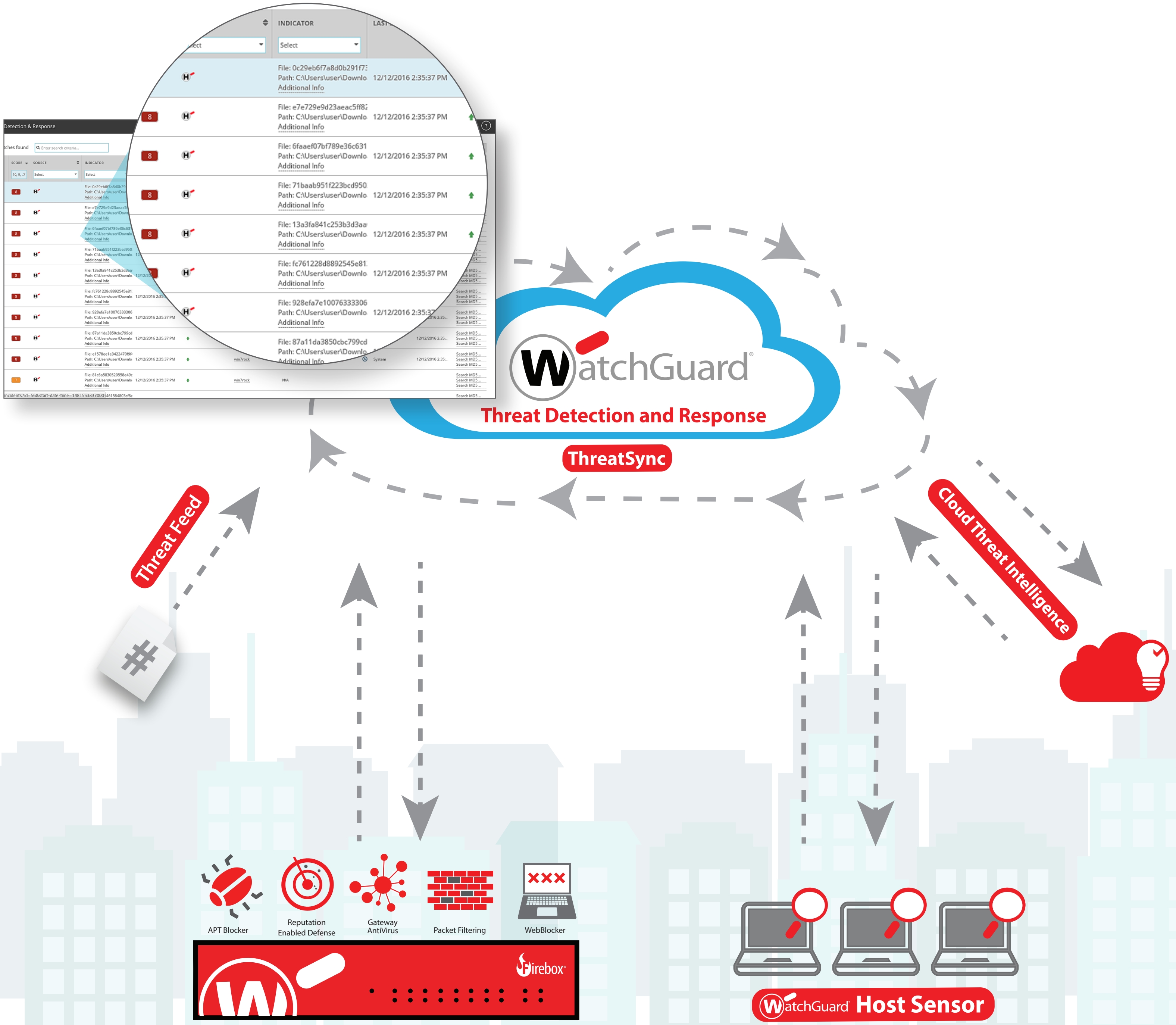
Improved Security with Correlation

ThreatSync, TDR's cloud-based correlation and threat scoring engine, improves security awareness and response across the network to the endpoint.

ThreatSync can collect network event data from several other security services on the Firebox, including APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus and WebBlocker. These events are correlated with threat activity detected via the WatchGuard Host Sensor and enterprise-grade threat intelligence.

ThreatSync then analyzes this threat data to provide a comprehensive threat score and rank overall severity. Specific response actions will be transmitted back to the Host Sensor including quarantine file, kill process or delete registry value.

This proprietary technology not only decreases time to detection by enhancing visibility into threats on both the network and the endpoint, but ultimately empowers confident response by generating a comprehensive threat score to improve time to remediation.



		INDICATOR	LAST
	H	File: 0c29eb6f7a8d0b291f73 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
8	H	File: e7e729e9d23aeac5ff82 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
8	H	File: 6faaef07bf789e36c631 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
8	H	File: 71baab951f223bcd950 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
8	H	File: 13a3fa841c253b3d3aa Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
	H	File: fc761228d8892545e81 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:37 PM
	H	File: 928efa7e10076333306 Path: C:\Users\user\Downlo Additional Info	12/12/2016 2:35:3
		File: 87a11da3850cbc799cd Path: C:\Users\user\Downlo Additional Info	

One Appliance, One Package, Total Security

Threat Detection and Response is available through WatchGuard Total Security Suite, which also includes advanced security solutions like APT Blocker, WebBlocker, Gateway AntiVirus, Intrusion Prevention Service and Reputation Enabled Defense.

While each of these security solutions can defend against advanced threats, users benefit most when security defenses work in tandem, providing the strongest protection and maximum efficiency without impacting performance on the Firebox.

Product	Support	TOTAL SECURITY	Basic Security
Stateful Firewall	✓	✓	✓
Mobile VPN	✓	✓	✓
Branch Office VPN	✓	✓	✓
Application Proxies	✓	✓	✓
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		✓	
Support	Standard (24x7)	**Gold (24x7)**	Standard (24x7)

Firebox Model	Included Host Sensors
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	250
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

Need More Host Sensors?

Threat Detection and Response includes a set number of Host Sensors based on your Firebox M Series, T Series, Firebox Cloud or FireboxV model. Additional Host Sensors are available through an upgrade offering, as needed.

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

Threat Detection and Response service includes a set number of Host Sensors, based on appliance model. Additional Host Sensors are available for purchase and add to overall host sensor quantity available to the account.

WatchGuard

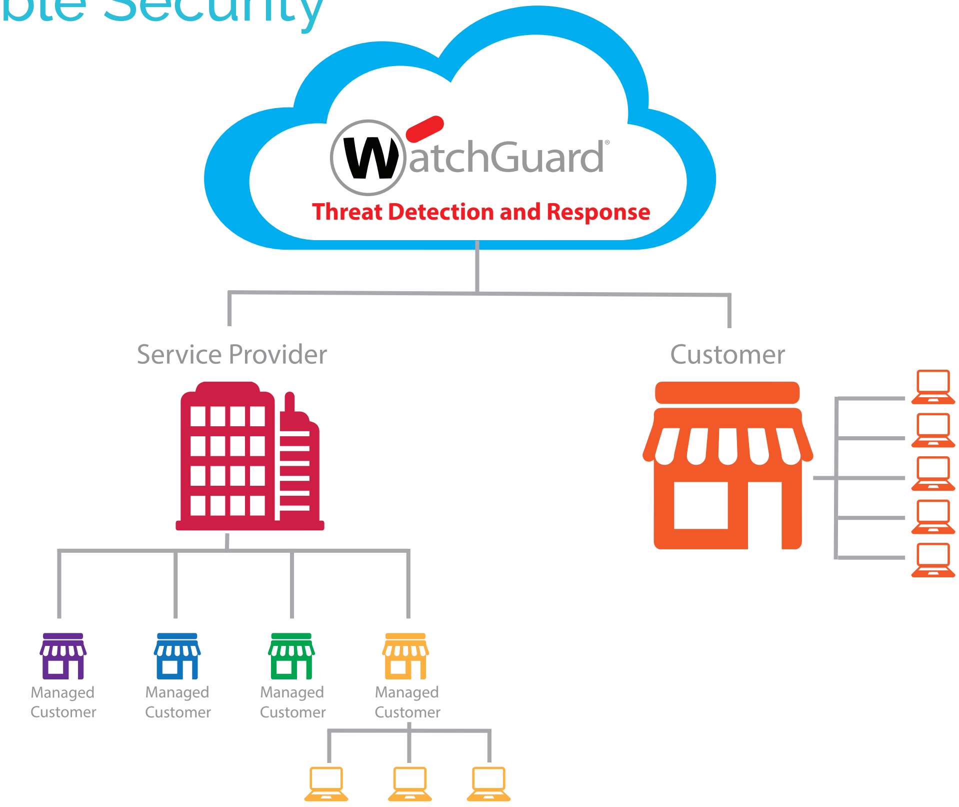
THREAT DETECTION & RESPONSE

Manageable, Scalable Security

Threat Detection and Response enables users to easily scale and manage their security. The cloud-based service makes it easy for administrators and operators to quickly deploy Host Sensors across their entire organization, create policies and perform one-click remediation.

TDR can easily scale and grow with your business. While each instance of TDR includes a set number of Host Sensors based on an existing appliance, upgrade packages make it easy to add more Host Sensors to meet your organizational needs.

If managing security services isn't the best option for your organization's valuable time and resources, our extensive network of MSSP Partners enables you to leverage the benefits of Threat Detection and Response while they take care of the day-to-day operations.



Learn more about Threat Detection and Response. For more information on WatchGuard's newest security service, please visit our website at **www.watchguard.com/TDR**.

How to Get Started

WatchGuard has the industry's largest network of value-added resellers and service providers. To get started, visit our website to find the best partner for your business, or opt to contact us directly and we will answer any questions you may have and get you set up with the perfect partner for your requirements.

- Visit our "Find a Reseller" page to find a partner near you: **http://findpartner.watchguard.com**
- Speak with a WatchGuard security specialist: **www.watchguard.com/wgrd-sales/emailus**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. Part No. WGCE66961_031317