

Putting Everything Together with WatchGuard's ThreatSync Technology

Introduction

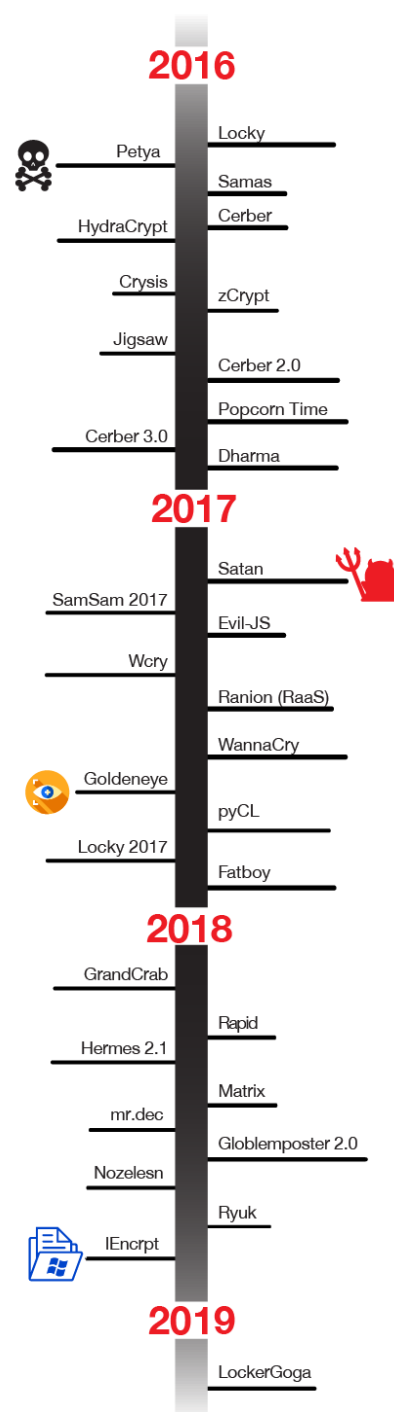
Hackers have become increasingly sophisticated and coordinated in their advanced malware attacks against small and midsize businesses (SMBs). These threats are focused on gaining access to your organization by attacking your weakest threat vector - your endpoint devices - and then spreading to the network. Having your endpoint and network work together to defend against these threats provides not only smarter, but stronger security. ThreatSync™, the threat scoring and prioritization component of Threat Detection and Response, enables organizations of all sizes to do just that.

The Growing Threat

For years, SMBs operated in a blissful world free from the malware attacks that plagued enterprise organizations. The proliferation of malware as a service and the dark web has made malware easier to acquire and more efficient to deploy. Hackers can now generate the same return of investment on an attack against an SMB as they can from a large enterprise.

Additionally, the accessibility of ransomware has flipped the script on advanced attacks. Hackers no longer need to focus on gaining access to information that is valuable to others, they simply need to block your access to the data that's critical to your business operations. By making the ransom amounts reasonable, most organizations are willing to make the payment and move on with their day.

Ransomware Timeline



Knowing Your Network

Clarity into events happening within your network is essential. Knowing which devices are connected, which are consuming the most bandwidth, and what threats are lurking enables you to improve security and productivity. While the feed of information on network events from the Firebox® provides invaluable information, it becomes even more powerful when combined with data from the endpoint and threat intelligence feeds.

WatchGuard's innovative ThreatSync technology leverages data collected from multiple security services enabled on a Firebox running our Total Security Suite, including WebBlocker, Reputation Enabled Defense, Gateway AntiVirus, packet filtering and APT Blocker. For example, a threat blocked at the Firebox may have made its way to an endpoint by any number of other avenues. If the endpoint is infected, ThreatSync can then enable remediation tactics and stop the threat in its tracks.

Seeing Activity on the Endpoint

End users tend to be the most sought-after targets, and the most vulnerable attack point for any organization. You might rest easy when these devices are safely nestled behind the firewall, but what happens when they leave the safety of the office? Or what about remote and branch office employees that are always outside of your network security perimeter? Existing AV solutions are great at preventing known threats from infiltrating endpoints, but devices coming in and out of your network that aren't protected by AV can still present the highest risk to the security of your organization.



It's critical for organizations of all sizes to not only know what devices are connecting to their network, but to know what is happening on those devices. With the WatchGuard Host Sensor, a core component of Threat Detection and Response, IT administrators can now continuously monitor and detect malicious behaviors on end-user devices. ThreatSync collects and analyzes this data, comparing it to the data from the Firebox to create a comprehensive threat score and rank.

Leveraging Threat Intelligence

Threat feeds are lists of known malware signatures that are collected from global sources and updated regularly. These lists can be critical in stopping new threats from infiltrating your environments and gaining access to critical data. There are a lot of vendors that make it their business to build and manage these lists, charging customers high fees for access.

Threat Detection and Response extends these threat intelligence capabilities to SMB organizations. ThreatSync compares the event data collected from the Firebox and Host Sensor with our various threat feeds to quickly determine if the threat has been seen elsewhere. If the threat is known to the threat feeds, it will quickly engage with the Firebox and/or Host Sensor to remediate the threat.



The Power of Correlation

Organizations have been living in the world of preventing threats for many years. But we've seen that no matter how great your preventative security is, there is always the next new threat waiting around the corner to attack your organization. Prevention cannot be the only tool in your security arsenal.

Detection and response are coming of age as security methods, adding more visibility into the network and the endpoint, respectively. But allowing these systems to operate in silos doesn't tell the full story of what's happening to your organization. Enter correlation.

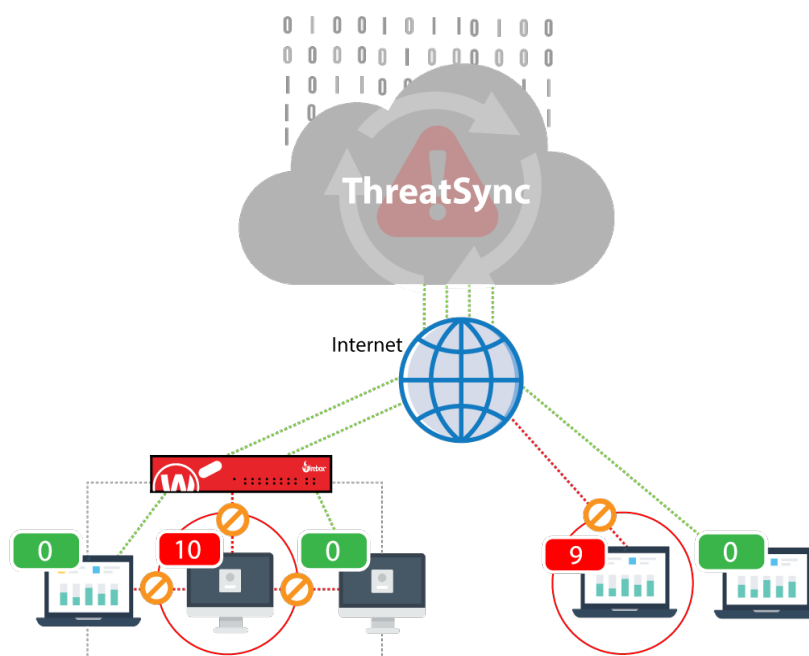
Correlation is the brains behind the operation. It's what takes the mounds of information that these security solutions produce, connects the dots, and actually makes sense of it all. By taking a comprehensive look at both your endpoint and network together, you can get a better sense of which threats are the most severe. Visibility into which threats have infiltrated the endpoint enables IT administrators to quickly and confidently respond to the most dangerous threats before they can spread.

Actionable Insight with ThreatSync

ThreatSync is WatchGuard's Cloud-based correlation and threat-scoring engine, improving security awareness and response across the environment from the network to the endpoint. ThreatSync collects event data from the WatchGuard Firebox, WatchGuard Host Sensor and threat intelligence feeds to then correlate and analyze this data. Through our proprietary algorithms, ThreatSync assigns a comprehensive threat score, grouping similar threats into incidents that require a response.

ThreatSync not only provides visibility into events taking place on both the network and the endpoint, but by delivering a comprehensive threat score and rank, security teams know which threats are the most critical and require immediate attention. Threat Prioritization enables organizations to decrease time to detection and remediation. Response activities triggered by ThreatSync include containing the host, quarantining the file, killing the process, and deleting registry key persistence.

ThreatSync also enables operators to set up and configure email notifications when an incident or indicator is detected on the network or endpoint. You can also set ThreatSync to send an email alert when a threat has been remediated based on the policies you've already set. With email notifications from ThreatSync, take a step back from the dashboard and still know what's happening on your network from wherever you are.



Correlation in Action: Ransomware Prevention with WatchGuard's ThreatSync Technology

Ransomware is a strain of advanced malware plaguing organizations today, becoming increasingly focused on SMBs and distributed enterprises in the last few years. This type of malware is often delivered through a phishing email containing a malicious attachment or URL. Once downloaded to the device, ransomware will try to connect to a control and command server for further instruction for encrypting the files and halting business productivity. A ransom will be posted and once paid, usually via Bitcoins, the hacker will supply the decryption key to unlock the device.



This type of malware actually infects the endpoint and leverages the network to spread the attack throughout your organization. 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.

WatchGuard's ThreatSync technology detects an event on the Host Sensor when a malicious file attempts to install. When the malware tries to call out to the malicious server, a network event is detected on the Firebox and another indicator is created, increasing the overall incident score. Any event that is occurring on both the network and endpoint automatically receives the most severe threat score, a 10.

When enabled, policies automatically will instruct the Firebox to block the malware from calling out to the malicious server by containing the host to prevent the infection from spreading, and will then 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, machine-guided remediation.

WatchGuard Threat Detection and Response

Threat Detection and Response correlates network and endpoint security events with threat intelligence to detect, prioritize and enable immediate action to stop malware attacks.

This security service includes four components:

- ThreatSync – our cloud-based correlation and scoring engine
- Enterprise-grade threat intelligence capabilities
- Lightweight Host Sensor
- Host Ransomware Prevention module (Windows only)

Threat Detection and Response enables users to better detect and respond to advanced threats inside of their network and on their endpoints quickly and efficiently, protecting their organizations from threats by correlating events from the Firebox and Host Sensor to pinpoint malicious activity using heuristics, behavioral analysis, and threat intelligence feeds and assigning it a comprehensive threat score.

Best of all, Threat Detection and Response is included within WatchGuard's Total Security Suite, providing a comprehensive set of security services on the network and endpoint through one license and one appliance.

For more information on ThreatSync and Threat Detection and Response, please visit our website at www.watchguard.com/TDR.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard'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. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

