WatchGuard Threat Detection & Response

The Threat Landscape for SMBs

News headlines are flooded with reports of cyber attacks against large enterprise organizations. But what you don't see in the news are the small and midsize businesses (SMBs) and distributed enterprises that fall victim to these malware attacks each and every day. In fact, the U.S. Securities and Exchange Commission actually reports that SMBs are the principle targets of cyber crime. In 2014, over 60% of all targeted cyber attacks were against SMBs and 75% of all spear-phishing attacks are directed against SMBs.

In 2014, over **60%** of all **targeted cyber attacks** were against **SMBs** and **75%** of all **spear-phishing attacks** are directed against **SMBs.**

What makes these attacks more difficult for SMBs is the cost associated with them. Many of these businesses, roughly half of them in fact, actually go out of business within six months of a cyber attack. SMBs are expected to face the same threats as enterprises, but with smaller budgets and fewer resources. How can SMBs win the battle against cyber crime without breaking the bank?

The Shift from Signatures

Hackers seem to have security vendors figured out. Criminals create a new form of malware that gets past antivirus. This malware strain will infect a few companies before being detected, and security companies will then work quickly to create a signature to block future attacks. Once they've been blocked a few times, these criminals either ditch the malware altogether or run it through an obfuscator to change the signature. The process repeats between a new malware variant and a new signature again and again.

In recent years, we've seen the shift from focusing on signatures as the key way to defend against threats. Security vendors are getting smarter and looking to approach the malware battle by identifying and blocking behaviors that malware threats rely on to function. Not all variants behave exactly the same way, or follow the exact same steps, but there are some common behaviors that can be tracked to improve detection.

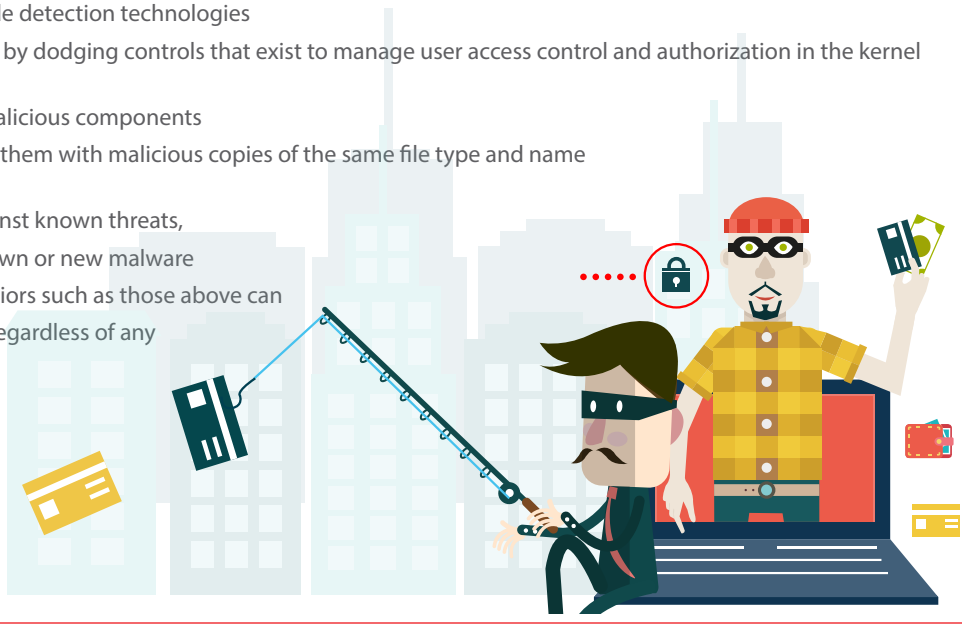
Understanding Malware Behaviors

Malware moves in some not-so-mysterious ways. While hackers are always evolving and changing their methods of attack, there are a few consistent behaviors that most malware tends to follow.

Here are a few of their favorite steps:

- Sneaks a destination hosting malware into a Microsoft macro to download and execute the malware
- Spawns and deletes itself in order to evade detection technologies
- Attempts to gain administrator privileges by dodging controls that exist to manage user access control and authorization in the kernel of the operating system
- Modifies files or processes by injecting malicious components
- Deletes original system files and replaces them with malicious copies of the same file type and name

Signatures are great and necessary defense against known threats, but organizations need a way to stop the unknown or new malware variants as well. Tracking combinations of behaviors such as those above can enable the detection of new malware variants, regardless of any changes made to their signature.



Detection with TDR

WatchGuard's newest security service, Threat Detection and Response, leverages multiple forms of detection through the WatchGuard Host Sensor to find advanced malware threats.

Signatures – As mentioned before, signatures are a critical line of defense in the fight against malware. You always want to have an arsenal of collected known threats. WatchGuard Threat Detection and Response leverages enterprise-grade threat intelligence feeds to confirm if a suspicious event on the endpoint is in fact a known threat.

Heuristics –Rather than relying on signatures, TDR uses rules or algorithms to look for commands that could indicate malicious intent. This method of detection can quickly flag a threat without the need for it to execute. TDR leverages over 175 heuristics through the WatchGuard Host Sensor.

Behavioral Analysis – Since malware threats tend to follow certain behaviors, tracking these steps can provide robust detection for unseen malware variants. Our Host Ransomware Prevention module tracks behaviors traditionally associated with ransomware attacks to actually prevent these attacks before file encryption takes place.

Network Detection – The network is an important source of information of attacks and performance usage. Visibility into unusual or blocked traffic patterns, visits to malicious or risky websites, as well as detecting botnets and other threats is critical in protecting your organization. TDR leverages WatchGuard's industry-leading advanced network security solutions to collect and detect threats on the network.

The Power of Correlation

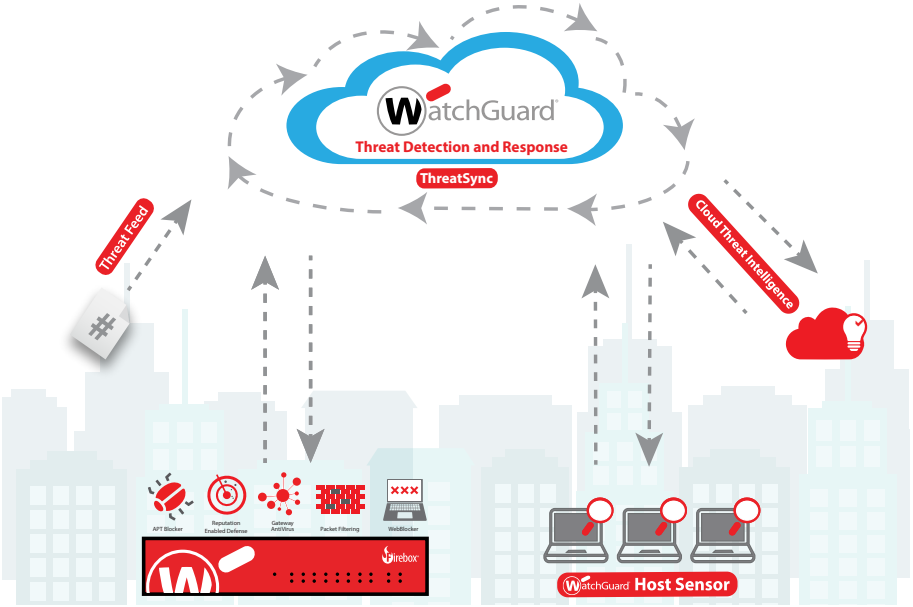
Collecting data from a variety sources is just smart security. But if those sources are operating completely separate of each other, it doesn't provide a comprehensive view of your organization. Correlation takes the mounds of information that these security solutions produces, connects the dots, and actually makes sense of it all. Decrease the time needed to detect and remediate threats by analyzing data from multiple security sources so IT administrators can clearly see which threats are the most severe and need their immediate attention.

Getting the Full Picture with ThreatSync

Looking at security through the lens of correlation is really the only way to get a full picture of your organization's security. ThreatSync, WatchGuard's cloud-based correlation and threat scoring engine, provides actionable insight into the threats attacking both the network and the endpoints.

ThreatSync collects, correlates and analyzes even data from the WatchGuard Firebox, WatchGuard Host Sensor and threat intelligence feeds. Through our proprietary algorithms, ThreatSync assigns a comprehensive threat score, grouping similar threats into incidents that require a response.

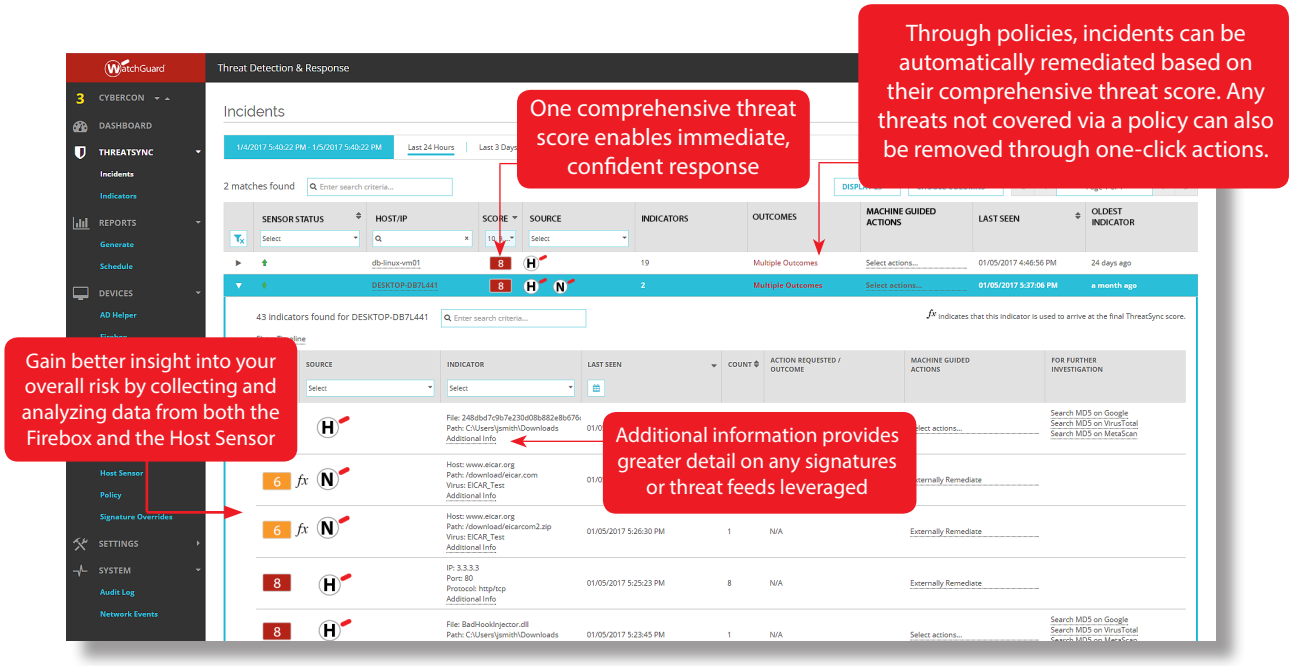
ThreatSync not only provides visibility into events taking place on both the network and the endpoint, but by providing a comprehensive threat score and rank, security teams know which threats are the most critical and require immediate attention. Threat prioritization enables organizations to decrease time to detection and remediation, as well as decrease the number of dedicated resources required to remove threats.



Automating Response with TDR

For SMBs with constrained and limited resources or distributed enterprises that lack technical staff at each branch location, it can be difficult to take action on each and every threat that needs attention. Automation can be key in quickly and effectively detecting and remediating threats. Automating response enables organizations to free up constrained resources to focus on other areas of security. It also improves time to remediation which can decrease infection dwell time and get the organization back on track.

WatchGuard TDR enables users to easily set up policies to enable automation based on organizational needs. Through threat scoring and prioritization provided by ThreatSync, users can set up policies to initiate remediation based on a threat score or range including kill process, quarantine file and delete registry key value. For example, organizations at low risk of attack may only choose to automate response for high ranking threats scored at 8 or above. However, should they find themselves at a higher risk of attack they could choose to automatically remediate threats scored at a 6 or above.



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.

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.

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