Breaking Down Security Silos:

Achieving Security Bliss through Correlation

Whether you're a distributed enterprise organization with 10 branch offices or a small to midsize business with 10 employees, disparate solutions and environments can lead to gaps in security information. These security silos are a major issue facing IT teams struggling to connect information across headquarters and branch offices, or dealing with incompatible network and endpoint solutions.

Here are a few common "silos" that you may find yourself in today.

1

As security threats against organizations of all sizes have continued to grow, we've seen the adoption of a bolt-on approach to security. This involves adding new problem-specific solutions to your existing infrastructure even if they don't communicate with one another. This can create silos in your organization between unrelated security solutions.

2

Distributed enterprise organizations can find inconsistancies in the security applied at the headquarters verses that applied to branch offices. Having different levels of security makes sense for these types of organizations, but it can still create a silo for IT teams to manage multiple security systems and locations.

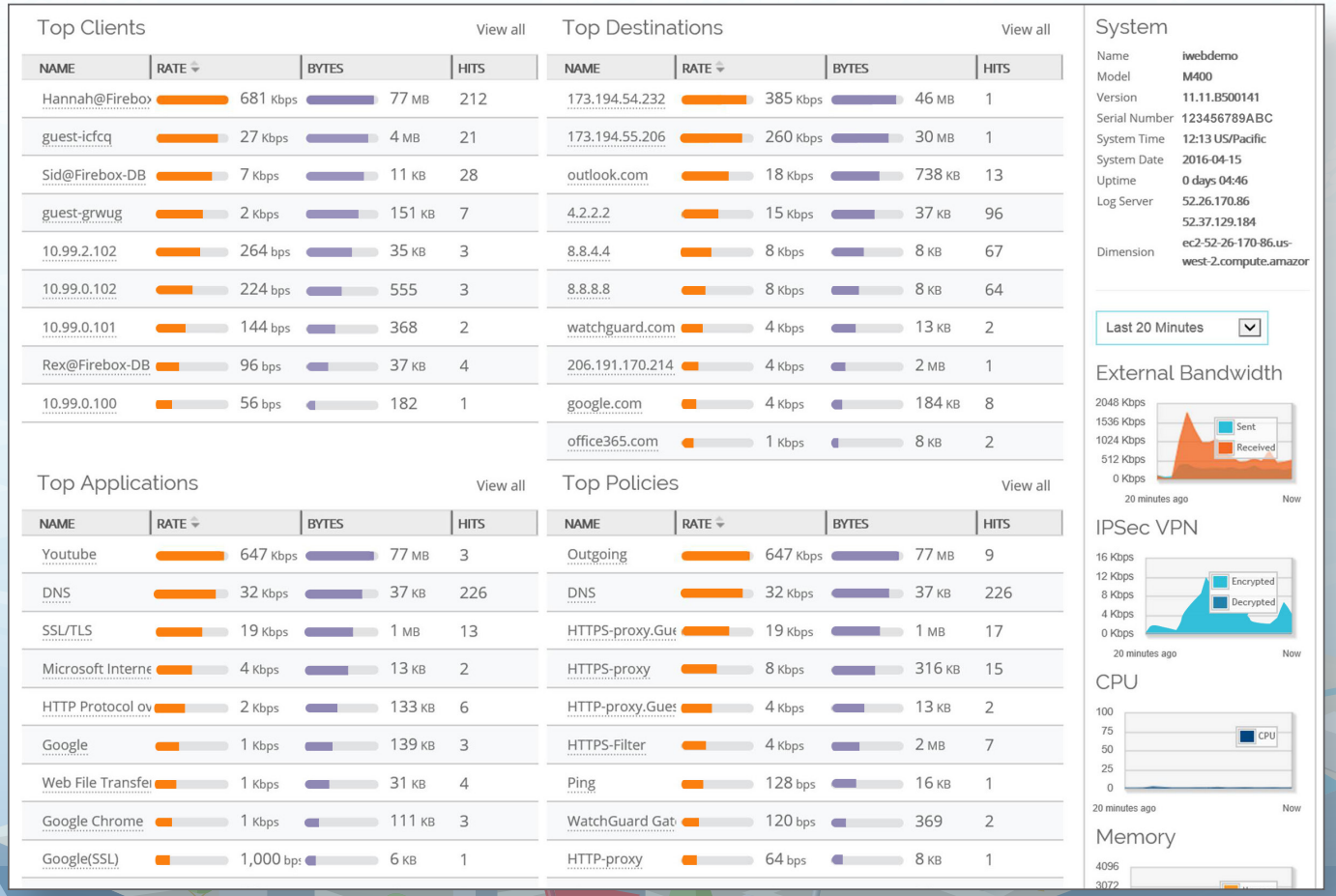
3

Remote employees can be particularly susceptible to threats as they rarely find themselves behind the firewall. Not having complete visibility into these remote devices can create an easy attack vector for hackers looking for an in to your network.

Starting with the Network

The network contains a treasure trove of security information. Having visibility into unusual or blocked traffic patterns, visits to malicious or risky websites, as well as detecting botnets and other threats is a critical step in protecting your organization. It's also important to know which devices are connected to your network, ensuring that only those with privileges and the proper security policies in place have access.

Knowing what's happening in your network can also provide information on the throughput and performance impacts based on usage. Visibility into which users are consuming the most bandwidth, and what they're using it for is critical in controlling performance shortages.



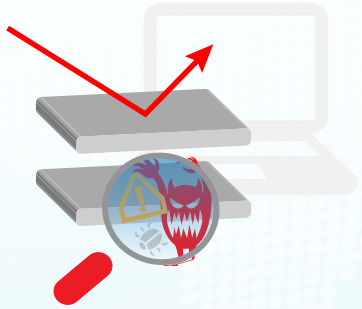
Network

Endpoint

Moving to the Endpoint

Visibility into your endpoints starts with knowing your devices and ensuring that the proper security is in place to protect them. It's also critical to know if any users are particularly susceptible to threats, or are already infected.

There are really **two layers of visibility** into protecting the endpoint:
blocking what you know and **finding what you don't**.



Existing antivirus solutions that leverage signatures are a great way to block the threats that we already know about. However, there can often be gaps in this layer of protection since patch updates are performed weekly or only as needed.

Detecting what you don't know can be a bit trickier. There are a variety of solutions that utilize different methods to determine if an event is a threat. Whether you track heuristics, behavior analysis, or changes to files, processes and registries, visibility into the endpoint is critical. Without this information, organizations can find themselves exceedingly vulnerable to malware and ransomware attacks.

Getting Smarter with Threat Intelligence

Gartner defines threat intelligence as *"evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."*

Sorry…. What? Basically, threat intelligence is collecting all of the information that we know about an existing or recently released threat to inform potential victims in hopes of blocking the threat using signatures. That sounds tedious and time-consuming. It shouldn't surprise you, but... there are vendors that are willing to do this, charge a BUNCH of money for it, and provide it mostly to enterprise organizations.

There are plenty of threat feeds available for free, but it's important to remember that you get what you pay for. Free threat intelligence feeds are generally not updated regularly, meaning that you could still miss a threat detected today, or even this week. Additionally, enterprise-grade threat intelligence feeds tend to work best in tandem, but are too expensive for small and midsize businesses.

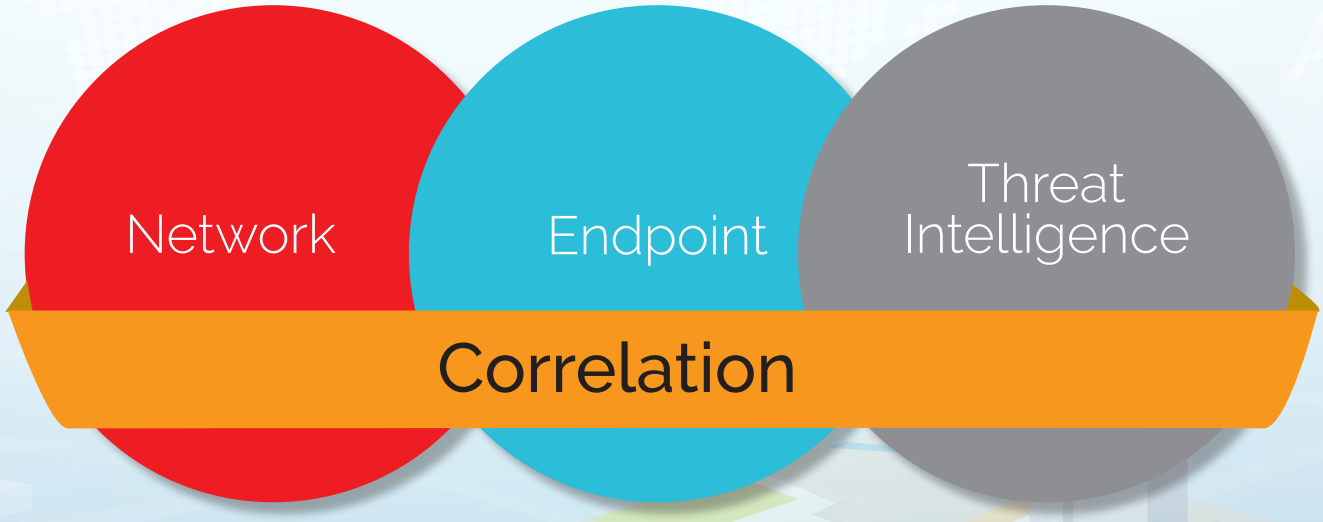
But threat intelligence is an important element in defending against the ever-growing number of threats that small and midsize businesses face. These sites are updated in almost real time, providing the most accurate data on the known threats that can cause serious harm to an organization.

Putting Everything Together with Correlation

Having robust information gathered individually from the network, endpoint and threat intelligence feeds is critical for protecting your organization. However, it's hard to really understand what's going on while this data is still operating in silos. The magic really happens when you bring them all together through correlation.

Correlation takes visibility into these different sources to the next level. By combining all of the event data collected in one place, organizations can better respond through actionable insight. Analyzing and prioritizing this information better equips IT teams to confidently respond to the threats that are most treacherous for their security or business productivity. This becomes incredibly important for organizations with limited time and resources, by decreasing the time to detection and enabling efficient, effective action against the most severe attacks.

Correlation

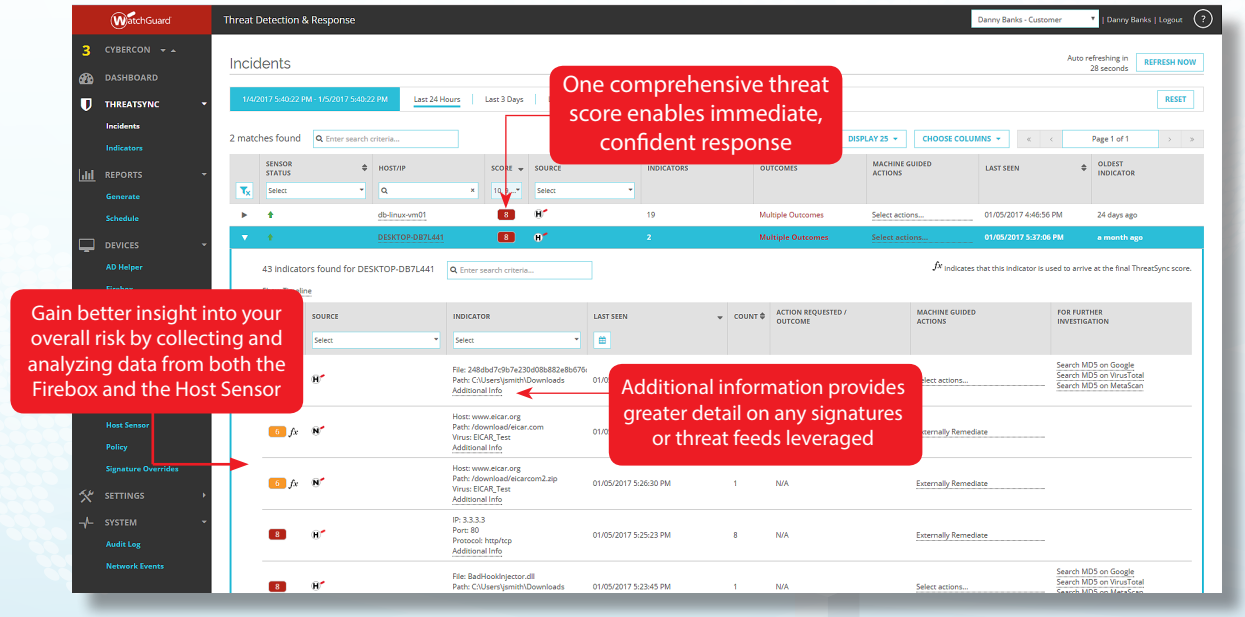


Correlate, Prioritize, and Respond with WatchGuard

If correlation is so great, why have you never heard of it before? Honestly, that's a great question. And the simple answer is that it's not an easy thing to do, and it's especially not easy to automate.

But WatchGuard's newest security service, Threat Detection and Response (TDR), provides enterprise-grade correlation capabilities for small and midsize businesses and distributed enterprises.

ThreatSync, the cloud-based scoring and correlation engine component of TDR, analyzes threat data from the Firebox®, WatchGuard Host Sensors installed on endpoints, and third-party threat intelligence feeds. ThreatSync then delivers a comprehensive threat score based on threat severity to guide remediation. Want to take a closer look at a potential threat? Suspicious files can be sent for deep analysis and rescoring by WatchGuard's APT Blocker, a next-generation cloud sandbox.



Best of all, Threat Detection and Response is included with the Total Security Suite, and even collects input from other advanced security services in the suite, including APT Blocker, WebBlocker, and Reputation Enabled Defense (RED). WatchGuard is the only UTM vendor to provide all of these security services through one offering, and the only one to provide robust correlation capabilities for organizations of all sizes.

Correlate. Prioritize. Respond.

WatchGuard's Threat Detection and Response service provides enterprise correlation capabilities for small and midsize businesses and distributed enterprises. Don't just think there might be a problem, know if there is with industry-leading solutions that help illuminate your endpoint, detect and correlate threats, and protect your most important assets.

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-grade protection to hundreds of thousands of businesses worldwide. To learn more, visit **WatchGuard.com/TDR**.