



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 inconsistencies 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.

### Top Clients View all

NAME	RATE	BYTES	HITS
Hannah@Firebox	681 Kbps	77 MB	212
guest-icfcq	27 Kbps	4 MB	21
Sid@Firebox-DB	7 Kbps	11 KB	28
guest-grwug	2 Kbps	151 KB	7
10.99.2.102	264 bps	35 KB	3
10.99.0.102	224 bps	555	3
10.99.0.101	144 bps	368	2
Rex@Firebox-DB	96 bps	37 KB	4
10.99.0.100	56 bps	182	1

### Top Destinations View all

NAME	RATE	BYTES	HITS
173.194.54.232	385 Kbps	46 MB	1
173.194.55.206	260 Kbps	30 MB	1
outlook.com	18 Kbps	738 KB	13
4.2.2.2	15 Kbps	37 KB	96
8.8.4.4	8 Kbps	8 KB	67
8.8.8.8	8 Kbps	8 KB	64
watchguard.com	4 Kbps	13 KB	2
206.191.170.214	4 Kbps	2 MB	1
google.com	4 Kbps	184 KB	8
office365.com	1 Kbps	8 KB	2

### Top Applications View all

NAME	RATE	BYTES	HITS
Youtube	647 Kbps	77 MB	3
DNS	32 Kbps	37 KB	226
SSL/TLS	19 Kbps	1 MB	13
Microsoft Intern	4 Kbps	13 KB	2
HTTP Protocol ov	2 Kbps	133 KB	6
Google	1 Kbps	139 KB	3
Web File Transfer	1 Kbps	31 KB	4
Google Chrome	1 Kbps	111 KB	3
Google(SSL)	1,000 bps	6 KB	1

### Top Policies View all

NAME	RATE	BYTES	HITS
Outgoing	647 Kbps	77 MB	9
DNS	32 Kbps	37 KB	226
HTTPS-proxy.Gue	19 Kbps	1 MB	17
HTTPS-proxy	8 Kbps	316 KB	15
HTTP-proxy.Guest	4 Kbps	13 KB	2
HTTPS-Filter	4 Kbps	2 MB	7
Ping	128 bps	16 KB	1
WatchGuard Gat	120 bps	369	2
HTTP-proxy	64 bps	8 KB	1

### System

Name: iwebdemo  
 Model: M400  
 Version: 11.11.B500141  
 Serial Number: 123456789ABC  
 System Time: 12:13 US/Pacific  
 System Date: 2016-04-15  
 Uptime: 0 days 04:46  
 Log Server: 52.26.170.86  
 52.37.129.184  
 Dimension: ec2-52-26-170-86-us-west-2.compute.amaz

Last 20 Minutes

### External Bandwidth

2048 Kbps  
1536 Kbps  
1024 Kbps  
512 Kbps  
0 Kbps

20 minutes ago Now

### IPSec VPN

16 Kbps  
12 Kbps  
8 Kbps  
4 Kbps  
0 Kbps

20 minutes ago Now

### CPU

100  
75  
50  
25  
0

20 minutes ago Now

### Memory

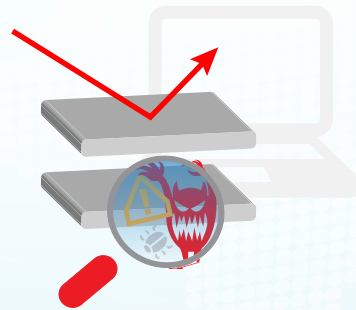
4096  
3072

Network

## Moving to the Endpoint

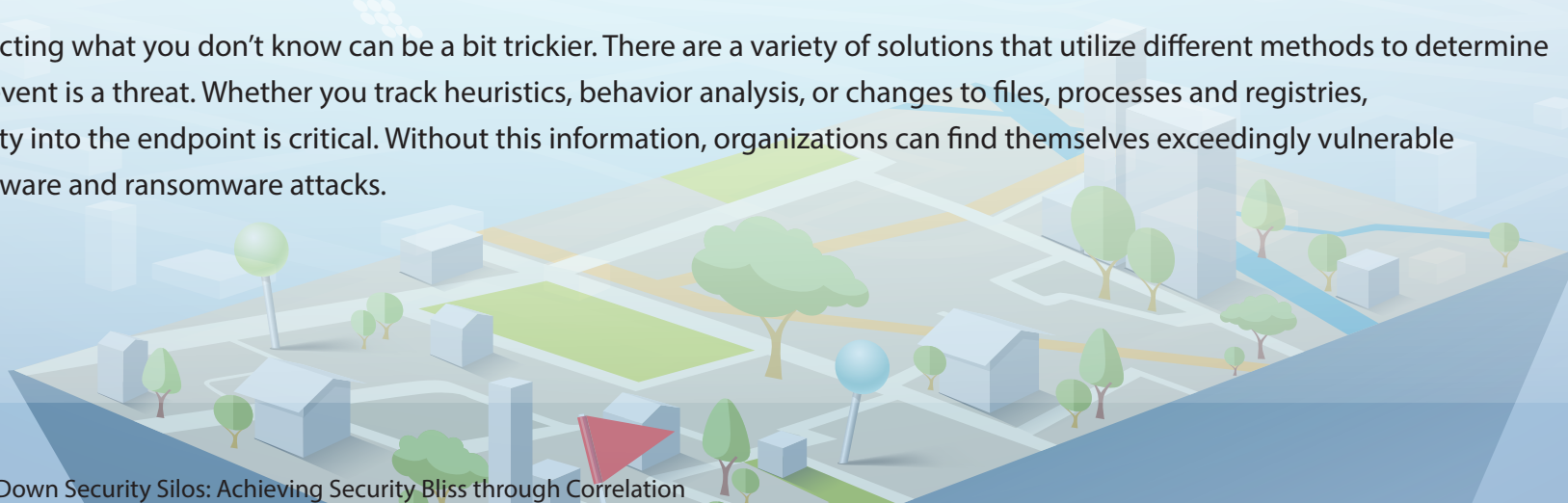
Visibility into your endpoints starts with knowing your devices and ensuring that the proper security is in place to protect them. It's also critical to know if any users are particularly susceptible to threats, or are already infected.

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

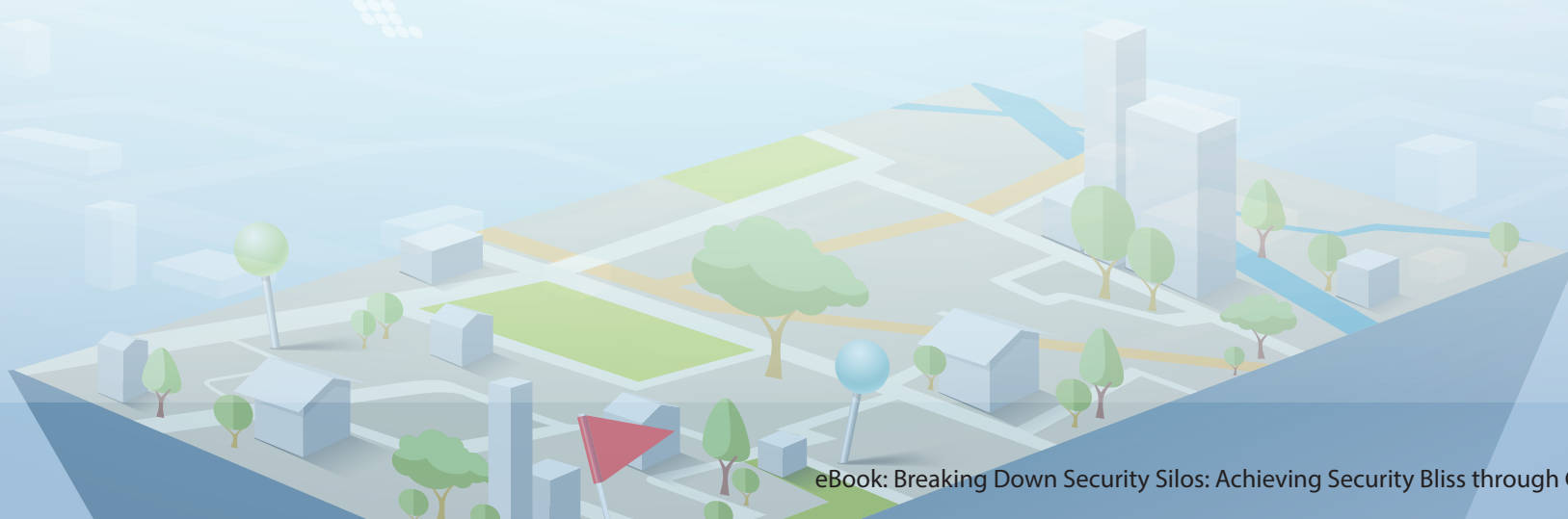
Gartner defines threat intelligence as *“evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”*



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.

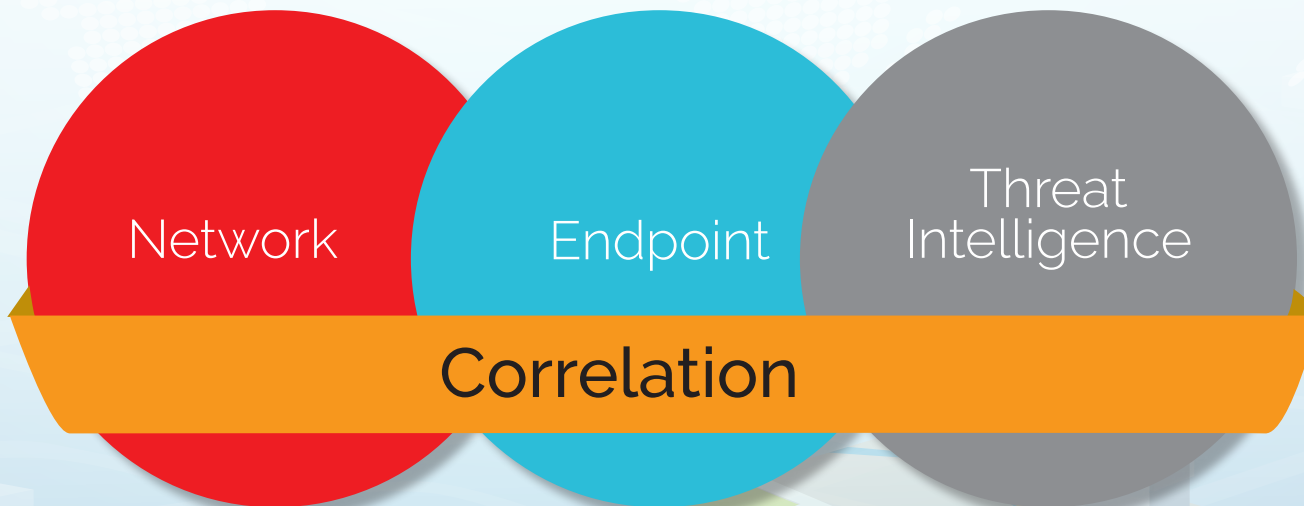


## Putting Everything Together with Correlation

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.

The screenshot displays the WatchGuard Threat Detection & Response interface. A red callout box points to a '3' in the 'SCORE' column, stating: "One comprehensive threat score enables immediate, confident response". Another red callout box points to a table of indicators, stating: "Gain better insight into your overall risk by collecting and analyzing data from both the Firebox and the Host Sensor". A third red callout box points to a specific indicator entry, stating: "Additional information provides greater detail on any signatures or threat feeds leveraged".

SENSOR STATUS	HOST/PIP	SCORE	SOURCE	INDICATORS	OUTCOMES	MACHINE GUIDED ACTIONS	LAST SEEN	OLDEST INDICATOR
Select	Select	Select	Select	Select	Select	Select actions...	Select actions...	Select actions...
	db-linux-vm01	3	H*	19	Multiple Outcomes	Select actions...	01/05/2017 4:46:56 PM	24 days ago
	DESKTOP-DB7L441	3	H*	2	Multiple Outcomes	Select actions...	01/05/2017 5:37:06 PM	a month ago

SOURCE	INDICATOR	LAST SEEN	COUNT	ACTION REQUESTED / OUTCOME	MACHINE GUIDED ACTIONS	FOR FURTHER INVESTIGATION
Select	Select	Select	Select	Select	Select actions...	Select actions...
H*	File: 2484bd7c9b7a230d0b8824eb676; Path: C:\Users\jammh\Downloads; Additional info	01/05/2017 5:23:45 PM	1	N/A	Select actions...	Search MD5 on Google; Search MD5 on VirusTotal; Search MD5 on MetaScan
H*	Host: www.eicar.org; Path: /download/eicar.com; Virus: EICAR_Test; Additional info	01/05/2017 5:26:30 PM	1	N/A	Externally Remediate	
H*	Host: www.eicar.org; Path: /download/eicar.com; Virus: EICAR_Test; Additional info	01/05/2017 5:26:30 PM	1	N/A	Externally Remediate	
H*	IP: 3.3.3.3; Port: 80; Protocol: http/tcp; Additional info	01/05/2017 5:25:23 PM	8	N/A	Externally Remediate	
H*	File: BadHookInjector.dll; Path: C:\Users\jammh\Downloads; Additional info	01/05/2017 5:23:45 PM	1	N/A	Select actions...	Search MD5 on Google; Search MD5 on VirusTotal; Search MD5 on MetaScan

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](https://www.watchguard.com/TDR).

