PRODUCT BRIEF

ThreatARMOR™: Threat Intelligence Gateway

WHICH SECURITY ALERTS DO YOU CHOOSE TO INVESTIGATE?

On average, it takes a company 170 days to detect a breach in their security system.[1] Is it because hackers are becoming more stealthy and experienced? Is it because their security system is not robust? The answer is neither. The company's security system detected the breach the second it occurred and notified the IT team…but the team chose not to investigate it.

Alert fatigue is a common phenomenon affecting most IT security teams today. In fact, 79% of security professionals feel overwhelmed by the volume of threat alerts their company receives.[2] Because of this, only an average of 29% of malware alerts are investigated, giving hackers a free pass into the system.[3] The large volume of threat alerts is directly linked to the amount of traffic fed to security tools. Security tools are not optimized for massive-scale blocking of malicious traffic, which causes performance to suffer and an overload of false positive alerts. Tools need the most relevant data so that alerts are investigated earlier and breaches are detected faster.

Highlights

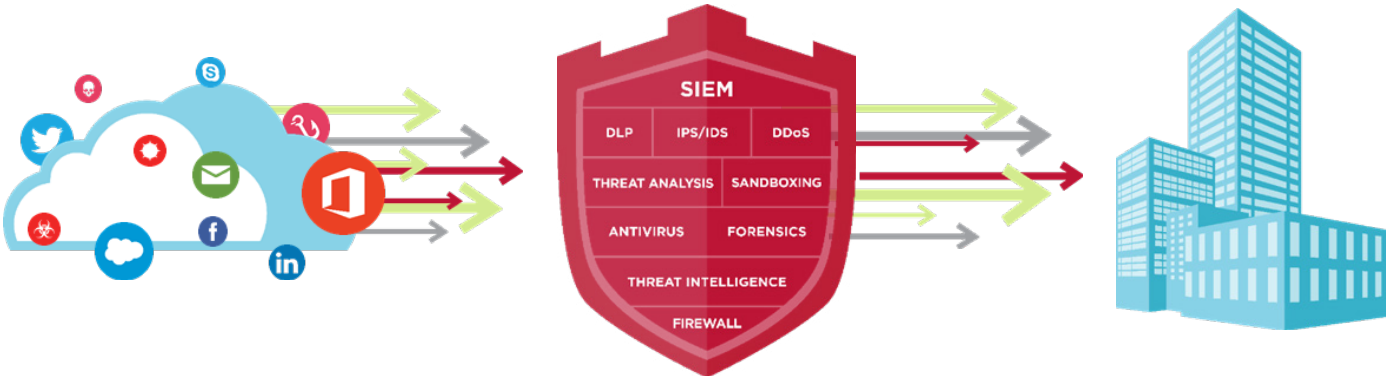
- Alert fatigue contributes to only 29% of malware alerts being investigated
- Security tools are not optimized for massive-scale blocking of malicious traffic
- ThreatARMOR can block up to 80% of malicious connections and over 4 billion IP addresses at line rate
- Deploy ThreatARMOR in 30 minutes or less

[1] Ponemon Institute LLC, "The State of Malware Detection & Prevention," (March 2016): 1.
[2] Greg Masters, "Crying Wolf: Combatting cybersecurity alert fatigue," https://www.scmagazine.com, (June 9, 2017).
[3] Ponemon Institute LLC, "The State of Malware Detection & Prevention," 1.

ixia
A Keysight Business

A THREAT INTELLIGENCE GATEWAY FOR YOUR TOOLS

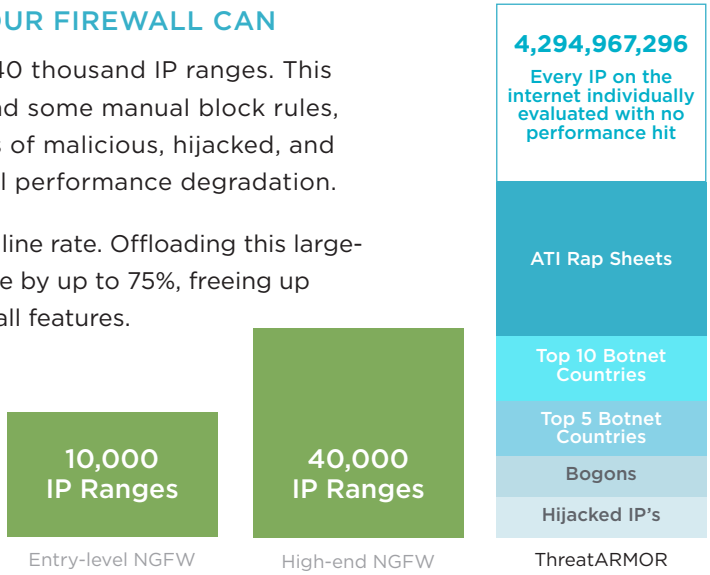
Ixia's ThreatARMOR™ alleviates the work done by your tools by automatically blocking network communication necessary for malware to download instructions or transmit data. Backed by a non-stop threat intelligence feed, ThreatARMOR™ detects and blocks known bad IP addresses, network probes, phishing clicks, and traffic from untrusted countries, reducing the risk of attacks such as zero-day ransomware mutations. ThreatARMOR™ can block up to 80% of malicious connections that threaten the network and generate floods of security alerts. This type of massive-scale blocking allows ThreatARMOR™ to offload work from your tools so that they function quickly and efficiently.



BLOCK MORE IP ADDRESSES THAN YOUR FIREWALL CAN

Next-gen Firewalls can typically block 10 to 40 thousand IP ranges. This is enough to handle a handful of countries and some manual block rules, but not enough to handle the tens of millions of malicious, hijacked, and unregistered IP addresses without substantial performance degradation.

ThreatARMOR™ can block over 4 billion IP's at line rate. Offloading this large-scale IP blocking increases firewall performance by up to 75%, freeing up resources while enabling more advanced firewall features.



Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info