SOLUTION BRIEF

ThreatARMOR: Block Threats, Reduce Your Attack Surface, and Prevent Alert Fatigue

Part of Keysight's Security Operations Suite

Which Security Alerts Do You Choose to Investigate?

On average, it takes a company 280 days to identify and contain a data breach.[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 critical concern for security operations (SecOps). In fact, Cisco reports that only 56% of security alerts are investigated, of which only 34% are deemed legitimate.[2] Because of this, only 51% of legitimate alerts are remediated — comprising a mere 9.7% of alerts overall — leaving a host of open vulnerabilities for attackers to exploit. The large volume of threat alerts is directly linked to the amount of traffic fed to security tools. However, security tools are not optimized to block malicious traffic at massive scale, which causes latency and an overload of false positive alerts. Without the most relevant data, it's much harder for security operations to respond to relevant alerts, investigate attacks, and detect potential breaches.

Highlights:

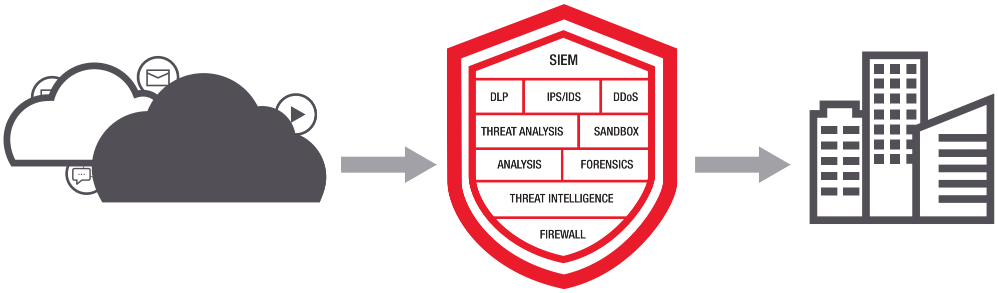
- Part of Keysight's Security Operations Suite of enterprise security tools.
- Minimize SIEM alerts by preventing bad actors from accessing your network.
- Block up to 80% of malicious connections (and over 4 billion IP addresses) without latency or downstream impact.
- Deploy in 30 minutes or less.

[1] IBM Corporation, "Cost of a Data Breach Report", (July 2020).
[2] Cisco and/or its affiliates, "Cisco 2018 Annual Cybersecurity Report," (February 2018).

KEYSIGHT TECHNOLOGIES

A Threat Intelligence Gateway for Your Tools

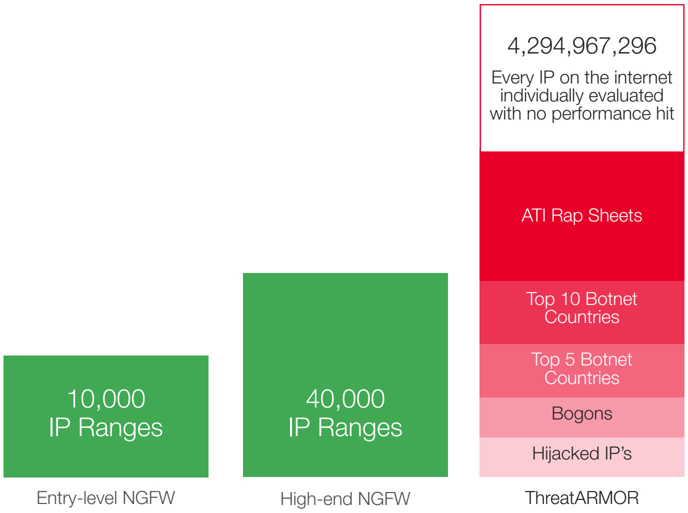
Stop making your tools do all the hard work. Keysight ThreatARMOR™ automatically blocks all network communications necessary for malware to download or transmit data. Backed by a non-stop threat intelligence feed, ThreatARMOR™ detects and blocks known bad IP addresses, network probes, phishing clicks, 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 enables security operations to focus on real threats while helping your tools work faster and more 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.



Keysight Knows Security Operations

Keysight has been in the business of testing and improving network security for more than 15 years. Since 2005, we've helped make the world a safer place by testing some of the most popular security tools on the market — including firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS). At the same time, our Application and Threat Intelligence (ATI) Research Center collects and analyzes threats from across the globe in real time — and is a trusted partner of SecOps teams and top security vendors alike.

That's why we've taken our leadership in network and security test and built a collection of tools for enterprise SecOps teams. Along with ThreatARMOR, Keysight's Security Operations Suite also includes:

- Threat Simulator: a breach and attack simulation platform

Don't wait for attackers. Fight back against alert fatigue and strengthen security operations with ThreatARMOR.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES