FireEye + Keysight – Zero Trust Visibility and Security

Overview

Zero Trust is a response to trends such as cloud adoption, BYOD, and remote work where assets are not located within the well-defined perimiter of an enterprise-owned boundary. No implicit trust is granted to assets or user accounts based solely on their network location or asset ownership. The focus is on enabling secure resources, services and workflows regardless of where those live. Visibility and mitigation of security threats are as important as ever, but the challenge of seeing all potential attacks is heightened due to the decentralized, dynamic nature of Zero Trust deployments. Keysight and FireEye have partnered on a joint solution to ensure complete visibility and security analytics of Zero Trust environments.

Keysight’s Visibility Solution provides FireEye with the data required to conduct its security analytics, whether from on-premise, cloud, virtual, or remote. Such ubiquitous visibility is crucial in Zero Trust deployments since assets are no longer confined to Enterprise boundaries and ownership. FireEye products such as Network Security and Forensics, Email Security, and their Intrusion Prevention capabilities analyze the collected data, feeding it to FireEye Helix Security Platform, which offers a single pane of glass for security analytics from all the tools.

Sample Keysight and FireEye Joint Deployment

- Visualize and analyze security threats regardless of where they occur; on-premise, cloud, virtual, remote
- Stop zero-day, malware and advanced targeted attacks
- Gain visibility into encrypted traffic to find hidden security attacks
- Easily scale deployments while lowering total cost of ownership
- Deploy turnkey solutions inline or out of band
How it works

Keysight visibility solution includes Taps, CloudLens, & Network Packet Brokers which provide aggregation, filtering, and directing exactly the right data to FireEye


Amidst a fast-changing threat landscape, made all the more challenging by recent trends such as Zero Trust architectures, FireEye helps organizations defend their networks against any attack at any stage:

- At headquarters, branch, cloud, and remote locations
- Hidden within inbound Internet traffic or outbound communications
- Exploits targeting Microsoft Windows, Apple OS, or application vulnerabilities

FireEye Security Suite includes:

**FireEye Network Security and Forensics**
An advanced threat protection and breach detection solution with centralized analysis and visibility into the world’s most sophisticated attacks. FireEye Network Security and Forensics helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted, and other evasive attacks hiding in Internet traffic and facilitates efficient resolution of detected security incidents in minutes with concrete evidence, actionable intelligence and response workflow integration.

**FireEye Email Security**
A secure email gateway that comes in cloud- and server-based versions that stops threats with first-hand knowledge of cyber-attacks. The solution blocks malware, phishing URLs and impersonation techniques, leaving attackers no chance to take advantage of users.

**FireEye Endpoint Security**
Provides comprehensive endpoint defense using multiple protection engines, combined with customer deployable modules to block malware and exploits, detect advanced attacks, and provide response tools and techniques developed by the world’s leading frontline responders.

**FireEye Helix Security Platform**
A SaaS security operations platform that allows organizations to take control of any incident from FireEye Helix is a SaaS security operations platform that allows organizations to take control of any incident from detection to response. FireEye Helix integrates disparate security tools and augments them with next generation SIEM, orchestration and threat intelligence capabilities to capture the untapped potential of security investments.
Keysight Visibility Solution: Enables FireEye Security Analysis

Cybersecurity requires complete visibility from the premise to the data center to the cloud and back. Combining intelligent visibility from Keysight with FireEye creates scalable, reliable access to vital data from your hybrid enterprise cloud network, Zero Trust, and other network deployments. Traffic is delivered to FireEye with the help of and easy-to-use drag and drop interface.

Keysight Visibility Solution includes Taps, Network Packet Brokers, and CloudLens, which collect and aggregate data for all network access points whether on-premise, virtual private network, private cloud, or public cloud. Whether workers are in the office, connecting from home, or accessing resources using the cloud, data collection at both physical and virtual permitters is assured. Keysight features such as SSL decryption can also further expose hidden threats for analysis.

Keysight network packet brokers (NPBs) optimize the use of FireEye Network Security and other monitoring solutions by distributing or “load balancing” traffic to multiple tools to promote rapid scalability and fast response. NPBs can optionally filter out traffic not needed for analysis, or mask fields containing sensitive personal information such as social security or credit card. Furthermore, Keysight can share traffic with other purpose tools that also need access to the data.

Keysight’s external Bypass Switch solutions bring visibility and additional resilience to inline deployments, monitoring the health of inline FireEye appliances and adding failover protection. Bypass sends heartbeat packets to FireEye appliances and automatically re-routes traffic when heartbeats are not returned as expected due to link or power failure, devices being taken out of service for maintenance and other unforeseen events.

Keysight Visibility Solution is tested and proven in joint deployments with FireEye.

About FireEye

Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber-attacks. FireEye has over 10,100 customers across 103 countries, including more than 50 percent of the Forbes Global 2000. www.fireeye.com

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