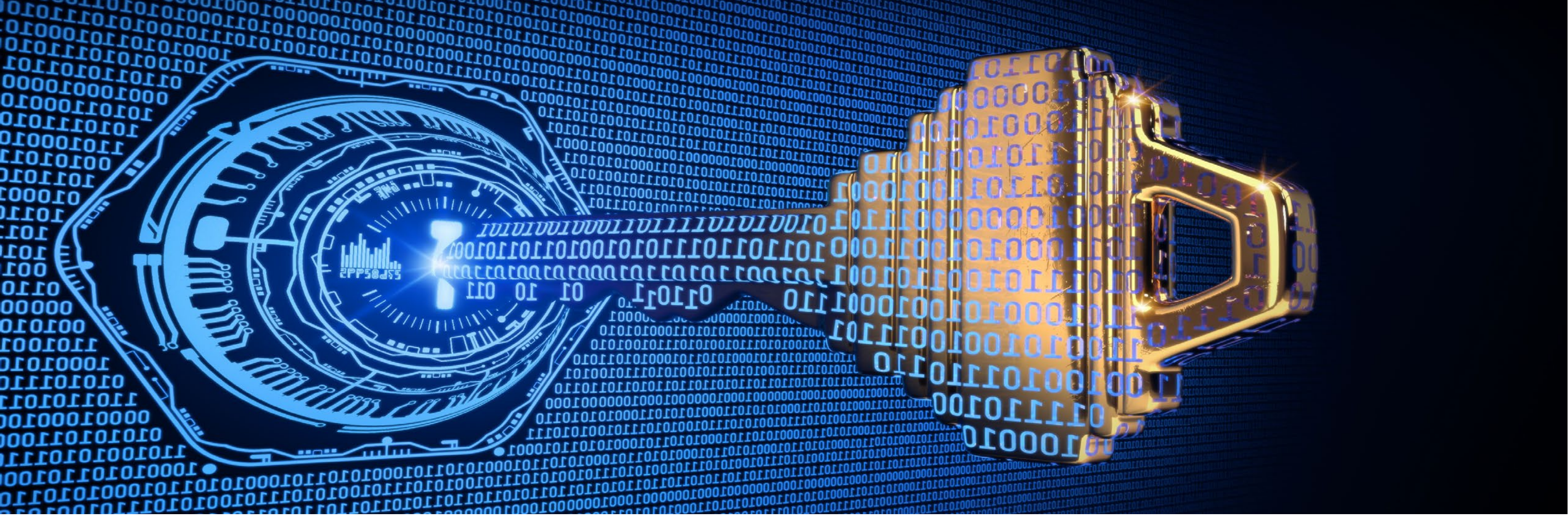

Understanding the Key to Zero Trust Security

If You Can't See the Problem – You Can't Fix It

A visibility architecture is critically important to any zero trust architecture. The reason is simple – you need to be able to see any (and all) security threats to be able to stop them. This isn't just talk. If you can't see when and where a security attack started or be able to see the lateral movements that a piece of hidden malware is making in your network, then your security architecture is going to fail. What you don't know literally can and will hurt you.

Where Do You Start?

While directives like the Office of Management and Budget M-22-09 are intended to focus government agencies on implementing a Zero Trust architecture as fast as possible, you'll need to realize two things. First, you need a solid plan to integrate network visibility along with the zero trust architecture change in philosophy of authenticating anything and everything as agencies move away from the perimeter-based security model to the zero trust model. Neither the CISA Zero Trust Maturity Model nor the M-22-09 call out a visibility architecture directly. However, attempting to implement a zero trust architecture without addressing data visibility will make it difficult to achieve success. This is because you need the underlying visibility features and framework to allow you to secure your data, expose threats, validate the security architecture (which is called out in M-22-09), and implement proper logging practices (called out in the OMB M-21-31 memorandum). Second, plans will probably change some, if not a lot, as you progress along the zero trust implementation path. The important point to understand is the need to design a zero trust architecture flexible enough to allow for change.

A visibility architecture consisting of taps, network packet brokers, and security and monitoring tools. Network packet brokers allow the data capture, filtering, and dissemination of essential agency data and delivery to purpose-built solutions for proper monitoring and analysis. Additionally, taps are a convenient, reliable, and flexible component that can be place anywhere in the network and provide a full copy of relevant and meaningful network data. Network taps provide a 100% copy of the network traffic without the undetectable packet loss sometimes associated with SPAN ports. SPAN ports also force you to collect data from one type of location – layer 2 or 3 switches.

The packet broker then enables you to optimize network data from the taps. Packet broker operation can be in either two forms – inline or out of band. Inline packet brokers allow you to optimize the cost and effectiveness of your inline security solution (intrusion prevention system, web-application firewall, etc.)

which prevents as much bad traffic as possible from entering the network. By using a packet broker and inline security tools you may be able to eliminate up to 80% of security threats right at the edge of the network. You will still need your other Zero Trust architecture components to thwart the different forms of malware that make it past the defensive line.

An out-of-band packet broker is used to filter and eliminate any unnecessary traffic before being sent to other security and monitoring tools like an intrusion detection system or purpose-built threat hunting tool.

How to Fortify Your Network

To implement use cases relevant to government agencies, Keysight Technologies offers a wide range of security solutions including:

- Taps – Includes a vast array of interfaces including copper (10/100/1000 MB) and optical (1/10/25/40/50/100/400 GE). Keysight also has a large portfolio of tap split ratios including 50/50, 60/40, 70/30, 80/20, and 90/10 splits.
- Vision series packet brokers – Supports zero packet loss for full featured, non-blocking monitoring up to 400 GE. Keysight's patented GUI interface is intuitive and easy to use which saves significant programming time and cost.
- Inline Vision series packet brokers – Supports internal high availability as well dynamic load balancing to create cyber resilience with security appliance survivability and self-healing architectures
- SecureStack application – Integrated SSL/TLS decryption for the Vision series packet broker that exposes hidden security threats while removes the inefficient and heavy decryption burden from your security tools
- AppStack application – Provides high-value intelligence features for the Vision series packet broker that delivers empirical data to identify bandwidth usage by application type, flow data, geolocation, and various pieces of user data to look for indicators of compromise and an early warning of potential problems.
- iBypass – external bypass switches that increases your network reliability with superior fail-over and fail-back techniques
- CloudLens – Allows you to capture and filter packet data in public and private cloud networks.
- Threat Simulator – A BAS solution that performs continuous tests of your live network cyber security defenses, WAF, and web policy engines to identify any vulnerabilities. A Recommendation Engine provides easy-to-follow instructions on how to optimally configure your security products to close those gaps and improve security. Recommendations can also be integrated directly to a SIEM.
- Cyperf – Simultaneously generates both legitimate traffic mixes and malicious activities across a complex network of proxies, software-defined wide area networks, TLS inspection, elastic load balancers, and web application firewalls for cloud networks.

Reach out to us and we will show you how to fortify your network against multiple threat vectors.

Learn more at: www.getnetworkvisibility.com/ZeroTrust

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/

KEYSIGHT