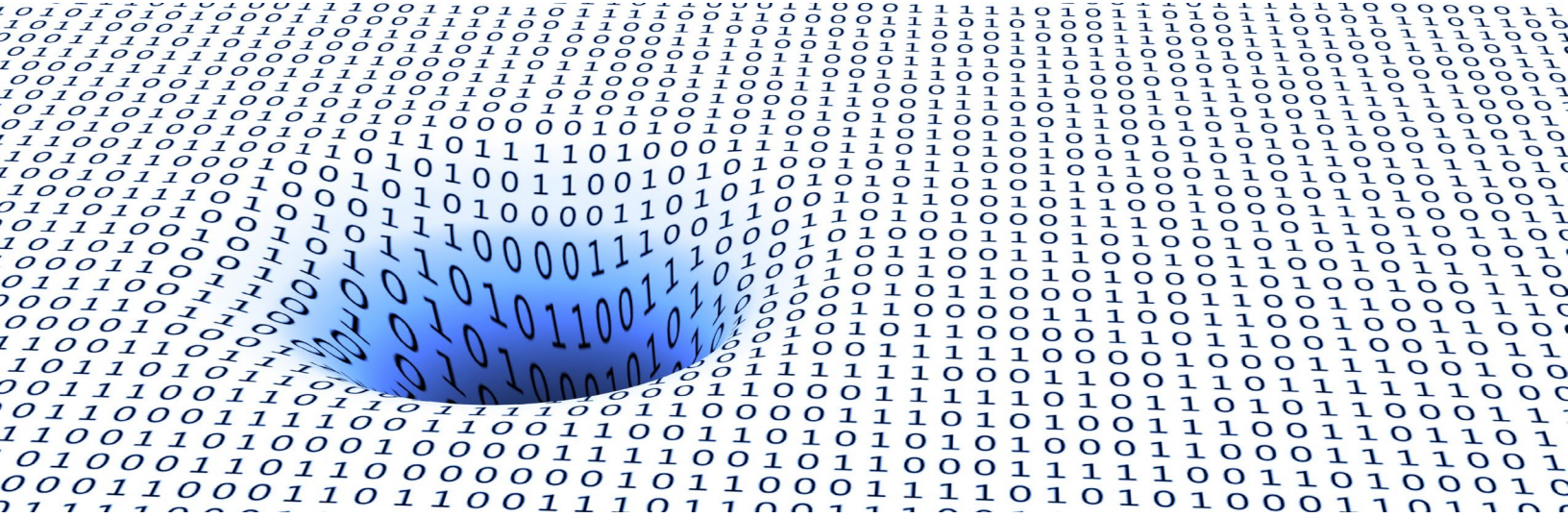

Overcoming Four Zero Trust Deployment Pitfalls

As everyone in the network security field knows, Zero Trust is gaining traction as a favored architecture. It's also being mandated by Executive Order and OMB directives to government agencies. However, Zero Trust is not one set of defined practices — there can be many optional strategies and components involved. In fact, Zero Trust is really a journey. The architecture will shift as you make multiple adjustments to create the "right" level and type of security that your agency, mission or enterprise demands.

However, when designing and implementing your Zero Trust architecture, there are some common factors (pitfalls actually) that can get overlooked or dismissed that will hurt your architecture. Here are four of them.

1 Don't Forget About a Visibility Architecture

For any network security project, network visibility is the keystone. This is because the visibility architecture captures key pieces of data that help secure the network. To expose security threats, the first place to start is to create a visibility architecture that consists of taps (for data collection), a network packet broker (for data manipulation), and purpose-built security tools, like intrusion detection systems (IDS), to examine the data. By integrating this visibility technology into your security architecture, you can clearly see what is (and what is not) happening on your network and implement proper adjustments as needed.

2 You Need Packet Visibility

Packet data will be critical to your security architecture as it can provide a single source of detailed truth. Don't misunderstand. While flow data is good, it only provides general trend information, not actionable details if you want to perform any type of threat hunting. Log data is also useful, but it can be corrupted or even erased by malware. Only packet data gives you all of the details that you need, like: who, what, where, when, and how. The devil truly is in the details. Metadata can never tell the whole story whereas packet data holds the absolute truth.

3 Make Sure to Validate Your Security Architecture

While it may seem obvious to thoroughly test your architecture, many engineers shortcut the process because it either takes too much time, costs too much money, or "just isn't necessary." Unfortunately, security operations center (SOC) teams end up finding out that this reasoning is flawed. The last thing you want is to discover a flaw in your design when your agency network is attacked. Government agencies should consider using test and modeling tools to help them validate the completion of their goals. In addition, validation isn't just required at initial deployment, it's needed all the time. Every change to your network (hardware updates, software updates, minor configuration change to a firewall or intrusion prevention system (IPS), or SIEM, whatever), can affect your network in hidden ways.

4 It's Not Just About Prevention — You Also Need to Respond Quickly

Zero Trust isn't just about defensive security. Government agencies should be especially concerned about security breaches and ransomware in the current geopolitical climate. Attacks could come at any time. Therefore, you need to implement offensive components as well. This means implementing both threat hunting capabilities to actively look for threats on the network and cyber resilience mechanisms to quickly mitigate and remediate the effects of a successful attack.

Whether you are looking to enhance your Zero Trust architecture or achieve M-21-31 / M-22-09 compliance, Keysight is here to help. We have various network visibility and network security solutions for both NIST and CISA compliance.

Reach out to Keysight Technologies and we can show you how to optimize your security solutions.

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/