WHITE PAPER

What You Need to Know for a Successful Zero Trust Security Deployment

Trust No One, Verify All

The Zero Trust (ZT) model of security is increasingly being adopted by enterprise and government security teams, and with good reason. Perimeter focused security architectures that default to high trust levels on internal networks are ill suited for today's edgeless enterprises that increasingly support mobile and remote workers as well as large numbers of IoT devices. Zero Trust is typically associated with network segmentation, as a way to concentrate granular security controls and manage attacks. But Zero Trust is far more than just segmentation.

Zero Trust Is a Team Sport

There isn't a single Zero Trust solution. The architecture is composed of numerous components, that when taken together, form a new approach to address today's cyberthreats. The good news is that you can leverage many of the cybersecurity tools you already own within an overall Zero Trust framework. For example, next-generation firewalls (NGFW), security information and event management (SIEM), and asset discovery tools. However, it is vital to be sure that these security tools are deployed and used correctly in two important ways.

- Do they have the full network visibility they need to detect threats?
- Can you automatically validate that these tools are detecting and stopping the threats correctly?

Framework for Zero Trust

Forrester Research has created a framework called the Zero Trust Ecosystem. The framework contains seven pillars as follows:

1. Network – the ability to segment, isolate and control the network
2. Data – secure and manage the data, categorize and encrypt data both at rest and in transit
3. People – secure the people using the network and business infrastructure

Have You Verified Your Zero Trust Deployment?

Do your security tools really have the visibility they need to detect and mitigate threats?

Can you validate that your Zero Trust solution is configured correctly and working as planned?

Are you maximizing the value of your security investments?

KEYSIGHT TECHNOLOGIES

4. Workload – secure cloud networks, apps, and other things used to make businesses operate
5. Devices – isolate, secure, and control all devices accessing enterprise resources
6. Visibility and Analytics – provides useful analytics and data points for correlation
7. Automation and Orchestration – automate Zero Trust elements and provide more control of disparate systems

A ZT approach leverages an ecosystem of different security tools and processes to be workload-first, data-driven, and identity-aware rather than static and perimeter-based.

The Key to Successful Zero Trust Security Deployments: Visibility & Validation

Tools like NGFW, SIEM, asset discovery, end point detection (EDR) all play an important part in your cybersecurity framework. But are you sure that these tools are getting all the data they need to do their jobs? And are you also sure that they have been implemented and configured correctly? It is recommended that the Zero Trust mindset must apply to visibility to your security tools and then validation that these tools are working correctly.

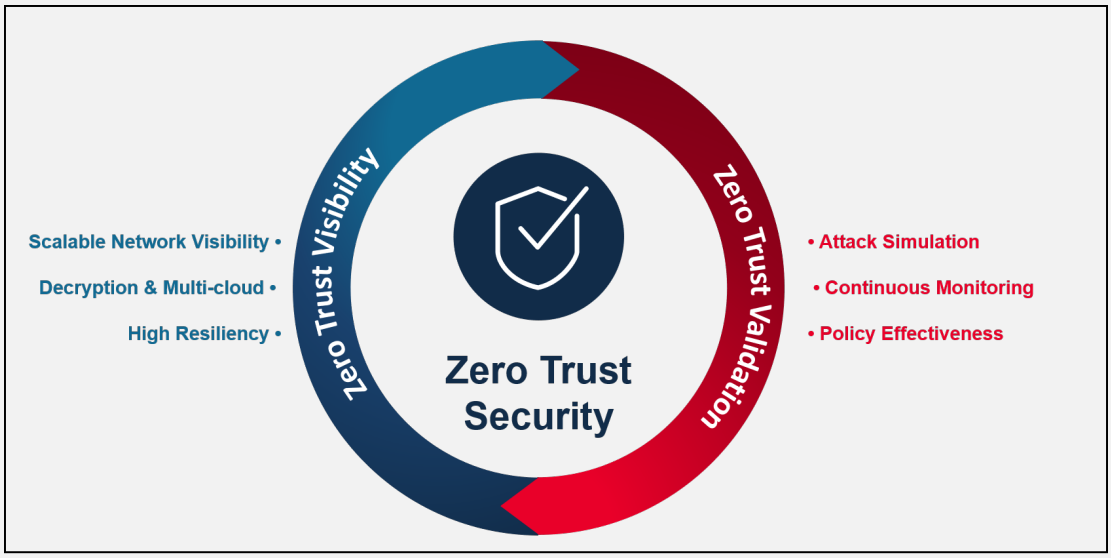

Figure 1. Zero Trust Visibility & Validation Lifecycle Solution

Building a robust security infrastructure is only one half of the equation. You must also integrate 'checks and balances' to ensure the effectiveness of your design and the policies built within it. Building and testing your security infrastructure is not a onetime singular event. But rather it should be a continuous process that is ingrained into your security processes. The threat landscape is everchanging and dynamic. Your security practice should be as well, otherwise, you're already at a disadvantage against your cyber adversaries.

Zero Trust Visibility – Are Your Tools Getting the Right Data?

Forrester Zero Trust emphasizes the importance of visibility. “Visibility is the key in defending any valuable asset. You can’t protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the tell-tale signs of a breach in progress and to stop it. Zero Trust mandates significant investment in visibility and analytics across the business — regardless of location or hosting model.”

Many security tools ingest network traffic (packet data) as their primary data source to detect and prevent threats. These security solutions include: NGFW, web application firewalls, asset discovery solutions, sandbox solutions, forensic recorders and intrusion prevention/detection solutions (IPS/IDS). Network data provides the granularity needed to detect many threats that log data cannot. And unlike logs, packets cannot be manipulated by hackers to cover their tracks. Network based security solutions also have the benefit of not requiring agents to be deployed and managed.

In short, network data is the most detailed and comprehensive data source for cybersecurity. And network-based security tools compliment log based SIEM solutions and agent-based end point protection (EDR) tools.

Network Visibility Challenges

Although network traffic is a critical data source for Zero Trust visibility, todays modern networks make it challenging to provide security tools the packet data they need. These challenges are driven by two key factors:

- Network Scale
  - Increasing network speeds – Networks are increasing from 10G to 40/100G and this can overwhelm security tools capacity.
  - East-West traffic – It is no longer adequate to deploy tools at the perimeter and the spine of the network. As part of a Zero Trust architecture, lateral traffic (East-West) must also be monitored to detect and block threats that have gotten through the perimeter. A whopping 80% of typical enterprise traffic is East-West.
  - Limited budgets – Most companies do not have budgets to upgrade all their security tools to keep up with the increases in network speeds and the growing tsunami of East-West traffic.
- Network Complexity
  - Data encryption – Encryption is a key tenant of Zero Trust and over 85% of traffic is encrypted today. However, many security tools are unable to inspect and analyze SSL/TLS encrypted traffic creating a critical blind spot.
  - Cloud – Hybrid cloud deployments that cross multiple public clouds and on-premise data centers are increasingly common. However, accessing packets across multiple public cloud platforms (Amazon Web Services (AWS), Microsoft Azure, Google Cloud, etc.) is a significant challenge.
  - Virtual blind spots – Virtual East-West traffic between VMs in a private cloud often never leaves the server it is hosted on. As a result, this traffic cannot be monitored from a physical network SPAN port or tap. Since so much of Zero Trust focuses on detecting lateral movements in the kill-chain, this is a large visibility challenge.

Visibility Best Practices for Zero Trust

Implementing a visibility architecture solves the above visibility challenges and is a best practice for Zero Trust. An intelligent visibility solution provides security and monitoring tools with fast, easy access to all required traffic from your hybrid IT environment — networks, data centers, and private and public clouds. A well-constructed visibility solution uses taps to capture and send traffic to an out-of-band network packet broker (NPB) where it is aggregated and filtered. The NPB then passes the traffic to your security and monitoring solution so it can cost effectively analyze the relevant data needed from anywhere in the network.

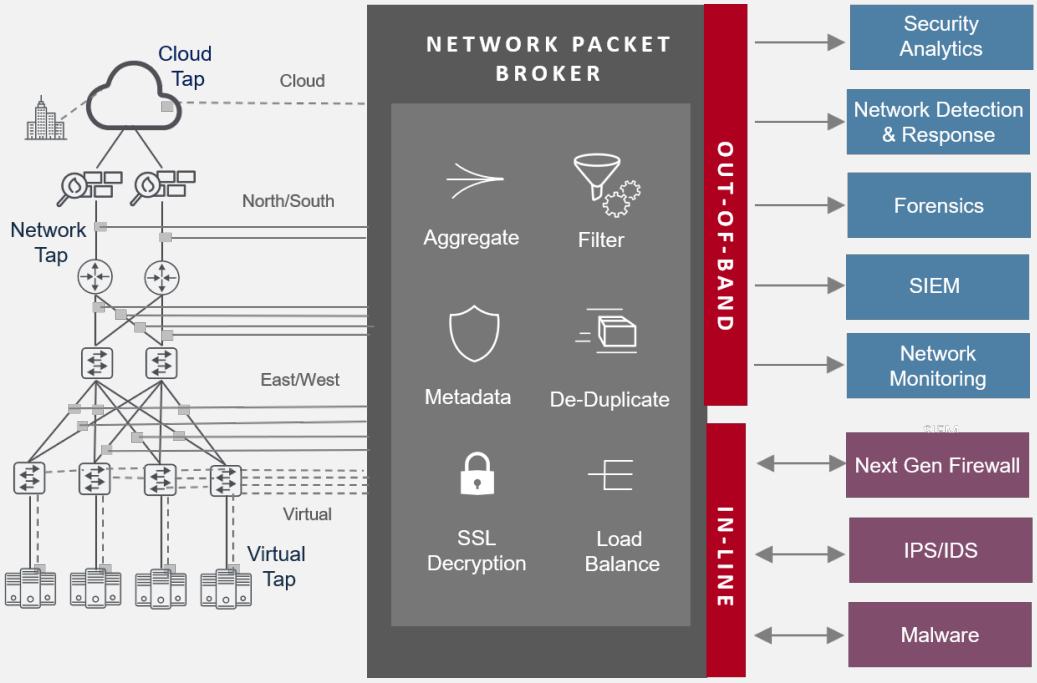

Figure 2. Best Practice Visibility Architecture

Benefits include:

- Complete, easy access - NPBs aggregate and process traffic from multiple virtual or physical taps (or SPAN ports) placed throughout your data center or cloud network
- Ability to scale & optimize tool resources - NPBs filter out unwanted data (duplicate packets and unnecessary data) and load balance traffic across multiple out-of-band monitoring tools to extend their use and value
- Active SSL decryption – encrypted traffic can be de-crypted for tools to inspect and then re-encrypted to maintain Zero Trust best practices

- Complete East-West visibility – both virtual or physical east-west traffic can be accessed and sent to analytics tools to detect/block lateral threat movements
- High resiliency for micro-segmentation – bypass switches eliminate single points of failure and allow tools to be maintained or upgrade without taking down the network
- Public cloud visibility – multi-cloud support for AWS, Microsoft Azure, Google, including Kubernetes deployments
- Cost savings – payback is often under two years due to reduction in tools required

Zero Trust Validation – Are Your Tools Configured and Working Correctly?

Many companies adopt Zero Trust practices to protect their valuable data, but then have no way to validate that their security investments and practices are actually working together as planned to detect and prevent breaches. As mentioned earlier, Zero Trust is a team sport. But how can you verify the different components (NGFW, EDR, SIEM…) are configured correctly? For example:

- Are the right signatures installed on internal E-W firewalls?
- Are the right log messages from cybersecurity tools reaching the SIEM and being alerted upon correctly?
- Does your Zero Trust network segmentation have any gaps that that are allowing unauthorized access?
- Have misconfigurations caused by human error compromised my security? In fact, according to Ponemon, nearly half of all breaches stem from human error, system glitches, and misconfigurations. (Cost of a Data Breach Report. Ponemon / IBM, 2019)

Traditionally, issues like these have been addressed with penetration testing and red teams that actively try to get past a production network's defenses. However, this approach is high risk (because the attacks could damage the production network) and provides insights from a single point in time only.

Another approach is vulnerability scanning tools that scan networks and applications for known weaknesses. While this approach does not pose any kind of risk, its effectiveness is significantly more limited. Since the results of these scans may be thousands of pages long and don't always contain remediations, SecOps teams are often unable to take comprehensive action.

Neither of these two traditional approaches meet the key Zero Trust tenant of automation and orchestration discussed earlier. The validation of security needs to be done in an automated way, and provide remediations, not just a list of problems. A better approach is the use of breach and attack simulation (BAS) solutions.

Breach and Attack Simulation – Validate, Don't Trust

Once you have your security architecture in place, a BAS solution can immediately test your security defenses. This test is an incredibly important activity. Numerous studies about network breaches over the last 10 years have proved one thing for sure — your network will be tested for weakness by a hacker at some point in time. Therefore, either you test it first, or they will test it for you. It is your choice, but the legal and financial consequences should be far less devastating if you test the defenses first.

BAS tools enable users to send relevant, targeted attacks from an untrusted zone to container-based software agents deployed within protected zones. By performing automated assessments, SecOps

teams can readily assess critical security solutions in their production networks — such as NGFWs, web application firewalls (WAFs), and data loss prevention (DLP) solutions. Moreover, should inline security solutions fail to mitigate a simulated attack, the tool will immediately alert SecOps teams to the vulnerability.

Simulated attack categories include the following:

- malware and spear-phishing campaigns
- data exfiltration
- cross-site scripting
- database exploits (such as SQL injections)
- advanced persistent threats

This is a valuable service on its own, but some tools go a step further. Upon discovering a vulnerability, BAS platforms such as Keysight's Threat Simulator also include step-by-step remediation instructions. This way, security teams get more than a notification of a potential problem — they receive actionable intelligence that empowers them to close whatever gaps they find.

Your BAS solution should perform the following tasks:

- malware and spear-phishing campaigns
- data exfiltration
- Recommend specific remediation actions to close any identified gaps
- Generate alerts that can pass on to your SIEM solution to close the validation loop from both prevention and alerting perspectives

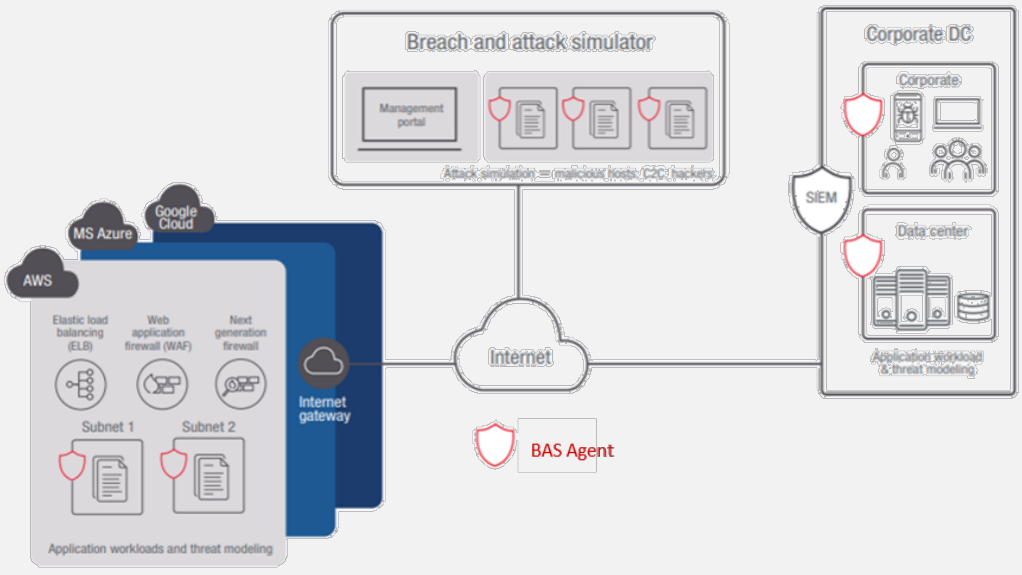

Figure 3. Overview of Breach and Attack (BAS) Solution

The benefits of validating your Zero Trust architecture with a Breach and Attack Simulation solution are many, including:

- Validate the cybersecurity effectiveness of live networks – all the time
- Improve the effectiveness of your existing security tools, before investing in more tools
- Quickly identify misconfigurations and policy gaps
- Analyze detection & blocking capabilities

Putting it All Together – Complete Lifecycle Approach to Zero Trust

No matter where you are in your Zero Trust journey or what specific security tools are part of your cybersecurity architecture, it's important not to overlook two key underpinnings of Zero Trust solution:

- Visibility – Be sure that that your security tools get all the data visibility they need.
- Validation – Once armed with the right data, continuously and automatically verify that your security architecture is detecting and blocking threats as planned. Right size your investment in security tools and identify misconfigurations that can compromise your Zero Trust strategy.

Contact Keysight to learn how our visibility solution portfolio and breach and attack simulation solution can seamlessly interoperate with your entire security infrastructure to provide the visibility and validation to make your Zero Trust journey a success.

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