TITANIA | Use Case

Nipper Resilience: Zero Trust

An introduction to Zero Trust for NOC and SOC teams

In answer to the rise in cyber attacks on critical national infrastructure, in 2021 President Biden set the expectation for all federal agencies to implement Zero Trust architecture (ZTA) within their networks. In January 2022, the Office of Management and Budget (OMB) then released a memorandum setting forth the requirement for federal agencies to meet certain implementation deadlines. But it is not just Federal agencies that are looking at Zero Trust architecture as a way of improving the security of their networks. According to a recent KPMG study, 80% of organizations across other sectors now plan to embrace a Zero Trust security strategy.

But what is Zero Trust and how can it be achieved?

Put simply, Zero Trust assumes you have been breached, so you can no longer trust and therefore need to verify that all users, devices and applications are compliant with mandated policies, every time they connect to the network.

The National Institute of Standards and Technology (NIST) defines Zero Trust as the concept of minimizing uncertainty in enforcing accurate, least privilege perrequest access decisions in a network that is viewed as being compromised. A Zero Trust paradigm requires network owners to address each asset individually and ensure it operates within security and compliance policy requirements.

Network managers need to continually assess all devices rather than assume they are in a secure state, or at least check security and compliance as and when configurations change. Verifying rather than trusting that devices maintain a secure configuration is a key Zero Trust principle and one that progressive frameworks like PCI DSS 4.0 are now adopting. Unintentional configuration drift can expose the network and make it vulnerable to attack, and must be mitigated as a priority.

> "Zero Trust is a cybersecurity strategy developing an architecture that requires authentication or verification before granting access to sensitive data or protected resources at a financial cost by reducing data loss and preventing data breaches. This security model eliminates the idea of trusted networks, devices, personas or processes, and shifts to multi-attribute and multi-checkpoint based confidence levels that enable authentication and authorization policies under the concept of least privileged access."
>
> **Source:** Department of Defense (DOD), Zero Trust Reference Architecture, Version 1.0, February 2021

> **"...the average cost of a breach was USD 1.76 million less at organizations with a mature Zero Trust approach, compared to organizations without Zero Trust."**
>
> Source: IBM's Cost of Data Breach Report, 2021

Organizations should have zero tolerance for not adopting Zero Trust, meaning it needs to be an absolute must for network managers, for organizations and partners.

Although achieving Zero Trust should not be seen as a binary action, rather it is a journey to improve the security and compliance posture of a network and will take time to complete with various stages of maturity. This time to implement should not put organizations off from starting. Particularly when considering IBM's Cost of Data Breach Report, 2021 which found that "the average cost of a breach was USD 1.76 million less at organizations with a mature Zero Trust approach, compared to organizations without Zero Trust."

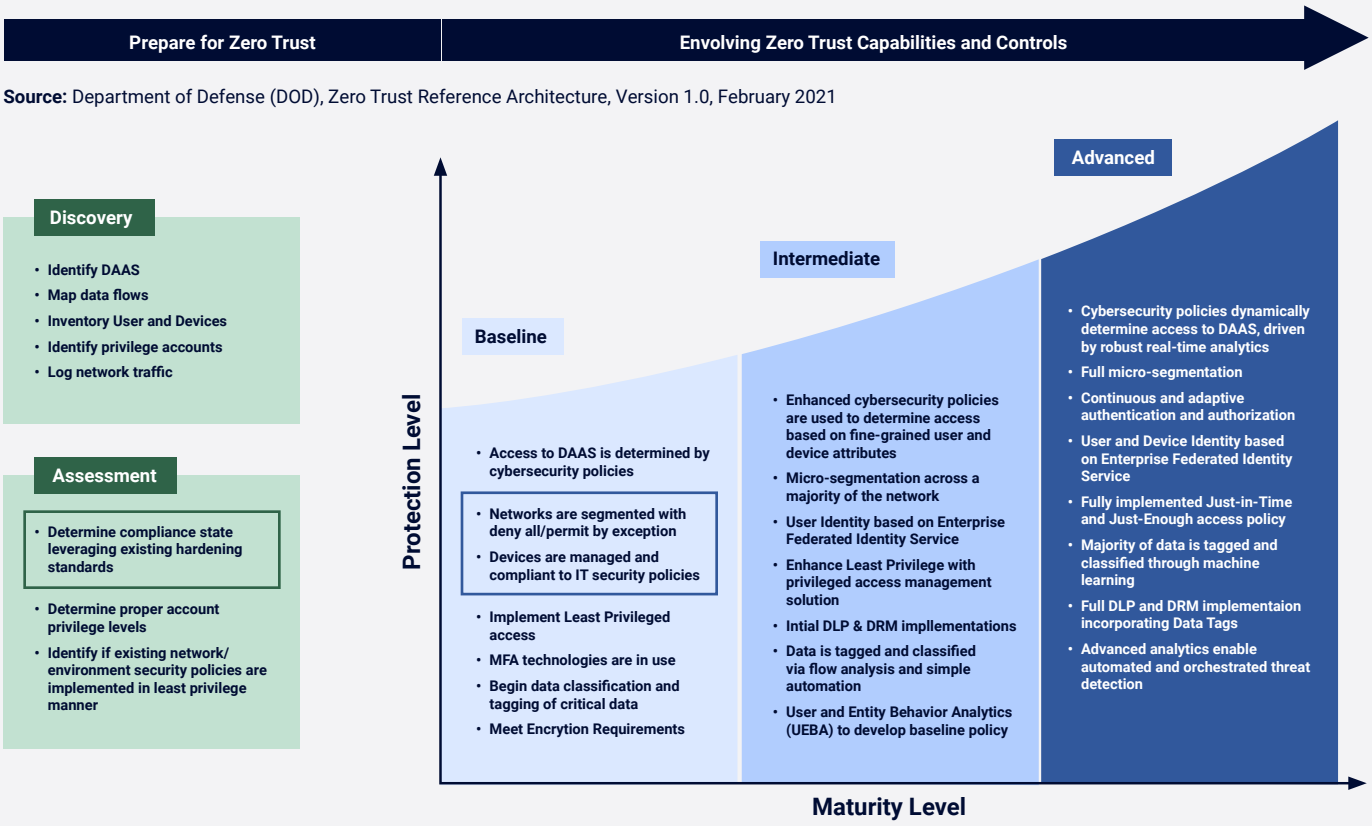
Zero Trust Maturity Model

There are five major tenets of Zero Trust identified in the DoD's Zero Trust Reference Architecture:

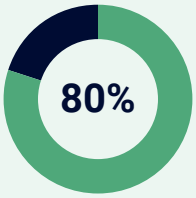
- **Presume breach**
- **Never trust, always verify**
- **Scrutinize explicitly**
- **Apply unified analytics**

As part of this architecture, the Zero Trust Maturity Model has been established, showing five distinct stages of maturity, starting with preparedness, and then moving towards evolving capabilities and controls.

Here, Zero Trust is not shown as a single technological solution, but an evolution of capabilities and controls that starts with identifying and assessing the current status before evolving capabilities and controls in order to develop Zero Trust maturity, moving through the levels from baseline to advanced.



Source: Department of Defense (DOD), Zero Trust Reference Architecture, Version 1.0, February 2021



It is not just Federal agencies that are looking at Zero Trust architecture as a way of improving the security of their networks. According to a recent Market Dynamics Survey, 80% of organizations across other sectors now plan to embrace a Zero Trust security strategy.

How Nipper and Nipper Resilience can work towards Zero Trust Maturity

Whilst Zero Trust is as much of a mindset, as it is a technology and process, the highlighted areas in the previous diagram show how the use of Nipper and Nipper Resilience can support businesses on their road to Zero Trust maturity.

Nipper and Nipper Resilience are designed to provide network owners with full visibility of misconfigurations in their network devices, complete with risk prioritized remediation recommendations.

Where other tools focus on firewalls only – Nipper and Nipper Resilience automate the accurate assessments of switch and router security and compliance as well. These devices are especially important for Zero Trust, which assumes the perimeter has been breached. Furthermore, as 80% of all network traffic is inside the perimeter, switches and routers, when configured correctly, play a fundamental role in preventing lateral movement across the network.

If compromised, firewalls, switches and routers potentially pose a critical risk to the confidentiality, integrity and availability of data, systems and services. Verifying that they remain secure, every day, or every time their configuration changes, is simply not achievable with legacy automation systems that have inherent issues with accuracy because of methods of analysis - and they do not scale.

The only way to accurately detect misconfigurations in firewalls, switches and routers, is to analyse the device configuration as a single entity to consider interdependencies across the network. Nipper automates this analysis, and in doing so, provides a granular level of detail to determine the impact to the network if the misconfiguration is exploited, how easy it is to exploit the issue, and the time required to remediate the risk. Nipper reports then automatically prioritize remediation recommendations based on risk, allowing network professionals to update their mitigation workflows accordingly.

As part of the assessment phase for Zero Trust maturity, Nipper can help also assess the compliance state of firewalls, switches and routers, discovering any vulnerabilities, identifying where configurations drift away from a secure and compliant state, and recommending how to mitigate the risk to improve the compliance posture of the network.

Nipper Resilience gives NOC, SOC and Incident Response teams the real-time information they need to assure critical networks are ready to defend against industry-specific attacks, resilient to innocent accidental errors, and quickly recoverable in the event of a disruption or disaster. Nipper Resilience is now providing a risk-focused approach to misconfiguration detection and remediation that is accurate, timely, and scalable – an essential capability for companies committed to Zero Trust security.

About Titania

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally.

Whether organizations need real-time visibility and analysis of every network change to get ahead of threats, segmentation violations, and potential network disruptions. Or scheduled network posture and device vulnerability assessments to enhance attack surface security and demonstrate compliance. We have a solution for every stage of the journey to network readiness and resilience.