Deep Observability is Foundational to Zero Trust

Gaining complete visibility into the network is like lighting up the whole street. When it comes to implementing Zero Trust, this is the best place to start.

JOHN KINDERVAG
Zero Trust and Importance of Network Visibility, 2023.

Why is Deep Observability Foundational to Zero Trust?

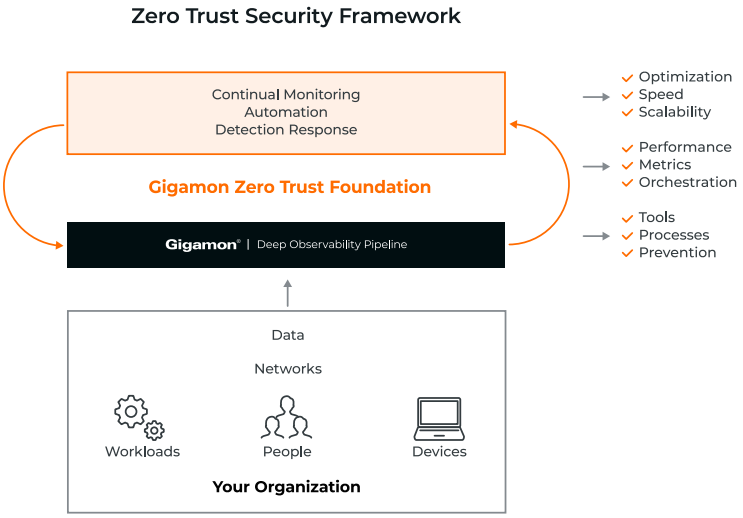
The major Zero Trust models and NIST SP 800-207A *(A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments)* identify network visibility as a critical aspect of Zero Trust success. Among the many reasons for this:

- Network visibility is essential for understanding the current state and security of the network, whether it's on-premises, in a private or public cloud, or across a hybrid cloud infrastructure
- When an endpoint or workload is compromised, log-based telemetry from that asset can no longer be trusted, whereas network visibility provides immutable telemetry
- BYOD and IoT devices, as well as OT systems, often cannot support agent-based security, leaving these endpoints unmonitored and exposed to compromise

Deep observability is essential to identify threats and arm your security tools with the data they need to safeguard the network and accelerate your progress toward Zero Trust. Gigamon provides deep observability, not just for the network pillar of the Zero Trust model, but also the data and application layers.

How the Gigamon Deep Observability Pipeline Enables Zero Trust

The Gigamon Deep Observability Pipeline provides complete visibility into all network traffic, whether from on-premises, private, virtual, container, or public cloud environments. Critically, this includes visibility into lateral (East-West) traffic and activity between virtual machines and containers. Gigamon also provides visibility into encrypted traffic using both highly efficient central decryption and our ground-breaking Gigamon Precryption™ technology. After acquiring network traffic, Gigamon transforms, optimizes, and distributes traffic to the security tools enforcing your Zero Trust policies.



Case Study

U.S. Department of Defense

In 2019, the National Security Agency, Defense Information Systems Agency, and U.S. Cyber Command began a multi-phase Zero Trust reference architecture project. The top objectives of the project were to apply Zero Trust architecture (ZTA) concepts to establish stronger defenses against unauthorized lateral (East-West) movement, protect against privilege escalation, and eliminate blind spots across the entire network, including on-premises and hybrid cloud infrastructure.

During the initial planning and design process, the project team determined that a scalable, centralized visibility approach was a key requirement for the reference architecture. The Gigamon Deep Observability Pipeline provided a centralized approach for network traffic collection and routing, giving the tools responsible for enforcing ZTA policies the visibility they needed to be effective.

"At first the implementation did not include Gigamon visibility solutions, but midway through, the team determined that the Gigamon Deep Observability Pipeline is critical to tie everything together and provide crucial visibility into the physical, virtualized, and cloud environments."

We ran a test and realized we couldn't see certain events because we weren't inspecting the packets going across the wire. At that point, phone calls were made and we brought Gigamon on.

DAVID JONES
U.S. Department of Defense

Gigamon Deep Observability Benefits for Zero Trust

Eliminate blind spots – Gigamon provides complete visibility into North-South, East-West, container, encrypted traffic, and IoT/OT or BYOD-generated traffic. This deep observability is foundational to Zero Trust success.

Detect lateral movement and internal threats – Endpoint security can be evaded and compromised. When this occurs, Gigamon can observe anomalous user, device, and application behavior, which is critical to detecting security risks and threats.

Enable an "Assume Compromise" Philosophy – Gigamon generates network-derived application metadata that continuously verifies all network activity, including log data, in line with the "assume compromise" Zero Trust philosophy.

Optimize existing tools – Gigamon reduces unnecessary network data sent to SIEM, NDR, and other security tools by 50 to 60 percent using techniques such as de-duplication and advanced filtering, enabling these tools to detect threats more quickly and precisely.

Summary

The Gigamon Deep Observability Pipeline has provided mission-critical capabilities for operationalizing Zero Trust projects, including cloud-based projects.

For more information on how Gigamon is enabling government and commercial organizations to meet their Zero Trust goals, please visit the Gigamon Zero Trust information hub at engage.gigamon.com/zero-trust.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

02.24_01