




1

Safe Harbor Disclaimer

Any forward-looking indication of plans for products is preliminary and all future release dates are tentative and subject to change. Any future release of products or planned modifications to product capability, functionality, or features are subject to ongoing evaluation by Gigamon, and may or may not be implemented and should not be considered firm commitments by Gigamon and should not be relied upon in making purchasing decisions.

2



A Recognized Leader in Deep Observability

The Gigamon Deep Observability Pipeline harnesses network intelligence to amplify the power of security and observability tools.

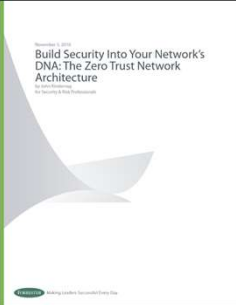
This enables you to assure security and compliance, speed root-cause analysis and lower operational costs for your hybrid- and multi-cloud infrastructures.

5


Evolving Approaches to Zero Trust

12 Years and Counting

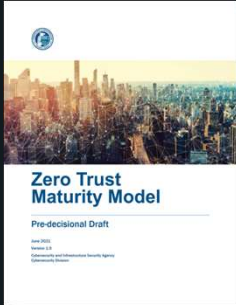
John's Original Paper (2010)



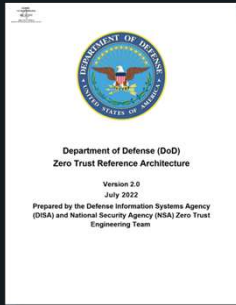
NIST SP 800-207 (2020)



CISA ZT Maturity Model (2021)



DoD ZTA Reference Architecture v2.0 (2022)



Also: Executive Order 14028 (US Government Only)

6

Very Evolving...

- + NIST SP 800-207 is the referenced basis for almost all things which have inherited the "zero trust" moniker
 - + Models/Architectures/Roadmaps/etc... (some formal, some informal)
 - CISA Zero Trust Maturity Model v2 (US civilian agencies and associated entities)
 - DoD Zero Trust Reference Architecture v2 (US DoD and IC)
 - Forrester Zero Trust Model
 - Cloud Security Alliance Zero Trust Standards
 - UK NCSC Zero Trust Model
 - ZTNA and SASE
 - Beyondcorp
 - NSTAC Zero Trust Approach
 - Gartner ZTA Strategic Roadmap
 - Others? Probably...
- Gigamon actively contributes to policy and standards around ZTA.
- See: <https://blog.Gigamon.com>

Gigamon actively contributes to policy and standards around ZTA.

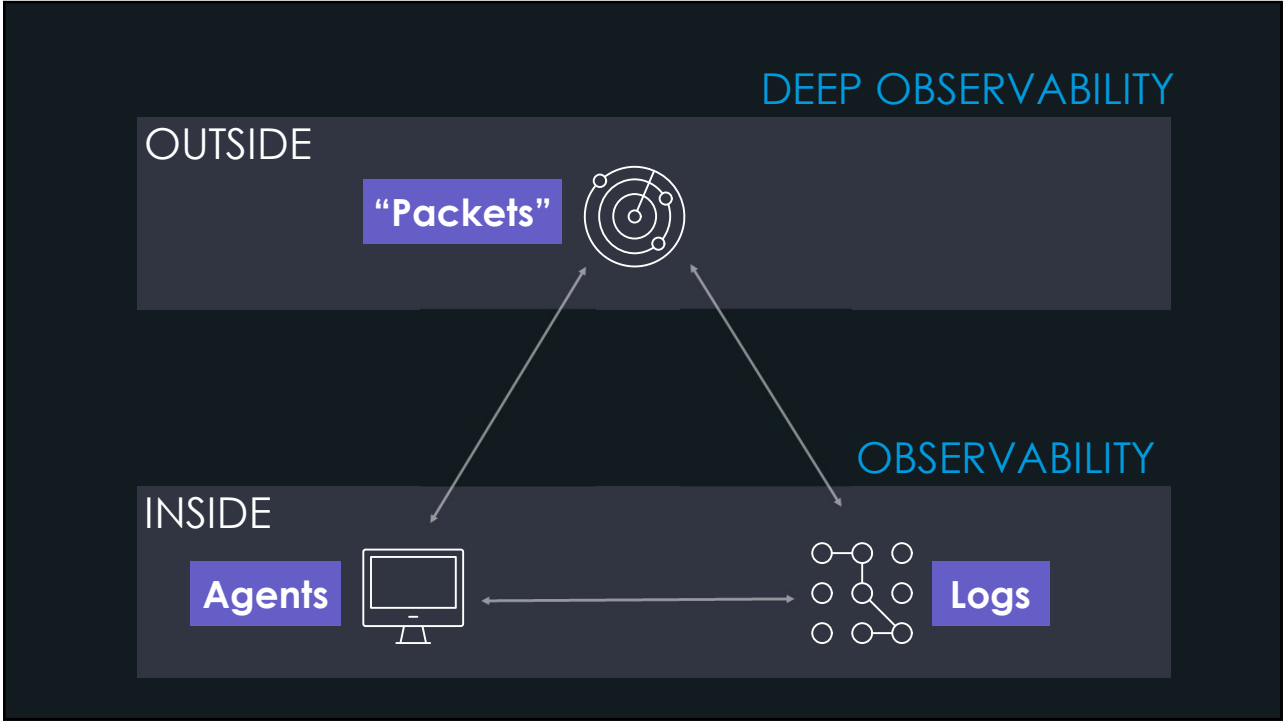
See: <https://blog.Gigamon.com>

7

Just Some General Observations...

- + While the overwhelming number of orgs are pursuing a cloud strategy, the majority will remain hybrid for the medium- to long-term
- + Partial enterprise coverage for ZTA, or islands of non-interoperable ZT infrastructure, will result in non-optimal outcomes
 - This is not to say that any implementation won't be staged in both maturity and environment
 - Complexity: Public cloud, private cloud, containers, SaaS, on-prem/datacenter, industrial, mobile (device), mobile (platform)
- + There is a workload focus inherent in most of the early approaches to ZTA
 - This is a reasonable consequence of moving the control close to the data
 - But denying other approaches, including the network, is unreasonable
 - Heavy focus on logging, without thinking about log assurance
 - Static macro- and micro-segmentation isn't nearly as effective as some ZTA architects think it is
- + There is some major cognitive biases evident:
 - Familiarity bias: "our environment are the bits we're familiar with, and that's all that matters"
 - Confirmation bias: "our data only lives on IT managed workloads/endpoints/devices"
 - Illusory truth effect: A serious over-estimation of the value and efficacy of data classification
 - Optimism bias: A compromised device/workload which doesn't have sensitive data remains a potential risk to the enterprise
- + Supply chain threat modeling still developing

8



9

“The enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not be [sic] able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests.”

NIST SP 800-207, Section 3.4.1(3) “Network Requirements to Support ZTA”, page 21

10

At the log source

- The cyber-relevant event must be noticeable by the "system"
- It must have been anticipated by the code developer
- The code developer must have coded it into the software
- Logging must be configured correctly – with the logging level set to generate the log

In Transit

- The event must be sent from the log source to the log collection system without loss, duplication or modification

At the log collector

- The log message must be ingested successfully
- It must be normalized into a standard informational taxonomy, which is expressive enough to properly represent it
- That taxonomy must allow it to be understood (in isolation or with other messages) to map to the cyber-relevant event
- An alert to a person or system must occur, which allows the event to be managed
- That person or system has to action a process which addresses the cyber-relevant event

11

11

Tracking NS andEW Network Flows in Cloud Environments

Doesn't Seem Very "Cloud Native"

Why do it?

12

12

Network-based ZTA Significantly Simplifies Hybrid Deployments

- + Network traffic is common across all environments:
 - Multi-public cloud
 - Private clouds
 - On-prem
- + Supports applications, workloads and devices which cannot run EDR (or even do logging):
 - Legacy compute (mainframes)
 - IoT/OT/ICS/SCADA etc.
 - BYOD
 - SaaS

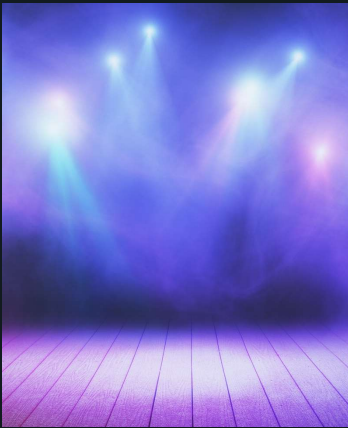


13

Avoiding Telemetry Normalization

Shining a Light on Threats

- + AI/ML approaches to anomaly detection are very important
 - Detecting anomalies is much easier if data from multiple environments all looks the same (does not need normalization)
 - Traffic processed into metadata accelerates AI/ML algorithms
- + All attackers will try evasion techniques, but preventing evasion from the network over time is extremely difficult
 - PE selectively directing in-flight, transparent decryption of TLS traffic is a critical required capability
- + Supply chain attacks and highly sophisticated threats like implants are invisible to logging and EDR, but will be seen from the network



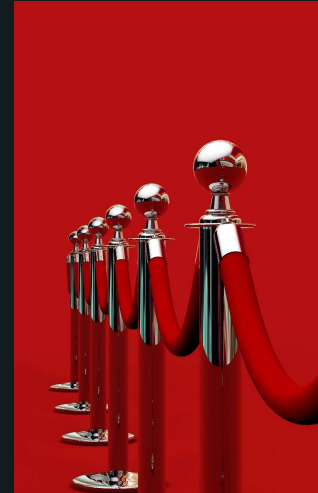
14

Deep Observability is Essential for Macro- and Micro-Segmentation

Reinforcing the Need for Deep Observability

- + Segmentation is required by multiple ZTA standards
 - DoD RA
 - OMB M-22-09
- + Reduces attack surface, degrades attacker lateral movement
- + It's hard to get right in brownfields deployments
 - Typically much easier for cloud deployments
- + Forrester reported:
 - "11 out of 14 customer references tried one of these [segmentation] approaches and did not achieve their desired security outcome."
- + But once you get it right, isn't segmentation enough?
 - I mean, do I really need visibility if an attacker can't move laterally?
 - Yes, you do... as the DoD ZTA pilot showed

Ref: "Best Practices for Zero Trust Microsegmentation", Forrester Research, 27 June 2022.



15

Key Point:

We are not saying do deep observability alone
We are saying do logging and agents and deep observability

Defense in depth is the best
way of driving out implicit trust

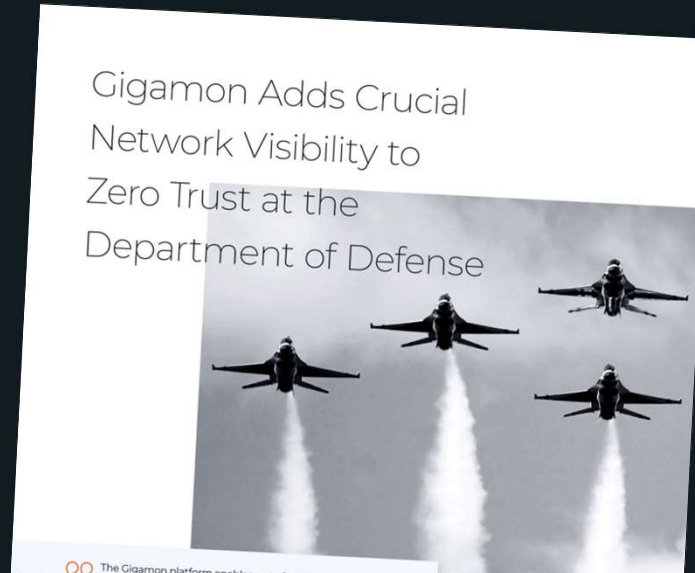
16

Case Study: Department of Defense

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're weren't inspecting the packets going across the wire. At that point, phone calls were made, and we brought Gigamon on," he [David Jones, DoD] says."

Source: <https://www.gigamon.com/content/dam/resource-library/english/case-study--use-cases/cs-department-of-defense.pdf>



17

In Summary

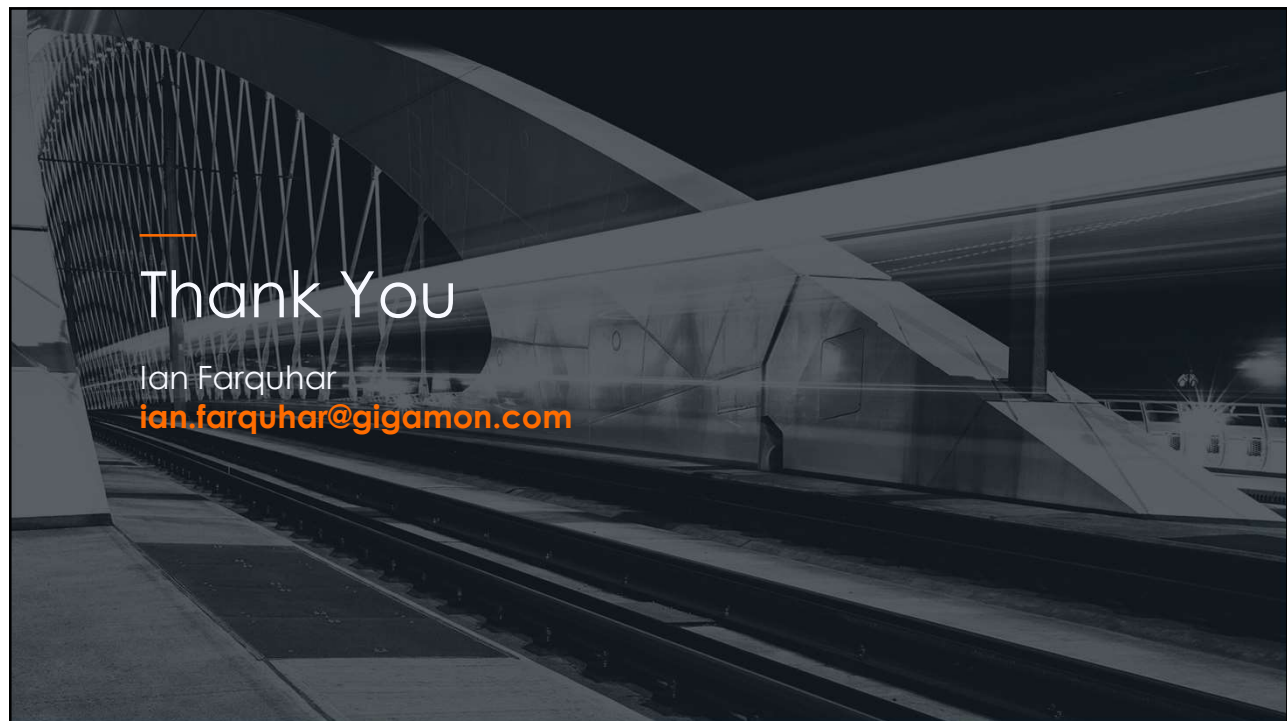
- + Deep Observability (visibility of network flows irrespective of the environment):
 - Provides the PE visibility of lateral movement of risks through the environment
 - Accelerates deployment in multi-cloud hybrid environments
 - Improves data ingest and correlation by AI/ML, improving anomaly detection
 - Makes segmentation easier (possible) to achieve in legacy and brownfields hybrid environments, both before (planning) and during (debugging)
 - Also: where segmentation is implemented on the endpoint, supports detection of evaded agents
 - Stops network segmentation blinding you to potential threats on the segmented network (best of both worlds: constrained but fully visible)
 - Supports devices, applications and workloads which do not log and/or cannot run EDR
 - Supports correlation across logging, EDR and agents detecting successful attacks on those controls
 - Deep observability is extremely difficult to evade
 - Detection of sophistication threats, e.g. below the firmware and supply-chain delivered HW and SW implants

18

Closing Thoughts

- + It is critical that we don't implicitly trust our controls
 - Correlating multiple sources of telemetry is the best way of detecting compromised controls
 - CISA seems to have recognized this in v2:
 - "Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that **automate telemetry correlation across all detection sources**."
- + We need to start thinking about protection of the ZTA infrastructure
 - Especially the policy engine/analytic capability
 - Not only from direct attack, but also "poisoning" of AI/ML/UEBA to evade detection
- + Multi-vendor ZTA is the norm and fundamentally desirable
 - Implicit trust in the vendor? Yes – let's start to have that wider discussion about trust!
 - Vendor community needs to start to work together to build solid interoperability capabilities

19



20