Gigamon Introduction
Secure your ICS-OT infrastructure

Marko Rämö
Regional Sales Director, Nordics & Baltics

Vilnius 8th May, 2024

The World Runs on Gigamon

4,400+
Customers Worldwide

4.7/5.0
Customer Satisfaction

140
Global Patents

83
of the Fortune 100

7
of the Top 10 Global Banks

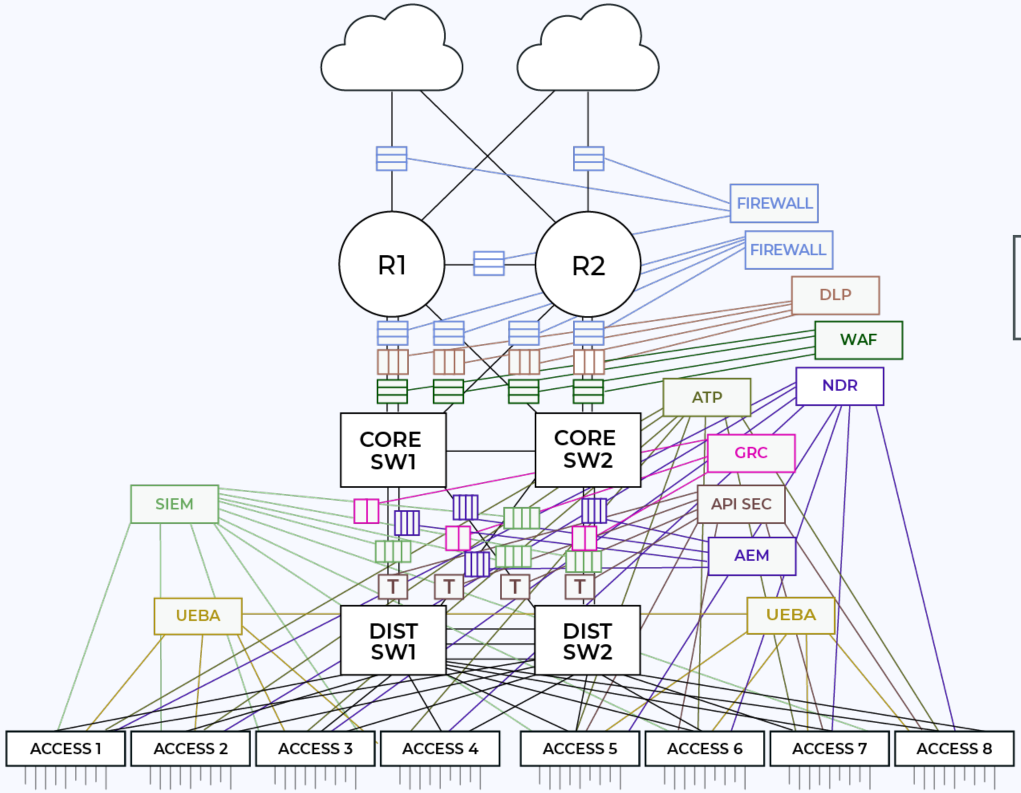
10
of the Top 10 US Federal Agencies

8
of the Top 10 Healthcare Providers

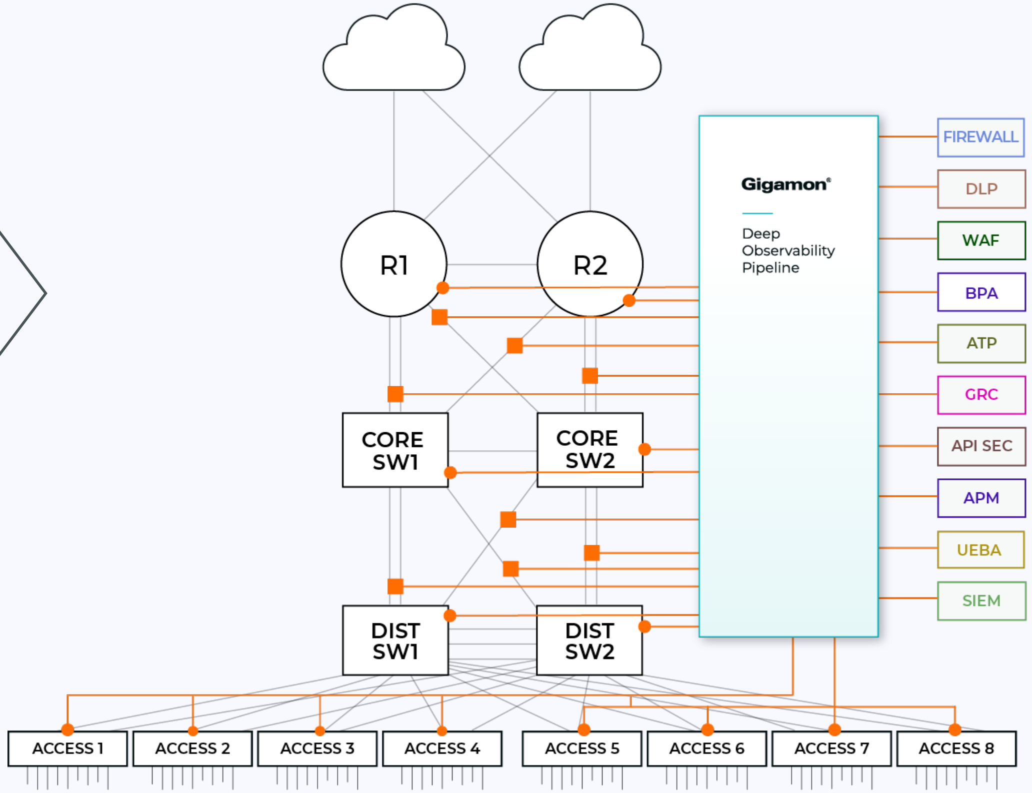
9
of the Top 10 Mobile Network Operators

Gigamon innovation; Reduce complexities, provide visibility

Complexity → Blind Spots, Cost, Inflexibility



Visibility → Security, Efficiency, Agility



Customer Traffic and Cost Savings

80%

REDUCTION

—

in traffic to tools reported by a state and local government entity

50-79

PERCENT REDUCTION

—

in traffic to tools reported by the University of Kansas Health System

80%

REDUCTION

—

in traffic to tools reported by an enterprise telecommunications service

WITH GIGAMON

TOTAL COST SAVINGS

$1,265,800

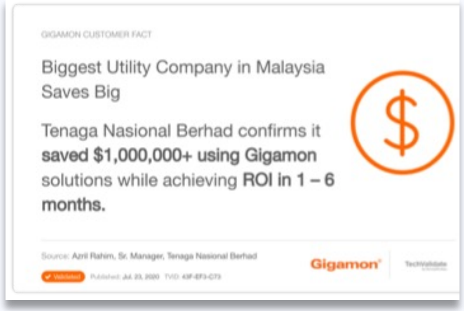
GIGAMON ROI PAYBACK

4 Months

AVERAGE TRAFFIC REDUCTION

50% DEDUP

47% APP INTEL



GIGAMON CUSTOMER FACT

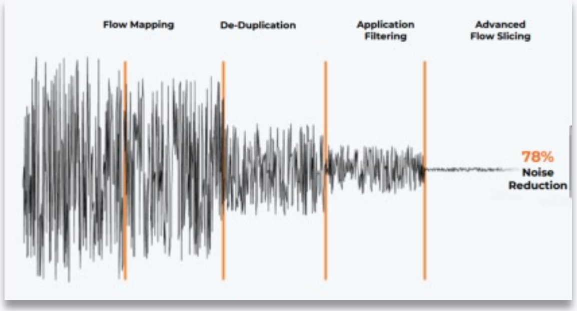
Biggest Utility Company in Malaysia Saves Big

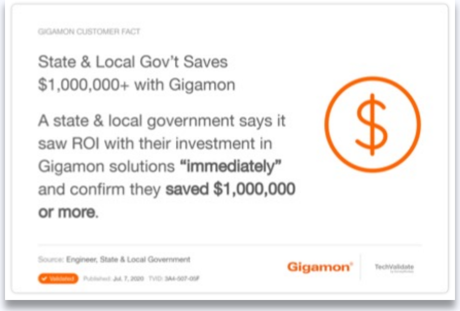
Tenaga Nasional Berhad confirms it **saved $1,000,000+ using Gigamon** solutions while achieving **ROI in 1 – 6 months.**

Source: Azril Rahim, Sr. Manager, Tenaga Nasional Berhad

✓ Validated Published: Jul. 23, 2020 TVID: 43F-EF3-C73

Gigamon® | TechValidate





GIGAMON CUSTOMER FACT

State & Local Gov't Saves $1,000,000+ with Gigamon

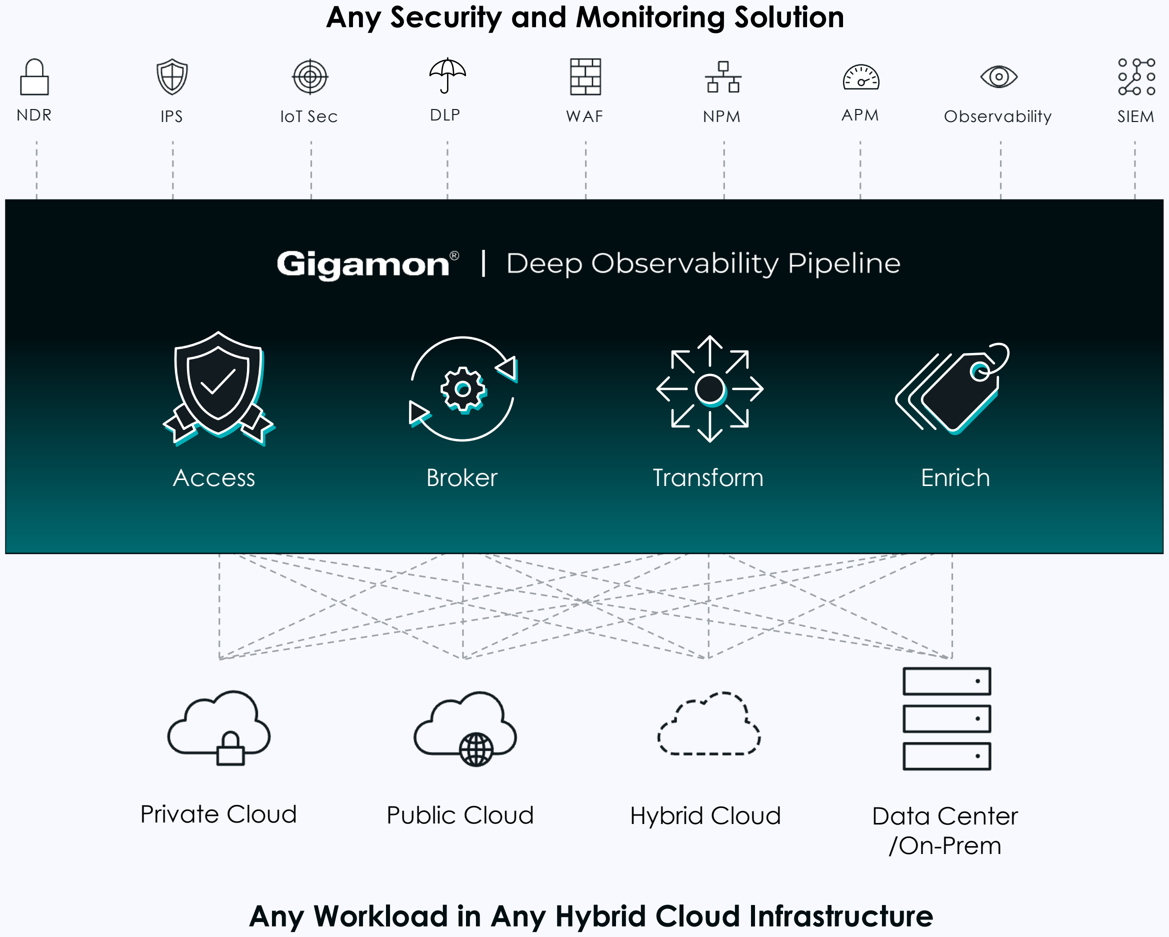
A state & local government says it saw ROI with their investment in Gigamon solutions **"immediately"** and confirm they **saved $1,000,000 or more.**

Source: Engineer, State & Local Government

✓ Validated Published: Jul. 7, 2020 TVID: 3A4-507-05F

Gigamon® | TechValidate

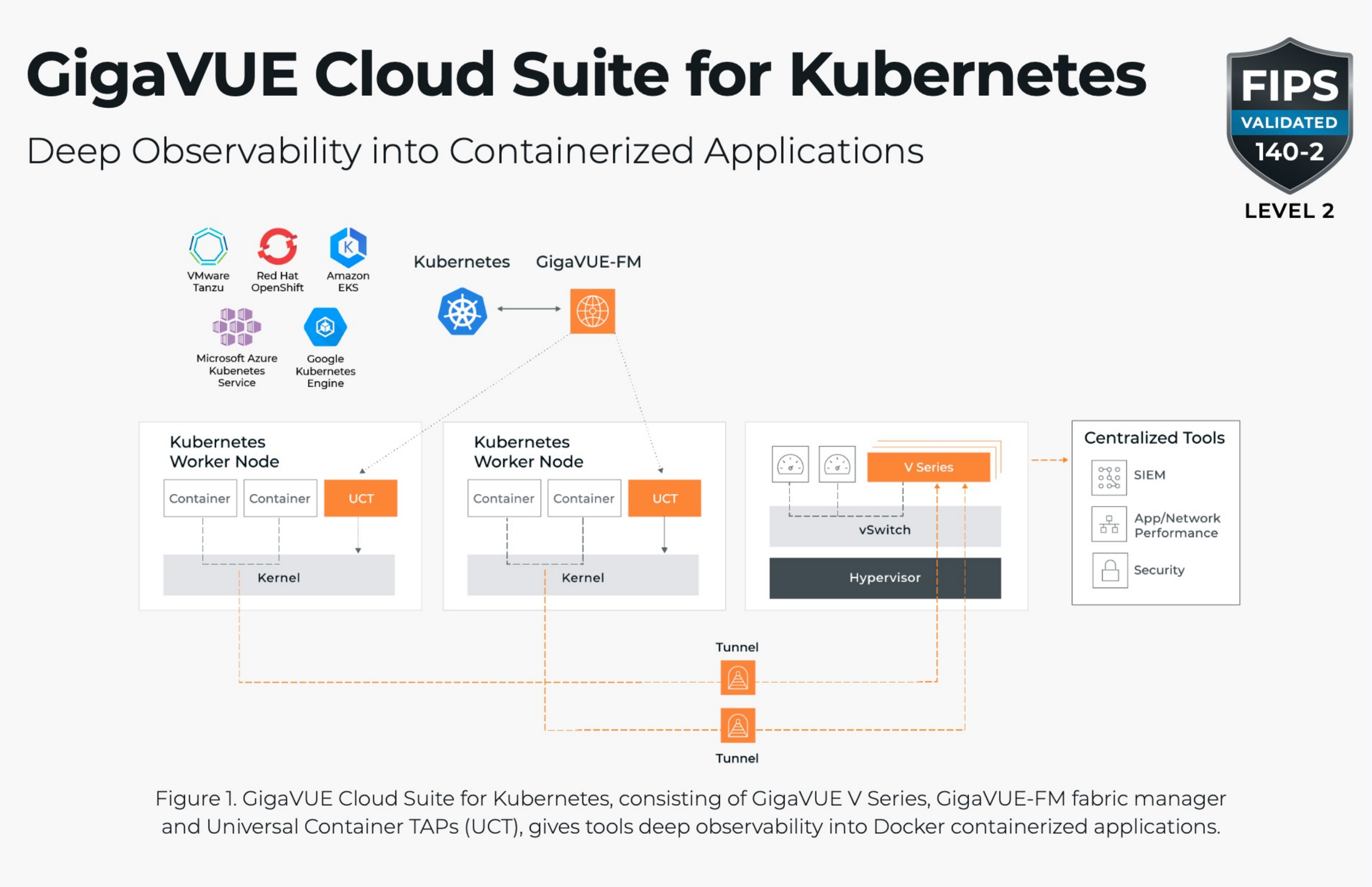
Everything is becoming interconnected: OT & IT, on-prem, hybrid cloud



Key Pipeline Benefits

1. Single access: Physical, virtual, containerized traffic
2. Unmatched insights: Intelligence extraction
3. Single source of truth: Security, performance, and intelligence
4. Cost Savings: Massive signal-to-noise improvement of data to tools

Visibility into containers, East – West Lateral movement

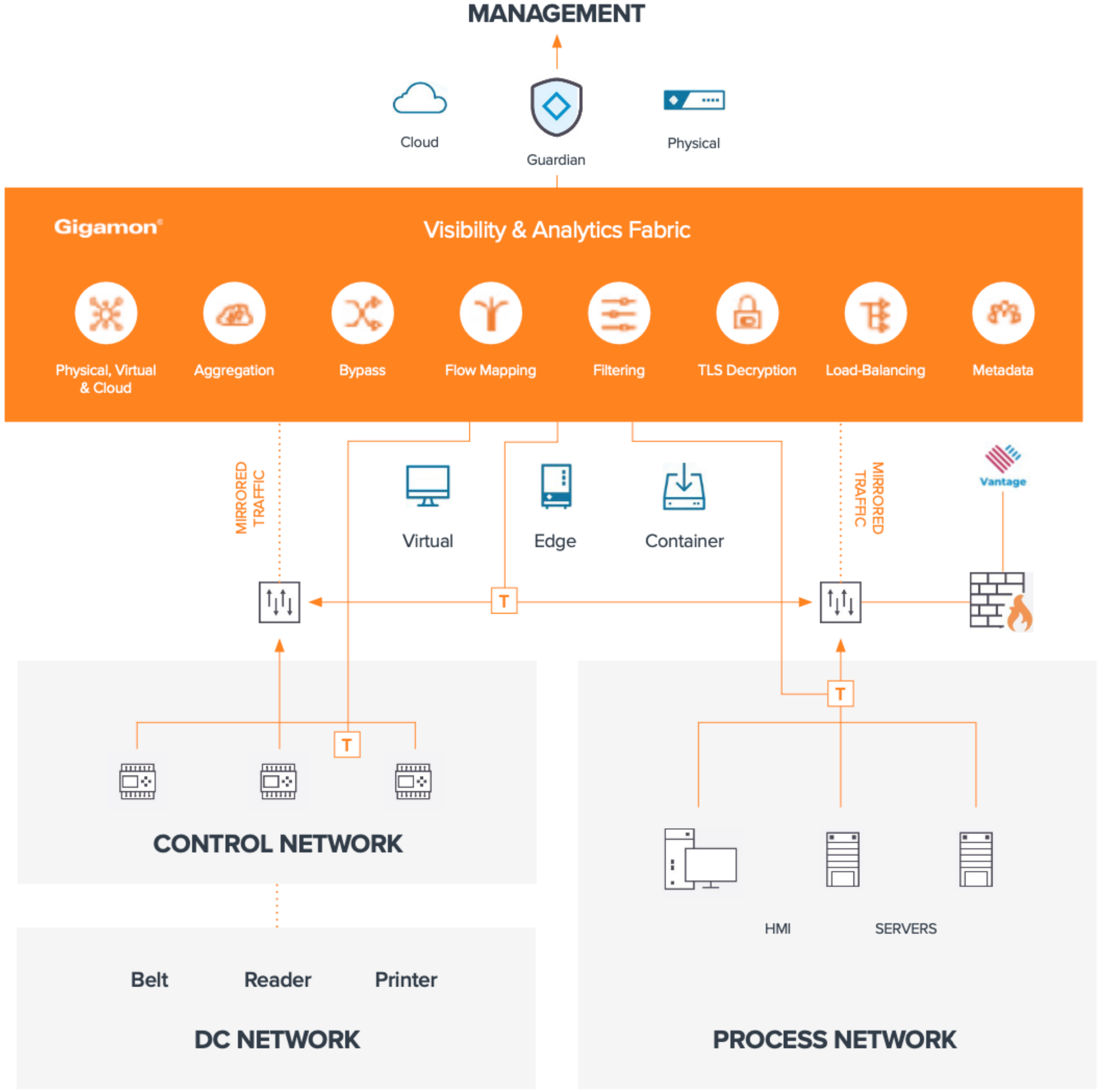


GigaVUE Cloud Suite for Kubernetes

Deep Observability into Containerized Applications

Figure 1. GigaVUE Cloud Suite for Kubernetes, consisting of GigaVUE V Series, GigaVUE-FM fabric manager and Universal Container TAPs (UCT), gives tools deep observability into Docker containerized applications.

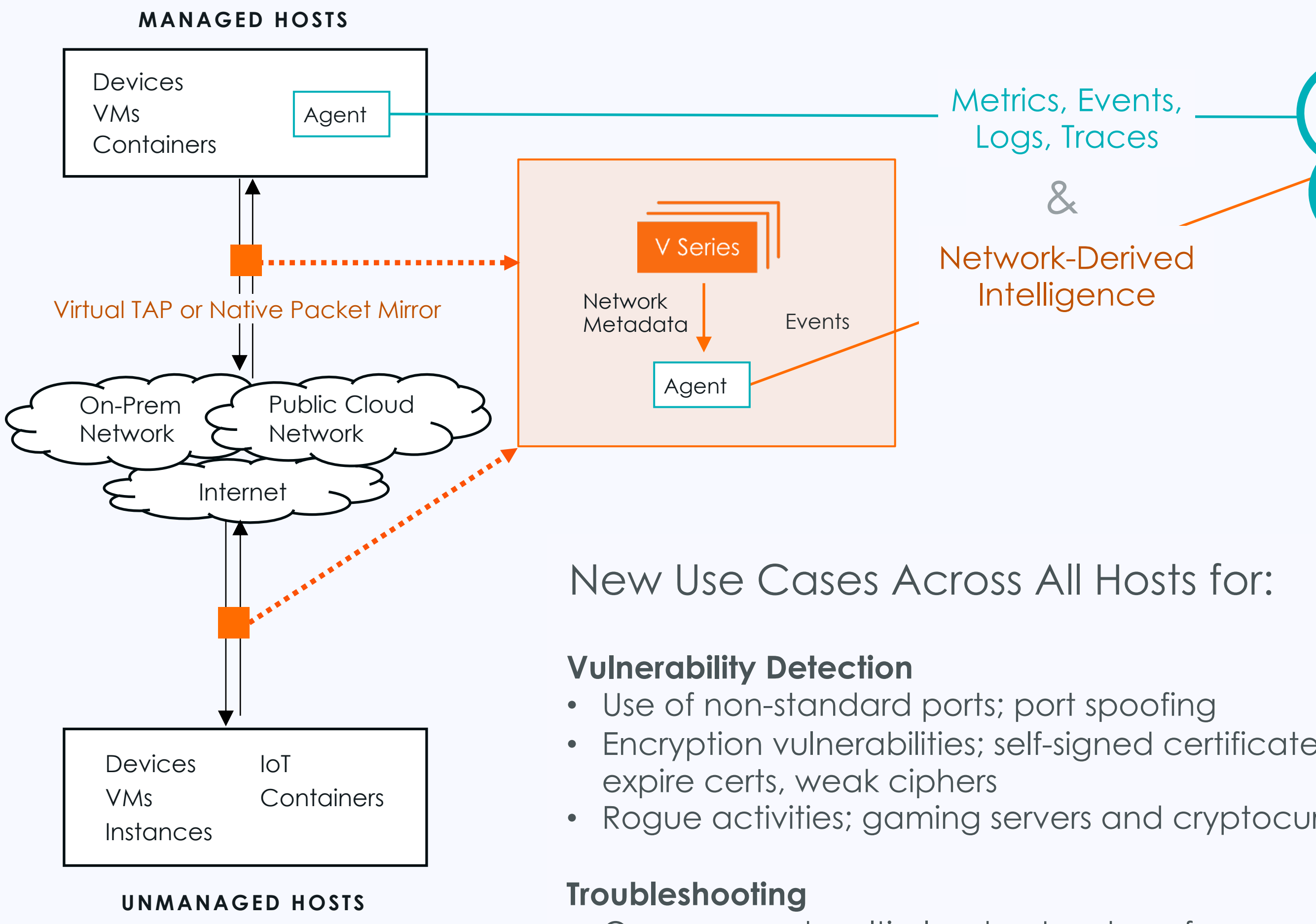
NOZOMI NETWORKS DEPLOYMENT WITH GIGAMON

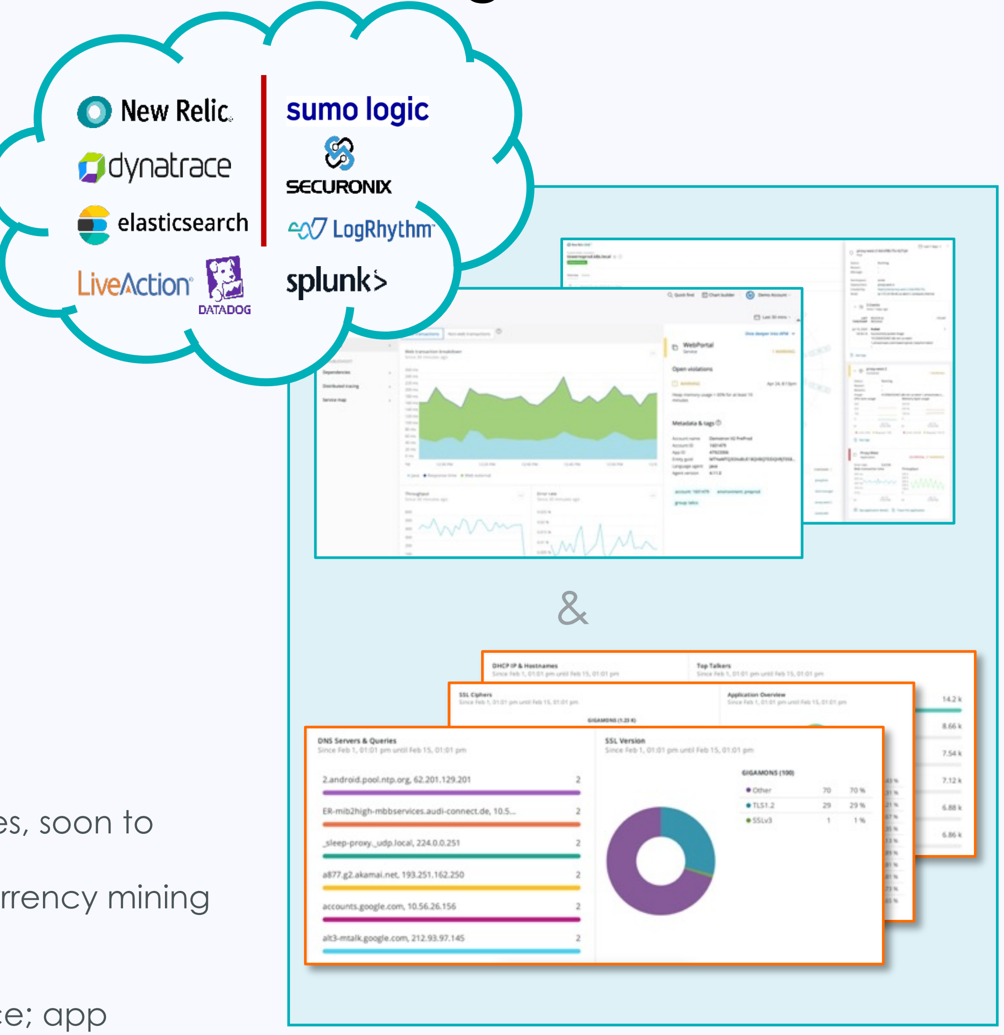


PROTECT YOUR OT WITH GIGAMON AND NOZOMI NETWORKS

- The Gigamon optional unidirectional taps ensure that OT product traffic is not negatively impacted
- No matter where your device traffic is coming from, including wireless sources for remote devices, Gigamon ensures no blind spots across your network. This even includes visibility into identity and access management activity to further ensure fundamental security
- Availability is mandatory for OT production networks. The Gigamon active/passive taps and inline bypass provide fail-open capability to ensure constant availability, including when maintenance may be required on security tools
- Gigamon sits between the OT business network, manufacturing, process network and tools, such as Nozomi Networks, to provide visibility regardless of medium (physical, virtual, cloud) and including east- west traffic.

Strengthening Observability and SIEM with Network Intelligence





New Use Cases Across All Hosts for:

Vulnerability Detection

- Use of non-standard ports; port spoofing
- Encryption vulnerabilities; self-signed certificates, soon to expire certs, weak ciphers
- Rogue activities; gaming servers and cryptocurrency mining

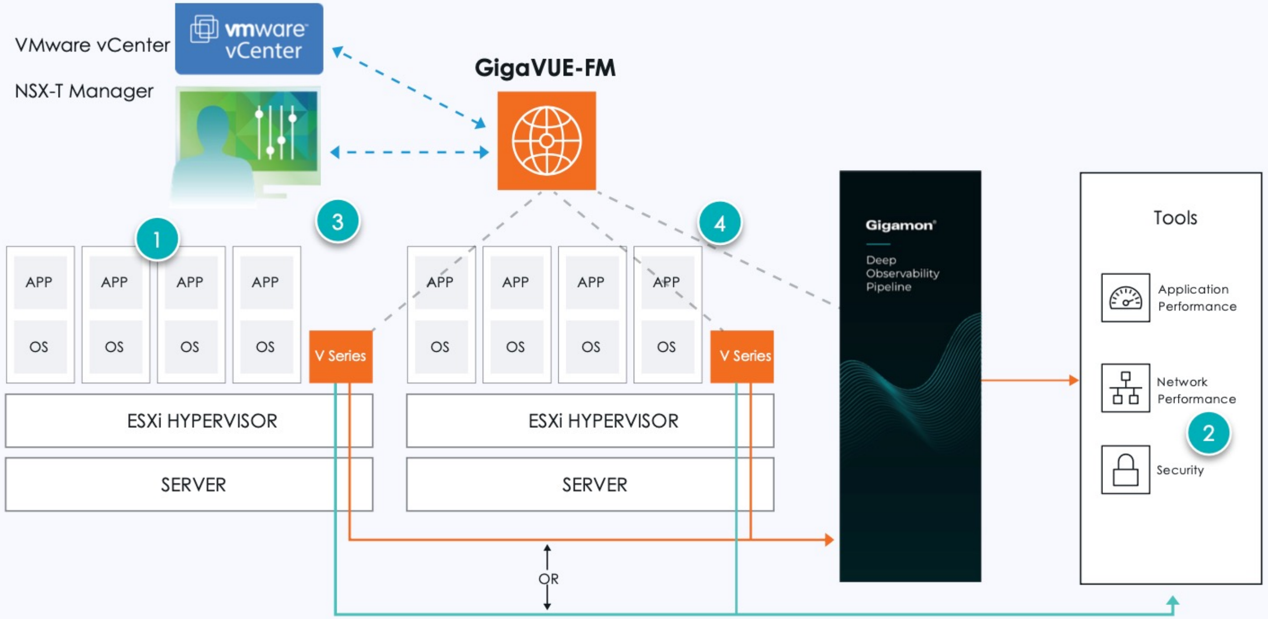
Troubleshooting

- On-prem and multi-cloud network performance; app response perf. vs. network

Private & Public Cloud Visibility

Private Cloud Visibility Benefits

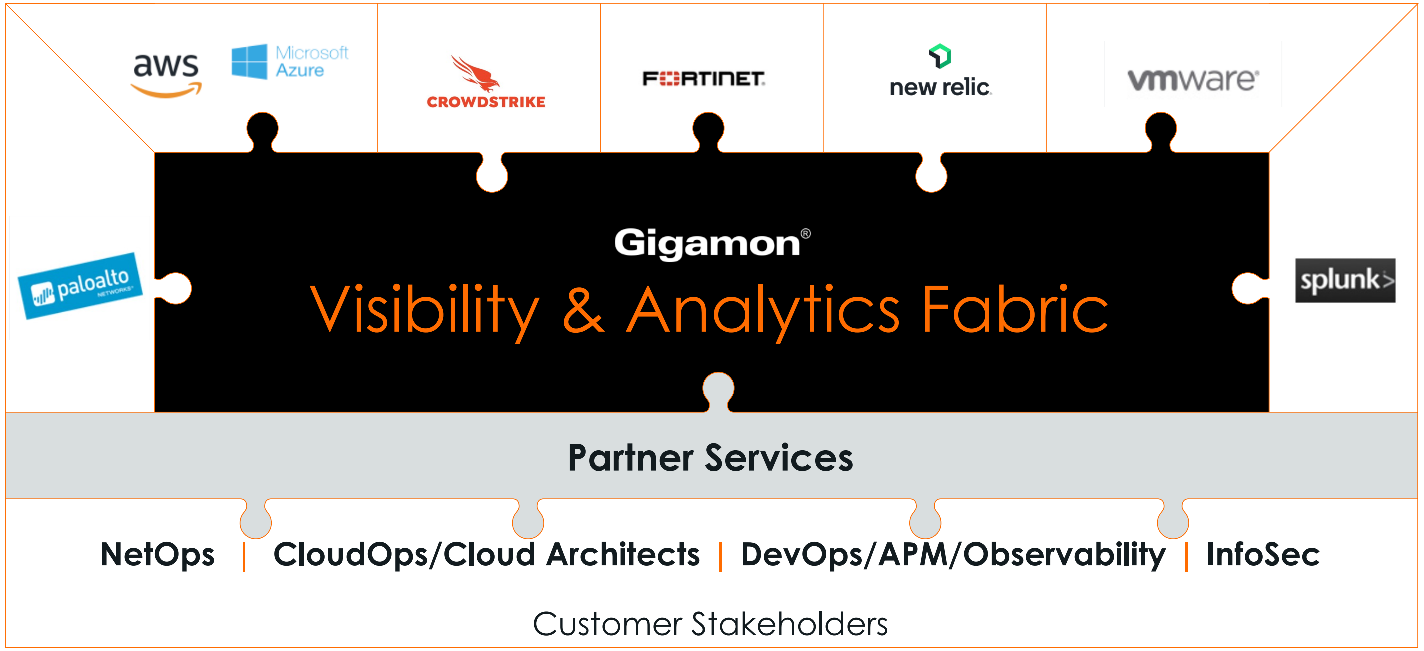
Nutanix, OpenStack (Red Hat), and VMware (ESXi, NSX-t)



1. Eliminate All Blind Spots
   - Access all traffic on each host, down to each VM,
2. Improve Security Posture
   - Ensure security tools see all appropriate traffic at packet or metadata level
3. Optimize Costs
   - Flow mapping and GigaSMART help remove irrelevant traffic
4. Streamline Operations
   - Auto-discover hosts and send traffic to tools using "Automatic Target Selection"
   - Minimize manual efforts and errors through automation.

Integrate Gigamon Into Your Ecosystem Opportunities

Optimize over 130 tools across your partners hybrid environments



Gigamon®

Visibility & Analytics Fabric

Partner Services

NetOps | CloudOps/Cloud Architects | DevOps/APM/Observability | InfoSec

Customer Stakeholders

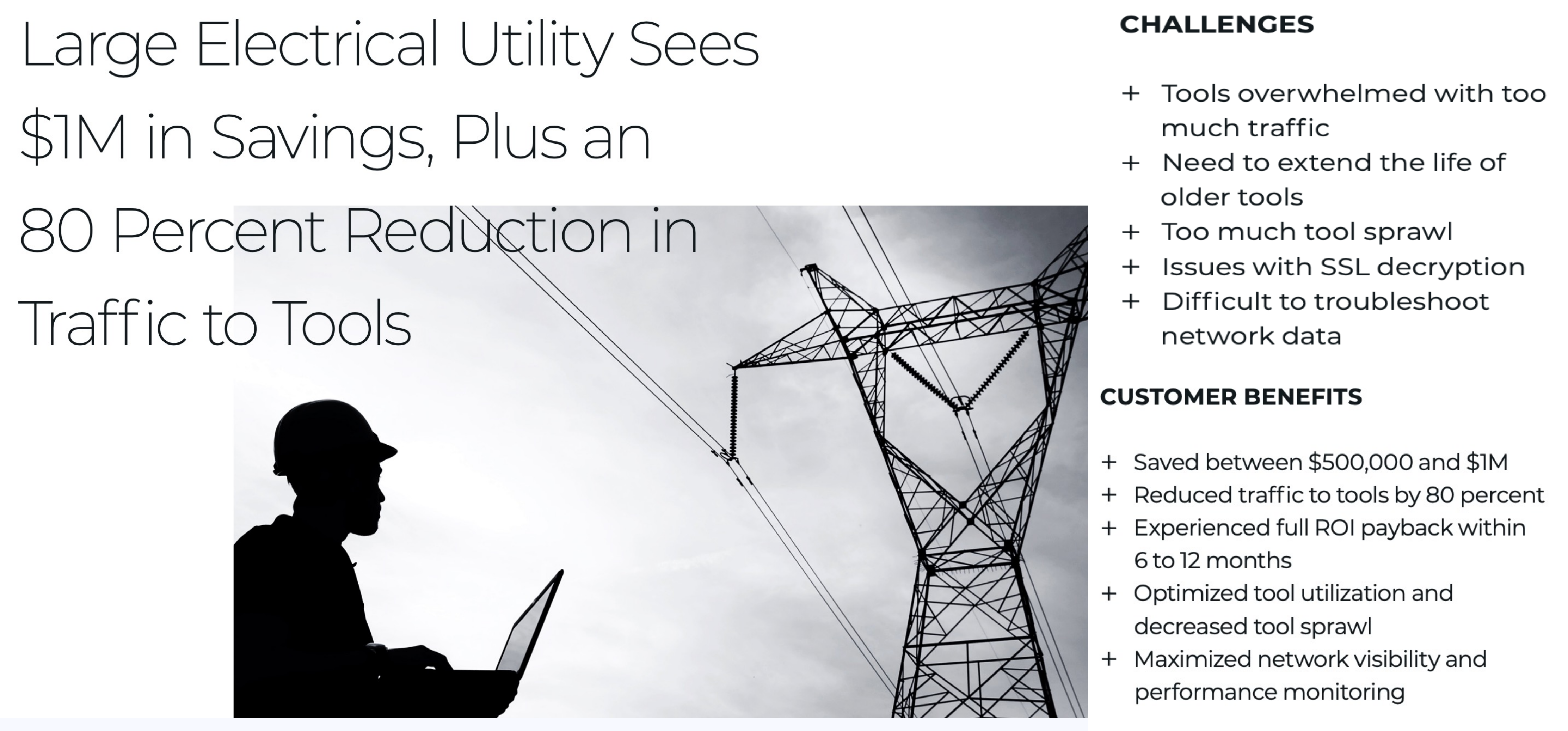
THE CHANNEL CO. CRN SECURITY 100 2023

The Power of Partnerships

Gigamon has an established and growing technology partner ecosystem that includes industry-leading vendors from across the following market segments:

- **Security and vulnerability management**
- **Network performance management**
- **Observability**
- **Cloud**
- **Service Provider**

Customer Case Study: Large Australian Electrical Utility



Large Electrical Utility Sees $1M in Savings, Plus an 80 Percent Reduction in Traffic to Tools

CHALLENGES

- Tools overwhelmed with too much traffic
- Need to extend the life of older tools
- Too much tool sprawl
- Issues with SSL decryption
- Difficult to troubleshoot network data

CUSTOMER BENEFITS

- Saved between $500,000 and $1M
- Reduced traffic to tools by 80 percent
- Experienced full ROI payback within 6 to 12 months
- Optimized tool utilization and decreased tool sprawl
- Maximized network visibility and performance monitoring

Customer Case Study: Land Bank Philippines

Case Study

Full Visibility Finally Possible for the Land Bank of the Philippines

Challenges

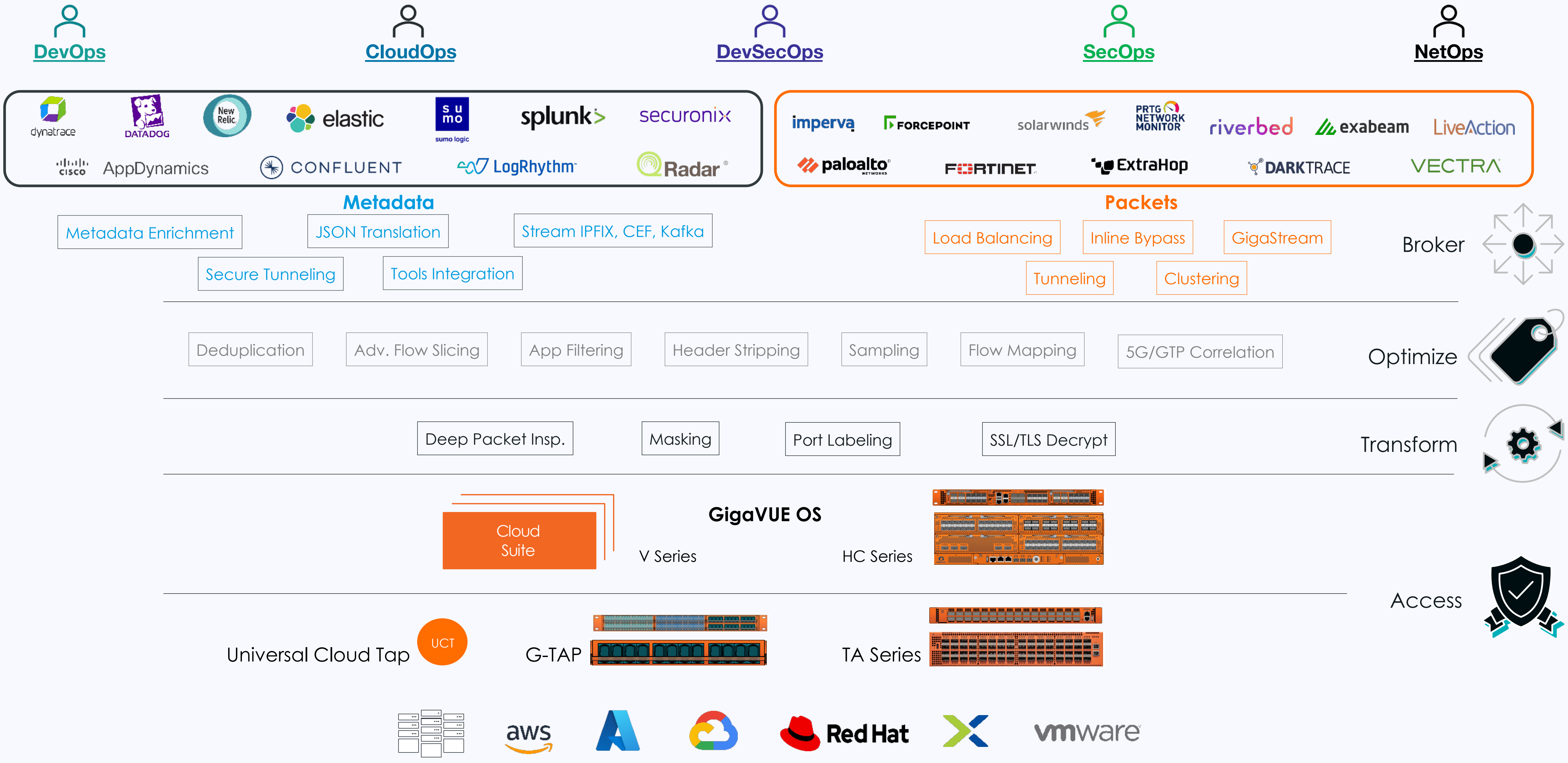
- Troubleshooting network data
- Eliminating blind spots in encrypted traffic
- Gaining a single source of visibility across physical, virtual, and cloud environments

Customer Benefits

- Achieved tremendous CapEx ROI
- Reduced traffic to tools by 80 percent
- Improved network and security monitoring
- Experienced full ROI payback within 6 to 12 months
- Maximized network visibility
- Accelerated threat prevention, detection and response time
- Decreased tool sprawl and costs

Gigamon Architecture

Bridging Teams, Tools and Telemetry



DevOps   CloudOps   DevSecOps   SecOps   NetOps

dynatrace, DATADOG, New Relic, elastic, sumo logic, splunk>, securonix, cisco AppDynamics, CONFLUENT, LogRhythm, Radar

imperva, FORCEPOINT, solarwinds, PRTG NETWORK MONITOR, riverbed, exabeam, LiveAction, paloalto NETWORKS, FORTINET, ExtraHop, DARKTRACE, VECTRA

Metadata

Metadata Enrichment | JSON Translation | Stream IPFIX, CEF, Kafka | Secure Tunneling | Tools Integration

Packets

Load Balancing | Inline Bypass | GigaStream | Tunneling | Clustering

Broker

Deduplication | Adv. Flow Slicing | App Filtering | Header Stripping | Sampling | Flow Mapping | 5G/GTP Correlation

Optimize

Deep Packet Insp. | Masking | Port Labeling | SSL/TLS Decrypt

Transform

GigaVUE OS

Cloud Suite

V Series

HC Series

Universal Cloud Tap

UCT

G-TAP

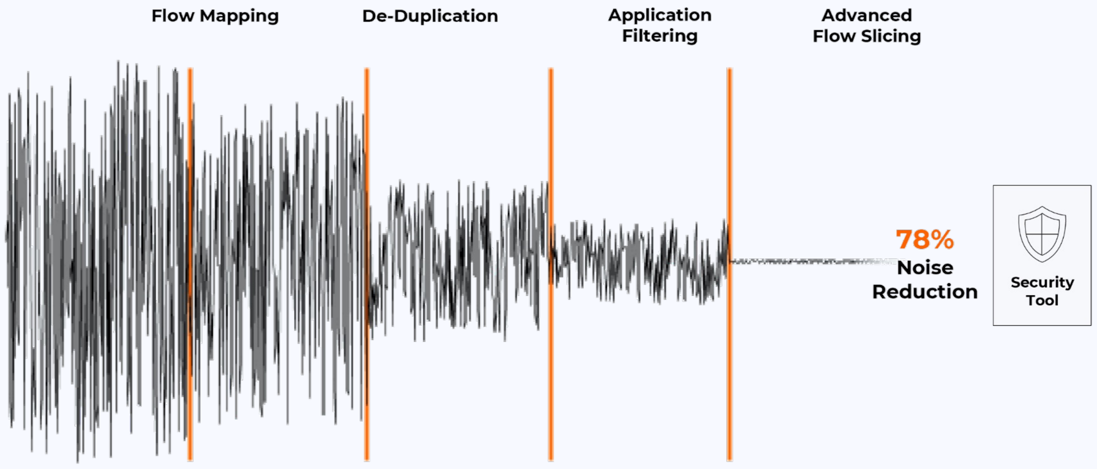
TA Series

Access

aws, Red Hat, vmware

How Gigamon Improves Efficiency of Monitoring Tools

	TRAFFIC REDUCTION	TOOLS HELPED
1. DE-DUPLICATION • Duplicate packets represent more than 50% of network traffic • Gigamon removes the need for existing tools to process duplicate packets – increasing performance and freeing up tool capacity.	50%	• IDS • NPM • APM • DLP • Forensics • NDR
2. APPLICATION FILTERING • Gigamon gives you the power to direct specific application flows to only the tools that need to see them. • By removing irrelevant or low-risk application traffic such as video streams, antivirus pushes, and Windows updates, you'll increase tool efficiency and effectiveness.	50%	• IDS • NPM • APM • DLP • Forensics • NDR
3. FLOW MAPPING • Gigamon allows mapping of specific traffic flows, from specific TCP ports, while filtering out the rest • Gigamon customers have seen 20–30 percent traffic reduction to their tools after applying Flow Mapping.	25%	• IDS • NPM • APM • DLP • Forensics • NDR
4. ADVANCED FLOW SLICING • Gigamon eliminates bandwidth issues and processing burden by slicing payloads and packets from long data flows. • You can decide to forward just the first set of packets in the flow, then slice or drop the rest — reducing traffic by up to 60 percent.	90%	• IDS • NPM • APM • DLP • Forensics • NDR



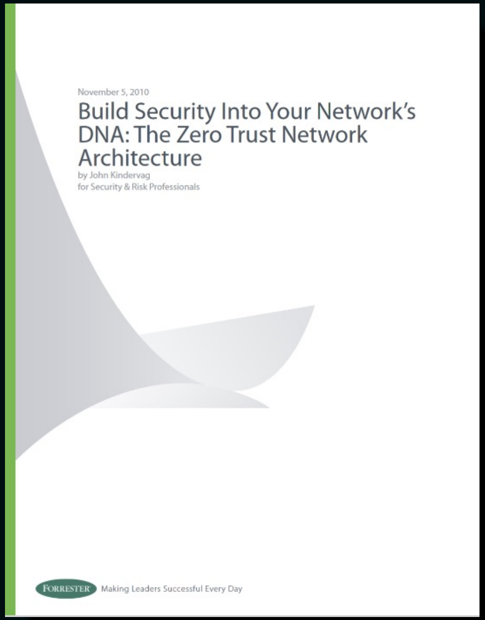
Through our patented traffic-reduction capabilities, such as Flow Mapping®, De-Duplication, Advanced Flow Slicing, and Application Filtering Intelligence, Gigamon can dramatically streamline traffic going to tools without compromising data fidelity.

How Gigamon Deep Observability Pipeline is Deployed in Zero Trust Architecture

Evolving Approaches to Zero Trust

12 Years and Counting

Original Kindervag Paper (2010)



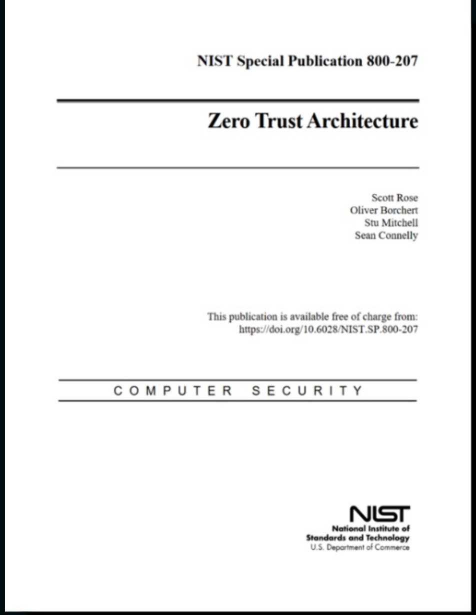
November 5, 2010

Build Security Into Your Network's DNA: The Zero Trust Network Architecture

by John Kindervag
for Security & Risk Professionals

FORRESTER Making Leaders Successful Every Day

NIST SP 800-207 (2020)



NIST Special Publication 800-207

Zero Trust Architecture

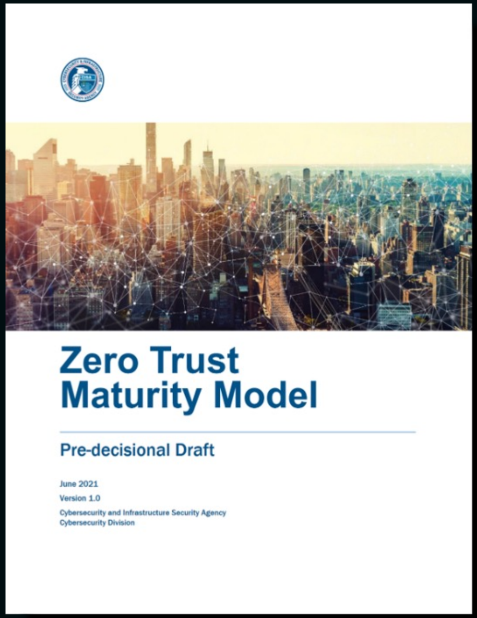
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

CISA ZT Maturity Model (2021)



Zero Trust
Maturity Model

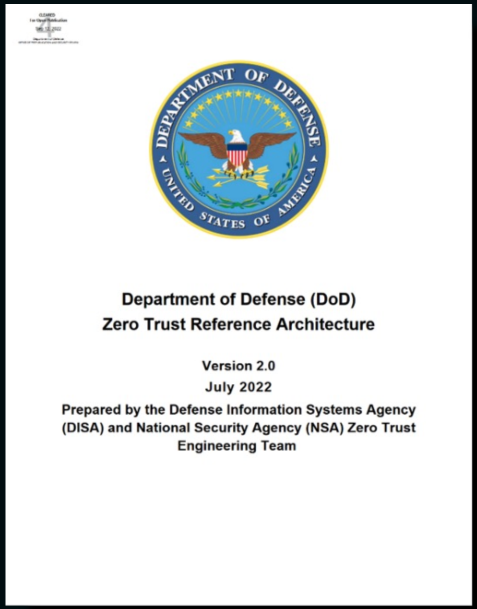
Pre-decisional Draft

June 2021

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

DoD ZTA Reference Architecture v2.0 (2022)



CLEARED
For Open Publication
Sep 12, 2022
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

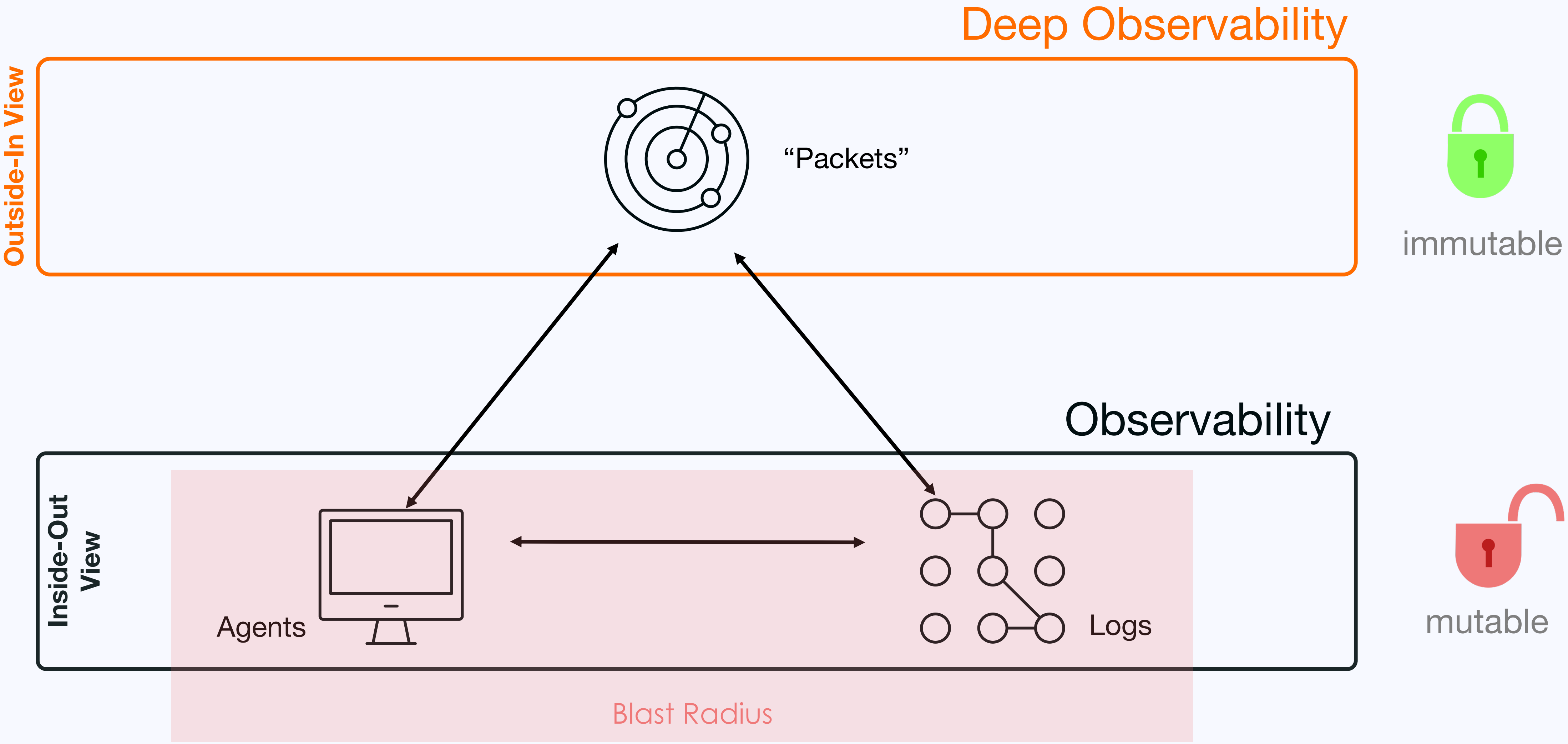
DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

What is Deep Observability?

Recommendation: Logging + Agent + Deep Observability



Network Visibility is Already in the Standards

"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."

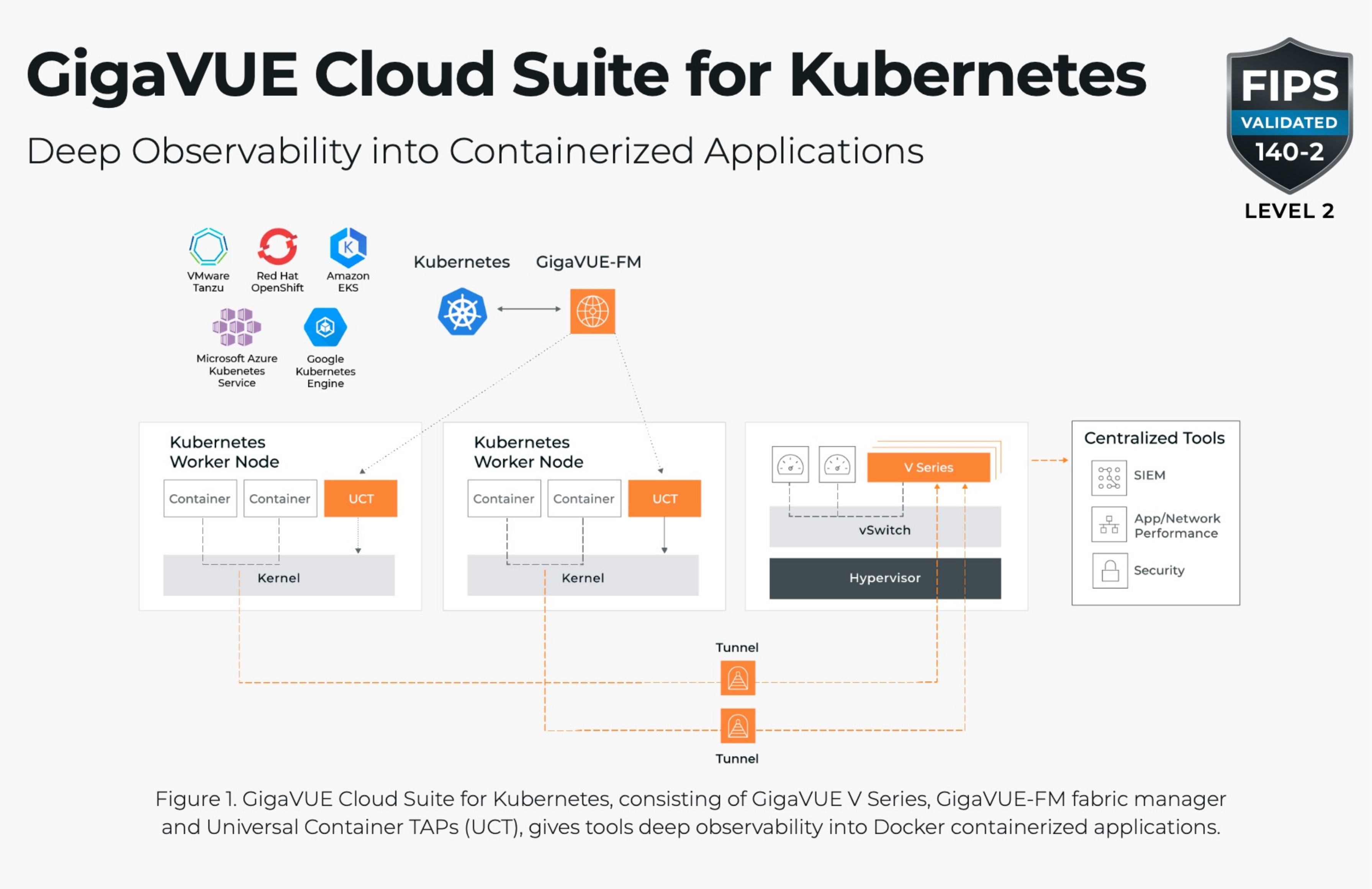
NIST SP 800-207, Section 3.4.1(3) "Network Requirements to Support ZTA", page 21

Deep Observability Makes Threat Detection More Powerful

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)
  - Processed into metadata by Gigamon's GigaSMART Application Metadata Intelligence, AI/ML detection of threats is massively accelerated AI/ML algorithms
- It is much harder for an attacker to avoid detection with deep observability present
- Deep Observability gives you the ability to selectively decrypt SSL/TLS with Gigamon's Inline SSL Decryption
- Supply chain attacks and highly sophisticated threats like implants are invisible to logging and EDR, but will be seen by Deep Observability

Visibility into containers, East – West Lateral movement



GigaVUE Cloud Suite for Kubernetes

Deep Observability into Containerized Applications

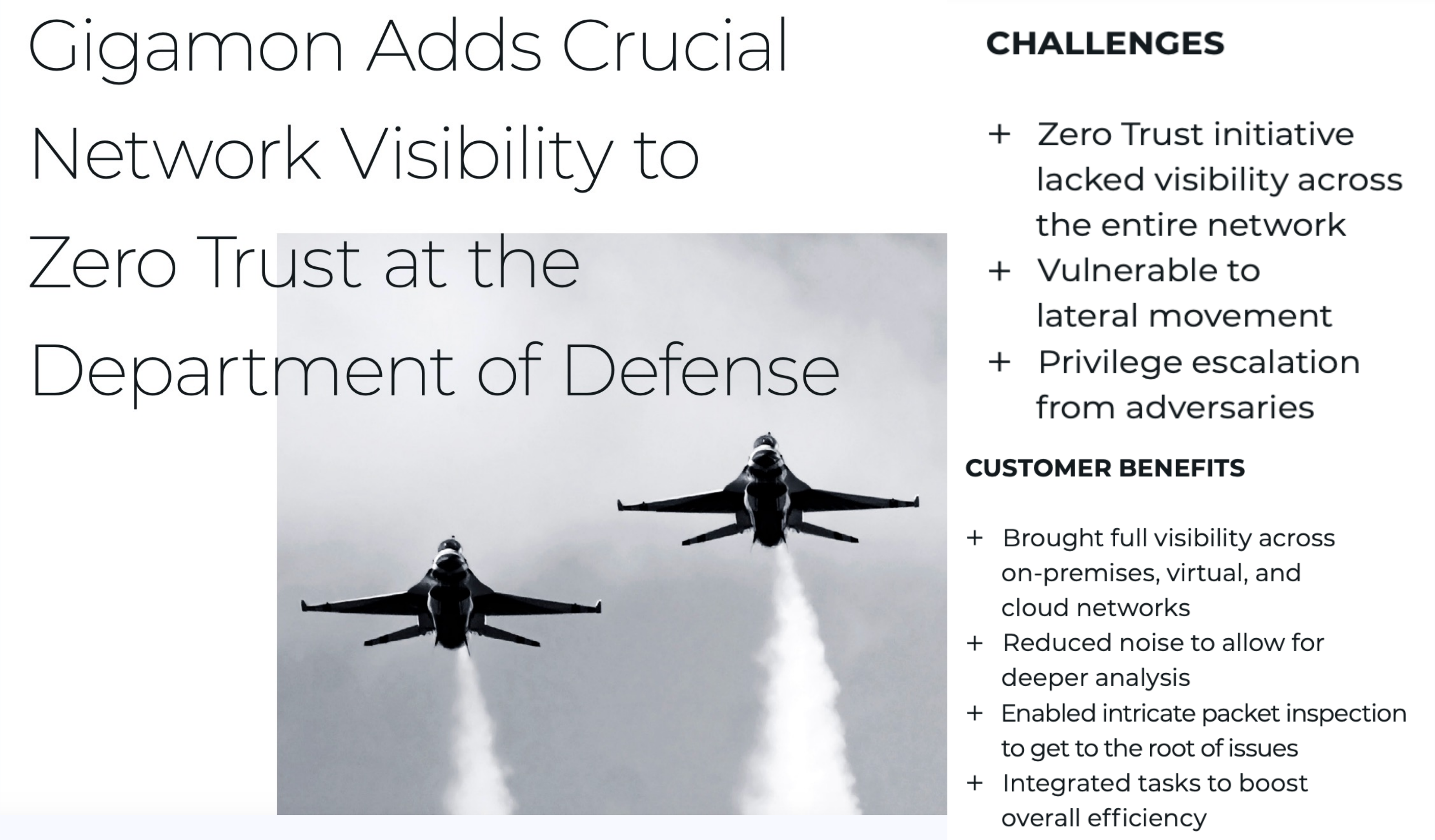
FIPS VALIDATED 140-2 LEVEL 2

Figure 1. GigaVUE Cloud Suite for Kubernetes, consisting of GigaVUE V Series, GigaVUE-FM fabric manager and Universal Container TAPs (UCT), gives tools deep observability into Docker containerized applications.

Deep Observability Simplifies Zero Trust

- Network traffic is common across all environments:
  - Multi-public cloud
  - Private clouds
  - On-prem
- Supports devices which cannot run EDR (or even do logging):
  - Legacy compute (mainframes)
  - IoT/OT/ICS/SCADA etc.
  - BYOD
- How can you collect network traffic from all of these locations: Gigamon

Customer Case Study: US Department of Defense



Gigamon Adds Crucial Network Visibility to Zero Trust at the Department of Defense

CHALLENGES

- Zero Trust initiative lacked visibility across the entire network
- Vulnerable to lateral movement
- Privilege escalation from adversaries

CUSTOMER BENEFITS

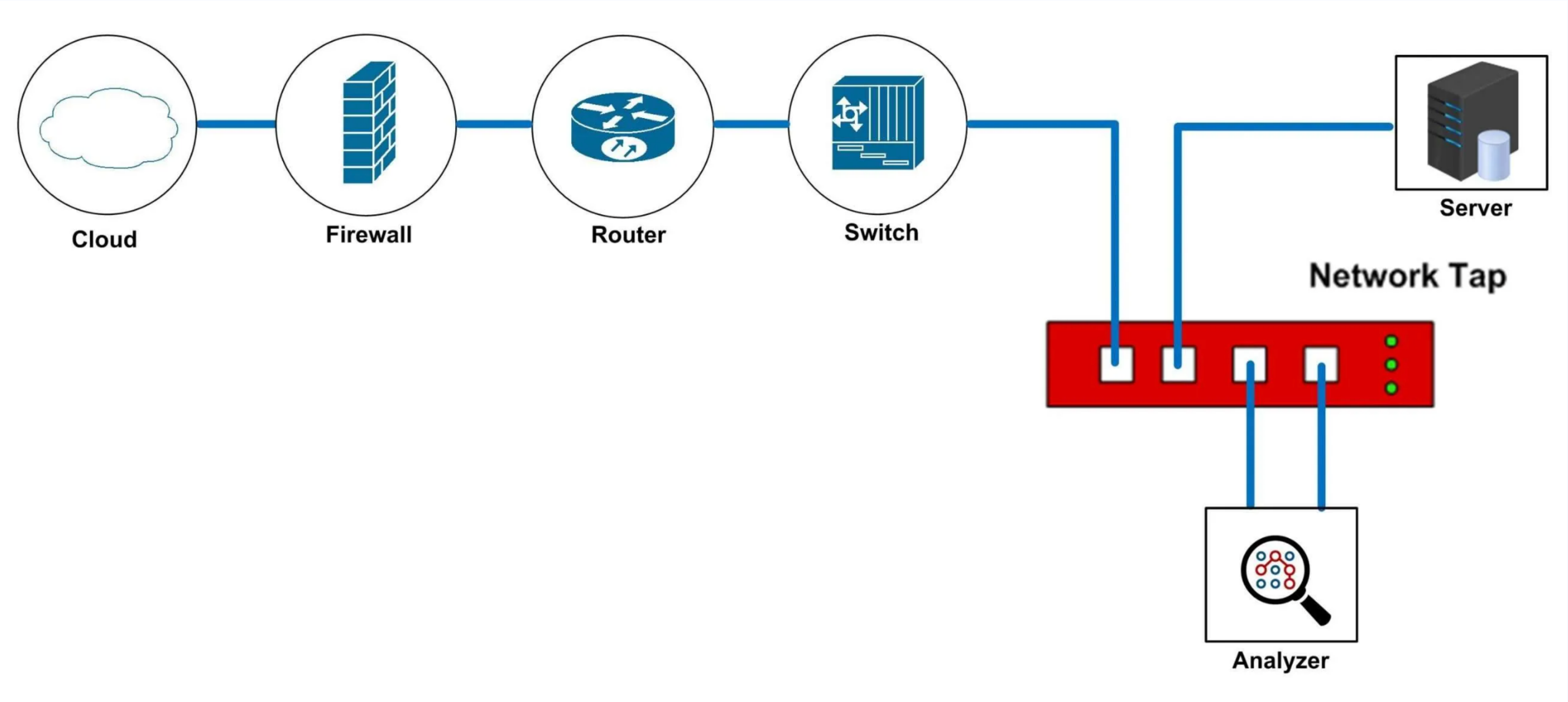
- Brought full visibility across on-premises, virtual, and cloud networks
- Reduced noise to allow for deeper analysis
- Enabled intricate packet inspection to get to the root of issues
- Integrated tasks to boost overall efficiency

Gigamon®

Q&A

Network TAP Description

A network TAP (short for Test Access Point) is a hardware device that is placed on a network segment, allowing you to access and monitor network traffic. Network taps allow traffic to flow without interruption or interference. As long as they are connected, a network taps will create an exact copy of both sides of traffic on the network. All monitoring and analysis tools that are connected to the tap will receive exact copies of the network traffic.



Gigamon®

Thank you

Marko Rämö
Regional Sales Director
Nordics & Baltics

Marko.ramo@gigamon.com
+46 730 45 06 56