SOLUTION BRIEF

endace
Record. Respond.

Gigamon®

Meeting Federal Requirements for Investigation and Remediation

Background

The US Presidential Mandate M-21-31 and White House Executive Order 14028 impose stringent obligations on Federal organizations to improve cybersecurity readiness. Under the terms of the mandate, Federal organizations must meet or exceed detailed network monitoring and logging capabilities which include being able to make logs and full packet capture data available, on request, to CISA and/or FBI, for investigations. Appendices in M-21-31 specify what monitoring data must be collected and how long it must be retained for.

The Problem

Many organizations don't have the infrastructure needed to meet these mandated requirements. In particular, many cannot isolate, capture, continuously record and store the full packet (pcap) data and deliver the real-time monitoring required by the mandate – which requires a minimum of 72 hours of full packet capture data.

Organizations need a solution that:

- Is cost-effective and scalable.
- Provides continuous, always-on packet capture (not triggered capture) that satisifies the requirements of M-21-31.
- Delivers the required functionality while being easy-to-use and fast to implement.
- Can integrate with existing security solutions and workflows
- Can be deployed on all the organization's infrastructure – including on-premise, private and public cloud.
- Has the flexibility to change easily to meet evolving needs.

Benefits

- Always-On recording to capture all traffic.
- Store weeks or months of full packet capture data for a complete record of network activity.
- Rapid search and data-mining.
- Full visibility across complex networks including Hybrid and Multi Cloud, including visibility into encrypted traffic.
- Easy to deploy, integrates with existing infrastructure. Open architecture to work in multiple environments.
- Delivers accurate, reliable, tamper-resistant forensic data to your security tools and teams.
- A proven, reliable and scalable solution that has been implemented in many government and military environments around the world.
- Meets or exceeds M-21-31 mandated compliance requirements at all levels – E1 through E3.
- Compliant with FIPS 140-3 and NIAP NDcPP 2.2E.

The Solution

By combining Gigamon's GTAP and GigaVUE products with Endace's always-on packet capture, organizations gain unparalleled control over, and visibility into, the traffic traversing their on-premise and cloud networks as well as an accurate historical record of all network activity.

Using GTAPs and GigaVUE, customers can access network traffic from anywhere in their hybrid cloud infrastructure and direct it all to their network security and performance monitoring tools, including EndaceProbes.

Traffic can be transformed using the powerful aggregation, filtering/masking, duplication/de-duplication, decryption, metadata generation and other capabilities of GigaVUE.

EndaceProbes can record and store days, weeks or months of full packet capture data from on-premise, public or private cloud environments. Multiple EndaceProbes can be connected to provide a unified, hybrid cloud recording fabric.

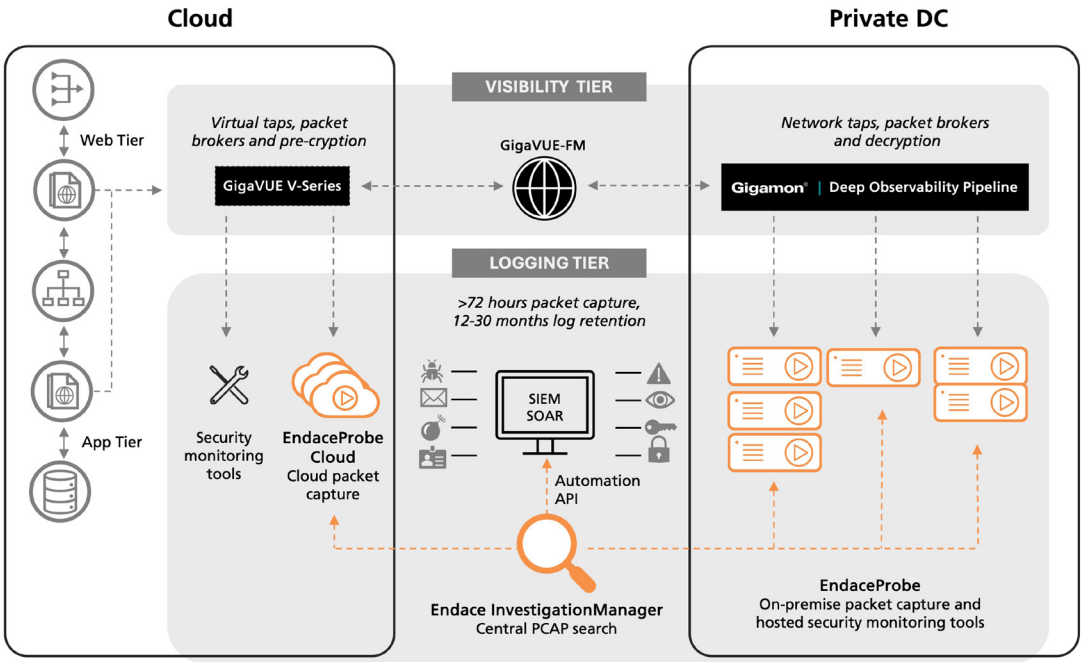
This fabric enables rapid, centralized search, data-mining and analysis of recorded traffic, and integrates directly into security tools from Cisco, Palo Alto Networks, Splunk, IBM and many other vendors to enable faster, more efficient investigation and resolution of network security and performance issues.

Conclusion

Together, Gigamon and Endace have implemented proven solutions for government and military customers around the globe. Our joint solution enables Federal customers to easily meet the specific requirements of the M-21-31 mandate.

More importantly, implementing this joint solution ensures your network is underpinned by an architecture that dramatically improves your visibility into - and ability to defend against – current and future cyber threats. It also ensures your infrastructure has the flexibility to adapt as your organization's cybersecurity needs evolve.

How it works



Solution Components

- G-TAP™ and GigaVUE™ HC and TA series with Decryption
- GigaVUE Cloud Suite and Universal Cloud Tap™ with Precryption™
- EndaceProbe™ Always-On Packet Capture for On-Premise and Cloud
- EndaceFlow™ high performance NetFlow generation
- Turnkey integrations with popular SIEM, NGFW, NDR, SOAR, and orchestration tools