Gigamon®

Without deep observability, you could end up with your hair on fire.

Network-derived intelligence detects threats your existing security tools can’t see.

The CISO Conundrum

According to *Forbes*, the number of large organizations with a multi-cloud strategy is predicted to rise to 85 percent in 2024[1] as organizations seek to balance business agility with cyber security in cloud transformations.

At the same time, the cost and scale of cyberattacks are at an all-time high, with global cybercrime costs projected to reach $10.5 trillion by 2025.[2] As a result, CISOs are faced with the challenge of securing and monitoring their complex infrastructure from a threat landscape that is constantly becoming more sophisticated while also containing cost and complexity. Despite record spending on the latest security strategies and tools, like SASE, EDR, network micro-segmentation, and SIEMs, CISOs still struggle to keep up with the growing tide of emerging threats, particularly ransomware and insider breaches.

1. Marr, B. (2024, February 20). The 10 biggest cloud computing trends in 2024 Everyone must be ready for now. Forbes.
2. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.

How Breaches Affect the Bottom Line

The cost of a security breach reaches far beyond dollars and cents, impacting business in profound ways:

- Disrupting business operations by causing downtime and lost revenue
- Damaging an organization's reputation and customer loyalty through IP and customer data theft.
- Making it more expensive (maybe even impossible) to purchase cyber-insurance.
- Exposing the organization and its officers to the risk of regulatory and compliance fines and possibly jail time.

Your security tools are doing a great job. As far as you know.

Without deep observability, you could end up with your hair on fire.

Your Network's Biggest Blind Spots: Lateral and Encrypted Traffic

With increasing cloud adoption also comes increasing cost and complexity in securing and managing hybrid cloud infrastructure. Different infrastructure components have their own monitoring tools and processes, leading to a fragmented stack of siloed tools that doesn't offer a complete picture of what's really happening across your hybrid cloud infrastructure.

Your security tools are tough on North-South threats and surprisingly chill about East-West ones.

Most security tools inspect north-south traffic but often neglect lateral movement — which can lead to devastating consequences for your organization. If threat actors breach your network, they can move freely across your hybrid cloud infrastructure undetected, ultimately accessing your organization's most sensitive data.

The Gigamon Deep Observability Pipeline is the one solution singularly focused on eliminating this blind spot by providing the lateral East-West visibility needed to detect previously unseen threats, including ones that may already be inside your network.

The dangers lurking in encrypted traffic

Given that 95 percent of all web traffic is encrypted,[4] organizations that lack visibility into encrypted traffic are exposed to hidden threats their existing security tools can't see. And as encryption trends up, so do the opportunities for threat actors to exploit encrypted channels.

Every network has something to hide. Until now.

Decrypting all traffic can be costly and complex, demanding high compute power while increasing latency and reducing performance — until now. Gigamon offers a powerful combination of patented solutions that makes gaining visibility into encrypted traffic affordable and scalable, including our award-winning Precryption™ technology and GigaSMART© TLS/SSL Decryption.

Among organizations that experienced an attack over encrypted channels in the past year, 85 percent witnessed attacks over "trusted" channels, like the legitimate websites of trusted organizations or third-party vendors — a stark reminder that no TLS/SSL-encrypted traffic can be assumed secure.[5]

4. Google Transparency Report
5. Zscaler ThreatLabz 2023 State of Encrypted Attacks Report
6. 2024 Gigamon Hybrid Cloud Survey

The Preparedness Gap

Overconfidence in the safety of encrypted traffic creates huge blind spots ripe for exploitation.

76%
OF CISOS
trust encrypted traffic is secure

63%
OF CISOS
believe encrypted traffic is less likely to be inspected

86%
OF CYBERTHREATS
are concealed in encrypted traffic

62%
OF COMPANIES
saw an increase in attacks over encrypted channels in the past year[6]

Even the Best Security and Observability Tools Have Blind Spots

See the whole iceberg with deep observability.

Traditional and native cloud tools that gain visibility exclusively through metric, event, log, and trace (MELT) data are limited in what they can identify and how deeply or broadly they can monitor today's complex infrastructure.

The Gigamon Deep Observability Pipeline goes beyond traditional observability approaches by extracting intelligence directly from network traffic and efficiently delivering it to your tools in real time. With this network-derived intelligence, your tools can detect previously hidden threats and help mitigate the cost and severity of an attack.

> Deep observability helps eliminate blind spots by giving your tools the network-derived intelligence and insights needed to detect threats that would have previously flown under the radar.

7. CrowdStrike 2024 Global Threat Report

The Growing Importance of Real-Time Threat Detection

Cyberattacks are getting faster and more aggressive as attackers shorten the time between initial entry, lateral movement, and breach.

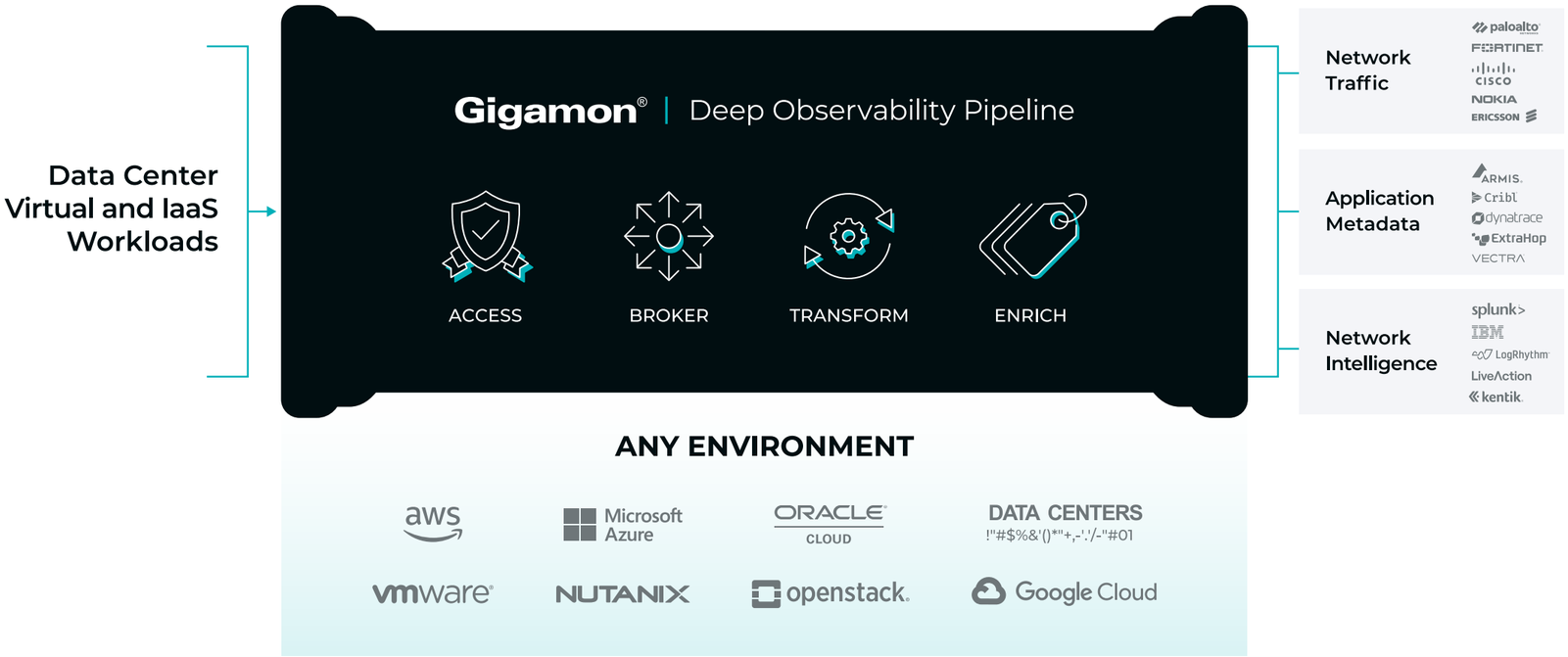
62 Minutes

The average time it takes for a threat actor to move from an initially compromised host to another within the organization has sped up by 23 percent since last year, with some taking only minutes to succeed.

204 Days

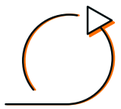
It takes organizations an average of 204 days to identify a data breach and 73 days to contain it.[7]

A Purpose-Built Deep Observability Pipeline



The Gigamon Deep Observability Pipeline, based on GigaVUE Cloud Suite™, efficiently delivers network-derived intelligence to your cloud, security, and observability tools. This helps eliminate security blind spots and reduce tools cost, so you can better secure and manage the hybrid cloud infrastructure.

Supercharge Your Security Tools to Achieve Tangible Outcomes



Increase Agility, Reduce Costs

The answer to fortifying your security posture is not necessarily investing in more tools. In fact, having too many tools has proven to be less effective in detecting and mitigating threats by overwhelming security teams and creating data silos that lead to visibility gaps and blind spots.[3]

Gigamon optimizes tools' performance and effectiveness to help organizations manage tool sprawl, reduce costs, and above all gain the deep observability you need to eliminate blind spots.

Save Operational Costs

By optimizing and improving signal-to-noise ratio of network traffic ingestion, Gigamon customers often realize 50-60 percent savings on tools spend and deferral of in-year new capacity purchases. Gigamon also eliminates the need for costly cloud gateway and load balancing services, reducing the cost of cloud traffic acquisition from 0.75 cents to 0.04 cents per gigabyte.

Deep observability makes your existing security and observability tools up to **90 percent more efficient** and can reduce tool and bandwidth costs by up to 50 percent - enabling the typical mid-sized customer to achieve a 4-6 month ROI.

3. 2020 Cyber Resilient Organization Report

Put out the fire before it even starts.

Without deep observability, you're vulnerable to unseen threats.

A Market Leader in Deep Observability

650 GROUP Market Intelligence Research
#1 MARKET SHARE LEADER
Deep Observability
2023

According to the market intelligence research firm 650 Group, Gigamon is a market leader in Deep Observability with 63 percent market share in 2023.

The most security conscious government agencies and businesses around the world rely on Gigamon for tangible risk reduction.

4,000+
CUSTOMERS WORLDWIDE

10/10
U.S. FEDERAL AGENCIES

8/10
TOP HEALTHCARE PROVIDERS

83/100
FORTUNE 100 COMPANIES

7/10
TOP GLOBAL BANKS

9/10
TOP MOBILE NETWORK OPERATORS

A couple of incidents that we had within the last six months we were able to catch quite quickly—within about an hour or so of the time the attacker took ownership of a server. We were able to catch them just in time before any real damage was done. And the reason is we have security tools in place, and Gigamon is feeding all the data into those security tools.

Kajeevan Rajanayagam,
Director of Cybersecurity at University Health Network

"Organizations continue to move more and more workloads to the cloud, yet these hybrid and multi-cloud environments create significant security challenges because of the lack of visibility. Creating a turnkey solution with Gigamon and Vectra AI is a game changer for cloud security. We'll now be able to offer our global customers a complete cyber defense solution for any and all cloud networks, delivering the deep observability they need from Gigamon with a best-in-class, AI-based threat detection, investigation and response platform from Vectra AI – combined into a single offering."

Paul Eccleston,
SVP EMEA for Exclusive Networks

"Last year we saw the impact of new cybersecurity threats, with public coverage of breaches, ransomware, and data leaks," "These vulnerabilities make deep observability, and the East-West visibility it provides into encrypted traffic, a critical foundation for all organizational operations, driving demand in today's security and IT budgets. Gigamon maintained its leadership position with its Deep Observability Pipeline, bringing an innovative approach to securing and managing modern hybrid cloud infrastructure."

Alan Weckel, Founder and Technology Analyst at 650 Group

Final Thoughts

At Gigamon, our purpose is to protect the hybrid networks and data of the largest, most complex organizations on the planet. We're obsessed with learning, collaborating, and innovating to deliver solutions that safeguard organizations from cyberthreats. With input from employees, partners, and customers, we have developed a deep observability pipeline that offers the highest level of hybrid cloud security available today.

Let Gigamon supercharge your cloud, security, and observability tools by giving them something they don't have: **actionable network-derived intelligence and insights.**

Learn more about deep observability

Gigamon®

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