Mercury Gains Comprehensive AWS Security Observability with Netography Fusion®

Cloud-first FinTech company significantly reduced cost while achieving improved security detections across their multi-cloud network

MERCURY

Company
Mercury

Industry
FinTech

Size
600+ employees; $50 billion in transactions in 200+ countries

"Network infrastructure breeds complexity, so the sooner you can get effective network monitoring and security in place, the better. A lot of security vendors were trying to sell me deep packet inspection that I didn't need and at a cost I wasn't willing to pay."

Branden Wagner, Head of Information Security, Mercury

Challenges

- Lacked real-time visibility into AWS activity for 100% cloud-based network
- Tired of using costly virtual appliances
- SecOps team was frustrated with the inability to visualize connections outside of organization, see protocol usage, or detect data exfiltration

Solution

- Netography Fusion®

Results

- Replaced costly virtual appliances with 100% SaaS Fusion platform
- Reduced deployment time and costs
- Eliminated delays in awareness with real-time detection
- Accelerated response and data sharing with built-in integrations with Panther SIEM platform and Slack
- Achieved massive scalability to monitor 100% of cloud activity

Snapshot

Mercury is a cloud-first fintech company trusted by over 200K startups to confidently run all financial operations. All of Mercury's infrastructure is in the cloud and employees work from wherever they are, all over the world.

Branden Wagner, head of Information Security at Mercury, saw the challenges financial services companies faced when relying primarily on transport layer security (TLS) inspection and packet capture to secure their infrastructure and ignore metadata and the insights it can provide without ever having to do packet decryption. According to Wagner, "*Network infrastructure breeds complexity, so the sooner you can get effective network monitoring and security in place, the better.*" He was looking for a better approach to securing Mercury's infrastructure.

Netography Fusion was the obvious choice — a modern platform that can deploy quickly and scale massively. From Mercury's perspective, being cloud-based means they are everywhere and nowhere. They needed a cloud-native network security partner that could understand that kind of communication and protect it so that money can flow securely.

Solution

Netography Fusion is cloud-native and leverages the power of context-enriched metadata to give security, network, and cloud operations teams comprehensive awareness of anomalous and malicious activity as soon as it appears. Its 100% SaaS architecture eliminates the burden of sensors, taps, or agents. Mercury was able to deploy in an afternoon — from populating Netography Fusion with data, to visualization and gaining insights for action.

Now, Mercury has an estimated 95% of its network covered by Netography, and the team is planning to continue to scale to 100% for informative and actionable data across the entire network.

Results

Fusion delivered a wide range of benefits to Mercury, including:

- Real-time detection eliminated delays in awareness
- The ability to identify users from Office of Foreign Assets Control (OFAC) sanctioned countries
- Built-in integrations with Panther SIEM platform and Slack; accelerated response and data sharing
- Massive scalability to monitor 100% of cloud activity

Fusion's use of context-enriched metadata has significantly accelerated his team's ability to respond to anomalous activity. As Wagner explains, "*Context labeling capabilities brought extreme visibility; for example, making it easy to differentiate Snowflake data from GitHub data and get host names, all without having to check IP addresses.*"

Additionally, Fusion's custom dashboards help Mercury address questions from key audiences like auditors, and tailored views enable a better understanding of what is happening across their multi-cloud environments. Netography also integrates with Mercury's SIEM platform where they can add more context and take action, as well as with Slack and email for alerting and data sharing.

About Netography

Netography is the leader in using context-enriched metadata to detect activity that should never occur in your multi-cloud or hybrid network. Netography Fusion® is a 100% SaaS, cloud-native platform that provides real-time detection and response to compromises and anomalies at scale, without the burden of deploying sensors, agents, or taps.

Based in Annapolis, MD, Netography® is backed by some of the world's leading venture firms, including Bessemer Venture Partners, SYN Ventures, and A16Z.