NETOGRAPHY

CASE STUDY

Global B2B SaaS Service Provider Automates Discovery, Onboarding, and Monitoring of New VPCs and VNets

Netography Fusion® eliminates risk of unknown workloads causing data breaches in AWS, Azure, and GPC environments

Company
Global B2B SaaS Service Provider

Industry
SaaS Service Provider

Size
3,000+ employees

"We needed to guarantee that any VPC or VNet that lights up in any region would be monitored because the risk is that a compromise will occur in an unexpected virtual network and when we go to investigate, we'll find out that no logs are available."

—Infrastructure Security Architect, Global B2B SaaS Service Provider

Challenges

- Lacked continuous network security monitoring in a dynamic multi-cloud network with 1000s of VPCs & VNets and 100s of accounts.
- Engineering-led organization was expanding cloud infrastructure utilization at a pace beyond the security team's ability to monitor it.
- Cloud NDR vendors' proposals required an unsustainable number of virtual appliances and monitoring nodes.
- Cloud vendors' proprietary solutions created silos of visibility and blind spots.

Solution

- Netography Fusion®

Results

- Achieved immediate onboarding and monitoring of all unmonitored VPCs and VNets; security team can now onboard hundreds of new VPCs and VNets in hours.
- Reduced potential for compromise of unmonitored workloads with automated real-time discovery and onboarding of all new VPCs & VNets.
- Ensured immediate application of policies and creation of historical logs for forensic purposes if needed in future investigations.
- Delivered holistic observability of anomalies and post-compromise activity across multiple clouds with significantly lower total cost of ownership (TCO) than competing proposals.

Snapshot

Global B2B SaaS service provider was experiencing the “wild west” of multi-cloud computing, with its developers and engineers spinning up new virtual networks faster than the security team could monitor. The operations team was overwhelmed as it tried to meet policy requirements to monitor every new VPC or VNet in every region. With thousands of VPCs and VNets across hundreds of accounts in its multi-cloud network, the team could not onboard new virtual networks promptly, leaving them unmonitored and potential compromise targets.

The service provider asked their incumbent NDR provider for a quote to monitor all VPCs and VNets across its multi-cloud network, but the proposal required an unsustainable number of virtual appliances and monitoring nodes. Other cloud vendors’ proprietary approaches were either comparably priced and/or lacked the platform coverage to monitor all activity, creating silos of visibility.

The B2B SaaS service provider approached Netography because of Netography’s proven ability to provide a holistic view of all activity in multi-cloud networks.

Solution

Netography Fusion® was the right choice, with its 100% SaaS cloud-native architecture and automated discovery, onboarding, and monitoring of any new VPCs or VNets.

Fusion’s frictionless architecture enabled the company to start monitoring any VPC and VNet in its environment without the burden of deploying sensors or agents. This significantly reduced the company’s TCO while improving its network security and observability.

Fusion is the fastest and easiest way to observe anomalous or malicious activity in real-time, including lateral movement, data exfiltration due to ransomware, and trust boundary violations.

The Fusion platform delivers a holistic view of all activity in your applications, clouds, accounts, and environments. It analyzes network activity logs across your AWS, Azure, Google, IBM, and Oracle clouds. It enriches this network metadata with dozens of context attributes from your tech stack to speed your response with a real-time, contextualized view of anomalous and malicious activity.

Results

Fusion delivered a wide range of benefits, including:

- Reduced potential for compromise of unmonitored workloads with automated real-time discovery of new VPCs & VNets.
- Ensured immediate application of policies and creation of historical logs for future forensic investigations.
- Lowered total cost of ownership (TCO) significantly and delivered holistic observability of anomalies and post-compromise activity across multiple clouds, including lateral movement.
- Fusion’s open detection models enabled the customer to quickly create customized detections to meet their specific requirements and built-in integrations with other cloud technologies to automate response workflows.
- Significantly lowered TCO associated with discovering, onboarding, and monitoring new VPCs and VNets.

About Netography

Netography® is the leader in holistic network security and observability. The Netography Fusion® platform is the fastest and easiest way to detect anomalous and malicious activity in your multi-cloud, single-cloud, or hybrid network. 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 or agents.

Based in Annapolis, MD, Netography is backed by leading venture firms, including Bessemer Venture Partners, SYN Ventures, and A16Z.