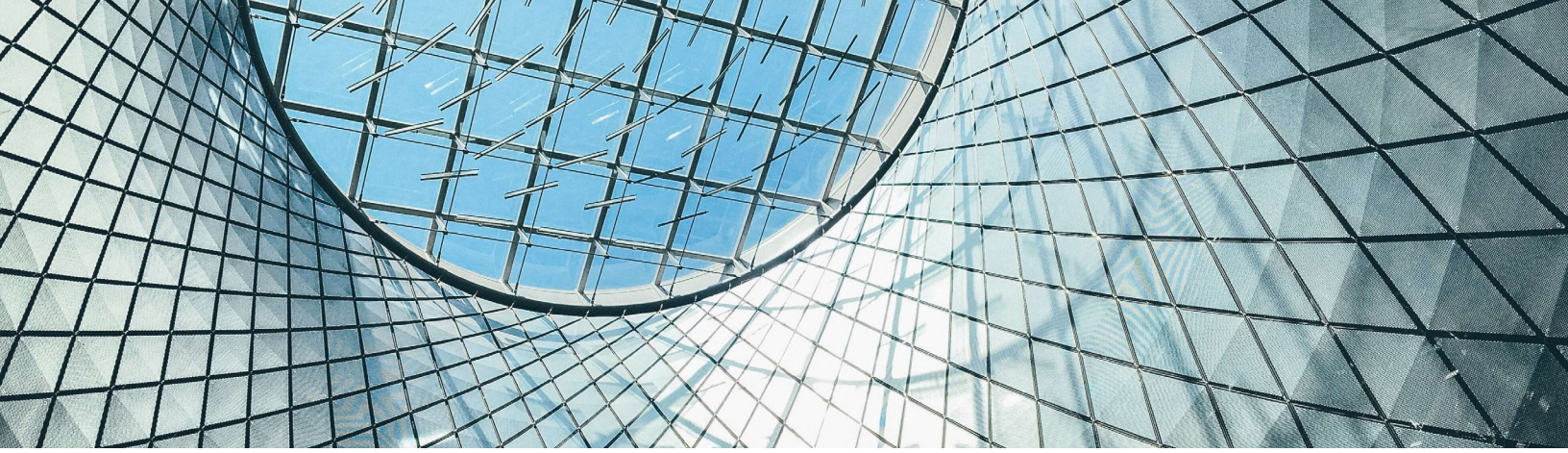

Market Insight Report Reprint

Coverage Initiation: Netography looks to change the network security landscape

November 9, 2023

by Eric Hanselman

Network security faces greater challenges due to increasing infrastructure complexity. To address this issue, Netography is aiming to deliver deeper insight by coupling greater context with better analysis, and has adopted a cloud-scale approach by combining extensive visibility with analytics and context integration.

S&P Global
Market Intelligence

Introduction

The focus on security visibility tends to ebb and flow between the various techniques that security practitioners have at their disposal. Strategies differed as tradeoffs were made between endpoint, network and infrastructure in attempts to sort out which offers the best insight. Netography is seeking to settle these debates by pulling in telemetry from on-premises and cloud, and applying better analytics to correlate activity and identify security threats.

This is an approach that could address the challenges that face the hybrid, multicloud world in which most enterprises find themselves. It also could tackle the issues associated with typical network detection and response (NDR) systems. Being able to span dissimilar chunks of infrastructure and align the event streams coming out of them with observability efforts — as they are taking place — is no small feat, but one that has great value to security teams wrestling with complexity.

THE TAKE

The perennial problems with security tools are the tradeoffs between depth of visibility and complexity of operation. Depth often comes with a loss of context, as monitoring points are far removed from the knowledge of what is creating the activities being monitored. Legacy network security approaches have always had to intuit the needed context, which is one of the reasons why AI had seemed so promising. Shifts in enterprise infrastructure to more hybrid operations have left older technologies behind in the whirl of complexity that is the modern environment. Netography has adopted a cloud-scale approach to this age-old problem by combining extensive visibility with analytics and context integration at levels that go beyond those legacy tactics. It is an approach that could deliver better insight and simplify security operations, but has to overcome resistance to these improvements.

Context

Netography aims to bridge the divide between the various sources of operational information in the modern enterprise and the understanding that can be formed from them. Over time, security teams have prioritized different information sources from the various parts of their siloed security tools, depending on where they felt they gained the best views. Endpoint received a strong focus until bring-your-own-device initiatives made agent deployments problematic. Network sensing in the early days of intrusion-detection and -prevention systems was detailed, but the high volumes of alerts could make it complicated to manage, and increasing levels of encryption masked content, despite it being a more resilient vantage point.

More recently, what started as endpoint detection and response (EDR) has been supplanted by extended detection and response (XDR) as the market once again realized that endpoint alone was not enough. Cloud infrastructure throws off vast quantities of telemetry, but to be useful it has to be correlated with the existing security tool suite. Netography is seeking to ingest all of these sources and make sense of them in ways that haven't been addressed by other approaches.

Founded in 2018 and headquartered in Annapolis, Md., the company's team includes network security veterans Dan Murphy as chief technology officer, who previously worked at Neustar and F5 Inc., and CEO Martin Roesch, who is well known as the founder of SourceFire (acquired by Cisco Systems Inc. in 2013) and is a pioneer in network security. It has raised a total of $48 million in funding, most recently a $45 million series A round in November 2021 led by Bessemer Venture Partners and SYN Ventures, with participation from existing investors Andreessen Horowitz, Harpoon Ventures Management, Mango Capital and Wing Venture Management. Netography has about 50 employees.

Already, the vendor has had to wrestle with one of a startup's more difficult conundrums — whether to pursue a promising project that might distract from its core product. In September, Netography spun off an extended Berkeley Packet Filter project that it had developed. Co-founders and former chief architect Barrett Lyon leads the new venture. Mango Capital is funding a seed round for the company. The eBPF initiative has seen significant interest and application as a kernel-level source of operational telemetry. It will face a field of other contenders, including Isovalent with the Cillium open-source project, Datadog Inc., Cisco's Splunk Inc. (via its purchase of Flowmill) and Sysdig. As a consumer of telemetry, it makes sense for Netography to develop a telemetry generator.

The company is addressing a range of needs, including replacing traditional NDR, compromise detection and threat hunting, security information and event management augmentation, and compliance validation. The latter is an area where many enterprises struggle to integrate information from hybrid and multicloud environments — correlation and coordination can be difficult without a single source of truth.

Technology

At its core, Netography Fusion is a network defense platform (NDP) with capabilities that go beyond the basics of NDR to offer more comprehensive visibility, detection and control. Its primary data feed is flow data from cloud and on-premises environments.

What makes Netography different is the extent of the context that it ingests to decorate that flow data and the analysis it performs. It is a challenge to do this at scale, which is a problem that has been identified by others. Analysis of flow data is something that has been done since the early days of networking. For instance, Boundary built a system that did massive raw network data ingest but struggled with scale, given the scope of its efforts and the technology available to the company.

Netography is betting that its approach to cloud scale can leverage flow data with greater intelligence. Flow data is attractive as it can offer a higher-level abstraction of a network conversation, rather than single packets. It also creates lower volumes of management traffic that has to be backhauled for analysis. Most network devices and all cloud services generate flow data, so it is easier to obtain. Agents or collectors aren't usually needed.

The historic argument against using flow data has been that it doesn't provide enough detail of the actual network traffic compared with deep-packet inspection (DPI) approaches. As network speeds rise, much greater percentages of network traffic are encrypted and zero-trust controls are put in place, DPI has become more difficult to implement successfully. Faster and more distributed networks require more and faster DPI engines to do analysis. Many enterprises have had to resort to complex networking arrangements such as network packet brokers to filter and route traffic for analysis to prevent DPI systems from being overwhelmed.

Encryption presents additional complications to DPI approaches. The latest network security protocols, including TLS 1.3, are built to protect against intermediate decryption, whereas earlier versions had allowed simpler observation of encrypted traffic. While there are still ways to intercept and decrypt traffic, there is the issue of having repositories of decrypted traffic that then become a target of attackers looking for troves of data, requiring proof of sufficient protection. As concerns about data privacy heighten, analysis techniques that rely on decryption have become less palatable.

Netography pulls in context from Active Directory, DNS, configuration databases, asset management systems and vulnerability management systems, as well as EDR, NDR and XDR systems. The vendor integrates this information with threat and vulnerability feeds to prioritize active threats. It builds comprehensive associations across these information sources that it says enable it to identify attacks in near real time. Netography notes that the associations it builds allow it to validate attacks rather than alert about activity that might lead to an attack, reducing alert volumes. The data collection that it builds also facilitates retrospective analysis, providing a useful tool for threat hunting.

Interestingly and a bit refreshingly, Netography doesn't lead with AI claims about its analytical capabilities. There is a significant amount of analytical work being done via a collection of techniques. New detection tools are added through Netography Detection Models that encompass detection and characterization capabilities that look at activity around attacks, as well as exploitation. NDMs can be used to kick off workflows for investigation and remediation.

Products

The vendor's main offering, the Netography Fusion Network Defense Platform, is delivered as SaaS. NDP's management console features consolidated views of network activity across the full set of infrastructure resources that are being monitored, and across multiple teams. It includes built-in integrations with identity providers such as Microsoft Corp. with Active Directory, and can extend to IoT and OT environments via integrations with the likes of Claroty.

Deployment is simply a matter of directing flow data to the platform and bolting up to context sources. Netography offers the optional NetoFlow Connector as an infrastructure gateway to filter, consolidate and encrypt traffic being sent to its monitoring environment. Fusion is sold on an annual subscription basis with pricing based on flow ingest rate and the retention period for ingested data.

Competition

While Netography faces competition from traditional network detection and response approaches, its key selling challenge will be overcoming entrenched approaches. For many, letting go of DPI and the need for internal packet views, even though they have become less useful and less available, is a significant step.

There are many contenders that are deploying advanced analytics on network traffic. Darktrace PLC has been a well-known face of AI-powered NDR while Vectra AI, ExtraHop and NetScout Systems Inc. are among the independent network security providers. There are open-source projects as well, including Suricata and its companion Zeek, that cover parts of the NDR space, are in wide deployment, and form the core of other offerings. There have also been acquisitions over the years from the likes of Palo Alto Networks Inc. and VMware Inc. as they sought to add network security expertise.

Additionally, there have been divestitures such as Gigamon's sale of its ThreatInsight division — obtained in its purchase of ICEBRG — to Fortinet Inc. Core networking specialists like Arista Networks Inc., Cisco and Juniper Networks Inc. all lay claim to network security functionality. Cloud suppliers have network security capabilities that also vie with Netography, but like the other players above, they address only parts of the whole that Netography works to pull into a single view. A handful of newer entrants, including Cynamics, Lumu, MixMode and StellarCyber, have also adopted a similar NDP strategy.

SWOT Analysis

STRENGTHS

Netography's analytics at scale with significant amounts of context can provide visibility into ways that have been hard to extract from legacy approaches that have difficulty spanning modern hybrid and complex environments. Its simplicity of deployment lowers the transitional energy required for adoption.

WEAKNESSES

A mindset change is needed in security teams to shift the compartmentalized approaches that exist today. This will require stepping out of their comfort zones to adopt better ways of addressing a complex problem.

OPPORTUNITIES

Having built complex associations across network traffic, there is an opportunity for Netography to extend some of the compliance capabilities into application-level perspectives and cloud security posture insight.

THREATS

Major rivals have already claimed the ability to pull together disparate telemetry, and will continue to assert that their methods are sufficient.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence