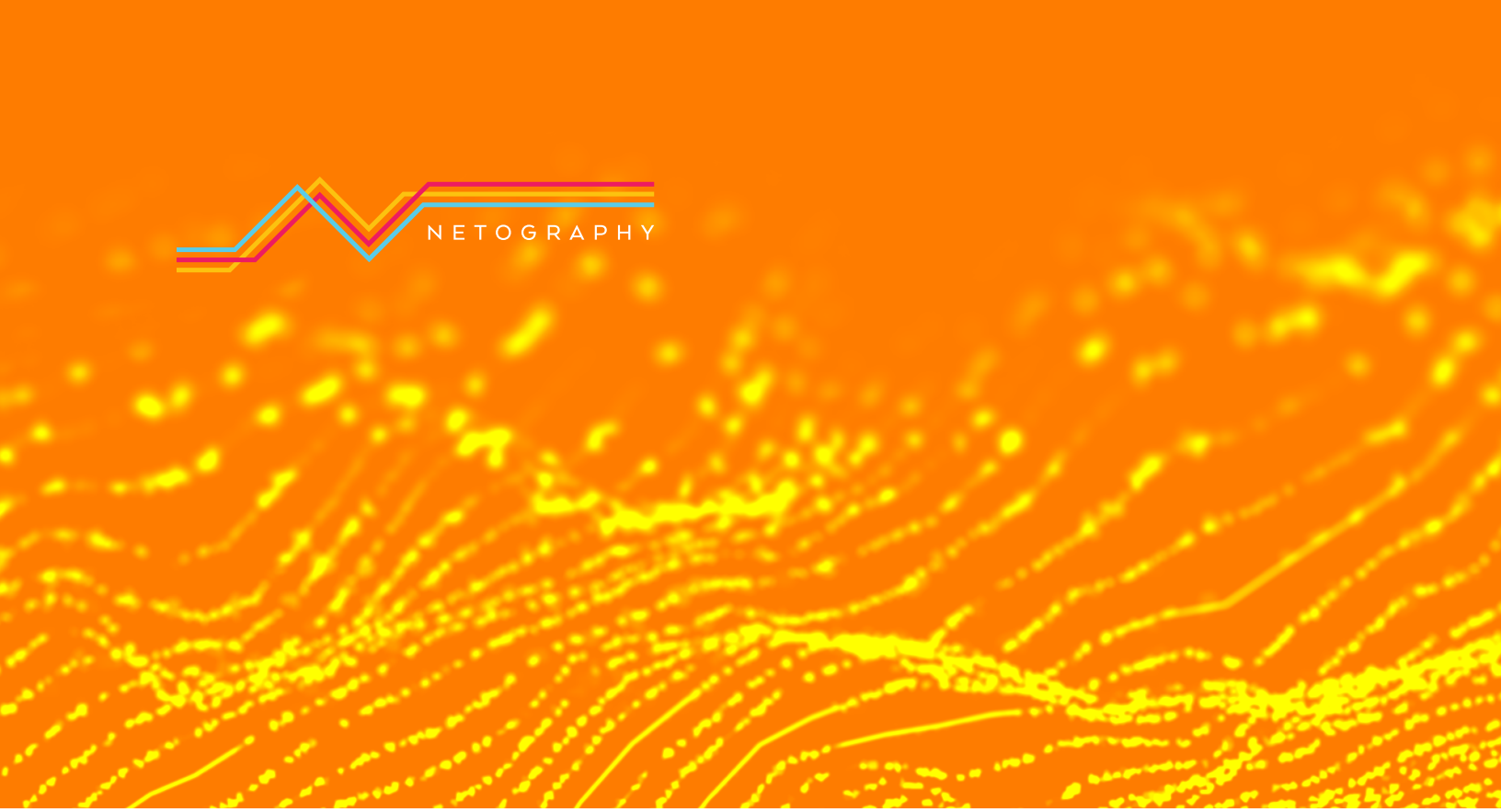


A Reckoning: The Massive Implications of Losing Network Visibility & Control

Networks have become atomized, which means they are dispersed, ephemeral, encrypted, and diverse. The old rules and technologies designed to secure enterprise networks have become unsuited for the security requirements of Atomized Networks.

This is what's required.

By Martin Roesch

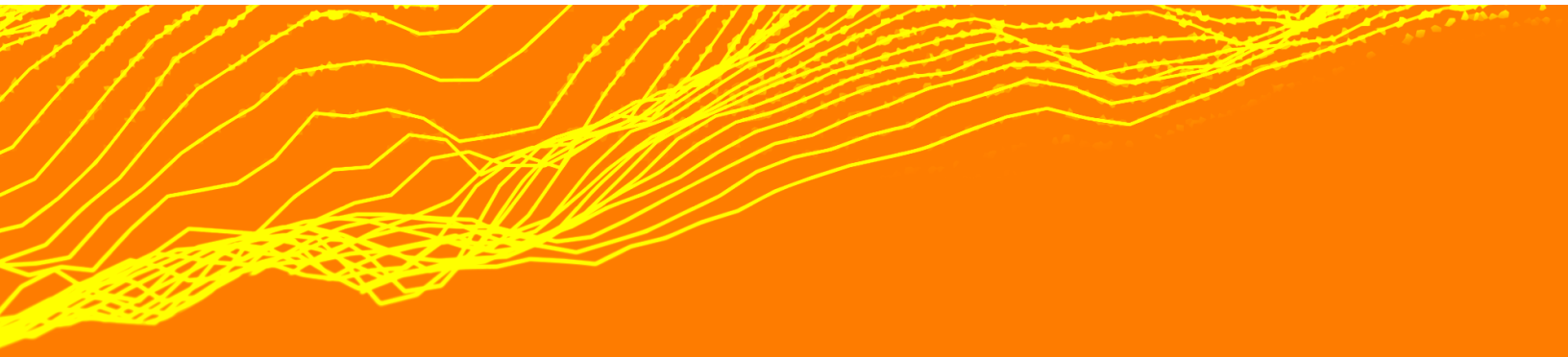


Table of Contents

Author's Foreword

Curiosity about the composition of networks and the activities of their components and users drove me to develop Snort as the 90s came to a close. At the time, exploitation of networks was increasingly recognized as a threat to the nascent commercialization of the internet. The available security tools of the day were expensive, hard to use, and limiting for those trying to defend themselves. Open source software was similarly early in its adoption as enterprise technology. I built Snort, and then Sourcefire, with the idea that giving people powerful tools to enable their ability to defend themselves against all comers and to marry world-class open source technology and enterprise business needs together was a huge shift that security operators were waiting for.

Now, we're on the cusp of another major movement and the next shift that needs to happen.

You might have heard me talk about some of these themes before because the fundamentals of security haven't changed. What has changed is the environment security professionals operate in—the composition of the networks we need to protect, the categories of attacks we face, the teams we operate within, and the effectiveness of the capabilities we've relied on historically. To be able to defend our environments, we must fully appreciate what today's networks really look like and the doctrinal shift that's required in enterprise security. Some of the core approaches to network security are being obsoleted. Nothing has replaced them. And no one seems to appreciate this.

While endpoint detection and response (EDR) and Zero Trust architectures are critical, the importance of network visibility and control has gotten lost in the hype, and new categories of attacks reveal the consequences of the reduction in capabilities. Attackers have plenty of places to hide as networks, and entire enterprises, become atomized. So, our approach to securing the modern enterprise network must adapt. Instead of trying to secure our environments with architectures and technologies developed decades ago, a new architecture and approach must be forged.

Current Problem: Atomization of Networks

The pandemic kicked off a rapid evolution of networks that have become composites of multi-cloud, hybrid-cloud, and on-premises infrastructure, with mobile and remote workers accessing data and applications scattered across this complex and fluid computing environment. We refer to this evolution as the "atomization of networks" and the implications for network security are massive.

We refer to this evolution as the "atomization of networks" and the implications for network security are massive.

Environments are dispersed, not just geographically from office to office and data center to data center. With the cloud, we may also have hundreds of cloud instances on one cloud or across multiple clouds. In the software-as-a-service (SaaS) world, our applications and data are hosted on someone else's infrastructure. This can all be spun up in a matter of minutes, without the knowledge and buy-in of security teams. Many devices connecting to the Atomized Network are simply out of our control—personal devices, critical infrastructure assets, and rogue smart devices. And, as a chief information security officer (CISO) said to me about his cloud infrastructure concerns during the height of the pandemic, "the only thing that keeps me up at night is that I've got a thousand developers working from home, and they all have credit cards."

In this ephemeral environment, the concept of a defined edge no longer exists and the traditional view of North-South and East-West traffic has limited utility. We try to secure the chaos—across clouds, instances within clouds, untethered endpoints, and physical spaces—with a dispersed set of tools and operational teams with potentially very little overlap.

Technologies responsible for network security are being obsoleted by the major evolutionary pressure brought about by the Atomized Network. And nothing has replaced them.

Meanwhile, the pervasive use of encryption in security-as-a-service and Zero Trust environments blinds deep packet inspection (DPI) technologies. And there is no way to deploy DPI technologies in relevant timeframes when they are primarily delivered on appliance-based architectures and the concept of defined locations has all but disappeared. Technologies responsible for network security are being obsoleted by the major evolutionary pressure brought about by the Atomized Network. And nothing has replaced them.

Zero Trust architectures and EDR were supposed to obviate the need for network-based threat detection and protection. But Zero Trust identity-based access permission models can be bypassed or circumvented. And while EDR provides unique value for dealing with client-side attacks, it has limitations. Once an attacker has access to the network, where network security has been falling by the wayside, attackers have plenty of places to hide, taking advantage of the gaps between the siloed technologies and teams who manage them.

We are facing a reckoning. The Atomized Network is dispersed, ephemeral, encrypted, and diverse. So, organizations are blind to the composition of their networks and entire categories of attack and compromise detection. The fallout is evident:

— An attacker bypassed multi-factor authentication (MFA) by spamming a contractor's MFA device, repeatedly requesting the user to confirm they were logging in. Eventually, the user relented and clicked "yes," and the attacker was in and able to move laterally to gain access to cloud infrastructure.

— Via remote code execution (RCE) over the network, an attacker leveraged a vulnerability, broke into a device, and established presence on the device without interacting in a way that would cause the installed EDR agent to detect hostile activities. At that point, the attacker used Active Directory to map the network and spread laterally, deploy ransomware extensively, and disrupt significant portions of the network.

Enterprises struggle to defend the Atomized Network because they have no way to see the users, applications, data, and devices they have, what they are doing, and what's happening to them.

Back to Fundamentals: Before, During, and After

Amidst this fog of war, it is important to understand the security tasks that must be performed and which tools are used to complete them. Security scope and the threat continuum are core principles the security industry has been built around, and what drive the security capabilities we deploy to protect enterprise networks. I used these two frameworks when I changed the market before, which are still relevant to explain why we need to change the market again.

Security scope. For years organizations have put forward the ideas of a "defense in depth" approach, layering multiple tools to arrive at a set of capabilities intended to fully secure their network. But the truth is, defense in depth doesn't exist. It's a misnomer. What we are dealing with most of the time is defense in adjacent scope. As a simple example, an NGFW doesn't deal with malware, and EDR doesn't deal with network-based threats encoded in network protocols. Each of these tools and, for the most part, the array of different security technologies we deploy has its own scope of coverage and its own scope of responsibility. Aside from the feature/function race between vendors within product categories, there is very little real functional overlap. Broadly speaking, network-based tools are scoped for different classes of attacks than endpoint-based tools.

We also have different time periods in which security occurs: before an attack happens, during an attack, and after we've been compromised.

Threat continuum. We also have different time periods in which security occurs: before an attack happens, during an attack, and after we've been compromised. In each phase of this threat continuum, there are different tasks and tools we use to complete them. But the actual time within each phase to do the job is not equal.

Before an attack, we have a "nigh-infinite" amount of time to prepare defenses and make it hard to be compromised in the first place. Over the years, the names and categorization of the tools have changed, and today we deploy tools like cloud security posture management (CSPM), attack surface management (ASM), firewalls, and zero trust network access (ZTNA). We also do tasks like vulnerability management and patching to enforce compliance policies. We spend a lot of time discovering, configuring, and hardening the environment, so it is difficult for an attacker to compromise a network in the first place. But if an attacker does get through and if all goes well, we've mitigated the damage an attacker can do. At least that's the promise of ZTNA with its blast containment concept with the goal of forcing authenticated access to resources on the network and devices and encrypting everything—including network traffic—by default.

At the point of attack, we typically have milliseconds to detect and prevent an attack with EDR, an intrusion prevention system (IPS), or a next-generation firewall (NGFW). For example, when a possible RCE exploit is being transmitted over the network or traversing a device, we have to detect and decide whether or not we will block it in real-time. If we detect and make the right decision, we're in good shape. If we don't, our "During" technology has no more opportunities to detect and do something about that attack unless it is a component of an architecture designed to deliver continuous capability beyond the point of attack in the after phase, and most are not.

> *The reality, at this point, is that many enterprises are hamstrung because they have become functionally blind to the composition and activities of their Atomized Networks, and when there is a compromise that ultimately translates to longer dwell time and more damage done by attackers.*

After an attack, we once again have a "nigh-infinite" amount of time to figure out that we've been compromised and then scope, contain, and remediate using tools like cloud detection and response (CDR), log management, SIEM, SOAR, and network detection and response (NDR). In reality, we need to do this as quickly as possible because the corollary is that attackers also have a nigh-infinite amount of dwell time, and the longer they have access to a compromised network, the more damage they can do. They can and frequently do remain undetected for months or even years and damage can escalate massively. This is our chance to detect and stop the activities of an attacker post-compromise as they establish persistence, spread laterally, and exploit their access.

When we think about the threat continuum, organizations spend a lot of time and effort focused on the "Before" phase—discovering, configuring, and hardening the environment. The goal is to make it hard to break into a network at all in the first place and hopefully obviate the need for other security technologies. In practice, there are always methods of getting in that people don't anticipate. Authentication mechanisms can be subverted, vulnerabilities in software can be exploited, and identity-based access control systems can be abused to gain deep access into the network. So, it's important to get a handle on the "During" and "After" phases because rapid response can mean the difference between a minor incident and a major breach.

The reality, at this point, is that many enterprises are hamstrung because they have become functionally blind to the composition and activities of their Atomized Networks, and when there is a compromise that ultimately translates to longer dwell time and more damage done by attackers.

— For the past seven years, the average time to identify and contain a breach has been 277 days.
— In 2022, the average total cost of a data breach reached a record high of $4.35 million, with the US being the costliest country with an all-time high of $9.44 million.
— 83% of organizations studied experience more than one data breach.

It's a grim situation. However, through bold thinking and innovation, at Netography we are on a trajectory to change it.

Time to Evolve

We need to recognize the world for what it is, not what it used to be, and build for that world. If we continue to be constrained by old thinking, we'll never be able to reduce the mean time to detect (MTTD) and mean time to respond (MTTR) and start driving down the cost of a data breach.

> *Technologies scoped and responsible for network security in the During and After phases—NGFW, IPS, and NDR—are losing potency and becoming at risk of going away because of three evolutionary pressures on DPI technologies delivered on appliances: deployment, encryption, and cost.*

Real-time plus retrospective technologies provide more "at bats" to identify the presence of a threat actor post-compromise so that we can scope, contain, and remediate attacks. But several of the core technologies scoped and responsible for network security in the During and After phases—NGFW, IPS, and NDR—are losing potency and becoming at risk of going away because of three evolutionary pressures on DPI technologies delivered on appliances: deployment, encryption, and cost.

— The Atomized Network makes comprehensive deployment of appliances impossible. Physical appliances require power, cooling, and spec'ing so they can't move easily to address evolving needs. Coverage is also limited to whatever network's packets can be presented to it, so the ability to monitor traffic using an appliance-based architecture is outstripped as networks disperse into the cloud and ephemeral workload environments.
— Zero Trust and software-as-a-service have accelerated the broad usage of encryption, blinding many of the capabilities of DPI, primarily attack detection and packet analysis capabilities. Workarounds like hardware-assisted decryption can create scalability issues as decryption consumes overhead, increases costs, and hampers performance.

— The costs of an appliance-based architecture are considerable. Physical devices must be shipped to locations when and where capabilities are required. Supporting infrastructure, including packet brokers and decryptors, must be in place. And ongoing lifecycle management of hardware and software, plus configuration and manual updates, limit agility and create ongoing operational costs.

We thought we had built a better mousetrap with Zero Trust and moving to the cloud, but the need for network-based security has not lessened. Two-thirds of enterprises don't see moving fully to the cloud, ever. And when authentication mechanisms are subverted or identity-based access control systems are abused to gain deep access into the network, the pervasive use of encryption makes compromises incredibly difficult to detect or prevent with existing network technologies. In the absence of traditional defensive analysis, validation, and protection on the network, attacks can land unhindered on a device and the only line of defense at that point is EDR.

EDR is obviously valuable and provides unique visibility into local processes and system activities. However, its capabilities to detect and contain are limited if the attacker uses techniques outside its scope of coverage and area of responsibility. Additionally, many endpoints and networked devices, including IoT devices, serverless platforms, routers, switches, and critical infrastructure assets, are incapable of running EDR agents. Furthermore, many organizations aren't aware of every endpoint connected to their Atomized Network, and even if they are, that endpoint may be out of their control, from the high-tech vending machine in the breakroom to a consultant's smart device. Entire classes of devices can be left unprotected, so having an effective network security architecture beyond access control and access brokering is even more important.

With as many security technologies as are available now, the solutions have not evolved with the problem. Instead, they have only been developed to target parts of the problem with no regard for the whole, which has created functional and operational gaps in threat detection and prevention on the network.

Visibility into network traffic moving to, from, between, and within clouds presents its own set of challenges. Traditional network security tools don't support cloud environments, and cloud-based tools focus on providing visibility into specific cloud environments but very rarely into multi-cloud or the rest of the infrastructure. Additionally, all clouds are not created equal, and few standards exist for the type of data and level of visibility cloud providers offer. Detecting and stopping attacks is incredibly difficult, given the opacity and gaps. Organizations are feeling the pain, with 45% saying they experienced a cloud-based data breach in 2021, and more than half believe security risks are higher in the cloud than on-premises.

With as many security technologies as are available now, the solutions have not evolved with the problem. Instead, they have only been developed to target parts of the problem with no regard for the whole, which has created functional and operational gaps in threat detection and prevention on the network; gaps that can only be addressed with a methodology and architecture for treating networks as a unified composite to be secured by an overarching platform.

The Atomized Network is dispersed, encrypted, ephemeral, and diverse. At Netography, we are rethinking network security visibility and control with a new architecture built for this atomized world with fundamental capabilities to inform operators what they've got, what it's doing, and what's happening to it.

> *With telemetry across the Atomized Network, we can see the users, applications, data, and devices we have, what they are doing, and what's happening to them. We can detect threats everywhere and determine the right actions to take and gain control.*

Security for the Atomized Network

I first advised and later joined Netography as CEO because if I had personally created the next technology to address the challenges of securing modern, enterprise networks, this would have been it. What co-founders Barrett Lyon and Dan Murphy created was extraordinarily visionary. Visibility is the critical foundation in understanding that there is a seismic shift in what networks look like and we need to be able to view the Atomized Network and network traffic in a unified way. With telemetry across the Atomized Network, we can see the users, applications, data, and devices we have, what they are doing, and what's happening to them. We can detect threats everywhere and determine the right actions to take and gain control.

This isn't possible when teams work in isolation using tools built for how the network used to be, not for how it is today. The Atomized Network is...

— Dispersed. We need a solution we can deploy across the entire Atomized Network with threat detection models we write once to protect everywhere, instead of a dispersed set of tools with different logic for detection, operated by siloed network, security, and cloud operations teams.

— Ephemeral: We need a solution that can be deployed on demand in seconds or minutes, instead of appliance-based models that take weeks or even months to deploy.

— Encrypted: We need a solution that is encryption agnostic, providing an equal set of capabilities to users regardless of the presence of encryption on a network.

— Diverse. We must be able to defend the network as one composite system, instead of relying on a panoply of diverse cloud and on-premises solutions that are separate and distinct.

> *That's why we invented Netography Fusion, which we refer to as an Network Defense Platform (NDP), a cloud-scale, network-centric platform, specifically architected to deliver unified capabilities regardless of the nature and location of what is being defended. At its core, Fusion generates a real-time network event stream with anomaly detection and compliance analysis.*

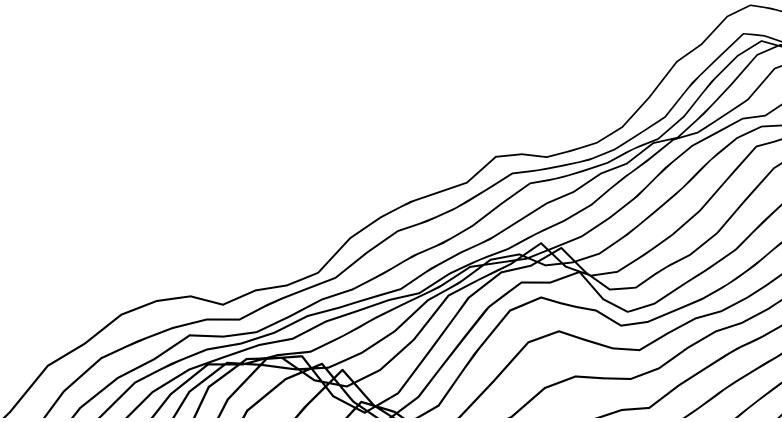
That's why we invented Netography Fusion, which we refer to as an Network Defense Platform (NDP), a cloud-scale, network-centric platform, specifically architected to deliver unified capabilities regardless of the nature and location of what is being defended. At its core, Fusion generates a real-time network event stream with anomaly detection and compliance analysis.

We've achieved this by reconstituting the network security capabilities disrupted by dispersion and encryption with an approach that lives off the land, relying on network flows, metadata, and enterprise context—not packets—to provide complete network visibility and control. Our SaaS-based universal platform deploys frictionlessly to deliver capabilities immediately when and where they're needed across the Atomized Network. A single portal provides a unified view of all data across the entire ecosystem, enriched with security and business context to provide a complete picture of what's happening so users can pinpoint malicious activity, monitor for compliance, and hunt threats. Security operations center (SOC) and cloud operations teams can detect and respond to attacks in real-time as they emerge with interoperability across the security stack, which provides the opportunity for rapid response so that attackers can't leverage their footprint in the network.

We've achieved this by reconstituting the network security capabilities disrupted by dispersion and encryption with an approach that lives off the land, relying on network flows, metadata, and enterprise context—not packets—to provide complete network visibility and control.

The industry continues to raise the bar for attackers with aggressive measures to make networks more difficult to hack. Yet history shows us time and again that controls can be abused, vulnerabilities in software can be exploited, and user error invariably happens. Network security will always be important to limit the "blast zone" of a compromise, reduce attacker dwell time, minimize the cost of breaches and downtime, and prevent future intrusions. However, to be effective, it needs to be architected for the Atomized Network.

With Netography Fusion, we tell you what you've got, what it's doing, and what's happening to it. We're where you need us, when you need us. We are immune to encryption. And we look at your network as a composite of its components, not as a pile of components with separate solutions to figure out what is there. It's the only security product that secures the Atomized Network.



Addendum: The Checklist

The gaps we have created in the industry for attackers to dwell in—and dwell in longer—because of our siloed technologies and teams have become a crisis. Organizations need a platform architected for a new era in enterprise security.

To discover the gaps you face, and the opportunity you have to better protect your environment, ask yourself the questions below. Go through them like a checklist, then, reach out and we'll be happy to show you what scalable, continuous network security and visibility across your Atomized Network looks like and how teams from across your organization can benefit.

Environment:

- ☐ Is your environment multi-cloud or hybrid? What types of tools do you use to protect them?
- ☐ Will you always have some on-premise infrastructure?
- ☐ Have you recently undergone a merger or acquisition and do you have visibility into and control of those networks?
- ☐ Do your security teams have the same level of network visibility and control across all geographic locations?
- ☐ Do you expect your network to continue to evolve?

Teams:

- ☐ Does it take more than 30 minutes for a new analyst to get up and running?
- ☐ Are your SOC and cloud teams able to work from the same, real-time set of data to collaborate on threat detection and response?
- ☐ Do your teams have the data they need when they need it to understand what is happening and respond rapidly?

Tools:

- ☐ Are you relying on DPI-based appliances for network visibility and control?
- ☐ Do you have EDR deployed on every endpoint? If not, how do you protect those endpoints?
- ☐ How do you protect your cloud/multi-cloud networks and monitor the traffic between them, and with your on-prem environment?
- ☐ Are you confident your asset inventory is accurate and always up-to-date?

Processes:

- ☐ Does it take more than 15 minutes to get the answer to a question, such as: "Are there any communications with country X?"
- ☐ How often do your security teams run reports and is it with enough frequency?
- ☐ How do you measure security effectiveness and efficiency and are you satisfied with your teams' performance?
- ☐ Can your compliance team answer auditors' questions in minutes?
- ☐ How do you handle remediation across your Atomized Network?

About the Author

Martin Roesch is the CEO of Netography, Inc. He has been one of the most formidable voices in establishing critical change in the cybersecurity industry over the past 25 years. As the creator of the Snort Intrusion Detection and Prevention System, Martin is a pioneer in the industry as one of the first entrepreneurs to successfully commercialize open-source software—in addition to creating the global standard for describing and detecting network-based attacks. In 2001 he founded Sourcefire, serving as CEO/CTO, until the 2013 acquisition by Cisco for $2.7 billion, where he went on to lead the Security Business Group as Chief Architect. He has received substantial recognition over the course of his career for innovation and was selected as one of the Top 25 Disrupters of 2013 by CRN Magazine as well as one of eWeek's Top 100 Most Influential People in IT. He holds a B.S. in Electrical and Computer Engineering from Clarkson University.

NETOGRAPHY

About Netography

Netography® has created the first network-centric platform that reconstitutes capabilities disrupted by the combined impact of encryption and Atomized Networks across the security world. Enterprises have become functionally blind to the composition and activities of their networks, resulting in increased dwell time and more attackers leveraging the gaps between the capabilities of an organization's other tools and the siloed operations teams who operate them.

Netography Fusion® is for enterprise security operations center (SOC) and cloud operations teams that need scalable, continuous network visibility across the Atomized Network – legacy, on-premises, hybrid, multi-cloud, and edge environments. With the Netography Fusion platform, these teams gain visibility and control of network traffic and context across users, applications, data, and devices, to see what they are, what they are doing, and what's happening to them.

Netography is the only company that delivers Security for the Atomized Network®. Based in Annapolis, MD, Netography is backed by some of the world's leading venture firms, including Bessemer Venture Partners, SYN Ventures, A16Z, and more.
For more information, visit netography.com.