Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

Why Comprehensive Network Visibility Is Foundational for Effective Threat Detection and Response

By John Grady, ESG Senior Analyst

May 2022

This ESG White Paper was commissioned by NETSCOUT
and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

Network threat detection and response is more important, yet more challenging than ever. Organizations must grapple with navigating an increasingly sophisticated threat landscape despite inefficient tools and a problematic shortage of cybersecurity skills. As a result, many organizations report network blind spots as a result of their increasingly diverse and dynamic environments, leaving them open to potential compromise. To address these issues, comprehensive visibility across the entire network should be a foundational element of any threat detection and response program. This helps ensure security analysts have the information they require to identify potential incidents quickly, diagnose threats accurately, and perform full, potentially packet-level investigations to contain attacks efficiently. NETSCOUT Omnis Security leverages NETSCOUT's strong track record of providing comprehensive network visibility via highly scalable packet acquisition and analysis in the most sophisticated network environments. When coupled with Omnis Cyber Intelligence, Omnis Security allows security analysts to harness this visibility to make cybersecurity more efficient and effective.

Comprehensive visibility across the entire network should be a foundational element of any threat detection and response program to help identify incidents quickly, diagnose threats accurately, and support efficient investigations.

The State of Threat Detection and Response

As the volume and sophistication of attacks continues to grow, threat detection and response has become a critical area of emphasis for many organizations. In fact, ESG research has found that 83% of survey respondents expect to increase spending on threat detection and response technologies, services, and personnel over the next 12-18 months.[1] Yet despite this prioritization, many organizations continue to struggle for a variety of reasons (see Figure 1). Specifically:

- Thirty-one percent said they spend most of their time addressing high priority and emergency threats, rather than strategy or process improvements. This puts security teams in an unending cycle of inefficiency where the inability to implement needed structural changes to the security program drives a continuous flood of incidents. Many security teams are understaffed and underskilled as it stands. The resulting burnout from always operating in a firefighting mentality only exacerbates the skills shortage.

- Twenty-nine percent indicated that they have blind spots on the network due to the inability to deploy agents. The acceleration of cloud adoption, coupled with the shift to remote work has dissolved the traditional network perimeter. Further, due to BYOD and IoT, the number of devices connecting to corporate resources has exploded. Maintaining comprehensive network visibility has become increasingly difficult for all these reasons.

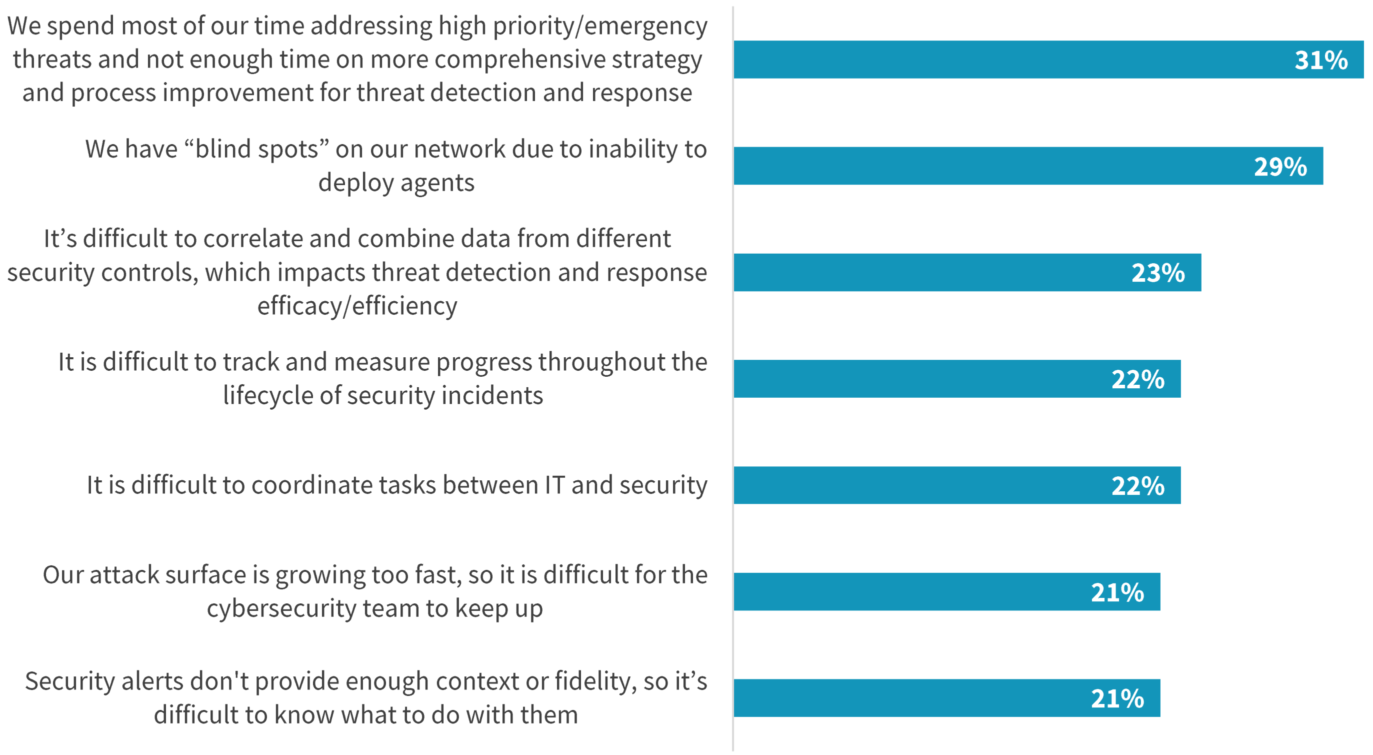
- Twenty-three percent say it is difficult to correlate and combine data across different controls. Directly related to the point above, as the environment has expanded, new tools have been added to close some of the aforementioned gaps. Unfortunately, this often results in siloed data sets across EDR, SIEM, and NDR tools which analysts must attempt to piece together—an often inefficient and ultimately ineffective process. As attacks have become more advanced, identifying and preventing lateral movement, privilege escalation, command and control traffic, and other stealthy behavior has become more difficult when visibility is limited to specific parts of the attack chain.

[1] Source: ESG Survey Results, *The Impact of XDR in the Modern SOC*, February 2021. All ESG research references and charts in this white paper are from this survey results set.

- Finally, 21% say that their alerts do not provide enough context or fidelity. The skills shortage again comes into play here. The inefficiency stemming from investigating false positives and working with incomplete information can be difficult to overcome when teams do not have the right number of analysts in the SOC or are forced to assign more sophisticated tasks to junior personnel.

Figure 1. Top Seven Threat Detection and Response Challenges

Which of the following would you say are your organization’s biggest challenges regarding threat detection/response? (Percent of respondents, N=388, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

The Visibility Paradox

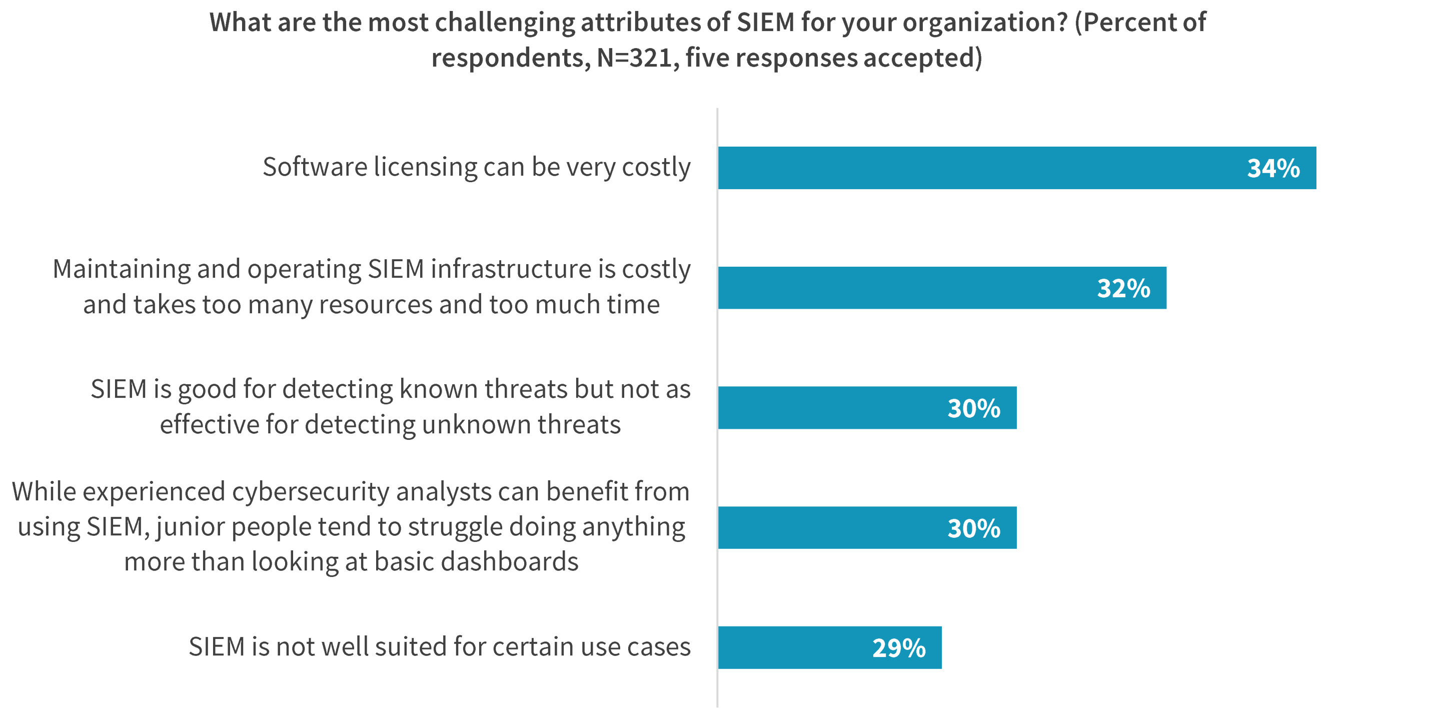
As noted, nearly one-third of organizations say they have blind spots on the network. This is a glaring statistic, as establishing comprehensive network visibility across the environment should be a foundational element of any threat detection and response program. With modern environments as diverse and dynamic as they are, security analysts must be able to understand the entities connecting to the network, the resources they are accessing, and external locations they are communicating with, at all times. Security teams use a variety of tools, some of which will be discussed further in this paper, to establish this type of visibility. Unfortunately, many have limitations or notable gaps that prevent them from delivering on all the points mentioned above.

Security analysts must be able to understand the entities connecting to the network, the resources they are accessing, and external locations they are communicating with, at all times.

SIEM

SIEM remains a staple in many SOCs for threat detection, incident investigation, and threat hunting. Yet many organizations continue to cite issues with the cost, complexity, and effectiveness of their SIEM (see Figure 2). A contributing factor to many of these difficulties is the dependence of SIEMs on logs from security controls and other infrastructure. The amount of log data generated in large environments can quickly become overwhelming for security teams, leading to higher operational expenses and making it difficult for analysts to find exactly what they need in a timely fashion. Further, log data is internal in nature and lacks external context such as threat intelligence. This can make it harder to detect never-before-seen attacks and can prevent analysts from quickly validating the severity and scope of a threat when a compromise does occur. Finally, attackers may disable log collection during an attack to cover their tracks, preventing the SIEM from detecting malicious activity.

Figure 2. Top Five SIEM Challenges



Source: ESG, a division of TechTarget, Inc.

Endpoint Detection and Response

Endpoint detection and response (EDR) has become a core component of endpoint protection strategies. However, devices represent only one avenue of attack, forcing EDR vendors to expand into adjacent areas such as cloud to provide broader coverage and visibility. Unfortunately, while deploying agents can be burdensome on traditional endpoints, it can become untenable in cloud environments. Server instances are often ephemeral or do not support agent implementations. Additionally, seamlessly inserting the deployment of security tools into agile development practices such as DevOps continues to be a work in progress for many organizations. Pivoting to the traditional network, IoT devices represent an increasingly important aspect of the attack surface and typically do not support agents. Regardless of location or device type, even when agents can be deployed, they can be disabled early in the attack chain, or the attacker can hide their tracks in registry or disk, leaving security teams blind to any subsequent malicious activity.

Cloud Service Provider Tools

Cloud service providers (CSPs) offer many of their own security tools supporting compliance, threat detection and response, and other use cases. While these tools can be simple to deploy via native CSP management consoles, they often do not extend to other CSP or traditional on-premises environments. This results in additional silos for both visibility and management, which introduces more complexity and can reduce security effectiveness.

Network Detection and Response

Network-based tools such as network detection and response (NDR) can help overcome some of the issues created by SIEM, EDR, and CSP tools. NDR provides a more holistic view of the broader environment. The agentless architecture alleviates some of the deployment complexities associated with agents and does not require insertion into DevOps processes. Additionally, because detection sits out-of-band, attackers cannot tamper with or circumvent the tool.

On the other hand, the way some NDR tools collect and store network traffic data can impact the effectiveness and manageability of the solution. Flow-based methods (such as NetFlow) which capture basic information such as source and destination IP address, port, and protocol are often not granular enough to help analysts uncover sophisticated attacks. On the other hand, full packet capture (PCAP) can be expensive and slow. While PCAP provides the granularity that flow records do not, it can be difficult to deploy at scale, prohibitively expensive to store data for more than a few days or weeks, and inefficient to search for specific data artifacts.

Intelligent Packet-based Network Visibility as a Key Pillar of Advanced Threat Detection and Response

So where should organizations be focusing and what should they look for in tools to support their threat detection and response initiatives? Despite the drawbacks of some NDR approaches, establishing network visibility is absolutely the right place to start and a fundamental requirement for effective cybersecurity. The network cannot be evaded, is extremely difficult to manipulate, and is always on. This makes the analysis of network data, in conjunction with other data types and security controls (such as SIEM and EDR), an increasingly critical discipline for cyber investigations. However, for this process to be effective, organizations require intelligent, packet-based network instrumentation. The most important characteristics to consider include:

Despite the drawbacks of some NDR approaches, establishing network visibility is absolutely the right place to start because the network cannot be evaded, is extremely difficult to manipulate, and is always on.

- Holistic network visibility. Security analysts need breadth and depth of visibility through both flow and PCAP collection. The combination of baseline, transactional data with the granular data of the packets themselves paints a complete picture from which analysts can draw more accurate conclusions. Further, by combining these into a single platform, analysts have consolidated access to a massive amount of metadata from which they can quickly triage alerts and move into more thorough packet-based investigations as needed, without having to pivot between different consoles.

- Scalability. The diversity of enterprise networks requires a variety of deployment options for full coverage across hybrid, multi-cloud environments. Traditional, on-premises data centers and other performance-sensitive locations require dedicated, performant hardware appliances. At the same time, branch and remote locations rely on software-based appliances running on commercial hardware and the cloud on virtual appliances. The flexibility to deploy the correct instrumentation based on location delivers the consistent, comprehensive views needed to close the network visibility gaps plaguing many organizations.

- High performance. In addition to holistic visibility and deployment flexibility for scalability, network-based tools must support full line-rate packet capture, real-time conversion to layer 3-7 metadata, and longer retention periods to enable deeper investigations. With many organizations moving or planning to move to 100Gbps in the data center, network visibility and security tools must follow or will become obsolete. The massive amount of data collected in these environments requires cost-effective, high-capacity storage for terabytes worth of data. These needs can quickly reach into the hundreds of terabytes when retention is extended beyond just a few days or weeks. Finally, the storing, indexing, search, analytics, and investigative capabilities of these tools must scale along with the data collection. Analysts should be able to quickly search and identify relevant data without a significant lag to ensure timely detections and investigations.
- Integration and export. These advanced network detection and response tools must also have the ability to integrate seamlessly into an existing cybersecurity stack and established processes. The use of open standards and published APIs can help enable this. Additionally, the massive amount of valuable raw metadata that is created by these NDR solutions should be capable of being exported to third-party data lakes, where it can be combined with other data sets, supporting custom threat analysis.

Advanced network detection and response platforms with these characteristics provide organizations with a comprehensive view across the entire digital infrastructure, including cloud. This is not to say that network-based solutions alone are the answer. However, network visibility and detection is critical to complement tools like SIEM and fill the gaps EDR and CSP tools cannot effectively cover. With intelligent network visibility tools, SOC teams can conduct highly contextual threat detection and investigation using packet-derived smart metadata that has linkages to full packet decodes if required. From a proactive perspective, this visibility into network traffic and entities can help teams build out zero trust strategies by understanding baseline behaviors to ensure the security architecture is correctly implemented. Additionally, a long-term, high-fidelity source of packets and layer-7 metadata that can be used for root cause analysis of attacks with long dwell times increases the likelihood that advanced attacks are detected and fully resolved. Finally, while these tools help organizations reduce their risk profiles, they importantly do so while leveraging existing investments in security infrastructure and personnel, an often-underappreciated aspect given the skills shortage discussed earlier.

> **With intelligent network visibility tools, SOC teams can conduct highly contextual threat detection and investigation using packet-derived smart metadata that has linkages to full packet decodes if required.**

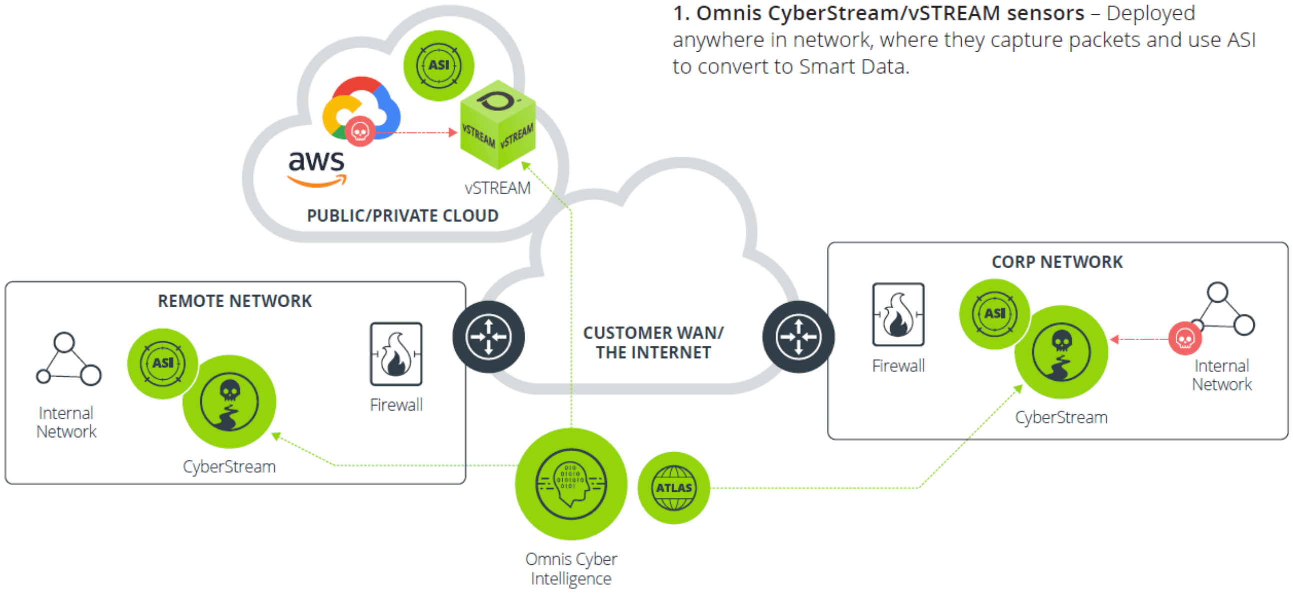
Introducing NETSCOUT Omnis Security

NETSCOUT has long been a leading provider of highly scalable, packet-based network and application performance analysis and network visibility solutions. Using its patented Adaptive Service Intelligence (ASI) technology, NETSCOUT solutions convert network packets into a rich source of layers 3-7 fully indexed metadata called Smart Data.

NETSCOUT Omnis Security

With NETSCOUT’s Omnis Security platform (see Figure 3), the vendor has expanded these same capabilities to address security use cases. NETSCOUT's Smart Data can be used by cybersecurity teams for comprehensive network visibility and more efficient cyber-threat detection, investigation, and response. In addition to basic attributes such as source and destination IP address, port and protocol, NETSCOUT Smart Data includes response times, error codes, protocol-specific information such as DNS requests and responses, browser and device type, and other information to help analysts better understand what's happening on the network.

Figure 3. NETSCOUT Omnis Security



1. Omnis CyberStream/vSTREAM sensors – Deployed anywhere in network, where they capture packets and use ASI to convert to Smart Data.

2. Omnis Cyber Intelligence – The central console that analyzes CyberStream/vSTREAM Smart Data; uses behavioral analysis and ATLAS/3rd party intelligence, for threat detection and highly contextual investigation.

Source: NETSCOUT

NETSCOUT allows customers a flexible approach to collect this information via a variety of network instrumentation. For existing NETSCOUT customers, packet acquisition occurs via their existing InfiniStreamNG (ISNG) and vSTREAM products. Alternatively, existing or new NETSCOUT customers can deploy dedicated CyberStream instrumentation for the same level of packet-derived network visibility. Both ISNG and CyberStream are available as purpose-built appliances or software that can run on industry-standard COTS servers. vSTREAM provides coverage for virtual and cloud environments, including AWS, Google Cloud, and Azure.

Specifications vary by instrumentation, but NETSCOUT can support customer environments up to 100Gbps, with up to 384TB of local storage. This provides continuous, highly scalable line-rate packet capture and longer retention, giving analysts a wider window in which to detect early signs of an attack or perform back-in-time investigations and to detect highly advanced and persistent threats. The wide range of deployment options ensures customers can instrument their entire environment, across on-premises data centers and cloud instances.

NETSCOUT Omnis Cyber Intelligence

NETSCOUT Omnis Cyber Intelligence (OCI) is the central console of the Omnis Security platform, which integrates with and fills the visibility gaps left by other cybersecurity tools. OCI leverages the Smart Data derived from ISNG, CyberStream, or vSTREAM instrumentation to provide comprehensive network visibility and more efficient cyber-threat detection and contextual investigation before, during, and after an attack occurs. OCI is infused natively with threat intelligence from NETSCOUT's ATLAS or with third-party intelligence feeds via STIX/TAXII. These feeds add context, analytics, and threat intelligence to the Smart Data collected through ISNG, CyberStream, and vSTREAM instrumentation, providing actionable insights for efficient cyber-threat detection and investigation.

OCI has four main uses cases: advanced early warning for the quick detection of attacks, continuous attack surface monitoring that enables security teams to detect vulnerabilities in their environment, contact tracing, and back-in-time investigation that enables security teams to detect threats by investigating near-term and long-term network activity. By providing visibility of both vulnerabilities and threats, OCI helps organizations reduce the risk of cyber-attacks.

The Bigger Truth

In some cybersecurity circles, the demise of the perimeter and de-emphasis of the network has been anticipated for years. The shift to remote work and further acceleration of cloud adoption over the last two years only exacerbated these predictions. Yet, while true that the perimeter has eroded and the network has fundamentally changed, many organizations have come to realize that network-based security tools remain vitally important to the protection of their environment.

The limitations of other tools with regard to coverage, scalability, and security requires a complementary approach that provides consistent visibility across the entire environment, makes security teams more efficient, and cannot be bypassed. Intelligent, highly scalable, packet-based network instrumentation addresses these needs. Through NETSCOUT's Omnis Security platform and Omnis Cyber Intelligence, security teams gain a unified, single-source-of-truth view of activity across the entire network, enabling them to quickly identify incidents, accurately diagnose threats, and efficiently perform investigations. As a result, organizations exploring advanced, packet-based network detection and response options should consider NETSCOUT Omnis Security.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188