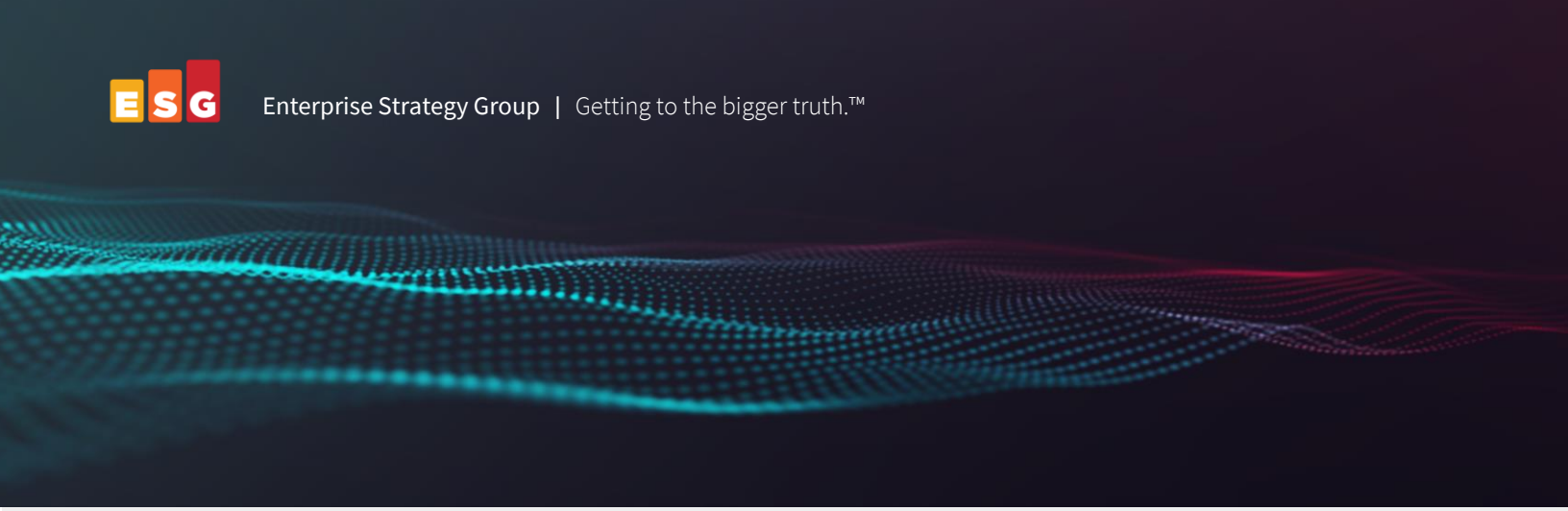


ESG WHITE PAPER

Network Security Without Borders

A Common Technology Stack for Network Security and Operations

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

August 2021

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

Contents

Executive Summary

In 2011, industry visionary Marc Andreessen wrote a now famous article titled, *Why Software is Eating the World.* The article correctly pointed out that software is at the heart of every modern industry—from retail to healthcare, to transportation, to financial services, and so on.

Ten years later, Andreessen's prediction is certainly true. It could be argued that this trend accelerated over the past few years, driven by digital transformation, cloud computing, and an increasing population of remote workers.

While the software revolution has led to impressive increases in business opportunity, employee productivity, and operational efficiency, it has also opened up new susceptibilities to cyber-attacks. This is certainly evident in recent waves of software vulnerabilities, supply chain compromises, and ransomware attacks.

There seems to be a mixed blessing here—business benefits on one hand and security risks on the other. What are the ramifications and how can CISOs improve their network security? This white paper concludes:

- Network security is growing much more difficult. A majority of organizations believe that network security is more difficult today than it was 2 short years ago.[1] And of those, many say that network security is getting *much* more difficult. Organizations point to factors like the increasingly dangerous threat landscape, an expanding attack surface, and a plethora of network security tools. SOC analysts also lament a lack of network visibility (end-to-end encryption) and growing sophistication and professionalism of the bad actors. Given this, it seems like existing network security models are a mismatch for protecting a modern hybrid IT infrastructure.

- There are organizational gaps between security and network operations teams. Managing network security difficulty demands tight collaboration and synchronization between security and networking teams, but ESG research reveals that 44% of organizations don't believe this relationship works well at all times.[2] It also exposes cross-organizational challenges around getting clear and concise network visibility, coordinating across different chains of command, and communicating between the groups. CIOs and CISOs must work together to address these challenges.

- Organizations need modern, scalable, and tightly integrated networking/network security technologies. Often times, networking and security teams maintain different technologies for monitoring and management, but this only exacerbates organizational problems. ESG suggests a common "network security without borders" technology stack that can be used to monitor and manage the network AND security. Security teams can use a common data repository, analytics tools, and security controls for threat prevention, detection, and response while networking teams leverage the same data to help with network throughput, availability, and end-to-end application performance, which at times can be the manifestation of a cyber-attack.

The State of Network Security

Today's hybrid IT infrastructure is highlighted by cloud-native applications, remote workers, and no discernible network perimeter, making network security a real challenge. In fact, ESG research indicates that 85% of organizations believe that network security is more difficult today than it was 2 years ago. Those who believe that network security is more difficult point to factors like (see Figure 1):

[1] Source: ESG Research Report, *The State of Network Security: A Market Poised for Transition*, March 2020. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.
[2] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

- An Increasingly sophisticated threat landscape. Organizations are under attack by an assortment of cyber-criminals, hacktivists, and nation states, who use social engineering techniques like spearphishing to compromise systems, move laterally across their networks, create privileged accounts, and steal valuable data. Many organizations find it difficult to monitor cyber-threats, correlate cyber-threat intelligence (CTI) with internal security telemetry, or keep up with the tactics, techniques, and procedures (TTPs) used by cyber-adversaries. Moreover, defenders are not keeping pace with training and education in alignment with what attackers are capable of doing. Hackers are using more complex and comprehensive tools, whereas internal users are seemingly less aware of what they do to reduce protection and become more complacent.

- A growing attack surface. Survey respondents pointed to an increase in the number of mobile devices, sanctioned/unsanctioned cloud applications, IoT devices, etc. These factors create a dynamic and continually growing attack surface. To maintain security in this environment, security teams must know what's connected to the network, scan for vulnerable assets, monitor network traffic, and fine tune security controls, difficult tasks when the attack surface is in a constant state of change.

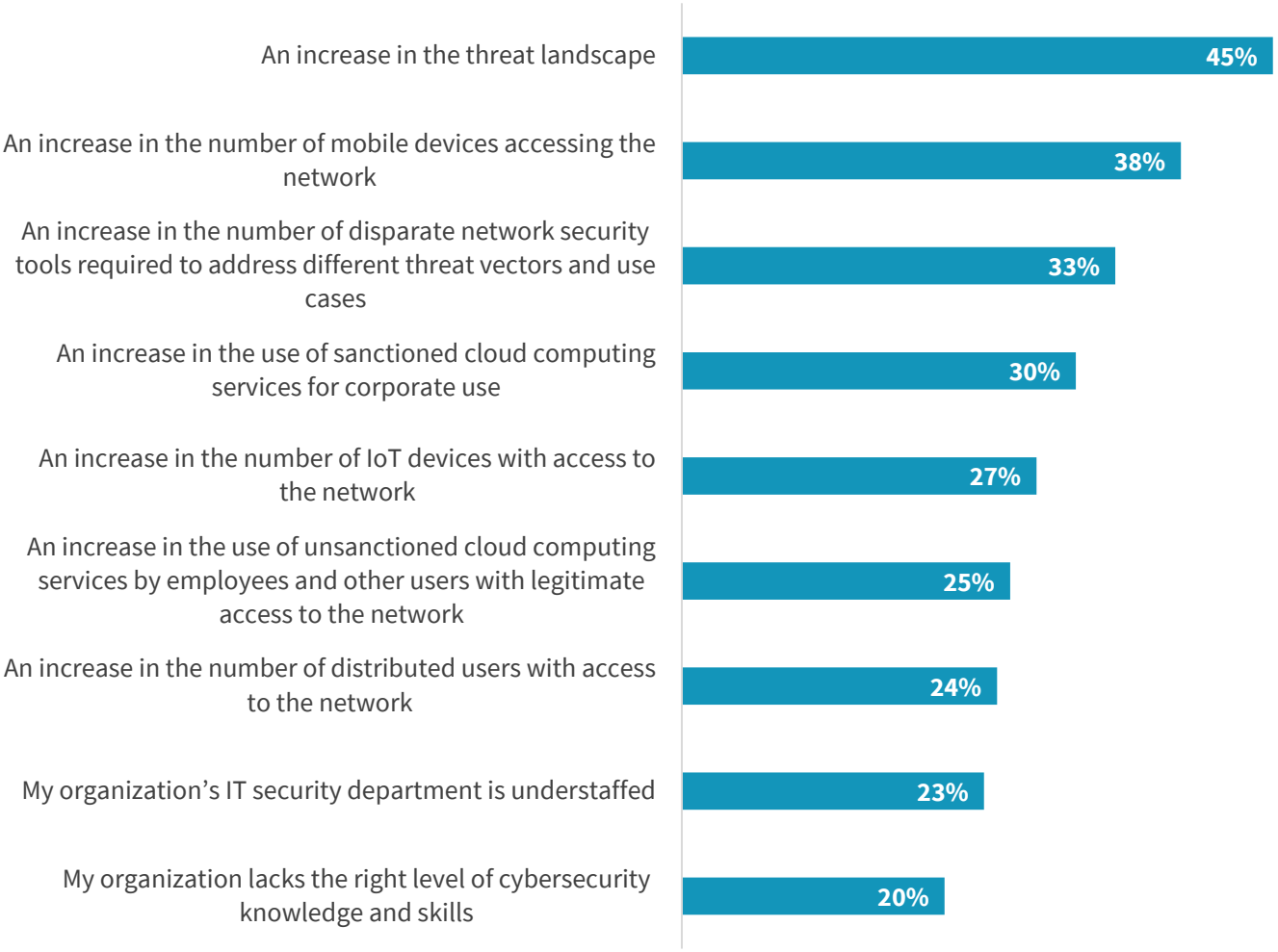
- Network security technology complexity. One-third of security professionals believe that network security has become more difficult because of an increase in the number of disparate network security tools required to address different threat vectors and use cases. With a growing attack surface, deploying, configuring, and operating an assortment of network security point tools will only become more cumbersome.

- The global cybersecurity skills shortage. Nearly one-quarter (23%) say that their organization's IT security department is understaffed, and likely overwhelmed, by the scale and complexity of cybersecurity. This is a common problem as other ESG research indicates that more than half of organizations claim they are impacted by the global cybersecurity skills shortage.[3]

[3] Source: ESG/ISSA Report, *The Life and Times of Cybersecurity Professionals 2020*, July 2020.

Figure 1. Reasons That Network Security Has Become More Difficult

You indicated that network security has become more difficult over the last two years. In your opinion, which of the following factors have been most responsible for making network security management and operations more difficult? (Percent of respondents, N=226, three responses accepted)



Source: Enterprise Strategy Group

Increasing network security difficulties have consequences, especially in areas like threat prevention, detection, and response. This is one reason why cyber-adversaries can maintain lengthy dwell times, move laterally across networks undetected, and conduct damaging and costly data breaches and ransomware attacks.

Organizational Issues Exacerbate Problems

As if network security wasn't difficult enough, problems are often aggravated due to poor cooperation, collaboration, manual processes, and communications between security and IT operations teams. Security and network operations teams must collaborate in areas like threat detection and response, but 44% of organizations say that this relationship does not work well all the time because (see Figure 2):[4]

- IT and security teams utilize separate tools and data as their sources of truth. Security teams view network security through network traffic analysis (NTA) and network detection and response (NDR) tools while networking teams use

[4] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

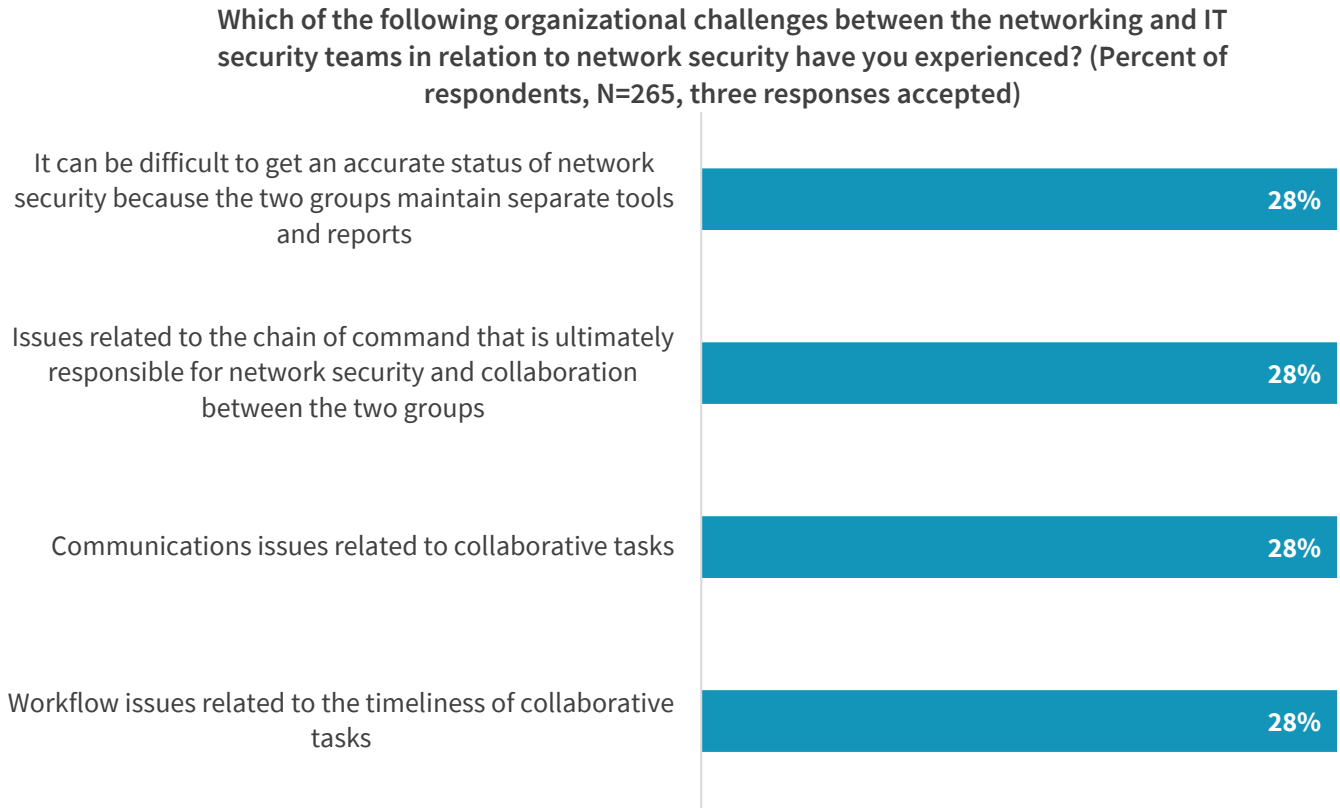
various tools to manage devices, traffic flows, network performance, etc. Unfortunately, this means that IT and security teams have their own views of network reality, leading to situations where each group is missing data and details necessary for keeping the network running at peak performance to support business operations. As teams scramble, network security threats and vulnerabilities languish, increasing cyber-risks.

- Different teams have different chains of command. Security and network operations organizations may be at odds with one another when it comes to goals and objectives. For example, the security team may find network vulnerabilities that need remediation but fail to convince network operations to prioritize fixes. These gaps create friction, as the teams should be collaborating on network hygiene, not bickering over who owns what.

- Communications gaps persist. Networking and security groups can speak different languages and thus talk past one another. This has technology roots with the use of different tools and the fact that both groups are overwhelmed with protecting the network while maintaining uptime and performance. Without the right controls in place, both groups will have different missions. The network teams always want the 'five nines' (99.999%) of availability and mean time between failure (MTBF), whereas the security team is measured by visibility and mean time to detect (MTTD), mean time to respond (MTTR), and mean time to acknowledge (MTTA). Differing focuses will pose a problem without management

- Workflow issues related to the timeliness of collaborative tasks. Group dynamics here are related to several factors. Both teams tend to rely on manual processes, creating problems with handoffs and process management. As previously stated, security and networking teams can also maintain separate tools for things like ticketing, case management, and interdepartmental communications. Coordinating data sets, processes, and tools creates overhead, leading to delays and human error.

Figure 2. Top Four Organizational Challenges Between Networking and IT Security Teams



Source: Enterprise Strategy Group

Aside from addressing legacy security issues, networking and security organizations have another reason for increased collaboration. With more network traffic traversing public cloud services and SaaS provider applications, large organizations are making significant changes to their enterprise networks, including creating private interconnects, using third-party network providers with peering relationships to leading IaaS/SaaS services, or building their own interconnect model at collocation (colo) facilities. These interconnects offer multiple benefits like increased throughput, predictable application/network performance, and simplified integration, but also add complexity and broaden the attack surface.

Network Security Without Borders

CISOs can't stop the ongoing momentum toward digital transformation, cloud computing, and remote worker requirements. Clearly, CISOs and CIOs must develop network security strategies featuring common goals and collaborative processes between security and network operations teams moving forward.

As security and networking teams come together, organizations should also think in terms of network security without borders by adopting a network security technology stack that offers cohesion and commonalities.(see Figure 3) and also:

- Prevents known and volumetric attacks as early as possible. Large organizations want "clean pipes" that can filter out known cyber-attack traffic and maintain peak network performance for business requirements. CISOs can address these needs by deploying stateless protection devices in front of stateful firewalls to help them block command-and-control (C2) traffic, state exhaustion DDoS attacks, known bad DNS domains, etc. These devices must be supported with strong, timely, and accurate threat intelligence that continually updates blocking lists in real time.

- Blocks suspicious and anomalous traffic in east/west traffic. IDS/IPS systems at network perimeters are still a requirement but standalone devices have been usurped by next-generation firewalls. This covers network ingress/egress but leaves internal networks susceptible to known attacks. To fill this hole, network security without borders should examine all east/west traffic using IDS/IPS technologies like open source Suricata. This can help security teams identify and filter out known "noise" that finds its way into the network quickly and efficiently.

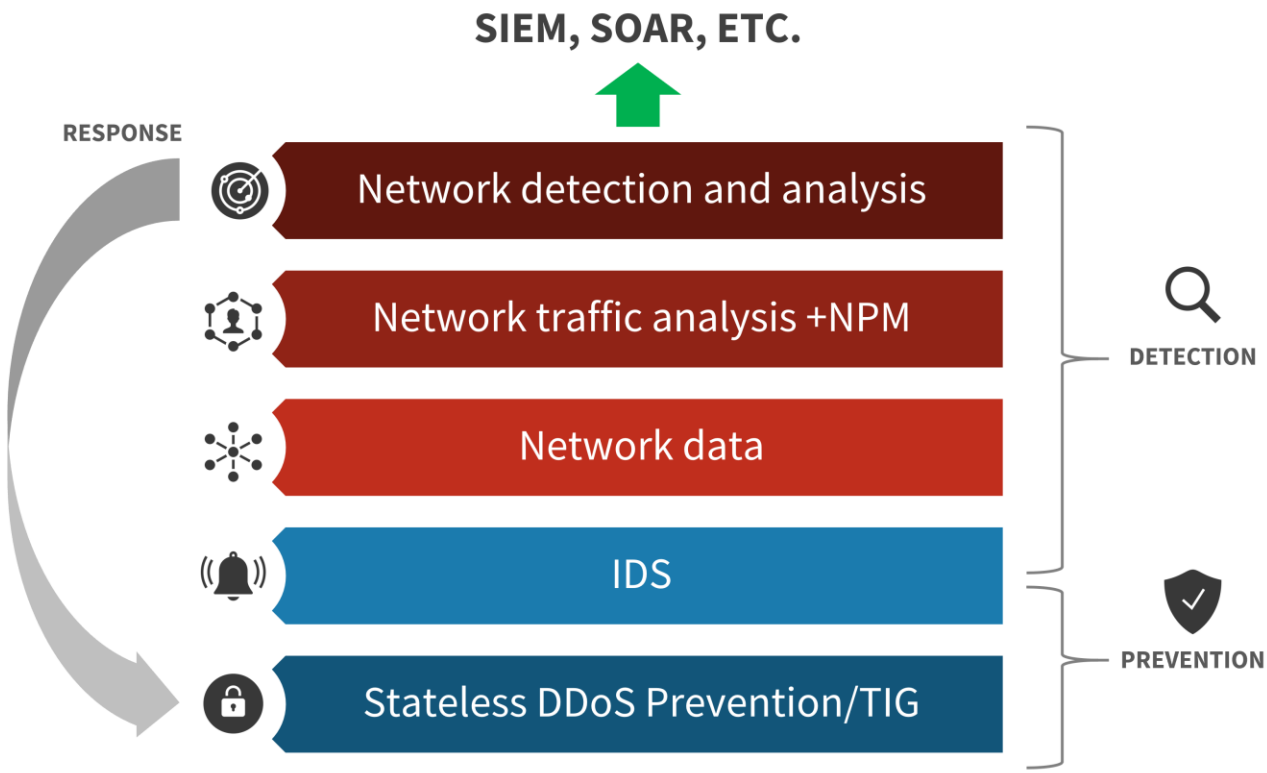
- Provides a common source of network truth. Networking and security teams need network and cloud visibility to maintain strong performance and detect/respond to security incidents. Rather than operate different tools that collect the same network data, organizations should move to common sources of line-rate packet acquisition classification, and local storage of network metadata and full packet capture (PCAP). The best solutions will go beyond raw data capture and storage by processing, indexing, and enriching network data, increasing its usefulness for incident detection, security investigations, and threat hunting. Network security data systems should also provide customizable dashboards, tailored to use case needs of networking and security teams.

- Offers network traffic analysis (NTA) capabilities. To keep the network running smoothly and safely, security and networking teams need to understand the behavior patterns of network traffic as well as the posture of every device connected to the network. This can help them identify and remediate rogue devices, misconfigurations, and vulnerable systems, while maintaining application performance for business operations. NTA visibility demands the right interface, graphics, and reporting capabilities built on top of the common network data repository. Armed with end-to-end network visibility, organizations can also monitor "normal" behavior in order to identify anomalies that could impact network security or performance.

- Delivers functionality for network detection and response (NDR). Aside from traffic analysis, organizations need a way to analyze network data and threat intelligence to detect and investigate anomalous, suspicious, and malicious network activities. Leading NDR systems can detect threats while providing access to a comprehensive source of metadata and network packets and guiding them through triage and investigations. NDR should also help SOC teams prioritize alerts, automate incident response processes, and pinpoint remediation actions like device cleanup/quarantine, blocking of malicious traffic, or network segmentation.

While a security without borders technology stack can improve threat prevention, detection, and response on its own, it should also help SOC teams get more out of existing technologies like security information and event management (SIEM) systems and security orchestration, automation, and response (SOAR) tools. Leading network security vendors will fulfill this requirement through technology integration, development partnerships, and knowledgeable system engineers who can help customers put the pieces together for maximum benefit.

Figure 3. Network Security Without Borders Technology Stack



Source: Enterprise Strategy Group

Network Security Without Borders and NETSCOUT

While many organizations have done their own custom technology integration to build a comprehensive network security stack in the past, some technology vendors now offer tightly integrated commercial alternatives. One such example is NETSCOUT and its OMNIS Security solution.

OMNIS Security focuses on the quality and relevance of network traffic data to provide a complete, in-depth, and highly available/agile (quickly retrievable and searchable) data set surrounding any potential attacks against an organization.

OMNIS Security enriches the data collected from the customer's network with threat intelligence from Arbor Intelligence Feed, with third-party feeds and classifiers as well as feeds from other security tools, including OMNIS AED, firewalls, and IDS/IPS devices, to help accelerate the investigation of potential attacks in OMNIS Cyber Investigator.

OMNIS offers all the layers for network security without borders by providing:

- OMNIS Cyber Investigator. Cyber Investigator is a security management application used for analyzing smart data collected by ISNG instrumentation, network baselines, and threat intelligence to detect all types of cyber-threats and enable workflows for further visualization and investigation. Cyber Investigator alerts can be sent to third-party SIEMs, and its data can be exported to third-party data lakes for further analysis.

- Infinistream NG/vStream as a network data source. Underpinning NETSCOUT OMNIS Security is the InfiniStreamNG (ISNG) platform. ISNG is a scalable packet acquisition, classification, and storage solution that can provide comprehensive and consistent visibility into any physical, virtual, or cloud environment (i.e., Amazon Web Services,

Google Cloud, Microsoft Azure, Oracle Cloud Infrastructure, and VMware NSX-V and NSX-T). ISNG uses Adaptive Service Intelligence (ASI) technology to convert raw network packets into indexed metadata (referred to as "smart data"). The ISNG platform also locally stores condensed, raw packets. ISNG and ASI created smart data to provide comprehensive north/south and east/west visibility across an organization's hybrid IT infrastructure for NetOps and SecOps use cases.

- Arbor Edge Defense. Deployed on the network perimeter in front of firewalls, Arbor Edge Defense detects inbound and outbound (e.g., north/south) threats such as DDoS attacks, scanning, brute force password attempts, malware, and other IoCs using stateless packet processing technology and threat intelligence from NETSCOUT ATLAS or third parties.

- IDS support. To protect internal networks and east/west traffic, OMNIS IDS provides intrusion detection using the Suricata open source signature and rules engine. OMNIS IDS can detect threats and then send alerts to the IDS Manager application running in its OMNIS cyber investigator console as well as to a SIEM/SOAR.

Along with its current offering, NETSCOUT has an aggressive roadmap, with plans for additional advanced analytics for threat detection, third-party technology integrations, and support for the MITRE ATT&CK and D3FEND framework.

NETSCOUT may not be the first vendor SOC teams think of for network security, but this situation may change given its OMNIS security offering and network security without borders technology stack. CISOs looking for integrated network security solutions for threat prevention, detection, and response may want to contact NETSCOUT to see how OMNIS security aligns with their present and future network security requirements.

The Bigger Truth

CISOs face two simultaneous forces: 1) In light of business trends like digital transformation, cloud computing, and remote worker support, the attack surface continues to grow in size and complexity, and 2) Network security is becoming more difficult due to factors like the dangerous threat landscape and tools proliferations.

To address these forces, security teams need all the help they can get. This starts by addressing any friction between security and network operations teams. CISOs and their CIO counterparts must ensure that these two groups have consistent goals, unified processes, and interoperable technologies so they can work together in harmony.

While bringing the organization together, security and networking teams should also consider common networking and security technologies that can support the need for protecting the network while maintaining network uptime and performance for business operations. Finally, security and networking team process and technology collaboration can lead to reduced cost due to shared instrumentation, training, and operational efficiencies. A "network security without borders" technology stack seeks to fulfill this goal with the right data, visibility, analytics, and threat detection capabilities.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188