Enterprise Strategy Group | **Getting to the bigger truth.™**

Research Insights Paper

Network Security Trends

Understanding the State of Network Security Today

By Dan Conde, ESG Analyst

January 2017

This ESG Research Insights Paper was commissioned by Gigamon and is distributed under license from ESG.

Contents

Executive Summary

Research Methodology and Goals

In the second half of 2016, Gigamon commissioned the Enterprise Strategy Group (ESG) to conduct a survey of 300 IT and cybersecurity professionals. Respondents to the survey all had responsibility and involvement in the planning, implementation, and/or operations of their organization's security policies, processes, and technical safeguards. Participants also had purchase decision-making authority or influence for network security products and services.

Survey respondents were located in North America and Western Europe. Multiple organization sizes were represented in the respondent base: 25% of respondents worked at organizations with 100-499 employees, 34% at organizations with 500-999 employees, and 41% at organizations with 1,000-4,999 employees. The survey included representation from many industries including manufacturing (22%), retail/wholesale (11%), financial services (16%), business services (8%), health care (5%), and communications and media (4%).

This research project was undertaken to evaluate the challenges, changes, best practices, and solution requirements for network security operations and network security tools. Respondents were questioned about organizational characteristics including staffing, coordination, and time to evaluate new technology. Respondents were also asked about technology considerations such as the use of automated models compared with manual processes, types of network visibility tools in use, use of security monitoring functions, and current and planned reliance on third-party services for network security.

Research Highlights

Based on the data collected from the research survey, this paper concludes:

- Network security operations today are as difficult as or more difficult than they were 24 months ago.
- Visibility across all corporate networks can be improved, resulting in an enhanced security posture.
- Organizations find they have not achieved an idealized state where automated processes provide effective network security operations.
- Adding more network security tools may not be the path toward improving visibility and threat mitigation.
- A platform-based architecture to enable visibility may allow organizations to make better use of the security tools they already possess.

Research Findings

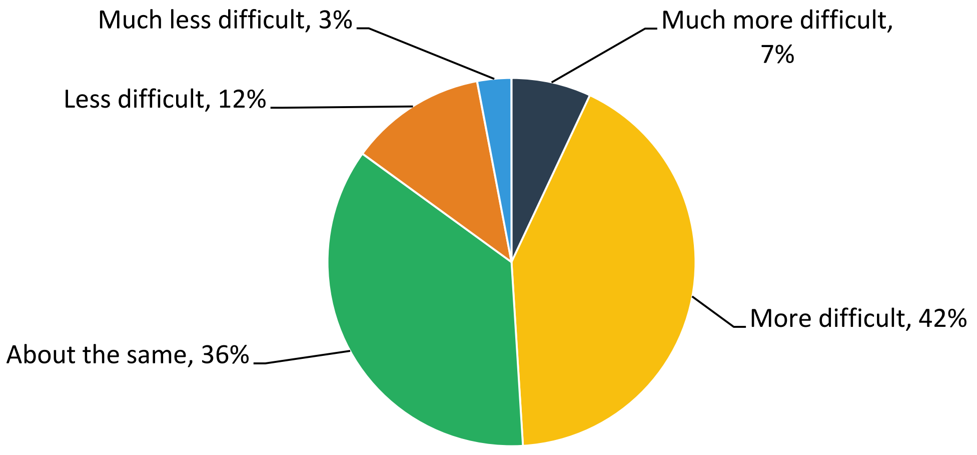
Current State of Network and Security Operations

ESG research consistently indicates that cybersecurity is a top priority[1] and challenge for IT organizations, exacerbated by an increasingly sophisticated threat landscape that is exacerbated by an ongoing cybersecurity skills shortage. Indeed, from a network security perspective, the increasing number of end-user devices, communication between physical and virtual devices, and sharing of data between cloud, data center, and campus networks creates challenges for organizations in terms of getting visibility into how the data is used and transmitted, and where there are potential threats.

When asked how to characterize network security operations (i.e., processes, workload, complexity, etc.) today compared with two years ago, 85% of organizations report they are as difficult as or more difficult than they were 24 months ago (see Figure 1).

Figure 1. Difficulty Associated with Network Security Operations over Time

How would you characterize network security operations (i.e., processes, workload, complexity, etc.) today compared with two years ago? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2016

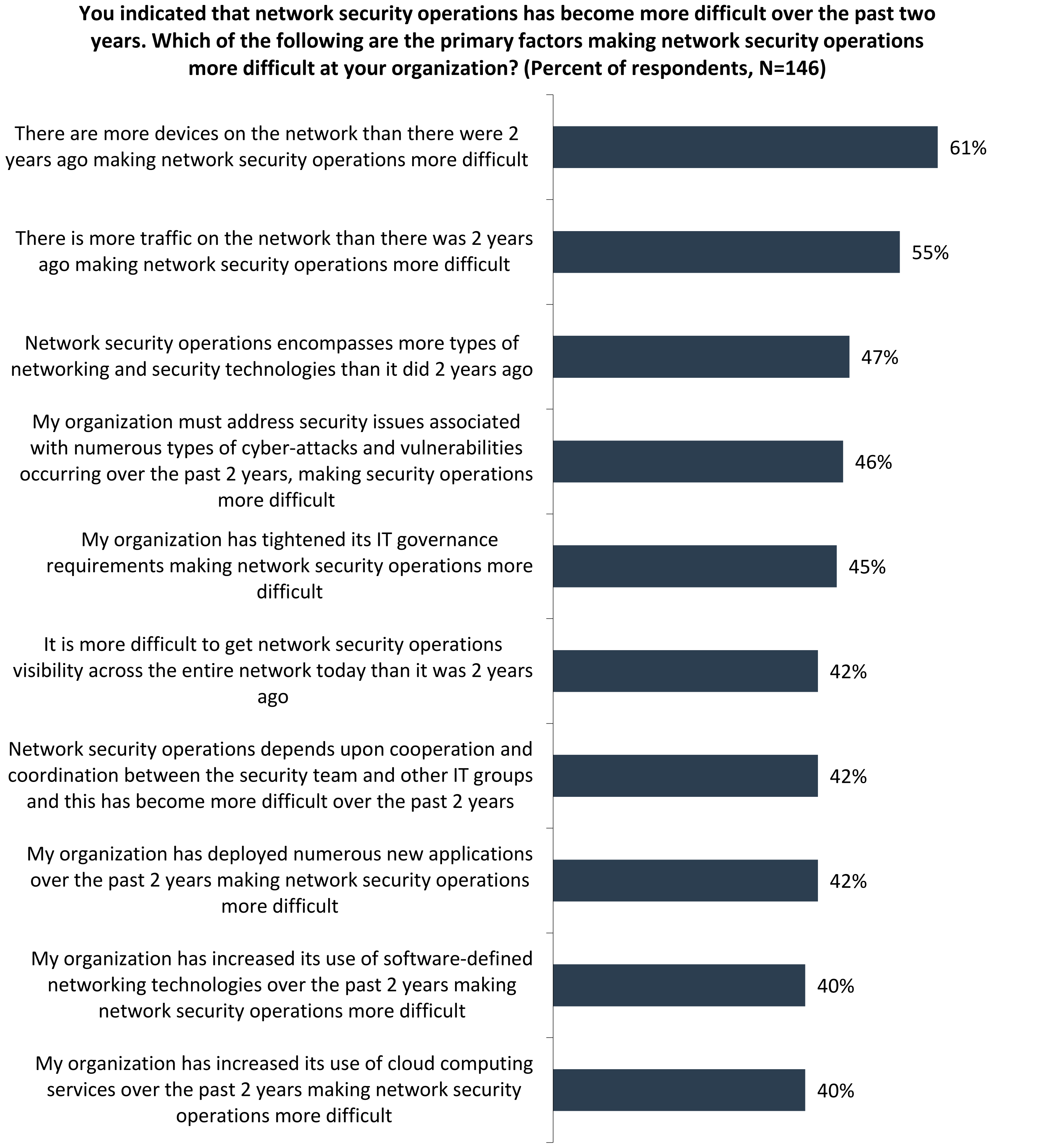
Among those respondents indicating that network security operations have become more onerous over the last two years, what is behind this trend? According to Figure 2, the most commonly cited factors include more devices on the network (61%), more traffic on the network (55%), network security operations encompassing more types of networking and security technologies (47%), and numerous types of cyber-attacks and vulnerabilities (46%).

When asked if their organization has good visibility across its entire network(s) to efficiently perform ongoing security and vulnerability analysis, 75% of respondents reported that they believe visibility across all of their corporate networks could be improved (see Figure 3). However, many organizations are already performing activities that provide for visibility. Indeed, when ESG asked if several key activities were being performed currently, a majority reported currently monitoring network traffic for performance, fault, and availability analysis purposes, analyzing network metadata for DNS monitoring, SSL certificate analysis, or user behavior analysis, and/or performing SSL decryption.

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

There is a paradox. Although these activities are commonly performed, enterprises *still* state that they lack the desired network visibility. When asked if their organization has good visibility across its entire corporate network, only 25% stated they have excellent network visibility, while 67% stated it can be improved, and 8% stated that they have limited visibility.

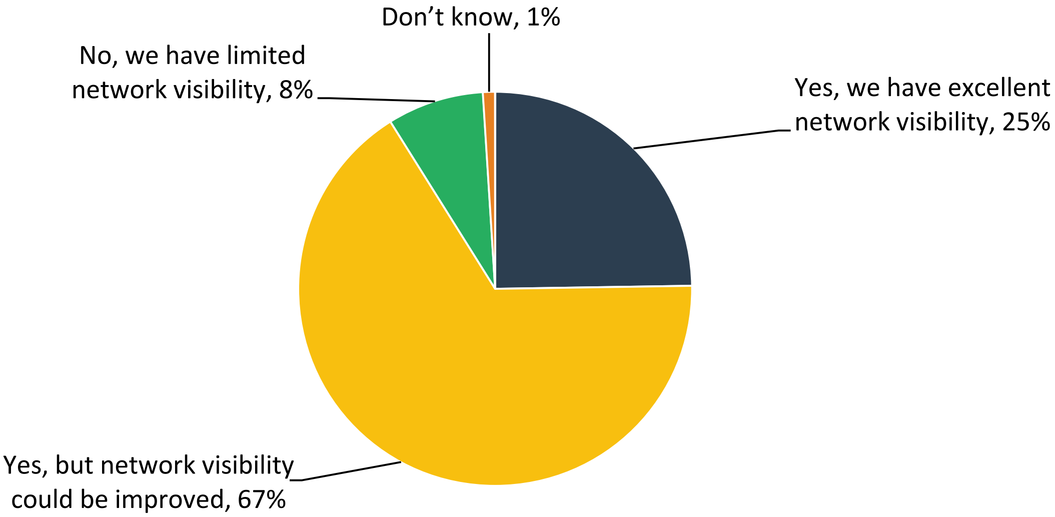
Figure 2. Top Ten Factors behind Increasing Difficulty Associated with Network Security Operations



Source: Enterprise Strategy Group, 2016

Figure 3. Level of Network Visibility

Do you believe your organization has good visibility across its entire corporate network(s) to efficiently perform ongoing security and vulnerability analysis? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2016

Challenges of Network and Security Operations

Eighty-five percent of organizations use inline security tools, and a majority (58%) of those apply software updates or make configuration changes to those tools at least monthly (see Figure 4). While it's important to keep these tools patched, it is also important to note that a shortfall of inline tools is that these changes and updates disrupt security operations and can actually create vulnerabilities.

Coordination between the network and security operations teams can be another pain point, with only 32% of the respondents indicating that coordination is easy when changes to inline tools are made. This issue is explored further in the next section.

Next Steps

Why are these processes and tools not providing the desired outcomes? Organizations should ask themselves several questions that may help close the visibility gap:

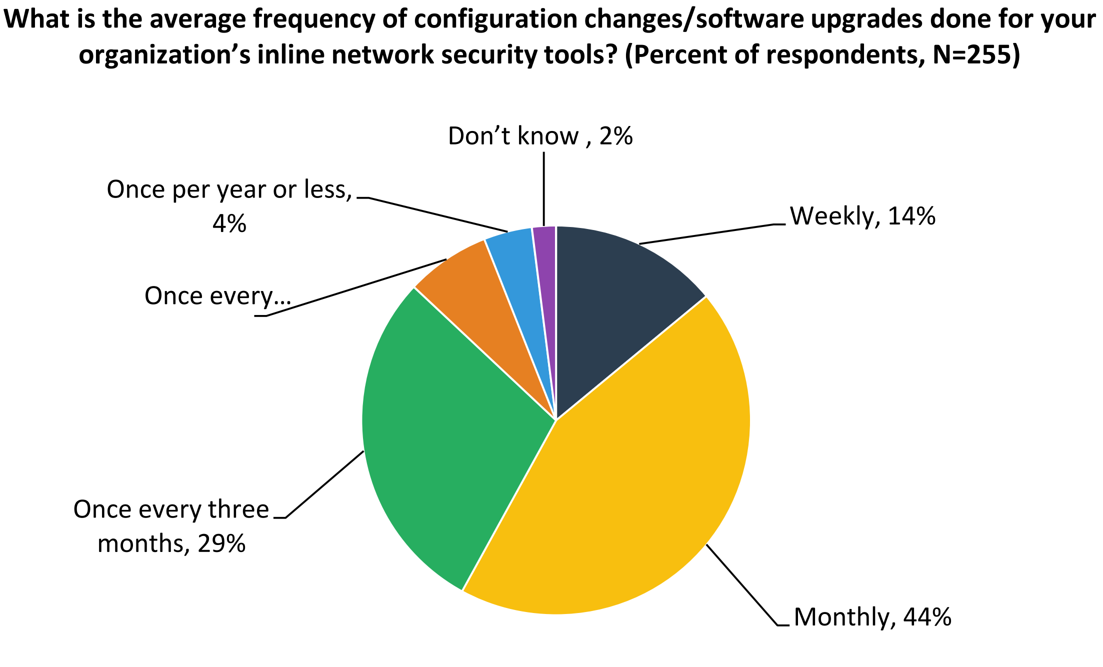
Can More Tools Help?

The survey data does not indicate that more tools will help. In fact, ESG's data shows that the typical number of tools organizations use per site is five to seven (stated by 64% of the respondents). Even larger organizations with more staff often are not choosing to use a greater number of tools. This indicates that these organizations feel that adding more tools to their environment is not an effective solution, even if they are not limited by the number of personnel to use those tools.

Can Organizational Changes Help?

Organizational improvements may allow organizations to make better use of existing tools. ESG's research data shows that three in ten organizations (30%) today do not have dedicated personnel for network and security operations. Within those organizations that do staff dedicated network and security groups, 93% reported that four or fewer staff were employed in that capacity. Moreover, security groups reported a great deal of focus on incident response. When asked how many individuals are dedicated to incident response, a plurality indicated that two individuals are dedicated to that function. Thus, it is very common for half or more of security operations staff to be dedicated to performing reactive incident response activities.

Figure 4. Average Frequency of Inline Network Security Tool Configuration Changes



Source: Enterprise Strategy Group, 2016

When ESG asked those organizations that are both staffing dedicated network and security teams and using inline security tools how difficult it is to coordinate efforts between relevant teams when making changes to inline network security tools, less than one-third reported it was easy.

The aggregate picture painted by this data is not positive. Many organizations do not currently staff dedicated security roles and those that do are still likely to be resource constrained—either from a headcount or skillset perspective. Additionally, collaborative challenges among the security team and other IT disciplines are fairly common.

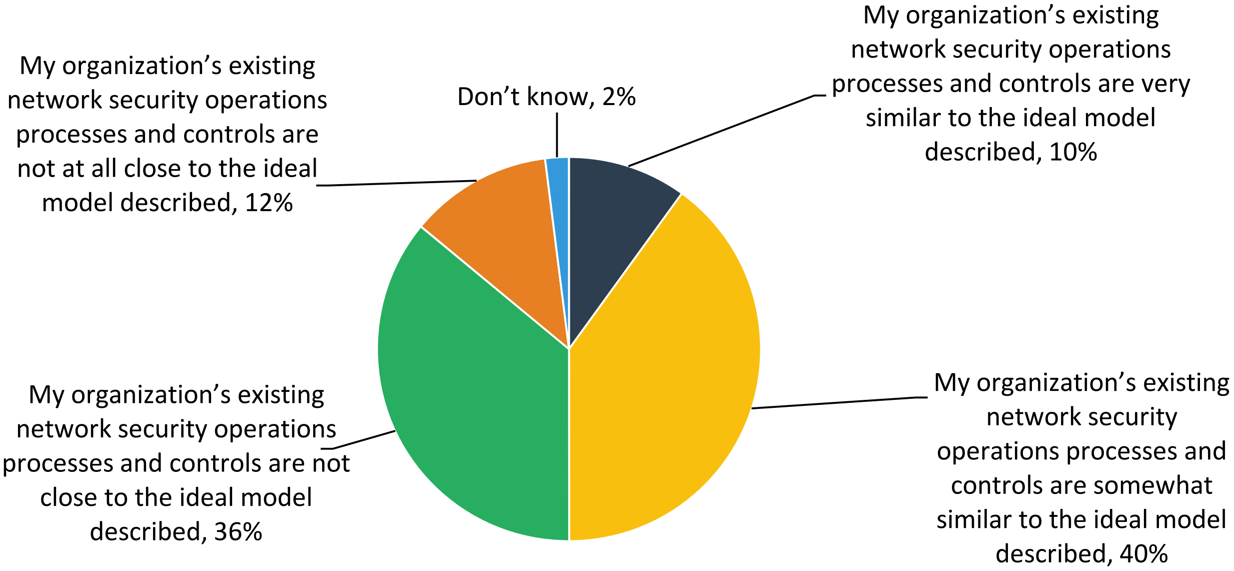
However, if security operations staff can become more effective and coordinate their tasks better with network operations staff, then security outcomes will be improved. Automation can assist in this area as well. If network and security processes can be automated, the need for manual coordination will be reduced. Automation may also reduce the amount of time spent on incident response and enable more time to be devoted to proactive and preventative activities.

Can a Different Architectural Approach Help?

Understanding where organizations stand today and comparing it with an ideal situation can shed more light on how IT organizations view themselves and where opportunities to improve exist. ESG asked organizations to imagine an ideal situation where the tools and processes needed to automate network security operations completely (such as central command and control for workflow, change control, testing, visibility, and auditing) were in place and compare that to their organization’s existing processes and controls. Only 10% of organizations felt that their organization’s existing network security operations processes and controls are very similar to this ideal model (see Figure 5). This large shortfall lends credence to the idea that the gap may be closed with a completely different architectural approach to network security that provides centralized command and control for operational tasks.

Figure 5. Comparison of an Ideal Automated Model to Existing Processes

Imagine an ideal situation where your organization had the tools and processes needed to automate network security operations completely (i.e., central command and control for workflow, change control, testing, visibility, auditing, etc.) across physical, virtual, and cloud infrastructure. How would you compare this type of automated model for network security operations to your organization's existing processes and controls? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2016

This type of centralized, platform-based architectural approach should allow disparate tools to be managed more effectively by enabling them to be viewed, administered, and monitored from a single console. Pairing tool consolidation with the automation of manual tasks should enable tools to function more effectively and processes to be more streamlined.

The notion of using automation to assist network security has been seen in another ESG survey, which indicated that the area with the strongest connection to network automation was network security.[2] This reinforces the finding that automation enables resources (both IT assets and people) to be used more effectively.

The Bigger Truth

As clearly evidenced by ESG's research data, most organizations can improve their network visibility and reduce their security vulnerabilities. However, they must make smart investments. Adding more point tools to an already fragmented security and monitoring environment may make security outcomes worse, not better. Rather, it is more likely that the typical organization can achieve better security outcomes by investing in staff (who are likely spread too thin today) or consolidating tools through a platform-based approach to visibility in which data, analytics, and reports from multiple tools can be aggregated and consumed in one control panel.

This architectural methodology to approaching these challenges is a particularly intriguing solution because it allows organizations to preserve investments in existing tools, making them work better, while also empowering the personnel

[2] Source: ESG Research Report, *Network Automation: Enabler of IT Process Goals*, July 2016.

who use them. Improving the utilization of existing IT and human resources within the organization is a prudent way to meet these challenges.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

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