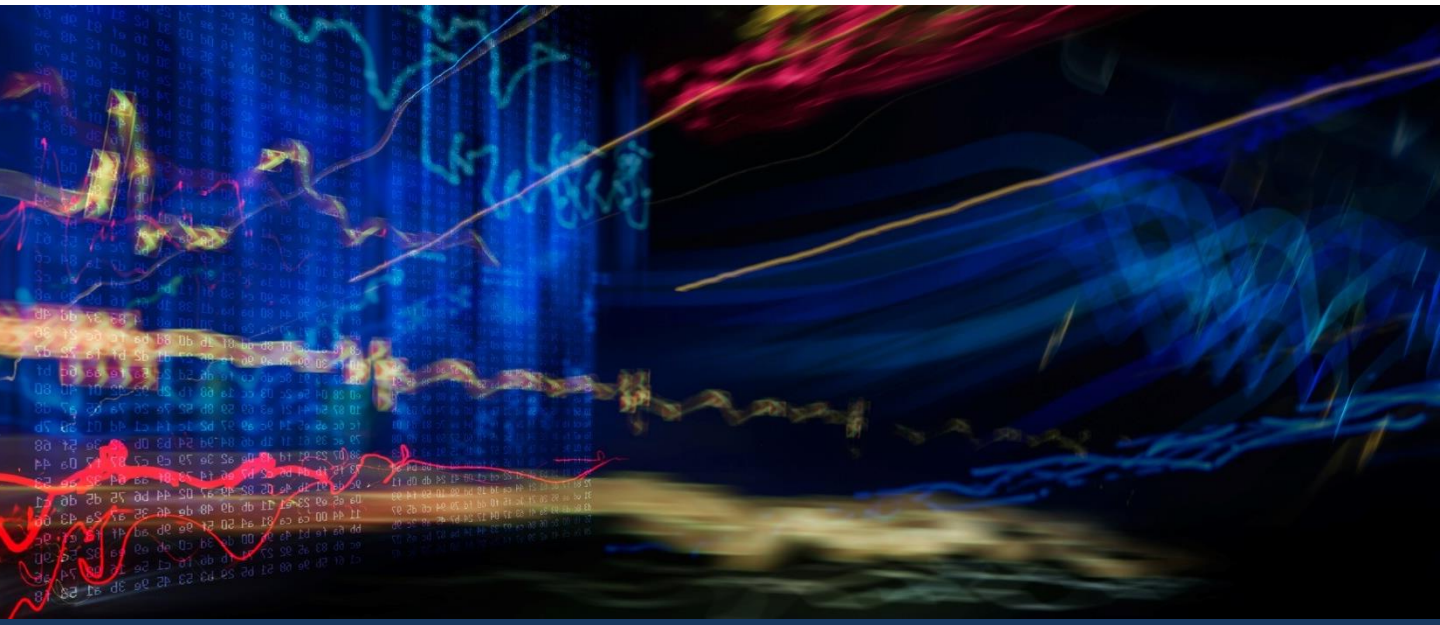


Network Security Monitoring Trends

By **Jon Oltsik**, ESG Senior Principal Analyst

August 2016

Contents

Executive Summary

In 2016, Cisco Systems commissioned the Enterprise Strategy Group (ESG) to complete a research survey of 200 IT and cybersecurity professionals with knowledge of, or responsibility for, network security and security analytics at their organizations. Seventy-four percent of respondents claimed direct involvement in purchasing cybersecurity products, while the remaining 26% said that they influence cybersecurity product procurement.

Survey respondents were located in North America and came from companies ranging in size: 25% of survey respondents worked at organizations with 3,000 to 4,999 employees, 31% of survey respondents worked at organizations with 5,000 to 9,999 employees, 18% worked at organizations with 10,000 to 19,999 employees, and 27% worked at organizations with 20,000 or more employees. Respondents represented numerous industry and government segments, with the largest participation coming from manufacturing (19%), financial services (banking, securities, insurance, etc.) (13%), information technology (12%), health care (11%), and retail/wholesale (11%). Note: Totals in figures throughout this report may not add up to 100% due to rounding.

This research project was intended to assess the current practices and challenges associated with network security monitoring related to people, processes, and technologies. Furthermore, respondents were asked about their future strategic plans intended to improve and enhance network security monitoring practices over time. Based upon the data collected, this paper concludes:

The value of network security telemetry is well understood. Survey respondents claim that they use network security monitoring for numerous use cases including "hunting" for malicious activities, detecting security breaches, and automating remediation tasks. Cybersecurity professionals also realize that network security monitoring success depends upon strong working relationships between security and network operations teams, and recognize that future network security monitoring efforts must extend to the cloud. All in all, cybersecurity professionals seem to appreciate the value of network security monitoring and have well-defined ideas on what's needed to make it work.

Large organizations collect, process, and analyze a lot of network security data. Network security monitoring depends upon the collection, processing, and analysis of a myriad of data sources including firewall logs, VPN logs, logs from networking devices, and proxy logs. Generally, network security monitoring data remains online for over 60 days and 10% of organizations keep this data online for a year or more. This adds up to a lot of data that must be structured and well organized if it is to equate to value.

Network security monitoring practices remain fraught with challenges. A majority (72%) of organizations believe that network security monitoring has grown more difficult over the past two years for a variety of reasons including an increase in malware volume, an increase in network traffic, and an increase in malware sophistication leading to cyber-attacks being able to circumvent traditional network security controls. As if this weren't bad enough, large organizations also report a number of network security monitoring challenges including network blind spots, communications issues between cybersecurity and network operations teams, and problems with timely data collection. Given this laundry list of issues, in some cases, network security monitoring isn't nearly as effective or efficient as it should be.

CISOs have aggressive network security monitoring plans for the next few years. A vast majority (91%) of organizations plan to increase their spending on network security monitoring over the next two years. Furthermore, CISOs have lots of network security monitoring plans including increasing cybersecurity training, integrating network security monitoring with other networking and security technologies, and investing in new network security monitoring tools.

Based upon the research collected and analyzed for this project, ESG believes that network security monitoring is in a state of transition. Large organizations must move toward network security monitoring architectures that are designed for integration and offer built-in intelligence.

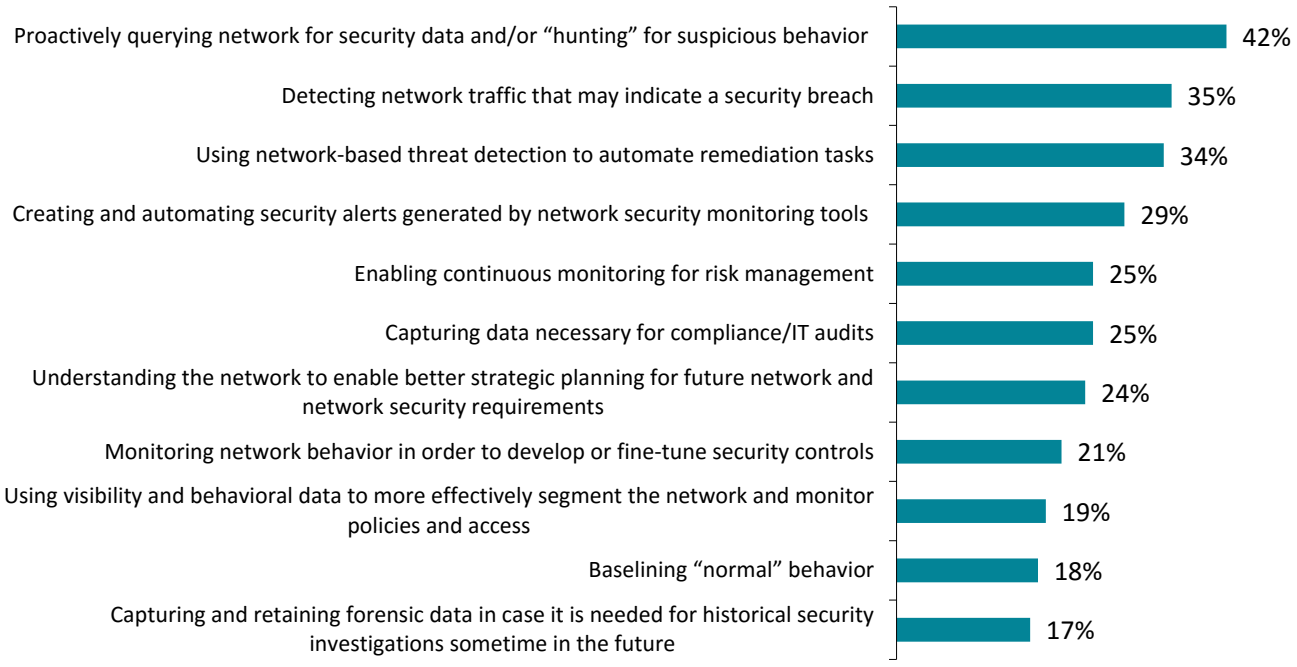
Network Security Monitoring Situational Analysis

According to ESG research, 80% of survey respondents say that network security monitoring is critical to their organization's overall cybersecurity strategy, while 17% say that network security monitoring is important (but not critical) to their organization's overall cybersecurity strategy. Why is network security monitoring such an imperative? Because it is an integral part of numerous use cases and goals. For example, 42% of respondents say that their most important objective for network security monitoring is proactively querying networks or "hunting" for suspicious behavior, 35% use network security monitoring for detecting security breaches, and 34% have a goal of using network-based threat detection to automate remediation tasks (see Figure 1). With this wide variety of security use cases, network security monitoring could be considered a foundational technology for cybersecurity.

FIGURE 1

Most Important Network Security Monitoring Objectives

With regard to monitoring network activity for security purposes, which of the following would you say are your organization's most important objectives? (Percent of respondents, N=200, three responses accepted)



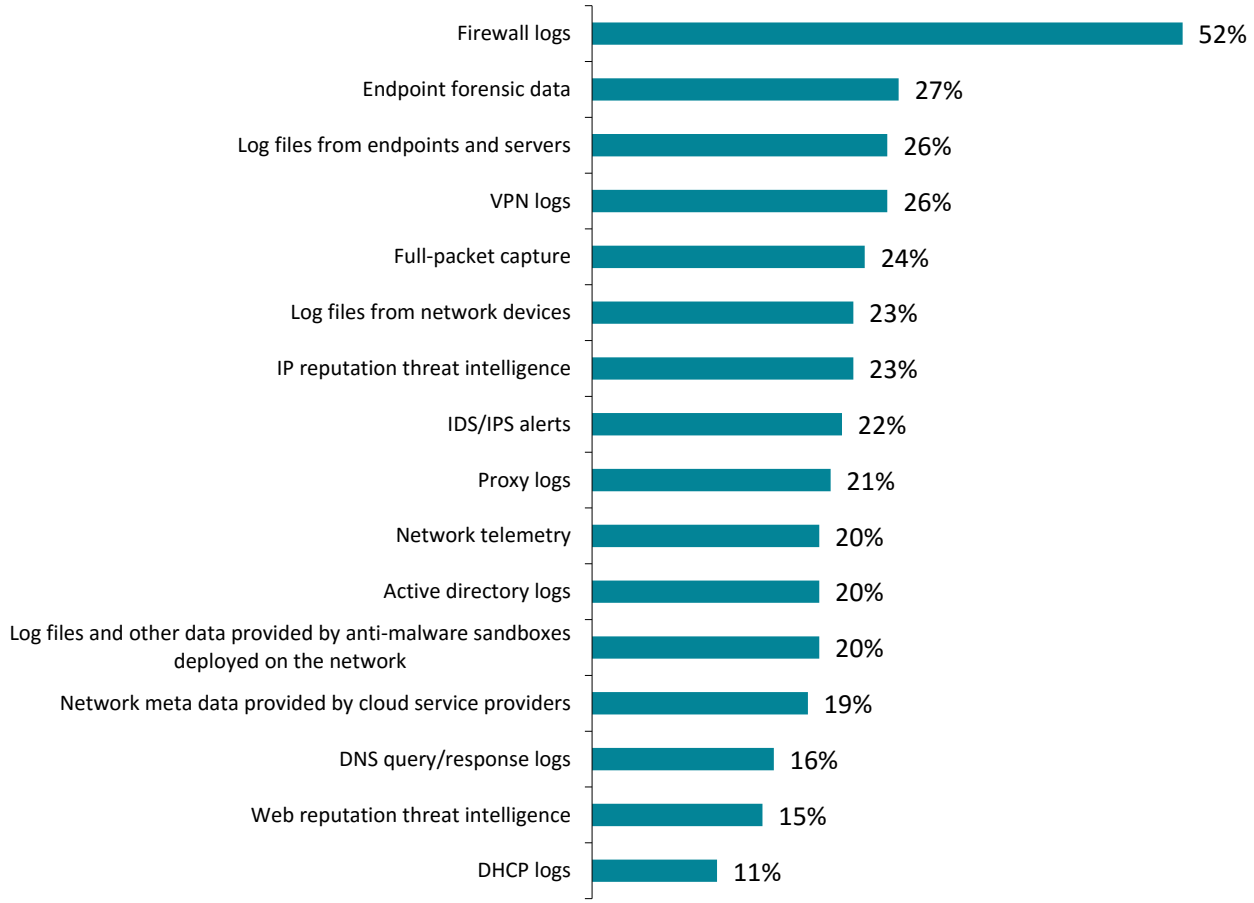
The ESG data also reveals that network security monitoring covers a lot of technologies that are valuable in helping to detect and respond to anomalous network behavior—more than half (52%) say that firewall logs are most valuable for this purpose, 27% say endpoint forensic data, and 26% say log data from endpoints and servers. It is also worth mentioning the role of network monitoring here—24% of respondents point to full-packet capture while 20% mention network telemetry data (see Figure 2). Seventy-one percent of organizations keep network security monitoring data online for 60 days or more, while 10% keep the data online for more than a year. Additionally, 25% of organizations believe they would benefit by retaining network security monitoring data online for a longer period of time.

Given this diversity, large organizations should look for network security monitoring technologies that can collect, process, and analyze data from a multitude of sources. Additionally, CISOs will want to work with network security monitoring vendors with mature ecosystems able to coordinate with industry partners and weave disparate tools into integrated network security solutions.

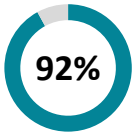
FIGURE 2

Most Important Network Monitoring Data Sources

Of all the network monitoring data sources your organization currently collects, which ones are most valuable for helping your organization detect and respond to anomalous network behavior and/or cyber-attacks in progress? (Percent of respondents, N=200, multiple responses accepted)



ESG found that the cybersecurity and IT professionals who acted as survey respondents had some strong opinions on network security monitoring technologies and the overall state of network security monitoring at their organizations (see Figure 3). For example:

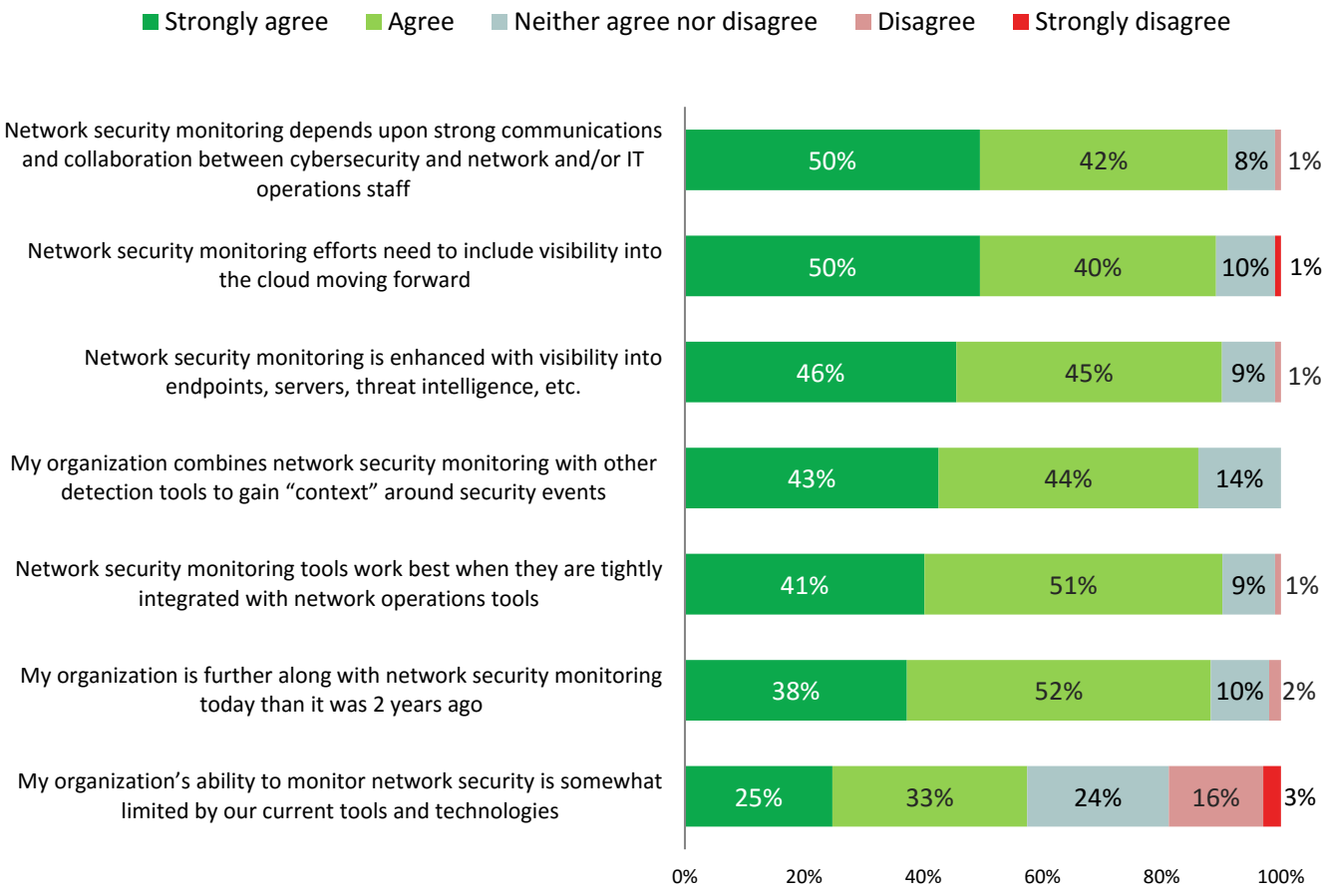


92% of respondents strongly agree or agree that network security monitoring depends upon strong communications and collaboration between cybersecurity and network and/or IT operations staff. This reflects the fact that successful incident response (IR) requires an effective working relationship between the group responsible for detecting security problems (i.e., security analysts, forensic investigators, SOC personnel, etc.) and those called upon to remediate problems with actual technologies (i.e., IT/network administrators, network operations, etc.). Given this, network security monitoring tools should be designed to accommodate the various requirements of both security and network operations teams.

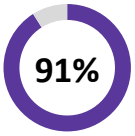
FIGURE 3

Opinions About Network Security Monitoring

Please check one response per row that best characterizes your opinion on each statement. (Percent of respondents, N=200)



90% of respondents strongly agree or agree that network security monitoring needs to include visibility into the cloud moving forward. This too makes sense as an increasing number of IT workloads and applications are moving to public and private clouds. Network security monitoring tools and processes must adapt to this reality with comprehensive visibility into cloud infrastructure.



91% of respondents strongly agree or agree that network security monitoring is enhanced with visibility into endpoints, servers, threat intelligence, etc. This point (and others in Figure 3) speak to the need for a "wide-angle" network security monitoring lens. In other words, network security monitoring tools should use multiple data sources to provide an end-to-end view of security incidents over time as they evolve and traverse networks and assets. This type of "wide-angle" visibility should provide the data needed for both real-time and historical investigations.

Network Security Monitoring: Critical but Challenging

Clearly, network security monitoring is a critical cybersecurity discipline, and survey respondents had strong opinions on the people, processes, and technology needed to make network security monitoring efforts successful. Unfortunately, getting these factors to work well together isn't always easy. In fact, 26% of survey respondents admit that network security monitoring has grown much more difficult over the past two years, while another 46% claim that network security monitoring has become somewhat more difficult over the past two years.

Why? ESG research points to (see Figure 4):

The threat landscape. More than one-third (34%) of respondents identify an increase in malware volume as contributing to difficulty with network security monitoring. Twenty-seven percent say an increase in malware sophistication that may lead to the circumvention of traditional network security controls is making monitoring more difficult. And 26% attributed increased monitoring difficulty to a rise in targeted attacks that may circumvent conventional controls. It seems certain that large organizations are facing more numerous and skillful cyber-attacks.

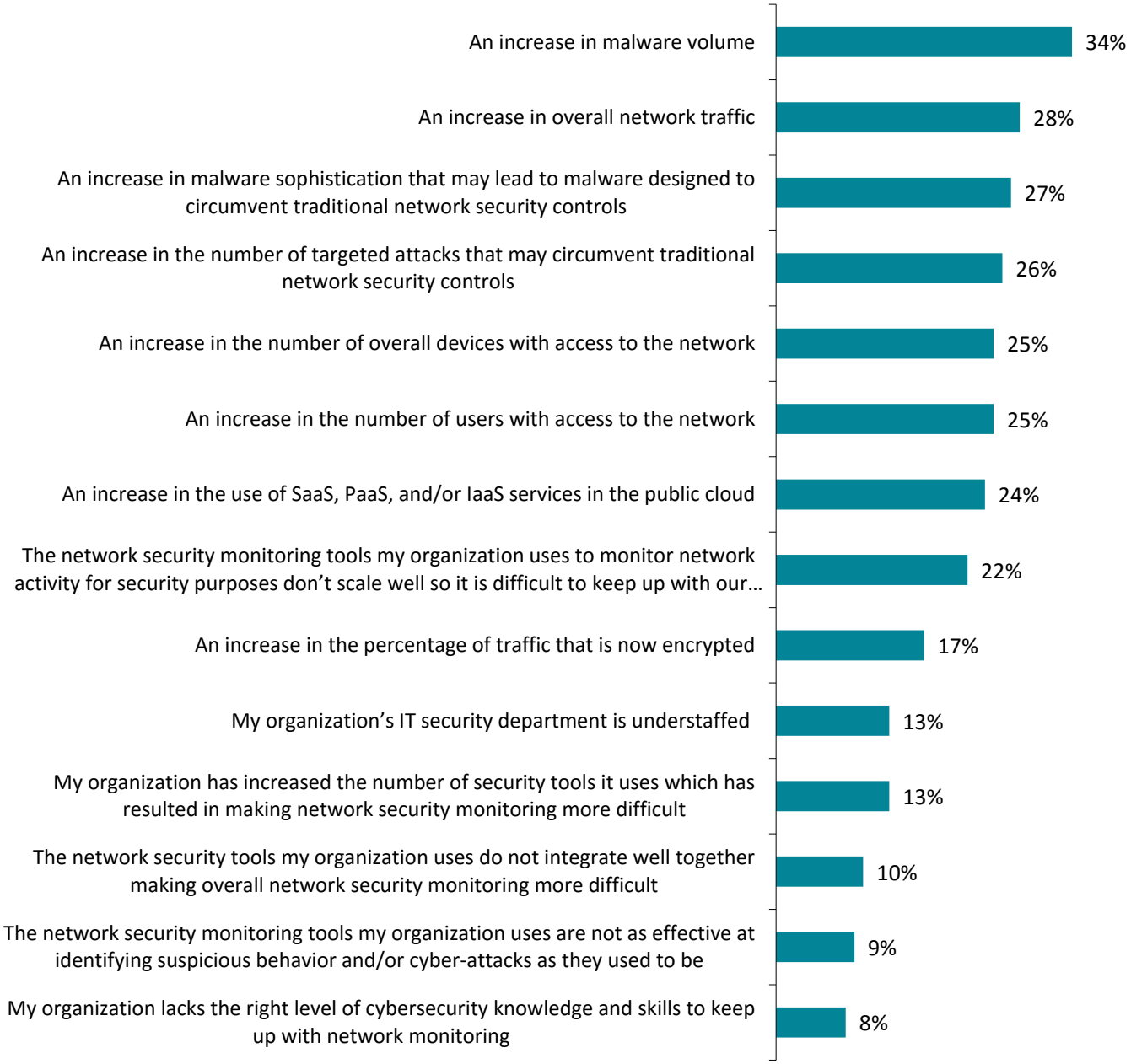
IT complexity. Note that 28% of respondents cite an increase in overall network traffic as leading to monitoring challenges, while 25% point to an increase in users and devices with access to the network. Furthermore, 24% say that network security monitoring is more difficult due to the increasing use of IaaS, PaaS, and SaaS in the public cloud.

Network security monitoring technology issues. Twenty-two percent of respondents claim that their network security monitoring tools don't scale well. These tools are no match for the threat landscape and IT complexity issues described above.

FIGURE 4

Why Network Security Monitoring Is Becoming More Difficult

You indicated that monitoring network activity for security purposes has become more difficult over the last two years. In your opinion, which of the following factors have made monitoring network activity for security purposes more difficult? (Percent of respondents, N=143, three responses accepted)



While the external threat landscape is making network security monitoring more difficult, large organizations are also coping with internal factors that complicate network security monitoring (see Figure 5). These challenges include:

Dealing with network "blind spots." Thirty-one percent of organizations say that the fact that they have one or several blind spots where they don't have adequate visibility into network security activities is one of their top challenges related to network security monitoring. Where are these blind spots? Forty-two percent of organizations report blind spots when monitoring non-corporate devices on the network, 39% report blind spots regarding user behavior monitoring, 39% have blind spots associated with network traffic flowing from corporate to partner networks, and 39% describe blind spots on internal Wi-Fi networks. These blind spots lead to negative ramifications including increased IT risk, a decrease in organizations' ability to "hunt" for malicious activities, and the inability to detect malicious behavior in certain portions of the network.

Organizational issues. Twenty-nine percent of organizations admit that they have some communications and process issues between the cybersecurity and network operations teams that can hinder their network security monitoring capabilities. This is especially concerning considering that 92% of survey respondents strongly agree or agree that network security monitoring depends upon strong communications and collaboration between cybersecurity and network and/or IT operations staff.

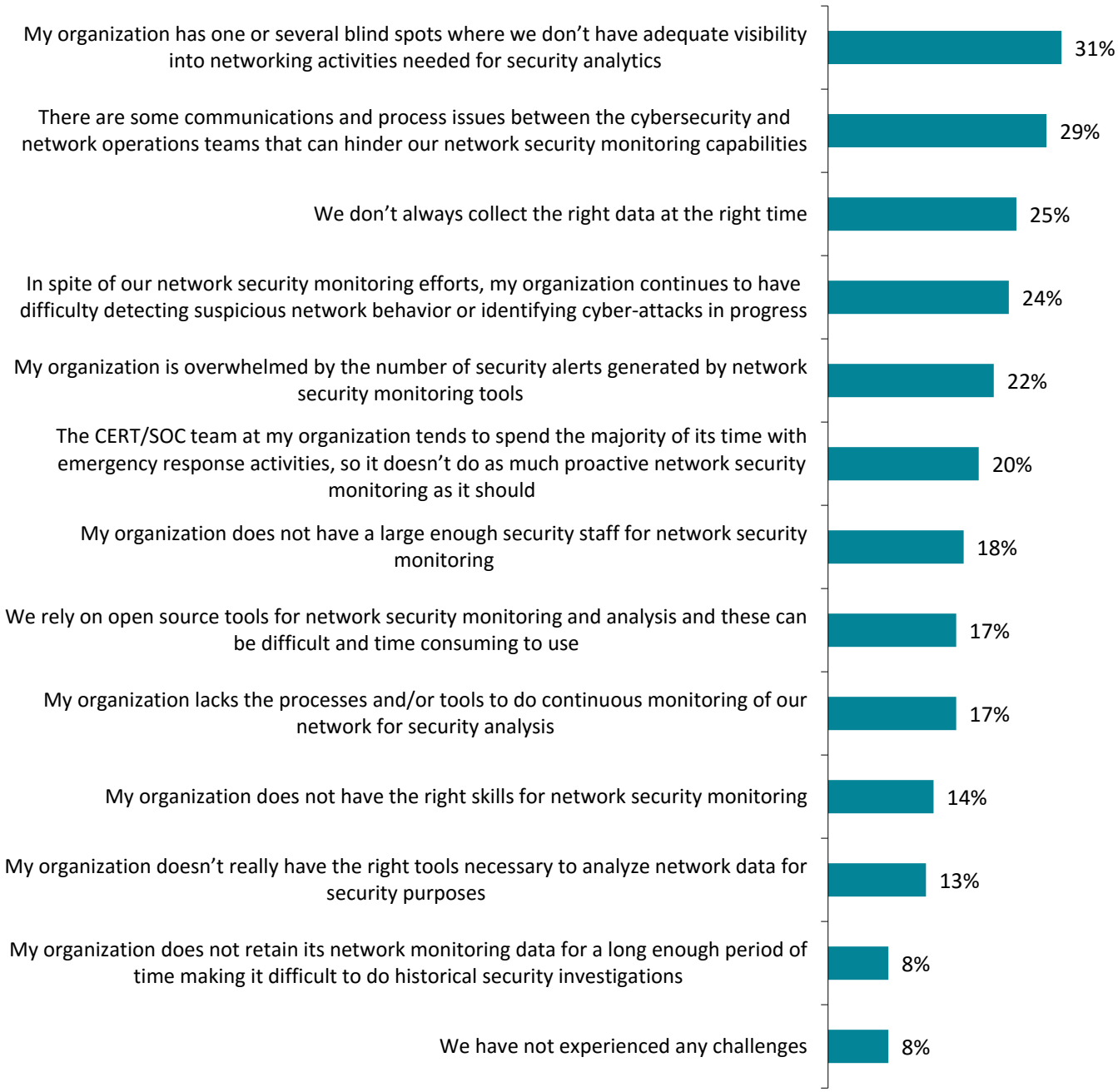
Temporal challenges. One quarter of organizations (25%) proclaim that they don't always collect the right data at the right time. This is especially disconcerting since network security monitoring is intended to provide real-time detection of cyber-attacks. Without adequate data, extended "dwell time" on the network for cyber-adversaries could escalate a minor security event into a major data breach.

Sadly, 24% of survey respondents say that in spite of their network security monitoring efforts, their organizations continue to have difficulty detecting suspicious network behavior or identifying cyber-attacks in progress. Network security monitoring may be considered critical by most organizations, but nearly one in four also admit that current network security monitoring efforts aren't very effective.

FIGURE 5

Network Security Monitoring Challenges

When it comes to network security monitoring, which of the following do you believe are your organization's greatest challenges? (Percent of respondents, N=200, three responses accepted)



Network Security Monitoring Future Strategy

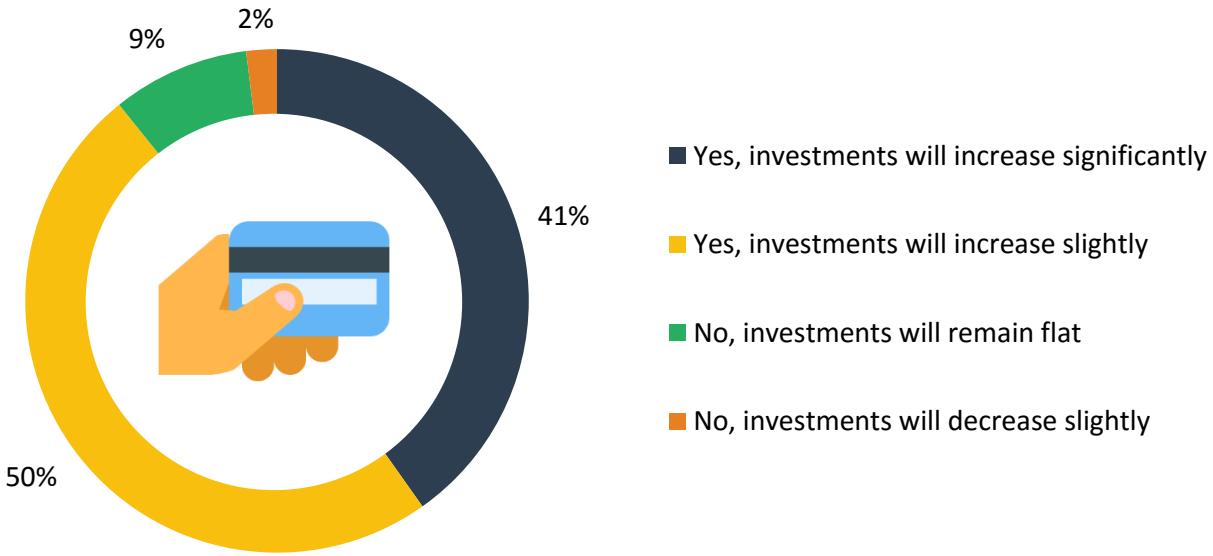
On one hand, cybersecurity professionals realize that network security monitoring is critical, and they understand what efforts are needed from a people, process, and technology perspective. On the other hand, network security monitoring grows increasingly difficult and is fraught with many challenges.

It appears that many CISOs are intent on addressing this situation (see Figure 6)—41% of organizations say that their investment in network security monitoring will increase significantly over the next two years, while another 50% say they will increase investment somewhat. Based upon the weaknesses and challenges described above, these firms will likely invest in areas like technology integration, comprehensive network coverage, improved threat detection, and tools that help promote collaboration and cooperation between cybersecurity and network operations teams.

FIGURE 6

Network Security Monitoring Investment

Over the next two years, do you believe that your organization will increase its investments in network security monitoring technologies, training, and resources? (Percent of respondents, N=200)



In addition to asking about budgets, ESG also asked survey respondents to identify some of their strategic priorities for network security monitoring. This list includes (see Figure 7):

Providing more training to existing staff on network security monitoring. As part of this project, ESG research also revealed that 59% of organizations cite a modest or significant shortage of personnel with strong network security monitoring skills. Recognizing this deficit, many CISOs will ramp up network security monitoring training for cybersecurity and network operations staff.

Integrating network monitoring/threat detection with network and security operations tools. ESG has seen a consistent appetite for security technology integration in all areas including network security monitoring. In this case, many firms want to integrate network security monitoring and threat detection tools with other technologies like SIEM, NPM, and incident response platforms.

Investing in new types of network security monitoring technologies. Based upon the research presented in this report, large organizations need network security monitoring tools featuring scalability, ease of use, and intelligent analytics. CISOs are ready to invest in these types of network security monitoring technologies.

Making changes to the IT organization to enable more collaboration. As stated several times, network security monitoring depends upon a collective and well-coordinated effort by cybersecurity and network operations teams. The ESG research indicates that organizations are willing to change organizational structures in order to improve this collaboration.

FIGURE 7

Strategic Plans for Network Security Monitoring

Which of the following activities does your organization have planned for the next 12 to 24 months? (Percent of respondents, N=200, multiple responses accepted)

The Bigger Truth

The ESG research demonstrates a precarious situation. Network security monitoring is certainly appreciated and cybersecurity professionals have strong opinions about what's needed for success. Nevertheless, many organizations aren't following their own advice, making network security monitoring efforts far less fruitful than they should be.

It is encouraging to see that most organizations understand this predicament, plan to increase network security monitoring spending, and are building a more comprehensive strategy for the future. As they look toward enhancing network security monitoring, large organizations should:

Gain a clear understanding of the difference between network security monitoring and SIEM and invest in both. Surprisingly, there is still some confusion around where and when to use SIEM and where and when to use network security monitoring. This is somewhat understandable since SIEM has anchored security analytics for the past decade. However, given today's threat landscape, SIEM should be enhanced with other types of analytics including network security monitoring. In an ideal situation, these two technologies complement each other, with SIEM focused on event correlation, rules, and dashboards, and network security monitoring pointed at monitoring traffic flows, connections, and packet-based content. Security teams should have a clear understanding of each of these technologies, their individual roles, and their collective value before proceeding.

Get the network operations team involved. While network security monitoring technologies will likely be purchased and operated by the cybersecurity team, it is important to get network operations involved with things like requirements definition, pilot projects, and escalation processes. The goal? Establish a common network security monitoring foundation that will be used collectively by both groups. This should help ease the communications/collaboration problems exposed in this report while aiding both teams to meet their group goals and objectives. It can also help turn network security monitoring into policies and enforcement in areas like granular network segmentation and user/device access controls.

Strive for integration. As the ESG research clearly indicates, network security monitoring success is highly dependent upon multiple points of integration with other technologies like endpoint security monitoring, SIEM, threat management, and threat intelligence. It is also worthwhile to look for opportunities to integrate network security monitoring and networking equipment for segmentation and access control purposes. This will help provide a comprehensive lens for security analytics.

Consider ease of use and automation. ESG research conducted earlier this year indicates that 46% of organizations claim to have a problematic shortage of cybersecurity skills.[1] Unfortunately, this means that cybersecurity organizations may not have enough people or time to use network security monitoring technologies effectively. Given this, CISOs should emphasize ease of use in all network security monitoring decisions. For example, network security monitoring tools should be simple to install, and meet the needs of junior security analysts, experienced forensic investigators, as well as the network operations staff. To address the skills shortage gap, network security monitoring technology should also have some capacity to automate processes and operations, offloading today's manual tasks.

Balance visibility and enforcement. In support of automation, network security monitoring should be aligned closely with security controls themselves. When network security monitoring tools detect threats or vulnerabilities, they should have the capacity to work with and modify various security controls. For example, when network security monitoring detects a highly suspicious connection, it should be able to work with network security controls to quarantine a system, terminate a connection, or create a new firewall rule. These kinds of capabilities depend upon the tight integration described above.

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