Research Insights Report

Network Security Operations Transformation: Embracing Automation, Cloud Computing, and DevOps

By Jon Oltsik, ESG Senior Principal Analyst and ESG Fellow

July 2018

This ESG Research Insights Report was commissioned by Tufin and is distributed under license from ESG.

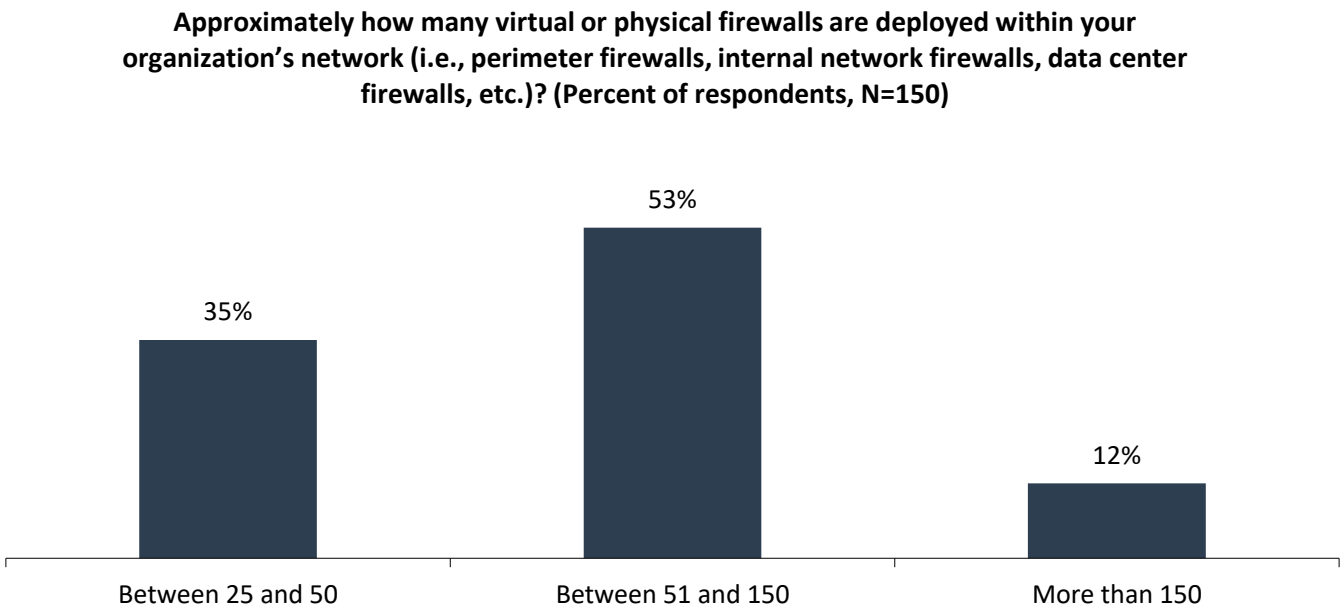
Contents

Executive Summary

In 2018, the Enterprise Strategy Group (ESG) completed a research survey of 150 IT and cybersecurity professionals with knowledge of, or responsibility for, network security operations. Survey respondents were in North America and worked at enterprise organizations (i.e., more than 1,000 employees). Respondents represented numerous industry and government segments, with the largest participation coming from manufacturing (18%), financial services (i.e., banking, securities, insurance, 17%), retail/wholesale (14%), health care (11%), and business services (9%). It should be noted that ESG conducted a similar research study in 2016. Survey responses and data points from each of these surveys will be highlighted within this research insights paper.

Survey respondents were also required to work at organizations with advanced network security operations needs. ESG used the number of firewalls in place at an organization to gauge its level of network security operations maturity. Thirty-five percent of respondents worked at organizations with between 25 and 50 virtual/physical firewalls, 53% worked at organizations with between 51 and 150 firewalls, and 12% worked at organizations with more than 150 firewalls (see Figure 1). Potential survey respondents with less than 25 firewalls were terminated from the survey process.

Figure 1. Number of Firewalls



Source: Enterprise Strategy Group

Based upon the research collected for this project, ESG concludes:

- **Network security operations continues to grow more difficult.** More than half of cybersecurity professionals surveyed for this project believe that network security operations are more difficult today than they were two years ago due to growth in network traffic, the number of connected devices, and increased cloud adoption. Respondents also believe that network security operations are more difficult because of increased frequency and severity of cyber-attacks to defend against and a higher number of vulnerable systems to scan, discover, and remediate than there were in the past. In total, the research portrays network security operations as complex, fragmented, and still reliant on manual processes.

- **Organizations understand they need network security operations automation.** The clear majority of organizations believe that automating network security operations is critical or very important for supporting their IT initiatives.

Why? Automation can help them enforce consistent security policies across hybrid clouds, improve staff efficiency, and minimize human error.

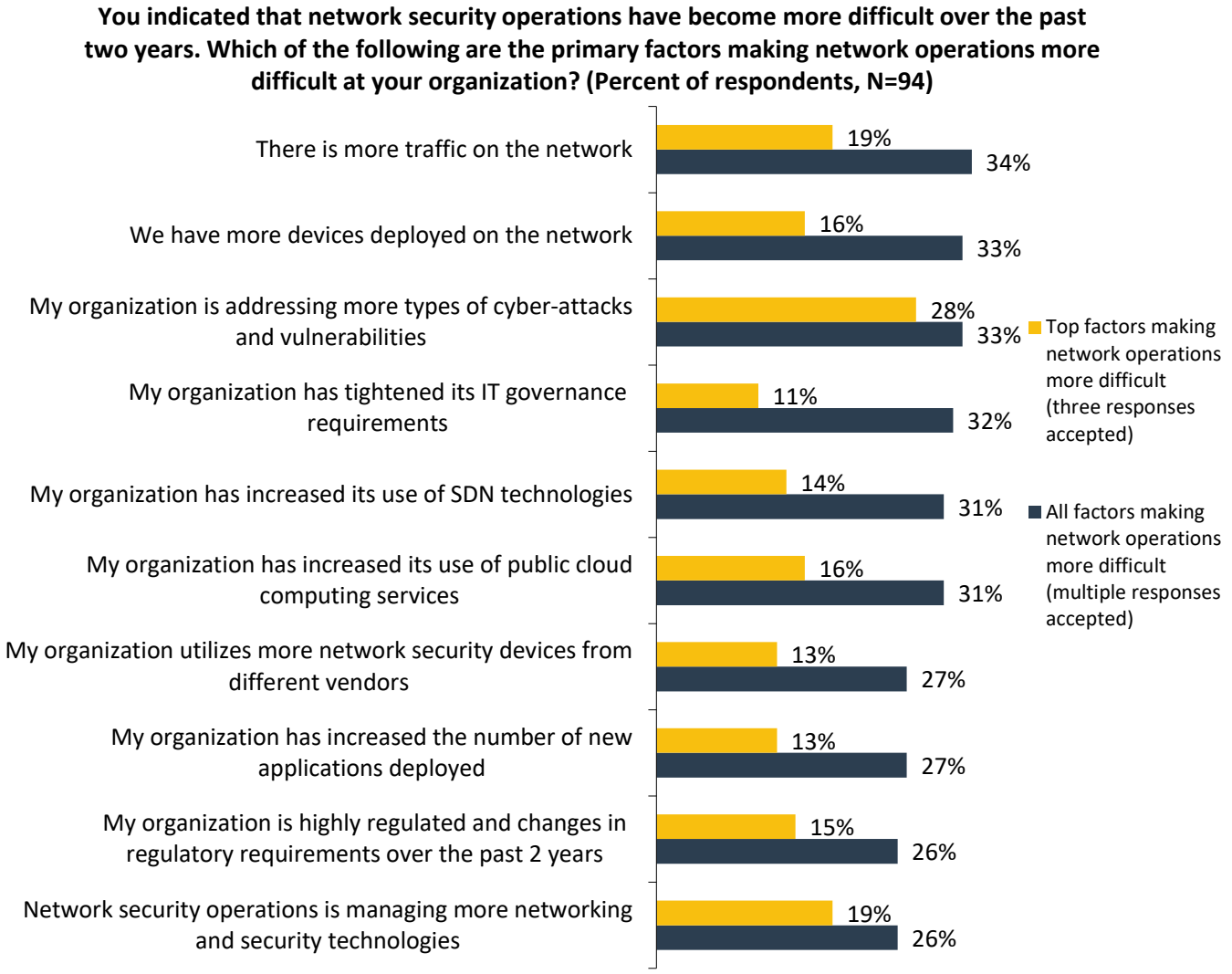
- **Cloud computing is aggravating network security's operational challenges.** This and other research leaves no doubt that organizations have embraced hybrid cloud computing and agile development and are increasing their use of containers and microservices. While cloud computing delivers many business and IT benefits, it can also exacerbate problems associated with network security operations. CISOs must address these additional challenges by consolidating network security operations to gain visibility into cloud workloads, manage security policy, and automate security processes.

State of Network Security Operations

Cybersecurity professionals agree that network security operations continues to grow more difficult. In fact, 62% of survey respondents say that network security operations have grown more difficult over the past two years because of factors such as (see Figure 2):

- **More network traffic.** Just over one-third (34%) of respondents say that network security operations is more difficult than it was two years ago because of the growth of overall network traffic.
- **More devices on the network.** Aside from additional network traffic, 33% of respondents say that network security operations is more difficult today than it was two years ago because there are more devices connected to the network. Often, these are IoT devices with minimal onboard security that communicate using esoteric protocols.
- **More cyber-attacks and vulnerabilities.** One-third of respondents say that network security operations is more difficult today than it was two years ago because of growth in the number of cyber-attacks and software vulnerabilities. These issues put pressure on security operations teams to improve the efficiency of threat detection and incident response processes and segment the network traffic to decrease the attack surface and ensure rapid threat containment.

Figure 2. Factors Making Network Security Operations More Difficult



Source: Enterprise Strategy Group

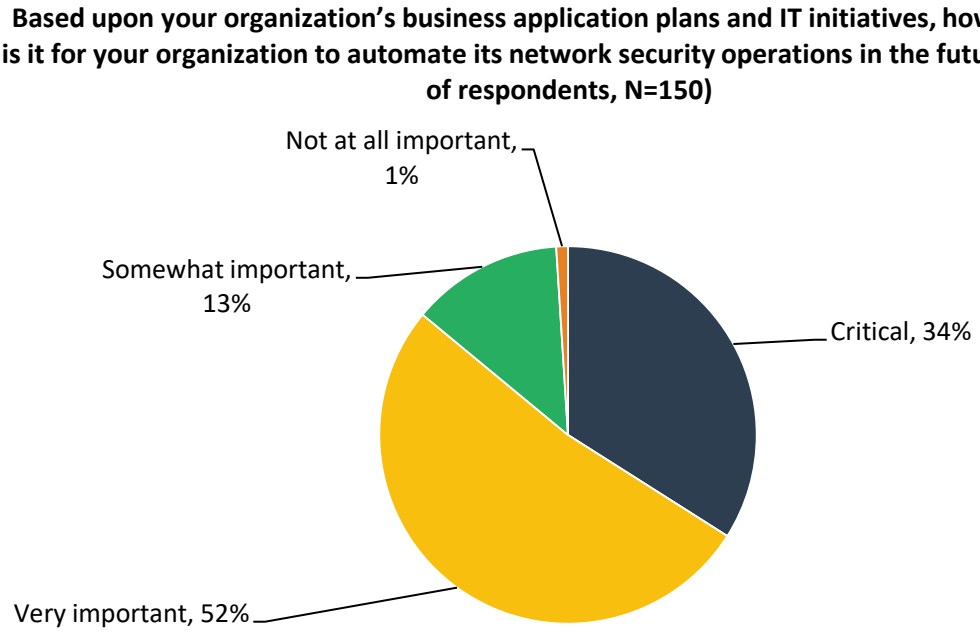
The current state of network security operations also impacts regulatory compliance, as 73% of respondents strongly agree or agree with the statement, "It can be difficult and/or time consuming to get an accurate account of network security controls for regulatory compliance audits."

Embracing Automation

While many responded that they have the right procedures in place, they use a combination of tools, and 65% recognize that modifying and/or implementing network security controls is still a very manual process that requires the expertise of multiple teams to execute. We see this dichotomy as reflective of the fact that organizations do have processes in place *and* they are inefficient.

What's needed? Respondents believe that they must align with the pace of business needs by automating network security operations as much as possible. More than one-third (34%) of respondents believe that network security operations automation is critical, while 52% say it is very important (see Figure 3).

Figure 3. Growing Importance of Network Security Operations Automation



Source: Enterprise Strategy Group

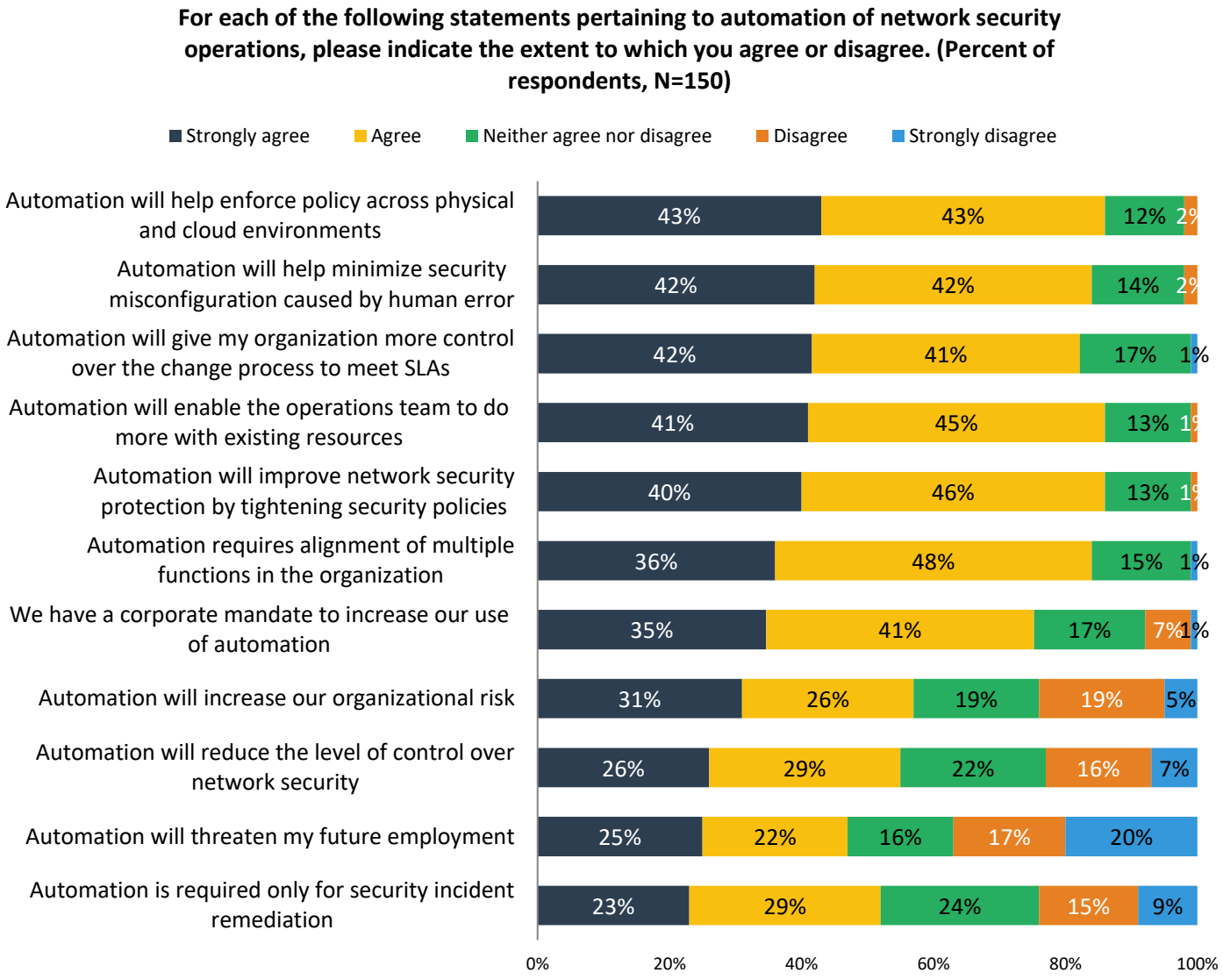
The cybersecurity professionals participating in this research project were also asked to identify the benefits of network security operations automation based upon a series of statements (see Figure 4). The data reveals that:

- Eighty-six percent strongly agree or agree that automation will help enforce policy across physical and cloud environments. By automating policies, security professionals believe they can standardize processes while creating common ways to measure status across hybrid clouds.
- Eighty-six percent strongly agree or agree that automation will enable the operations team to do more with existing resources. This is especially important given the global cybersecurity skills shortage. Other ESG research indicates that 51% of organizations report a problematic shortage of cybersecurity skills in 2018.[1]
- Eighty-four percent strongly agree or agree that automation will help minimize security misconfigurations caused by manual inputs. By programming policies into automation engines, security teams can help organizations avoid common human errors like security rule contention and misconfigurations. This is extremely critical as security and IT teams increase their knowledge and gain experience with hybrid cloud computing.
- Eighty-three percent strongly agree or agree that automation will give their organization more control over the change process to meet SLAs. This is particularly true in organizations embracing DevOps and orchestration for application deployment.

[1] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.

It is also worth noting that 57% say that automation will increase organizational risk. To some extent, this is to be expected as security professionals are paid to be skeptical and paranoid. Despite this cautious view, however, most survey respondents believe that automation is a net positive compared to today's reliance on manual security operations.

Figure 4. Network Security Operations Automation Gaps Remain



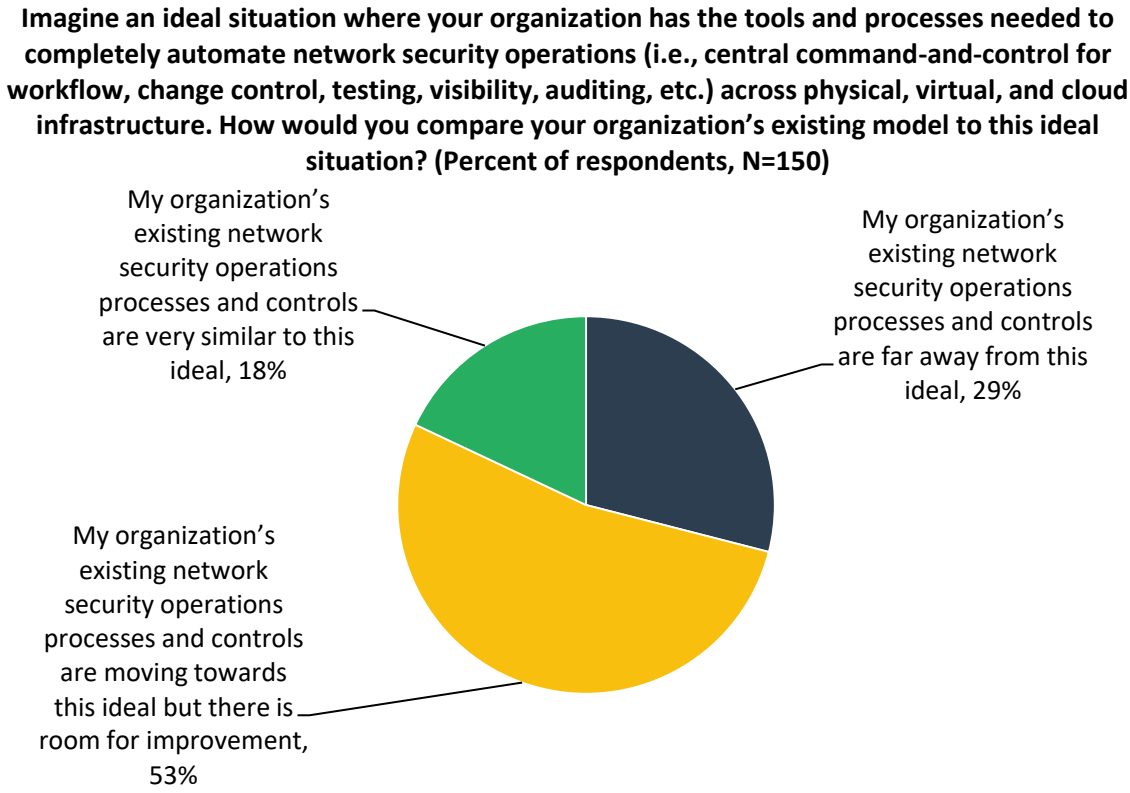
Source: Enterprise Strategy Group

The data indicates a trend where cybersecurity professionals are increasingly recognizing the potential benefits that can be achieved through automation. Unfortunately, a long road may lie ahead for many organizations. The research indicates that only 18% of organizations believe that they have existing security operations tools and processes in place to fully automate network security operations today. On the other hand, 53% say that their existing network security operations processes and controls are moving toward an ideal state but there is room for improvement.

Perhaps these organizations have started their automation journey by automating a few tasks using scripts or API integration. This is a good start but it is not a sustainable way to automate security operations. Alarmingly, close to one-third of respondents claim that their organization's existing network security operations processes and controls are far away from an ideal state necessary for network security operations automation (see Figure 5). CISOs must assess where

their organizations land on this continuum and then deploy technologies and re-engineer processes to move them ahead toward network security automation as soon as possible.

Figure 5. Network Security Operations Automation Gaps Remain

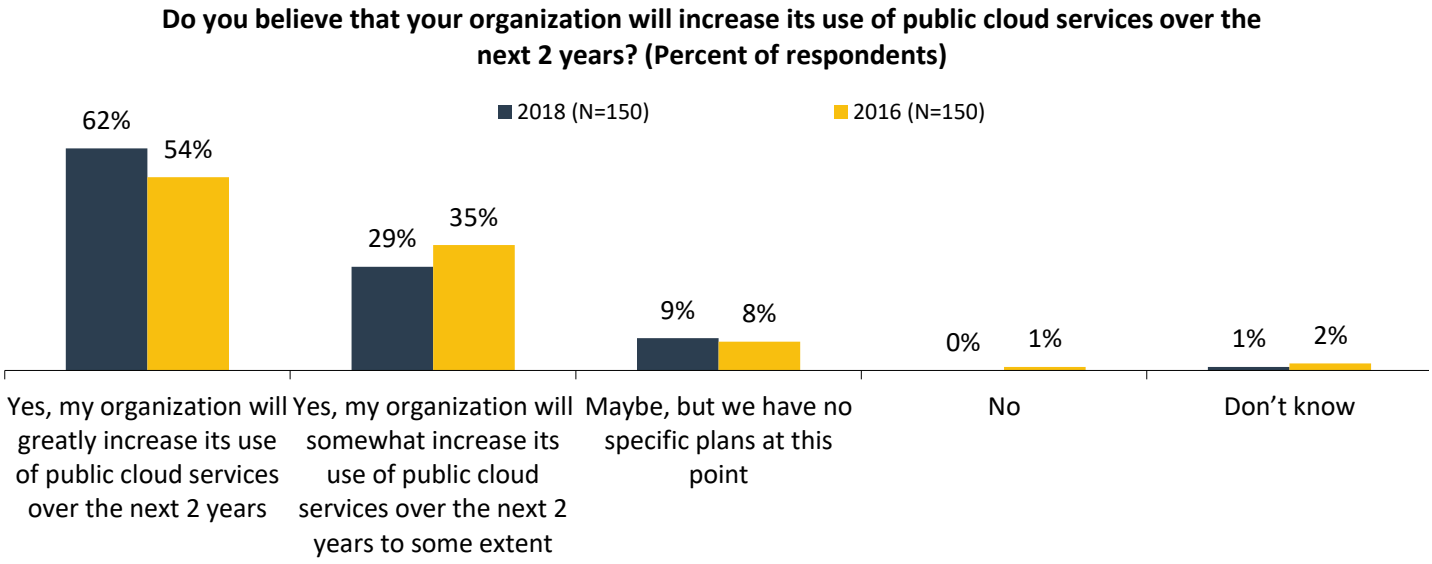


Source: Enterprise Strategy Group

On to the Cloud

The debate is effectively over—organizations are moving an increasing number of workloads to the public cloud. In fact, ESG research indicates that this trend has increased over the past two years. In 2016, 54% of respondents surveyed said that their organizations would greatly increase their use of public cloud services over the following two years. In 2018, this movement increased, and 62% now say that their organizations will greatly increase their use of public cloud services through 2020 (see Figure 6).

Figure 6. Growing Use of Public Cloud Services



Source: Enterprise Strategy Group

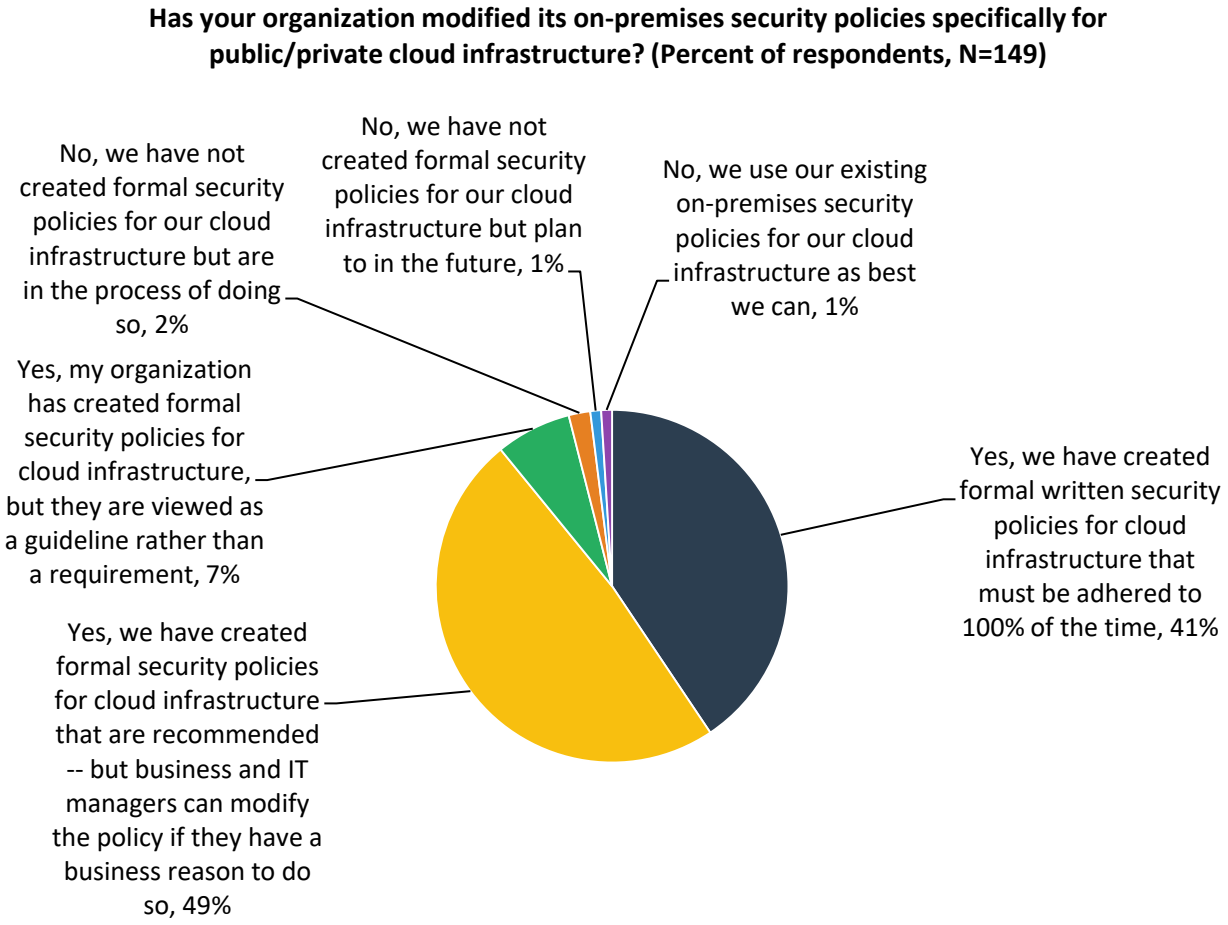
Public cloud usage has delivered measurable benefits to many firms. Some organizations report that the use of cloud computing has helped them accelerate application development and deployment. Cloud computing can also deliver lower costs by offloading server operations and maintenance to cloud service providers.

Cloud Computing, Network Security Operations, and Policy Enforcement

While organizations welcome these benefits, unique cloud security requirements can lead to additional overhead for cybersecurity teams as they modify existing network security operations. This is particularly evident when it comes to enforcing new security policies designed for hybrid clouds.

Only 41% of respondent organizations currently using private cloud and/or public cloud services have created formal written security policies for cloud infrastructure that must be adhered to 100% of the time. Forty-nine percent of organizations have created formal security policies for cloud infrastructure but business and IT managers can modify the policy if they have a business reason to do so (see Figure 7), making it difficult to enforce consistent security policies.

Figure 7. Organizations Are Modifying Security Policies for Cloud Computing



Source: Enterprise Strategy Group

Users tell ESG that these policy modifications can be complex. For example, specific policies may be needed when workloads connect across heterogeneous clouds or when application traffic flows to and from public and private cloud deployments. In instances like these, creating, enforcing, and monitoring cloud security policies requires multiple cloud, networking, and security technologies, making them difficult to manage.

Cloud computing security requirements are especially significant because security operations are already extremely complicated. Network fragmentation plays a role, as indicated by the fact that only 33% have a single cloud vendor, while over 60% indicated they have a multi-cloud environment.

The data shows that, for cloud, security policy creation and enforcement needs to be aligned with burgeoning agile application development and DevOps procedures. The research indicates that 45% of organizations have already adopted an agile development and/or DevOps model, while another 42% are in the process of adopting an agile development and/or DevOps model. The mix of workload types is another complicating factor of cloud security policies. Furthermore, 37% of organizations surveyed have application containers and/or microservices in production today while another 15% use containers/microservices for test and development today.

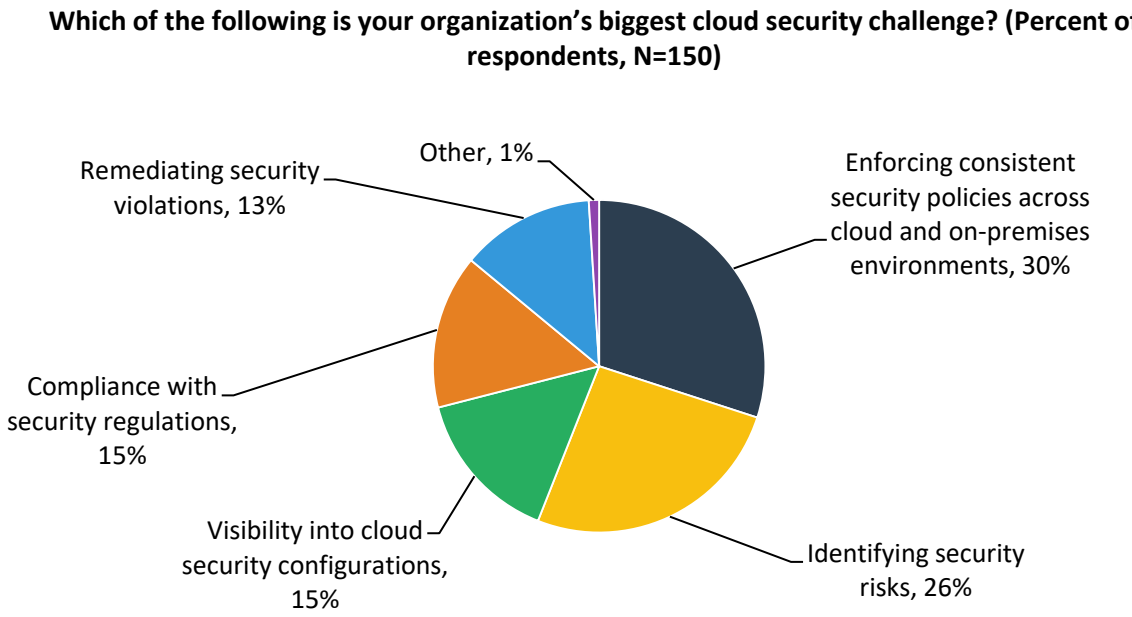
As agile development, DevOps models, and containers/microservices proliferate, security teams must align monitoring activities and security controls implementation with orchestration tools (i.e., Chef, Puppet, Ansible, Kubernetes, etc.) to support continuous integration/continuous delivery (CI/CD) pipelines. This means that cloud security operations and policies must be flexible while security tools must support APIs for cloud orchestration integration. Furthermore, security

teams must learn to work closer to developers and DevOps personnel to ensure that security policies align with application delivery and business goals.

Cloud Security Challenges

With the pressure for organizations to digitally transform, it's worth understanding and addressing today's most pressing cloud security challenges. Clearly, security policy management represents a demanding issue, as 30% of respondents believe that enforcing consistent security policies across cloud and on-premises environments represents their biggest cloud security challenge. Additional challenges include identifying security risks (26%), gaining visibility into cloud security configurations (15%), and regulatory compliance (15%) (see Figure 8).

Figure 8. Top Cloud Security Challenges



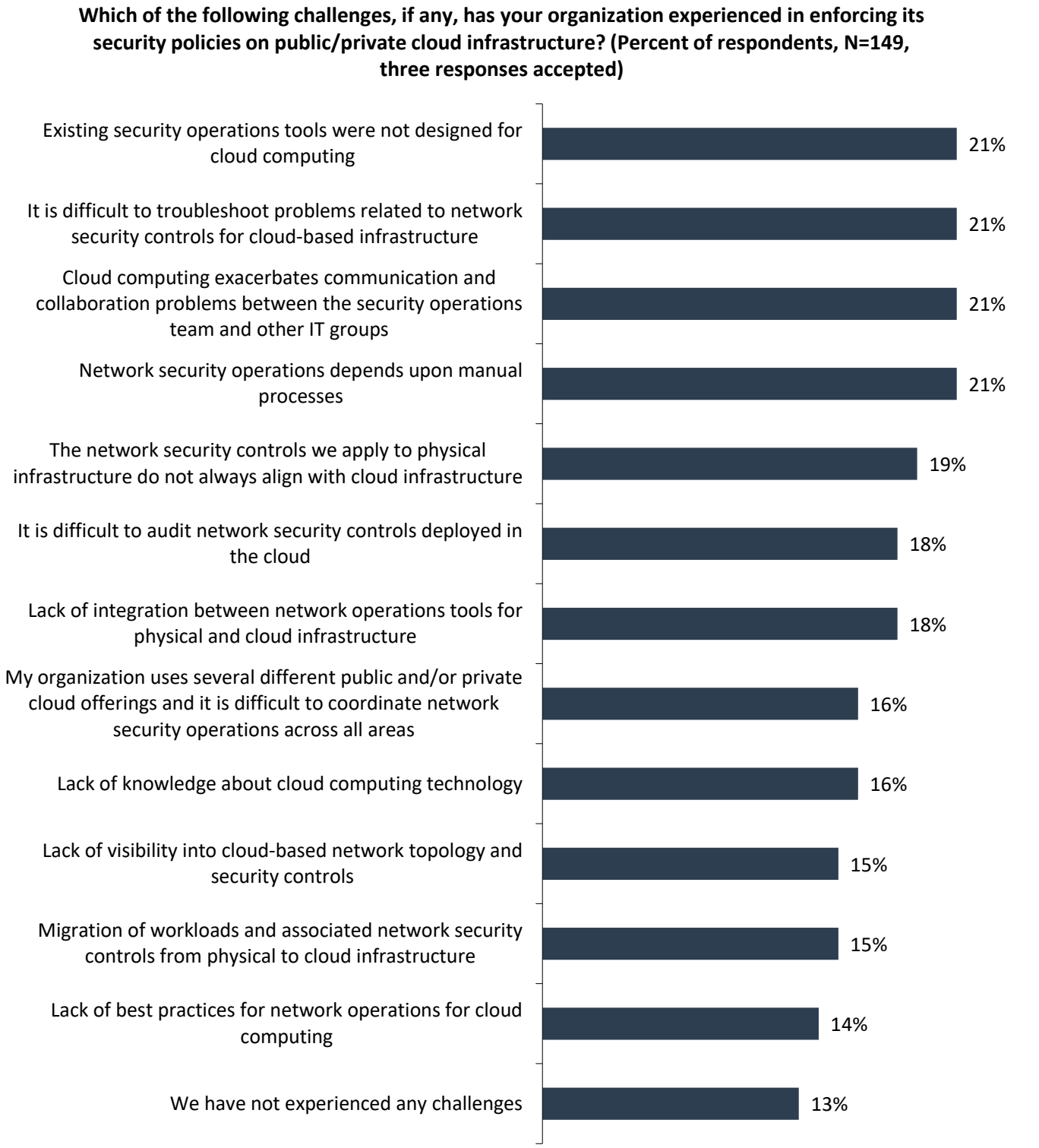
Source: Enterprise Strategy Group

Since enforcing security policies seems to be so problematic, ESG pushed further to ask cybersec professionals for more detail. While no one issue stood out, survey respondents currently using private cloud and/or public cloud services pointed to policy enforcement challenges for public/private cloud infrastructure in a variety of ways, including (see Figure 9):

- Technology problems. Twenty-one percent of cybersecurity professionals surveyed claim that existing security operations tools were not designed for cloud computing, making it challenging to enforce security policies.
- Troubleshooting problems. Twenty-one percent of those surveyed also indicate that it is difficult to troubleshoot problems related to network security controls for cloud-based infrastructure. This could be related to the design problems described above. Alternatively, security teams may not be familiar with cloud-based security controls or monitoring. Either way, troubleshooting challenges force organizations to dedicate excess time and resources to problem resolution.
- Organizational problems. Twenty-one percent of respondents say that cloud computing intensifies communications and collaboration problems between the security operations teams and other IT groups. This is probably because all these groups are learning the idiosyncrasies of cloud computing "on the fly." Regardless of the cause, security and IT teams must find common language and standard processes to address these issues.

- **Process problems.** Twenty-one percent of respondents admit that cloud-centric network security operations depend upon too many manual processes. Again, these issues add overhead to security operations processes. These issues can impact business benefits associated with agile development and DevOps.

Figure 9. Challenges Associated with Enforcing Cloud Security Policies



Source: Enterprise Strategy Group

The Bigger Truth

Based upon the research presented in this report, it is safe to conclude that when it comes to network security operations, there is much room for improvement. Existing tools and operations processes are misaligned for the cloud, forcing network security operations teams to adopt new tools or develop new processes for private cloud environments, various modern application technologies, and disparate public cloud service providers. This translates to constant dynamic changes and the need to scale network security operations significantly.

Achieving these goals will be nearly impossible through incremental changes. The research indicates that respondents agree that automation will require alignment of multiple functions within the organization (i.e., security, network operations, application developers, DevOps, etc.). CISOs must tighten existing operations and then prepare for cloud-ready security technologies and processes built for flexibility, scale, and affinity with DevOps orchestration. This data points to the need to begin automating network security operations as soon as possible. To ease this necessary transition, CISOs should:

- **Assess existing policies and procedures, formalize processes, and then automate.** The research clearly indicates that existing network security processes are too informal and manual, and require an assortment of tools. CISOs will have to dig into their policies and processes to find the biggest bottlenecks and inefficiencies. Armed with this list, organizations can then create priority lists, fix and formalize broken processes, establish consistent methodologies, and then measure progress and results.

- **Enlist help from CIOs.** Security teams can't make progress on an island and must find ways to bridge the gap between security operations and IT. Since cloud computing and growing IT complexity greatly impacts development and IT operations teams, CISOs should work with CIOs to establish and foster a DevOps culture across all technology domains. Additional cloud computing training is a good starting point, but CIOs and CISOs should also work to develop a cloud computing culture across their organizations that supports automation, orchestration, and security. The way forward is to establish shared goals, open lines of communication, and modify compensation plans so that everyone wins as the organization progresses.

- **Consolidate command-and-control through central policy management systems.** Network security controls are increasingly built into the infrastructure itself. Think VMware NSX, Cisco ACI, cloud computing security groups, etc. As this continues, CISOs should eschew purpose-built network security controls in favor of centralized policy management platforms that provide oversight and monitoring across network security controls regardless of their location, technology, or form factor. Network security automation that aligns with DevOps will also help here.

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188