FORRESTER®

20/20 Visibility Clarifies Network Security

Increasing Network Visibility And Team Integration Is Critical To Improving Security

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY INFOBLOX, JULY 2022

Table of Contents

Project Team:
John Lloyd,
Market Impact Consultant

Sarah Brinks,
Senior Market Impact Consultant, TL

Jenna Bonugli,
Associate Market Impact Consultant

Contributing Research:
Forrester's Infrastructure & Operations research group

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

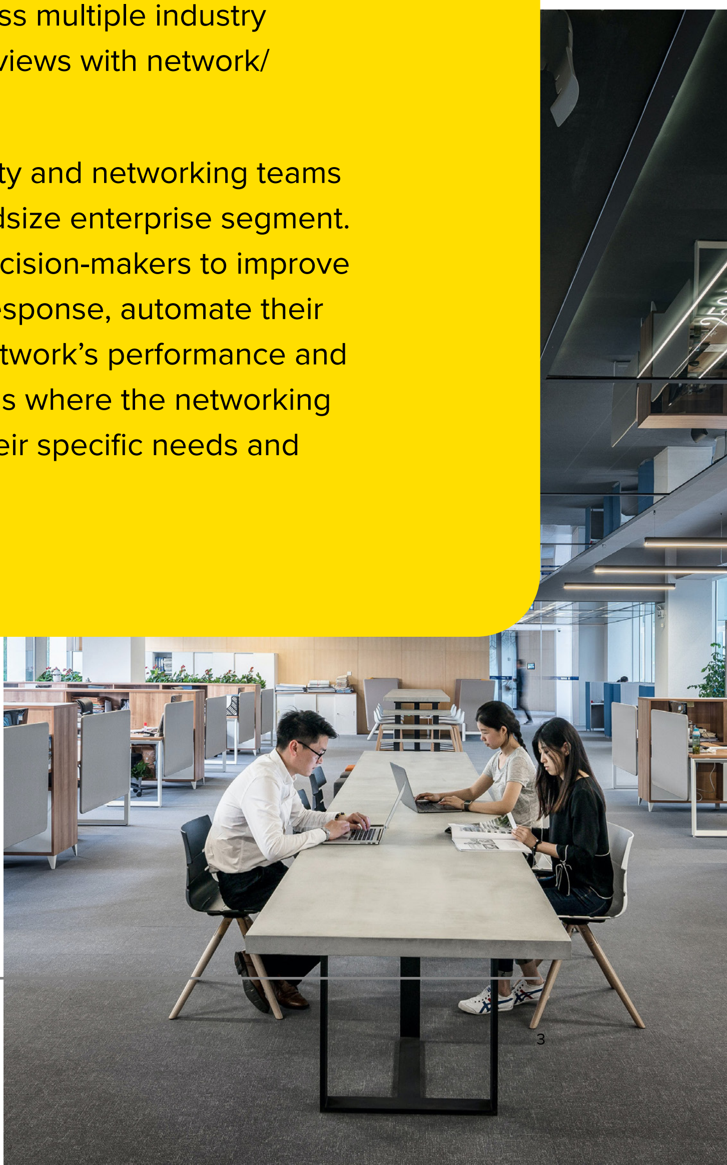
Executive Summary

Visibility is paramount to network security, because it helps organizations discover and understand what they are securing and from whom they're securing it. Poor network visibility impedes security response and capabilities. Without clear visibility, leaders struggle to know what is on their network, manage capacity, and identify tools at their disposal.

Even more fundamental than visibility is the integration and collaboration of the networking and security teams within an organization. If organizational barriers segment and silo these teams, a holistically sound security approach is impossible. If done right, an integrated approach can foster benefits, including better performance and capacity planning, reduced costs, and device discovery. In short, with integration comes visibility.

In May 2022, Infoblox commissioned Forrester Consulting to explore the need for better visibility to improve network security. Forrester conducted an online survey with 423 global IT leaders with responsibility for networking and security purchases and strategy decisions across multiple industry segments, and also completed two qualitative interviews with network/security leaders.

We found that the visibility and integration of security and networking teams is critical to network security for the commercial midsize enterprise segment. Improved visibility allows commercial midmarket decision-makers to improve their organizations' network security and security response, automate their audit/compliance tasks, and better manage their network's performance and capacity-planning needs. In midmarket organizations where the networking and security buyer are the same, we can identify their specific needs and barriers to improving visibility.



Key Findings

Security leaders are increasing their investments in network visibility. Ninety-seven percent of surveyed global IT leaders are already invested in or are planning to invest in new visibility tools/technologies over the next three years, and 61% think their organizations should invest more in network discovery for full visibility.

Solutions that improve visibility are in high demand. Nearly 80% of surveyed decision-makers see an integrated solution that benefits both their organizations' networking and security objectives as appealing, but three out of four surveyed global IT decision-makers (ITDMs) say they still have siloed teams. If more improvements in integration aren't made at a steady pace, organizations will not have visibility across teams and will, therefore, fall behind on their security goals.

Better visibility elevates security responses and capabilities. Eighty-one percent of surveyed decision-makers agree that better network visibility would improve their organizations' overall security/security response capabilities. Better network visibility offers many other benefits, including better network performance/capacity planning, more audit compliance capabilities, and operational efficiency.

Network Visibility And Team Integration Bolster Security

Visibility is the ability to discover all network devices and end hosts; plan for availability, bandwidth utilization, and other network capacity constraints; and identify when current network capacity might not meet future requirements. This is a critical aspect to securing and defending networks. Investing in network security within an organization that has no collaboration, communication, or visibility between teams and functions is a losing fight, which is why global IT leaders with responsibility for network and security investments are prioritizing enterprise security solutions that offer improved network visibility. However, visibility isn't one-dimensional — integration of security and network teams is critical for facilitating visibility and breaking down siloes to build up efficient and effective security capabilities.

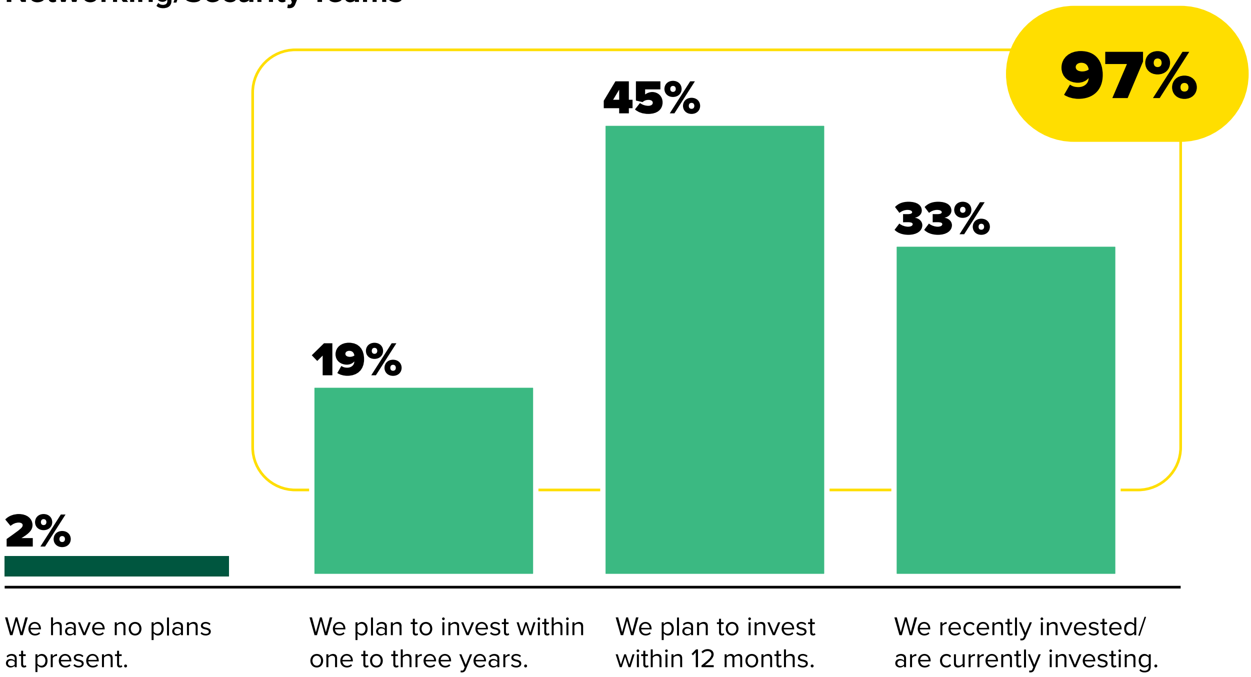
But before visibility is even possible, improvements in integration between organizations' security and networking teams must be made. If the day-to-day operations and buying solutions of these teams continue to be siloed, the effectiveness of an organizational security response will suffer.

After surveying 423 global IT leaders about the current state of network security at their organization, we found that:

- **There is synergy between visibility and security.** Ninety-eight percent of ITDMs are investing in their security capabilities to support an evolving network architecture. The top choice to support their security capabilities with network infrastructure is an investment in network discovery (61%). Almost all (97%) of respondents are already invested in or are planning to invest in new visibility tools/technologies over the next three years to support both their networking and security teams (see Figure 1).

Figure 1

Investment Plans For New Visibility Tools/Technologies To Support Networking/Security Teams



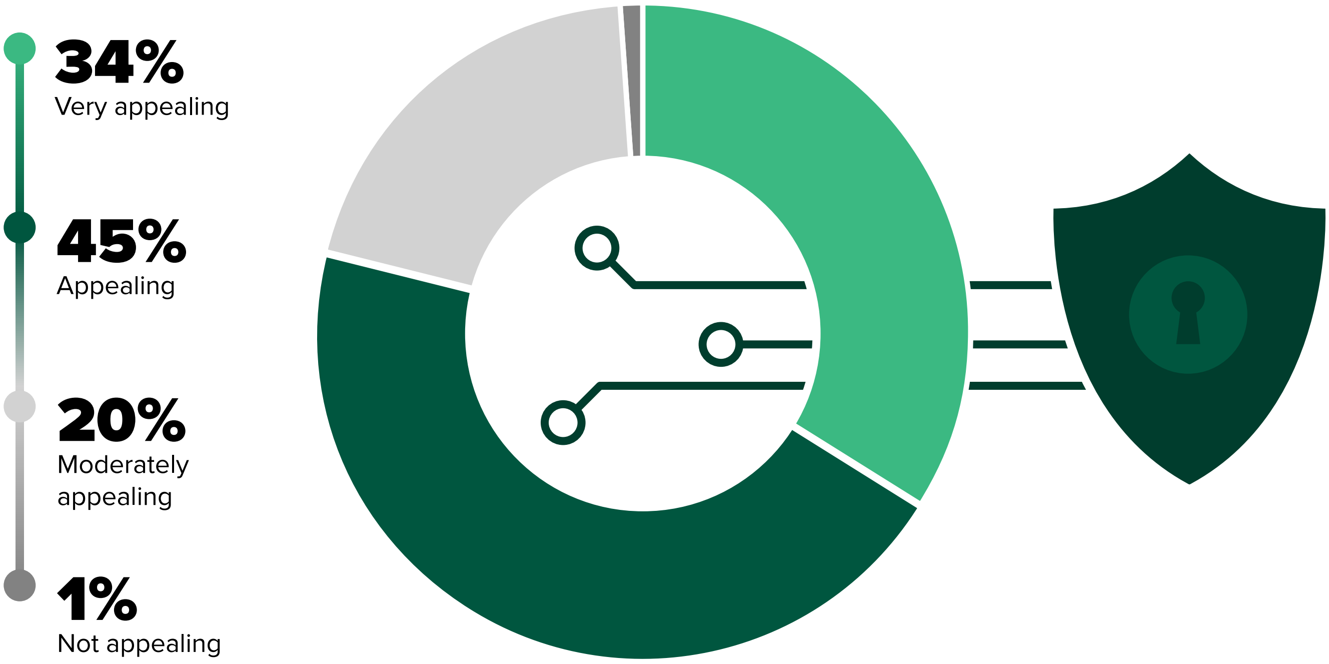
Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

- **Digital initiatives drive current investments.** Today, leaders are using more cloud platforms (73%) and software-as-a-service (SaaS) applications (64%), while leveraging more internet of things (IoT) operational technology (62%) as their top digital initiatives. To bring things full circle, these investments are motivated by use cases like security investigations (60%), troubleshooting (55%), and discovery of what's on the network (54%).

- **Integration of network and security objectives is key.** Seventy-nine percent of decision-makers see an integrated solution that benefits their organizations' networking and security objectives as appealing (with 34% of those respondents saying "Very appealing") (see Figure 2). To promote visibility, one-third of surveyed ITDMs have invested in new tools to support both networking and security teams, while another 64% plan to invest in the next three years. Overall, 98% of decision-makers have invested in security capabilities to support an evolving network architecture.

Figure 2

“How appealing is adding an integrated solution that benefits both your organization's networking and security objectives?”



Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

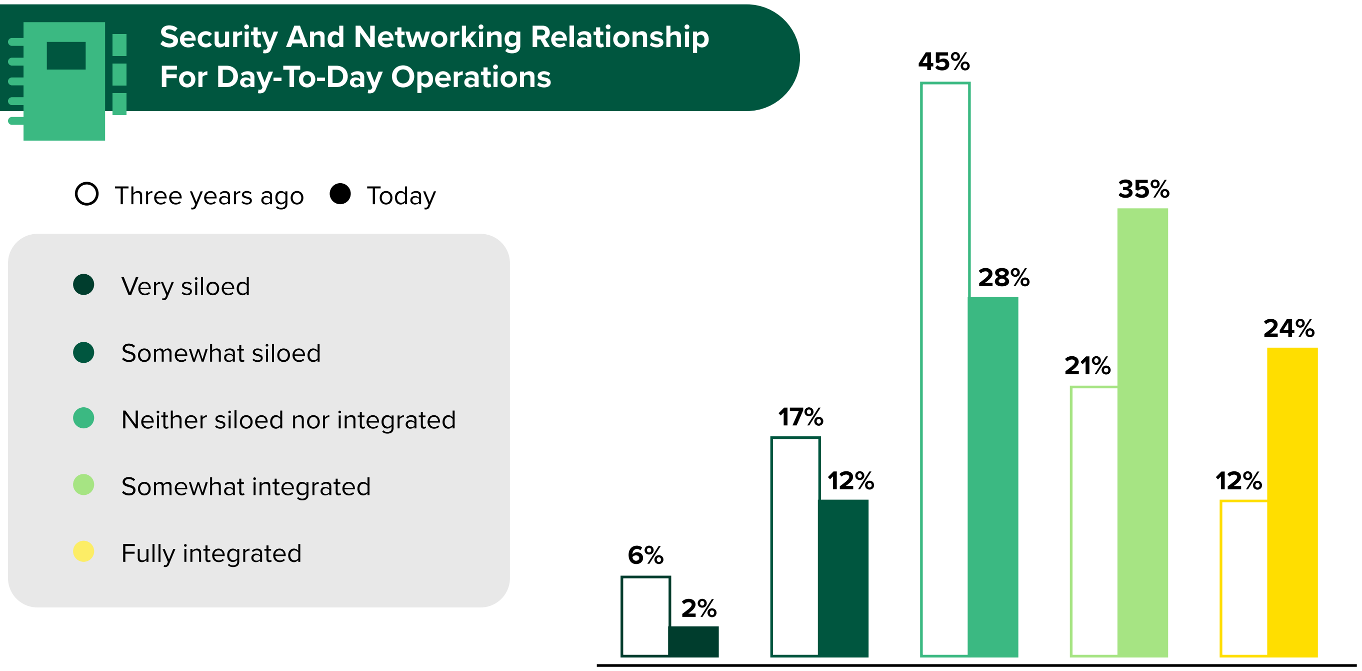
- **To improve visibility, integration must progress.** Steps to improve integrations within IT groups have been made, but further progress is essential for visibility. According to surveyed ITDMs, security and networking teams are nearly twice as likely to say they are fully integrated for day-to-day operations and when buying solutions compared to three years ago (see Figure 3). However, there is room to grow.

> “The people we hired, they're basically masters of pretty much everything and have proven themselves ... We don't really have a distinction between network and security. It's all the same people working on it.”

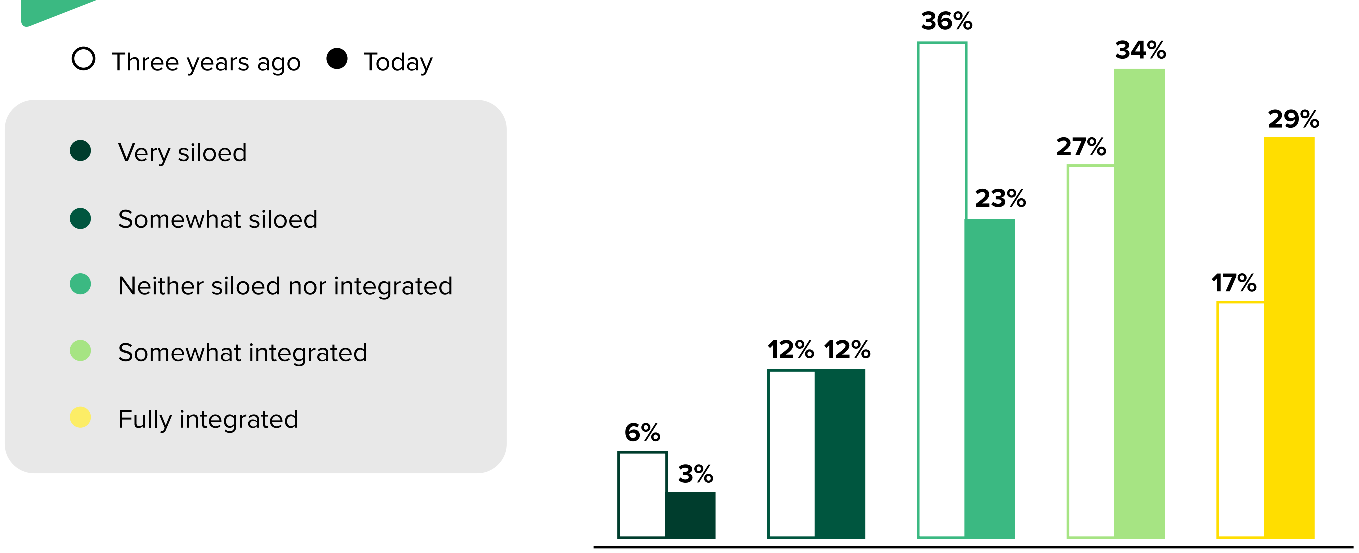
Senior IT infrastructure and cybersecurity director, sports franchise

Figure 3

Security And Networking Relationship For Day-To-Day Operations



Security And Networking Relationship For Buying Solutions



Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

Poorly Integrated Tools And Siloed Practices Block Visibility

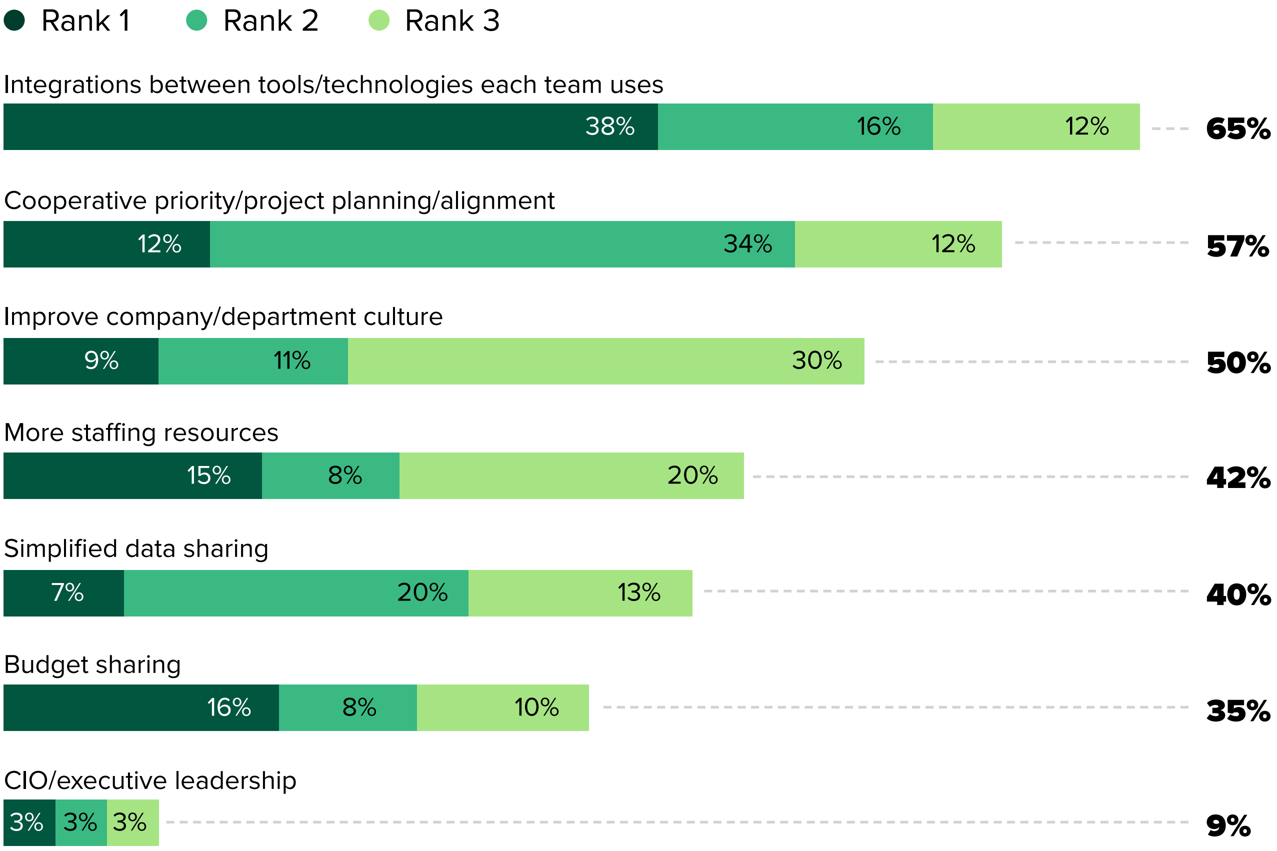
As the senior IT infrastructure and cybersecurity director at a sports franchise pointed out, “Cybersecurity is a daily, almost hourly challenge.” To address that high level of a demand, ITDMs must have clear visibility into what is on their network, protect their organizations’ data, and meet regulatory requirements. In some cases, the digital initiatives that ITDMs use to their strategic advantage can indirectly create barriers to integration across networking and security teams. High cost of technology and lack of skilled workers are also factors impeding the visibility between networking and security teams. ITDMs say that some security capabilities like domain name system (DNS) protection and investigation response are improving with room still to grow, but others have stalled.

If the common challenges that networking and security teams face are diagnosed, then leaders can see what needs to change in order to establish a clear line of sight for better visibility and security:

- **Increasing technology costs is a key challenge.** ITDM’s stated that increased security tool/technology costs (51%) are the top challenge impacting their organization. This underscores the need for holistic solutions that reduce costs and improve operational efficiencies.
- **Silos must come down to encourage collaboration.** ITDMs stated that integration between tools/technologies (65%) is the most significant factor requiring improvement to achieve better collaboration. Cooperative project planning/alignment (57%) and improving culture (50%) are also high on the list (see Figure 4). Only one in four ITDMs say that they do not have siloed teams. It is clear that improvements need to come from within to establish visibility.

Figure 4

Top Changes Needed To Improve Security And Networking Collaboration

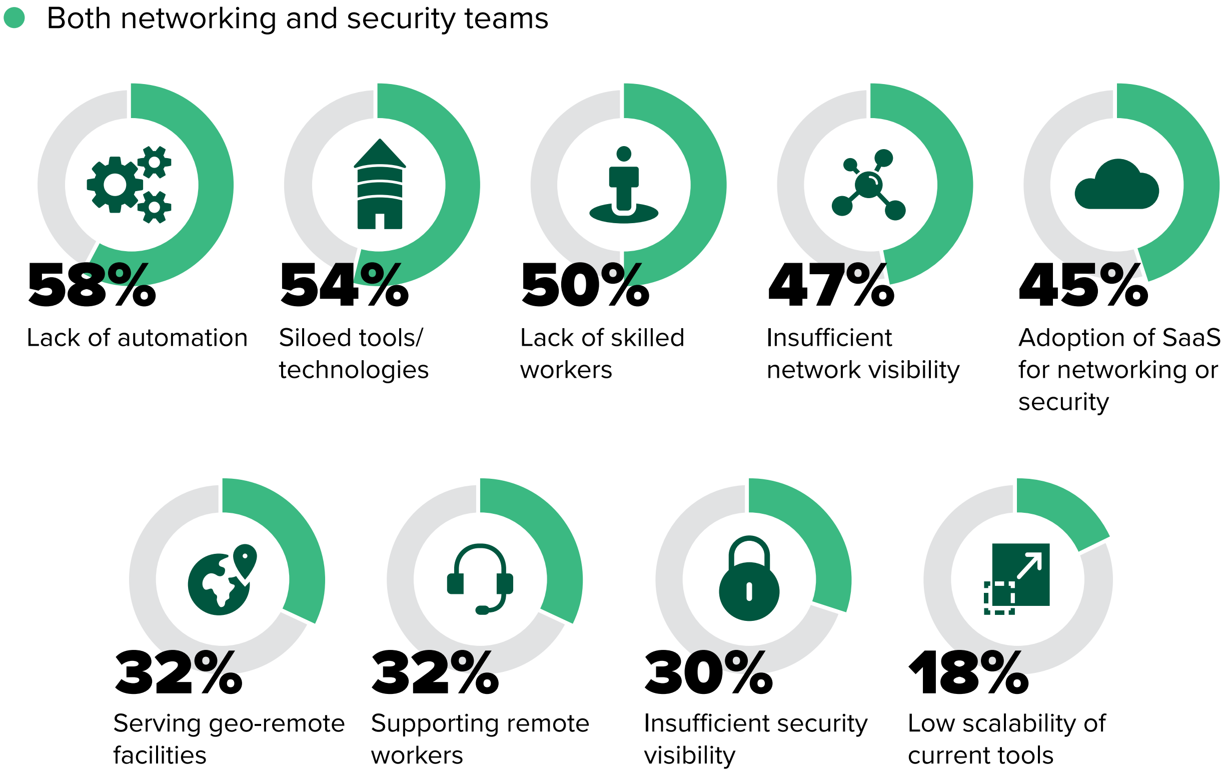


Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

- **A lack of skilled workers is a challenge shared by networking and security teams.** Not having enough skilled workers (50%) is impacting both networking and security teams (see Figure 5). Before an organization can create visibility and connect the efforts of these teams, they need the necessary resources to maintain the scale of their security operations and address common issues. Disconnected teams exacerbate organizationwide challenges like security technology costs (51%), long investigation times (49%), poor interteam communications (46%), and security insurance premium costs (33%).

Figure 5

“Which of the following create challenges for your organization's security and/or networking team?”



Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

> “I came from a very big IT shop, well over 500 people and it was extremely siloed, and it was tough to make meaningful changes. That's influenced our hiring practices. We spent more money on acquiring talent than normal. But that has paid off tremendously, because now we have talent that knows how to run the business and they’re deeply engaged.”

Senior IT infrastructure and cybersecurity director, sports franchise

Visibility Can Holistically Improve Security And Networking Capabilities

Visibility supports the pillars of critical security operations like threat detection, audit/compliance, and network performance and capacity planning. These functions require cost-efficient and modern infrastructure tools on which to function, acting as a cornerstone for improved network visibility.

From a tactical perspective, IP address management (IPAM) data magnifies the effectiveness of these functions by finding and pinpointing threats within the organization's environment. More broadly, however, are the benefits of improving the integration between networking and security teams. This can be a catalyst for improved visibility, efficiency, performance, and stability. So, for global enterprises looking for a holistically better security and networking landscape, better organizational integration is the crucial first step to achieving it.

> The top benefits that global IT leaders expected/experienced as a result of better integration were improved security visibility (**52%**), operational efficiencies (**47%**), and reduced costs (**42%**).

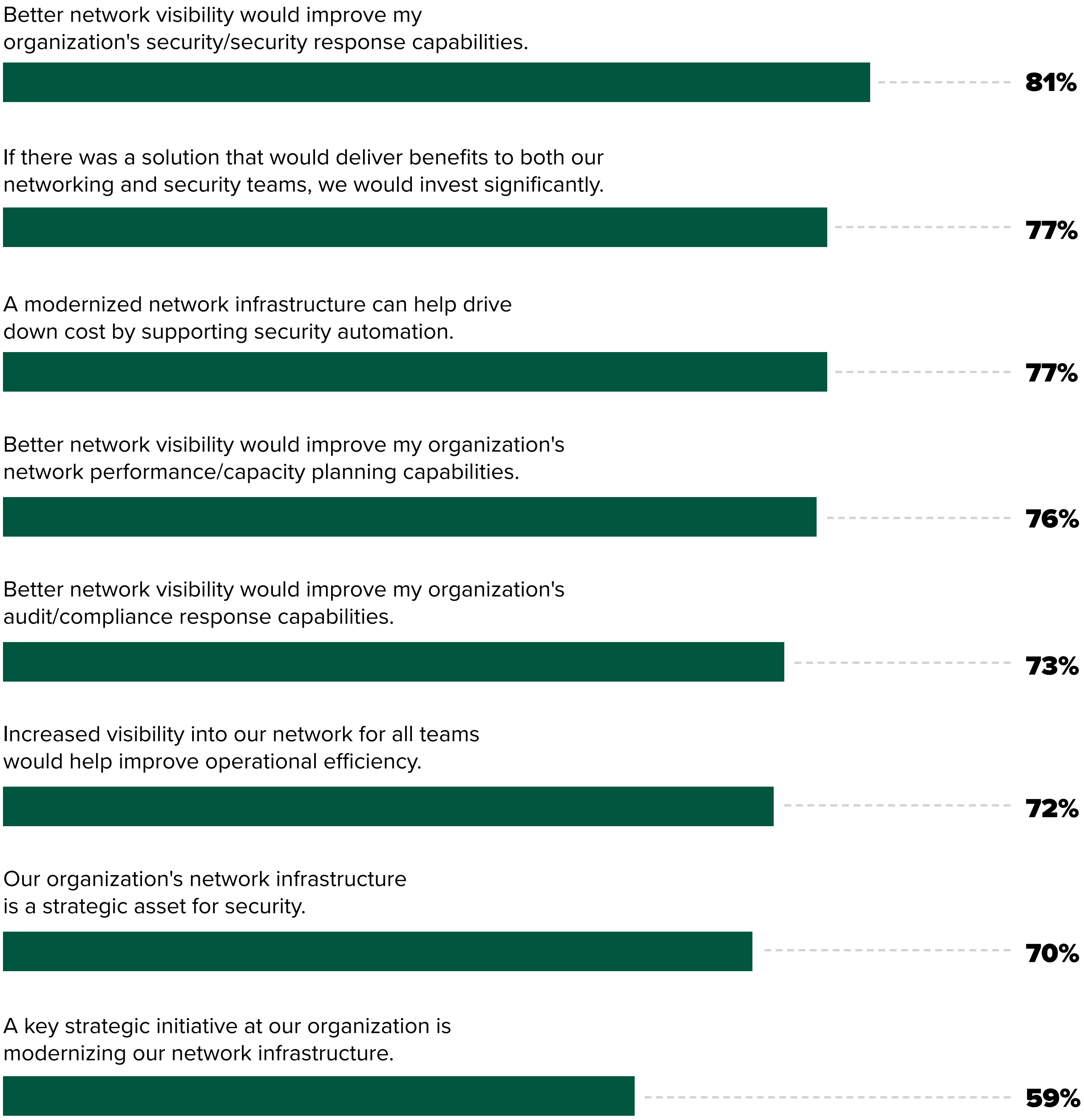
Here's what we found about the opportunities and benefits of visibility:

- **Visibility isn't just synonymous with security, but with efficiency and performance.** Surveyed security and network leaders agree that better network visibility improves security and response (81%), performance (76%), and operational efficiency (72%). IT leaders are ready to take action in support of incorporating better technology into their teams; 77% of respondents agree that modern infrastructure tools drive down the cost of these benefits through automation, and the same number would invest significantly in a solution like this to benefit both security and networking teams (see Figure 6).

Figure 6

"How much do you agree with the following statements?"

(Showing "Agree" and "Strongly agree")



Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

- **IPAM data offers the necessary visibility to identify threats.** Harnessing the power of IPAM data is a critical tool for finding security threats. Seventy-four percent of ITDMs agree that IPAM data helps detect devices associated with security events, and more than half agree that it helps pinpoint the location of devices (56%) and discover operating systems, firmware, and other device data visibility (54%). This is an integral part of an organization's security strategy and improving network visibility.
- **Performance and capacity planning are facilitated through network visibility.** Balancing workloads and operating the network at optimal performance is impossible without visibility. Detecting anomalous activity (48%), troubleshooting network performance issues (43%), and discovering OS, firmware, and other device data visibility (43%) are all examples of how crucial visibility is to aiding network performance and capacity planning.
- **Integration is the key to visibility and efficiency.** Connecting the efforts of security and networking teams unlocks benefits for the organization as a whole. The top benefits that global IT leaders seek and have experienced as a result of better integration are improved security visibility (52%), operational efficiencies (47%) and reduced costs (42%) (see Figure 7).

"A big part of our recent initiatives is seeing what's happening with various attackers when they go after east-west traffic. Whether they're hijacking an internet-of-things device or hijacking the PC, the more you can restrict that and make it very difficult for hackers to move around the environment, the better."

Senior manager of network infrastructure, legal organization

Figure 7

“What benefits would you expect/have you experienced from better integrating the networking and security teams?”

52%	Improved security visibility
47%	Operational efficiencies
42%	Reduced costs
41%	Greater network performance and stability
37%	Extended network visibility

Base: 423 global IT leaders with responsibility for networking and security purchases and strategy decisions
Note: Showing top 5 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Infoblox, May 2022

Key Recommendations

Forrester's in-depth survey of 423 global IT leaders about their needs and challenges around improving network visibility to improve security capabilities yielded several important recommendations:

Build Zero Trust with an identity-centric approach.

The driving force behind Zero Trust is an identity-centric approach, which is based on people, devices, workloads, and networks, to connect to data. Once the identities are known, technology teams enact policies and controls, creating microperimeters across the entire business. This identifies, inspects, and places new and uncontrolled devices in their proper domains.

Standardize and minimize.

Countless point solutions and components litter the halls of infrastructure and operations. Many have overlapping functions and capabilities that create waste, ranging from taking up internal resources, such as infrastructure and maintenance time, to paying warranty costs. In addition, every component added to system is a potential failure point, security hole, or inefficiency. Technology professionals should start with fundamental solutions such as DNS, dynamic host configuration protocol (DHCP), and IPAM (DDI), and maximize investments by using all the tools currently available within the company before purchasing new ones. Any request for a new purchase should go through a full review.

Educate before buying.

Most members of various technology teams don't know the full capabilities of many of the tools available to them for various reasons. This will lead to members acquiring new technologies to solve certain challenges. To maximize the value of the available resources, technology members across all domains should train on the current solutions.

Ensure cross-function teams leverage the same visibility data.

The creation of cross-functional teams using common tools can reap many rewards. Two major benefits reported center on reduction of mistakes made from different visibility information. The other benefit comes from teams aligning to the same goals using similar measured metrics. Thus, many organizations become more agile and adaptive to business and technology changes.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 423 global IT leaders with responsibility for networking and security purchases and strategy decisions across multiple industry segments and two qualitative interviews with network/security leaders at organizations in North America, EMEA, and APAC to evaluate and explore the need for better visibility to improve network security. Survey participants included decision-makers in full-time roles from practitioner to executive with responsibility for networking, infrastructure, IT, security and compliance. Questions provided to the participants asked about the current state of their organizations' security investments, challenges that impact their network visibility and team structure, and the benefits (if any) that they seek from having a more visible and integrated approach to security. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in March 2022 and was completed in May 2022.

Appendix B: Demographics

COMPANY SIZE	
15,000 or more employees	**4%**
8,000 to 14,999 employees	**9%**
5,000 to 7,999 employees	**23%**
2,000 to 4,999 employees	**28%**
1,000 to 1,999 employees	**36%**

ROLE (WITHIN IT DEPARTMENT)	
Cybersecurity	**26%**
Cloud architecture/orchestration	**22%**
NetOps	**16%**
SecOps	**13%**
DevOps	**12%**
Threat management	**10%**

RESPONDENT LEVEL	
Full-time practitioner	**3%**
Manager	**54%**
Director	**31%**
Vice president	**7%**
C-Level executive	**5%**

COUNTRY	
United States	**35%**
Canada	**15%**
France	**9%**
United Kingdom	**9%**
Germany	**8%**
China	**7%**
Japan	**7%**
India	**5%**
Australia	**2%**
New Zealand	**4%**

INDUSTRY	
Consumer product goods and/or manufacturing	**11%**
Business or professional services	**11%**
Retail	**10%**
Healthcare	**9%**
Financial services and/or insurance	**9%**
Manufacturing and materials	**8%**
Chemicals and/or metals	**7%**

FORRESTER®