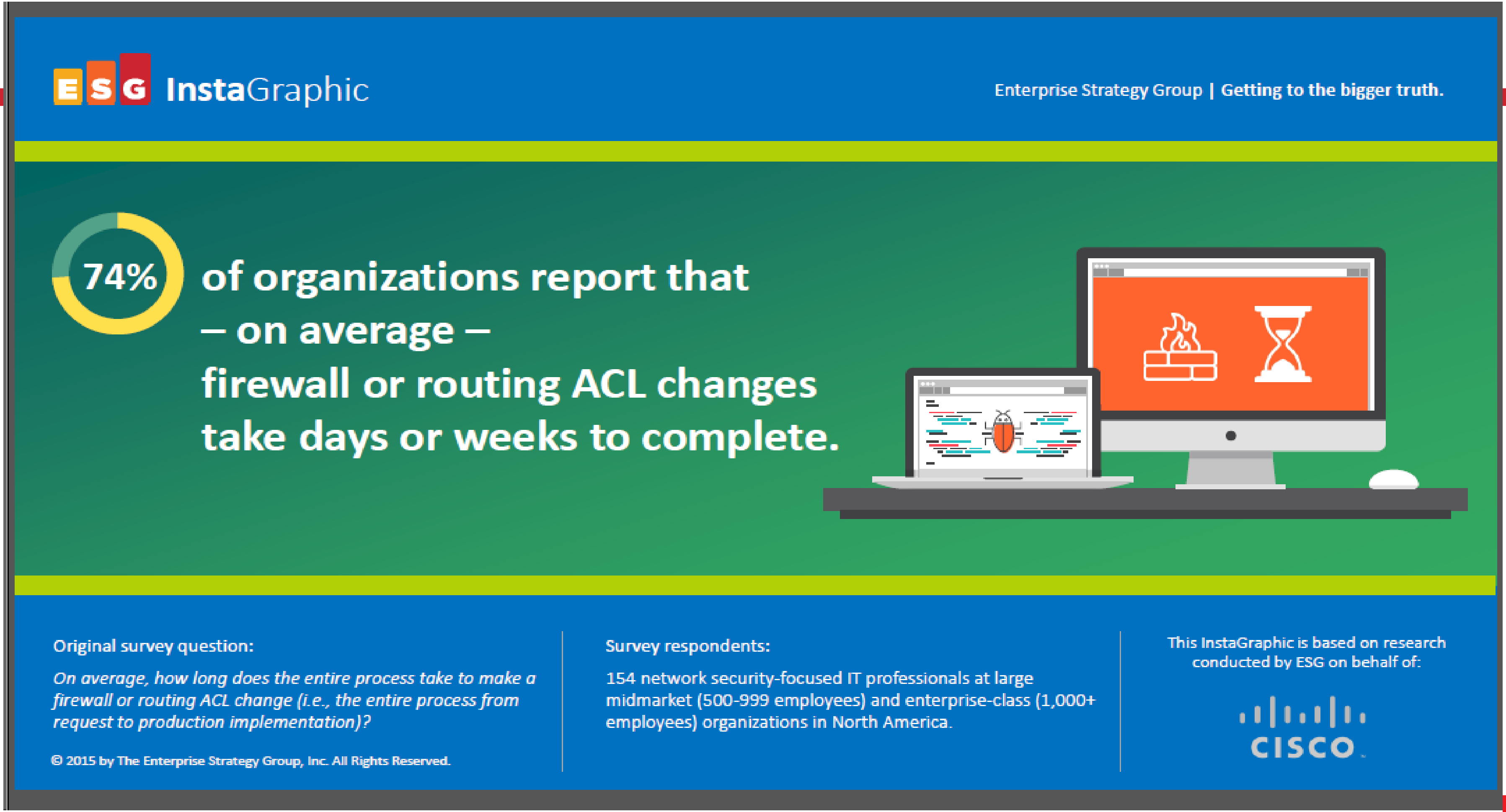
Enterprise Strategy Group | **Getting to the bigger truth.**™

Cisco: ACL Survey

Final Results

Jon Oltsik, Senior Principal Analyst

Summary of Key Findings



ESG InstaGraphic

Enterprise Strategy Group | Getting to the bigger truth.

74% of organizations report that – on average – firewall or routing ACL changes take days or weeks to complete.

Original survey question:

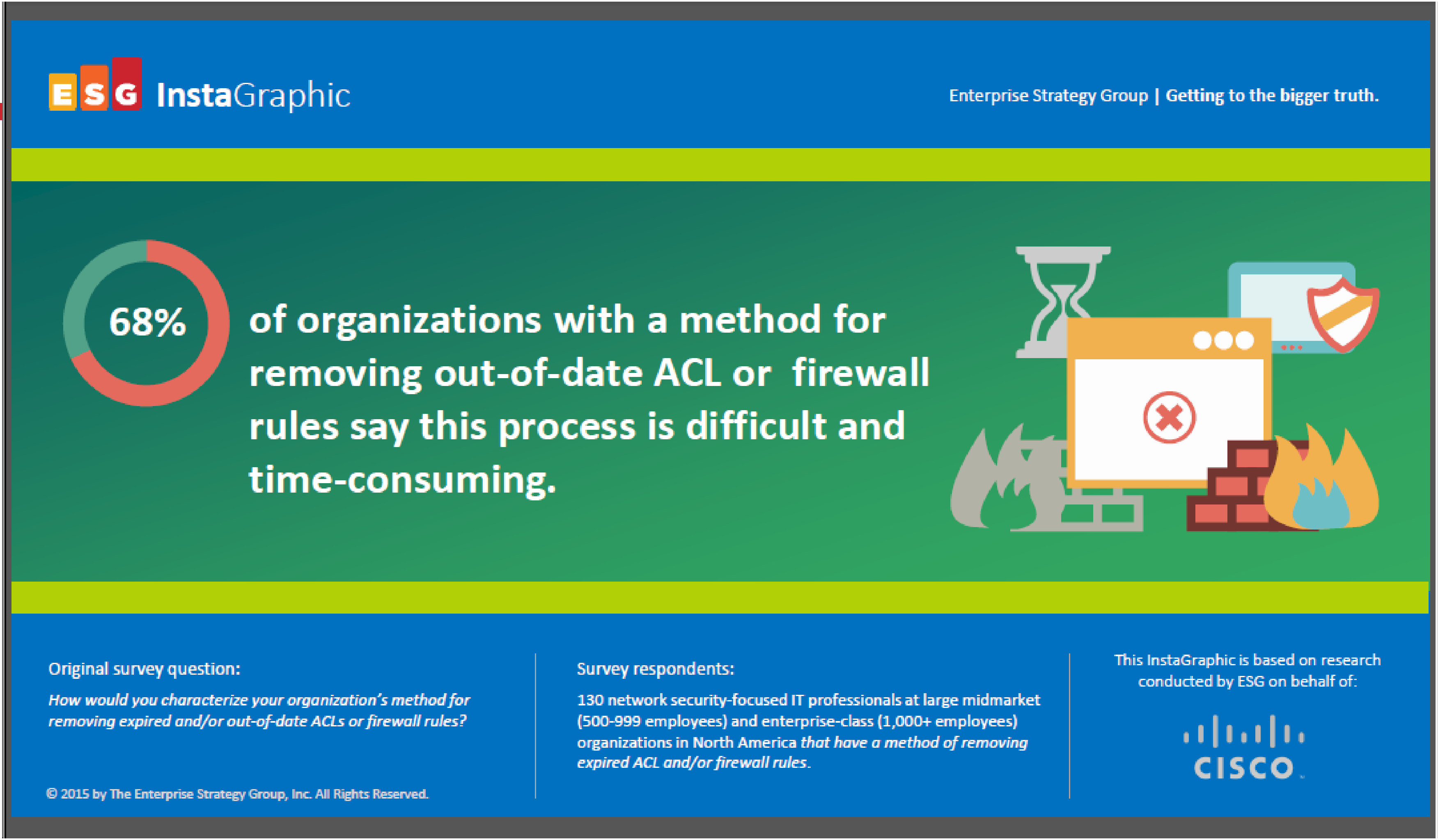
On average, how long does the entire process take to make a firewall or routing ACL change (i.e., the entire process from request to production implementation)?

Survey respondents:

154 network security-focused IT professionals at large midmarket (500-999 employees) and enterprise-class (1,000+ employees) organizations in North America.

This InstaGraphic is based on research conducted by ESG on behalf of:

CISCO



ESG InstaGraphic

Enterprise Strategy Group | Getting to the bigger truth.

68% of organizations with a method for removing out-of-date ACL or firewall rules say this process is difficult and time-consuming.

Original survey question:

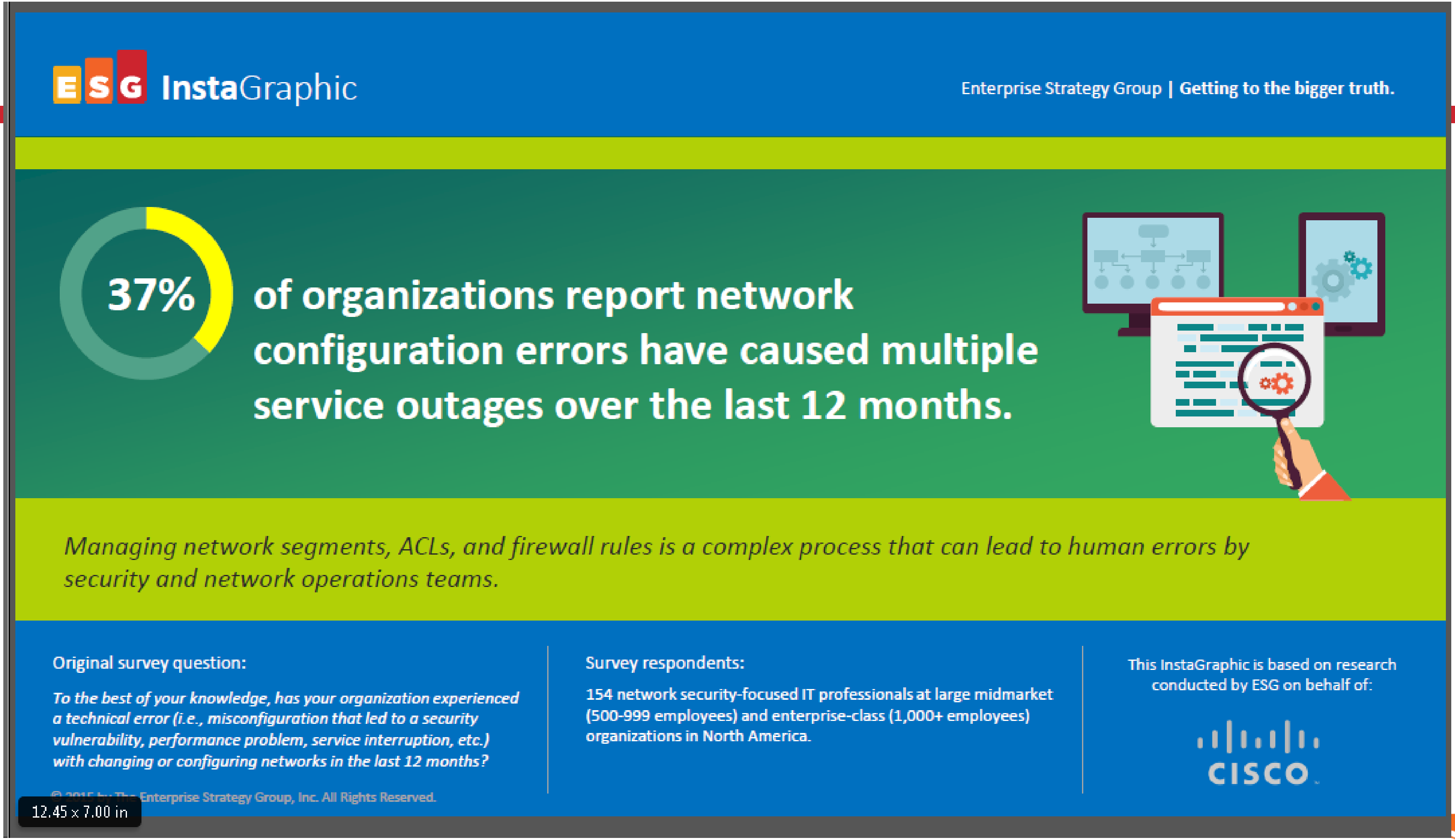
How would you characterize your organization's method for removing expired and/or out-of-date ACLs or firewall rules?

Survey respondents:

130 network security-focused IT professionals at large midmarket (500-999 employees) and enterprise-class (1,000+ employees) organizations in North America *that have a method of removing expired ACL and/or firewall rules*.

This InstaGraphic is based on research conducted by ESG on behalf of:

CISCO



ESG InstaGraphic

Enterprise Strategy Group | Getting to the bigger truth.

37% of organizations report network configuration errors have caused multiple service outages over the last 12 months.

Managing network segments, ACLs, and firewall rules is a complex process that can lead to human errors by security and network operations teams.

Original survey question:

To the best of your knowledge, has your organization experienced a technical error (i.e., misconfiguration that led to a security vulnerability, performance problem, service interruption, etc.) with changing or configuring networks in the last 12 months?

Survey respondents:

154 network security-focused IT professionals at large midmarket (500-999 employees) and enterprise-class (1,000+ employees) organizations in North America.

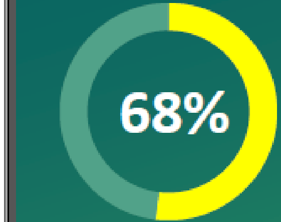
This InstaGraphic is based on research conducted by ESG on behalf of:

CISCO

12.45 x 7.00 in

ESG InstaGraphic

Enterprise Strategy Group | Getting to the bigger truth.



68% of organizations that have suffered lateral data center server attacks have confidence that additional network segmentation could <u>definitely</u> prevent future compromises.

This validates that granular network segmentation can be used as a threat prevention best practice.

Original survey question:

In your opinion, could some degree of further network segmentation (i.e., segmenting servers with specific additional security policies) help prevent a server compromise in your organization's data center?

Survey respondents:

154 network security-focused IT professionals at large midmarket (500-999 employees) and enterprise-class (1,000+ employees) organizations in North America.

This InstaGraphic is based on research conducted by ESG on behalf of:

CISCO

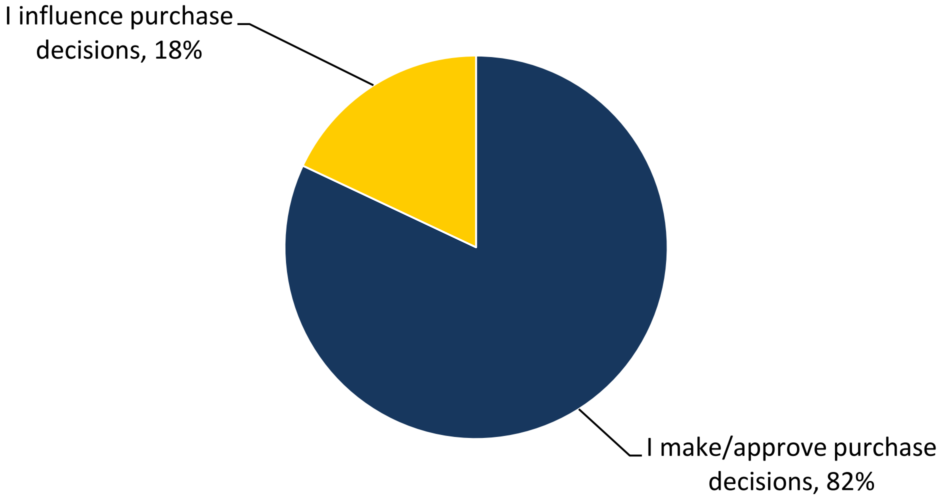
Project Overview

- 154 completed online surveys with IT/security professionals responsible for network security requirements and operations
  - All respondent organizations had to be using physical firewalls or virtual firewalls and access control lists (ACLs)
  - All respondent organizations had to have at least 1 data center operated worldwide
- Large midmarket organizations (defined as organizations with 500 to 999 employees) and enterprise organizations (defined as organizations with 1,000 employees or more) in North America
- Multiple industry verticals including financial, business services, manufacturing and retail

Demographics

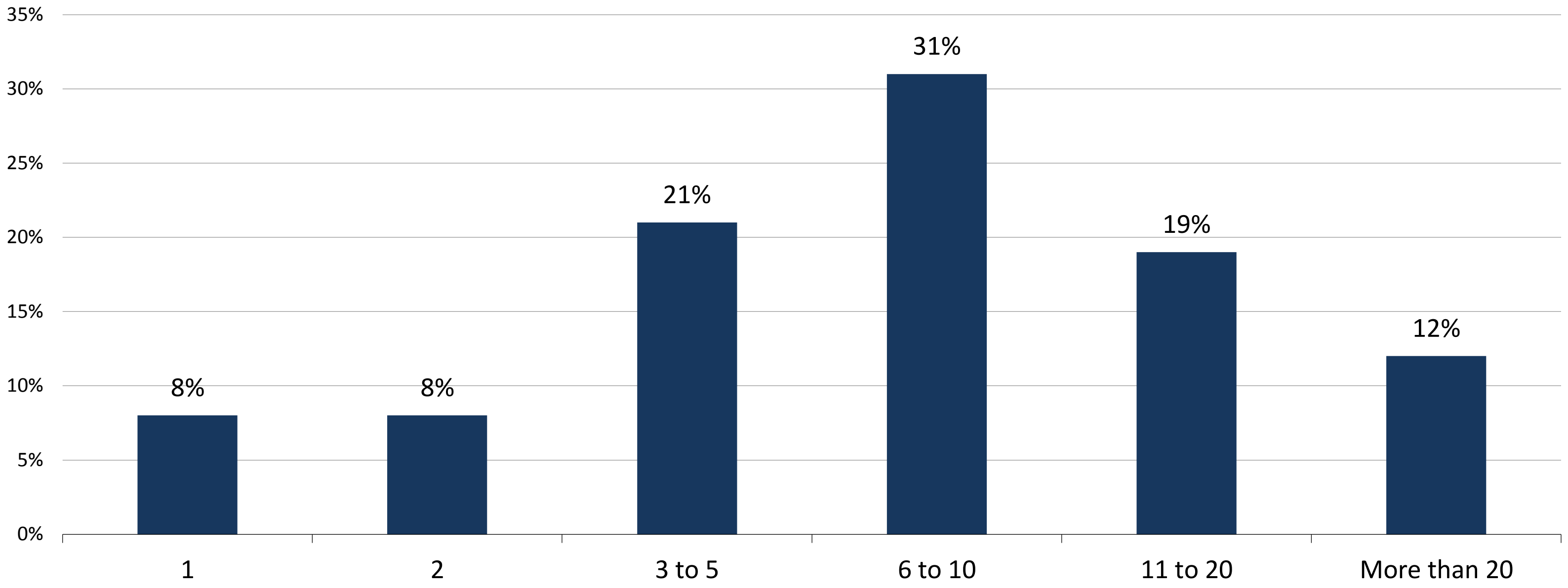
Respondents' Purchasing Influence for Network Security Technology Products and Services

To what degree are you responsible for making purchase decisions related to network security technology products and services? (Percent of respondents, N=154)



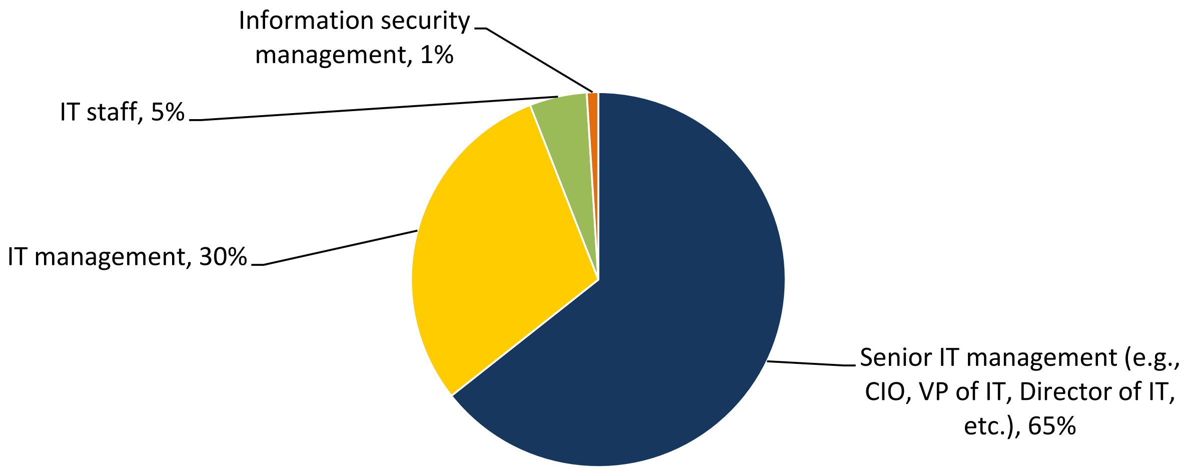
Number of Data Centers Worldwide

How many data centers does your organization operate worldwide? (Percent of respondents, N=154)



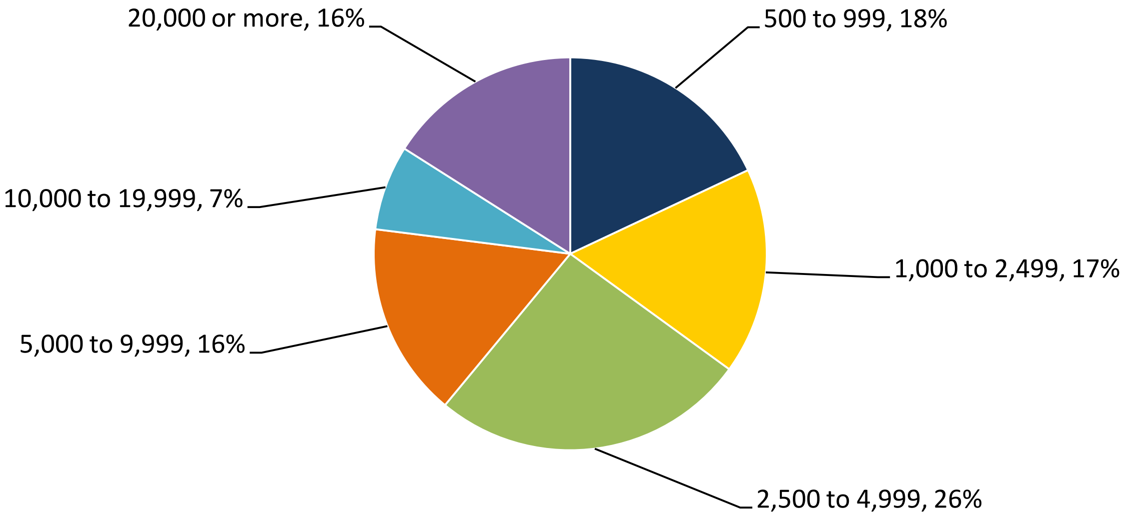
Respondents’ Current Job Responsibility

Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=154)



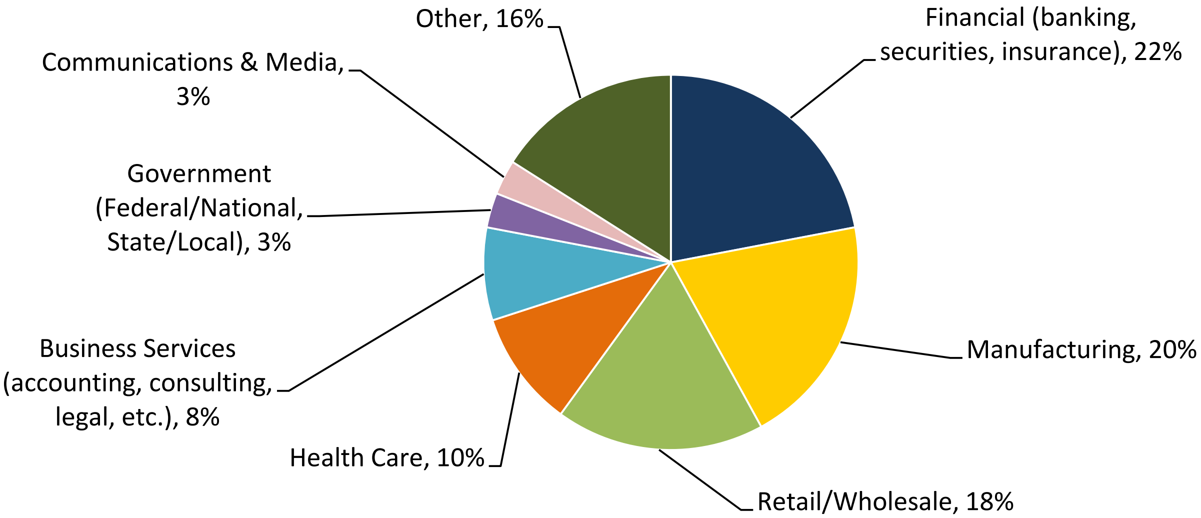
Respondents by Total Number of Employees Worldwide

How many total employees does your organization have worldwide? (Percent of respondents, N=154)



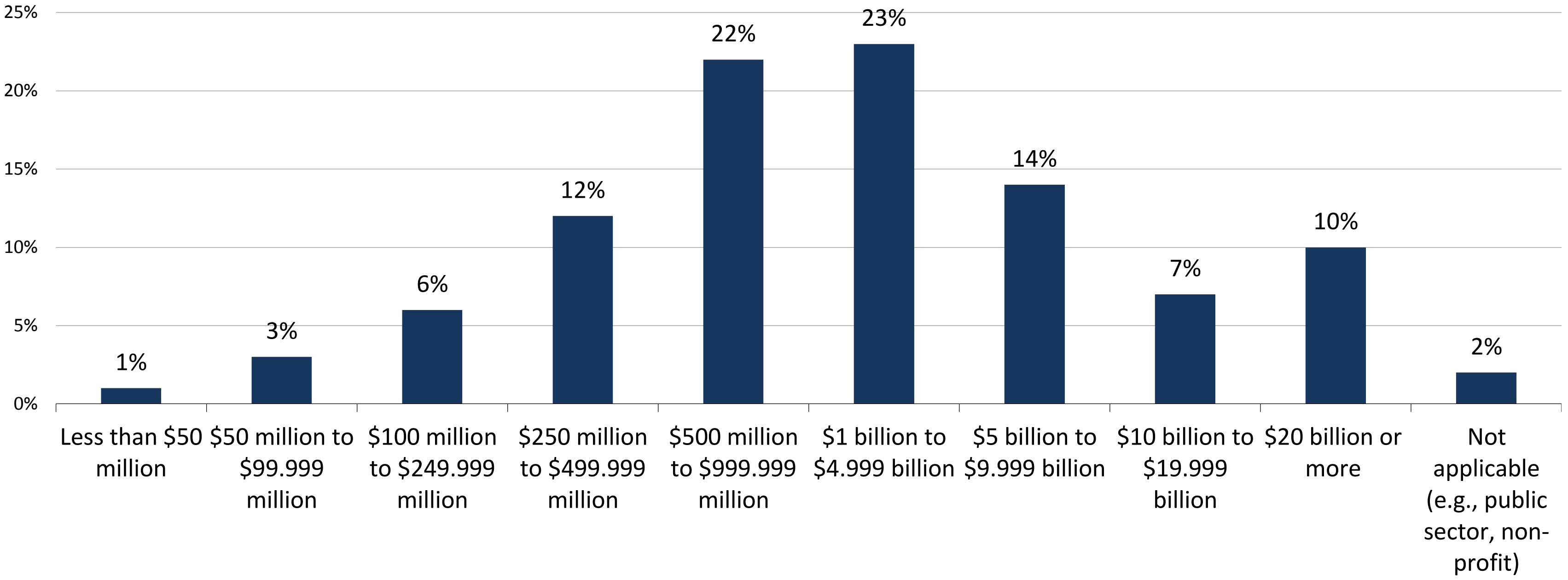
Respondents by Primary Industry

What is your organization's primary industry? (Percent of respondents, N=154)



Respondents by Annual Revenue

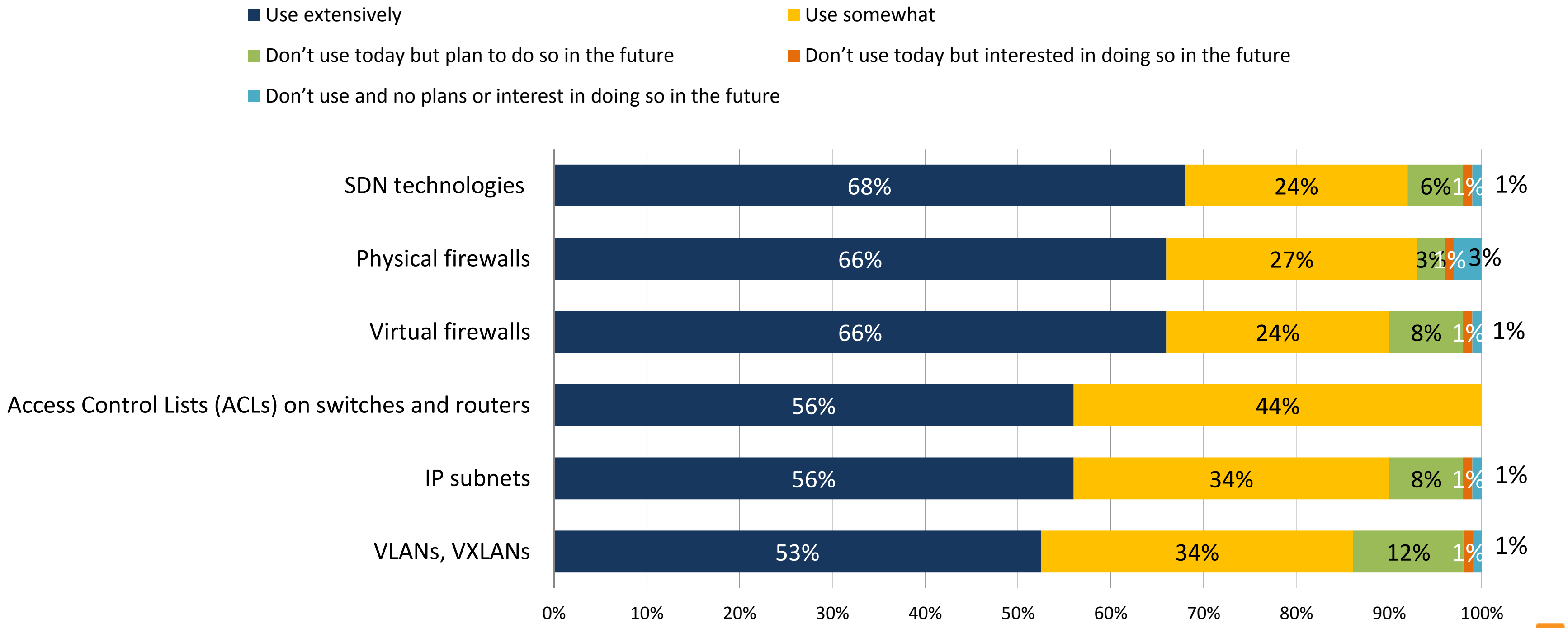
What is your organization’s total annual revenue ($US)? (Percent of respondents, N=154)



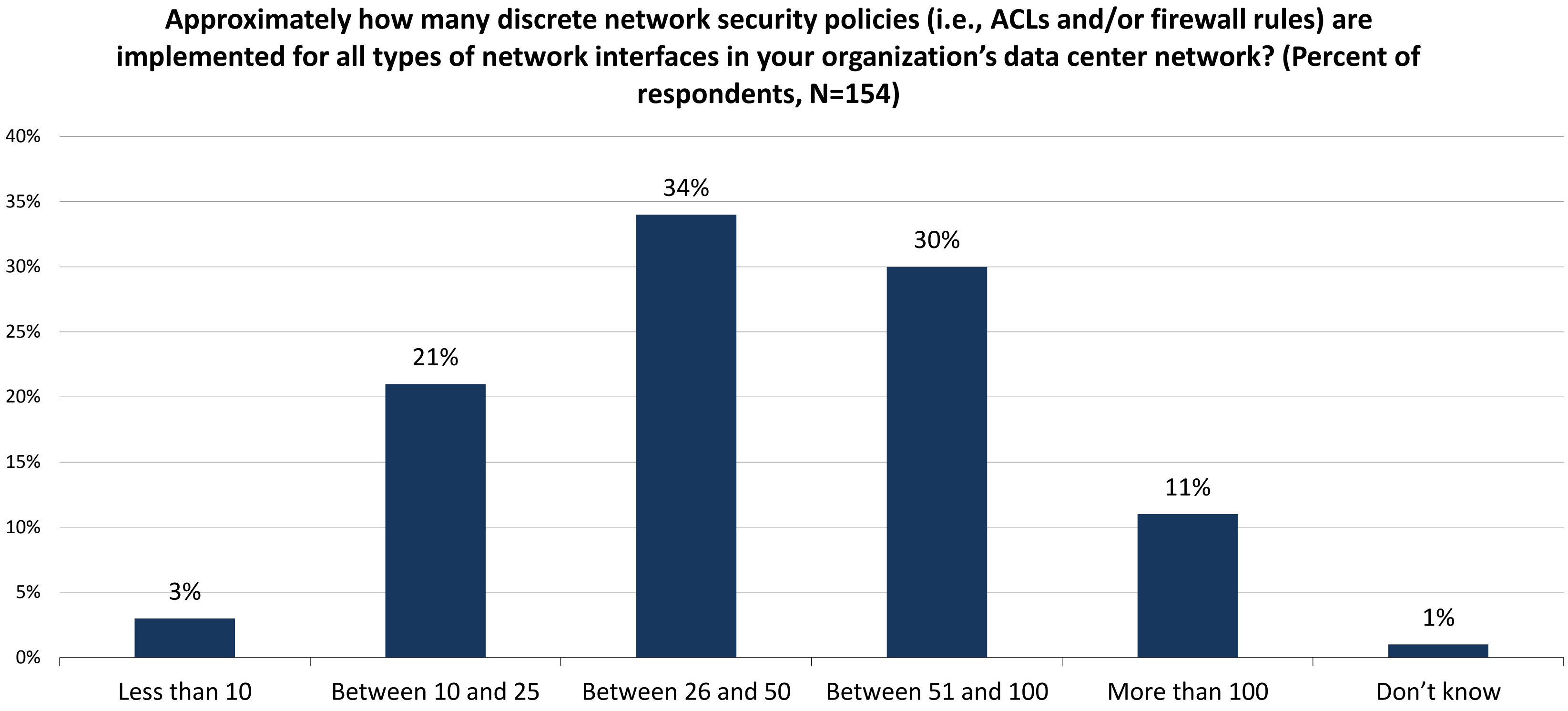
ACL/ACI

Technologies Used to Segment Data Center Networks

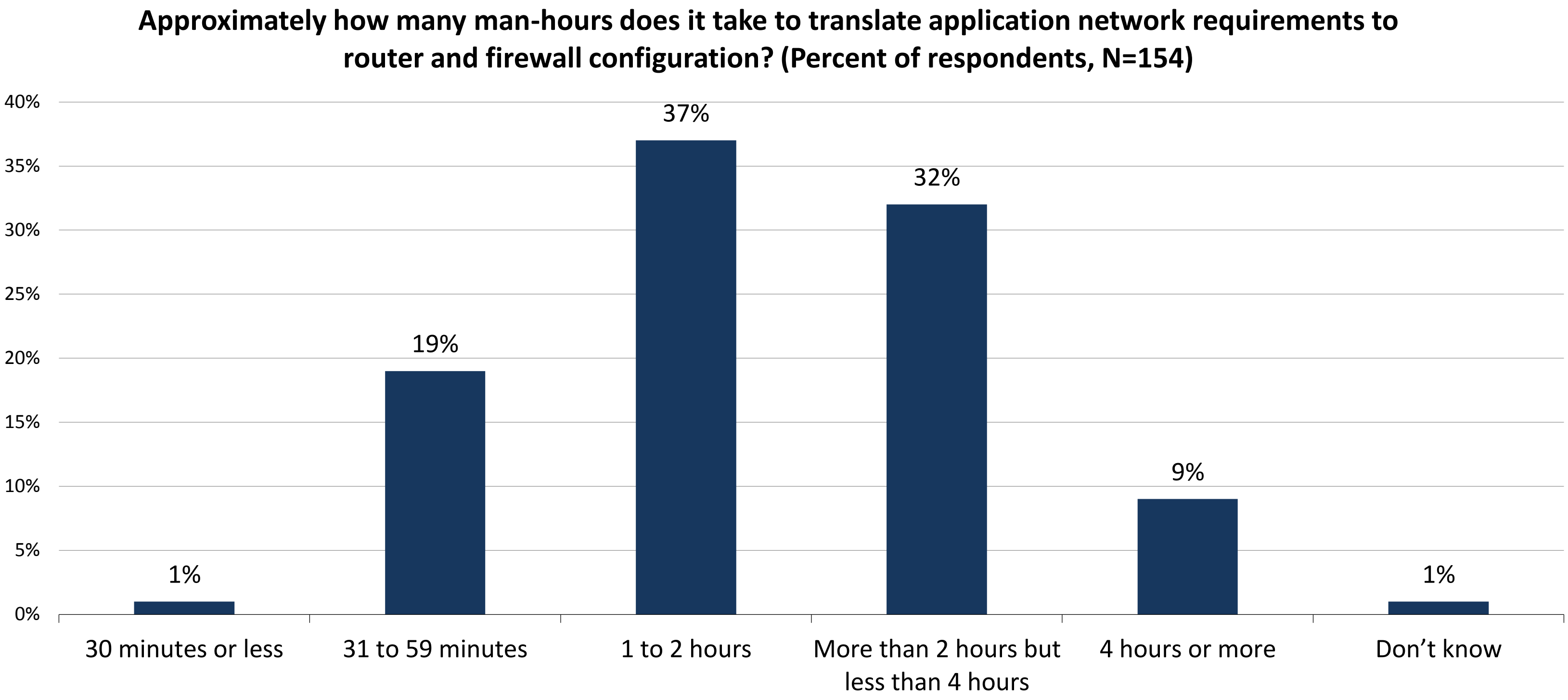
Which of the following does your organization use to segment its data center networks? (Percent of respondents, N=154)



Approximate Number of Discrete Network Security Policies Implemented for Network Interfaces in Organization’s Data Center Network

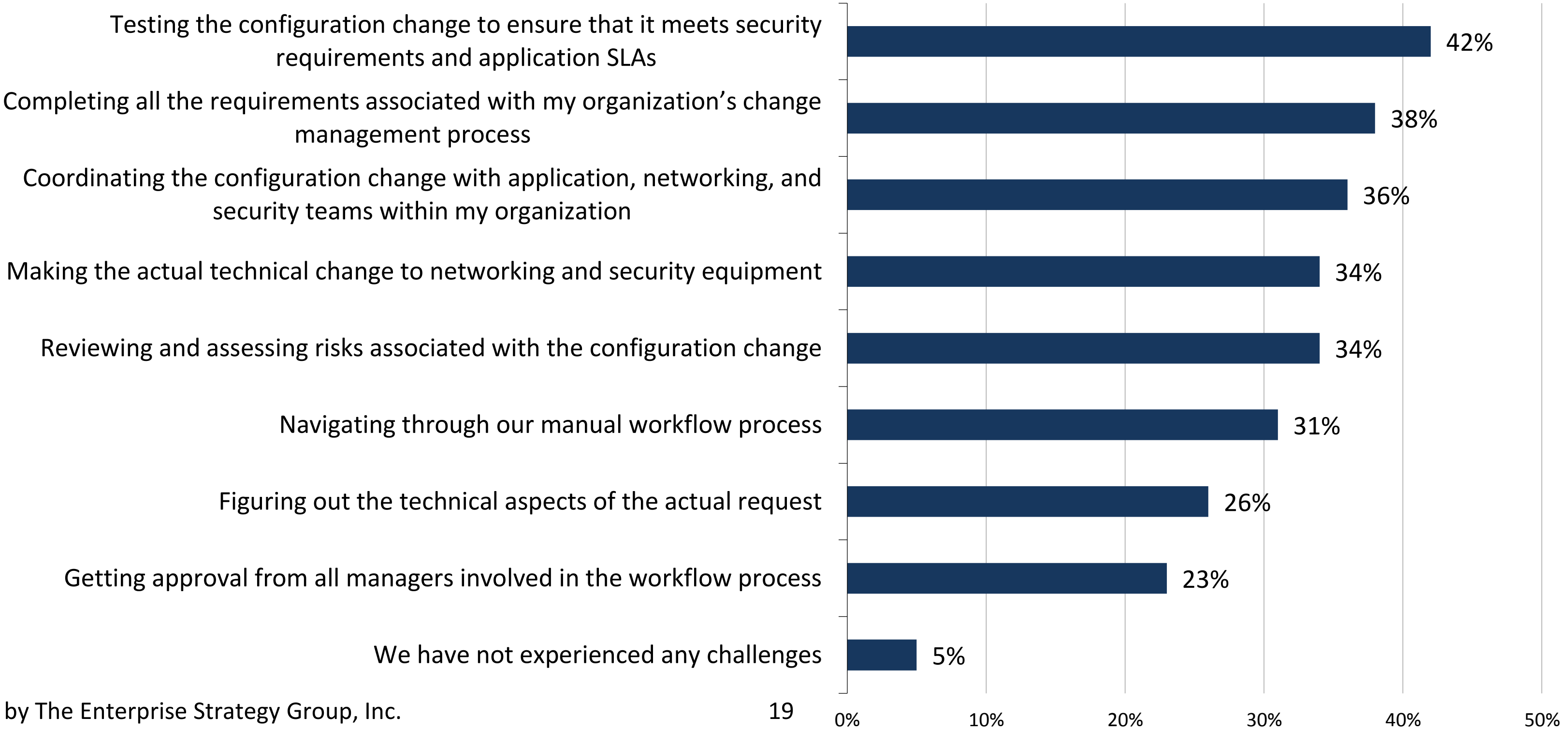


Approximate Number of Man-Hours Needed to Translate Application Network Requirements to Router and Firewall Configuration



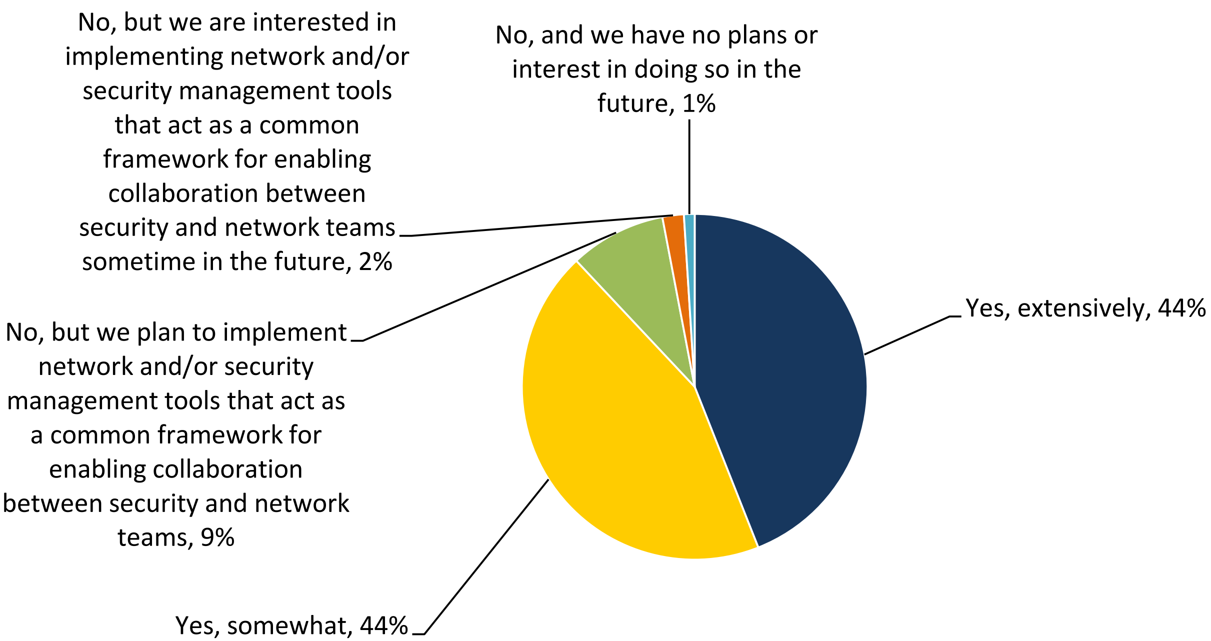
Challenges with Applying an Application Network Requirement to a Router and/or Firewall Configuration

Which of the following present the biggest challenges associated with applying an application network requirement to a router and/or firewall configuration for network security policy enforcement? (Percent of respondents, N=154, three responses accepted)



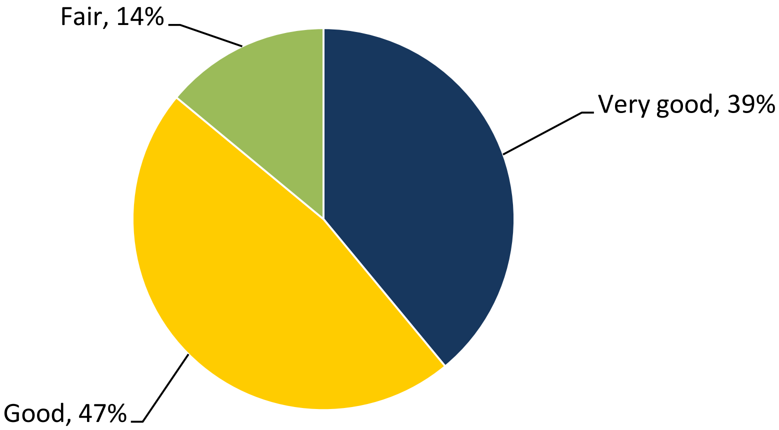
Use of Network and/or Security Management Tools Enabling Collaboration Between Teams

Does your organization employ any network and/or security management tools that act as a common framework for enabling collaboration between security and network teams? (Percent of respondents, N=154)



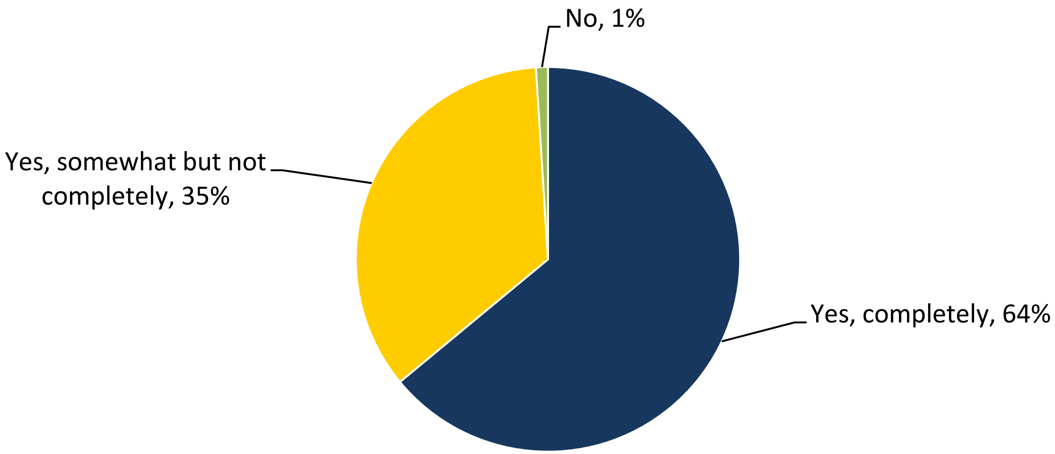
Organizations Rate the Effectiveness of Network and/or Security Management Tools

You stated that your organization employs network and/or security management tools that act as a common framework for enabling collaboration between security and network teams. How would you rate the effectiveness of these tools (i.e., integration, workflow, policy management, change management, monitoring, reporting, etc.)? (Percent of respondents, N=136)



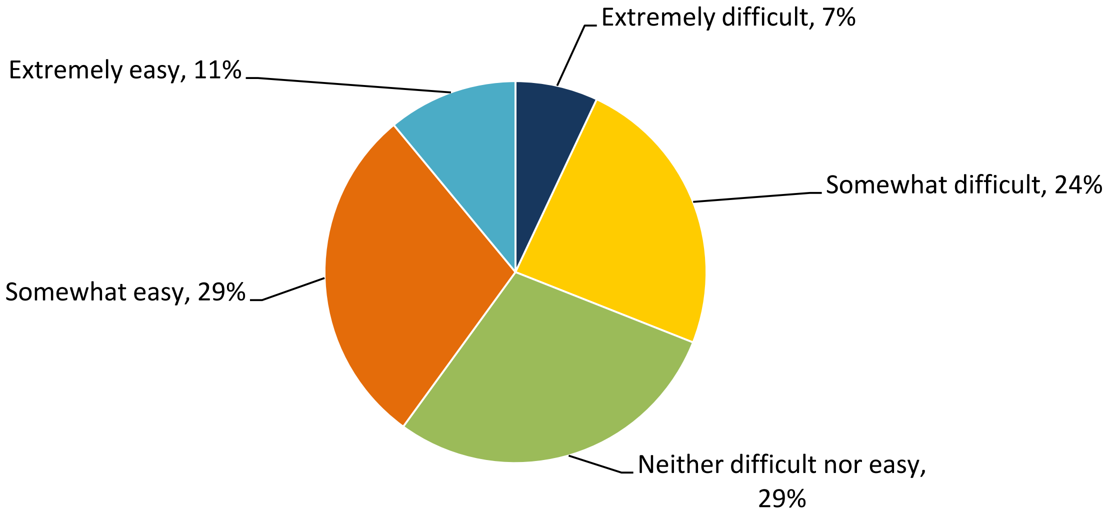
Can Security Team Look at Data Center ACL and Understand the Applications and Services to Which it Refers?

Is your organization's security team able to look at a data center ACL and readily understand the applications and services it refers to? (Percent of respondents, N=154)



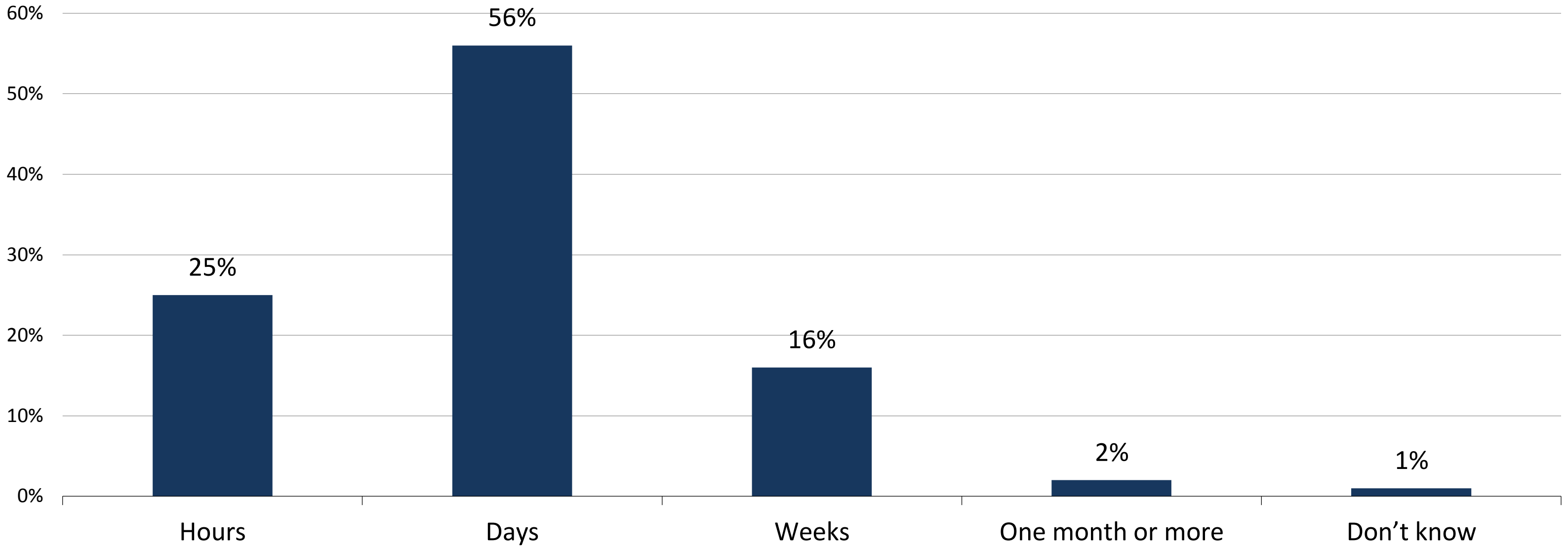
Difficulty of Understanding the Relationships Between ACLs and Specific Applications with Which Each ACL Aligns

How difficult would it be to review ACLs and understand the relationships between ACLs and the specific applications/services with which each ACL aligns? (Percent of respondents, N=152)



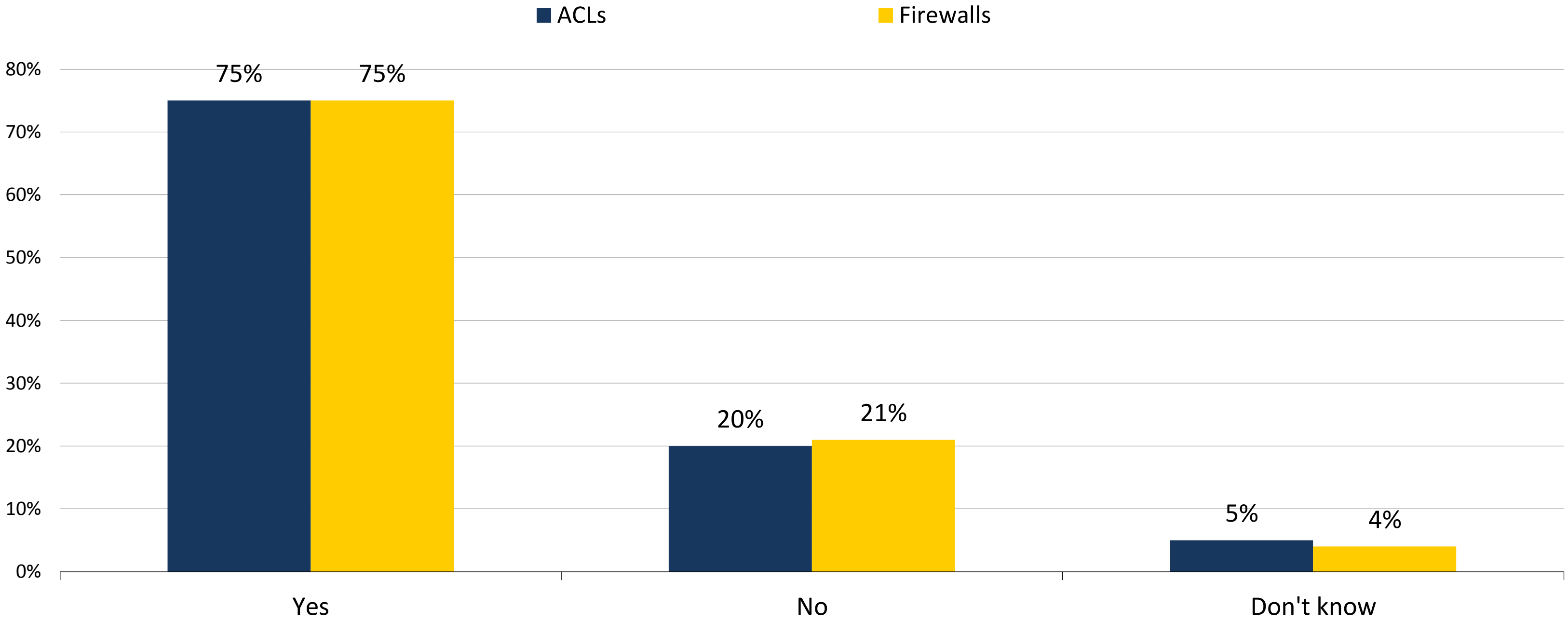
Time it Takes to Make a Firewall or Routing ACL Change

On average, how long does the entire process take to make a firewall or routing ACL change (i.e., the entire process from request to production implementation)? (Percent of respondents, N=154)



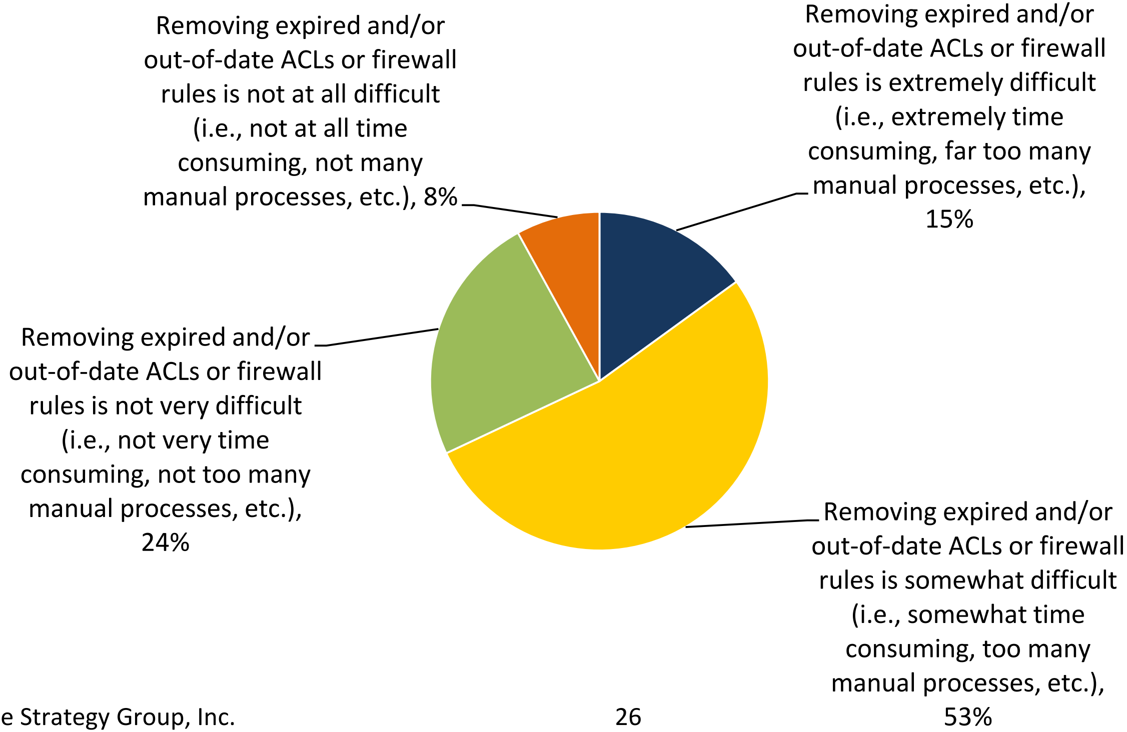
Method in Place for Removing Expired and/or Out-of-date ACLs or Firewall Rules

Does your organization have a method for removing expired and/or out-of-date ACLs or firewall rules? (Percent of respondents, N=154)



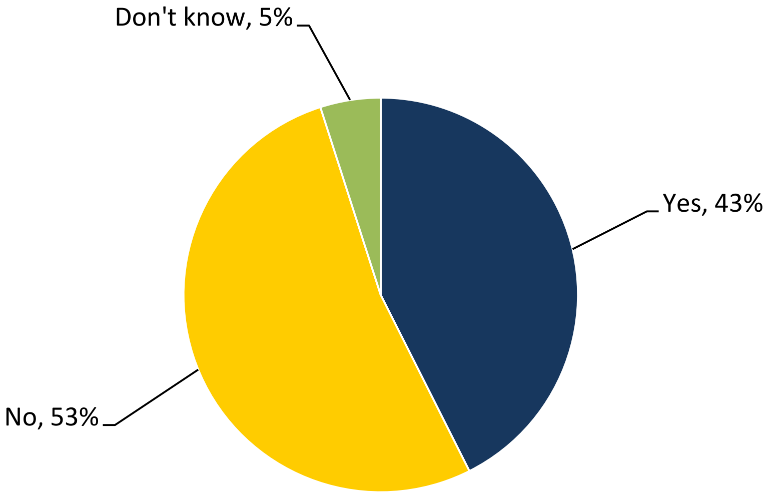
Respondents Rate Method of Removing Expired and/or Out-of-date ACLs or Firewall Rules

How would you characterize your organization’s method for removing expired and/or out-of-date ACLs or firewall rules? (Percent of respondents, N=130)



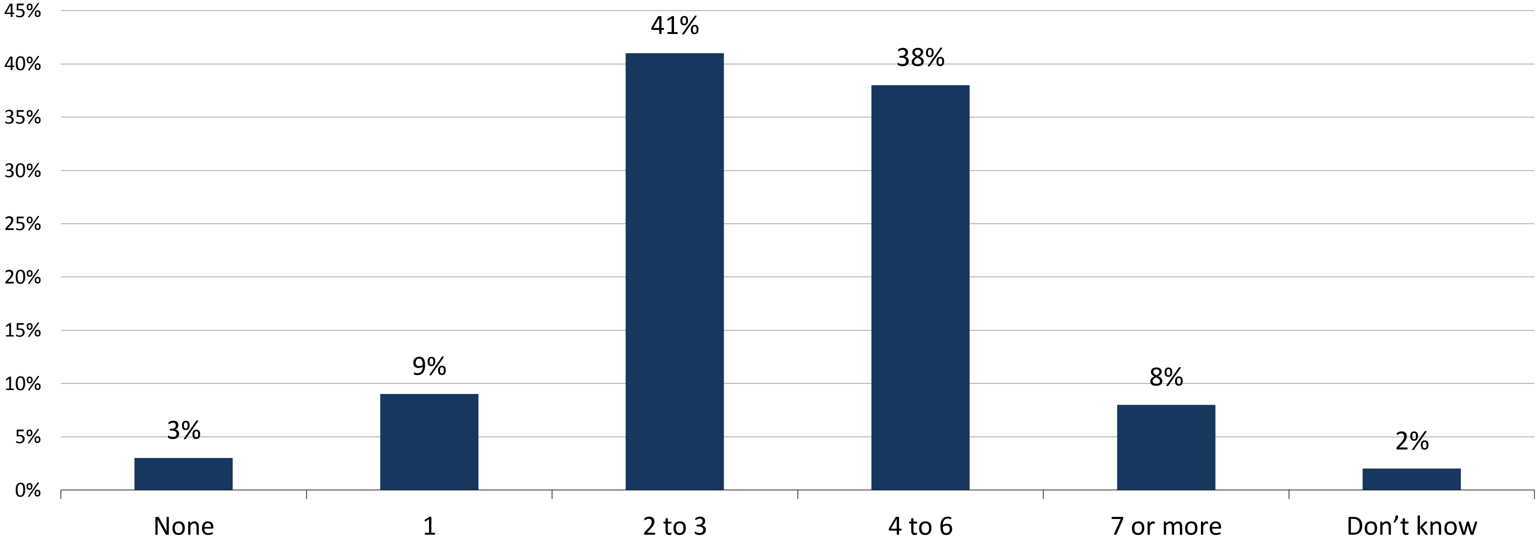
Have Organizations Experienced a Technical Error with Changing or Configuring Networks in the Last 12 Months?

To the best of your knowledge, has your organization experienced a technical error (i.e., mis-configuration that led to a security vulnerability, performance problem, service interruption, etc.) with changing or configuring networks in the last 12 months? (Percent of respondents, N=154)



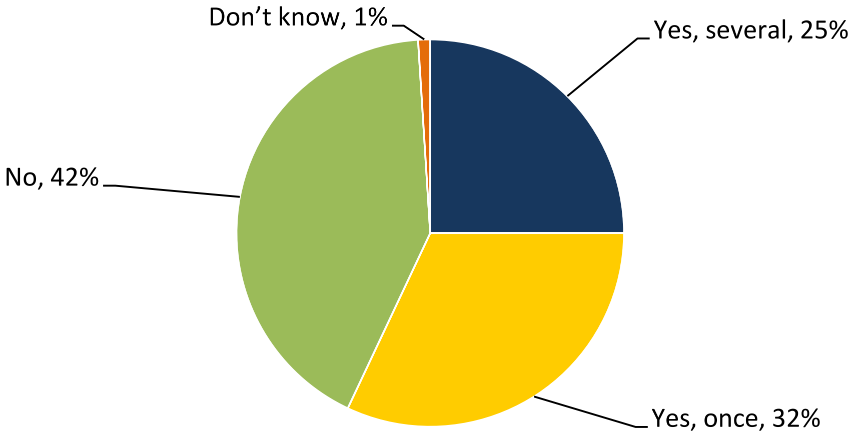
Approximate Number of Outages Due to Technical Error with Changing or Configuring Networks in the Last 12 Months

In the past 12 months, approximately how many outages would you estimate occurred within your organization as a result of an error or multiple errors in making network changes or configurations? (Percent of respondents, N=66)



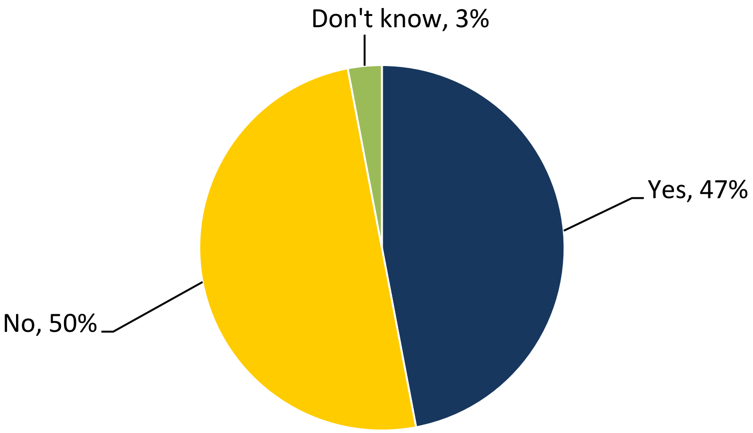
Have Organizations Experienced a Security Incident that Resulted in the Compromise of One or More Data Center Services in the Past 2 Years?

Has your organization experienced a security incident that resulted in the compromise of one or more data center servers in the past 2 years? (Percent of respondents, N=154)



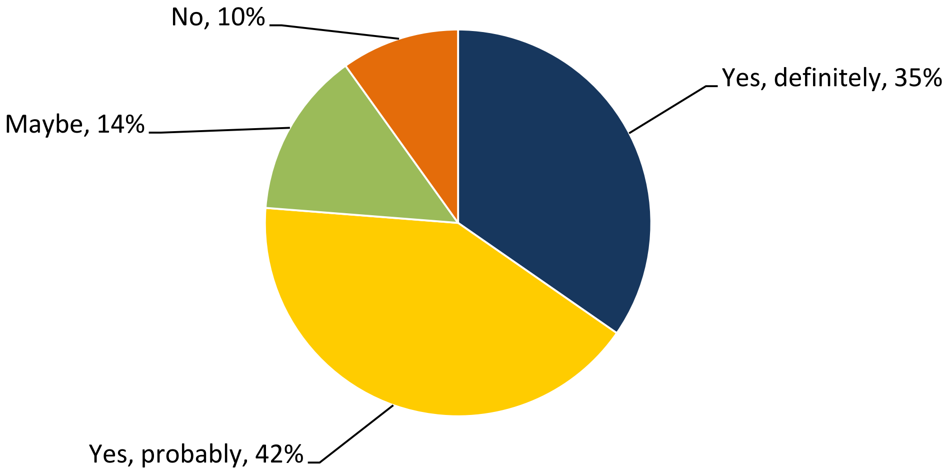
Was the Attacker Able to Move Laterally From One Data Center Server to Another?

Has your organization experienced a data center network compromise where the attacker was able to move laterally from one data center server to another? (Percent of respondents, N=88)



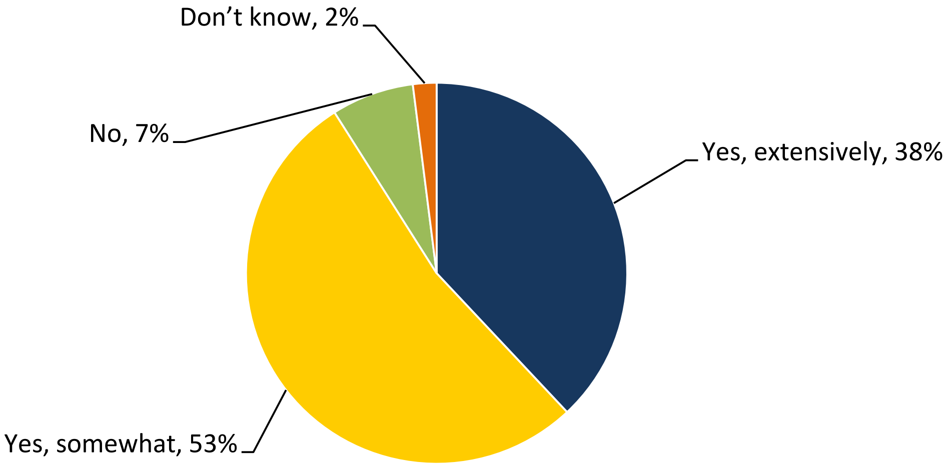
Could Some Degree of Further Network Segmentation Help Prevent a Server Compromise?

In your opinion, could some degree of further network segmentation (i.e., segmenting servers with specific additional security policies) help prevent a server compromise in your organization's data center? (Percent of respondents, N=154)



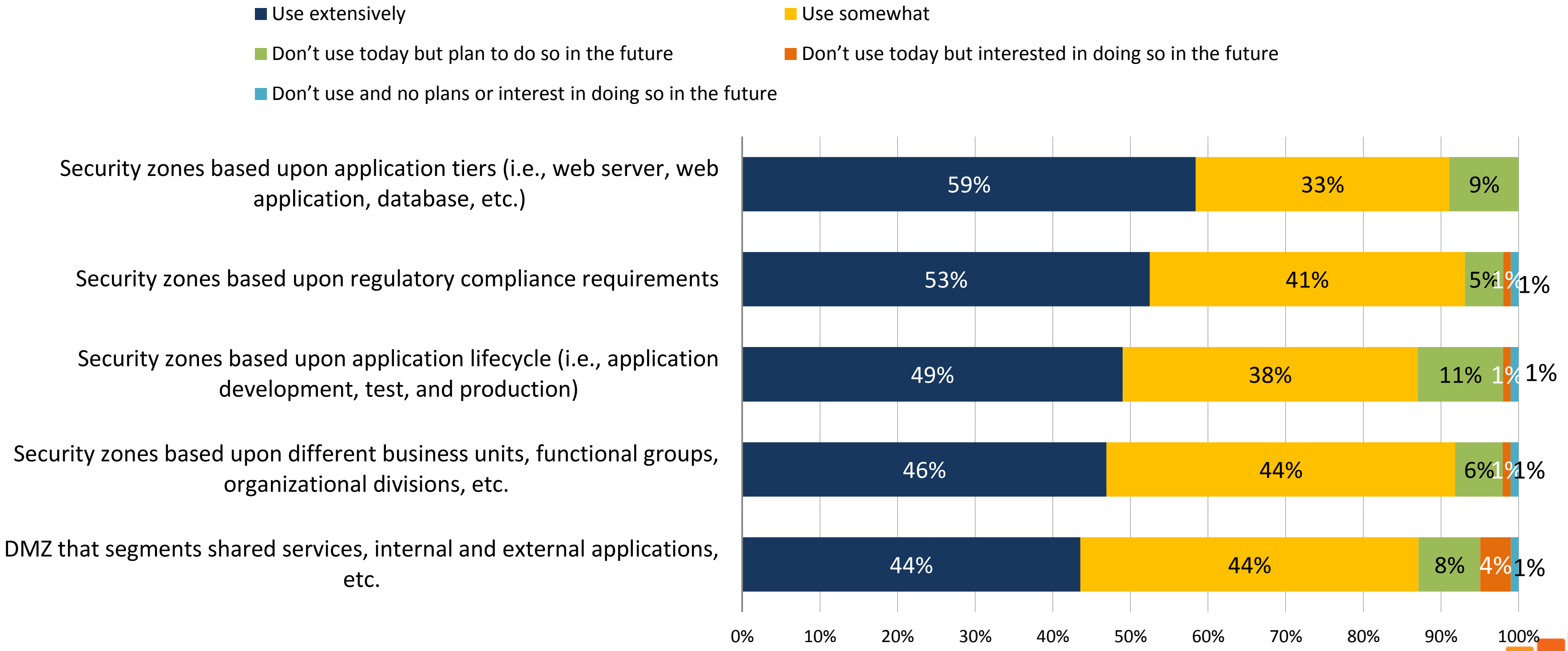
Use of Security Zones to Segment and Protect Data Center

Does your organization set up security zones to segment and protect its data center servers? (Percent of respondents, N=154)



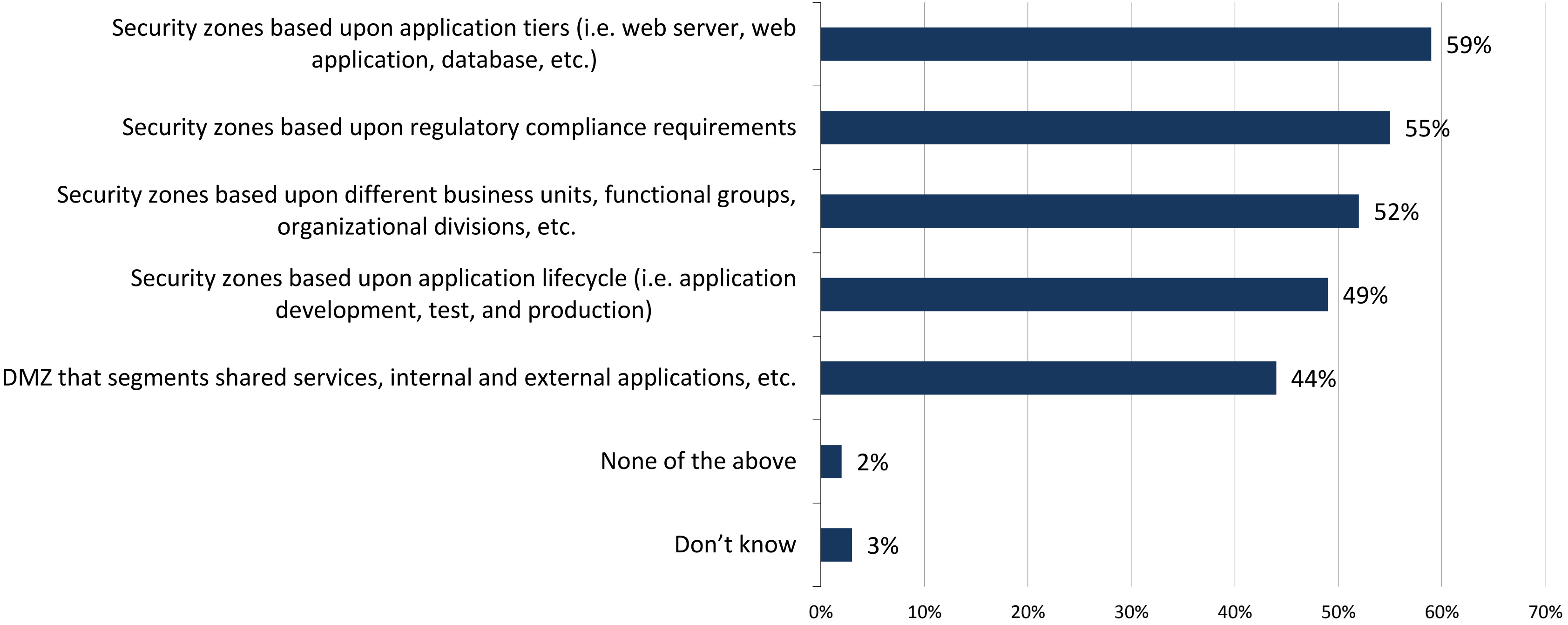
Types of Security Zones Employed

You indicated that your organization sets up security zones to segment and protect its data center servers. Which of the following types of security zones does your organization employ? (Percent of respondents, N=140)



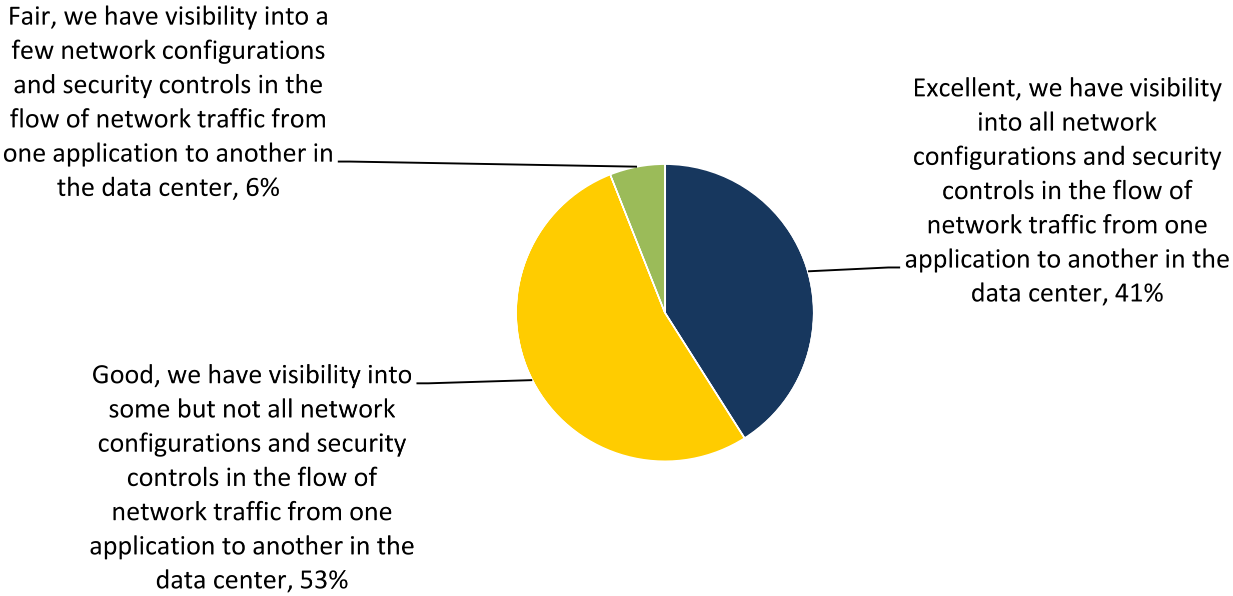
Types of Security Zones that Would be Used More Regularly if Organizations Could Set Up Security Zones More Quickly

In an ideal situation where your organization could set up security zones more quickly and easily, which of the following types of security zones, if any, would you use more regularly? (Percent of respondents, N=154, multiple responses accepted)



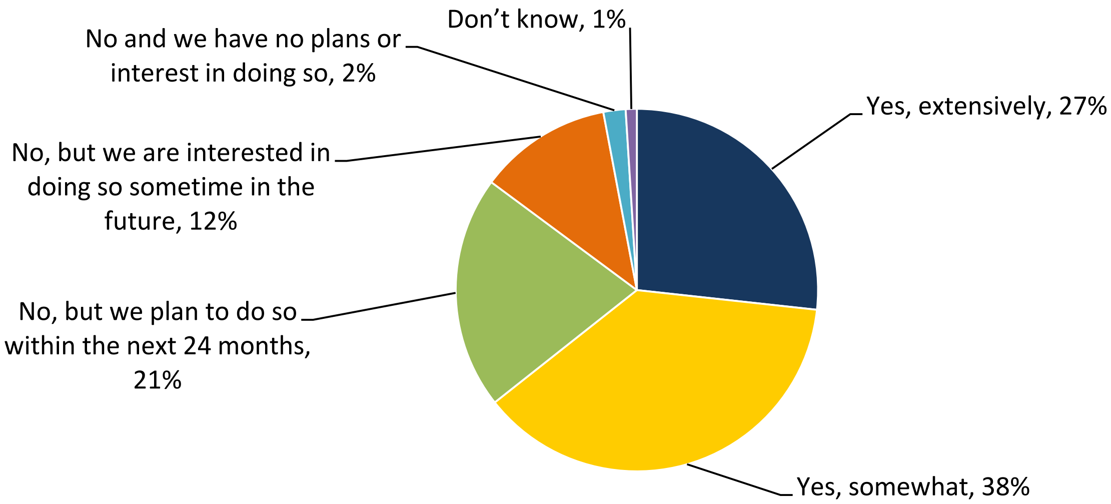
Respondents Rate Organization's Network Visibility into its Application Inter-dependencies

How would you rate your organization's network visibility into its application inter-dependencies (i.e., network configuration and network security controls involved in the flow of network traffic from one application to another in the data center)? (Percent of respondents, N=154)



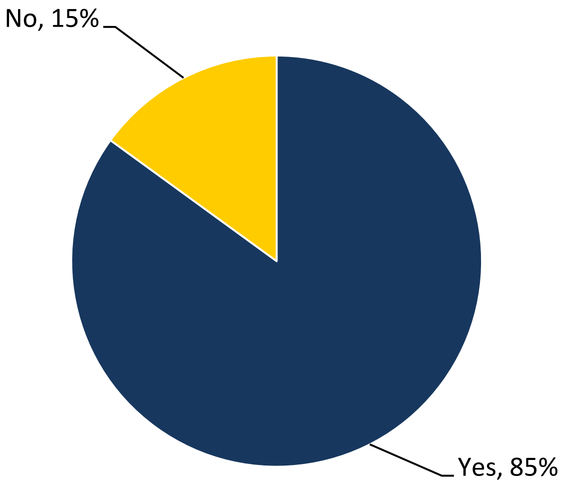
Adoption of IPV6 in the Data Center Network

Has your organization adopted IPV6 in its data center network? (Percent of respondents, N=154)



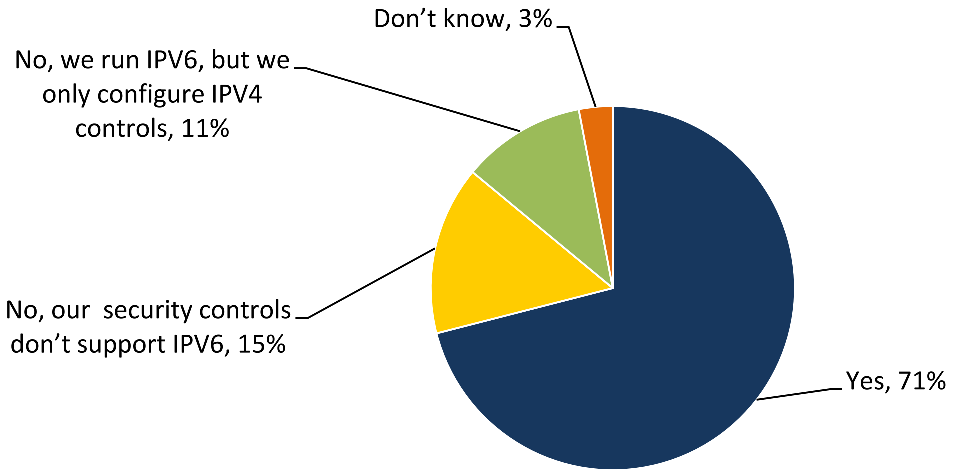
IPV6-Ready Security Controls in the Data Center

Does your organization have IPV6-ready security controls in its data center? (Percent of respondents, N=99)



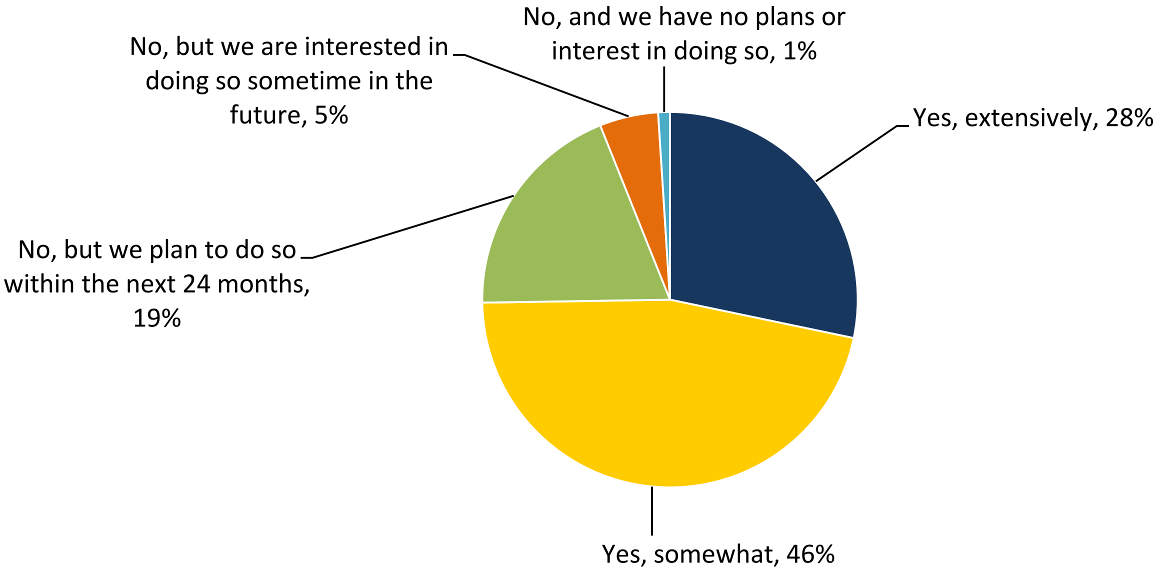
Are Security Controls for IPV4 also Controlling IPV6?

Are your organization’s security controls for IPV4 also controlling IPV6? (Percent of respondents, N=99)



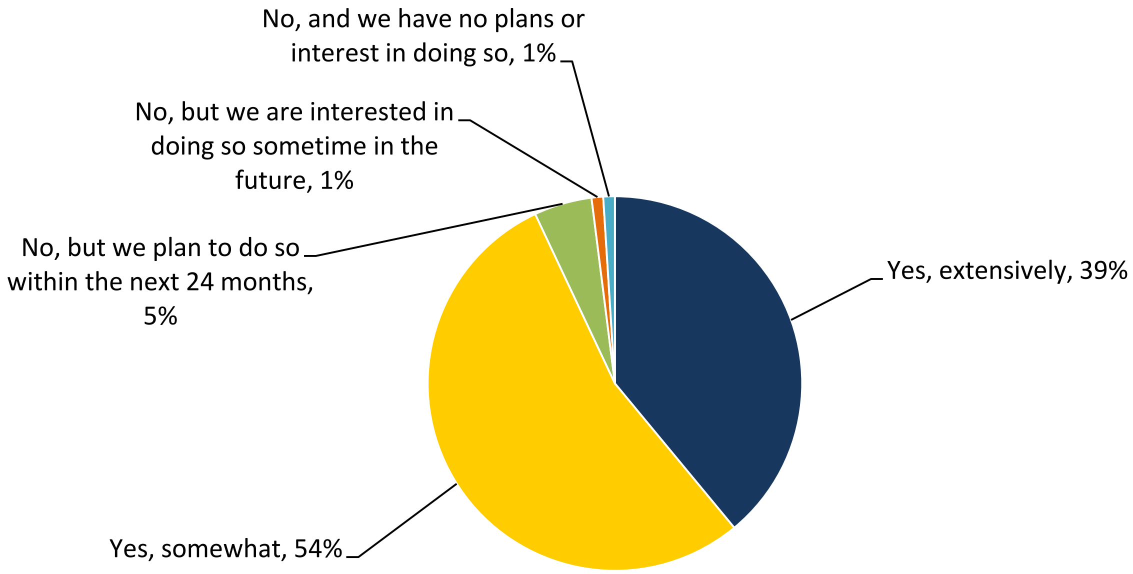
Use of Automation and Orchestration Tools to Accelerate Application Deployment in the Data Center

Many organizations are employing automation and orchestration tools to help them accelerate application deployment in the data center. Has your organization implemented these types of tools? (Percent of respondents, N=154)



Can Organization Automate the Provisioning of Networking Resources and Security Services based on Pre-defined Application Service Level Policies?

Can your organization automate the provisioning of networking resources and security services based on pre-defined application service level policies? (Percent of respondents, N=114)



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

Thank You.

Please contact us for more information

Jon Oltsik, Senior Principal Analyst
Jon.Oltsik@esg-global.com
508.381.5166

@ESG_Global

www.facebook.com/ESGglobal

www.linkedin.com/company/enterprise-strategy-group

www.youtube.com/user/ESGglobal