Insight | Cloud + Data Center Transformation

MARKETPULSE RESEARCH

Cybersecurity at a Crossroads:

The Insight 2021 Report

IDG

Commissioned by Insight Enterprises | February 2021

Sample

Field work	This survey was fielded between November 23, 2020, and December 14, 2020.
Total respondents	213 qualified U.S. completes

Method and objectives

Data collection	Online questionnaire
Audience	Respondents were qualified as follows: • Director-level titles and higher • IT/networking- and/or data security-related job function • Employed at mid- to large-size enterprises (1,500 or more employees), representing a cross-section of vertical industries
Research objectives	This study was developed to understand how scaling a distributed IT environment and the transition to a work-from-home model during the pandemic impacted corporate security strategies, priorities, and initiatives. Specifically, the survey was designed to: • Measure confidence levels in current enterprise security posture and identify its relative strengths and roadblocks • Understand cybersecurity modernization priorities in response to the sudden work-from-home and distributed IT environments • Identify the specific cybersecurity projects initiated/executed • Understand the challenges faced by IT leaders as they fortify their security posture

Respondent profile

Job title

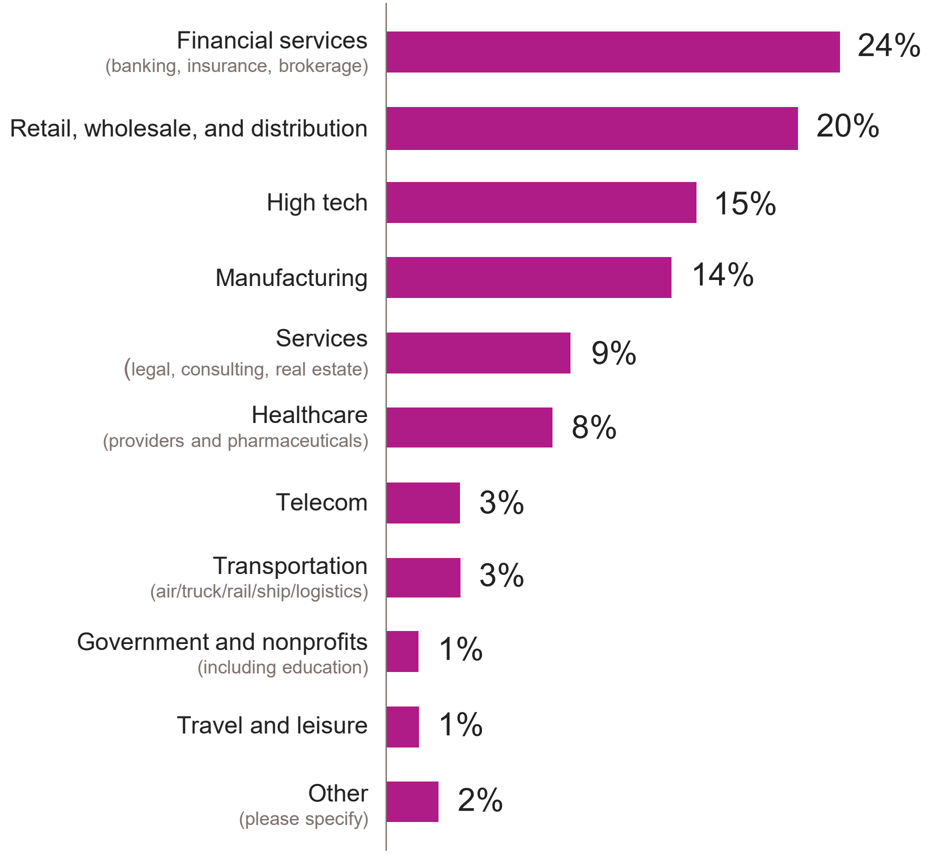
IT senior management	**68%**
CIO (Chief Information Officer) or top IT executive	37%
CTO (Chief Technology Officer) or equivalent	15%
VP IT/networking	16%
IT security management	**32%**
CSO, CISO, or top security executive	9%
VP IT security	6%
Director IT security	17%

All respondents are employed in an IT/networking and/or data security job function.

Number of employees

100,000 or more	6%
50,000–99,999	16%
30,000–49,999	7%
20,000–29,999	18%
10,000–19,999	7%
5,000–9,999	12%
2,500–4,999	16%
1,500–2,499	19%
Average	**21,300**

Primary industry



Results

Key findings

2020 RAISED THE CYBERSECURITY STAKES AS WELL AS BUDGETS

In 2020, the COVID-19 pandemic forced organizations to react quickly to the security needs of a remote workforce while also continuing to address the security considerations of today's increasingly distributed IT landscape in which data is generated on-premises, in the cloud, and on the edge. As a result, C-suite executives and board members began to take greater notice of their company's security posture, IT and security leaders accelerated security modernization projects, and cybersecurity budgets increased in a trend that will continue into 2021.

100% of respondents agreed that boards and executive teams are now more focused on the company's security posture than in the past, with 68% strongly agreeing and 32% moderately agreeing.

The vast majority agreed **that the distributed IT landscape (86%) and transition to a remote workforce (81%) created new IT security challenges for their organizations.**

96% increased their cybersecurity budgets in 2020, and 91% plan to do so again in 2021.

MOST HAVE LOW CONFIDENCE IN THEIR COMPANY'S SECURITY POSTURE

Despite the increased investment in cybersecurity in 2020, **three in four respondents (78%) expressed a lack of confidence in their company's IT security posture and saw room for improvement.** Only 22% felt very confident.

Respondents were least confident in their organization's security roadmap (32%), security-related technology and tools (30%), and internal teams and skill sets (27%). They reported the highest level of trust in their company's data management strategy, but even then, less than half (45%) voiced confidence in this aspect of security operations.

Key findings (cont.)

SECURITY PRIORITIES SHIFTED TO CLOSING IMMEDIATE SECURITY GAPS

Companies shifted cybersecurity modernization priorities in response to the challenges presented by the pandemic, focusing largely on closing immediate security gaps, implementing basic technologies that were easy to deploy, and leaving more complex, longer-range projects for a later date.

On average, companies accelerated 5–6 different cybersecurity initiatives, including threat visibility/identification (73%), incident response (70%), network security (68%), endpoint security (67%), application security (67%), and malware protection (64%).

Only 57% of businesses conducted a data security risk assessment during the year despite the new threats faced in the 2020 environment.

SECURITY STAFF EXPANSION TOOK A BACK SEAT

Despite the increase in security budgets and the large number of security projects undertaken in 2020, **only 27% of respondents reported expanding security staff in 2020.**

That left IT teams stretched extremely thin and without many of the specialists required to execute the wide range of tasks necessitated by the year's evolving threatscape.

41% plan to begin or resume staff expansion in 2021 along with modernizing security operations (42%).

Key findings (cont.)

LACK OF AUTOMATION IS THE #1 STUMBLING BLOCK

55% cited lack of automation as the top challenge in security operations and management, reflecting the increasing complexity of the security infrastructure and the need to quickly analyze the growing volumes of information generated by security tools.

Outdated network access control systems (47%), legacy infrastructure/software/tools that do not address today's threats and cloud environments (45%), and lack of skilled cybersecurity staff (43%) lead the list of hurdles.

YET CYBERSECURITY INTEGRATION PROJECTS DEMONSTRATE PROGRESS

Nearly 70% initiated projects to improve incident response by integrating it with companywide business continuity plans, indicating rising recognition of the risk that a cyberattack poses to company operations.

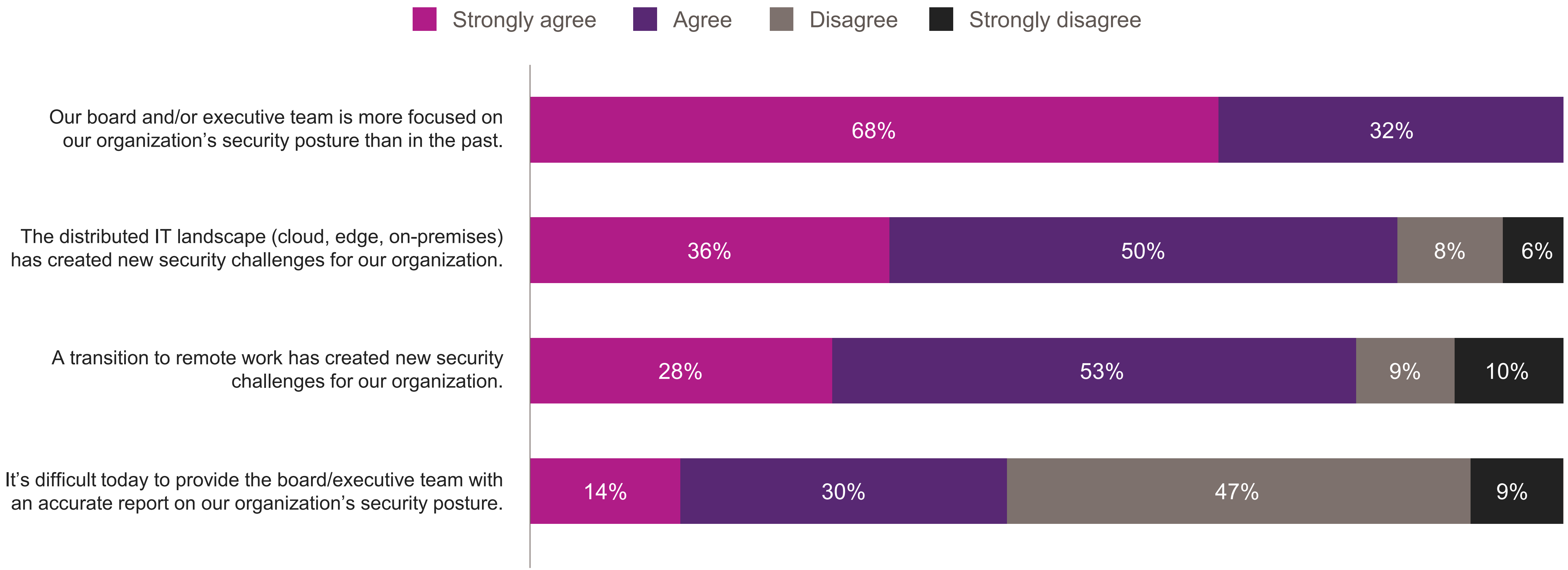
Cybersecurity is also being integrated into infrastructure and DevOps decisions (61%) and broader business operations decisions (59%), highlighting efforts to incorporate security protections into every aspect of IT as well as everyday business activities in order to better fortify organizations against cyberthreats.

Insight | Cloud + Data Center Transformation

New Cybersecurity Challenges

100% agree that boards & executive teams are more concerned about cybersecurity than in the past

Distributed IT/remote work increased C-suite security focus & security challenges

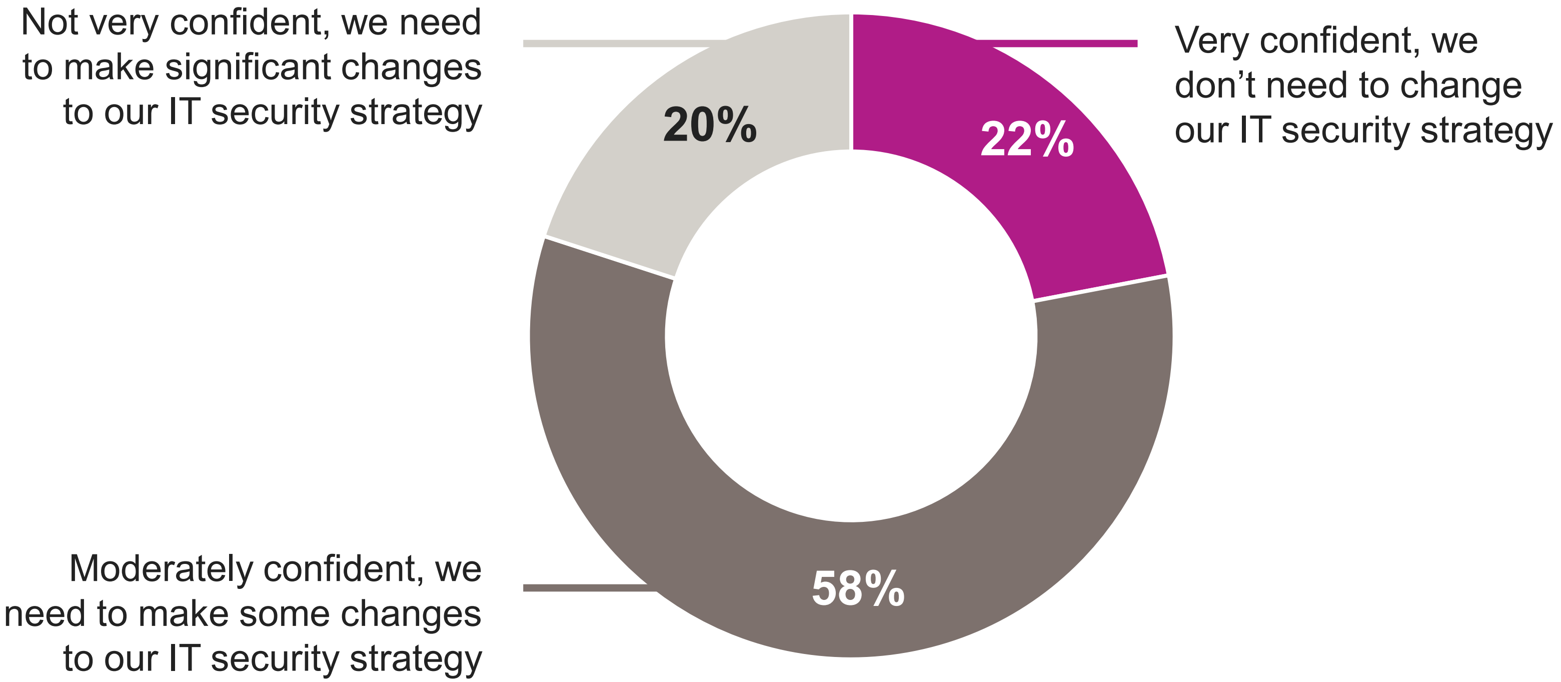


Q. Please rate your agreement with the following statements.

Insight. Cloud + Data Center Transformation

78% of respondents lack confidence in their company's current IT security posture

Only 22% say no changes are needed to improve security strategy



Large enterprises:
(10,000+ employees)

Very confident	19%
Moderately	68%
Not very	13%

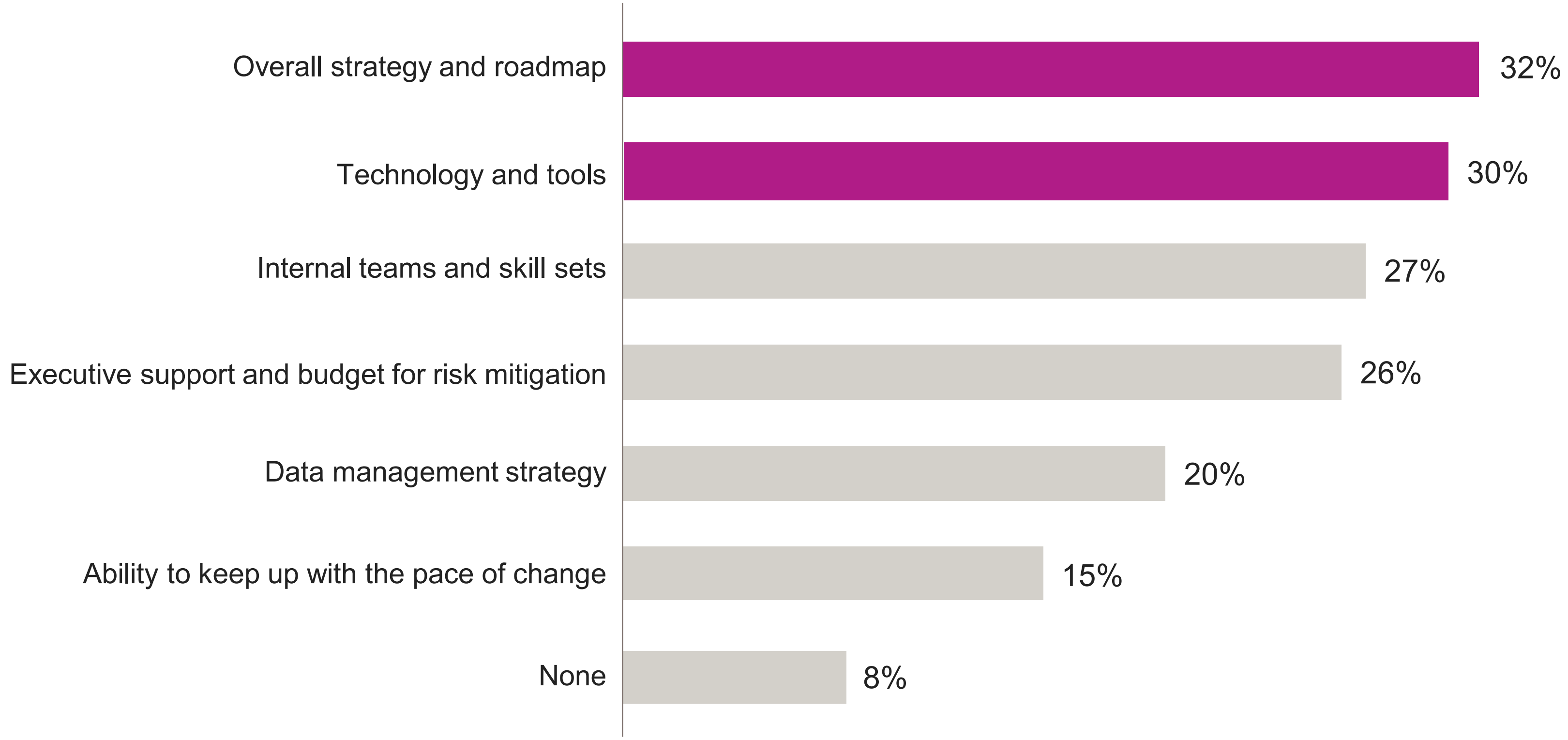
Midsize enterprises:
(1,500–9,999 employees)

Very confident	26%
Moderately	47%
Not very	27%

Q. How confident are you in your organization's overall IT security posture? (Please select one.)

Respondents are least confident in their company's overall security strategy and tools availability for adequate protection

Aspects of company security posture with the least amount of confidence



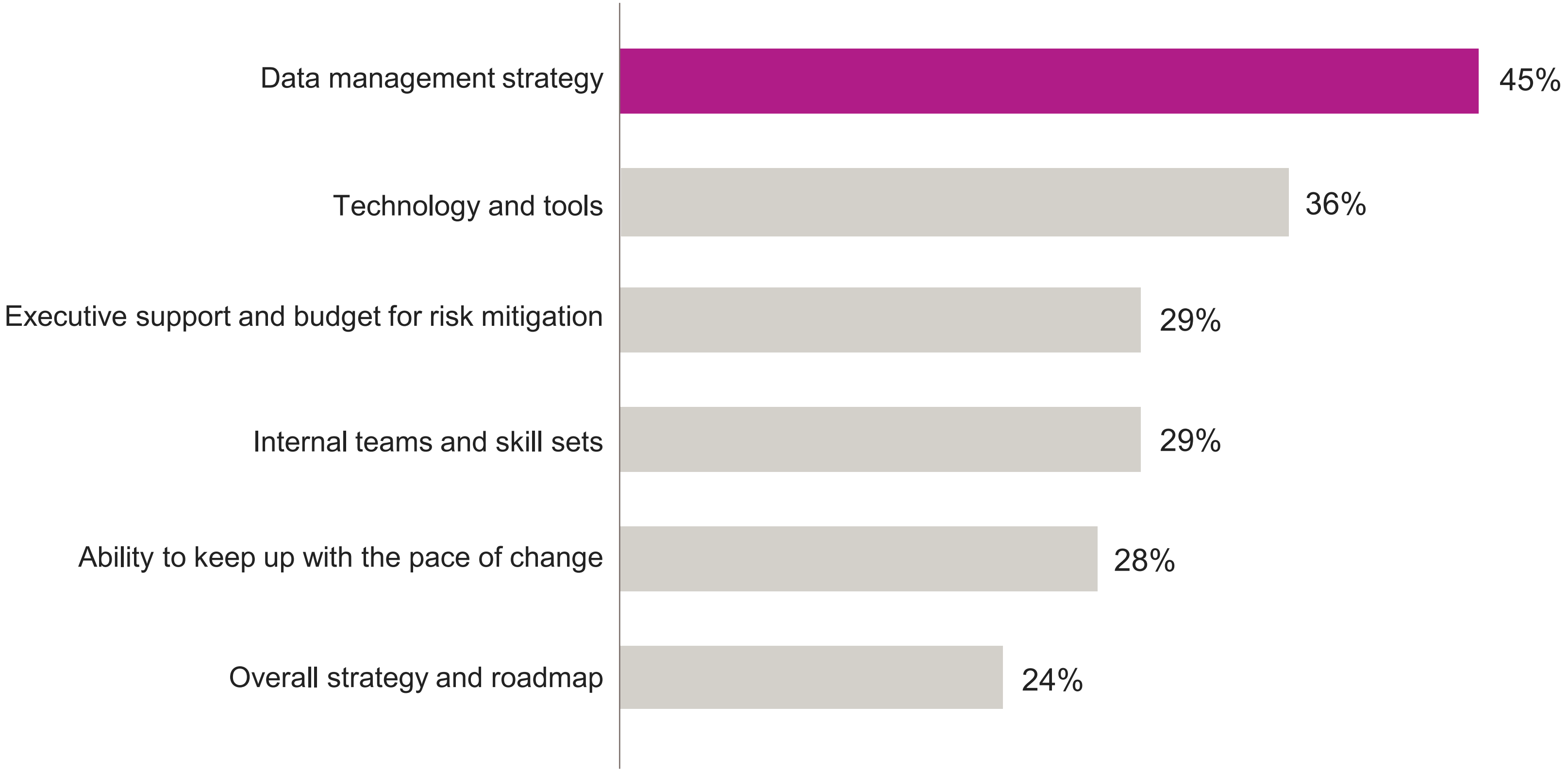
Large enterprises — Least confident (10,000+ employees)	
Overall strategy and roadmap	**42%**

Midsize enterprises — Least confident (1,500–9,999 employees)	
Internal teams/skills	**39%**

Q. What aspects of your security posture do you feel the least confident about? (Please select up to two.)

Respondents are most confident in their company's data management strategy, yet only 45% reported this confidence level

Aspects of company security posture with the greatest amount of confidence



Large enterprises — Most confident
(10,000+ employees)

Technology and tools	**42%**

Midsize enterprises — Most confident
(1,500–9,999 employees)

Executive support	**42%**
Ability to keep up pace	**35%**

Q. What aspects of your security posture do you feel the most confident about? (Please select up to two.)

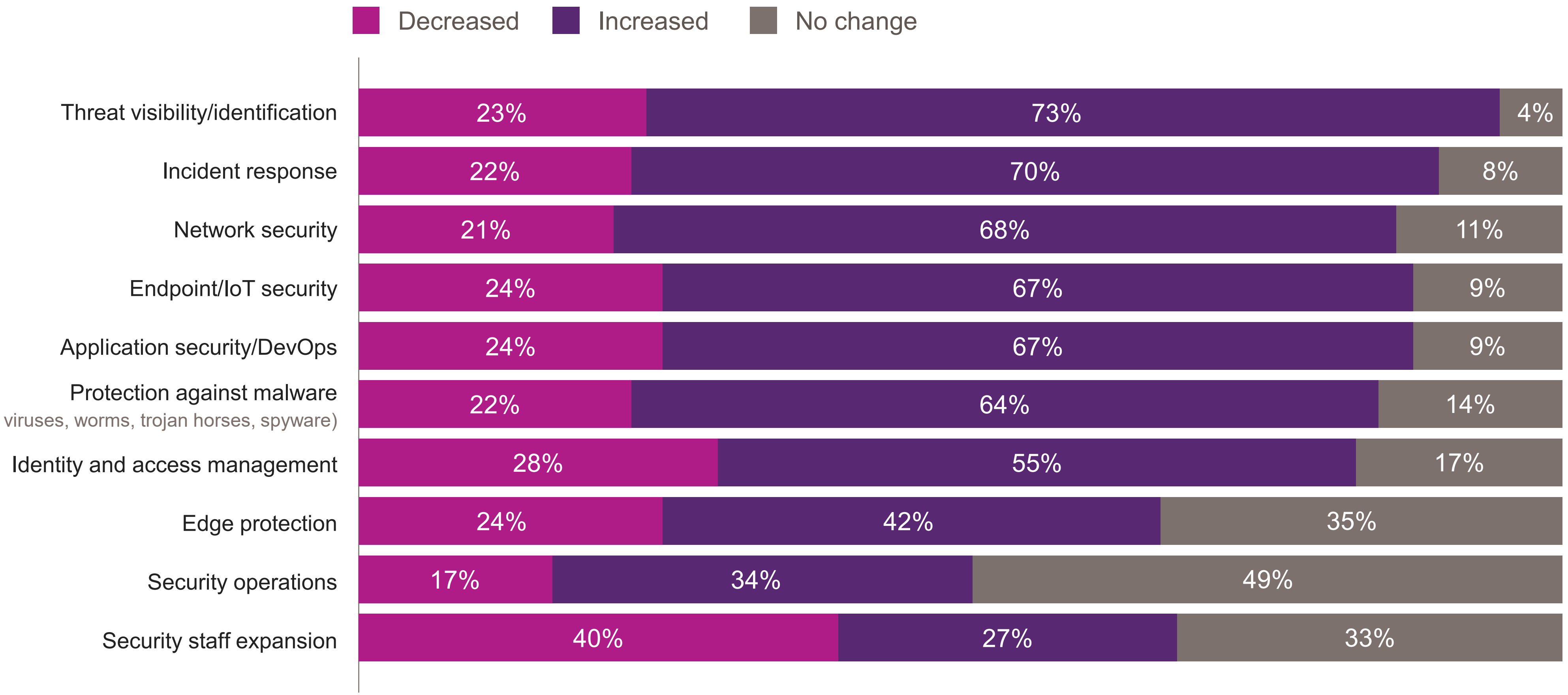
Insight | Cloud + Data Center Transformation

Top Priorities & Projects

Cybersecurity modernization priorities shifted in 2020 in response to the work-from-home/distributed IT environment

Companies accelerated 5–6 different IT security initiatives to address new threats, but security operations and staff expansion lagged.

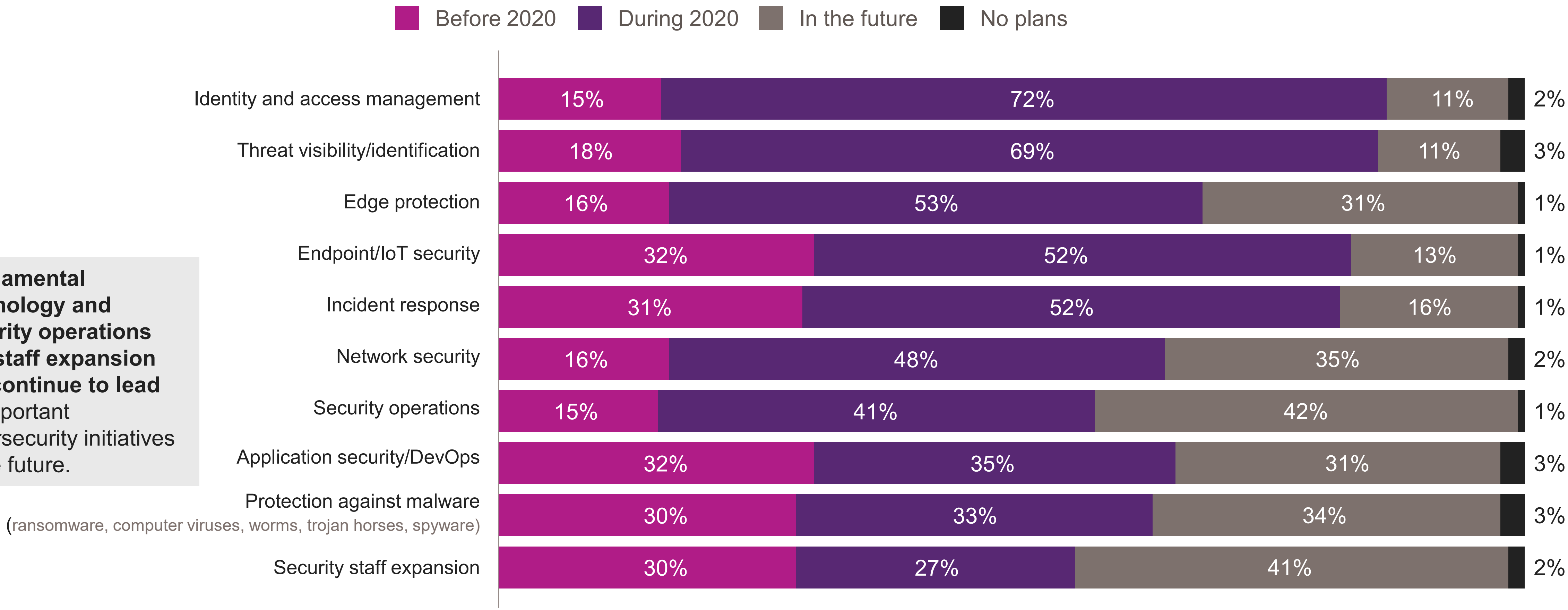
Impact of 2020 challenges on cybersecurity priorities



Q. How did the sudden expansion of work-from-home/distributed IT environment that accompanied the pandemic in 2020 impact your cybersecurity modernization priorities?

Modernization projects undertaken in 2020 largely reflected the need to address urgent security gaps created by remote work

Modernization projects before, during, and after 2020



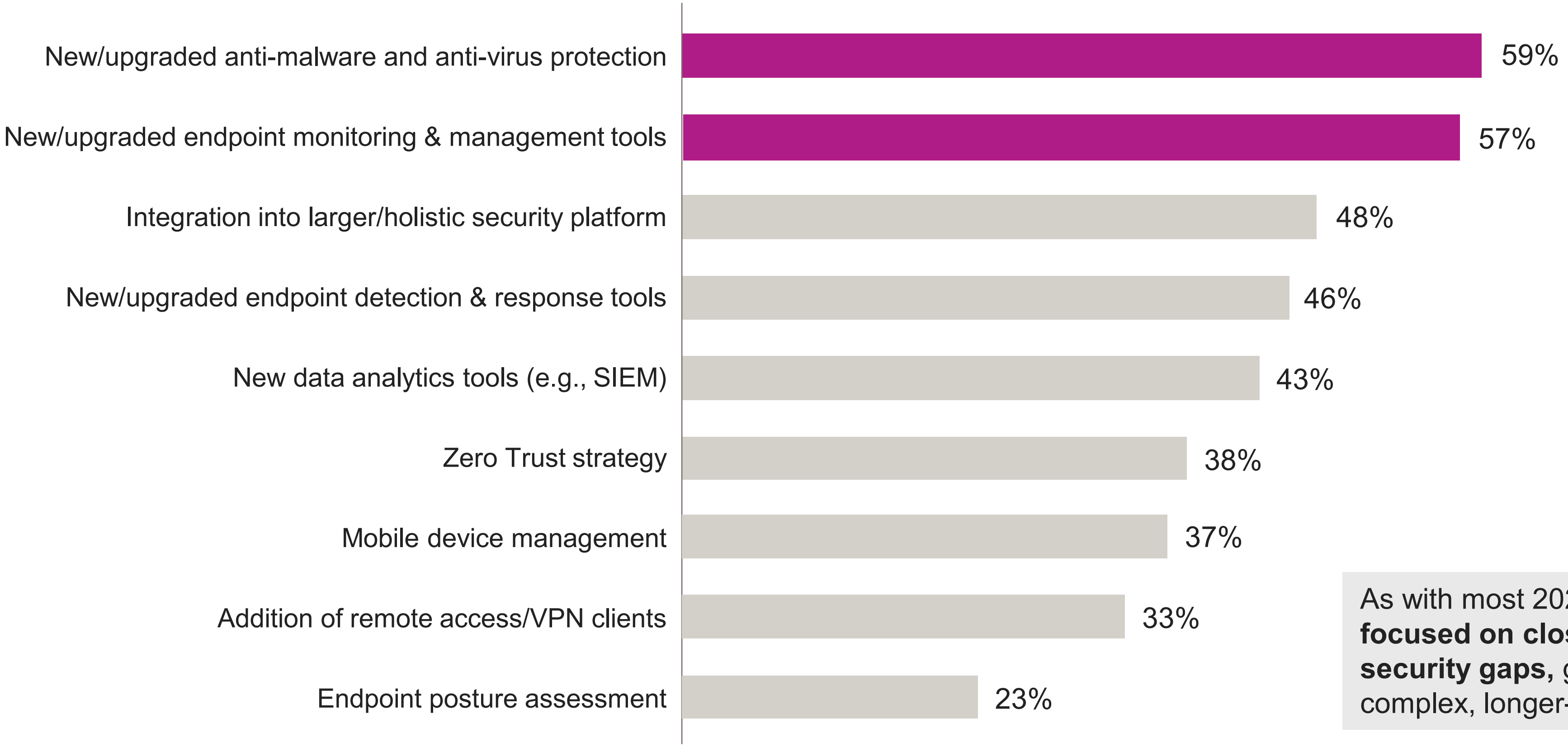
Fundamental technology and security operations and staff expansion will continue to lead as important cybersecurity initiatives in the future.

Q. Whether or not your priorities changed, what areas of cybersecurity did your organization work to modernize in 2020? (Please select one answer per row.)

NOTE: Rows may not add up to 100% due to rounding.

In the endpoint security category, the top projects were upgrades to anti-malware/anti-virus and endpoint management solutions

Endpoint security projects initiated/executed in 2020

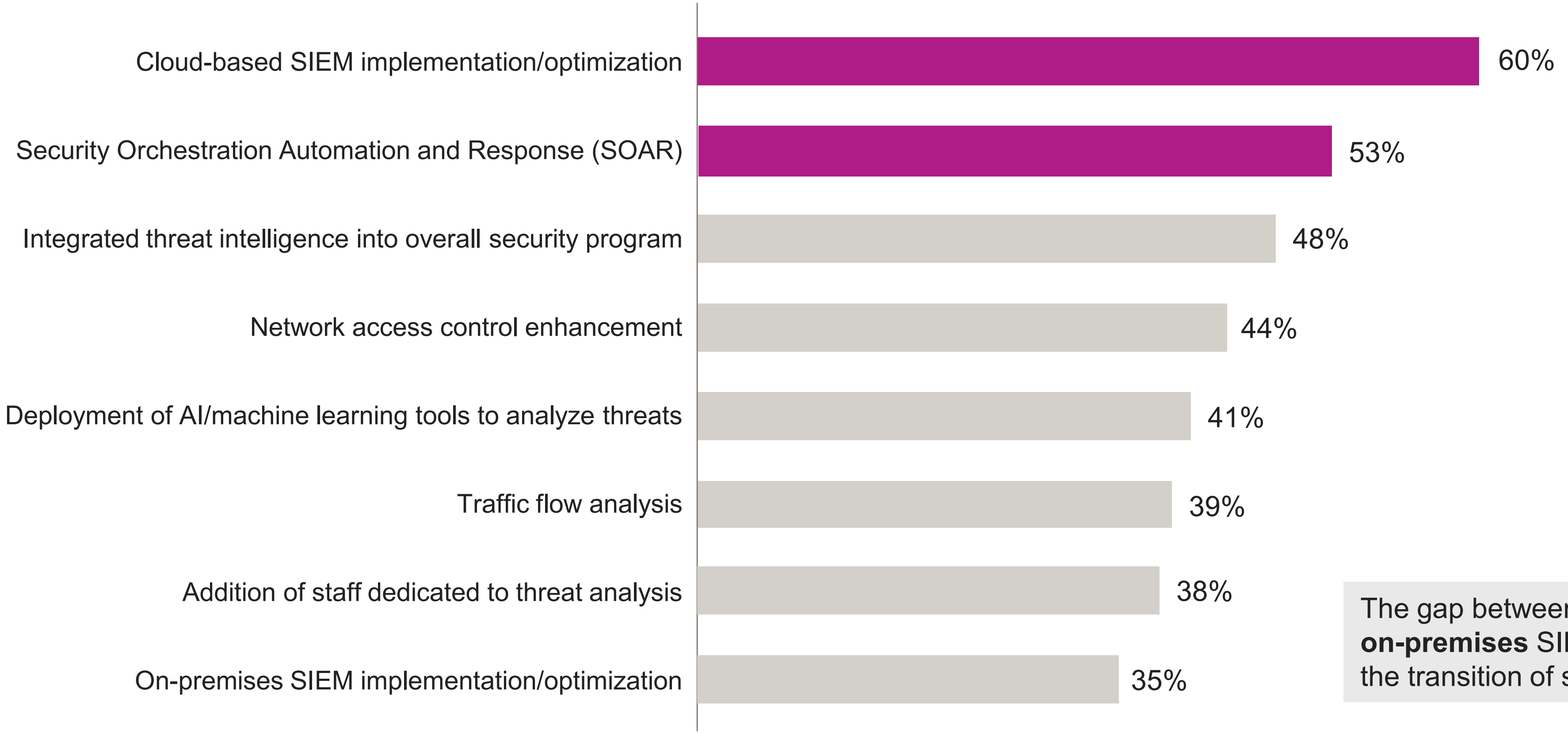


As with most 2020 projects, **IT teams focused on closing immediate security gaps,** giving lower priority to complex, longer-range initiatives.

Q. What endpoint security projects did your organization initiate or execute in 2020? (Please select all that apply.)

Cloud-based SIEM and Security Orchestration Automation and Response (SOAR) projects led threat identification initiatives

Threat visibility/identification projects initiated/executed in 2020

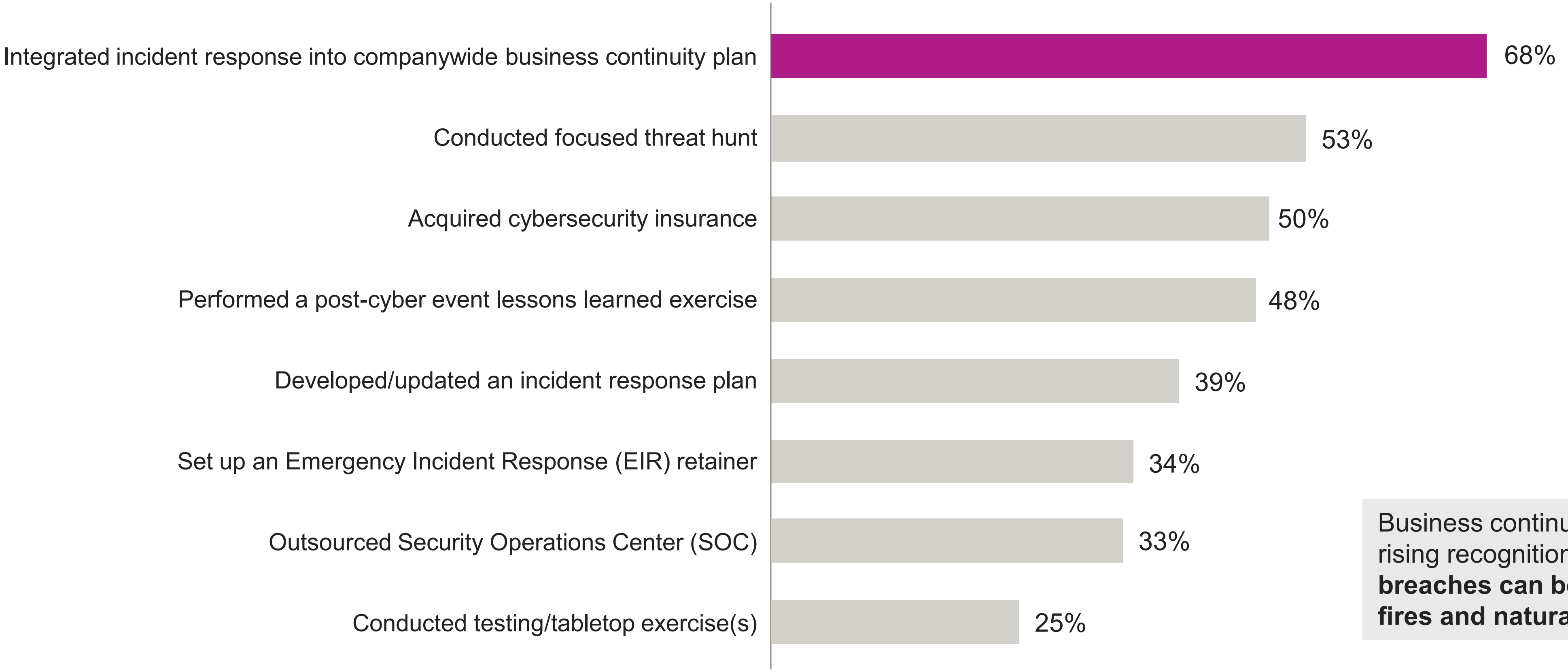


The gap between **cloud-based and on-premises** SIEM projects highlights the transition of security to the cloud.

Q. What threat visibility/identification projects did your organization initiate or execute in 2020? (Please select all that apply.)

Nearly 70% initiated projects to improve incident response by integrating it with companywide business continuity plans

Incident response projects initiated/executed in 2020

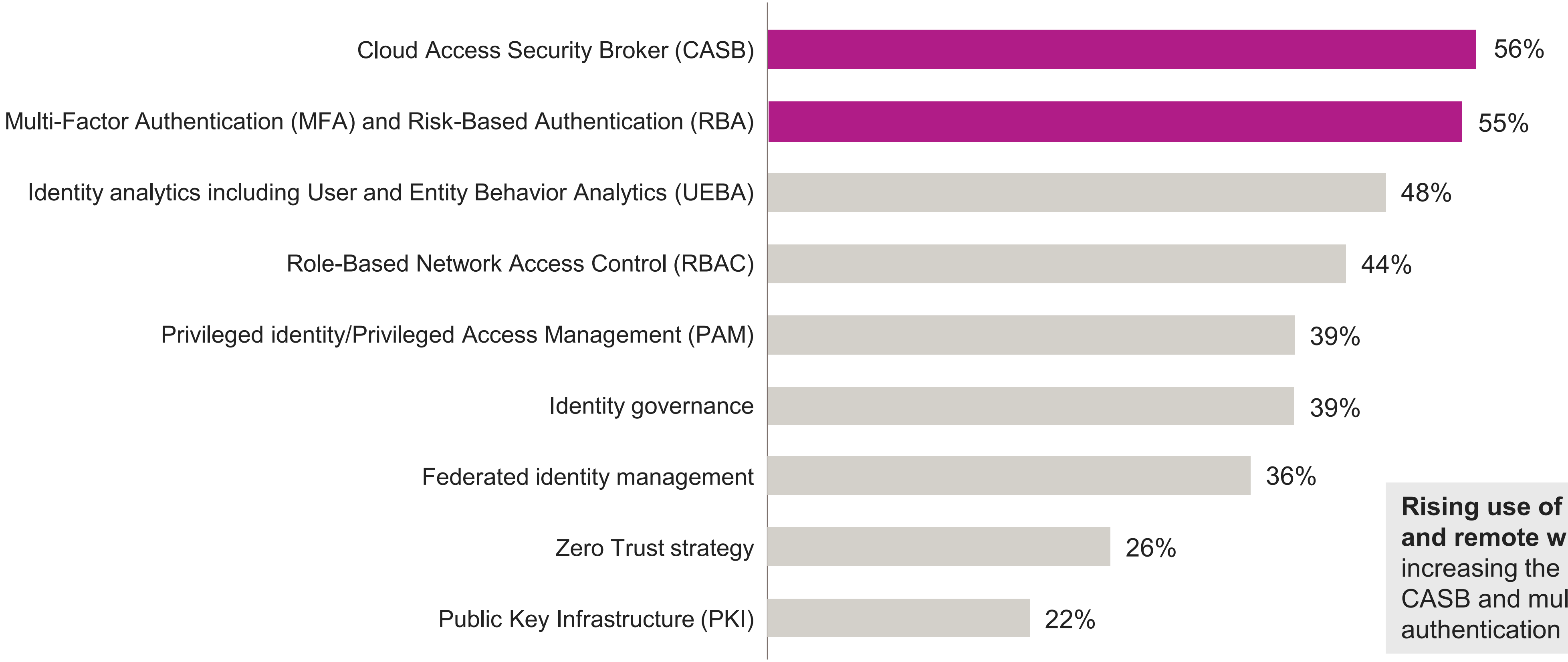


Business continuity integration shows rising recognition **that cybersecurity breaches can be as damaging as fires and natural disasters**.

Q. What incident response projects did your organization initiate or execute in 2020? (Please select all that apply.)

55%+ implemented new cloud access controls and multi-factor authentication to improve identity management

Identity management projects initiated/executed in 2020

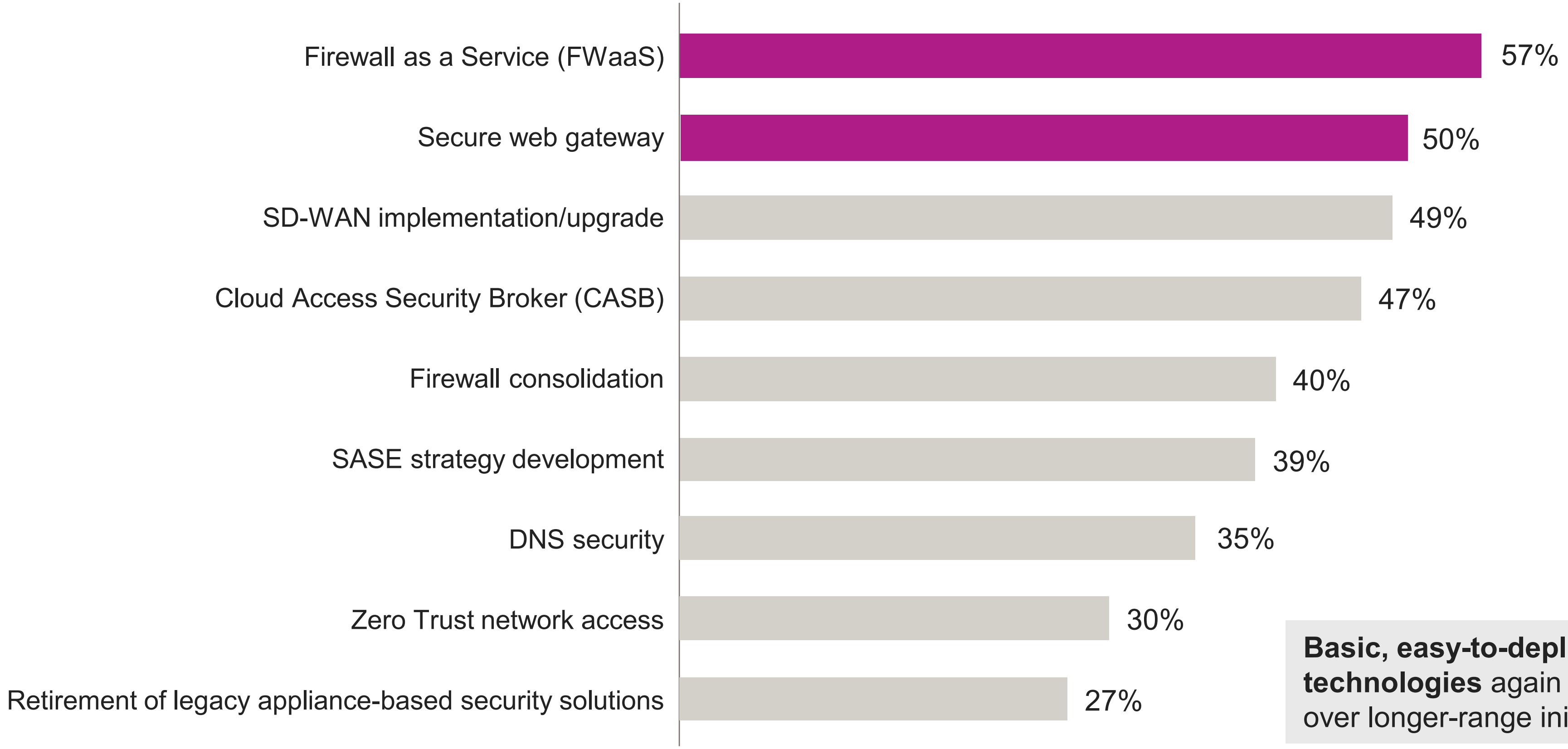


Rising use of cloud services and remote work are increasing the emphasis on CASB and multi-factor authentication projects.

Q. What identity management projects did your organization initiate or execute in 2020? (Please select all that apply.)

Topping the list of 2020 edge protection projects were cloud-based firewalls and secure web gateways

Edge protection projects initiated/executed in 2020



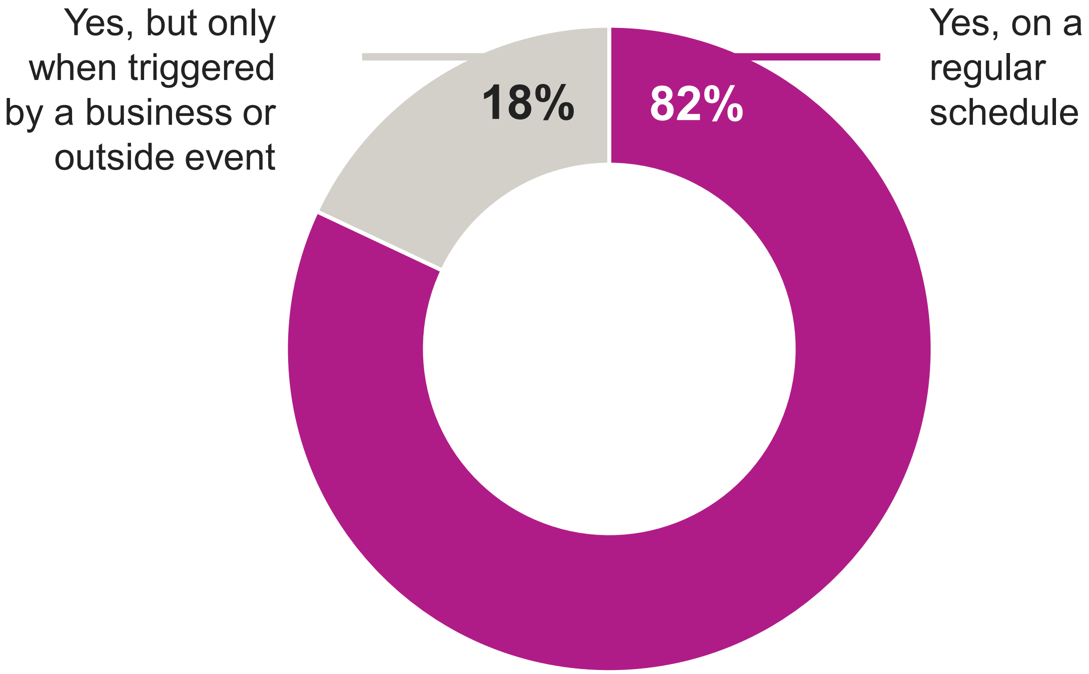
Basic, easy-to-deploy cloud technologies again took precedence over longer-range initiatives.

Q. What edge protection projects did your organization initiate or execute in 2020? (Please select all that apply.)

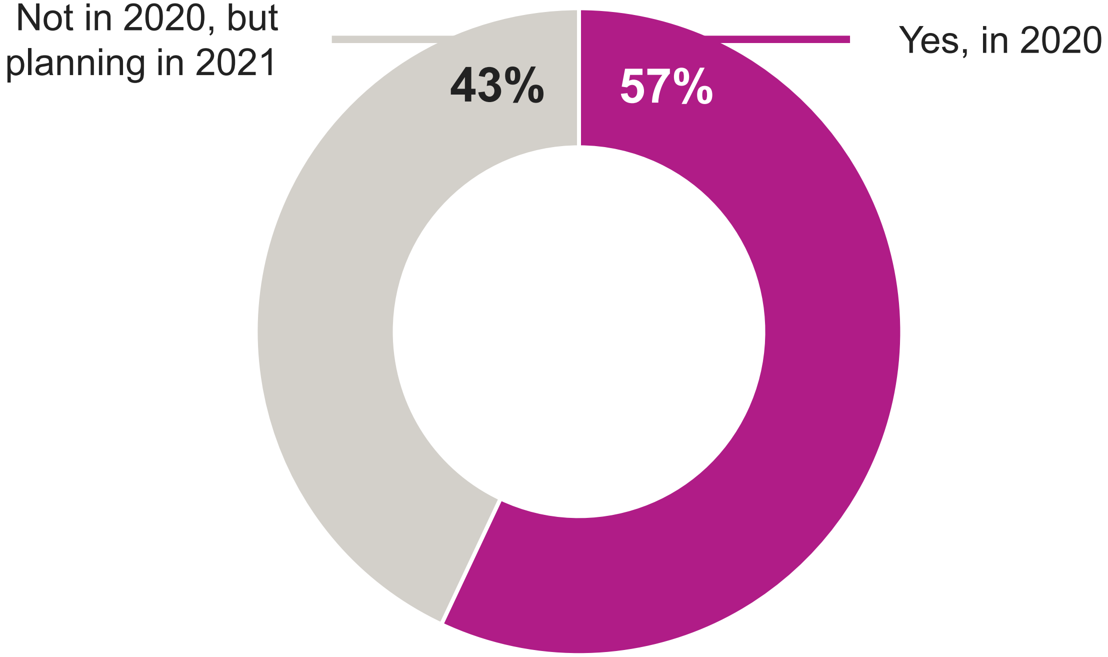
Security Operations and Management

Companies are vigilant about data security risk assessment, yet 43% did not conduct a risk assessment in 2020

All companies conduct some form of data security risk assessment



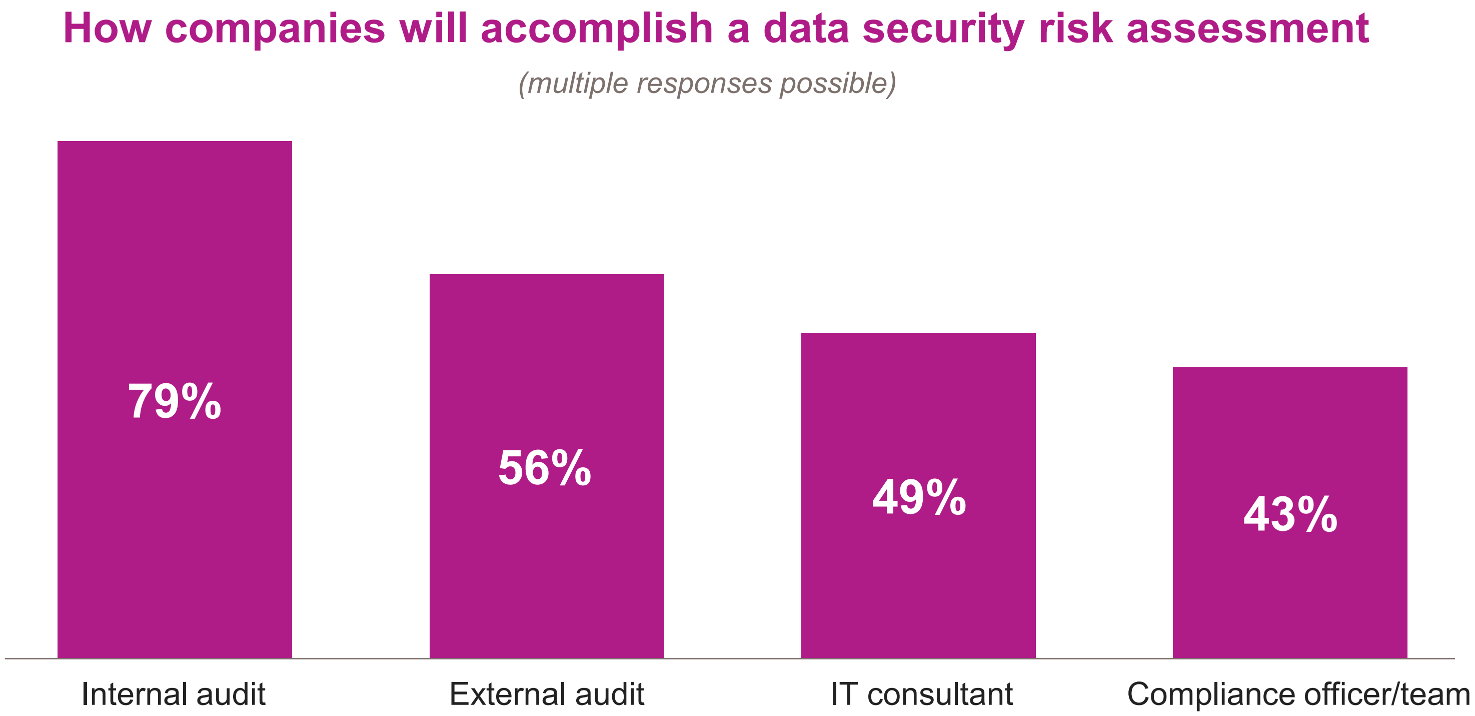
Only 57% of respondent companies conducted a data security risk assessment in 2020



Critical 2020 cybersecurity challenges likely sidelined many data security risk assessment projects.

Q. Does your organization conduct data security risk assessments?
Q. Did your organization conduct a data security risk assessment in 2020, or are you planning to do so in 2021?

Respondents use a combination of internal and external resources to accomplish a data security risk assessment



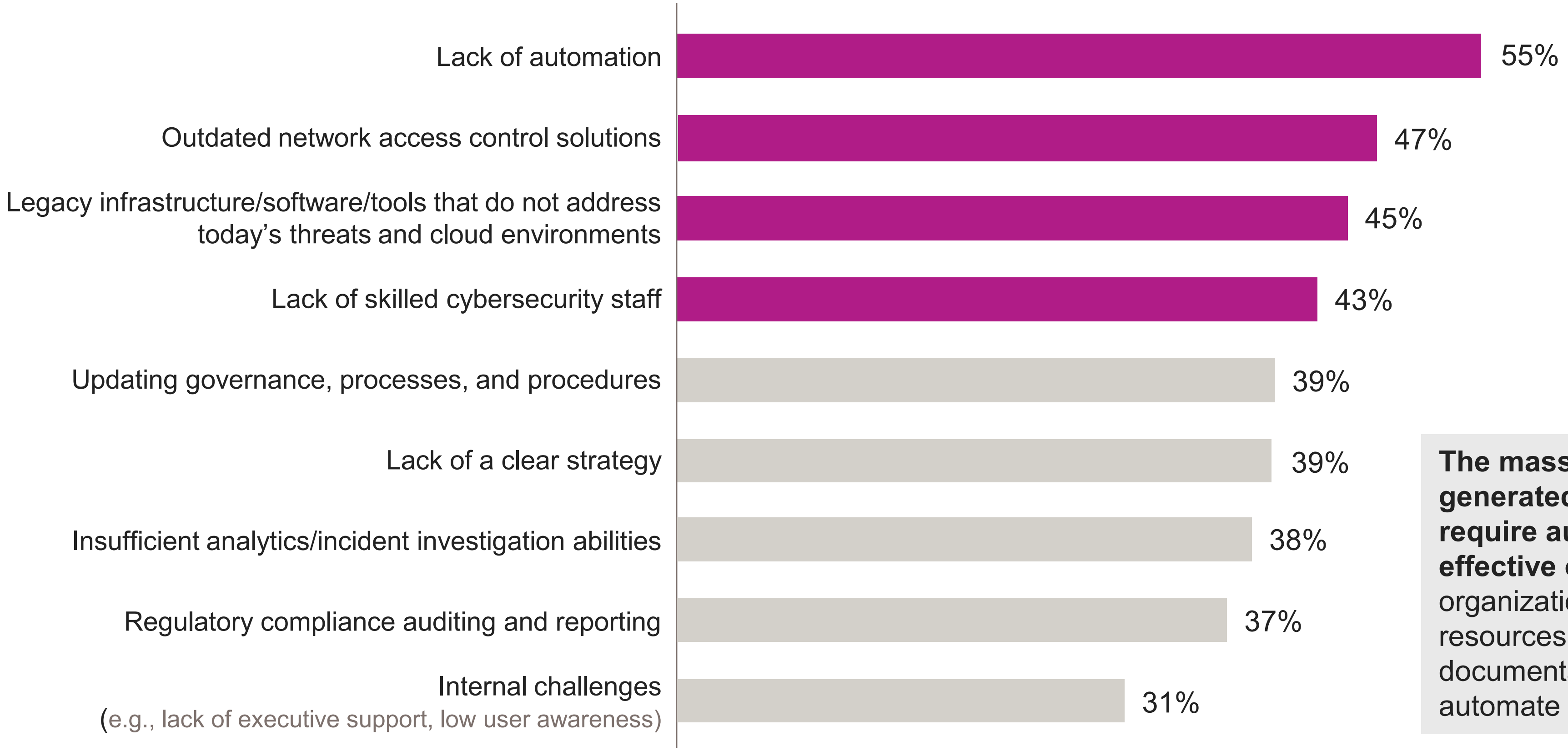
Execution by company size

	Midsize	Large
Internal	92%	67%
External	61%	50%
Consultant	29%	67%
Compliance officer	39%	47%

Q. If you planned or are planning to conduct a data security risk assessment, how did or will you accomplish it? (Please select all that apply.)

55% cite lack of automation as the top obstacle to security operations and management, followed by outdated technology and skills gaps

Major security operations and management challenges

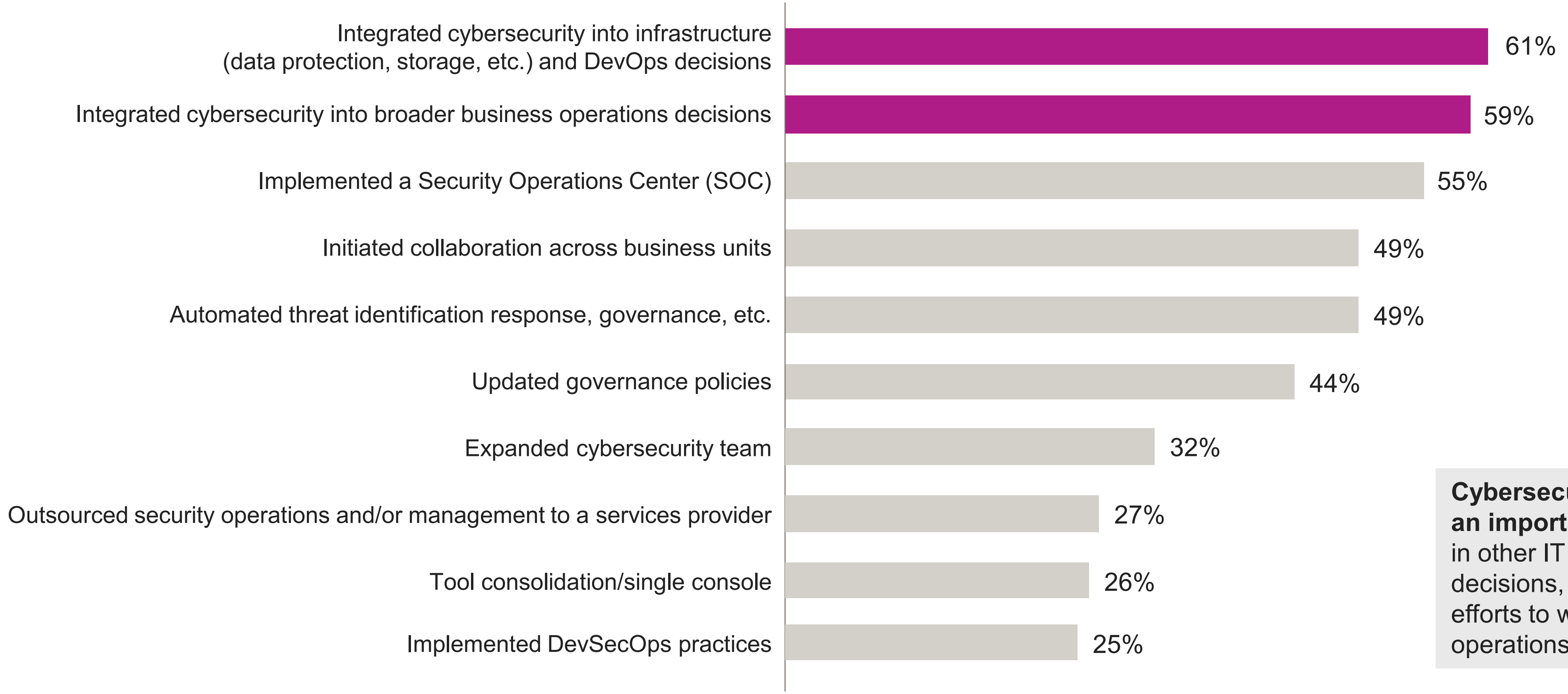


The massive data volumes generated by security tools require automation for effective oversight, yet many organizations lack the internal resources, tools, and detailed documentation required to automate security processes.

Q. What are your organization's major security operations and management challenges? (Select up to five.)

Integrating cybersecurity into infrastructure, DevOps, and business operations decisions topped 2020 security operations/management changes

Changes made to company's security operations/management in 2020

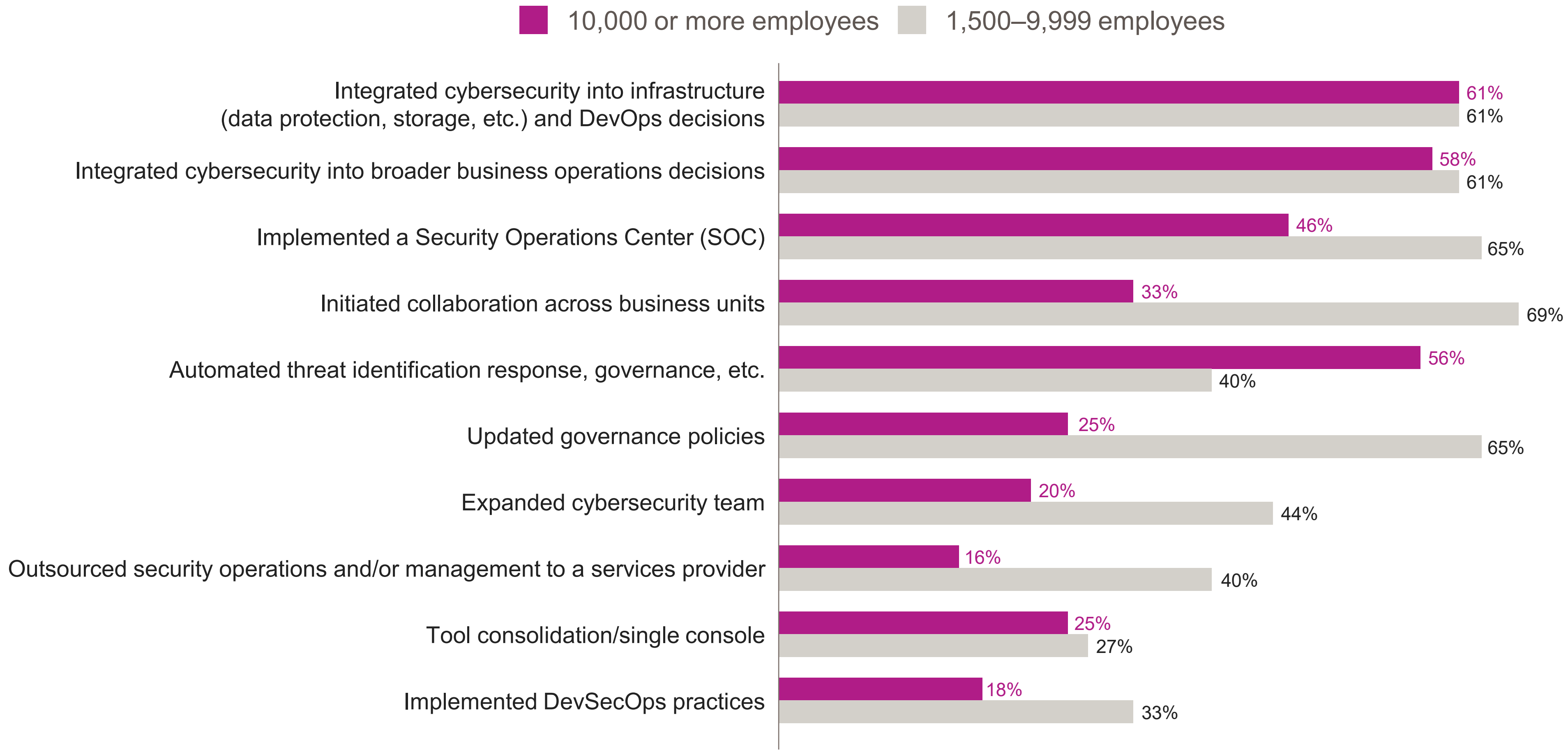


Cybersecurity is becoming an important consideration in other IT and business decisions, creating new efforts to weave it into overall operations.

Q. What changes did you make to your security operations and management in 2020? (Select all that apply.)

Midsize organizations made more security operations changes than enterprises in all areas except automated threat response

Changes made to company's security operations/management in 2020

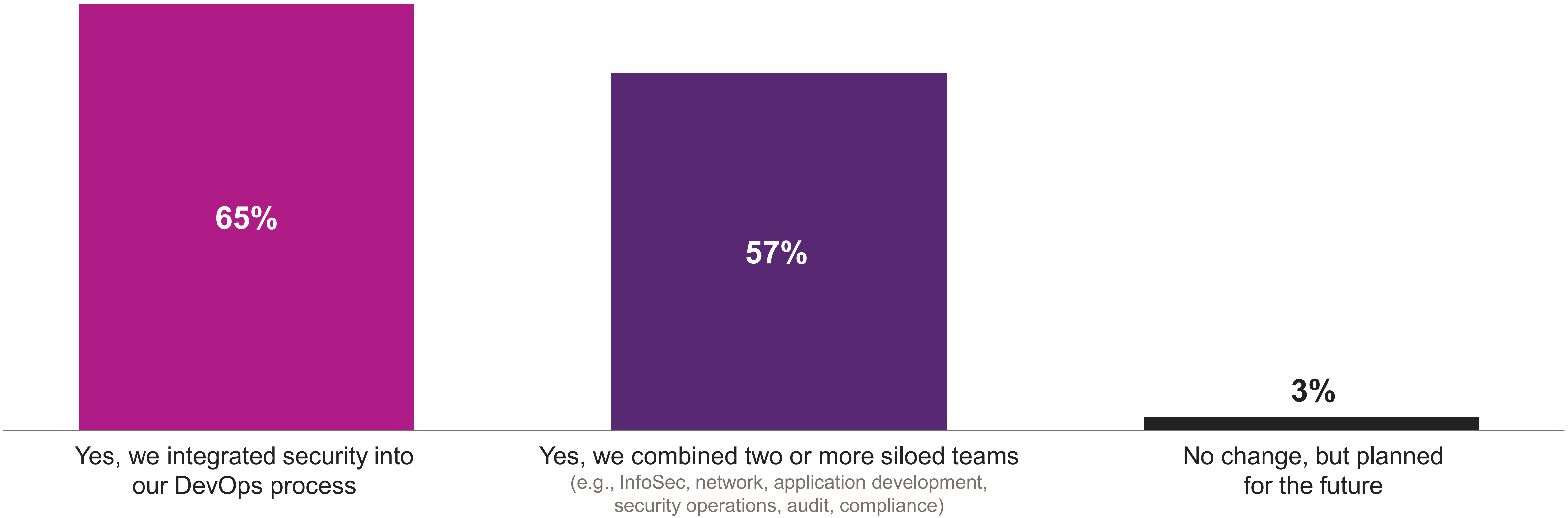


	10,000 or more employees	1,500–9,999 employees
Integrated cybersecurity into infrastructure (data protection, storage, etc.) and DevOps decisions	61%	61%
Integrated cybersecurity into broader business operations decisions	58%	61%
Implemented a Security Operations Center (SOC)	46%	65%
Initiated collaboration across business units	33%	69%
Automated threat identification response, governance, etc.	56%	40%
Updated governance policies	25%	65%
Expanded cybersecurity team	20%	44%
Outsourced security operations and/or management to a services provider	16%	40%
Tool consolidation/single console	25%	27%
Implemented DevSecOps practices	18%	33%

Smaller organizations are more agile than large enterprises in making major changes to their security operations.

Q. What changes did you make to your security operations and management in 2020? (Select all that apply.)

97% made initial changes to their team structure to more tightly integrate security in the overall IT strategy *(multiple responses possible)*

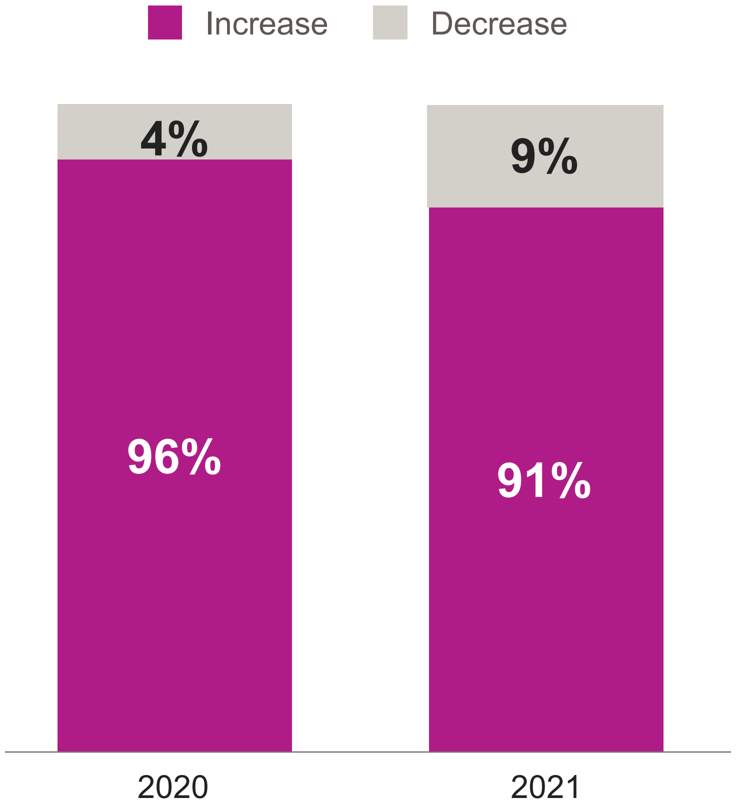


Q. Has your organization made any changes to its team structure this year to more tightly integrate security into your overall IT strategy? (Select all that apply.)

Cybersecurity Budgets

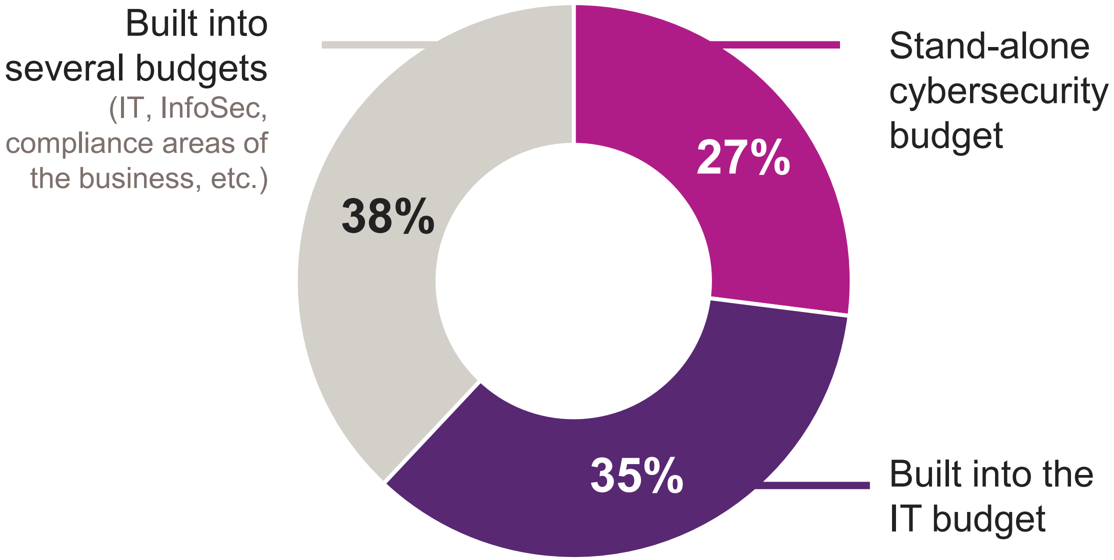
Nine in ten respondents will increase their cybersecurity modernization budgets again in 2021

Budget allocation for cybersecurity



Q. Is cybersecurity a stand-alone budget or is it built into other budget(s)?
Q. How did your overall cybersecurity budget change in 2020?
Q. How will your cybersecurity budget change in 2021 compared to 2020?

Cybersecurity is a line item on multiple enterprise budgets

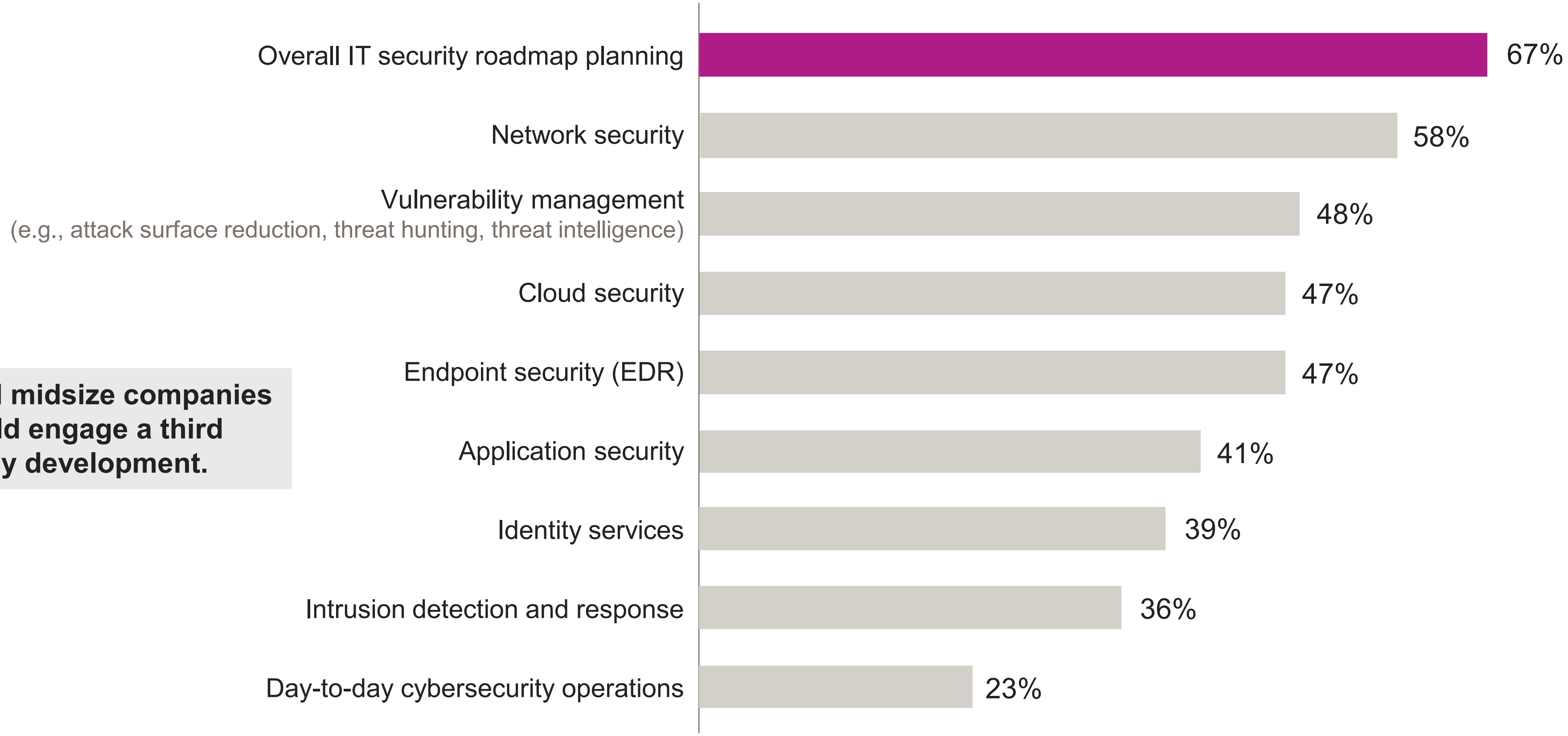


Midsize companies are more likely (38%) to have a stand-alone cybersecurity budget than large companies (18%).

Insight | Cloud + Data Center Transformation

Two-thirds (67%) currently or plan to seek assistance in developing an overall IT security strategy

Cybersecurity functions currently or planning to engage a third-party provider



Large (64%) and midsize companies (70%) alike would engage a third party for strategy development.

Q. For what cybersecurity functions are you currently engaging or planning to engage a third-party service provider?

For more information

Media inquiries

Jim Capalbo
Jill Schmidt PR
Tel. 847.946.2991
Email: jim@jillschmidtpr.com

General inquiries

Cheryl Scholz
Insight Enterprises
Tel. 952.279.4829
Email: cheryl.scholz@insight.com