SECURITY RESILIENCE IN FEDERAL GOVERNMENT

Government leaders share their perceptions on their organizations' ability to assess and manage IT risk across their IT environment.

PRESENTED BY FEDSCOOP

UNDERWRITTEN BY cisco SECURE

EXECUTIVE SUMMARY

Modernizing security systems to strengthen cybersecurity resiliency has taken on new urgency at federal agencies following the Executive Order on Improving the Nation's Cybersecurity. And at the end of 2022, congressional leaders signaled their support for security-strengthening initiatives when the passed the omnibus bill, that includes a $1.3 billion spending package for Cybersecurity and Infrastructure Security Agency (CISA) programs.

In this FedScoop survey we asked 165 prequalified government leaders, IT and security directors and managers, procurement staff and IT influences to measure the strength of their current security posture, the kinds of security incidents that are impacting their agencies, and the strategies they are taking to improve security resilience.

Agencies' greatest security risks

- Respondents reported the top security incidents that their agencies have faced in the past, including **network or system outage (56%), network or data breach (44%)** and **accidental disclosure (27%)**.
- **36%** of respondents indicated that the most recent security incident **occurred 3 to 12 months ago** and **12%** of respondents indicated that the most recent security incident **occurred less than 3 months ago**.
- Of the security incidents that affected agencies, **24%** of **respondents shared that they experienced a major security incident that impacted its security resilience**.

EXECUTIVE SUMMARY

Challenges to modernize IT risk management tools

Respondents identified their top challenges to implement modern IT risk management tools, including:

- Keeping up with the demands and growth of the mission (40%).
- Creating a security culture embraced by all employees (33%).
- Adapting to unexpected external change events or trends (30%).
- Containing the spread or scope of security incidents (30%).

Priorities to modernize security detection tools

Respondents reported several security capabilities they are planning to, or will plan to, implement to improve security resilience at their organization, including:

- **Extended detection and response (XDR)**, which 31% of respondents are currently implementing and 12% plan to implement in the future. 35% say they have it in place.
- **Endpoint detection and response**, which 25% of respondents are currently implementing and 12% plan to implement in the future. 42% say they have it in place.
- **Micro-segmentation of application workloads**, which 27% of respondents are currently implementing and 16% plan to implement in the future. 25% say they have it in place.

Priorities to modernize security policies

Respondents reported several security policies they are planning to, or will plan to, implement to improve security resilience at their organization, including:

- **Zero-trust access model**, which 26% of respondents are currently implementing and 16% plan to implement in the future. 35% say they have it in place.
- **Risk-based vulnerability management**, which 25% of respondents are currently implementing and 16% plan to implement in the future. 38% say they have it in place.
- **Enterprise single sign-on**, which 22% of respondents are currently implementing and 10% plan to implement in the future. 48% say they have it in place.

WHO WE SURVEYED

FedScoop surveyed 165 prequalified federal government IT decision-makers in a survey conducted online in December 2022.

Respondent by agency type

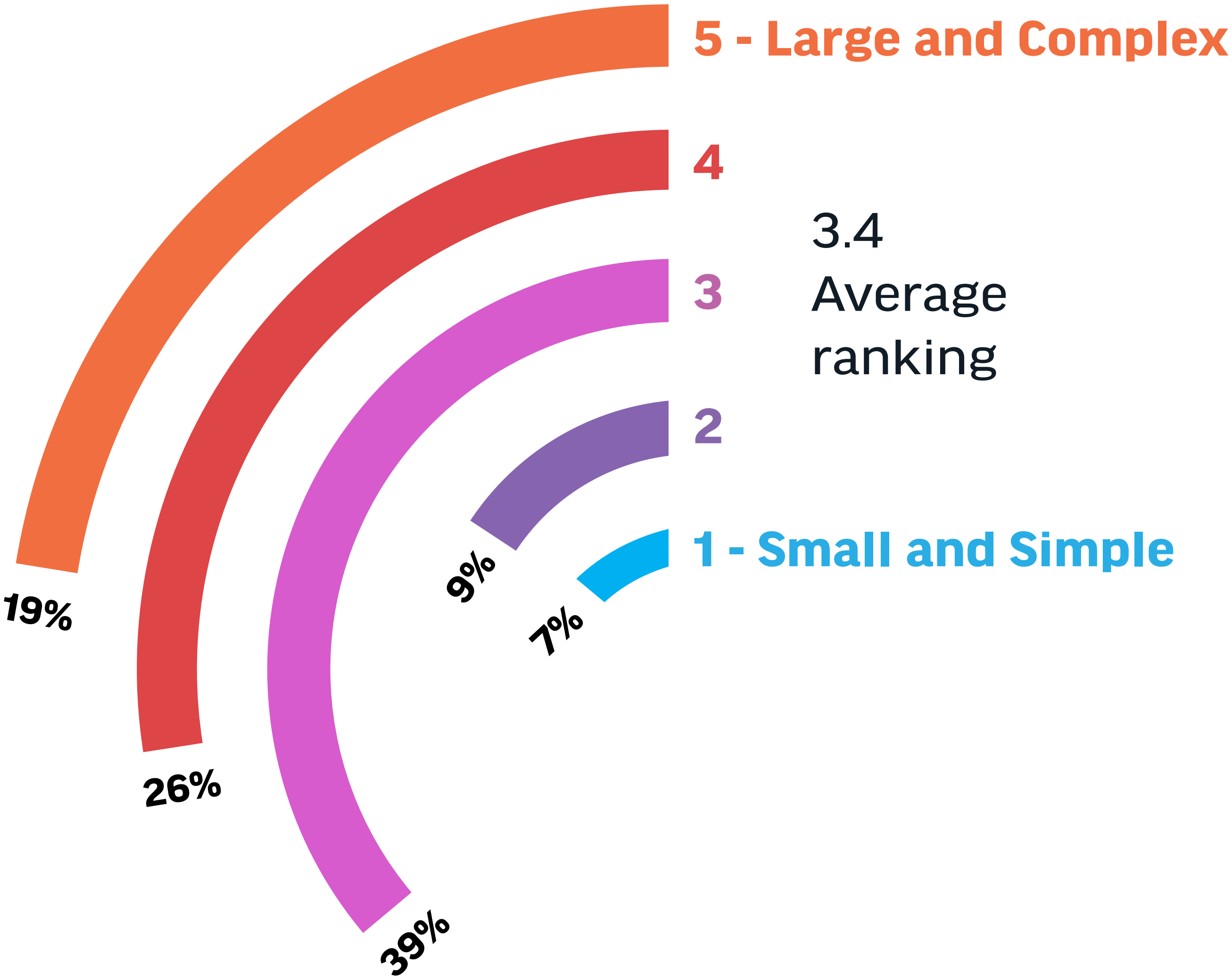
Federal Civilian Agencies	45%
Federal Defense Agencies	35%
Federal Government Contractor	19%

Respondent by job title

27%	IT Management
19%	C-Suite, Senior business, Program leader
16%	IT security management/staff
14%	Procurement official/staff
5%	IT influencer
4%	CIO, CTO, CISO
15%	Other (systems engineer, operations management)

THE SIZE OF IT ENVIRONMENTS AGENCIES ARE PROTECTING

How would you describe the size and scope of your organization's IT environment, in terms of the user base it supports?
Rank: 1 — "Small and Simple (support less than 250 users)" to 5 — "Large and complex (support more than 1 million users)"

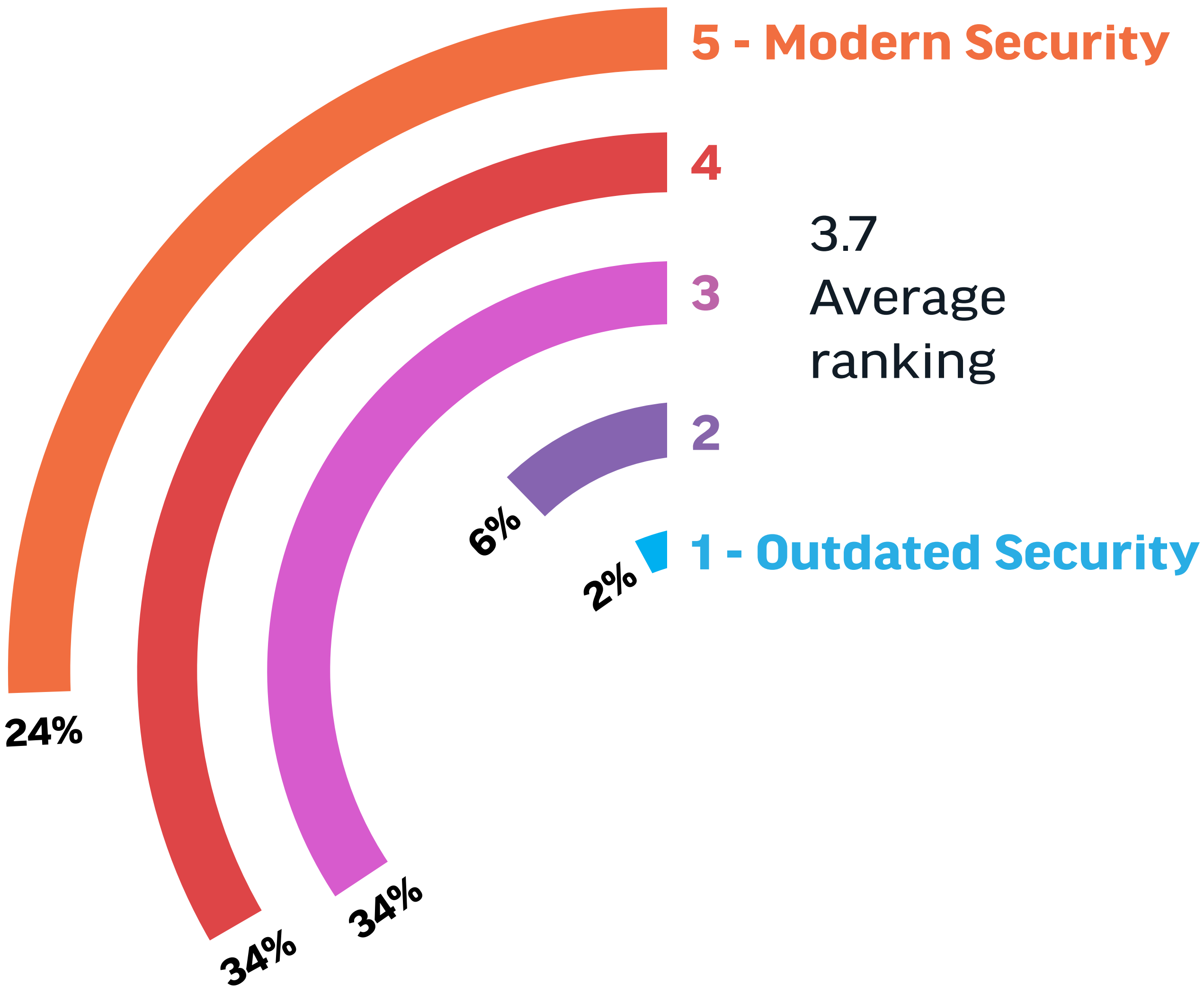


3.4
Average
ranking

Base: 165

THE AGE OF IT SECURITY ENVIRONMENTS AMONG AGENCIES

How would you rate your IT security environment (Rank 1 to 5), where 1 is "Outdated Security (Relies on non-integrated / legacy systems)" and 5 is "Modern Security (Relies on integrated / cloud-capable systems)?"

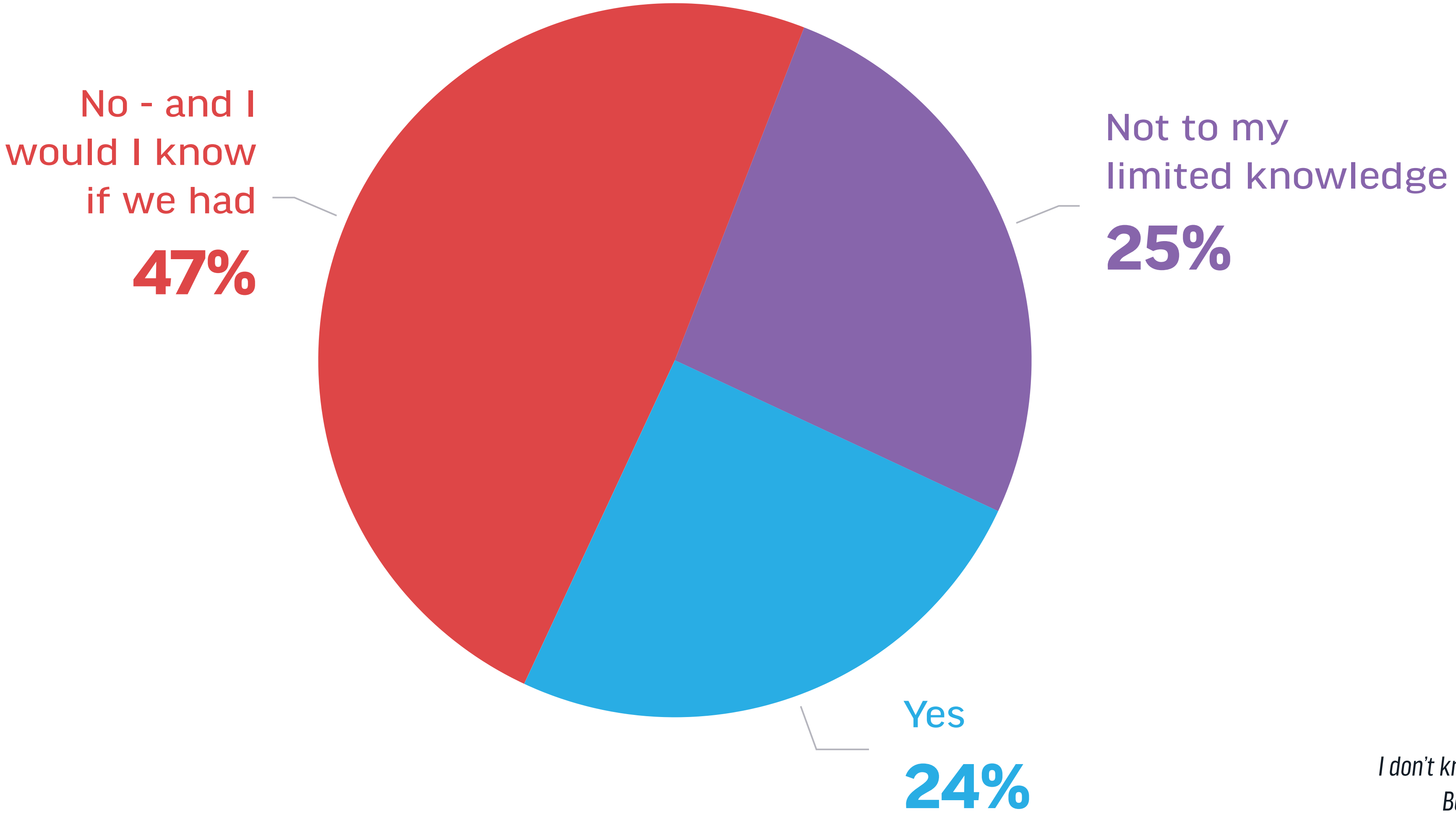


3.7 Average ranking

Base: 165

THE RISK OF MAJOR SECURITY INCIDENTS AMONG AGENCIES

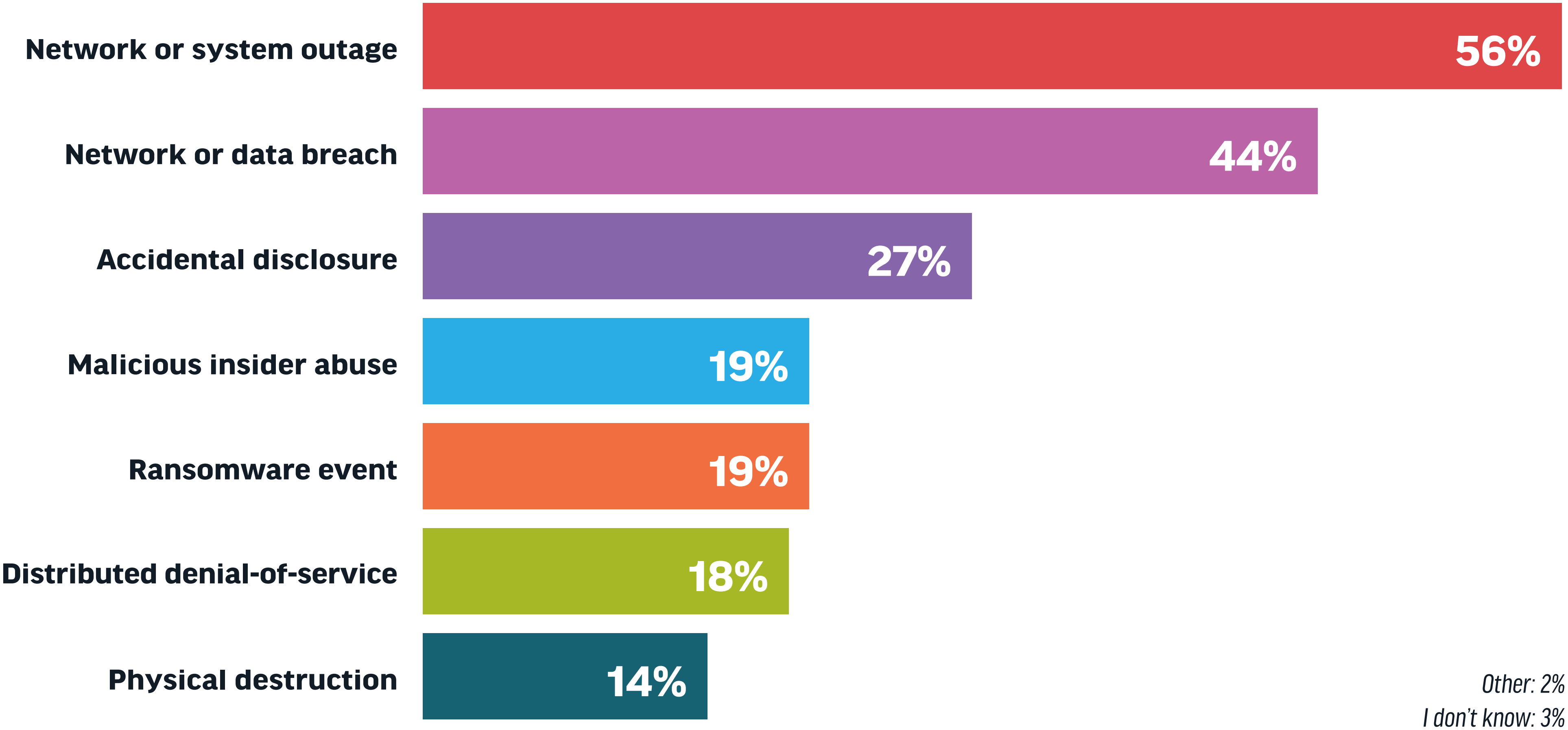
Has your organization experienced a major security incident that impacted its security resilience?



I don't know: 4%
Base: 165

SECURITY INCIDENTS WHICH HAVE IMPACTED AGENCIES

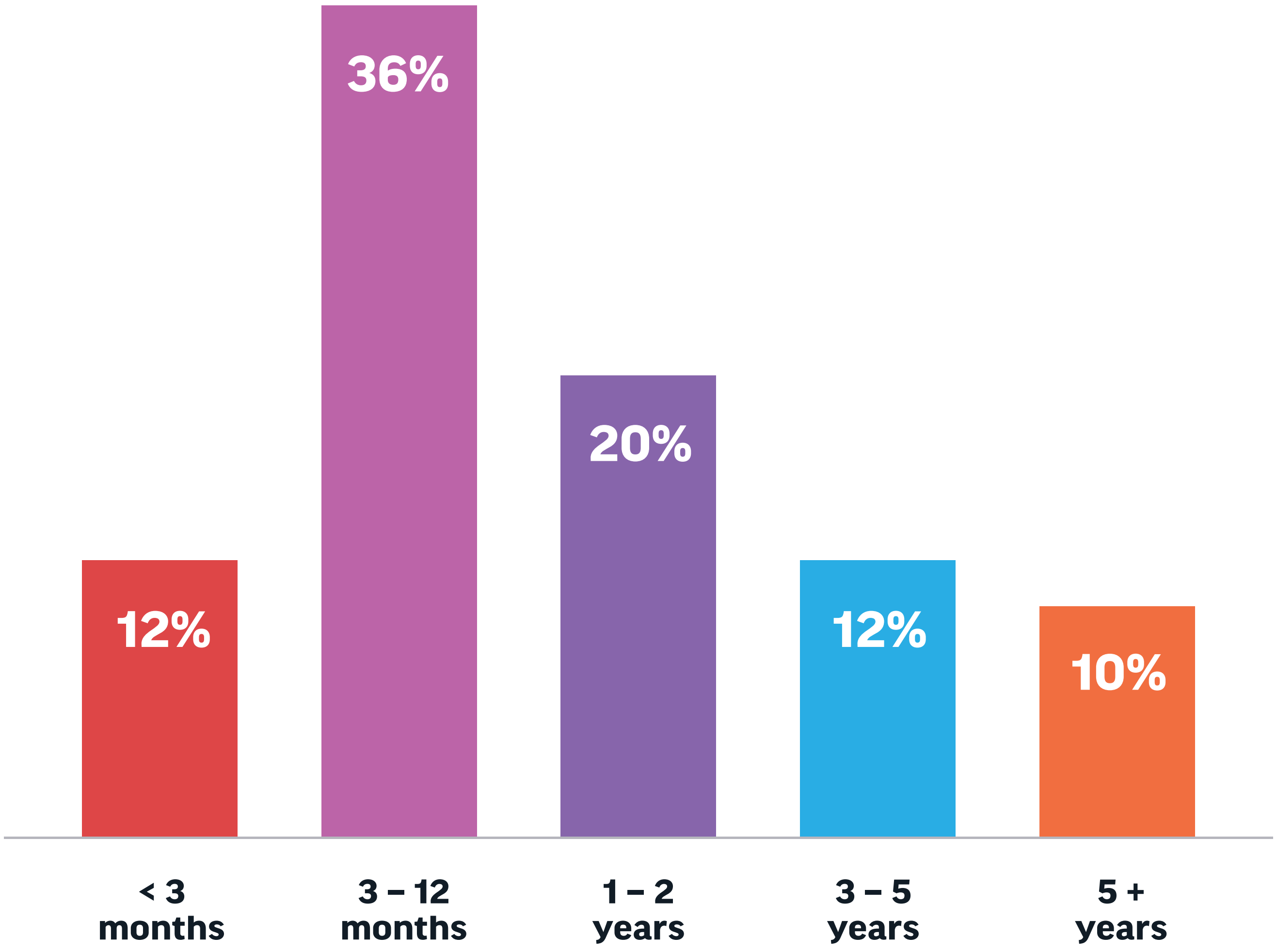
Which of the following security incidents have impacted your organization in the past?



Other: 2%
I don't know: 3%
Base: 165

TIME SINCE LAST KNOWN SECURITY INCIDENT

How long ago did the most recent cybersecurity incident occur?

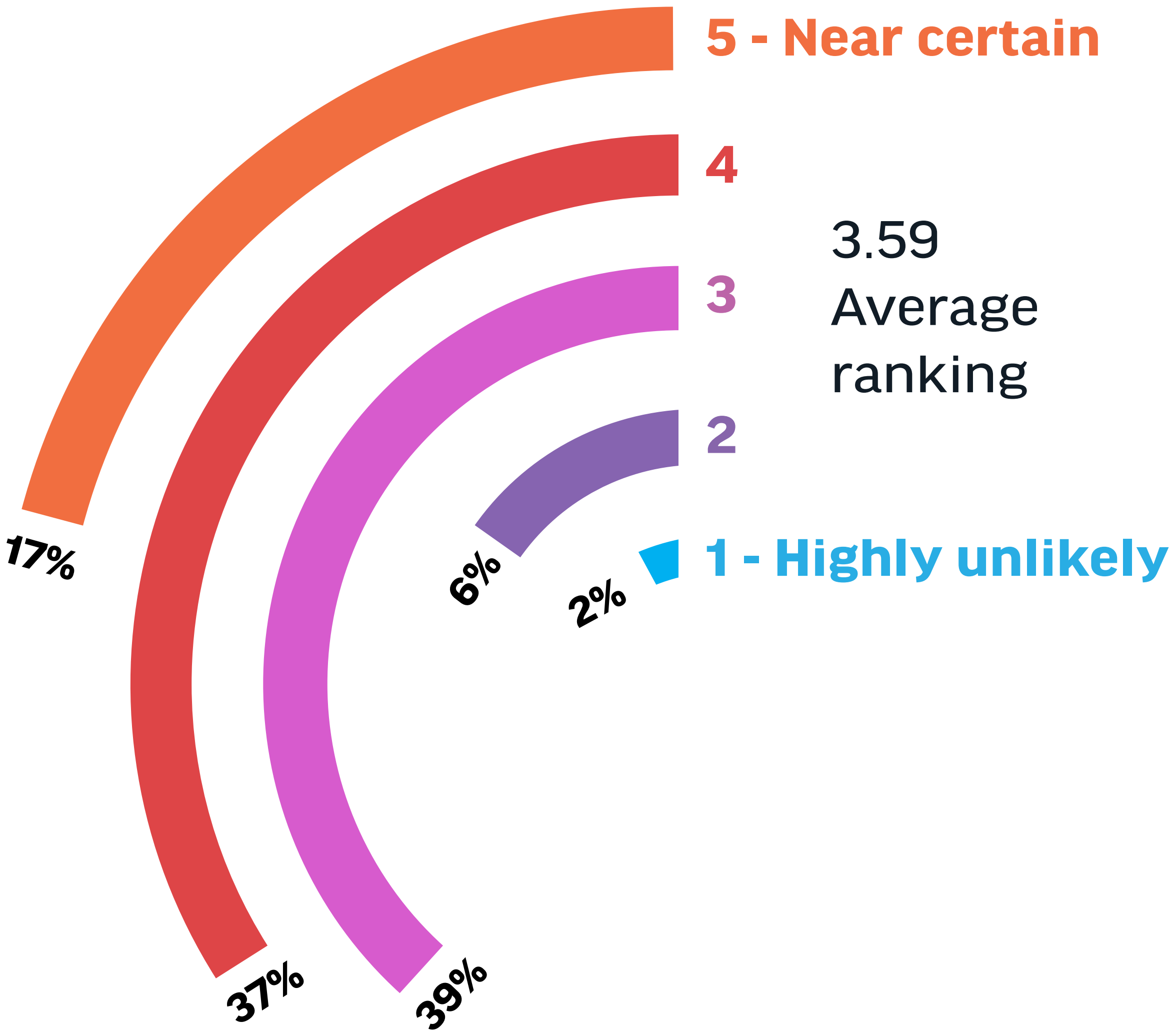


I don't know: 10%

Base: 165

HOW RESILIENT AGENCIES ARE AGAINST SERIOUS SECURITY INCIDENTS

How likely is it your organization would remain resilient through a worst-case (but still plausible) security incident if it occurred today? Rank: 1 — "Highly unlikely" to 5 — "Near certain"



Base: 165

LEADERS WHO OWN SECURITY RESILIENCE DECISION-MAKING AUTHORITY

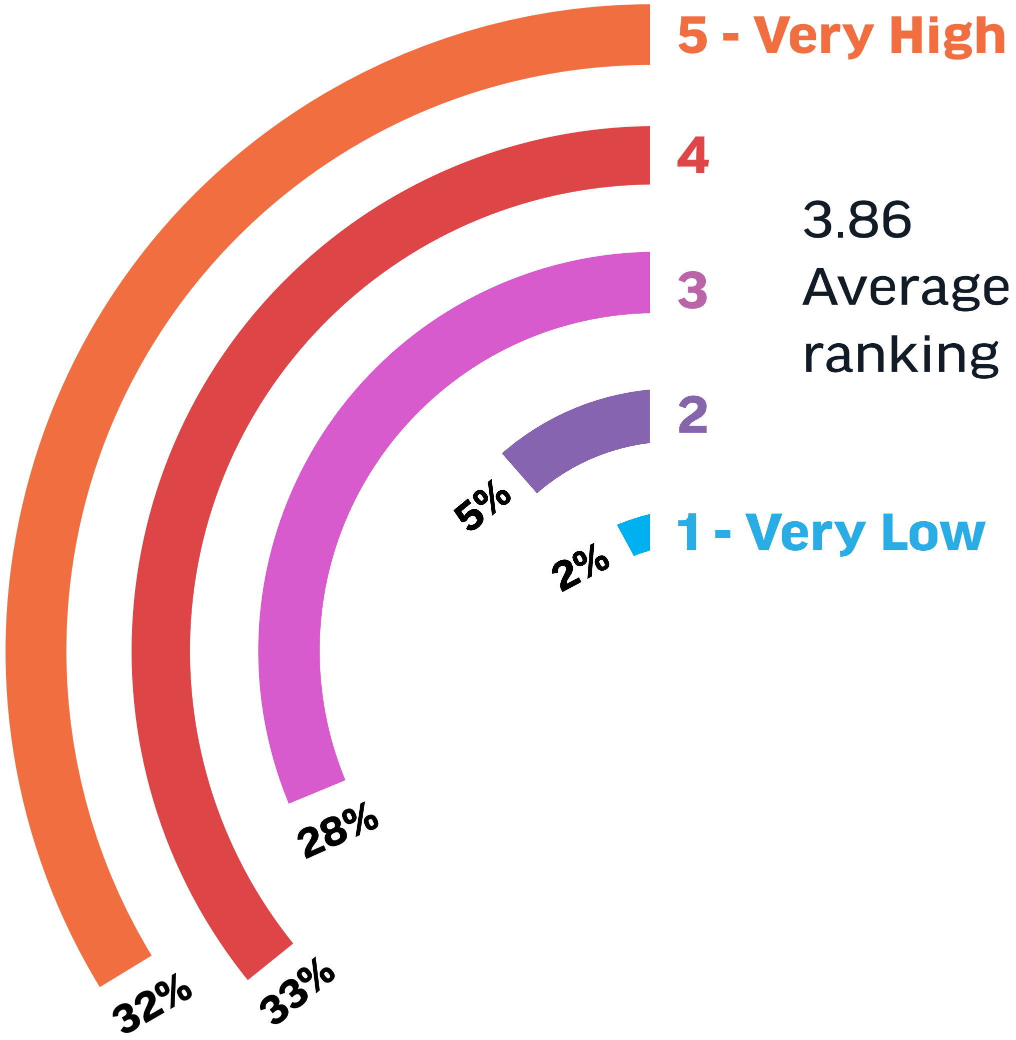
Who has primary responsibility for ensuring security resilience in your organization?

27%	CHIEF INFORMATION SECURITY OFFICER (CISO)
19%	CHIEF TECHNOLOGY OFFICER (CTO)
16%	CHIEF INFORMATION OFFICER (CIO)
15%	CHIEF OPERATING OFFICER (COO) / DEPUTY ADMINISTRATOR
13%	CHIEF EXECUTIVE OFFICER (CEO) / ADMINISTRATOR
1%	OTHER (IT DIVISION CHIEF, MANAGER)

I don't know: 9%
Base: 165

THE IMPORTANCE TOP EXECUTIVES PLACE ON SECURITY RESILIENCE

How important is security resilience for top executives at your organization?
Rank: 1 — "Very Low" to 5 — "Very High"



Base: 165

AGENCIES' BIGGEST CHALLENGES TO USE MODERN IT RISK MANAGEMENT TOOLS

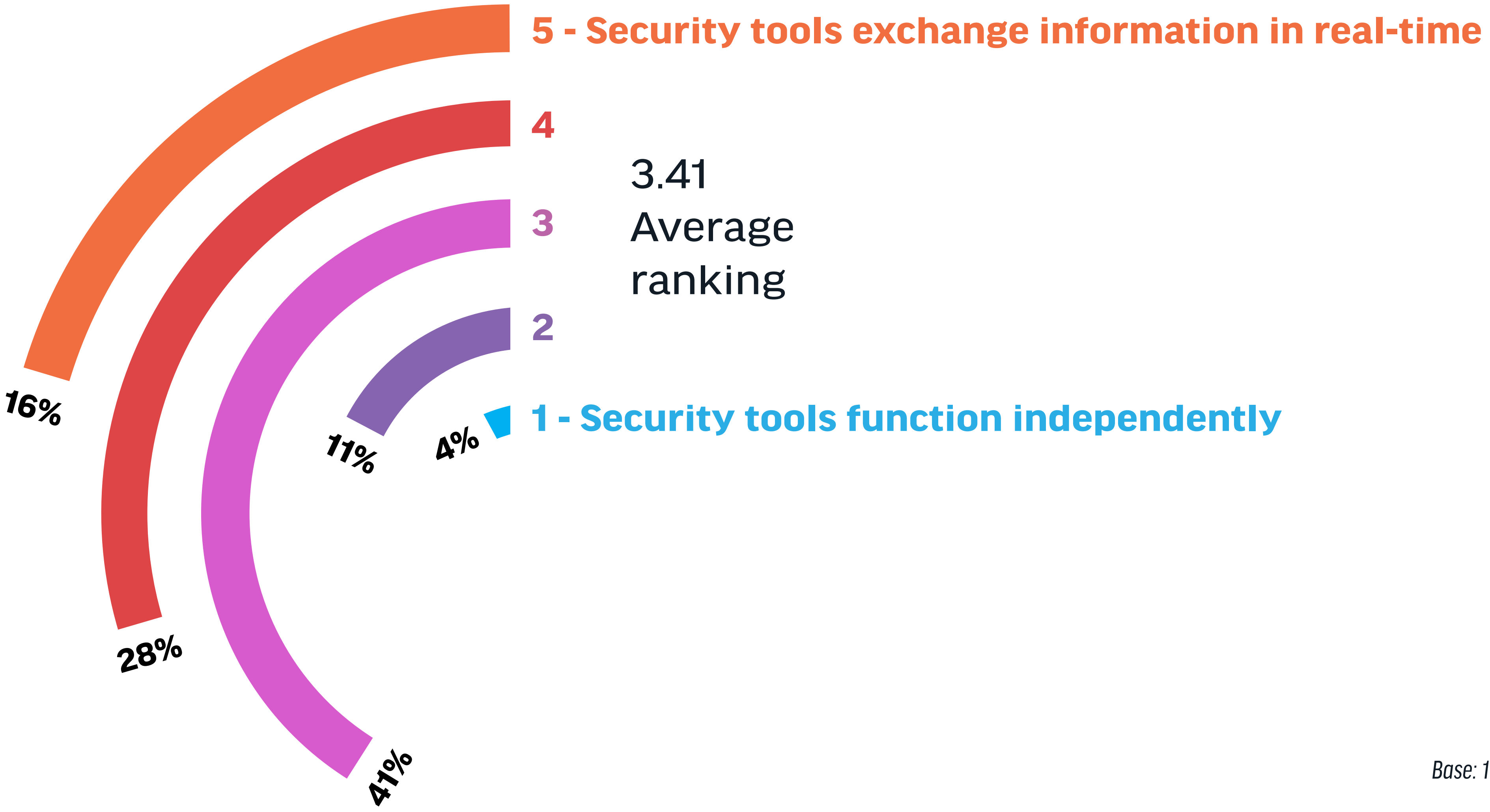
What are your organization's biggest challenges to implement modern IT risk management tools? (Select up to three)

Keeping up with the demands and growth of the mission	40%
Creating a security culture embraced by all employees	33%
Adapting to unexpected external change events or trends	30%
Containing the spread or scope of security incidents	30%
Preventing major security incidents and losses	27%
Continuing to mature and improve security capabilities	25%
Maintaining a cost-effective security program	22%
Recruiting and retaining talented security personnel	13%
Mitigating financial losses from security incidents	13%
Ensuring business continuity through disruptive events	10%

I don't know: 9%
Base: 165

THE LEVEL OF INTEGRATION OF AGENCIES' SECURITY TOOLS

How integrated are your organization's security tools?
Rank: 1 — "Most security tools function independently" to 5 — "Most tools can exchange information in real-time"

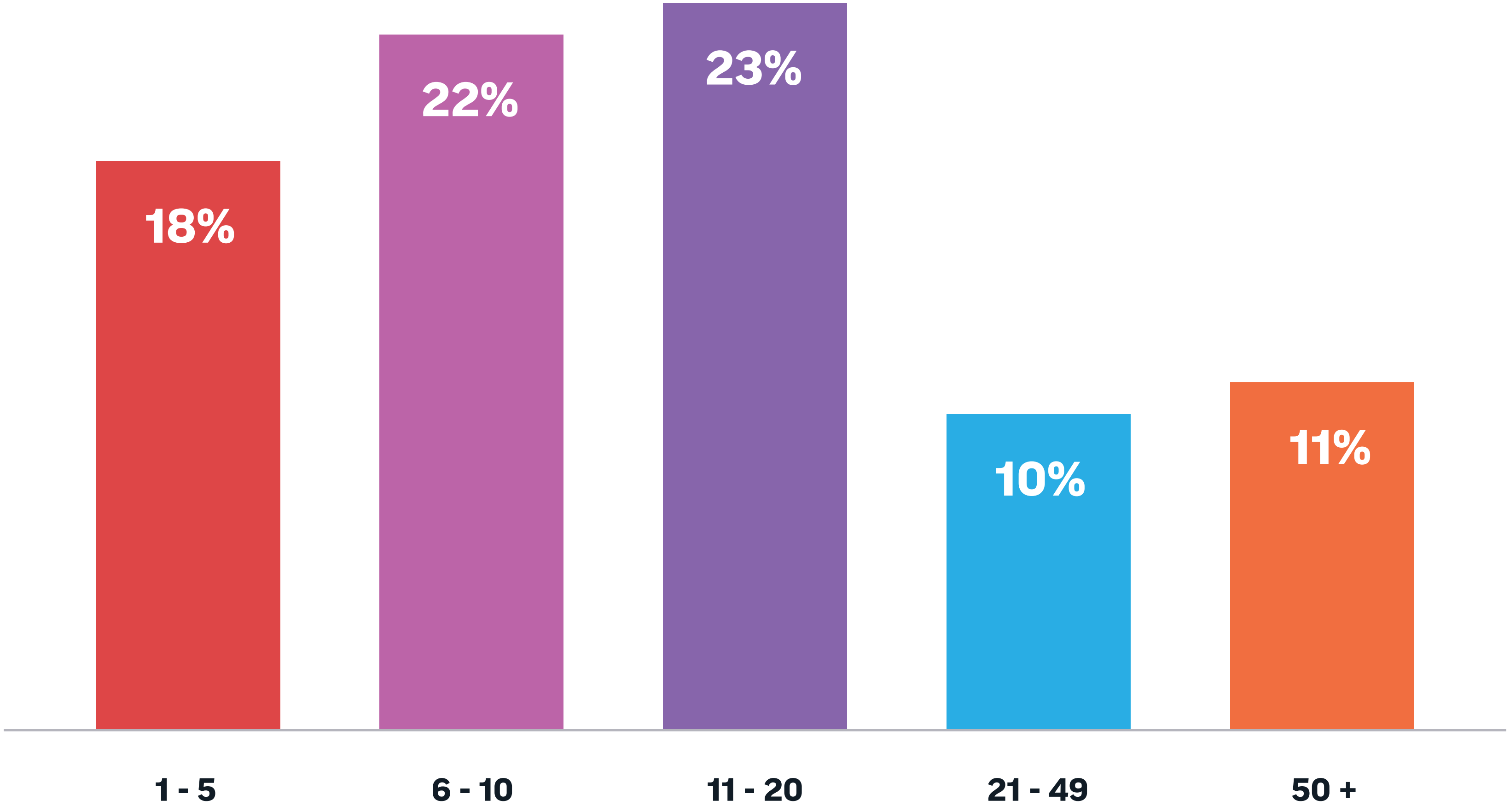


3.41
Average
ranking

Base: 165

THE NUMBER OF SECURITY VENDORS AGENCIES CURRENTLY USE

How many different vendors (i.e. brands, manufacturers) are currently used across your security technologies?

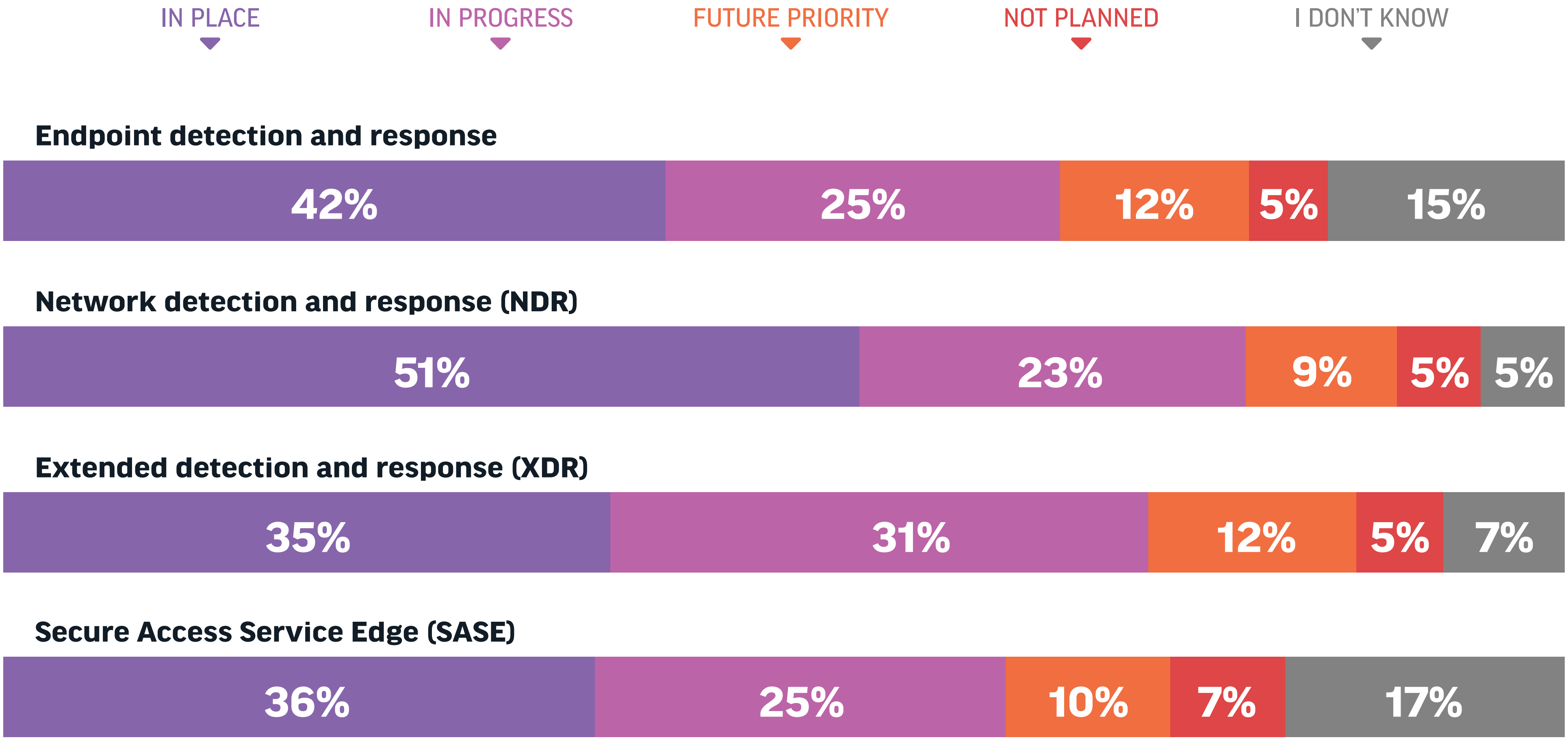


I don't know: 5%

Base: 165

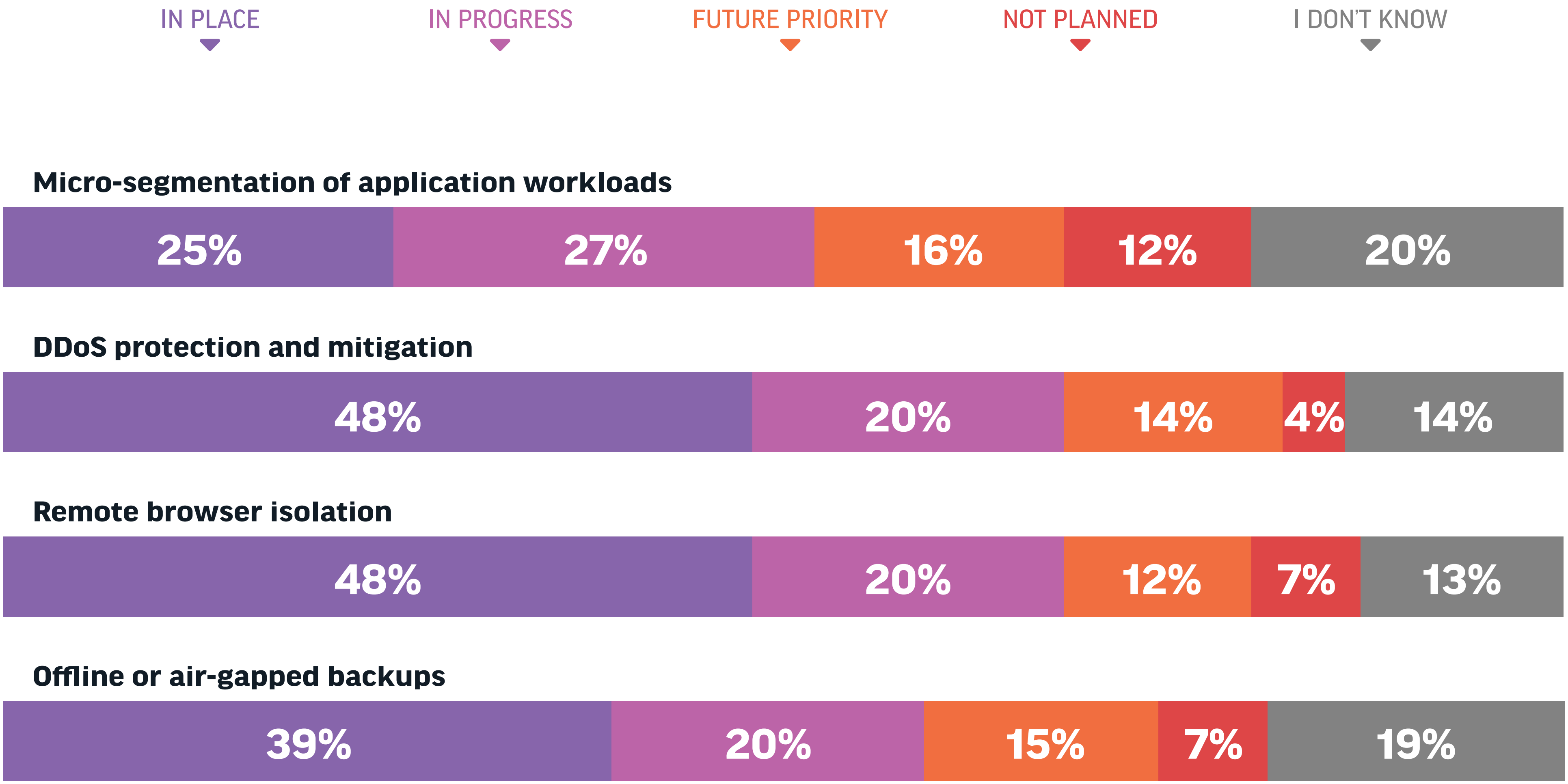
MODERN SECURITY DETECTION TOOLS

Which of the following are already in place, currently in progress, or planned for future implementation to improve security resilience at your organization?



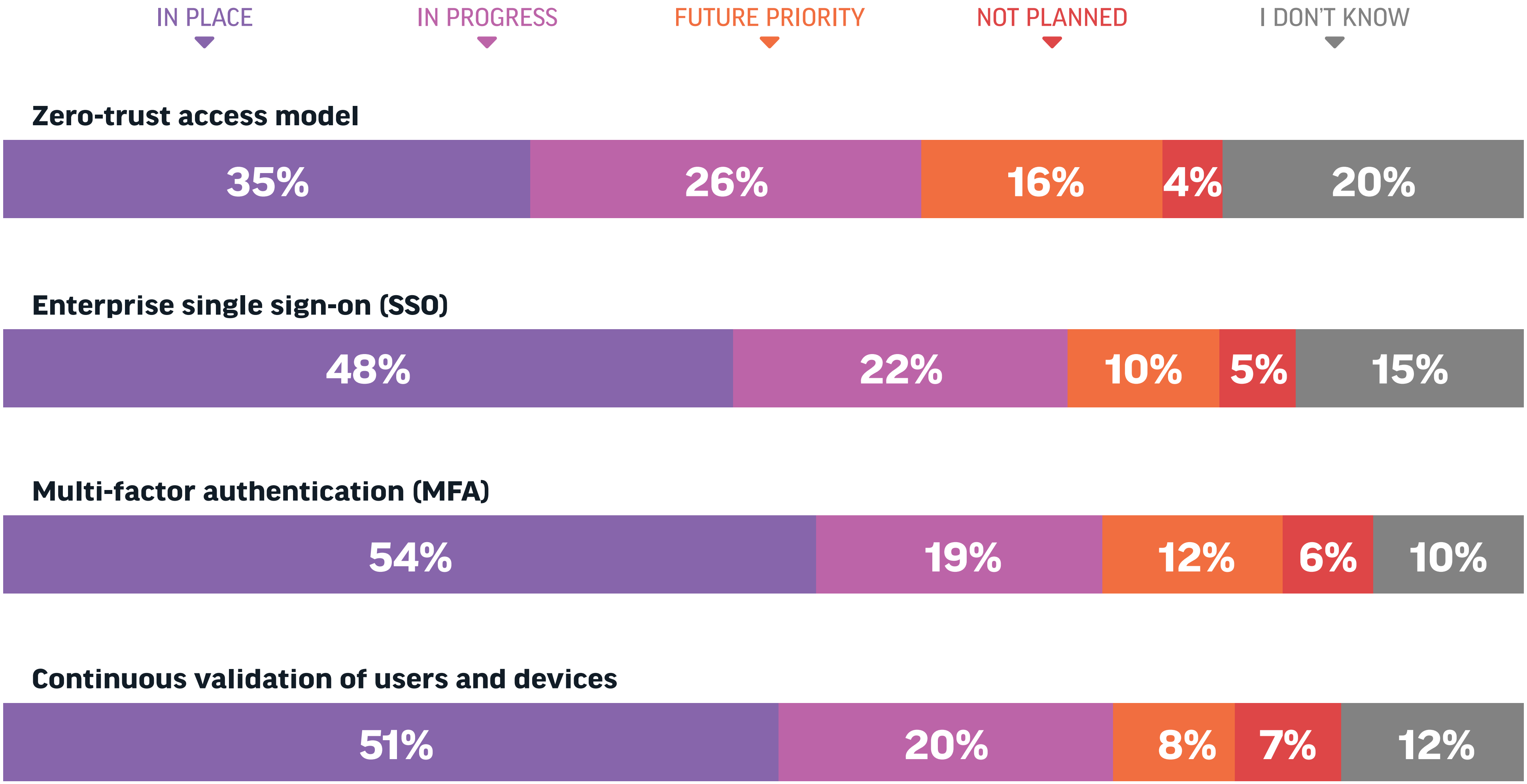
MODERN SECURITY CAPABILITIES

Which of the following are already in place, currently in progress, or planned future implementation to improve security resilience at your organization?



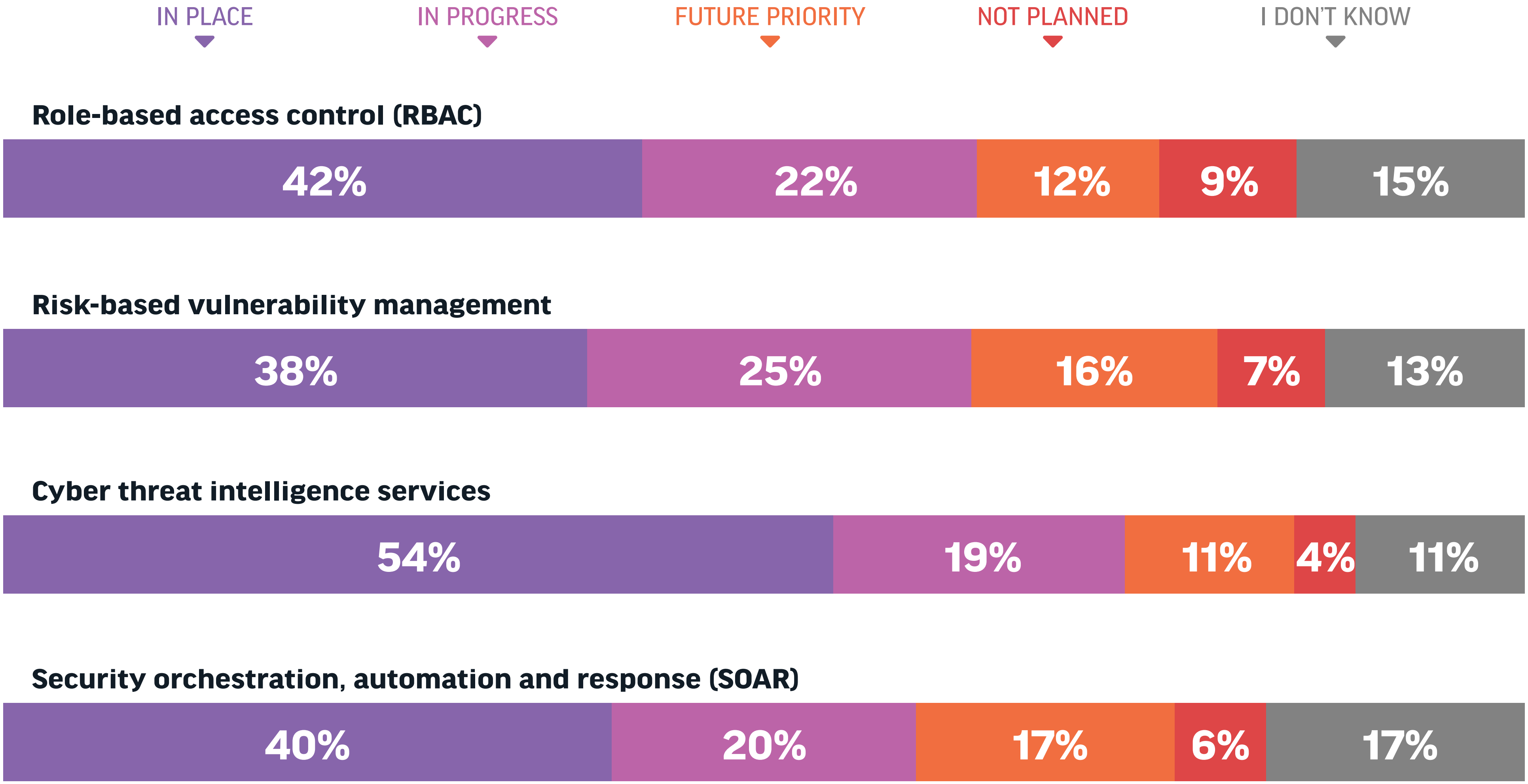
MODERN SECURITY POLICIES & CAPABILITIES

Which of the following are already in place, currently in progress, or planned future implementation to improve security resilience at your organization?



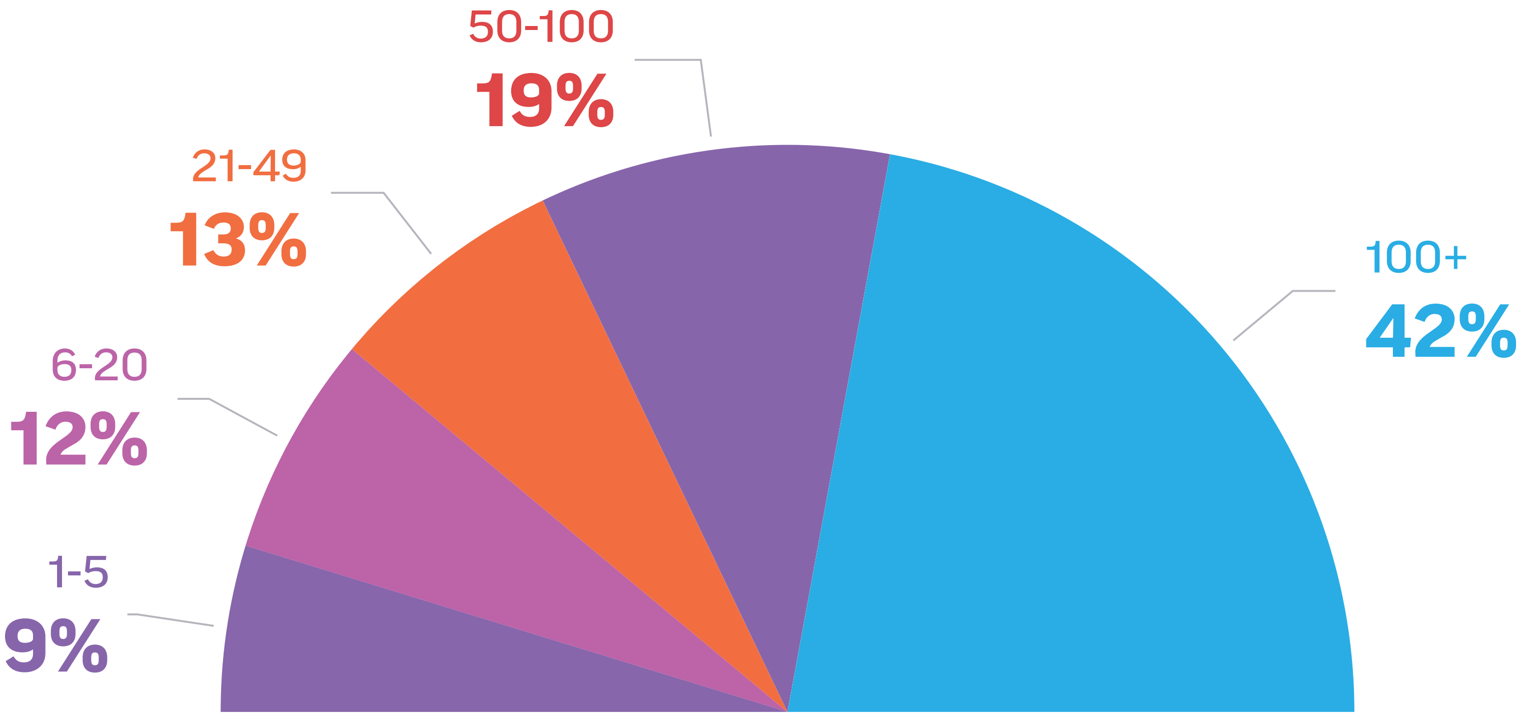
MODERN SECURITY POLICIES & CAPABILITIES

Which of the following are already in place, currently in progress, or planned future implementation to improve security resilience at your organization?



STAFF SIZES AT AGENCIES IN DEDICATED SECURITY ROLES

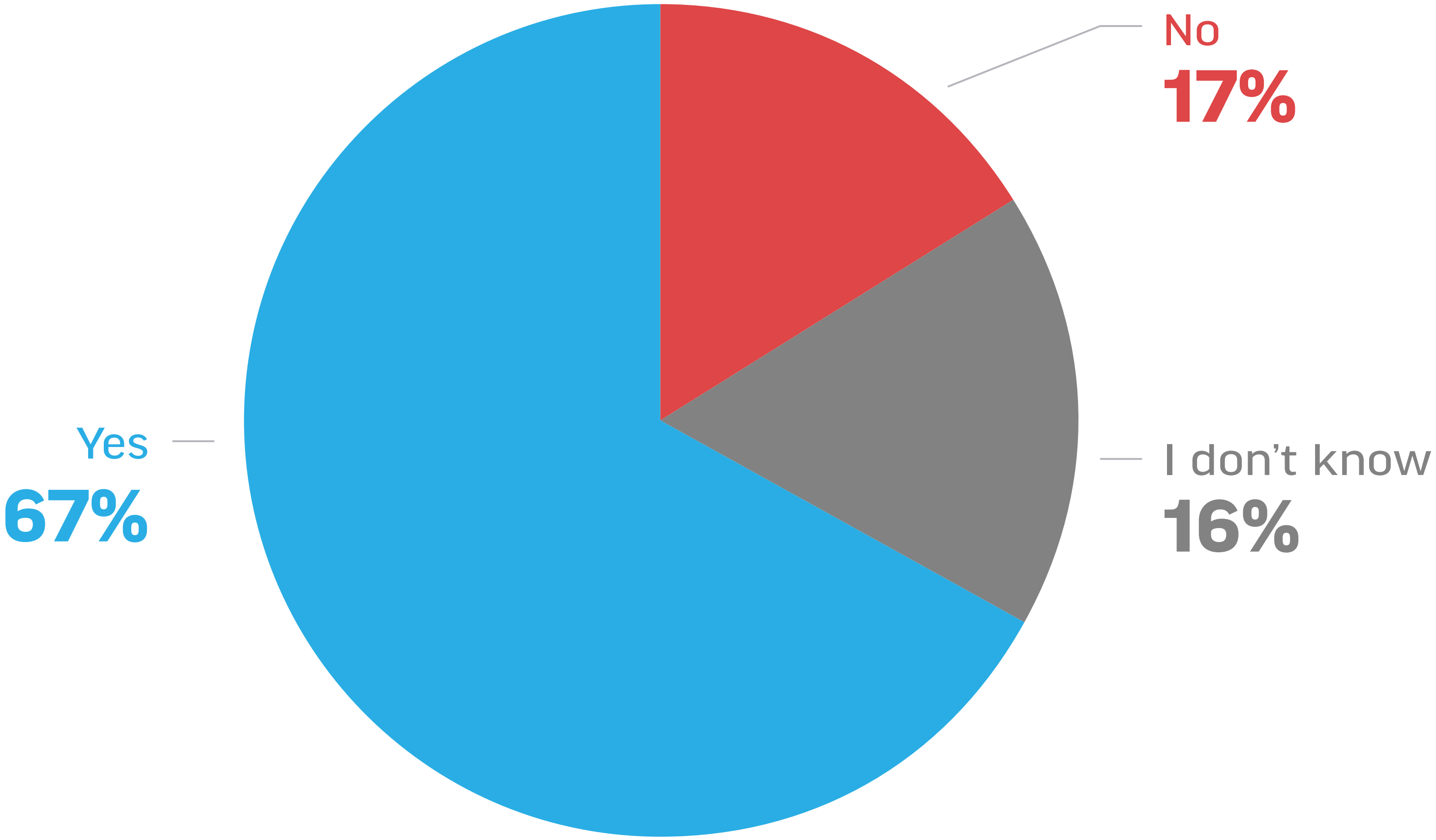
How many employees / contractors in your organization have dedicated security roles?



I don't know: 5%
Base: 165

AGENCIES' USE OF EXTERNAL RESPONSE SERVICES FOR UNEXPECTED CYBER EVENTS

Does your agency retain external response services to better respond to unexpected cyber events that might otherwise endanger resilience?



Base: 165

CONCLUSIONS

Meeting security needs

Agencies have come a long way in building security resilience within their organization. That said, more than half of respondents reported that their organization experienced a network or system outage in the past, and 44% experienced a network or data breach. In response, respondents report that their agencies have implemented endpoint detection and response (42%), network detection and response (51%) and over a third have extended network detection and secure access service edge in place to improve security resilience.

How the mission can impact security

The ability to implement modern IT risk management tools, however, is often hampered by the growth and demands of agency missions (40%), the lack of security culture embraced by all employees (33%), or the ability to adapt to unexpected external change events or trends (30%). Investing further in zero trust access, multi-factor authentication and continuous validation of users and devices are seen as key paths to mitigate security resiliency risks.

A need to improve security tool integration

More than half of respondents ranked their security tool integration as average to below average (e.g., “security tools function independently”). The number of tools in use partly hampers efforts to improve integration: 44% of respondents reported having 11 or more different security technology vendors working across their IT environment. Dispersed sources can limit visibility and leave agencies open to security threats.

A push to modernize security architecture

The report shows agencies are at varying levels of integration for modern security capabilities and policies. As leaders continue to push towards an integrated security architecture, they will want capabilities that support the ability to learn and adapt to changing security needs. That includes modern system management, integrated threat intelligence and the ability to integrate with other vendor security products and solutions using open-industry standards. It would be valuable for leaders to consider how modern route/switch and WAN solutions can improve their agencies overall security architecture and ensure scalability of networks to handle future growth.

Security incidents

Nearly half of the respondents reported their agency experienced a major security incident within the year. Cyberthreat actors, insider risks and network resiliency issues are expected to grow more difficult as agencies’ IT environments grow in complexity. Agency leaders will need to invest in newer tools that include extended detection and response, endpoint detection or secure access service edge to mitigate risks in their expanding environments and comply with frameworks, Executive Orders, and grant programs. Additionally, two-thirds of respondents said their agency now retains external response services to better respond to unexpected cyber events that might endanger resilience.

FEDSCOOP

FedScoop is the leading tech media brand in the federal government market. With more than 4.3 million monthly unique engagements and 202,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify ways to achieve common goals. With our website, newsletter and events, we've become the community's go-to platform for education and collaboration.

CONTACT

WYATT KASH
Senior Vice President Content Strategy
Scoop News Group
Washington, D.C.
202.887.8001
wyatt.kash@scoopnewsgroup.com