2024

CYBERSECURITY BUYERS REPORT

ActualTech
A FUTURE COMPANY

IN PARTNERSHIP WITH:

CYBERSECURITY MARKETING SOCIETY

In This Report

Introduction

To the Cybersecurity Marketer,

How can you capture the attention and interest of the enterprise cybersecurity buyer?

Once that attention and interest has been piqued- how can you 1) establish credibility and trust, 2) decipher buyer-organization dynamics, and 3) plan for maintaining sales momentum through extended, multi-month-long decision and procurement cycles?

Cybersecurity marketers face these challenges and more. Go-to-market messaging needs to match prospect pains, meetings for sales must be secured and expertise demonstrated to a sufficient level to build confidence in a purchase decision.

Without a doubt, these demands are much easier to meet when marketers are equipped with the data needed to limit guesswork regarding prospect challenges, needs, and requirements.

To that end, this Cybersecurity Buyers Report, prepared by ActualTech Media in partnership with the Cybersecurity Marketing Society, was developed to provide hard-to-get answers to the cybersecurity marketer's most burning questions.

In late 2023, ActualTech surveyed our audience of cybersecurity professionals and decision makers to glean:

This report provides intelligence and data points that will allow marketers to 'skip the guesswork' and better understand prospect challenges, needs and requirements.

1. The current **size, state, and sophistication** of their cybersecurity programs.
2. Their **top technology priorities**, including most-pressing threat concerns and overall IT-centric business goals.
3. The elements of their security stack they're **currently outsourcing** and what they're planning to outsource in the near future.
4. Their **buying and vendor selection process**, decision criteria, proof-of-concept concerns, and budgeting timelines.
5. The **marketing modalities and channels** that they find most valuable.

RESPONDENT DEMOGRAPHICS

For this report, ActualTech surveyed 327 senior cybersecurity professionals and decision makers at organizations of all sizes who have dedicated cybersecurity teams in the United States. Respondents were CISOs, Directors and Managers of Information Security, Data Privacy Officers, Senior Cybersecurity Analysts and similar roles. While all organization sizes were surveyed, **the data shown in the charts in Part 1 was filtered for companies of 500 employees or more.** Data from organizations below 500 employees is included in the Appendix. The questions were developed in consultation with the Cybersecurity Marketing Society.

In addition to the decision-maker data shown in Part one of this report, ActualTech surveyed the audience for in-depth insight into their current stance and planning for nine key areas of the cybersecurity technology stack, including:

- API Security
- Application Security
- Cybersecurity Insurance
- Data Security & Governance
- Endpoint Security
- Human Security
- Identity & Access Management
- Infrastructure & Network Security
- Security Operations

The results and insights for these survey areas are included in Part two of this report. Cybersecurity marketers can use these data points (and the surrounding takeaways) to better their align product positioning and messaging with real-world customer requirements.

While ActualTech Media is not a professional research firm, our access to the minds and trust of the cybersecurity professionals and decision makers in our audience uniquely positions us to gather answers to questions that other firms may not be able to procure, and then present that data through a marketing lens. It's our hope that this report makes your job as a cybersecurity marketer more data-informed and intentional.

OK, let's dig in!

– Geordie Carswell, CMO, ActualTech

NOTE

Part one of this report gives cybersecurity marketers important insights about their potential customers. It offers quick tips and actionable takeaways for cybersecurity marketing strategies. Instead of going into a detailed analysis of the data, it highlights brief key points that are designed for quick action.

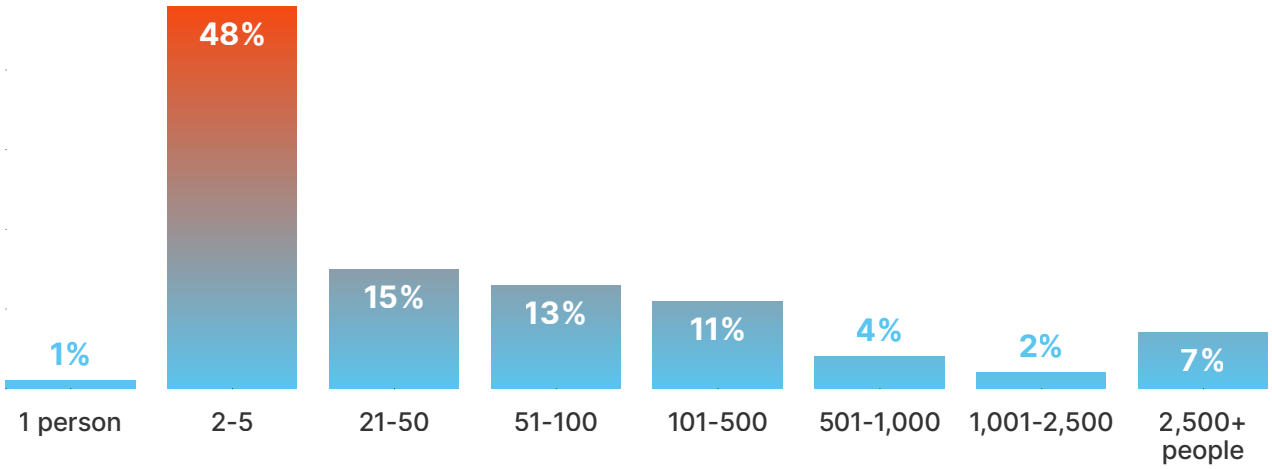
PART 1

Cybersecurity Decision Makers

LEVEL-SET AND DEMOGRAPHICS

Q1

How large is your overall information security team?



On nearly every information security team there is likely to be some level of specialization in roles happening, with no one person handling *every* aspect of cybersecurity.

At the same time, members of teams of 2-5 indicate that they are wearing multiple 'hats'- personally handling several areas of cybersecurity inside their organization.

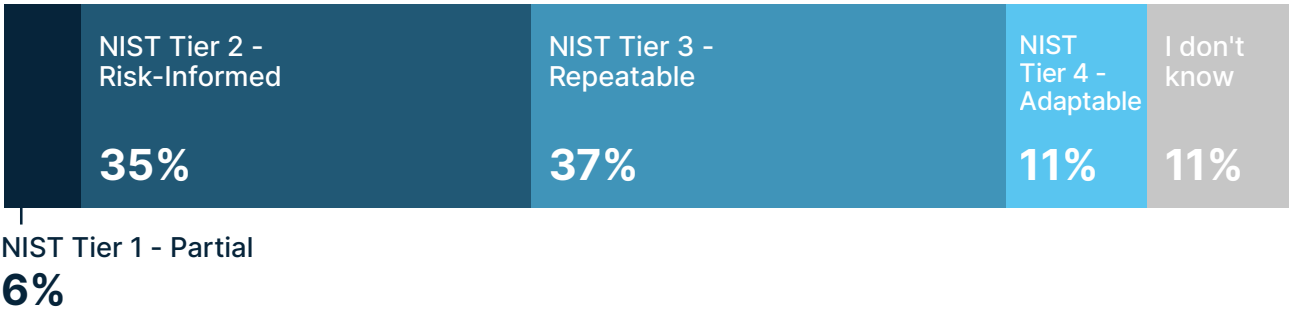
One takeaway here is that if even if your solution niche is small and your ICP is narrow, it's important to realize that responsibility for that function is likely being done by someone who has other things on their plate. Empathetic messaging and a focus on communicating the efficiency gains your solution can bring will strike a chord.

Even in organization sizes above 5,000 employees, 2-5 person teams still account for 20% of all teams. These people are likely to be overloaded and perhaps more open to outsourcing certain functions for relief.

Empathetic messaging and communicating the efficiency gains your solution can bring will strike a chord.

Q2

Describe the maturity of your cybersecurity program.



41% of respondents lack maturity in their cybersecurity program.

Some takeways: Their teams are likely still hungry for information about how to mature. As individuals, they're likely sensing that the world of cybersecurity is advancing faster than they can keep up with, and they'll be grateful for—and trust you more for—training them to know what's important (not in your self-serving story, but what's *really* important in the big picture) and helping them get better at their job.

The 48% who have more maturity (tier 3 and tier 4) want to keep it that way. They've worked hard for this level of maturity, and the rest of the business and customers now expect it. So, they're probably looking for an “edge”, or tips to help them stay one step ahead of the bad guys. Often, this level of cybersecurity maturity comes bundled with a high degree of confidence which, in unhealthy cases, can present as arrogance. While these folks are looking for an edge and are interested in new information, be careful not to talk down at them or accidentally insinuate that you know everything, and they know nothing in your quest to teach and offer useful insights.

The fact that 11% of cybersecurity decision makers *don't know* whether their organization is mature should be concerning. This seems like an opportunity to offer a rubric for evaluation or some training on assessing maturity and developing an action plan to create growth.

88% of respondent’s organizations (if you include the “I Don't Knows”) rank short of the top tier, which means there's plenty more work to do in helping cybersecurity departments mature. Again, tools and training for doing this will be helpful and build trust.

88% of respondent’s organizations rank short of the top tier, which means there's plenty more work to do in helping cybersecurity departments mature.

Q3

What are your company's key cybersecurity tech stack components/solutions?

Human security/training and identity access management have traction inside larger organizations, so marketers may now be able to focus on speaking to their differentiators rather than just the need to implement a program in the first place.

Only 50% report having cyber-risk insurance, representing a big opportunity for growth for insurance providers.

Under 50% have implemented SecOps to-date. This represents a big growth opportunity for vendors and MSPs in this area. An opportunity also exists for messaging around "operational maturity" and tools that enable that. Messaging should reinforce that security needs to become an integrated part of operations as opposed to a bolt-on or an afterthought.

Only 50% report having cyber-risk insurance, representing a big opportunity for growth for insurance providers.

Interestingly, Endpoint Security ranks as the top "key" technology. To some extent, this likely means that even though organizations are starting to train users well (eg. the Human Security & Training item), the primary concern is still protecting the client vector at a technology level.

Any of the areas that are "high-touch" for professionals could be outsourcing and/or automation solutions opportunities.

DRIVERS/PAINS FOR ACTION

Phishing is by far the top threat priority, obviously connected to ransomware and malware. Messaging that focuses on prevention, resilience and recovery is likely to resonate.

A big opportunity exists if your solution makes patching zero-day exploits easier through automation.

People are still the most significant vulnerability.

All of the highest-ranked items include "the human element". People are still the most significant vulnerability. Human element concerns should equate to training opportunities that could be served by vendors or MSPs in the space.

If your solution covers off multiple areas here in an integrated way, that's a good message. Think of using messaging like "who wants to handle each of these with individual tools?"

Q4

What threats are you prioritizing right now?

(Select all that apply and rank highest to lowest priority)

1	Phishing attacks
2	Ransomware
3	Malware
4	Zero-day exploits
5	Social engineering
6	Password attacks
7	Insider threats
8	Distributed denial of service (DDoS) attacks
9	Supply chain attacks
10	Shadow IT
11	Man-in-the-middle (MitM) attacks
12	Physical security breaches
13	Other

Q5

What are your overall corporate IT priorities or investments in the coming year?

(Select 5 and rank highest to lowest priority)

1	Cost optimization and efficiency
2	Cloud migration
3	Cybersec investments
4	Digital transformation projects
5	App/stack/tech modernization
6	Regulatory/compliance projects
7	Resiliency/business continuity projects
8	Data projects
9	Talent
10	Supply chain efficiencies/ improvements
11	Other

If your solution helps reduce cost and boost efficiency, that's a message that's going to resonate.

Prove how your solution can help. Think of using more case studies, hard numbers (even if anonymous), ROI calculators, guides like "Guide to Cost Optimization and Efficiency in Cybersecurity (or tool/solution area)".

For modernization or digital transformation projects, messaging around upgrading tools to meet the latest threats or needs could work. Talk about how your solution can accelerate this process. Think about what kinds of content/ assets/tools might help your prospects do this.

- **Cloud migration:** if your solution dovetails nicely with a cloud story, and you can help them make that move and win, that could resonate well.
- **Compliance and regulatory concerns:** Help them solve their pain here. Can your solution make compliance easier to achieve, maintain and report on?
- **Resiliency:** Think about how your solution could help prospects map out how to build, test and maintain resiliency.

Note: "Talent" ranks low here–a few takeaways:

Tools that help you do more with less will resonate. Example: if you lose a team member, you're maybe not backfilling that position. Or from the other angle: if the work demand increases, you're probably not getting extra team members to help.

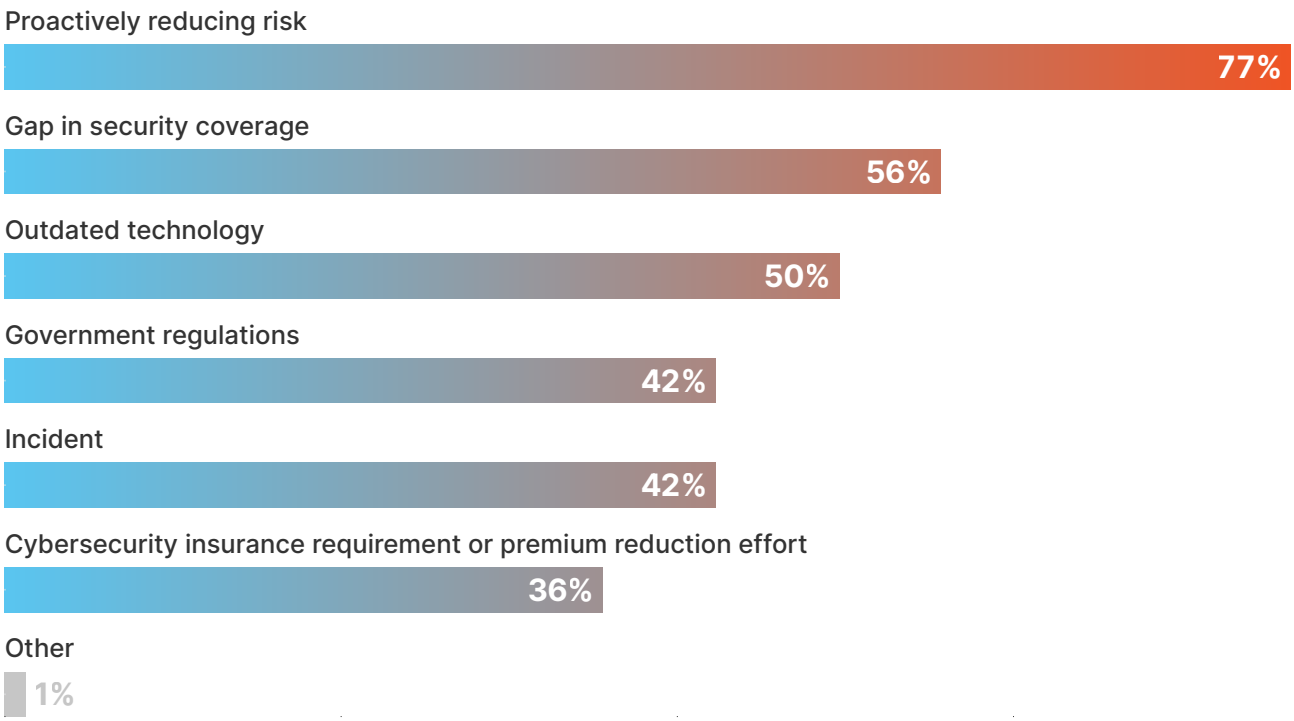
- **For the individual:** getting raises and new jobs is going to be harder, and the bar will be higher; therefore, any knowledge/training/edge you can give the individual to gain their trust, they're going to appreciate.

Because security decision makers won't be able to solve their problems with people, they may be on the lookout for technology that solves the same problems (but which they do have budget for, as opposed to people).

Q6

What are your primary motivators for engaging in a new solution purchase?

(Select all that apply)



Messaging that focuses on risk reduction could be effective. Focus on how your solution helps you be "proactive" or "one-step ahead" of risk.

On a related point, you could reinforce this by using the "Incident" group shown here. For example: *"42.3% of new security solutions are purchased as a result of an incident. Don't let that be you. Purchase proactively now."*

Content assets or lead magnets that focus on "how to cover gaps" in security coverage could be effective.

- **Outdated technology refreshes:** Could you help swing interest your way with "buy-back" or trade-in programs of some sort? This isn't limited just to hardware refreshes, a software "buy-back" program in the form of a discount or credit would also take advantage of this cycle.

If prospects are investing or replacing solutions due to new regulatory requirements, can you explain how your solution helps them become compliant?

If your solution helps prospect organizations comply with several regulatory requirements, consider creating solution landing pages with content that address each one of those areas. One landing or product page alone might not be specific enough to frame your value proposition.

- **Side idea:** Insurance requirements that prospects are facing could be an angle for pitch. Example: How your solution can help them stay compliant with the requirements in their cyber insurance policy.

Q7

What are the primary reasons you would engage with a managed service provider vs. managing a solution in-house?

(Select all that apply)

MSPs and firms that facilitate outsourcing of cybersecurity services will benefit from understanding what leads prospects to the decision to outsource.

Resourcing advantages and expertise gains are the biggest motivators to outsourcing a solution as shown here. Focus your messaging around those two areas. Don't focus exclusively on cost savings-cost savings is a factor but not a leading driver.

It's true, there will always be the bargain shoppers, but overall, people are outsourcing to get your skills and your availability, not to save money.

Further on resourcing advantages, the need for 24×7×365 SLAs that can't be delivered internally alone is driving outsourcing. Marketers can map out what that kind of newly available resourcing would mean to the business and make the infosec team scale more effectively.

- **Reducing busywork to allow for more strategic focus:** think about messaging that speaks to the newfound freedom available to previously overburdened internal resources. Example: "what could you accomplish with these tasks off your plate?"
- **Expertise:** This likely ties to compliance requirements and may represent an opportunity to message how you can help prospects achieve compliance via outsourcing or managed services.

Messaging around how they "can't be expected to keep up with everything, let us help" could resonate.

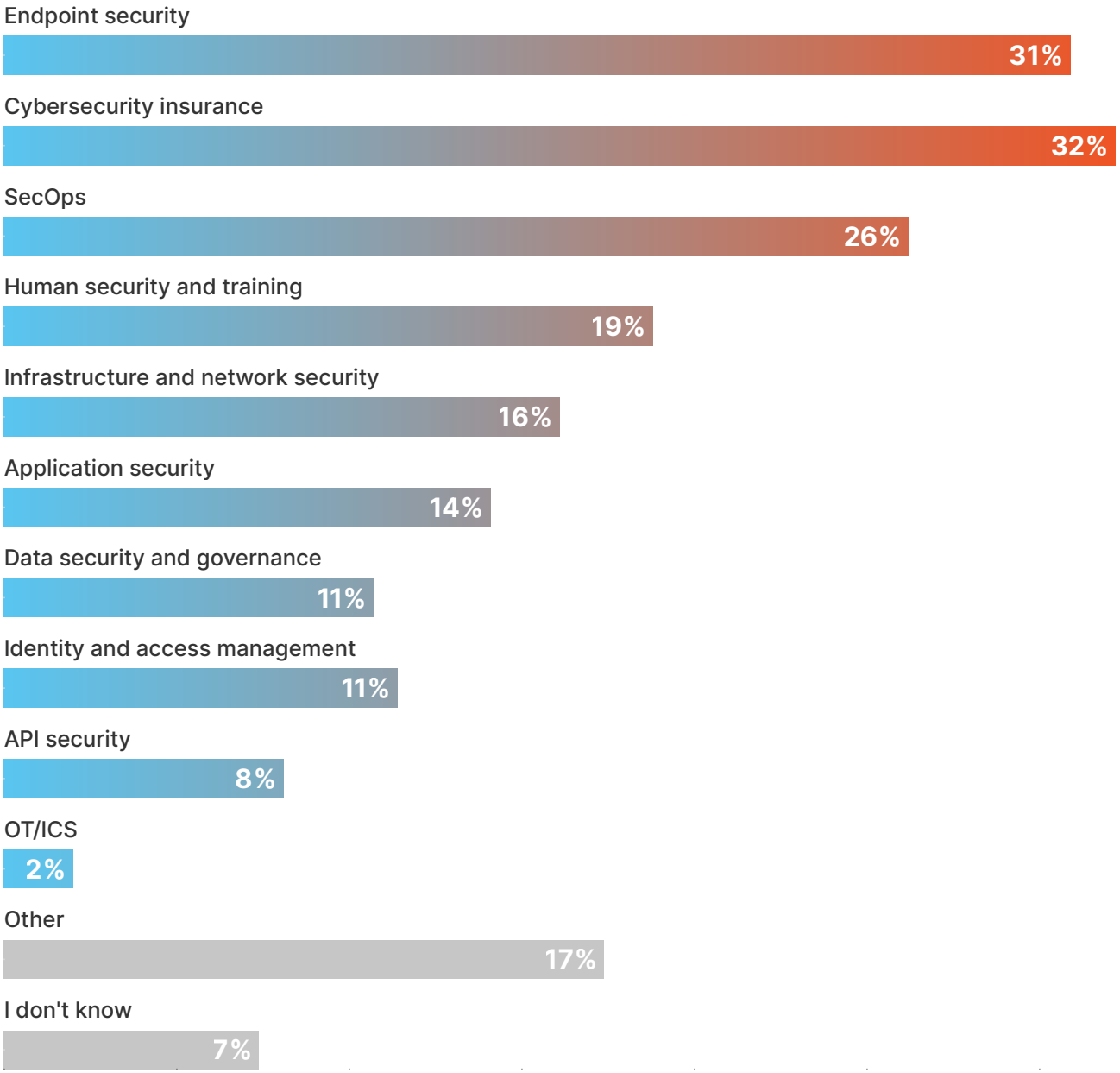
A focus on trust in messaging is important. Prospects are giving you access to their environment at a critical level – everything about your brand should convey that you not only have the expertise to help but they can trust you.

Example: Think social proof, certifications, industry partnerships—"these big partners work with us, we're trustworthy just like them."

Q8

What cybersecurity categories are you outsourcing right now?

(Select all that apply)



If you handle one of the least-outsourced areas, there's a huge amount of headroom to grow your practice area. In fact, all these areas shown have room for growth.

- **Note:** the "other" category shown might as well have been relabeled as "Penetration testing" – this was almost universally the "other" answer entered via an open text field option at 17%.

THE BUYING PROCESS & BEHAVIOR

The key, over-arching point in these data: This is a long game. Both sales and marketing need to be prepared and ready to nurture prospects along with assets, messaging and touch points for each stage.

Q9

How far in advance do you start your budgeting process for cybersecurity solutions?

30 days or less
1%

I don't know
4%

Success in netting a closed/won deal in under three months (from initial discovery to deal), is highly unlikely unless there was an urgent need or incident that precipitated the conversation. Be prepared for a longer sales cycle.

Generally, most prospects are on a 6–12-month purchase cycle. Plan accordingly, both in expectations and forecasting.

Given the budgeting and purchase timelines involved, prospects will need many touch points, awareness efforts, check-ins, value-added offers throughout the process to stay top of mind and in the consideration stage. Plan your marketing around this length of cycle.

To think about: What can you do to get in front of the budgeting process with clients? How can you help them plan their budget? Suggested solutions they can bake into their budgeting process?

Generally, most prospects are on a 6–12-month purchase cycle. Plan accordingly, both in expectations and forecasting.

Trying to get budget allocated for something prospects haven't already thought about or planned for is going to be difficult.

This reinforces importance of getting awareness and nurturing started early. Be top of mind when it comes to budget time, perhaps by giving prospects some ballpark figures to work with. Don't hold back budgetary pricing unnecessarily.

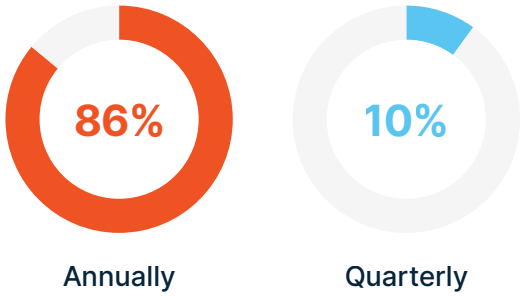
Even when a deal isn't won, start thinking about when a prospect will need to start planning renewal or replacement of the solution you lost out to. Can you start a marketing cadence to help them plan ahead, if even if they didn't go with you on round one? What's the average replacement/lifecycle of solution in your space?

Start thinking about when a prospect will need to start planning renewal or replacement of the solution you lost out to.

Could you help them see how to use budget they already have to solve more problems? For example: they were already going to spend $50,000 on endpoint security, but your tool does endpoint security *and* application security under one umbrella for a similar price.

Q10

Do you budget annually or quarterly?



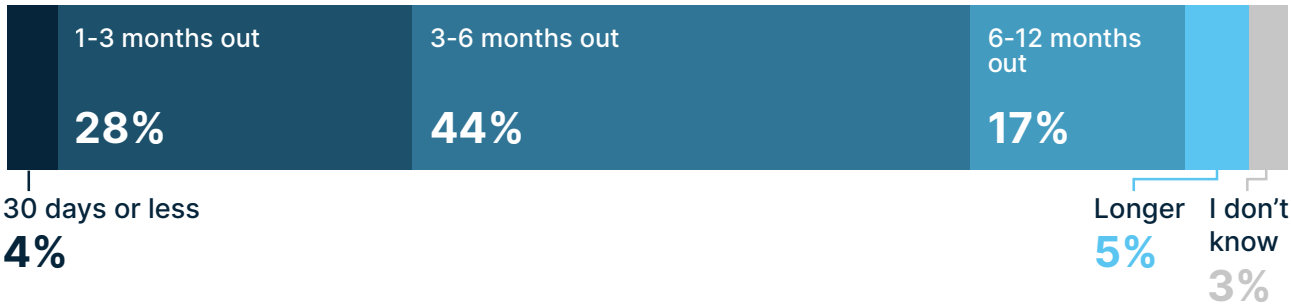
Vendor selection is a months-long process. Be ready for that.

Think about what that slow pipeline movement will mean for your in-progress marketing. How can you keep a consistent cadence of top-of-mind messaging that applies to the pipeline stage they're at?

Is your sales team aware and in-sync with you on how long this process will take and are they prepared and ready to be the distribution channel that you'll be using to get the helpful messaging and assets out to the client as you go? Sales will often have better touch points at these stages.

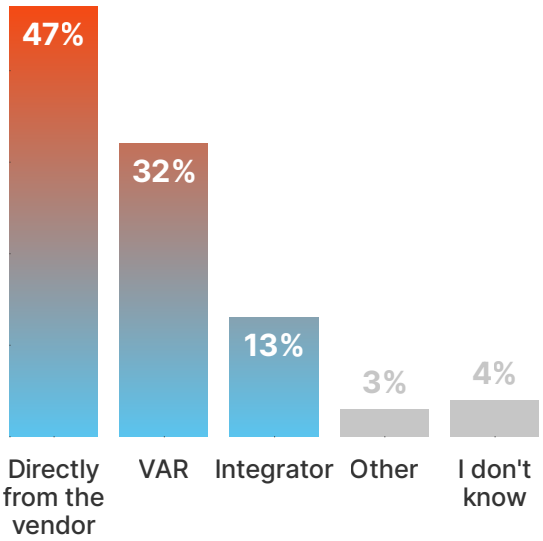
Q11

How long does your typical vendor selection process take? (From research to final decision)



Q12

Where do you typically prefer to procure cybersecurity solutions?



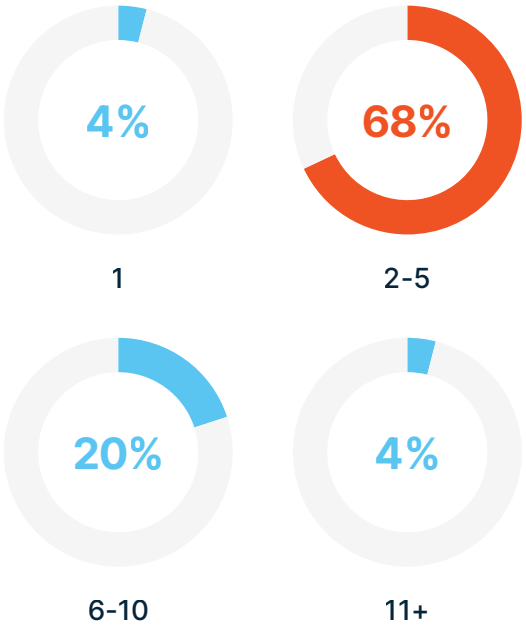
Good news: Buyers are willing to go direct to the vendor a fair bit of the time.

However, you will need also VAR distribution if you want to reach a large portion of the market. What's your current distribution strategy for VARs? Are you providing all the marketing support you can to your VAR or Integrator partners? Are you running programs with those VARs that will help them put you to the front of the line as they go to market?

If a deal originates with you directly, but the buyer wants to go through their VAR or an integrator, do you have the relationships in place to make sure that deal doesn't fall off the table or get routed to another player who is somehow incentivising the VAR to push their solution?

Q13

How many key members or stakeholders are typically on your decision committee for cybersecurity solutions?



Even in larger organizations, the buying committee may be smaller than you think.

For marketers, this is good news: fewer people may need to be targeted to achieve influence over the buying committee.

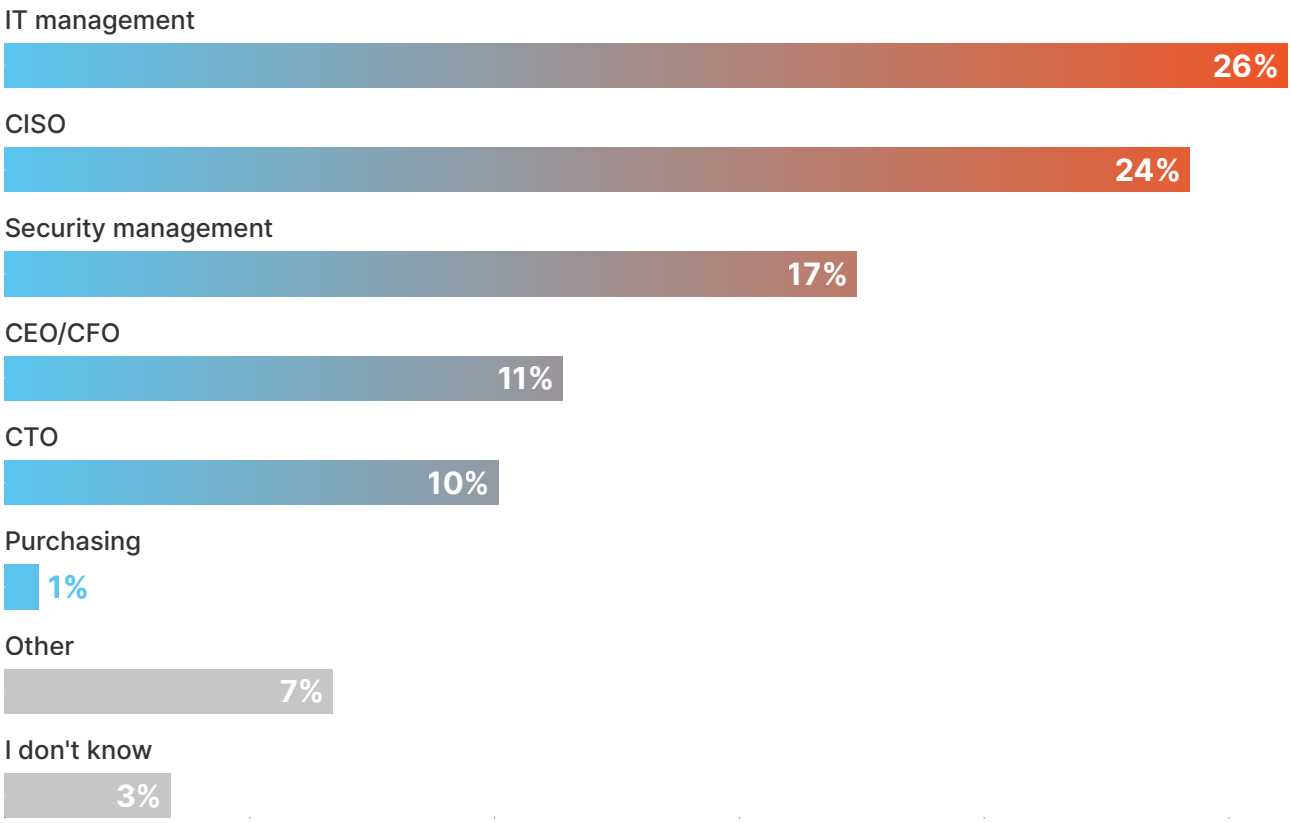
However, in organizations with more than 2500-5000 employees, the decision committee jumps to 11 or more 43% of the time, and 60% of the time in companies over 5000 employees.

As a result, as you look at your ABM account target list, realize that in organizations with 2500 employees and fewer employees, you're looking at a reasonably small stakeholder group to go after.

Above that, you're going to be talking to a lot more people who will care about different things and you'll have to figure out who those people are and what they care about. Your sales team should be able to survey similarly sized organizations in your existing customer base to get an idea of who all is on the committee and what their concerns were or are.

Q14

Who typically makes the final decision?



When it comes to calling the final shots, the decision-makers shown here hold sway.

In organizations with 500 or more employees as shown above, IT management still plays a lead role, followed by the CISO, the security management teams and C-level executives.

However, in organizations over 5,000 employees, the CISO takes the driver's seat with 28% saying that they are the final decision maker, followed by IT Management who are still heavily involved in the final decision-making at 23%, basically even with the security management team at 22%.

Collectively, in organizations over 5,000, the CTO/CFO/CEO roles make the call in 20% of the companies surveyed.

For marketers, there are clear implications. In smaller organizations (those under 5,000), focus on upper IT and security management, who make the final call about 40% of the time. The CISO makes the final call in only 13% of the time, likely because they don't have a CISO in the first place. In orgs under 500, the CEO or CFO makes the final call shortly after IT management, which makes sense given the organization size.

IT management still plays a lead role, followed by the CISO, the security management teams and C-level executives.

When it comes to decision criteria, features are king, but only insofar as they map to the requirements, pains, and challenges that the prospect has.

Pricing as shown here is likely relative to their budget.

Vendor and risk assessment likely combine into one criteria, they're "trust"-based concerns.

Stakeholder recommendations could be based on word of mouth from other industry people they trust or industry colleagues.

A previous relationship with the vendor may matter less than we think, and marketing and sales shouldn't don't rely on that – you'll have to win their business every single time.

Q15

What is your typical decision criteria when selecting vendors?

(Select all that apply and rank highest to lowest priority)

1	Product/service features
2	Pricing
3	Risk assessment
4	Vendor reputation
5	Support and licensing
6	Stakeholder recommendations
7	Supplier relationship
8	Sustainability and ethics
9	Other

Q16

When selecting a new cybersecurity tool, what is your primary goal or outcome?

(Select all that apply and rank highest to lowest priority)

1	Reduce risk
2	Increase visibility into security posture
3	Save time/automate processes
4	Reduce costs
5	Better metrics/dashboards
6	Sustainability and ethics
7	Other

When it comes to the motivation behind procuring new solutions, risk reduction is the number one driver.

"Risk" has two facets here: both the reduction of organizational risk (say, from a security incident), and reduction of personal career risk (eg. staking your reputation on a tool that fails to deliver).

The desire for increased visibility to understand exposure and the time savings gained through automation are also key purchase drivers.

Marketers can leverage the desire for automation gains by making it clear how much time and effort implementing a new solution or approach will save.

Q17

What are your primary concerns when considering running a proof-of-concept (PoC) with a cybersecurity vendor?

(Select all that apply and rank highest to lowest concern)

1	Scope
2	Integration with existing systems
3	Establishing evaluation and measurement criteria
4	Resource allocation
5	Data privacy and protection
6	Timeline
7	Vendor engagement and support
8	Stakeholder involvement
9	Exit strategy for the PoC
10	Other

Understanding potential roadblocks to getting a PoC implemented can help vendors address these concerns up-front and move the PoC process forward.

Presenting an already well-articulated scope for a PoC that makes it easier to agree to should result in greater success rates.

Consider creating a “PoC Concerns” battlecard that addresses the top concerns shown here or provide a trust-building “PoC Guide” that explains off how you address these concerns. Make sure to include detail about how to get off-boarded if they feel it wasn’t successful. Give them an “off-ramp.”

Presenting an already well-articulated scope for a PoC that makes it easier to agree to should result in greater PoC launch rates.

Q18

Where do you typically like to learn about new cybersecurity solutions?

Select all that apply and rank by most important to least important)

Webinars are not “dead” and are still the leading source of education about new cybersecurity solutions.

So-called “dark social” or industry friend/colleague recommendations also stand out. As a marketer, think about how you could create an army of ambassadors in the “dark social” space. Their recommendations have weight.

If your SMEs build a genuinely helpful presence on Reddit in advance of any pre-sales questions or opportunities or negative brand mentions that come up, you’ll be in a good position to respond effectively. A single dropped link from a trusted reddit user can drive significant traffic to your website.

Analyst reports are still used as a starting point or shortlist of vendors for buyers and may be worth the cost to play depending on the cost/benefit analysis. There’s also a reasonable expectation that tradeshows will continue to grow in 2024.

Think about how you can create an army of ‘ambassadors’ in the dark social space. Peer-based referrals carry serious weight.

PART 2

Cybersecurity Technology Stack

Part two of this report provides insight to the security posture of organizations across a broad range of topics including API security, application security, cybersecurity insurance, data security, endpoint security, human security, IAM, network security, and security operations.

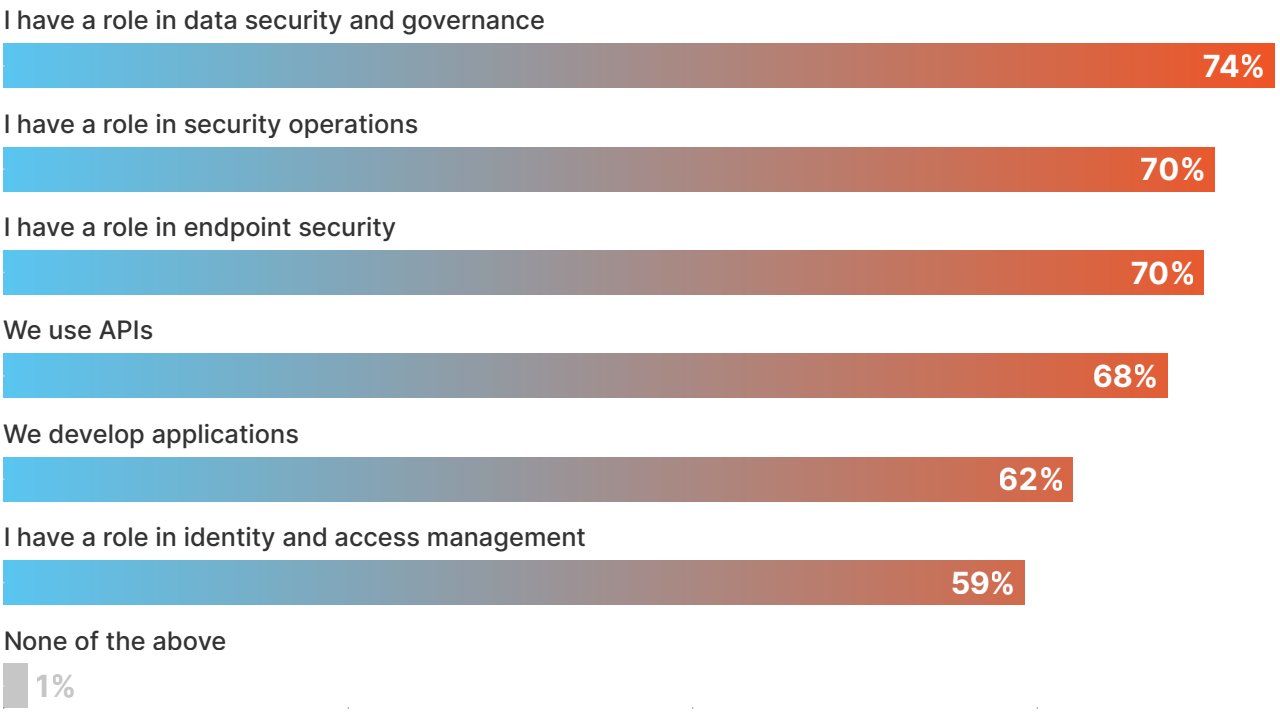
In general, the results indicate there are significant opportunities for improvement in API security, application security, IAM, and security operations in particular. Organizations have implemented robust security awareness programs for their employees, and endpoint security/network security is relatively mature in most organizations.

The results indicate there are significant opportunities for improvement in API security, application security, IAM, and security operations in particular.

Q1

Which of the following applies to you and/or your organization?

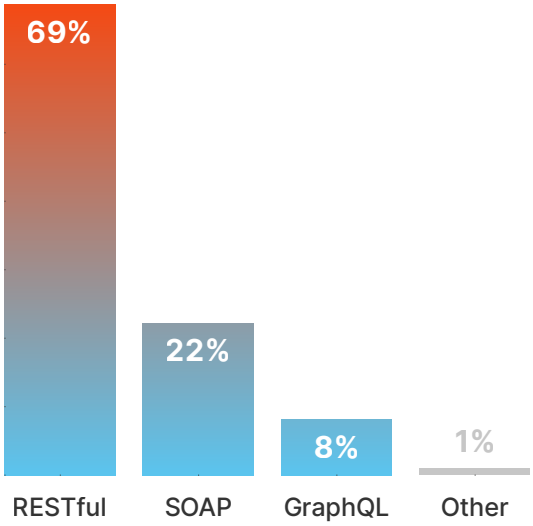
(Select all that apply)



API SECURITY

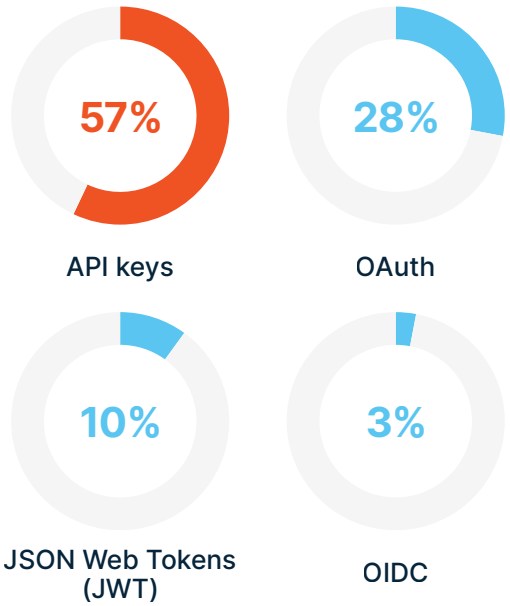
Q2

Which type of APIs does your organization primarily use?



Q3

How do you authenticate and authorize API users?



According to many industry analysts, API traffic now accounts for as much as 80% of all Internet traffic, and this volume is expected to continue growing. Given this trend and the critical nature of APIs to core business applications, API security needs to be a focus for organizations.

The shift to cloud-native applications built on microservices architectures leveraging REST, SOAP, and GraphQL APIs, among others, has greatly expanded the attack surface and provides many opportunities for threat actors to attack core business applications.

The majority of respondents (approximately two-thirds) use RESTful APIs, whereas SOAP APIs account for approximately 22% of APIs. While these APIs enable development velocity and efficiency, if API-focused security controls are not an integral part of the application development process, organizations will be exposed to ever greater risk of data breaches across their partner and software supply chain networks.

More than half of respondents use API keys to authenticate and authorize API users.

OAuth is used by approximately 28% of respondents, followed by JSON Web Tokens (JWT) and OIDC. While API keys offer simplicity for developers, this can be a double-edged sword: threat actors leverage this simplicity to compromise business-critical applications and application data. OAuth (specifically, OAuth 2.0) is a better option for both security and user experience, but adoption still significantly lags behind API keys. JWT, OIDC, and other API authentication/authorization protocols are typically used in combination with OAuth to further enhance security and to address specific use cases (such as database table lookups).

Q4

Are API security logs regularly monitored and analyzed?

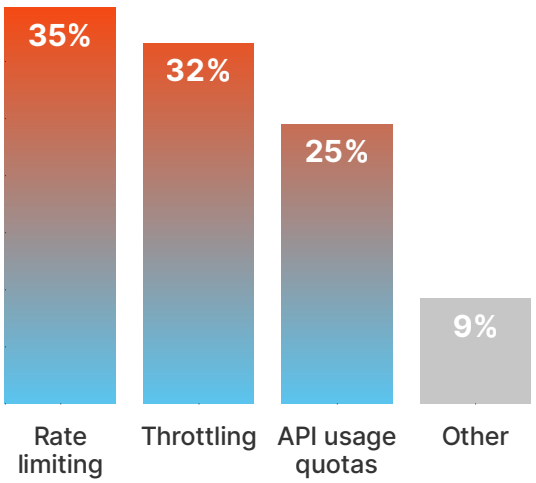
APIs are an increasingly attractive target for threat actors because of their generally non-interactive nature and performance efficiency, making it easier for attackers to avoid detection and exfiltrate data.

Real-time detection and monitoring is therefore essential to API security. Unfortunately, only approximately one-third of respondents monitor and analyze their API security logs in real time, while nearly one-half only do so periodically.

API traffic now accounts for as much as 80% of all Internet traffic, and this volume is expected to continue growing.

Q5

What measures are in place to prevent API abuse and excessive API calls?



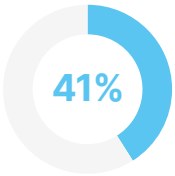
Rate limiting, throttling, and API usage quotas are important controls to help mitigate API abuse and denial-of-service (DoS) attacks, but should be considered complementary to more robust API security controls such as API gateways, authentication and authorization, and encryption.

Respondents used a variety of methods to prevent API abuse including rate limiting (approximately 35%), throttling (approximately 32%), and API usage quotas (approximately one-quarter).

Q6

Does your organization perform regular security assessments for APIs?

Yes, regularly scheduled assessments



Occassionaly, but not on a regular basis

No, we don't perform security assessments on APIs

Although regular network, data center, application, and cloud security assessments are fairly common, API security assessments are one area that most organizations need to improve—particularly given the rapidly evolving threat landscape as attackers continuously probe this ever-expanding attack surface.

Among all organizations, 62% either only test API security occasionally or don't test at all. Large organizations fared only slightly better with 65% testing only occasionally or not at all.

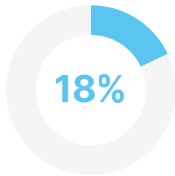
Regular API security training is a relatively low-cost way to enhance an organization's security posture across the entire API lifecycle.

Q7

Have you conducted security training specifically focusing on API best practices for developers?

Occasionally, when required

No, we haven't conducted specific API security training



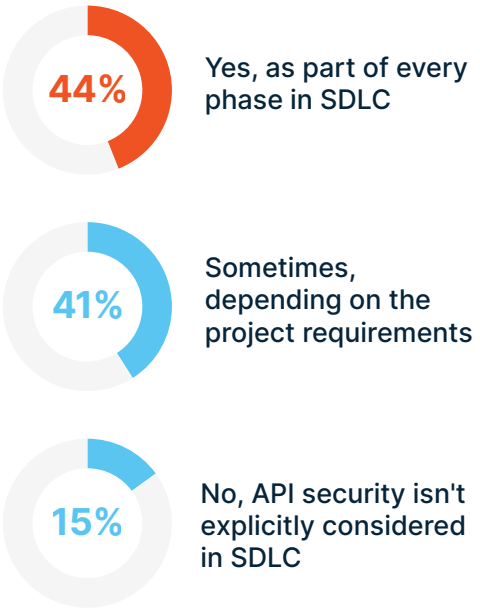
Yes, regularly scheduled training

API security training is another area of concern for organizations, with less than 20% of all respondents reporting that they provide regular training on API security best practices for their developers.

One-third provide no API security training, and approximately half only provide training occasionally. Regular API security training is a relatively low-cost way to enhance an organization's security posture across the entire API lifecycle.

Q8

Are API security practices included in the software development lifecycle (SDLC)?



Fewer than half of respondents reported that API security practices are an integral part of their SDLC.

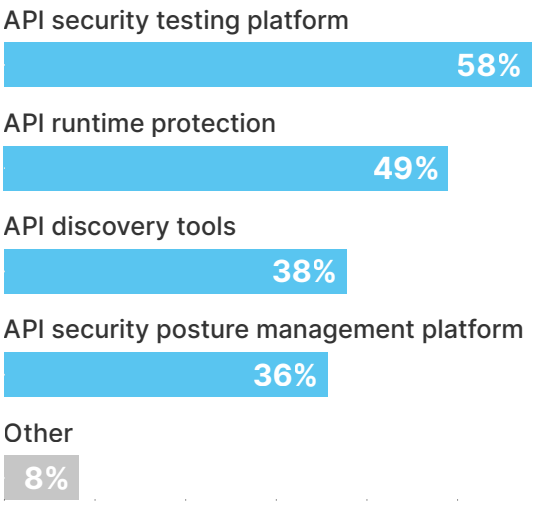
Approximately 56% reported that API security is either sometimes considered depending on the project requirements, or not considered at all. Given the integral role of APIs in applications, API security best practices need to be incorporated throughout the entire SDLC to reduce application development costs, accelerate velocity and time-to-market, and ensure a robust application/API security posture.

Approximately 56% reported that API security is either sometimes considered depending on the project requirements, or not considered at all.

Q9

Which of the following API security tools do you regularly use?

(Select all that apply)



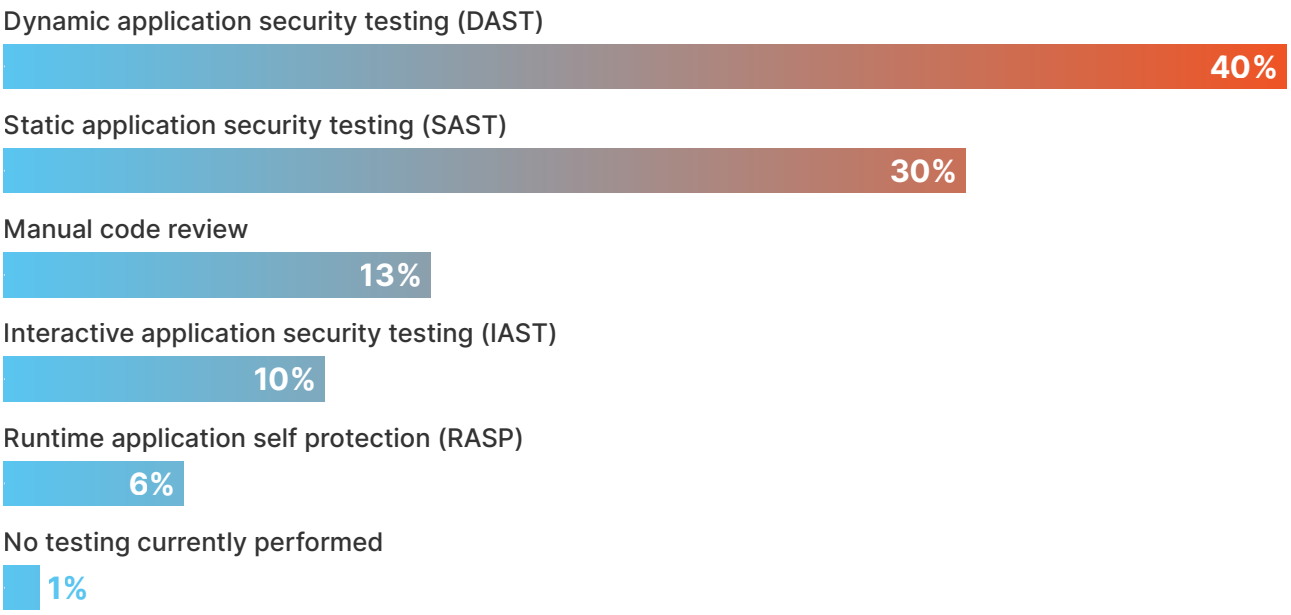
To properly address unique security requirements in APIs, organizations need to leverage API-specific security tools in much the same way that specialized security tools are used for networks, applications, and cloud resources.

API security tools are clearly an area that needs improvement across all organizations, as fewer than half of respondents reported using API security tools such as an API security testing platform, API runtime protection, API discovery tools, or API security posture management.

APPLICATION SECURITY

Q10

What application security testing techniques do you regularly use?



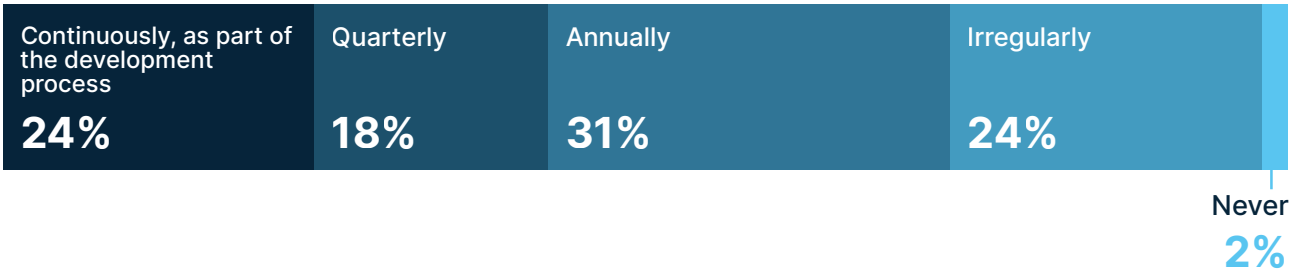
SAST and DAST tools have seen widespread adoption by application development teams, but more advanced tooling, such as IASP and RASP, is still lacking.

Most organizations (62% to 70%) today use a combination of SAST and DAST tools for application security testing, but IAST and RASP are not frequently used. Alarmingly, 14% of respondents only perform manual code reviews or no security testing at all, which exposes organizations to risks that extend beyond potential security breaches in their applications and data, such as higher costs and slower time to market to address security issues later in the application development lifecycle.

Most organizations (62% to 70%) today use a combination of SAST and DAST tools for application security testing, but IAST and RASP are not frequently used.

Q12

How often do you provide secure coding training to developers?



Q11

How do you handle third-party or open source components in your applications?

Use only well-known and trusted components

Regularly monitor and update them

No formal process in place

Less than half of all organizations provide continuous or quarterly secure coding training to their developers.

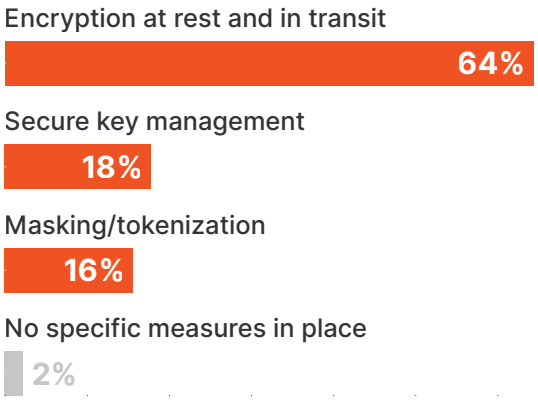
Unfortunately, more than half only provide training annually, irregularly, or not at all. Training is a relatively low-cost way to significantly improve application security, reduce software development costs, and accelerate time-to-market.

Security in third-party and open-source application components is an area in significant need of improvement.

Only roughly half of organizations (44%) limit the use of these components in their applications to those from well-known and trusted sources, and one-third (34%) regularly monitor and update third-party and open-source application components. Using components from unknown and/or untrusted sources exposes organizations to risk not only from a direct attack against their applications, but software supply chain attacks as well.

Q13

How do you manage sensitive data within your applications?



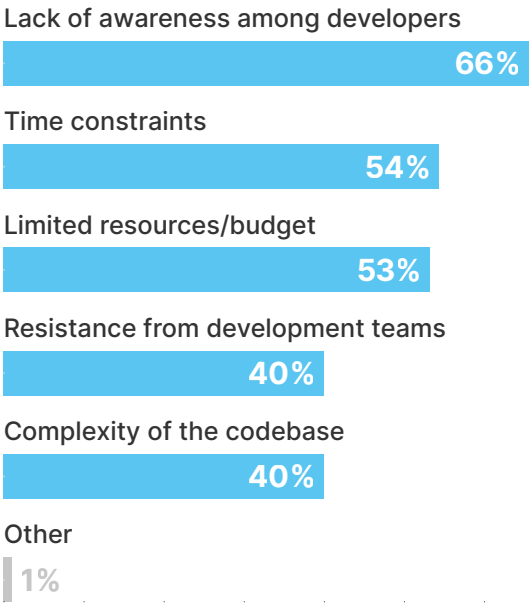
Application data security is a relatively bright area, as more than two-thirds of organizations use encryption to safeguard sensitive data in their applications.

Other commonly used techniques for securing application data include masking/tokenization (approximately 16%) and secure key management (approximately 18%).

Q14

What challenges do you face when implementing secure coding practices?

(Select all that apply)



Secure coding training helps address the issues of limited resources/budget and time constraints by addressing security requirements early in the SDLC, which helps reduce development costs and increase velocity.

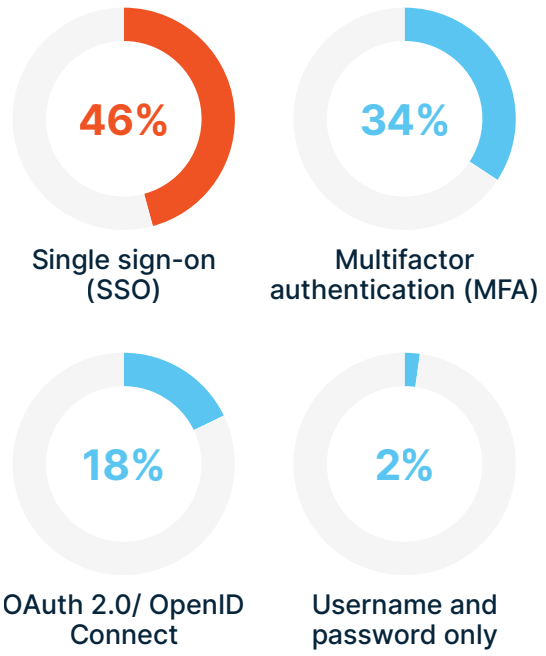
The top three challenges for organizations with regard to secure coding practices are:

- 1. Lack of awareness among developers
- 2. Limited resources/budget
- 3. Time constraints

This finding is not surprising given that less than half of organizations provide continuous or quarterly application security training for their developers. However, secure coding training is one of the most cost-effective ways to improve application security and also helps address the issues of limited resources/budget and time constraints by addressing security requirements early in the SDLC ("shift left"), which helps reduce development costs and increase velocity.

Q16

Which secure authentication methods do you use for applications?



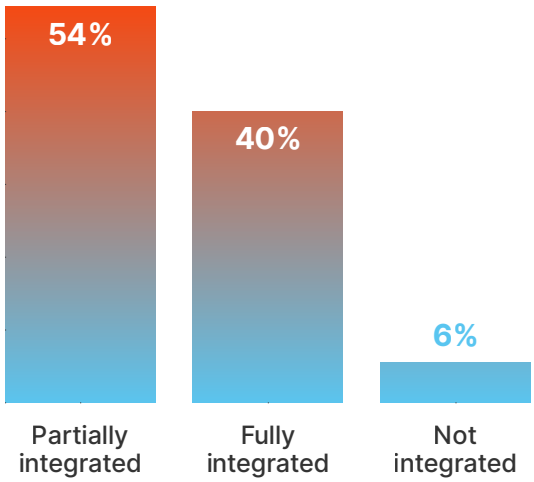
The use of secure authentication methods in applications is an area in need of significant improvement.

Only 34% of organizations use MFA to secure access to their applications. This is alarming, as MFA is so commonly used today and should be "table stakes" for all applications. SSO has been adopted by approximately 46% of organizations, which helps to improve the user experience (and security) by reducing "password fatigue" and limiting password re-use.

Only 34% of organizations use MFA to secure access to their applications.

Q15

Are security requirements and testing integrated into your development lifecycle?



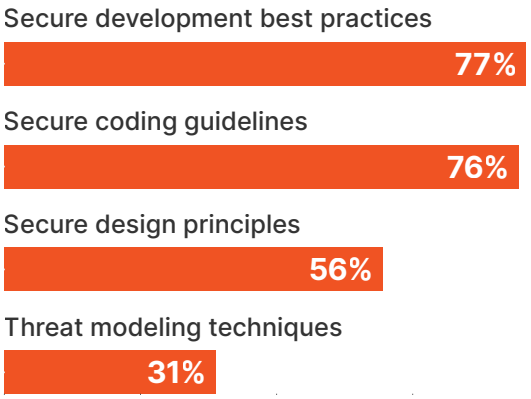
The majority of organizations (94%) ensure security requirements and testing are an integral part of their development lifecycle.

By addressing security requirements and testing earlier in the SDLC ("shift left"), organizations can improve the security of their applications, reduce costs, and reduce the need for costly delays due to code fixes later in the SDLC.

Q17

Which type of security training is provided to your application development team?

(Select all that apply)



Between 60% and 80% of organizations provide training on secure development best practices and secure coding guidelines, and 56% also provide training on secure design principles.

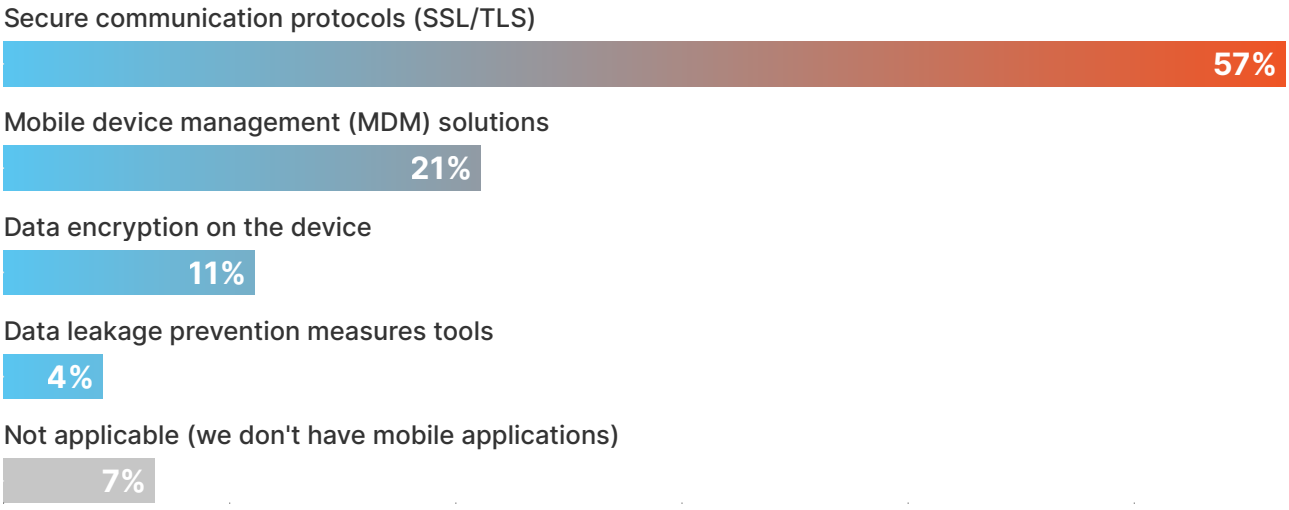
More advanced training, such as threat modeling techniques, is still relatively limited with approximately 31% of organizations providing this type of training to their development teams.

Use of SSL/TLS (specifically, TLS 1.2 or later) should be a de facto standard implemented in all applications (including mobile applications), yet only 57% of all respondents use SSL/TLS to secure data storage and transmission in their mobile applications.

Broader adoption of MDM and data encryption on devices is also needed.

Q18

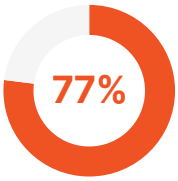
How do you ensure secure data storage and transmission in mobile applications?



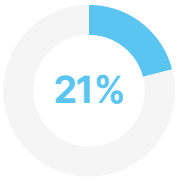
CYBERSECURITY INSURANCE

Q19

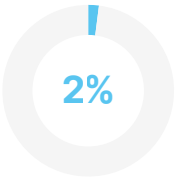
Does your organization have cybersecurity insurance coverage?



Yes, we have an active policy



No, we don't have any cybersecurity insurance

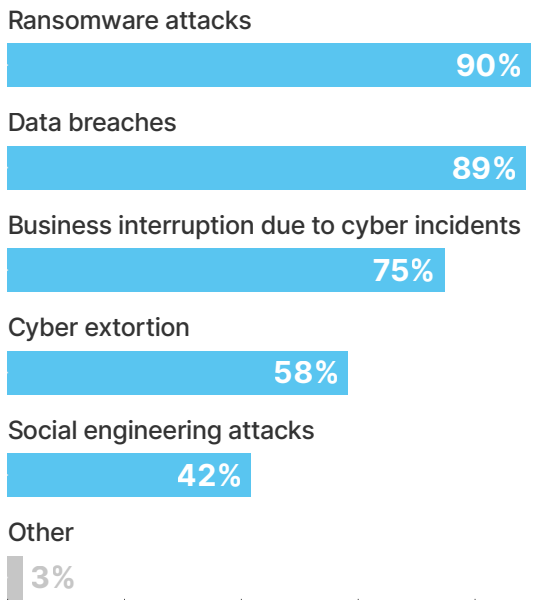


We had it in the past, but not anymore

Q20

What types of cyber incidents does/did your cybersecurity insurance policy cover?

(Select all that apply)



Cybersecurity insurance is an increasingly popular risk treatment (risk transfer) option for many organizations.

70% of all organizations and 77% of large organizations have active cybersecurity insurance policies, and nearly all (approximately 99%) are very confident or somewhat confident that their coverage is adequate.

77% of large organizations have active cybersecurity insurance policies.

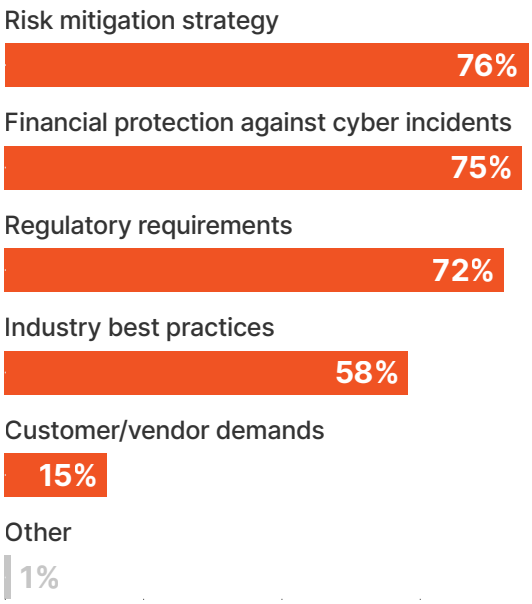
Most organizations maintain cybersecurity insurance policies which cover the greatest threats to their business.

These threats include ransomware attacks, data breaches, business interruptions, and cyber extortion.

Q23

What factors influenced your organization's decision to purchase cybersecurity insurance?

(Select all that apply)



The majority of respondents purchased cybersecurity insurance policies as part of their risk mitigation strategy, to offset financial losses, and to address regulatory requirements.

While only 10% of respondents reported actually filing a cybersecurity insurance claim, the overwhelming majority (92%) rated their carrier's response as excellent or good.

Beyond simply providing financial remedies, cybersecurity insurance services often include active support (either directly or through a third-party) during an incident including legal advice, forensic services, and incident response services.

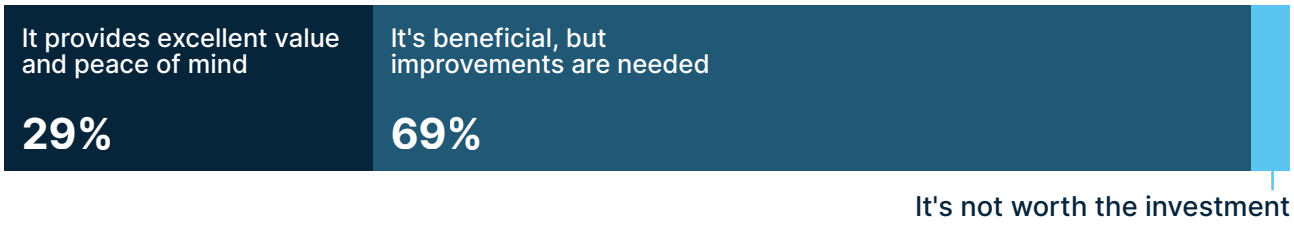
Despite overall positive feedback regarding the responsiveness of cybersecurity insurance providers, more than two-thirds of organizations (69%) feel that while cybersecurity insurance is beneficial, improvements are needed.

Q21

How would you rate the responsiveness and support from your cybersecurity insurance provider in response to the cyber incident?

Q22

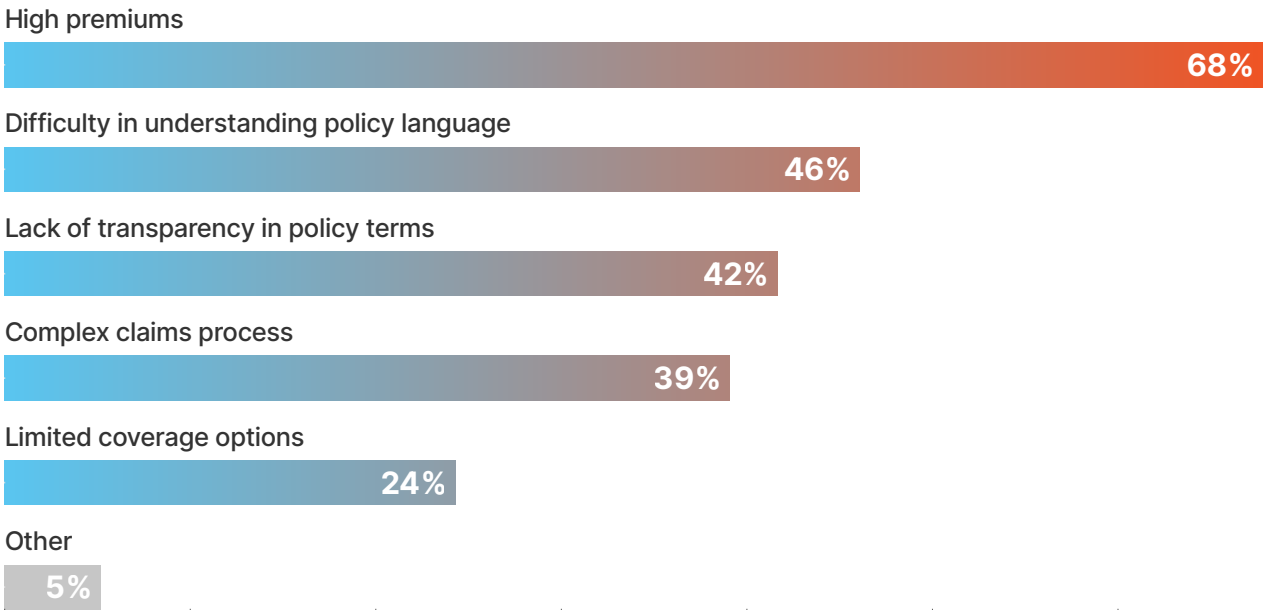
How would you assess the overall value of cybersecurity insurance coverage to your organization?



Q24

What challenges does your organization face when dealing with cybersecurity insurance providers?

(Select all that apply)



Common challenges cited by respondents with regard to cybersecurity insurance included high premiums, difficult policy language, lack of transparency, and complicated claims processes.

Cybersecurity insurance services often include active support during an incident including legal advice, forensic services, and incident response services.

DATA SECURITY & GOVERNANCE

Cloud storage, database security, and regulatory compliance were cited as the top three data security challenges for organizations of all sizes.

These same challenges were reported by large organizations, although regulatory compliance was considered a greater challenge than database security.

Accurately identifying and classifying your sensitive data assets is an important first step in data protection, but many organizations struggle to do so.

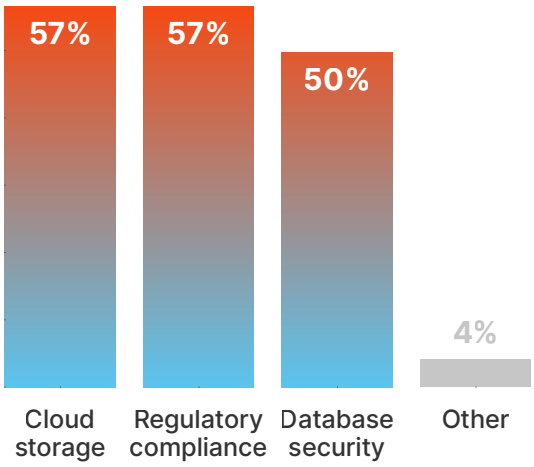
Approximately two-thirds of all respondents use data classification labels and more than half use data discovery tools to identify and classify sensitive data. However, there are many opportunities to improve accuracy and efficiency as only 21% of all organizations reported using automatic data profiling. As artificial intelligence and machine learning technologies mature, the accuracy of automatic data profiling solutions will significantly increase.

As artificial intelligence and machine learning technologies mature, the accuracy of automatic data profiling solutions will significantly increase.

Q25

What are your most significant data security challenges?

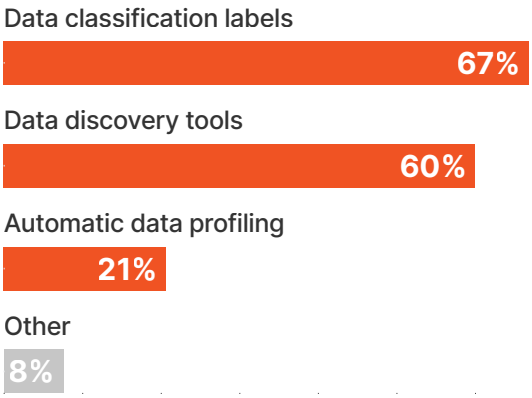
(Select all that apply)



Q26

What methods do you employ to identify and classify sensitive data?

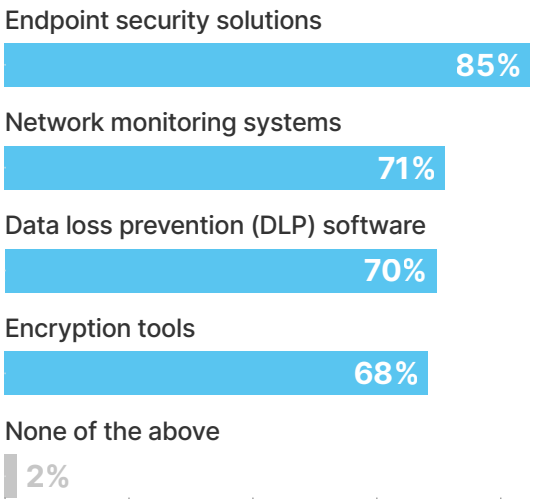
(Select all that apply)



Q27

Which technologies are utilized for data loss prevention in your organization?

(Select all that apply)



Various DLP solutions, including endpoint security, network monitoring, encryption, and DLP software have been broadly adopted by most organizations.

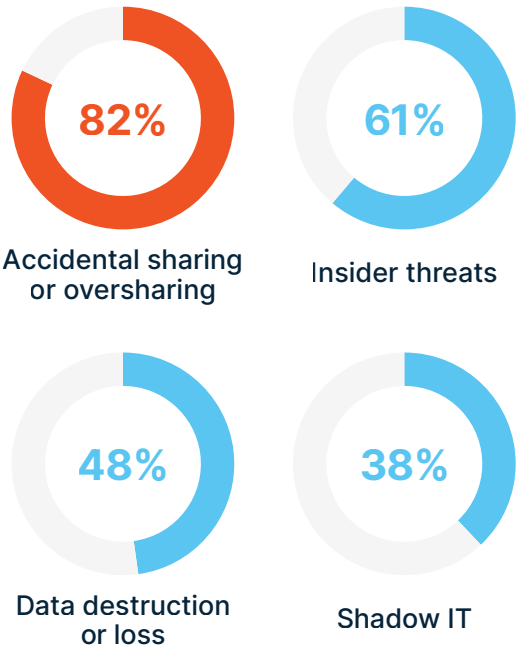
While these solutions have been available for many years, initial deployment, configuration, and ongoing maintenance of these solutions has often been a hurdle for many organizations.

Organizations need to ensure they are addressing both external and internal threats appropriately.

Q28

Which data security risks concern you most?

(Select all that apply)



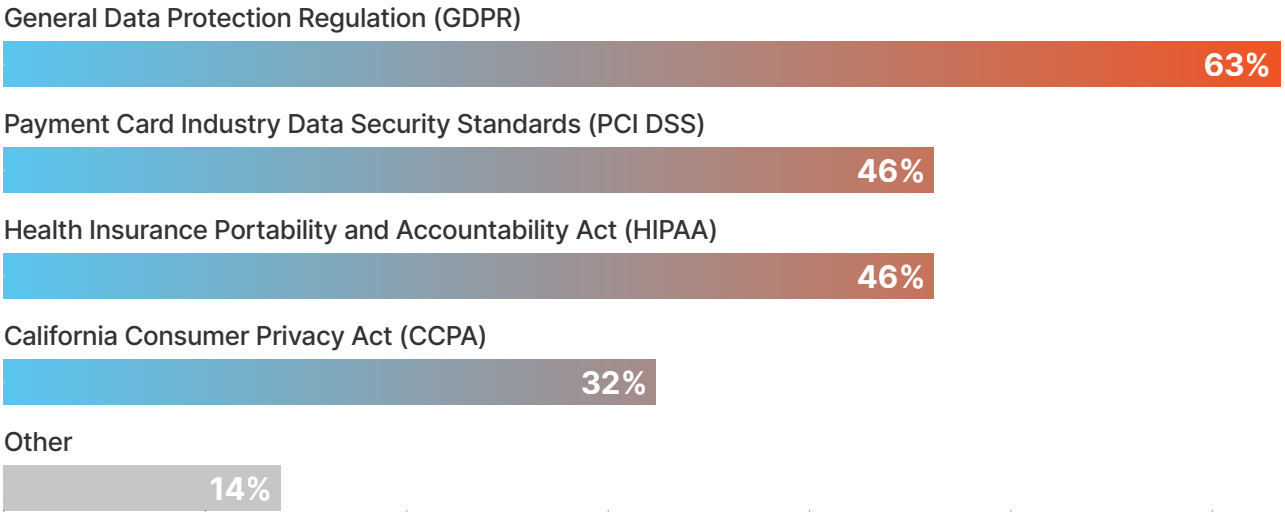
Interestingly, with regard to data security, most organizations are focused on various insider threats including accidental sharing or oversharing, data destruction or loss, shadow IT, and other insider threats.

Although such insider threats do represent a growing problem, organizations need to ensure they are addressing both external and internal threats appropriately.

Q29

Which of the following data security/privacy requirements is your organization subject to?

(Select all that apply)



Compliance with GDPR, PCI DSS, HIPAA, and CCPA (to a lesser extent) are the main regulatory requirements that organizations are subject to today.

While PCI DSS and HIPAA are primarily focused on data security, GDPR and CCPA are primarily focused on data privacy. Since the implementation of GDPR, many other countries and U.S. states have enacted data privacy laws, so it is likely that data privacy compliance will become an even bigger concern for organizations.

It is likely that data privacy compliance will become an even bigger concern for organizations.

Third-party risk management practices represent an opportunity for improvement as most organizations rely on static tools such as security certifications and audits, contractual obligations and SLAs, industry reputation, and data breach history (if known) rather than any third-party risk management tools.

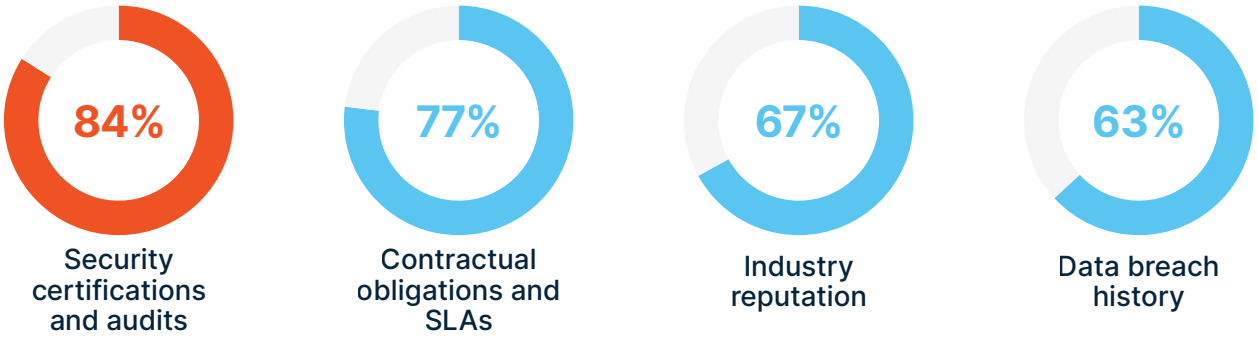
The 2020 SolarWinds attack and, more recently, the Johnson Controls software breach highlight the importance of addressing third-party risk for organizations across the entire supply chain.

The 2020 SolarWinds attack and the Johnson Controls software breach highlight the importance of addressing third-party risk for organizations across the entire supply chain.

Q30

Which factors are considered when evaluating third-party vendor data security practices?

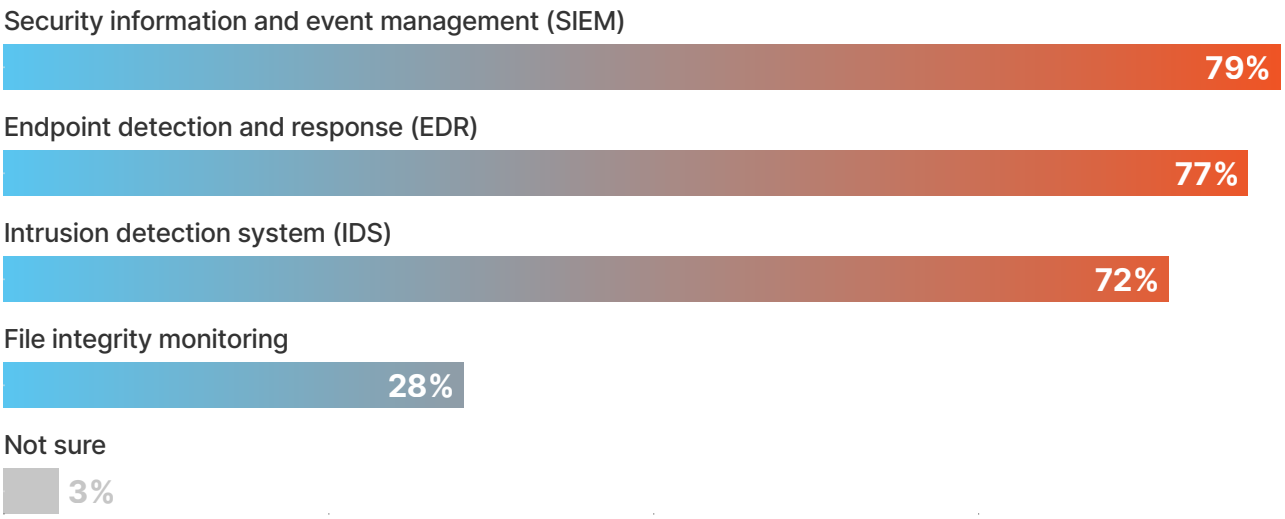
(Select all that apply)



Q31

How do you monitor and detect unauthorized access or data breaches?

(Select all that apply)



Most organizations leverage mature security tooling such as EDR, SIEM, and IDS to detect security issues in their environment.

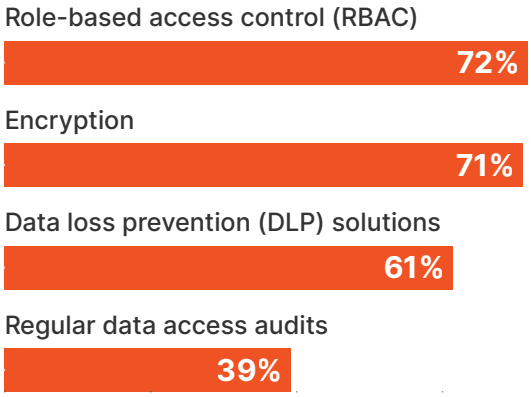
File integrity monitoring solutions have seen lower adoption rates, typically due to implementation challenges—whether real or perceived.

File integrity monitoring solutions have seen lower adoption rates, typically due to implementation challenges.

Q32

What measures does your organization employ to protect sensitive data from internal unauthorized access?

(Select all that apply)



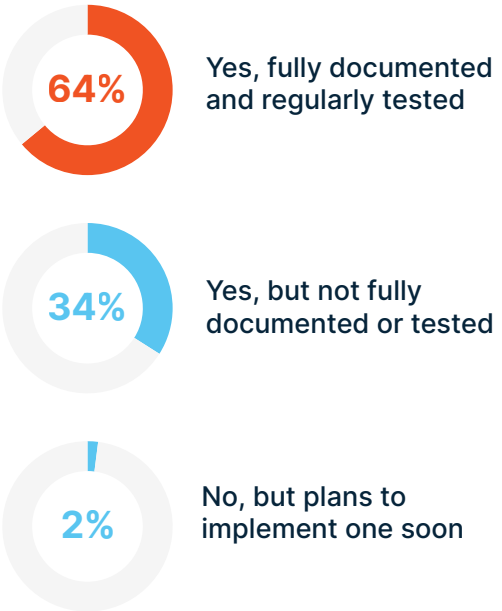
RBAC, encryption, DLP, and data access audits are most commonly used to protect sensitive data from insider threats.

However, more powerful and dynamic tools for insider threat management, such as user and entity behavior analysis and AI/ML technologies, need to be a part of efforts to address these threats.

The 2021 Colonial Pipeline ransomware attack is a poignant example of the importance of data backups and disaster recovery (as well as business continuity) plans.

Q33

Does your organization have a data backup and disaster recovery plan?



Over two-thirds of all respondents have a fully documented and regularly tested data backup and disaster recovery plan.

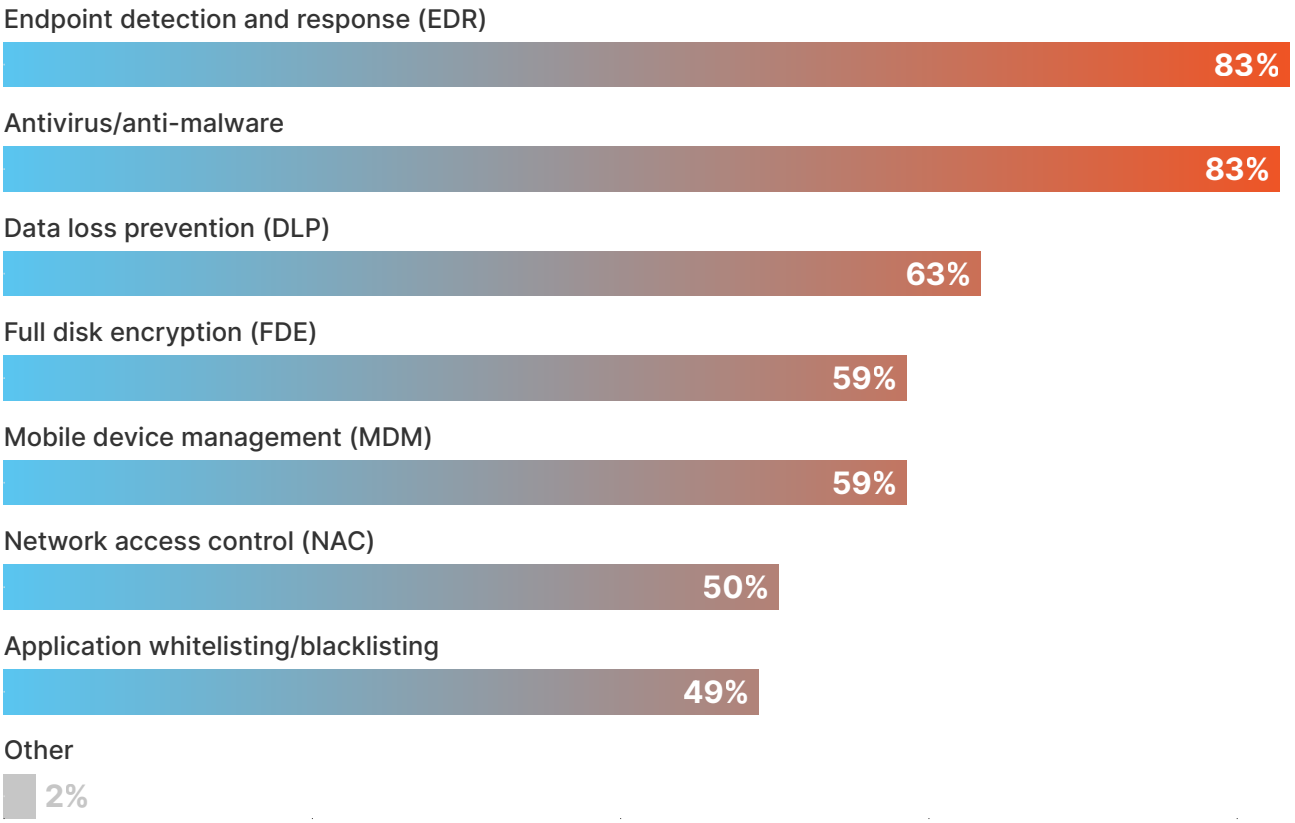
However, this still leaves one-third of all organizations essentially unprotected. The 2021 Colonial Pipeline ransomware attack is a poignant example of the importance of data backups and disaster recovery (as well as business continuity) plans. Although the decision to shut down critical systems was made very quickly and the ransomware threat was effectively contained, it took several days to restore critical systems to normal operation, resulting in supply chain issues along the entire U.S. eastern seaboard.

ENDPOINT SECURITY

Q34

Which endpoint security solutions do you currently use?

(Select all that apply)



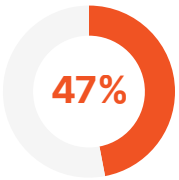
Most organizations demonstrate maturity in their use of endpoint security solutions which include EDR, antimalware, DLP, FDE, MDM, NAC, and application whitelisting/blacklisting.

The extensive use of multiple solutions on endpoints demonstrates the maturity of these vendor solutions, as well as organizational awareness that endpoints exponentially increase the attack surface (particularly in the wake of the global pandemic and the continuing trend to support work-from-home and work-from-anywhere) at the point that has traditionally been an organization's weakest link—the end user.

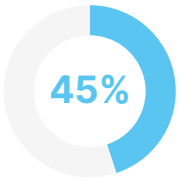
The extensive use of multiple solutions on endpoints demonstrates the maturity of these vendor solutions.

Q36

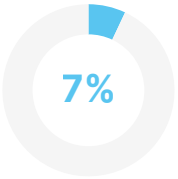
How do you manage and deploy security updates and patches to endpoints?



Automated patch management system



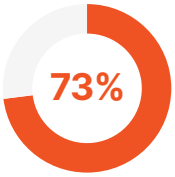
Combination of automated and manual



Manual updates

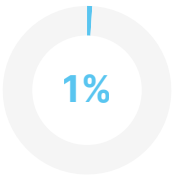
Q35

How do you enforce strong authentication on endpoints?



Two-factor authentication (2FA) or Multifactor authentication (MFA)

Mandatory password complexity requirements



Biometrics (fingerprint, facial recognition)

Nearly all organizations use automated patch management or a combination of automated and manual techniques for endpoints.

This follows the consumer trend toward automated patching found in iPhones and Windows 10/11 devices, among others.

Nearly three-quarters of all organizations use MFA to enhance endpoint security.

As in other use cases, strong MFA authentication (not SMS text) needs to be implemented as part of every security baseline configuration. Likewise, adoption of passwordless authentication options such as biometrics, which remains extremely low, needs to increase as passwords seem to be rapidly approaching a tipping point in which they are no longer considered effective for preventing unauthorized access to endpoints, systems, and applications.

Q37

How do you manage endpoints that are not regularly connected to the corporate network (e.g., field devices, remote sites)?

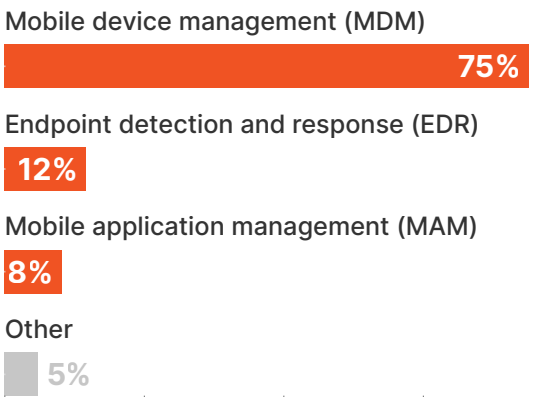
With the rapid growth of remote work and Internet of Things (IoT) devices, remote management of endpoints remains a major challenge for organizations.

Most report using remote desktop software and out-of-band management tools that may themselves introduce security risk to the organization. Although ransomware attacks have increasingly been the focus of media reporting, traditional data breaches—which often leverage weaknesses in remote access tools for initial access—remain a major threat that also needs to be properly addressed.

Although ransomware attacks have increasingly been the focus of media reporting, traditional data breaches remain a major threat that also needs to be properly addressed.

Q38

How do you manage security on mobile devices (e.g., smartphones, tablets)?

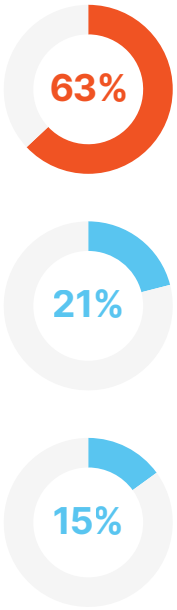


Most organizations today use MDM to manage security on mobile devices.

EDR and MAM are also used, but to a significantly lesser extent. EDR options for mobile devices are relatively limited and there is often a mistaken perception that they are not needed, particularly on iOS devices. MAM solutions offer organizations the ability to compartmentalize corporate data, without granting the organization access to personal data on mobile devices where BYOD is permitted.

Q39

How do you enforce encryption on endpoint devices?



- 63% Full disk encryption (FDE) is mandatory for all devices
- 21% Encryptions is applied based on data classification labels
- 15% No specific encryption policy

The majority of organizations (more than 80%) use either full disk encryption on endpoints or apply encryption based on data classification labels (which is reliant on accurate identification and classification of sensitive data).

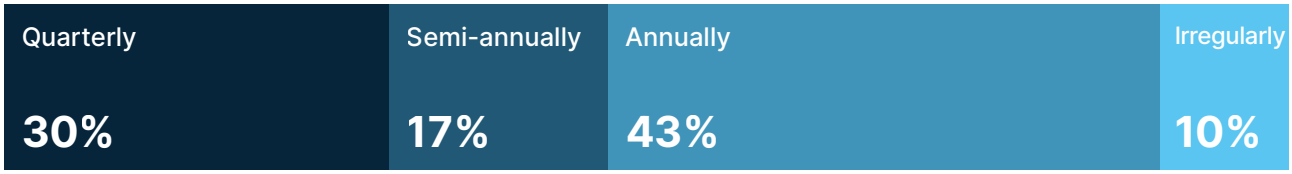
As compute power on endpoints has grown, there is less resistance to full disk encryption which offers a more complete protection strategy, including safe harbor provisions in many data security and data privacy laws in the event of a lost or stolen endpoint device.

As compute power on endpoints has grown, there is less resistance to full disk encryption which offers a more complete protection strategy.

HUMAN SECURITY

Q40

How frequently do you conduct employee training on endpoint security best practices?



Security awareness training is clearly an important component of any organization's security program, as evidenced by the fact that 85% to 90% of organizations reported that they conduct security awareness training for their employees at least annually, semi-annually, or quarterly.

Security awareness training should be a core component of any organization's information security program and is often a regulatory compliance requirement.

Security awareness training should be a core component of any organization's information security program.

Keeping users engaged with interesting, relevant, and timely training—regardless of the topic—is always challenging.

In much the same way that marketers and retailers try to engage their customers across multiple channels of the customer's choice, organizations need to use a variety of methods to engage their users. The majority of organizations today use push technologies such as email and online training platforms to deliver security awareness training to their employees. Intranet, videos/gamification, and posters are used to a lesser extent.

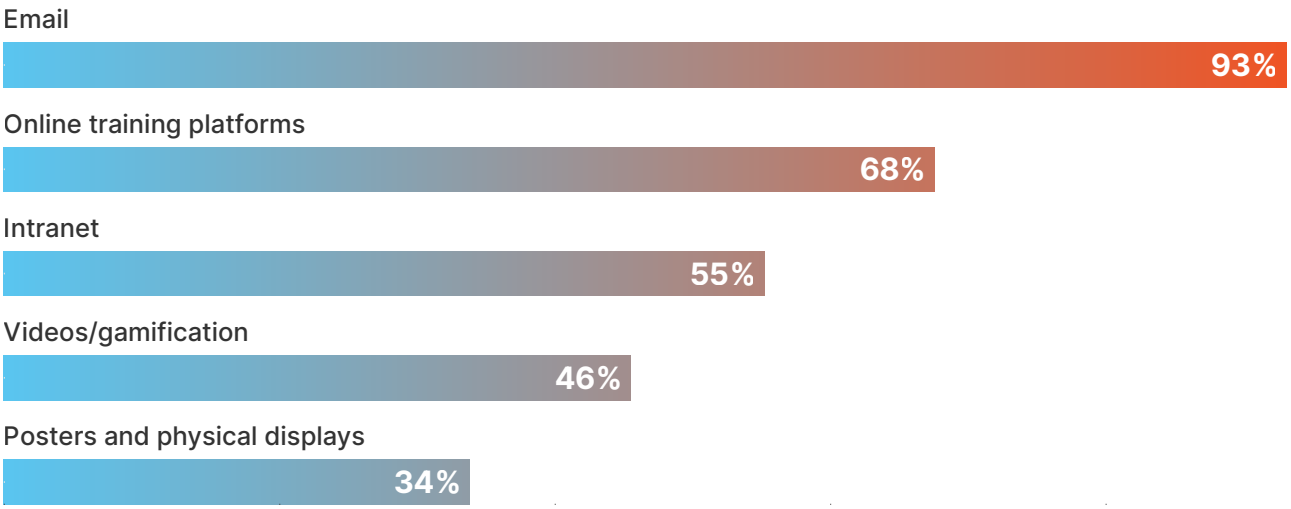
Phishing campaigns remain one of the most effective attack vectors for threat actors, despite the heightened focus on phishing threats.

Phishing simulations remain a core component of security awareness programs with approximately 87% reporting that they do phishing simulations monthly, quarterly, or two to three times a year. As phishing becomes increasingly difficult to detect, particularly with the growing use of AI/ML to target their victims more convincingly, phishing simulations will need to evolve to improve their effectiveness.

Q41

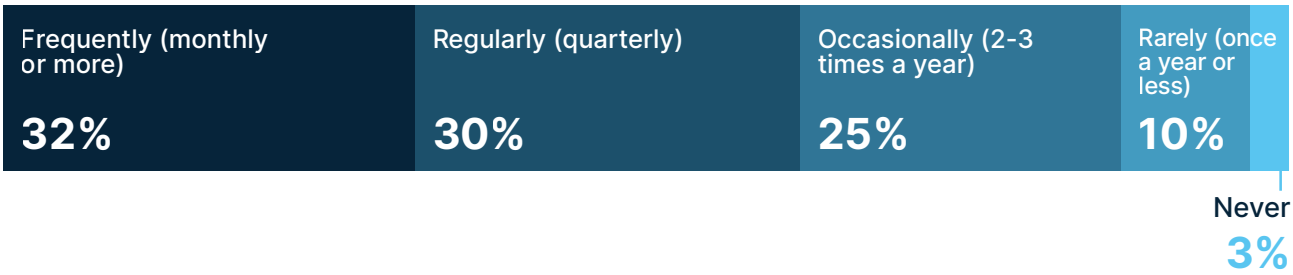
Which communication channels does your organization use to deliver security awareness messages?

(Select all that apply)



Q42

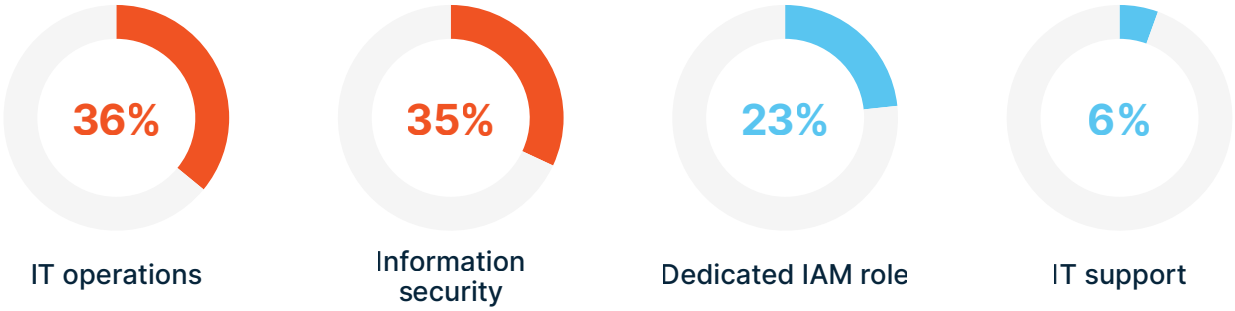
How often does your organization conduct simulated phishing exercises to test employee susceptibility to phishing attacks?



IDENTITY & ACCESS MANAGEMENT

Q43

Who is responsible for Identity and Access Management (IAM) in your organization?



IAM is commonly the responsibility of either IT operations or information security in most organizations, although nearly one-quarter of organizations (23%) have a dedicated IAM role.

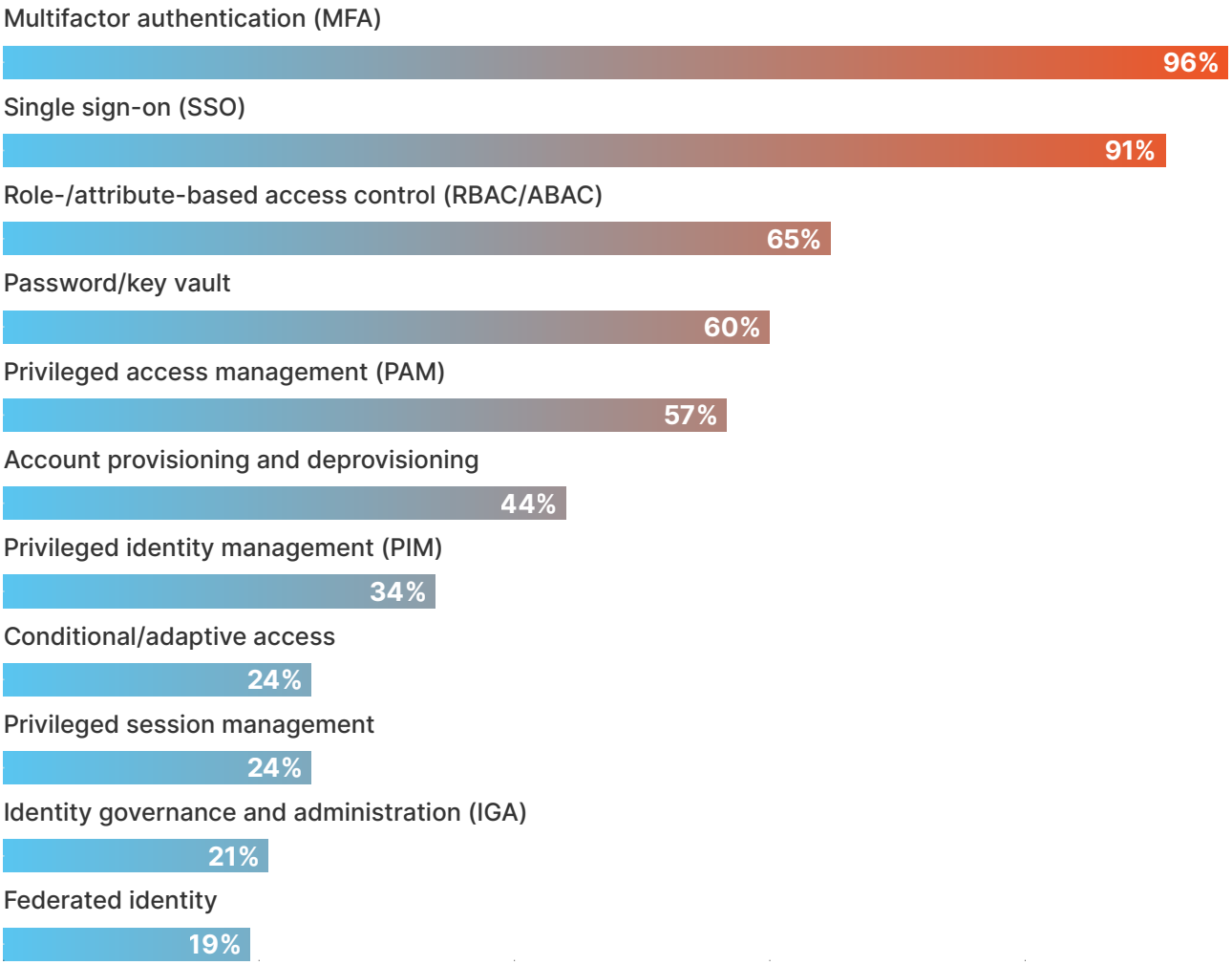
Regardless of the model adopted for IAM, organizations need to ensure segregation of duties, access reviews, and account provisioning/deprovisioning processes are in place.

Organizations need to ensure segregation of duties, access reviews, and account provisioning/ deprovisioning processes are in place.

Q44

Which IAM technologies or solutions does your organization currently use?

(Select all that apply)



MFA and SSO are the most commonly used IAM technologies across all organizations.

RBAC, key vaults, and PAM also see widespread adoption, but there are opportunities to further the adoption of these important IAM components. Similarly, account provisioning/deprovisioning, PIM, conditional access, privileged session management, IGA, and federated identity solutions have not yet seen widespread adoption, but are no less important to ensuring a comprehensive IAM strategy.

Account provisioning/ deprovisioning, PIM, conditional access, privileged session management, IGA, and federated identity solutions have not yet seen widespread adoption.

More than half of all organizations conduct access reviews continuously, monthly, or quarterly.

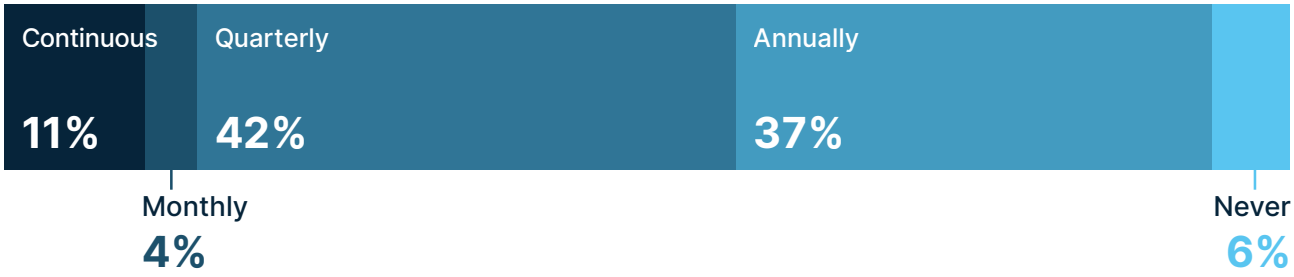
Unfortunately, this means that nearly half of organizations do so only annually or not at all. Access reviews are an important tool to ensure account deprovisioning processes are followed in a timely manner, inactive and dormant accounts are disabled/deleted, and permissions creep is limited within the organization.

Approximately 60% of all organizations use a combination of separate accounts, PAM, and RBAC to manage privileged access.

These are generally mature and well understood processes and tools for managing privileged access. PIM tools, which provide a more robust solution (for example, just-in-time access and approval-based role activation) have seen less adoption (30%).

Q45

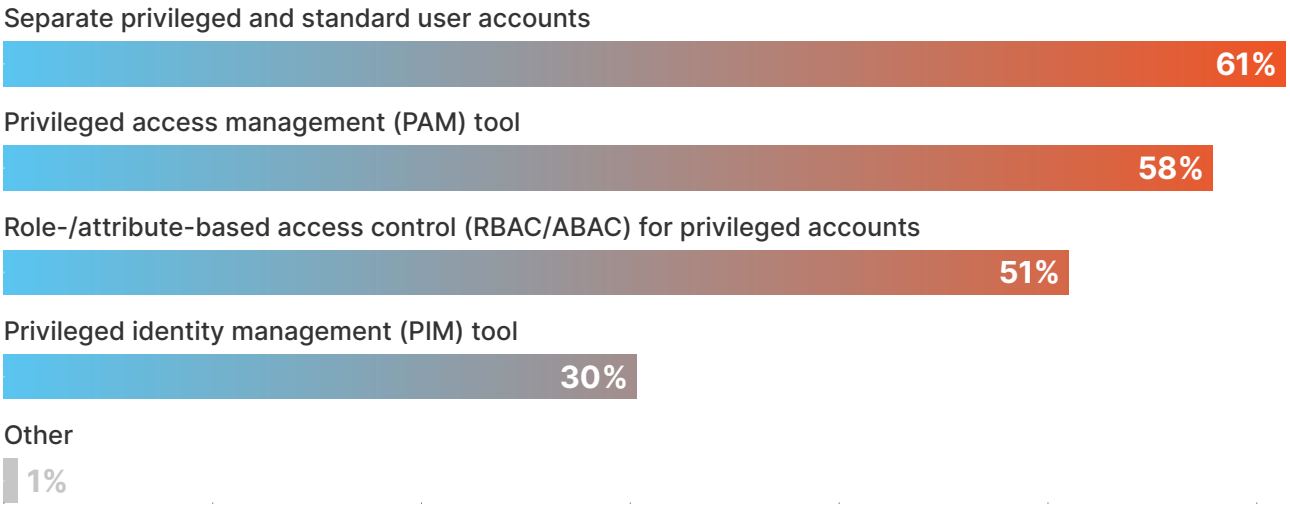
How often does your organization conduct access reviews to ensure least privilege access?



Q46

How do you manage privileged access within your organization?

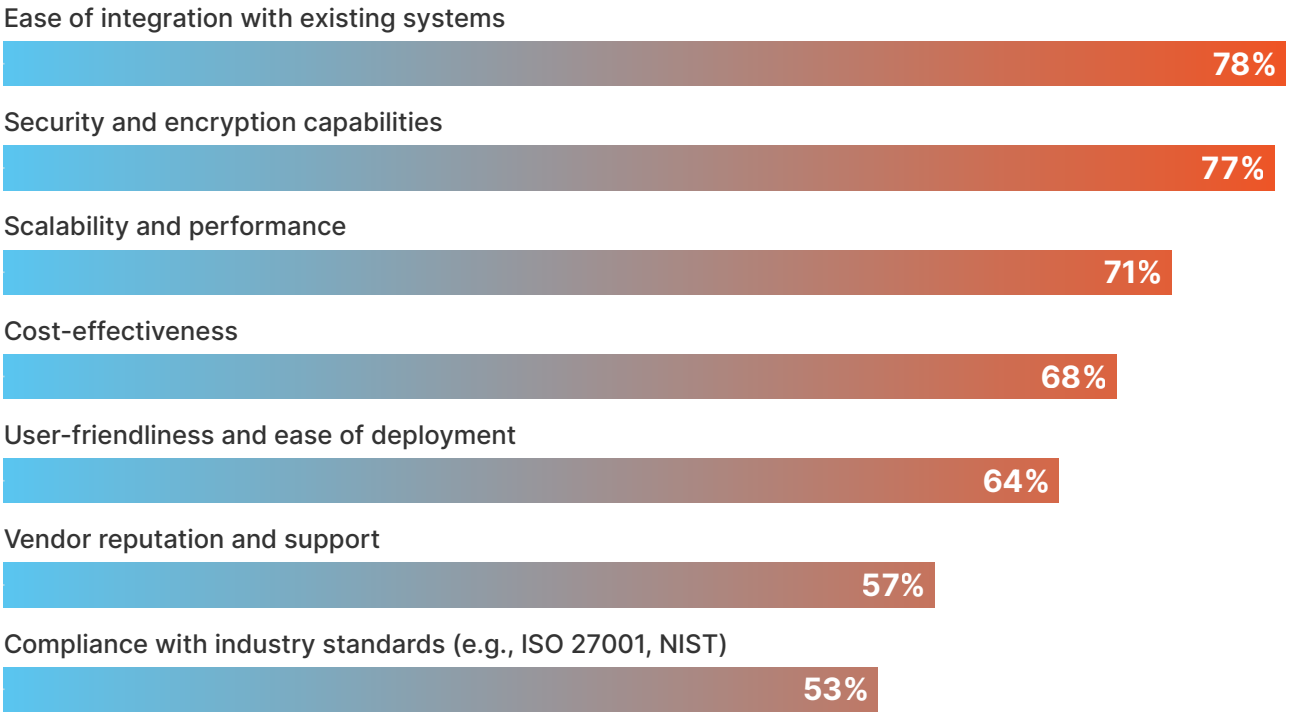
(Select all that apply)



Q47

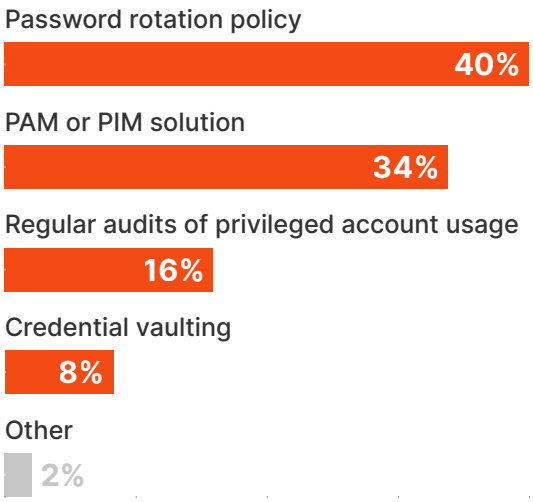
Which factors do you consider when evaluating IAM solutions?

(Select all that apply)



Q48

How do you ensure the security of privileged accounts and credentials?



Ease of integration with existing systems, security capabilities, and scalability and performance are the top factors that organizations consider when evaluating IAM solutions.

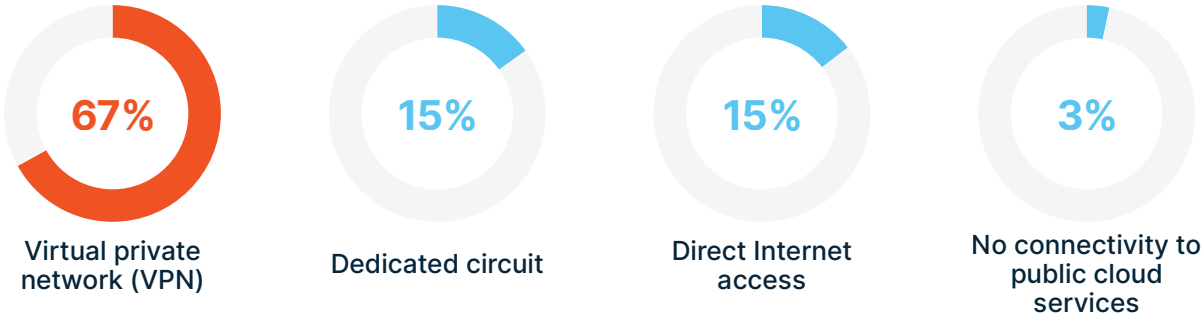
Other important decision criteria include cost-effectiveness, user friendliness and ease of deployment, vendor reputation and support, and regulatory compliance requirements.

While more than one-third of respondents use a PAM or PIM solution to secure privileged access, more than half rely on less sophisticated/manual—and less effective—methods including password rotations and regular audits.

In addition to PAM and PIM solutions, organizations need to adopt credential vaulting more broadly to ensure privileged accounts are not easily compromised by a threat actor.

NETWORK SECURITY

Q49 How do you connect your network to public cloud services?



As cloud adoption continues to grow, organizations increasingly recognize the importance of securing their communications to cloud services.

More than two-thirds of organizations connect to the public cloud via VPN access. Approximately 15% use a dedicated circuit (such as Azure ExpressRoute or AWS Direct Connect) for maximum security (and performance). At the opposite end of the spectrum, approximately 15% of organizations access their cloud services via DIA (secured with SSL/TLS encryption). Given the significant cost associated with dedicated circuits and the relatively limited control associated with DIA, VPN access will likely remain the preferred connection method.

Given the significant cost associated with dedicated circuits and the relatively limited control associated with DIA, VPN access will likely remain the preferred connection method.

Network vulnerability scanning is a bright spot as most organizations report scanning continuously (41%), daily (15%), or weekly (21%).

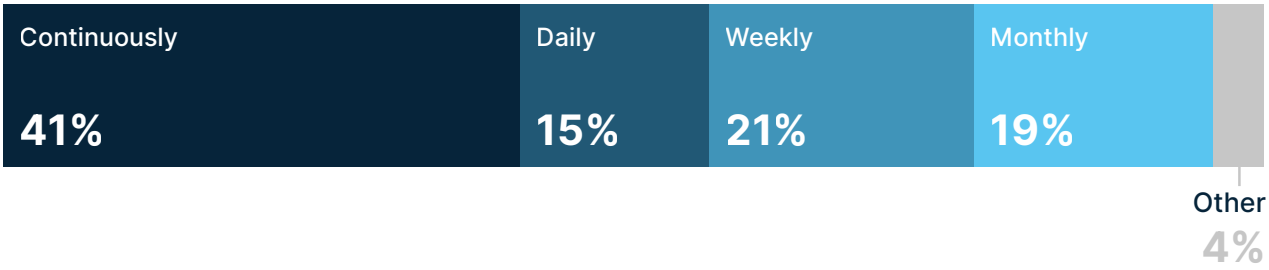
This is particularly important as the number of vulnerabilities discovered each year has grown exponentially over the past decade: there were 5,297 CVEs reported in 2012 compared to 25,227 CVEs in 2022—representing nearly a 500% increase in vulnerabilities.

Most organizations today use a combination of VLAN segmentation, physical firewalls, and virtual firewalls for workload segmentation in their networks.

Approximately 21% also use containerized firewalls. As cloud and container adoption continues to increase, virtual and containerized firewall deployments will likely also increase, enabling organizations to implement more granular microsegmentation and security policies across their cloud environments.

Q51

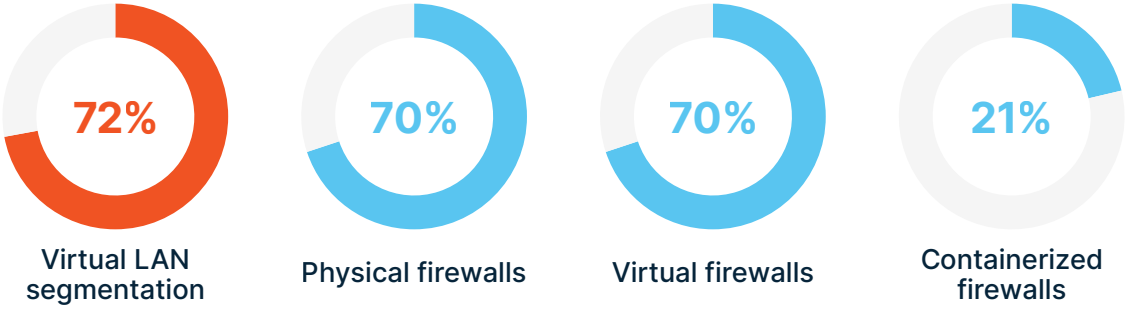
How often does your organization perform vulnerability scanning on network devices?



Q50

How does your organization segment application workloads in your network?

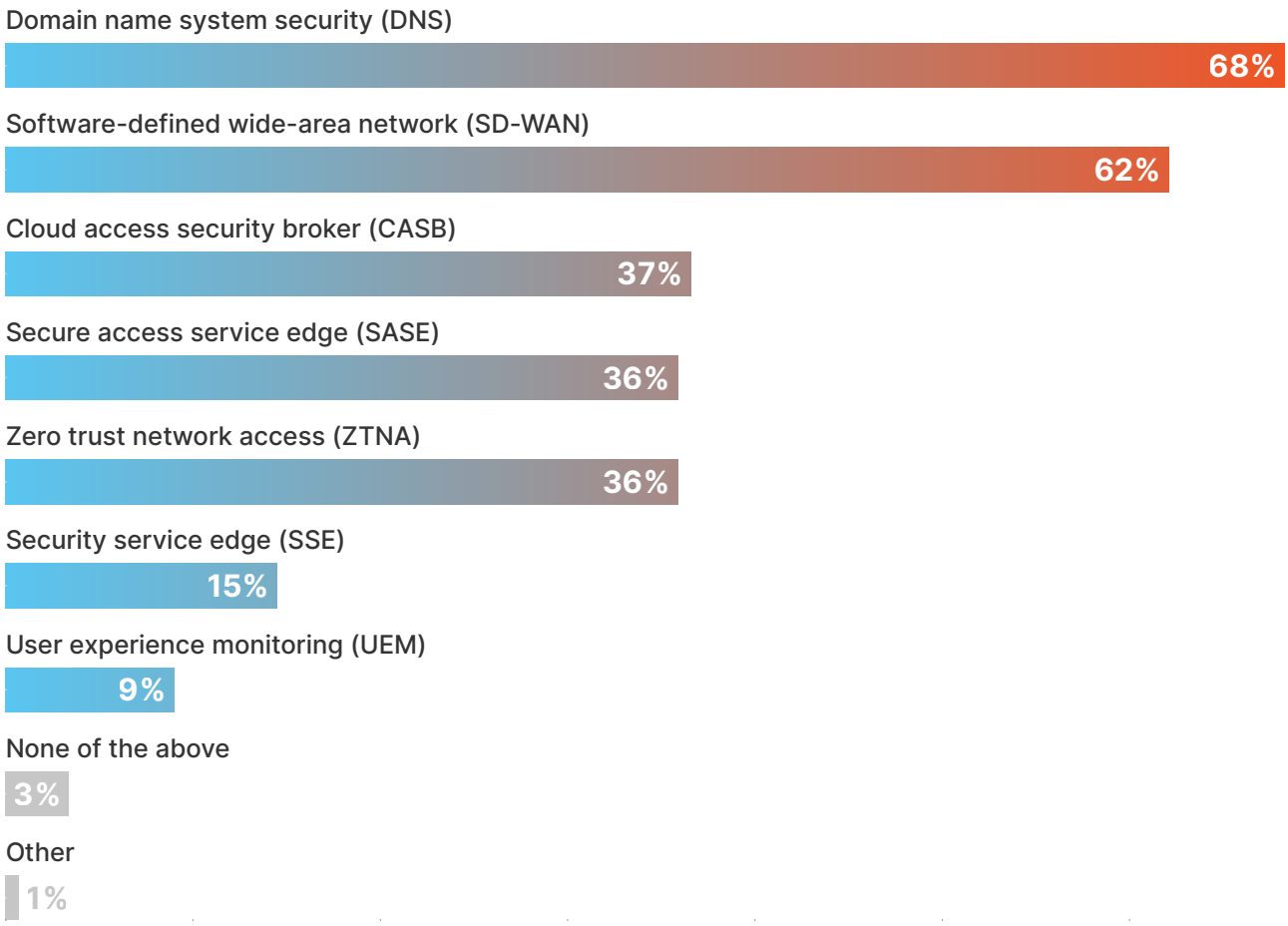
(Select all that apply)



Q52

Which of the following network security technologies does your organization use?

(Select all that apply)



DNS Security and SD-WAN are commonly deployed across all organizations.

CASB, SASE, and ZTNA adoption is growing, but is still deployed in fewer than half of all organizations. This limited adoption may be due to uncertainty and confusion as many vendors have attempted to rebrand or repurpose their traditional solutions to fit these emerging categories. Additionally, many of these individual technologies are core components of broader solutions. For example, SASE is considered to be an evolution of SSE that combines DNS Security, SD-WAN, CASB, ZTNA, and UEM (or variations thereof) into a single, unified platform.

CASB, SASE, and ZTNA adoption is growing, but is still deployed in fewer than half of all organizations.

Approximately one-third of organizations use DKIM/DMARC and DNS security tools.

Adoption of DNSSEC and SPF has been relatively limited. In all cases, adoption needs to increase significantly. All of these technologies/services need to be deployed as part of a comprehensive email security strategy given that email (specifically, phishing) remains an extremely vulnerable and effective attack vector for threat actors.

The majority of organizations use a combination of firmware updates, network segmentation, strong authentication, and device hardening to secure network-connected devices such as endpoints, mobile devices, and IoT devices.

However, adoption needs to increase as these are all generally well understood and relatively low-cost best practices that go a long way toward securing network-connected devices.

Q53

Which of the following DNS security technologies/services does your organization use?

Domain keys identified mail (DKIM)/domain-based message authentication, reporting, and conformance (DMARC)

Domain name system security extensions (DNSSEC)

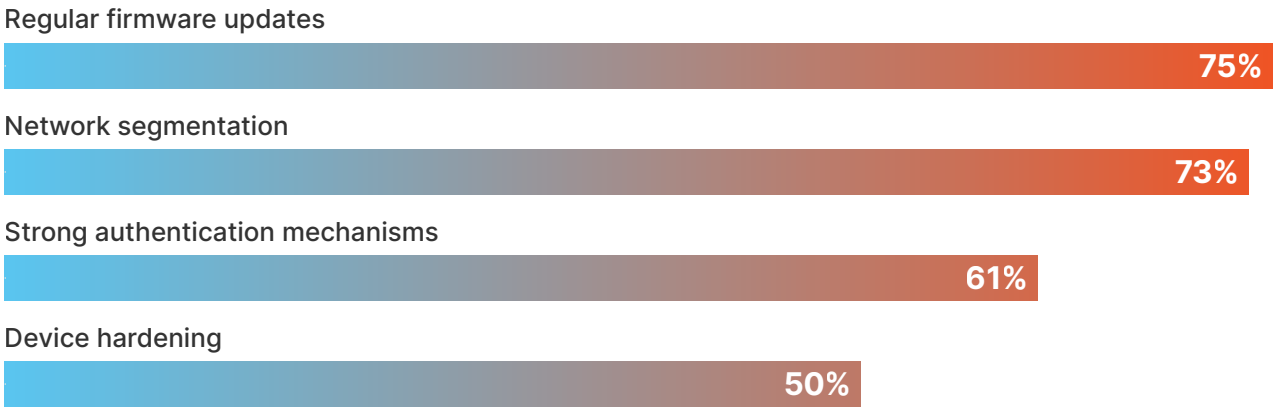
Domain name system (DNS) security

Sender policy framework (SPF)

Q54

Which best practices does your organization follow to secure network-connected devices (e.g., IoT devices)?

(Select all that apply)



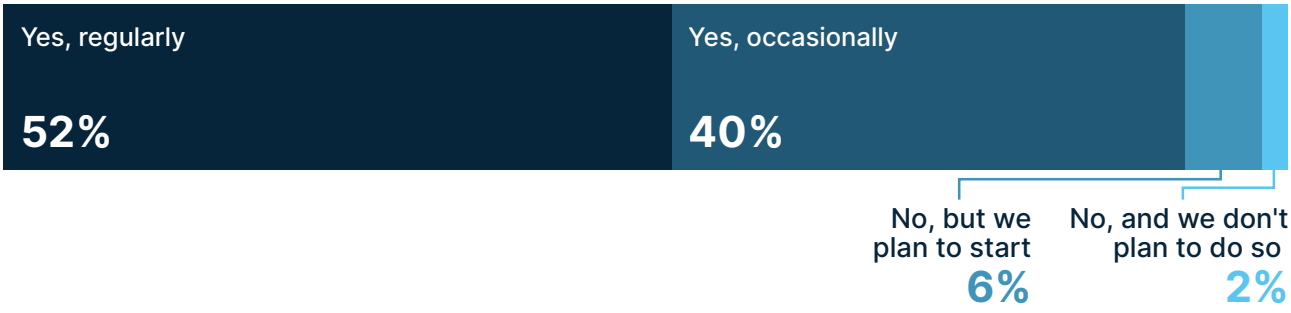
Network penetration testing and vulnerability assessments are part of a mature security program as evidenced by more than 90% of organizations conducting these tests/assessments either regularly or occasionally.

However, organizations need to be diligent in their selection of vendors to perform these services. In particular, penetration testing has become increasingly popular with executives leading to rapid growth in this segment with many new players that may lack the appropriate skills and experience, and more experience and established players at the opposite end of the spectrum who may be tempted to "rest on their laurels" and "rinse-and-repeat" an out-of-the-box engagement.

Penetration testing has become increasingly popular with executives leading to rapid growth in this segment with many new players that may lack the appropriate skills and experience.

Q55

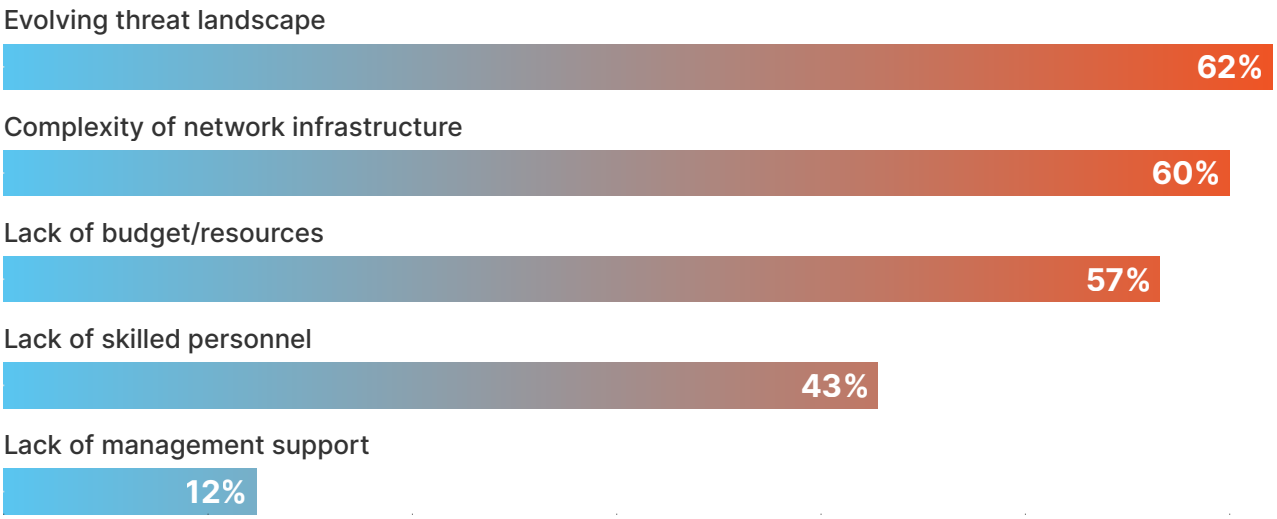
Does your organization conduct periodic penetration testing and vulnerability assessments on the network infrastructure?



Q56

What are the top challenges your organization faces concerning network security?

(Select all that apply)



Across all organizations, the evolving threat landscape, complexity of the network infrastructure, and lack of budget/resources were cited as the top challenges.

Although there is little that organizations can do to address the evolving threat landscape beyond keeping abreast of the latest threats, reducing complexity in network (and cloud) infrastructure is an area that IT organizations can directly address, which will often concurrently address other challenges (such as lack of budget/resources and lack of skilled personnel).

Reducing complexity in network (and cloud) infrastructure is an area that IT organizations can directly address, which will often concurrently address other challenges.

SECURITY OPERATIONS

The majority of organizations responded that they're able to detect and respond to network security incidents within hours.

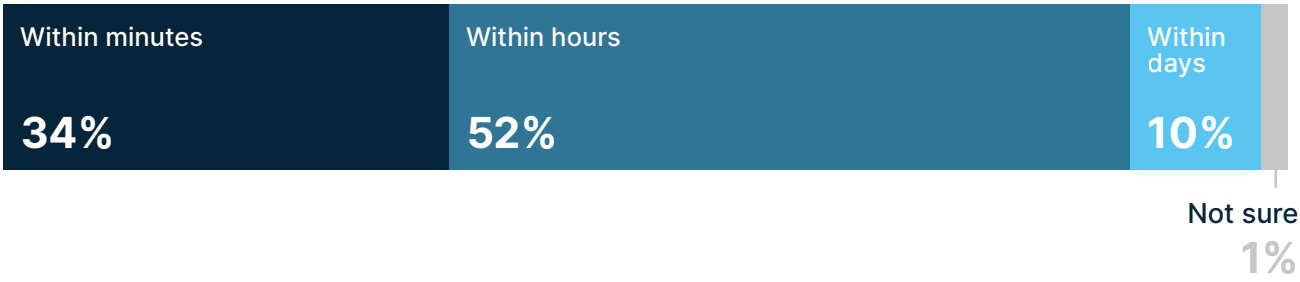
This is an alarming and perhaps overly optimistic response as the Verizon Data Breach Investigations Report (DBIR) and IBM Security Cost of a Data Breach consistently report breaches going undetected for many months (204 days, on average, to detect a breach according to the 2023 IBM Security report).

According to IBM Security, the average time to contain an incident in 2023 was 73 days.

However, respondents may have an unrealistic perception of their incident response capabilities as most (98%) responded that they can respond to and contain threats on endpoints in less than a day. This may also be attributed to an overreliance on EDR and antimalware tools to fully contain endpoint security incidents.

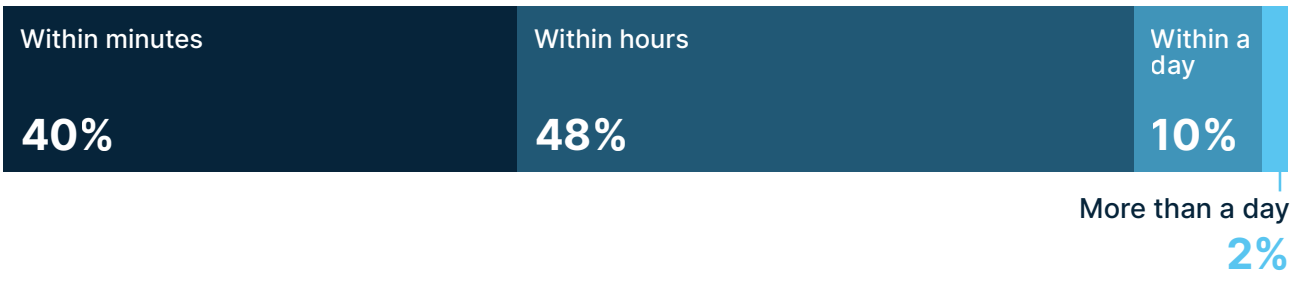
Q57

What is the average time it takes for your organization to detect and respond to network security incidents?



Q58

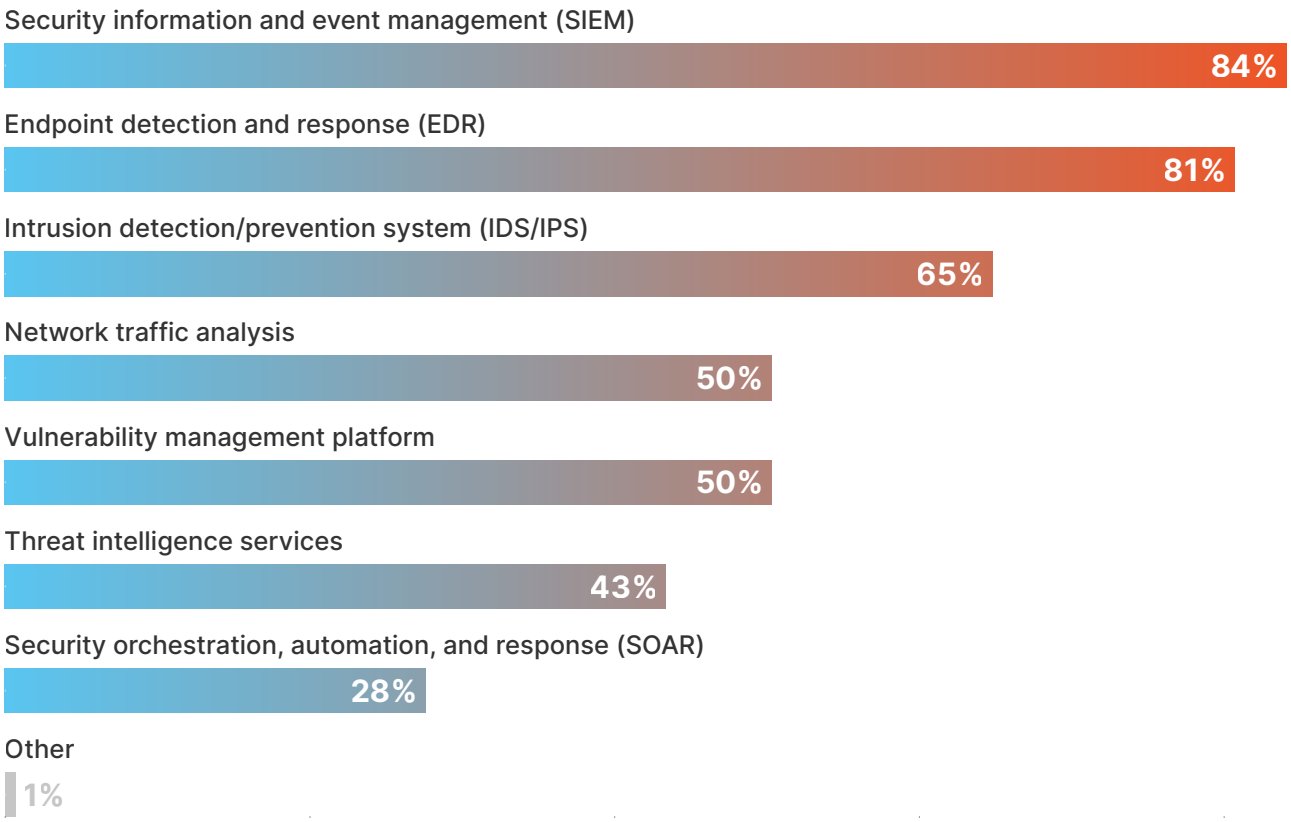
In case of a security incident, how quickly can you respond to and contain threats on endpoints?



Q59

Which security tools do you use on a regular basis?

(Select all that apply)



SIEM, EDR, and IDS/IPS are the most commonly used security tools across security teams.

Although important, SIEM, EDR, and IDS/IPS are more traditional and mature solutions that don't address the full spectrum of threats. Unfortunately, important tools such as NTA, vulnerability management, threat intelligence, and SOAR are not used as frequently, representing potential coverage gaps and inefficiencies. As these tools make extensive use of automation and AI/ML technologies, their role in security is becoming increasingly important as a force multiplier enabling organizations with limited resources to stay ahead of threat actors who leverage automation and AI/ML for malicious purposes.

Important tools such as NTA, vulnerability management, threat intelligence, and SOAR are not used as frequently, representing potential coverage gaps and inefficiencies.

More than half of organizations conduct SecOps exercises or simulations either weekly, monthly, or quarterly.

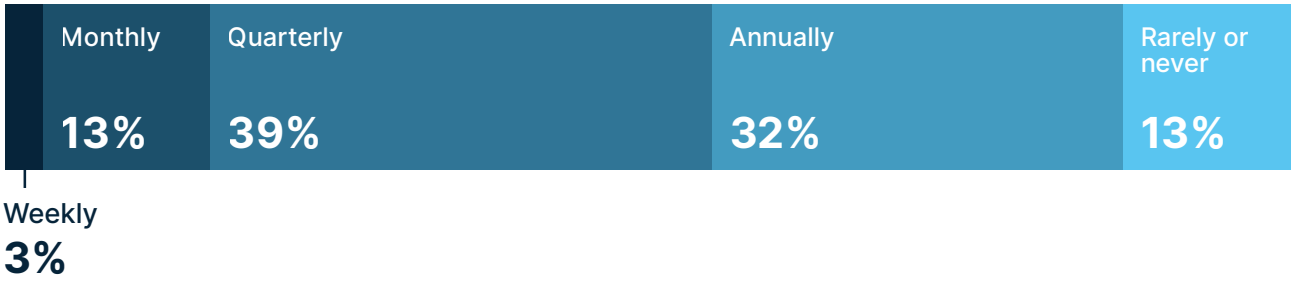
Still, nearly half do so only annually, rarely, or not at all. Even basic tabletop exercises are valuable for ensuring that SecOps and incident response teams understand and are able to perform their individual roles and responsibilities.

Common challenges across all organizations include limited staff resources, alert fatigue, and lack of correlation due to siloed tools.

These challenges are all interrelated and many security vendors are focused on delivering unified toolsets that can be used by cross-functional teams to improve incident response.

Q60

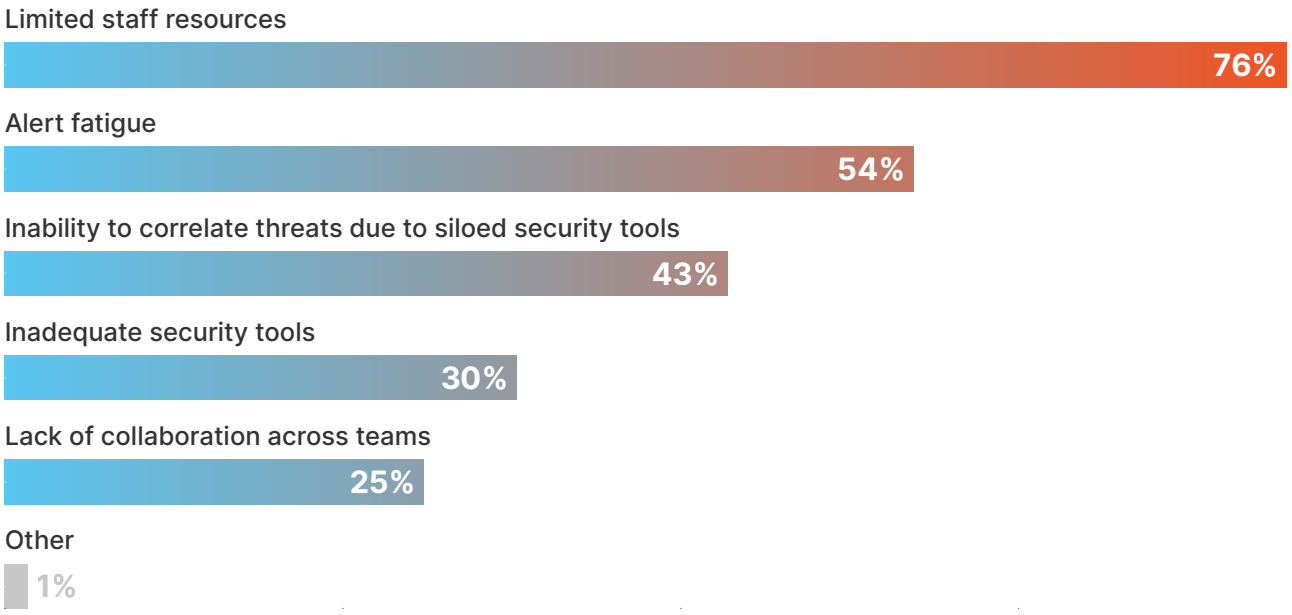
How often do you conduct SecOps exercises or simulations?



Q61

What are the major challenges you face in handling security incidents?

(Select all that apply)



Q62

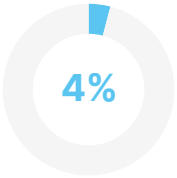
Do you use threat intelligence services to enhance your security operations?

Yes, we have at least one threat intelligence service

Yes, we subscribe to multiple threat intelligence services

Yes, we subscribe to multiple threat intelligence services, do our own threat intelligence research, and share threat intelligence with industry peers

No, but we are planning to start

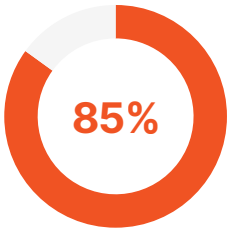


No, and no plans to use it

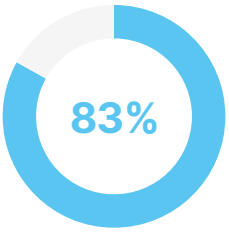
Q63

Which of the following playbooks have you created or plan to create?

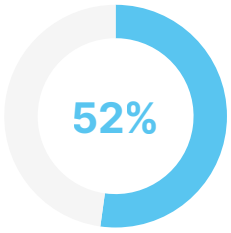
(Select all that apply)



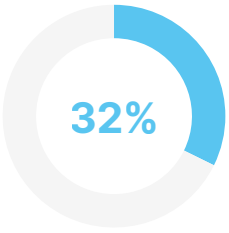
Ransomware



Phishing



Insider threat



Advanced persistent threat (APT)

Threat intelligence is critical to ensure organizations are continuously aware of new and evolving threats.

More than half of all organizations use multiple threat intelligence services to enhance their security operations. Less than 30% only use a single threat intelligence service, and nearly 18% are not currently using threat intelligence services.

Playbooks are a relatively inexpensive yet extremely effective tool for ensuring that SecOps and incident response teams can respond to common threats.

More than 80% of organizations have created playbooks to address ransomware and phishing, while approximately 50% have created insider threat playbooks.

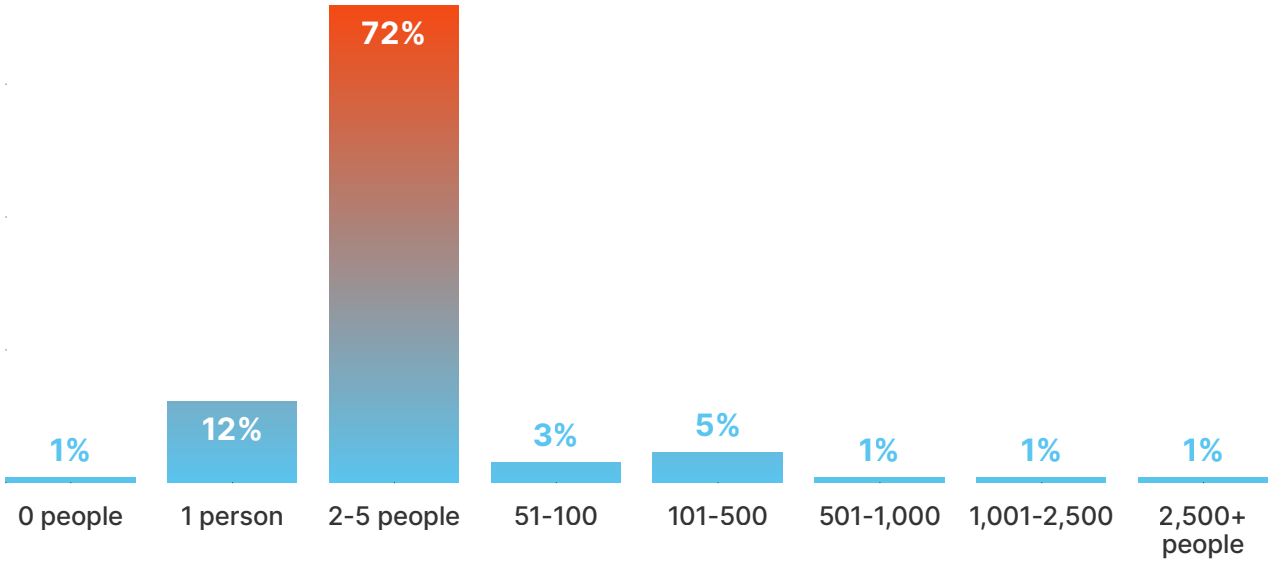
Appendix

COMPANY SIZE UNDER 500

LEVEL-SET AND DEMOGRAPHICS

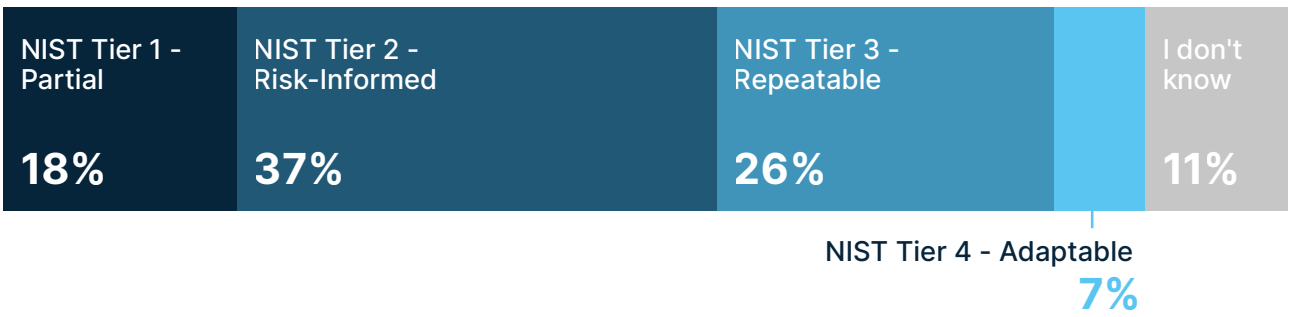
Q1

How large is your overall information security team?



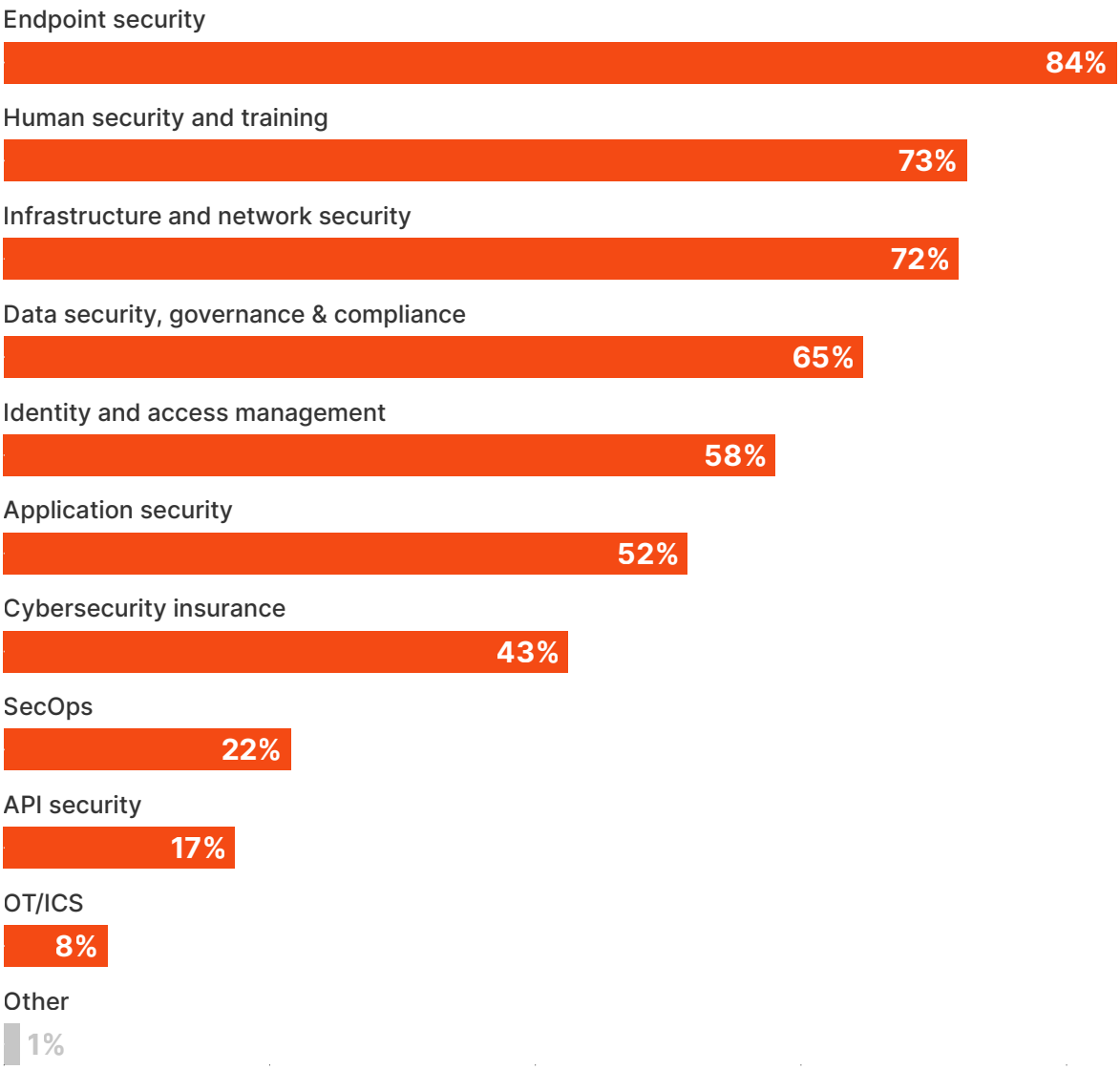
Q2

Describe the maturity of your cybersecurity program.



Q3

What are your company's key cybersecurity tech stack components/solutions?



DRIVERS/PAINS FOR ACTION

Q4

What threats are you prioritizing right now?

(Select all that apply and rank highest to lowest priority)

1	Phishing attacks
2	Ransomware
3	Malware
4	Social engineering
5	Password attacks
6	Zero-day exploits
7	Insider threats
8	Distributed denial of service (DDoS) attacks
9	Supply chain attacks
10	Man-in-the-middle (MitM) attacks
11	Physical security breaches
12	Shadow IT
13	Other

Q5

What are your overall corporate IT priorities or investments in the coming year?

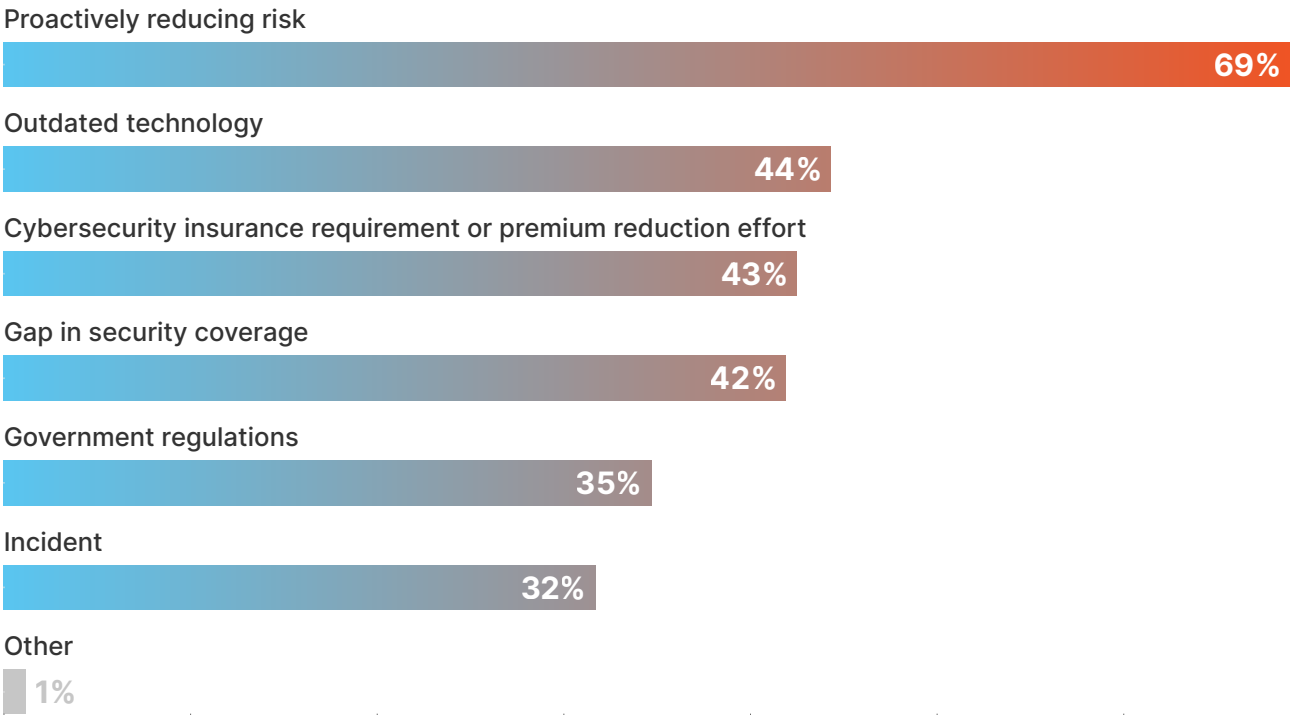
(Select 5 and rank highest to lowest priority)

1	Cost optimization and efficiency
2	Cybersec investments
3	Resiliency/business continuity projects
4	App/stack/tech modernization
5	Cloud migration
6	Regulatory/compliance projects
7	Digital transformation projects
8	Data projects
9	Talent
10	Supply chain efficiencies/ improvements
11	Other

Q6

What are your primary motivators for engaging in a new solution purchase?

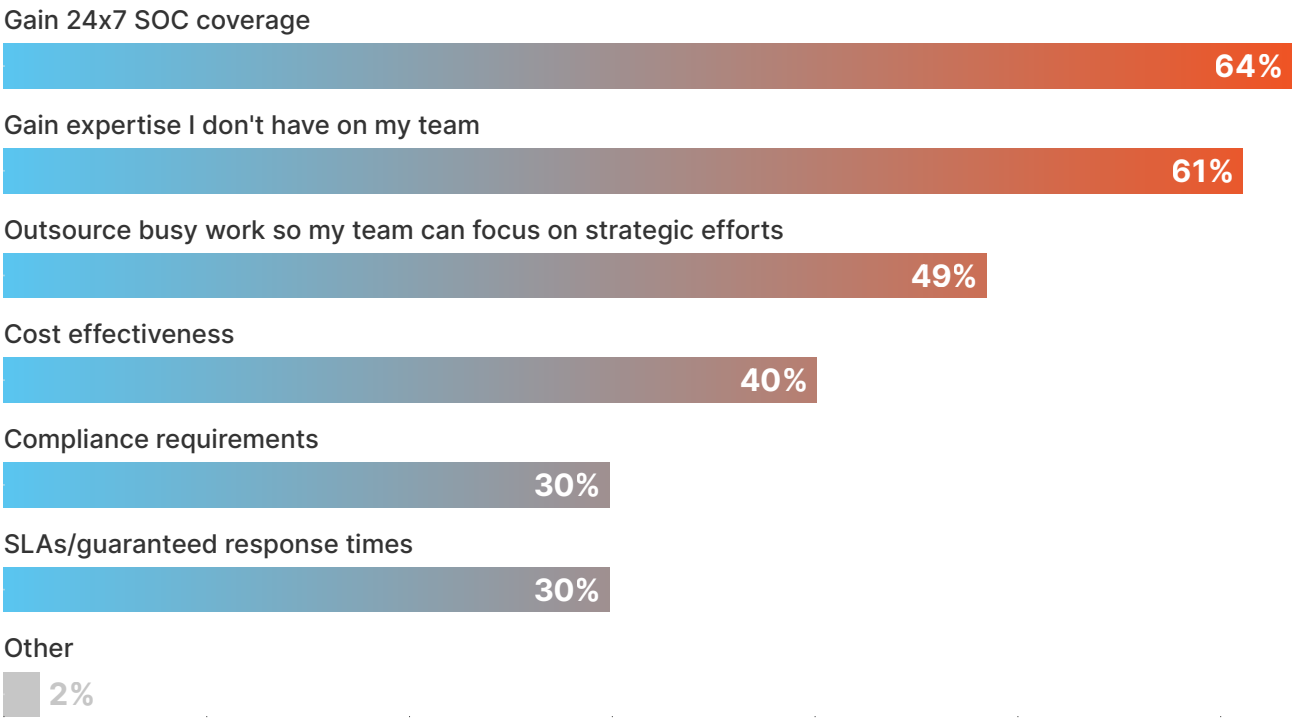
(Select all that apply)



Q7

What are the primary reasons you would engage with a managed service provider vs. managing a solution in-house?

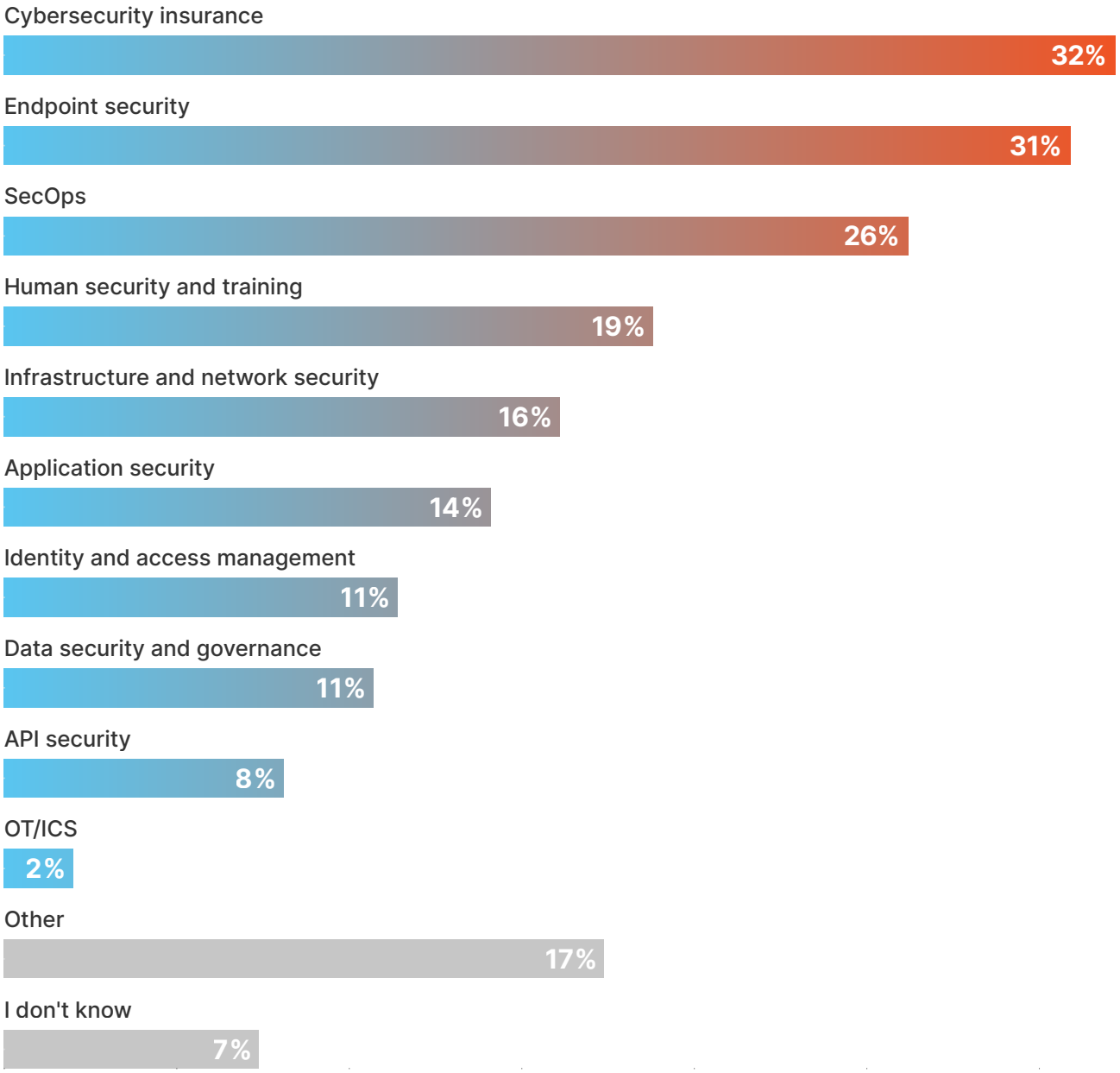
(Select all that apply)



Q8

What cybersecurity categories are you outsourcing right now?

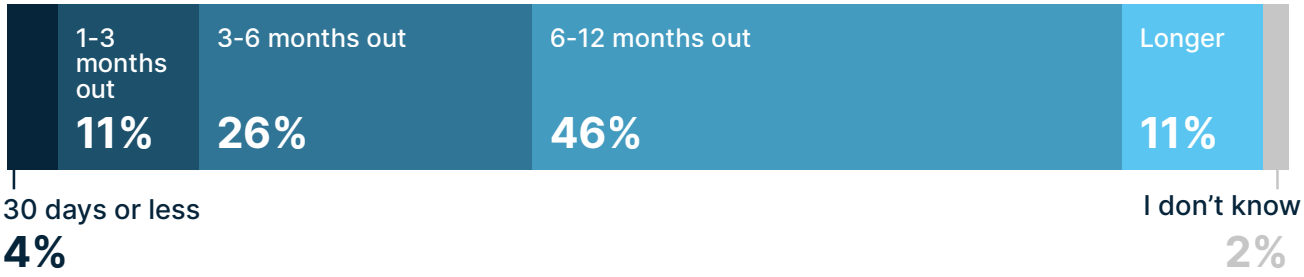
(Select all that apply)



THE BUYING PROCESS & BEHAVIOR

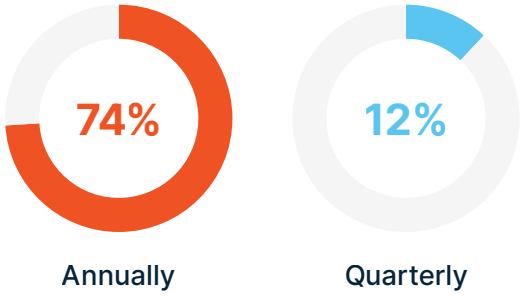
Q9

How far in advance do you start your budgeting process for cybersecurity solutions?



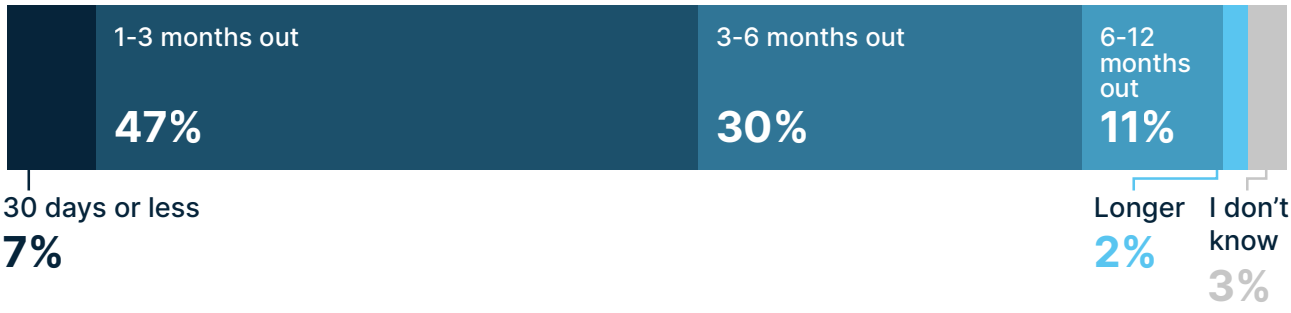
Q10

Do you budget annually or quarterly?

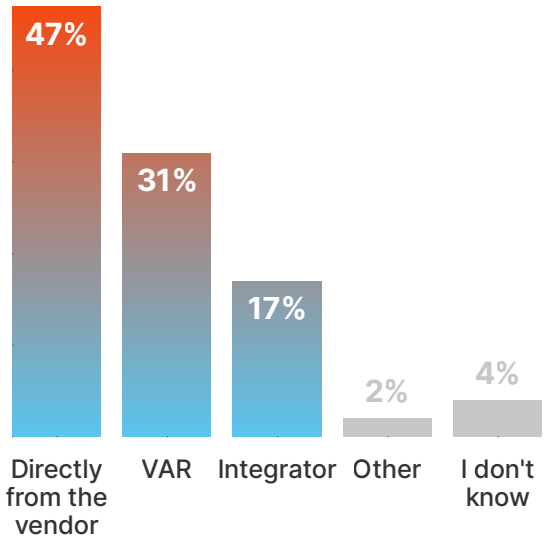


Q11

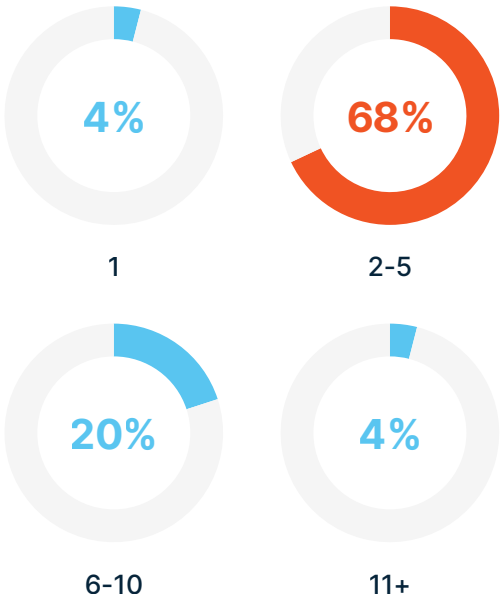
How long does your typical vendor selection process take? (From research to final decision)



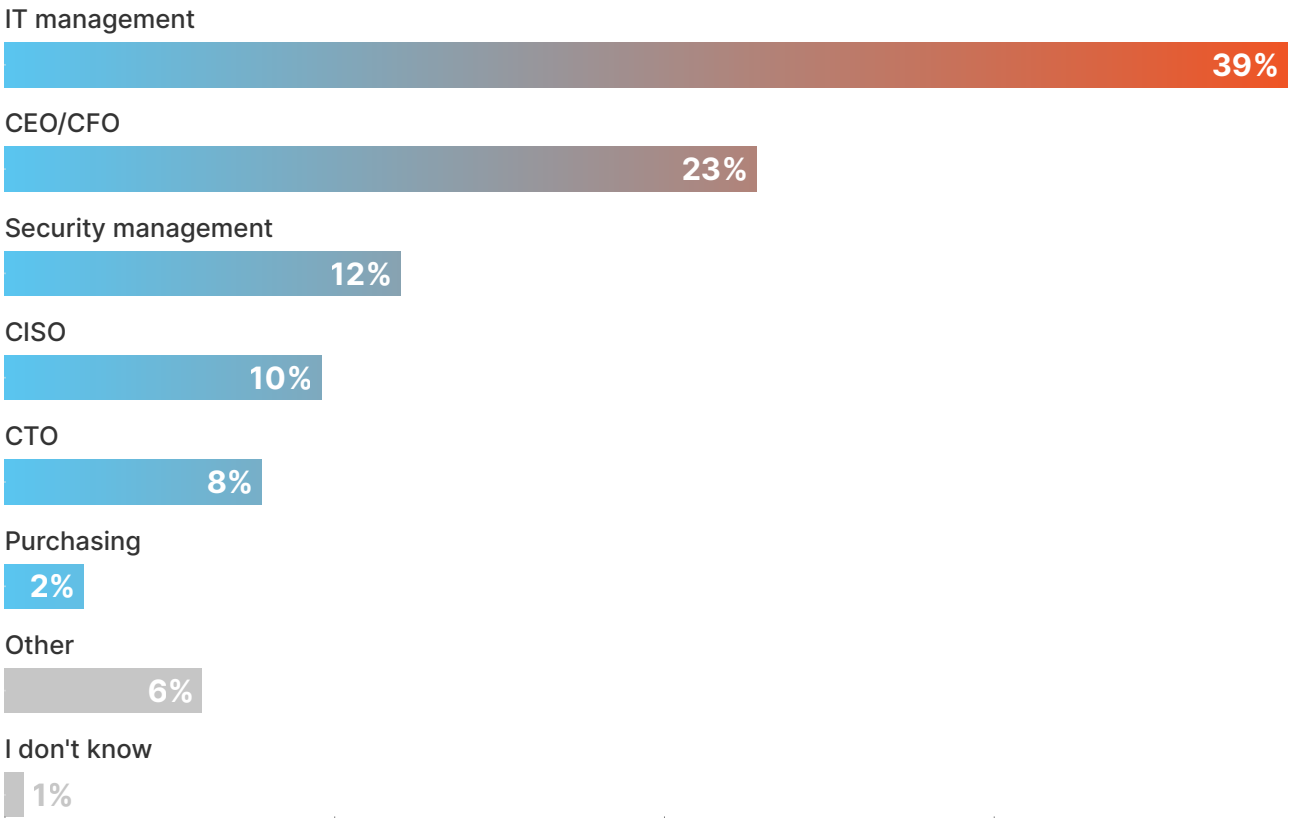
Q12 Where do you typically prefer to procure cybersecurity solutions?



Q13 How many key members or stakeholders are typically on your decision committee for cybersecurity solutions?



Q14 Who typically makes the final decision?



Q15

What is your typical decision criteria when selecting vendors?

(Select all that apply and rank highest to lowest priority)

1. Product/service features
2. Pricing
3. Vendor reputation
4. Support and licensing
5. Risk assessment
6. Stakeholder recommendations
7. Supplier relationship
8. Sustainability and ethics
9. Other

Q16

When selecting a new cybersecurity tool, what is your primary goal or outcome?

(Select all that apply and rank highest to lowest priority)

1. Reduce risk
2. Increase visibility into security posture
3. Save time/automate processes
4. Reduce costs
5. Better metrics/dashboards
6. Sustainability and ethics
7. Other

Q17

What are your primary concerns when considering running a proof-of-concept (PoC) with a cybersecurity vendor?

(Select all that apply and rank highest to lowest concern)

1. Integration with existing systems
2. Resource allocation
3. Scope
4. Establishing evaluation and measurement criteria
5. Timeline
6. Data privacy and protection
7. Vendor engagement and support
8. Stakeholder involvement
9. Exit strategy for the PoC
10. Other

Q18

Where do you typically like to learn about new cybersecurity solutions?

Select all that apply and rank by most important to least important)