Enterprise
Strategy Group™
by TechTarget

Generative AI for Cybersecurity:
An Optimistic but Uncertain Future

Jon Oltsik | Distinguished Analyst and Fellow

ENTERPRISE STRATEGY GROUP

JANUARY 2024

Research Objectives

Since the introduction of ChatGPT in November 2022, generative AI (GenAI) has been described as everything from a novelty and an economic boon to a threat to humanity. As this debate continued, GenAI took center stage at the RSA Conference 2023 with the introduction of and subsequent hoopla around Microsoft Security Copilot. Many other vendors have introduced similar capabilities since. Few would argue against the idea that GenAI (and AI in general) will have a profound impact on society and global economics, but in the near term, it introduces new risks as employees connect to GenAI applications, share data, and build homegrown large language models (LLMs) of their own. These actions will inevitably expand the attack surface, open new threat vectors, introduce software vulnerabilities, and lead to data leakage.

Despite these risks, generative AI holds great cybersecurity potential. Generative AI could help improve security team productivity, accelerate threat detection, automate remediation actions, and guide incident response. These prospective benefits are so compelling that many CISOs are already experimenting with GenAI or building their own security LLMs. At the same time, security professionals remain anxious about how cybercriminals may use GenAI as part of attack campaigns, and how they can defend against these advances.

Have organizations embraced GenAI for cybersecurity today, and what will they do in the future? To gain further insight into these trends, TechTarget's Enterprise Strategy Group (ESG) surveyed 370 IT and cybersecurity professionals at organizations in North America (US and Canada) responsible for cyber-risk management, threat intelligence analysis, and security operations, with visibility into current GenAI usage and strategic plans.

This study sought to:

- Identify current usage of and plans for generative AI.

- Establish how generative AI influences the balance of power between cyber-adversaries and cyber-defenders.

- Determine how organizations are approaching generative AI governance, policies, and policy enforcement.

- Monitor how organizations will apply generative AI for cybersecurity use cases.

KEY FINDINGS:

Generative AI Has a Foothold Today and Will Be Pervasive by the End of 2024

Many Are Already Developing Proprietary LLMs to Support a Variety of GenAI Use Cases
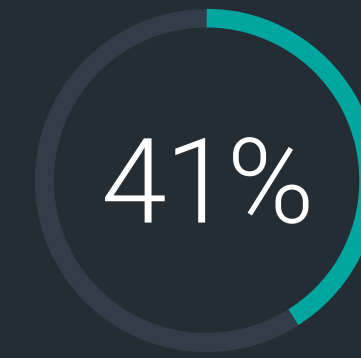
The research indicates that 85% of organizations have a proprietary large language model in place, while another 13% report that they are in the process of developing one. It's likely that many of these are early-stage projects based on open models. Nevertheless, this data indicates robust activity, forecasting rapid development of production applications in 2024.

Which business functions are ripe for GenAI applications? Organizations are well underway toward ubiquitous use of GenAI in areas like IT operations, software development, sales, research, and others. Like "shadow IT" in the past, growing use of GenAI will introduce cyber-risks as multiple departments and individual employees interact with open GenAI applications, experiment with open source, and create their own LLMs. CISOs must assess and communicate these risks while working with executives to create the right governance models and policies for risk mitigation. Additionally, security professionals must implement compensating controls and monitor users and networks for anomalous, suspicious, and malicious behavior.
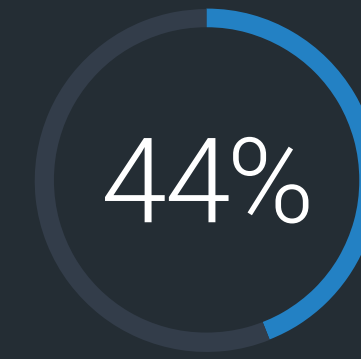
Top five current or planned GenAI use cases.

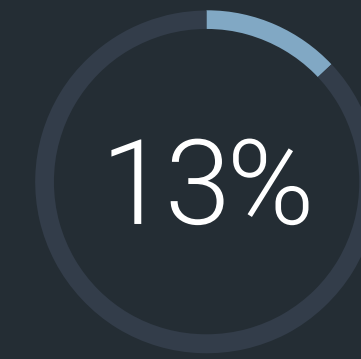| Use case	Percentage
IT operations	66%
Software development	36%
Sales	29%
Research	26%
Product development	25%

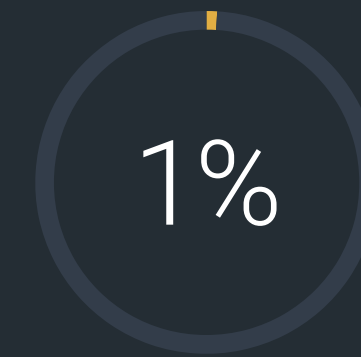**Development plans for proprietary large language models.**

41% LLMs are already a part of production generative AI applications
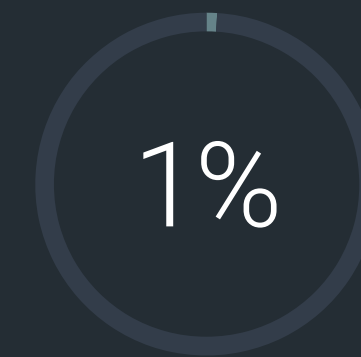
44% LLMs are already a part of an ongoing development project

13% We are just getting started developing our own LLMs

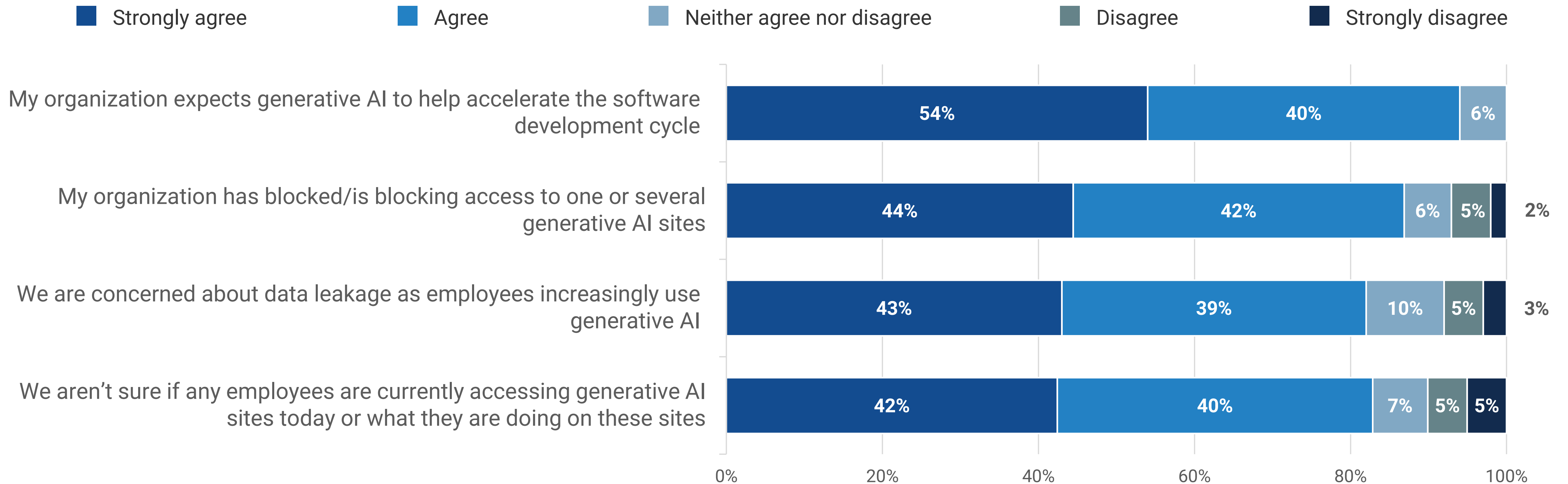**1%** We plan to develop our own LLMs in the future

1% We are interested in developing our own LLMs in the future

Pervasive Security Concerns for Generative AI

Mitigating GenAI risk is not some future requirement. Rather, organizations are already dealing with, or struggling to address, generative AI risks proactively. Respondents claim that their organizations are already blocking access to generative AI sites. Security professionals are also concerned about GenAI-driven data leakage and remain unsure as to whether employees are already accessing and using GenAI applications today. CISOs must address these risks before losing control of who does what with GenAI across the enterprise.

*"*Organizations are already dealing with, **or struggling to address**, generative AI risks proactively.*"*

Cybersecurity professionals' GenAI opinions.

Legend: ■ Strongly agree ■ Agree ■ Neither agree nor disagree ■ Disagree ■ Strongly disagree

My organization expects generative AI to help accelerate the software development cycle: 54% / 40% / 6%

My organization has blocked/is blocking access to one or several generative AI sites: 44% / 42% / 6% / 5% / 2%

We are concerned about data leakage as employees increasingly use generative AI: 43% / 39% / 10% / 5% / 3%

We aren't sure if any employees are currently accessing generative AI sites today or what they are doing on these sites: 42% / 40% / 7% / 5% / 5%

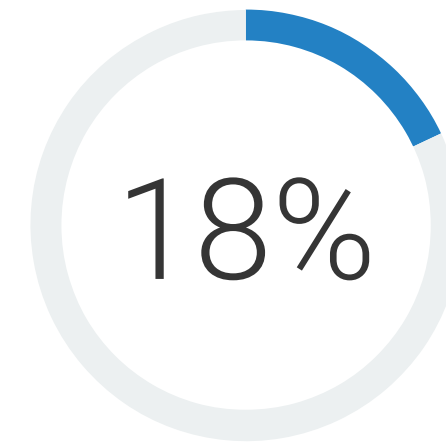**Plans for a specific GenAI governance structure.**

Many Are Getting Ahead of GenAI Governance, Especially Larger Organizations

Of course, most organizations have acceptable use policies and governance models in place today that may provide needed guardrails for GenAI usage. Recognizing additional risks associated with GenAI, many firms are creating specific governance models. Larger enterprise organizations, with the most at risk, are taking the GenAI governance lead, while their smaller counterparts lag. CISOs at these organizations must act as a catalyst to accelerate the creation of governance models, policies, and policy enforcement controls. Given the pace of GenAI innovation, delays will only lead to rapidly increasing risk.

10%

We already have
a specific GenAI
governance structure

18%

We are developing
a specific GenAI
governance structure

36%
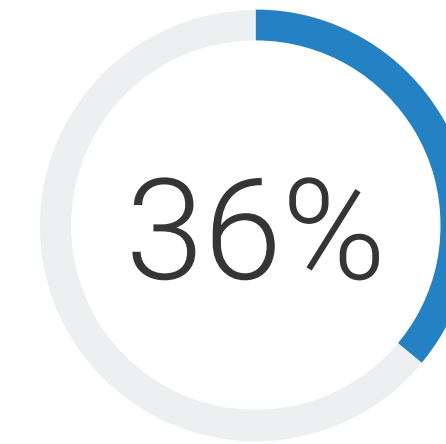
We are interested in
developing a specific GenAI
governance structure

2%
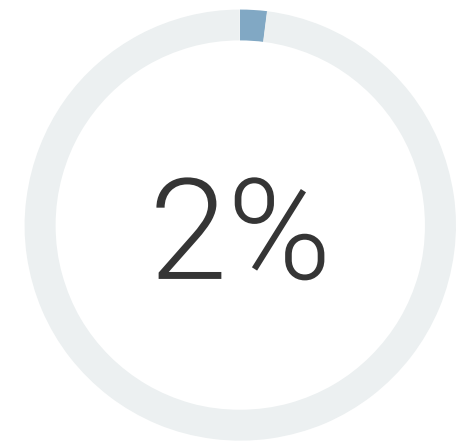
We believe our existing
governance and acceptable use
policies apply to generative AI

Percentage of organizations that already have a specific governance structure for the use of generative AI by company size.

34%

1,000 to 2,499 employees

41%

2,500 to 4,999 employees

73%

5,000 or more employees

Weakest Areas of GenAI Governance

While many organizations have created or are creating GenAI governance models, security professionals admit that these models have abundant weaknesses, including third-party risk management (29%), data leakage protection/rights management (27%), regulatory compliance (26%), and enforcing GenAI access policies (26%). Based on the data, it is safe to assume that most organizations have a myriad of these weaknesses in place today. Closing these gaps should be a 2024 priority.
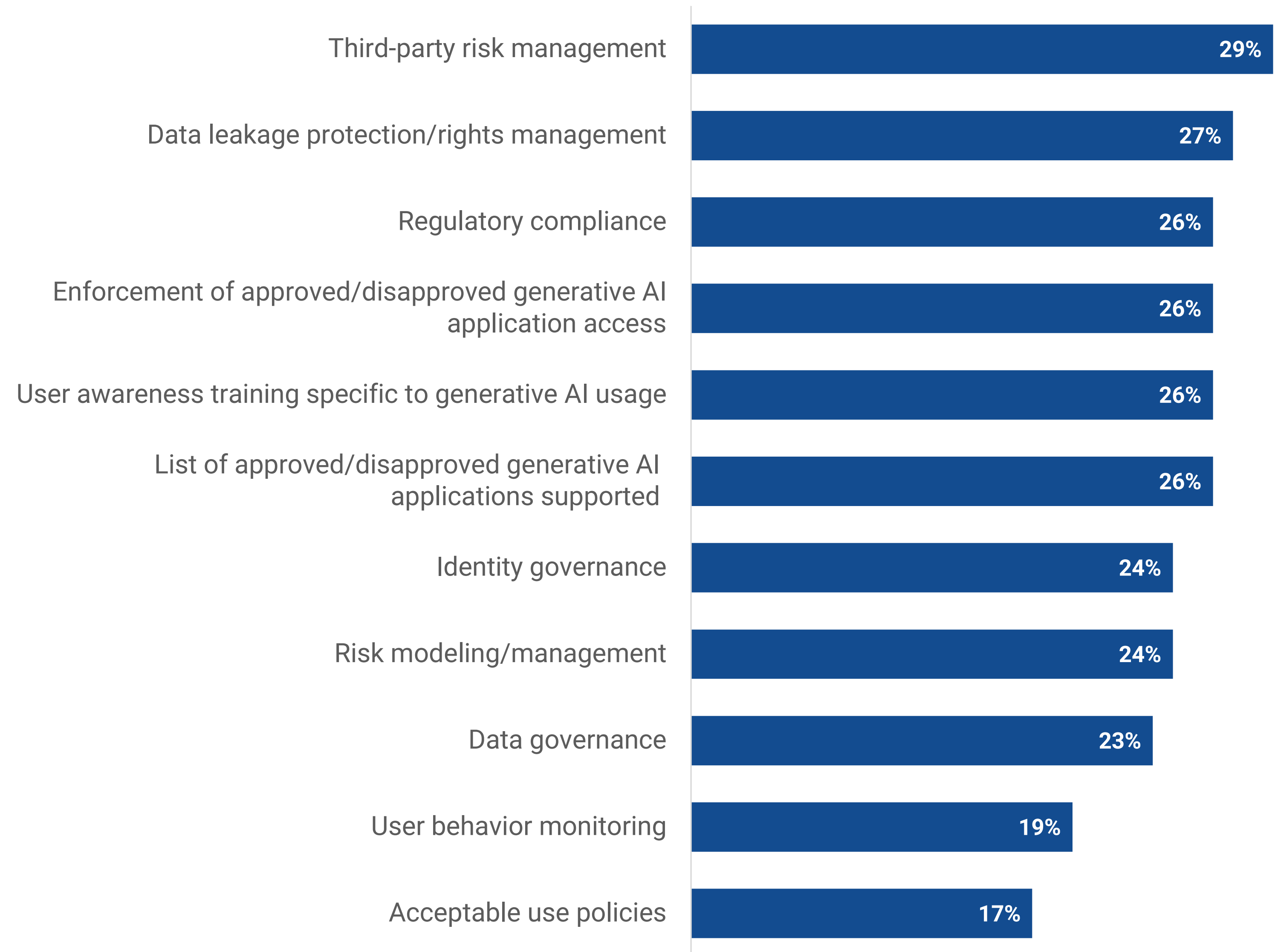
Weakest areas of generative AI governance and policy enforcement.

Category	%
Third-party risk management	29%
Data leakage protection/rights management	27%
Regulatory compliance	26%
Enforcement of approved/disapproved generative AI application access	26%
User awareness training specific to generative AI usage	26%
List of approved/disapproved generative AI applications supported	26%
Identity governance	24%
Risk modeling/management	24%
Data governance	23%
User behavior monitoring	19%
Acceptable use policies	17%

Organizations Anticipate Generative AI Risks

Generative AI Risks Associated With LLMs

As organizations experiment with GenAI applications and build their own LLMs, they face several application security challenges such as trust boundary risks (i.e., where data comes from or when it moves to an untrusted source), data management risks (e.g., data leakage or corruption), inherent underlying model risks, and general security risks. Security professionals are especially apprehensive about data management risks, while IT professionals' concerns focus on trust boundary risks. Organizations must reinforce their application security efforts with oversight, tooling, and testing to address specific GenAI application security.

Biggest risk to LLM and generative AI application development by role.

IT professionals with cybersecurity responsibilities Pure cybersecurity professionals Overall

Trust boundary risks
- 26%
- 47%
- 53%

Inherent underlying model risks
- 7%
- 9%
- 8%

Data management risks
- 63%
- 44%
- 36%

General security risks
- 4%
- 1%
- 2%

# GenAI Balance of Power Skews Toward Cyber-adversary Advantage

Of course, cyber-adversaries also have access to open GenAI applications and have the technical capabilities to develop their own LLMs. WormGPT and FraudGPT are early examples of LLMs designed for use by cybercriminals and hackers. Will cyber-adversaries use and benefit from LLMs? More than three-quarters of survey respondents (76%) not only believe they will, but also feel that cyber-adversaries will gain the biggest advantage (over cyber-defenders) from generative AI innovation.

Alarmingly, most security professionals believe that cyber-adversaries are already using GenAI and that adversaries always gain an advantage with new technologies. Respondents also believe that GenAI could lead to an increase in threat volume, as it makes it easier for unskilled cyber-adversaries to develop more sophisticated attacks. Security and IT pros are also concerned about deep fakes and automated attacks.

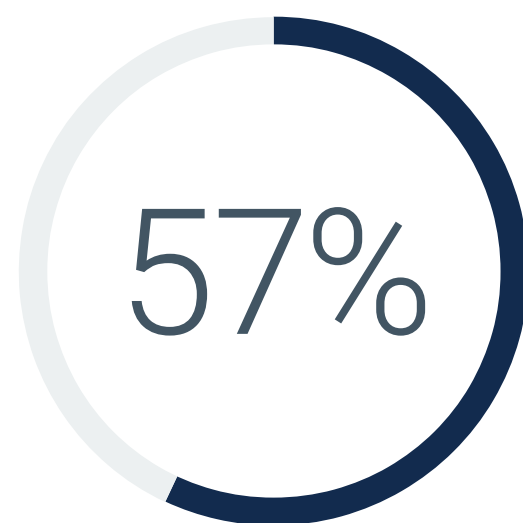**Group expected to gain <u>biggest advantage</u> from generative AI innovation.**

76%
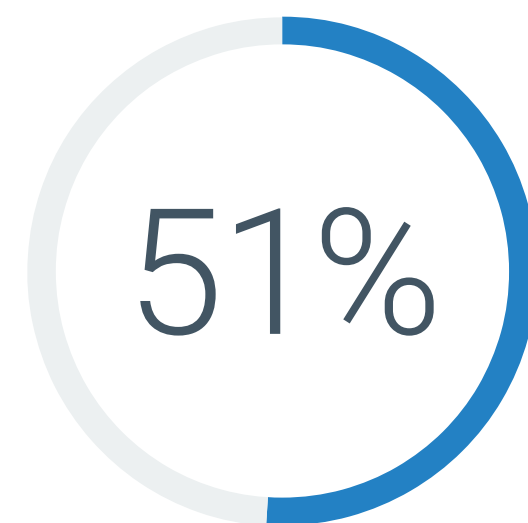### Cyber-adversaries
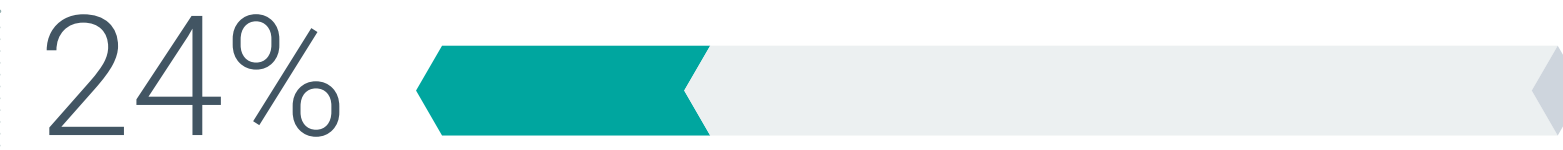
24%
Security defenders

Top five reasons cyber-adversaries will likely gain the biggest advantage from GenAI technology.

57%
Cyber-adversaries are already using generative AI technology to their advantage

55%
Cyber-adversaries always gain an early advantage with new technologies

51%
Generative AI makes it easier for unskilled cyber-adversaries to develop more advanced cyberattacks, so we anticipate greater volumes of attacks
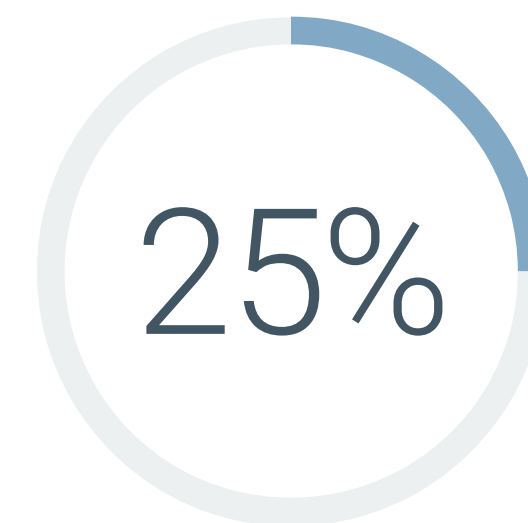
25%
Generative AI can help cyber-adversaries develop realistic deep fakes based on someone's voice or writing style, making it harder to detect malicious behavior
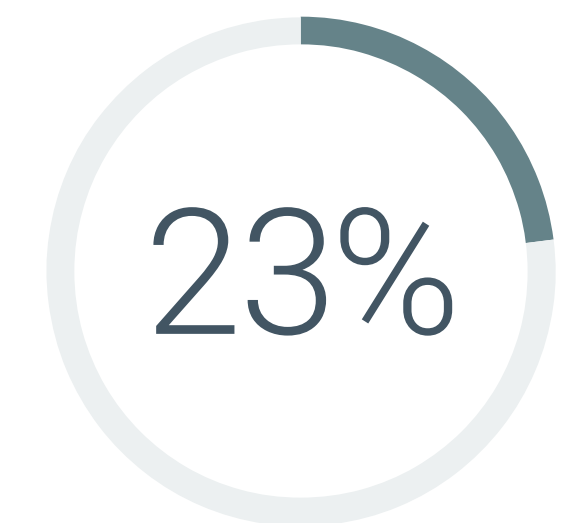
23%
Generative AI can help cyber-adversaries automate attacks

GenAI Broadens the Attack Surface and Expands Social Engineering Tactics

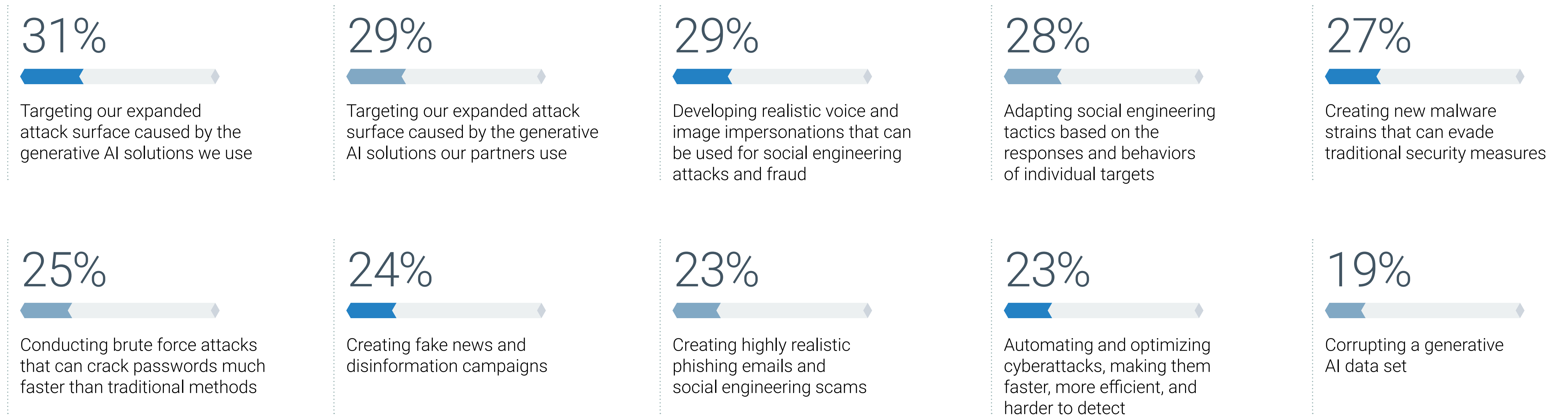Security professionals already have lots of ideas about how adversaries will use GenAI as a component of cyberattacks. Proprietary and partner-based GenAI systems will expand their attack surface, leading to unavoidable vulnerabilities and potential exploitation. Adversaries will use GenAI within phishing, business email compromise (BEC), and other types of deep fakes. There is also a concern about GenAI creating new types of malware (note: researchers have already created polymorphic malware using ChatGPT).

Given the unknown tactics, techniques, and procedures (TTPs), unclear balance of power, and potential GenAI threat vectors, cybersecurity professionals must stay vigilant by monitoring threat intelligence for signs of GenAI-based adversary TTPs and implementing the right controls for policy enforcement.

Most concerning use cases for cyber-adversaries using GenAI.

|				
31%	**29%**	**29%**	**28%**	**27%**
Targeting our expanded attack surface caused by the generative AI solutions we use	Targeting our expanded attack surface caused by the generative AI solutions our partners use	Developing realistic voice and image impersonations that can be used for social engineering attacks and fraud	Adapting social engineering tactics based on the responses and behaviors of individual targets	Creating new malware strains that can evade traditional security measures
25%	**24%**	**23%**	**23%**	**19%**
Conducting brute force attacks that can crack passwords much faster than traditional methods	Creating fake news and disinformation campaigns	Creating highly realistic phishing emails and social engineering scams	Automating and optimizing cyberattacks, making them faster, more efficient, and harder to detect	Corrupting a generative AI data set

Important Security Tools for GenAI Policy Enforcement

While GenAI introduces new types of threats and vulnerabilities, organizations aren't completely defenseless. In fact, existing tools like CASB, SIEM, application security technologies, and identity and access management systems can block threats and enforce policies. For example, CASB systems can allow access to designated web-based GenAI applications for credentialed users while denying access to others. IAM systems can be used to create these credentials based on roles and specific use cases. Application security technologies can scan source code and create threat models that look for trust boundary or data usage violations. SIEM systems can log activity and implement detection rules to alert on any anomalous behavior.

These tools can provide a foundation for GenAI security, but they will need to be configured and customized appropriately to adhere to organizational policies, regulatory compliance, and threats targeting industries, regions, and individual firms.
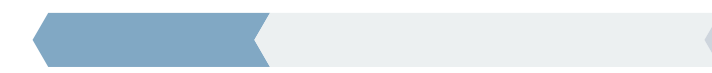
Most important security controls for GenAI policy enforcement.
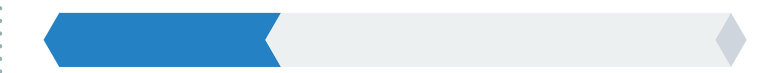
35%
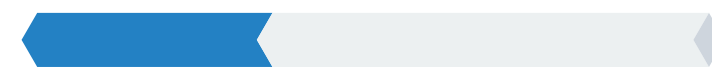
Cloud access security broker (CASB)
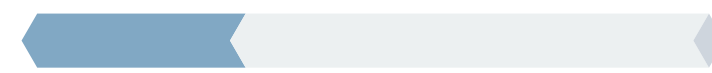
33%

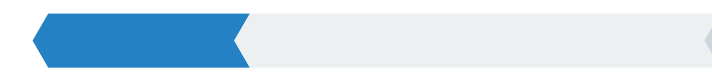Security information and event management (SIEM)
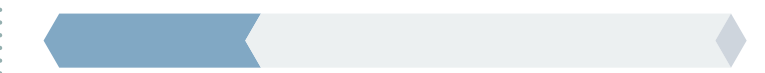
33%

Application security

31%

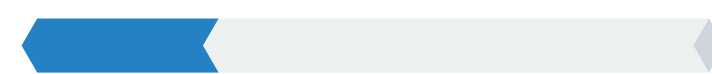Identity and access management (IAM)

30%
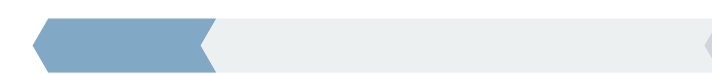
User behavior monitoring

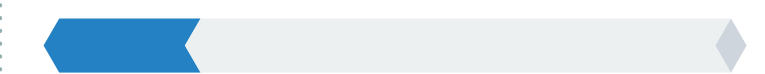**30%**

Email security

27%

Data loss prevention (DLP)
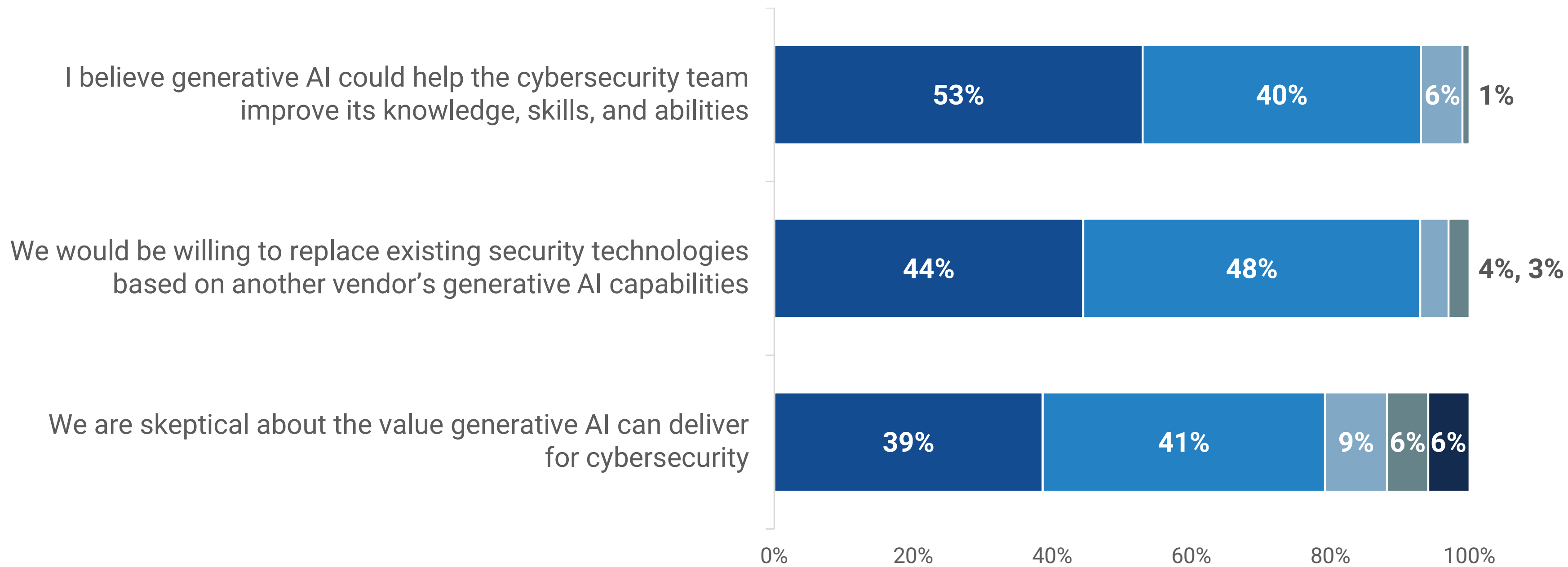
25%

Secure browser technology

21%

Firewalls

Security Professionals Are Cautiously Optimistic About Generative AI's Potential for Cybersecurity

Sentiments Toward GenAI and Cybersecurity

GenAI for cybersecurity elicits an emotional response from security and IT professionals, ranging from optimistic and excited to reserved and skeptical. Beyond these emotions, survey respondents had some concrete opinions: 93% believe generative AI could help them improve their knowledge, skills, and abilities, while at the other end of the spectrum, 80% remain skeptical about the value GenAI can bring to cybersecurity. Many (92%) believe their organization would be willing to replace existing technologies based on the GenAI capabilities of another similar product.

Level of agreement with statements related to using GenAI to fortify existing cybersecurity tools and processes.

I believe generative AI could help the cybersecurity team improve its knowledge, skills, and abilities
| 53% | 40% | 6% | 1% |

We would be willing to replace existing security technologies based on another vendor's generative AI capabilities
| 44% | 48% | 4%, 3% |

We are skeptical about the value generative AI can deliver for cybersecurity
| 39% | 41% | 9% | 6% | 6% |

0% 20% 40% 60% 80% 100%

"GenAI for cybersecurity **elicits an emotional response from security and IT professionals**, ranging from optimistic and excited to reserved and skeptical."
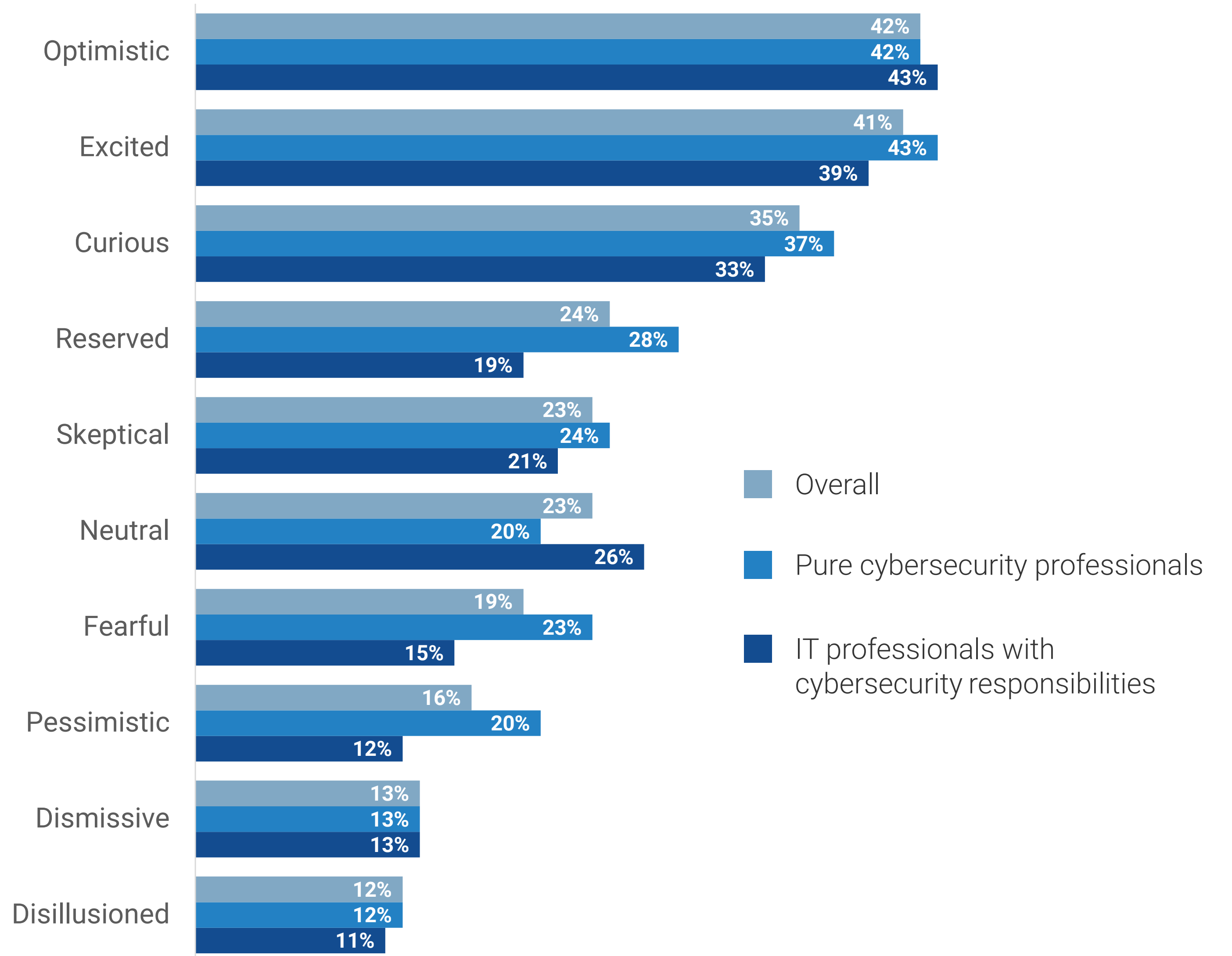
Jon Oltsik | Distinguished Analyst and Fellow
ENTERPRISE STRATEGY GROUP

"Given these misgivings, CISOs should champion GenAI for cybersecurity efforts while remaining judicious in its adoption."

Clearly, opinions vary widely, even between IT and security respondents. For example, security professionals tended to be more reserved (28% versus 19% for IT pros), fearful (23% versus 15% for IT pros), and pessimistic (20% versus 12% for IT pros). Alternatively, IT pros were more neutral than their security colleagues (26% versus 20% for security pros). Given these misgivings, CISOs should champion GenAI for cybersecurity efforts while remaining judicious in its adoption.

Sentiments of cybersecurity defenders regarding the potential impact of GenAI.

Optimistic: Overall 42%, Pure cybersecurity professionals 42%, IT professionals 43%
Excited: 41%, 43%, 39%
Curious: 35%, 37%, 33%
Reserved: 24%, 28%, 19%
Skeptical: 23%, 24%, 21%
Neutral: 23%, 20%, 26%
Fearful: 19%, 23%, 15%
Pessimistic: 16%, 20%, 12%
Dismissive: 13%, 13%, 13%
Disillusioned: 12%, 12%, 11%

Legend: Overall | Pure cybersecurity professionals | IT professionals with cybersecurity responsibilities

Security Professionals' Opinions on Machine Learning

While generative AI may be a shiny new cybersecurity object, other AI technologies, like machine learning, have been around for nearly a decade. With all these years of experience, 92% of respondents agree that machine learning has improved the efficacy and efficiency of cybersecurity technologies. Still, this benefit didn't come without baggage. It's apparent from this research that machine learning-based cybersecurity technologies created false positive alerts and needed tuning and customization. And while they've become commonplace today, it took many years for vendors to deliver valuable machine learning (ML) for cybersecurity. It's worth noting that 83% of respondents agree that looking back, the hype around machine learning for cybersecurity was excessive. Little wonder then why cybersecurity pros are reserved, pessimistic, and fearful of machine learning technology. With this experience, CISOs should take a prudent approach to GenAI implementation, looking for quick wins and incremental value rather than force multiplying results.

Level of agreement with statements related to machine learning and cybersecurity technologies.

■ Strongly agree   ■ Agree   ■ Neither agree nor disagree   ■ Disagree   ■ Strongly disagree

Statement	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
ML has improved the efficacy and efficiency of cybersecurity technologies	50%	42%	8%		1%
Security technologies including ML often require customization for our industry, region, and/or IT environment	50%	43%	6%		1%
My organization's experiences with ML will influence how we approach generative AI for cybersecurity	47%	46%	6%		1%
Machine learning algorithms generate excessive false positive alerts	47%	33%	9%	7%	4%
Security technologies including ML can be buggy, requiring lots of hands-on support from vendors	44%	40%	13%	2%	1%
Security technologies including ML often require tuning to improve alert accuracy	43%	49%	6%		1%
It took many years for security technology vendors to deliver ML that truly delivered incremental value	42%	49%	8%	1%	1%
My organization had to remove/replace one or several security technologies including ML because they never lived up to their promise	42%	42%	5%	8%	2%
Looking back, the hype around machine learning for cybersecurity was excessive	42%	41%	6%	6%	5%
My organization had to remove/replace one or several security technologies including ML because the vendor was acquired, impacting the quality of the product	38%	43%	10%	6%	3%

Promising GenAI Cybersecurity Use Cases

Enterprise organizations will likely upgrade existing tools like EDR, SIEM, and threat intelligence platforms (TIPs) with new versions containing GenAI functionality. Some of the more advanced organizations will create their own security LLMs or customize existing models to meet organizational, industry, and regional needs. As they experiment with open AI engines, their goals must include improving security efficacy, efficiency, and staff productivity.

To that end, survey respondents see a number of promising use cases, including improving security hygiene and posture management, guiding the cybersecurity staff with recommended actions, consolidating security technologies, and training junior employees. Along with these, ESG has seen practical use and strong results in two other areas cited: Security professionals are saving time by using GenAI to help them create summary reports (i.e., threat intelligence reports, incident response reports, cyber-risk status reports, etc.). Additionally, security teams are starting to rely on GenAI to help them better analyze threat intelligence germane to their organization, industry, and region. Security pros will also use GenAI for natural language queries, improving homegrown software and creating detection rules in the near future.

Areas in which GenAI is believed to hold the most promise for cybersecurity.

Area	%
Improving security hygiene and posture management	26%
Guiding the cybersecurity staff with recommended actions	26%
Accelerating threat detection and response	25%
Consolidating security technologies	24%
Training entry-level cybersecurity personnel	23%
Improving the quality of our homegrown software	23%
Creating summary security reports (i.e., security incidents, threats, executive reports, etc.)	22%
Creating detection rules	21%
Analyzing threat intelligence	20%
Using a natural language interface	20%
Automating processes	19%
Penetration testing and/or red teaming	16%

"These actions could scale staff productivity, but skeptical cybersecurity teams **aren't quite ready for autonomic processes just yet.**"

Response Actions for Low-risk GenAI Recommendations

Generative AI also has the potential to automate security processes like patching vulnerable software, quarantining a system, or disabling a user account. These actions could scale staff productivity, but skeptical cybersecurity teams aren't quite ready for autonomic processes just yet. If their organization were given a low-risk recommendation from a GenAI application, nearly three-quarters (71%) of respondents say that a staff member would review the recommendation before taking the remediation action manually, while 25% claim a staff member would review the recommendation and, if they approve it, allow the generative AI application to execute the remediation action. Only 4% would let the application execute the remediation action on its own without human intervention.

Approach to handling low-risk recommendations from a GenAI application.

71% A staff member would review the recommendation before taking the remediation action manually

25% A staff member would review the recommendation and, if they approve it, allow the generative AI application to execute the remediation action

4% The generative AI application would execute the remediation action on its own, without any human intervention

Areas in which security operations process automation supported by GenAI would be most helpful.

Generative AI and Security Process Automation

While security teams remain cautious, they do pinpoint where GenAI-based process automation could be helpful in areas like security investigations, orchestration across heterogeneous security controls, case management, and alert enrichment. Anecdotally, ESG has heard similar themes from CISOs. They'd like to automate alert triage processes to bolster the productivity of tier one/junior analysts. They believe GenAI could increase security analysts' throughput if it could string together individual alerts into attack chains and then enrich these attack chains with threat intelligence and put them in a MITRE ATT&CK context.

End-to-end GenAI-based process automation may be a scary thought for security teams. Perhaps they will get there over the next few years, but in the meantime, GenAI should be applied sensibly to low-risk, time-consuming processes that act as bottlenecks for security teams.

29%

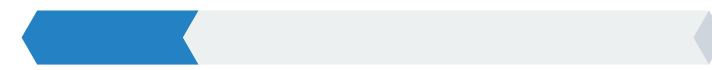Security investigations

26%

Orchestration across heterogeneous security controls
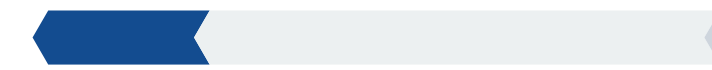
26%
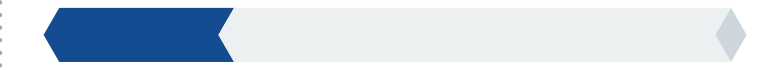
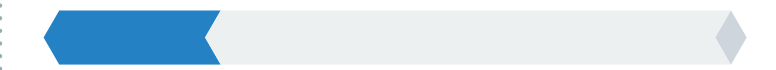General process automation

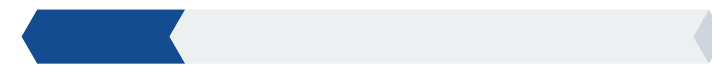**24%**

Security operations case management
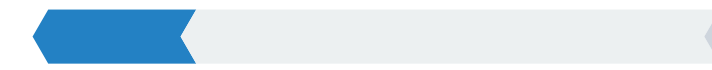
24%

Alert enrichment

24%

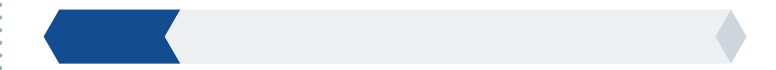Security operations ticketing system management

22%

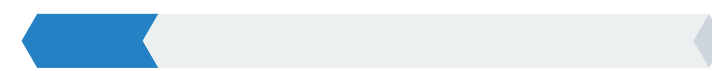SSL certificate management

22%

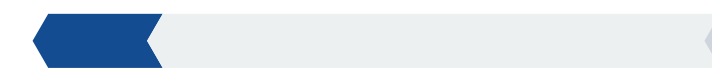Vulnerability management

18%

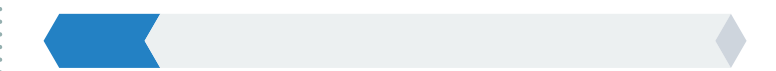Detection rule creation/generation

18%

Incident response/ automated remediation
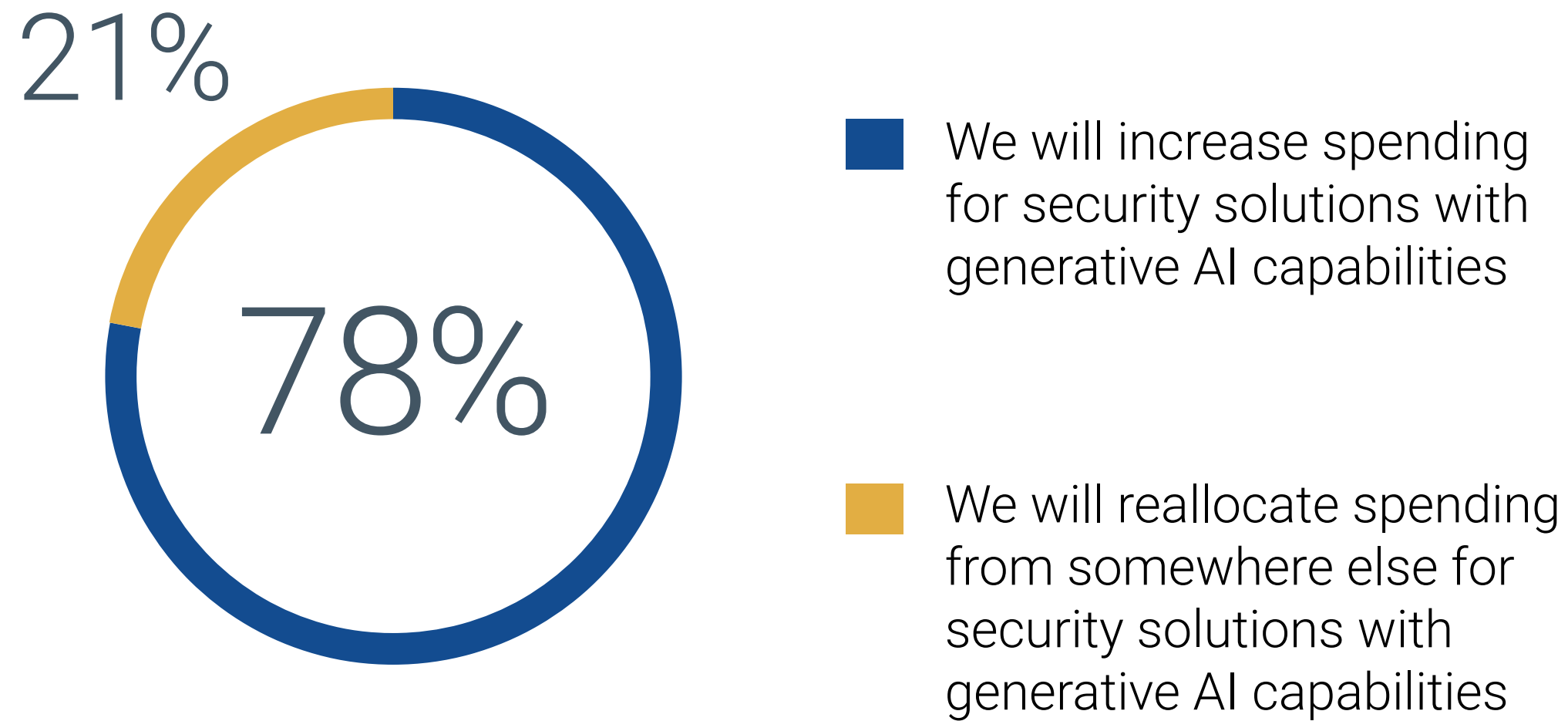
17%

Patch management

15%

Threat hunting

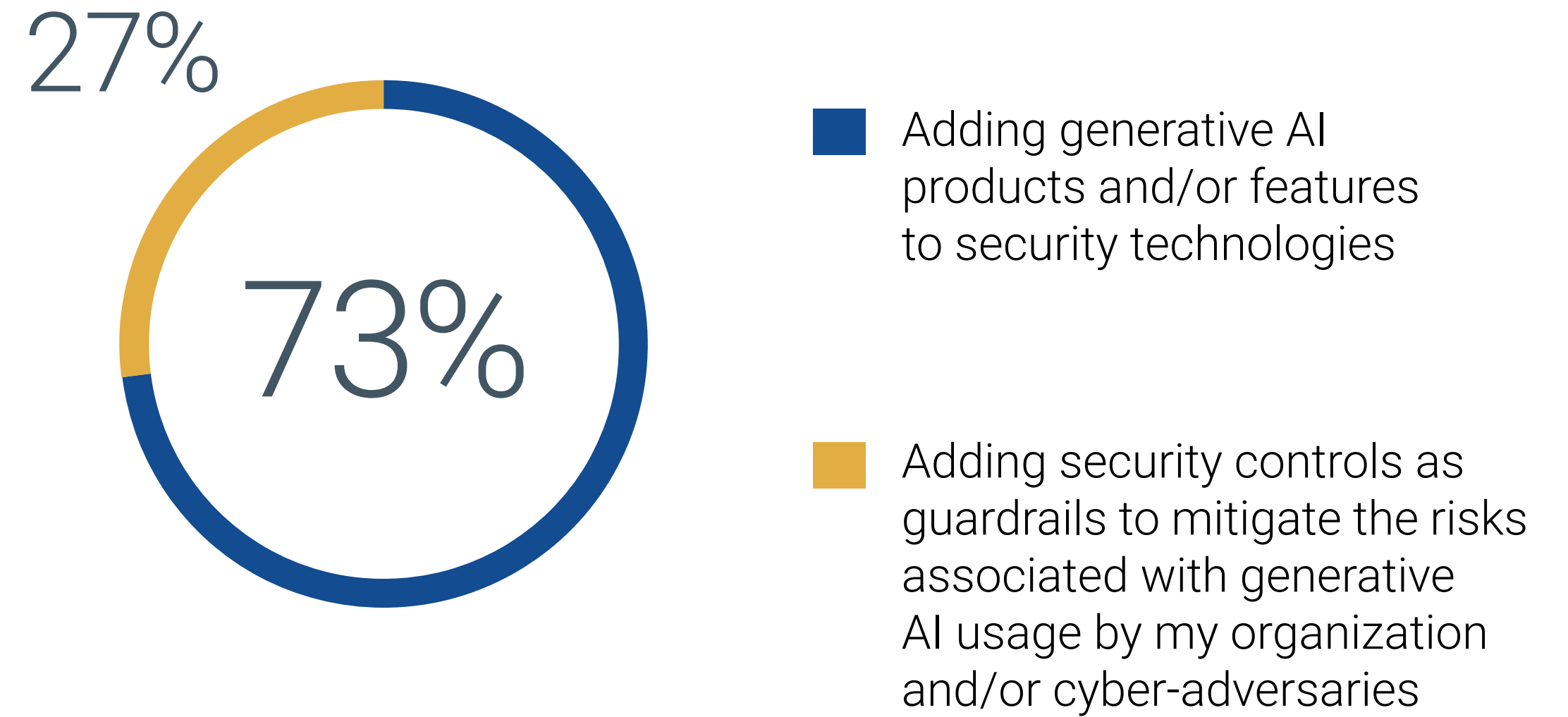# Generative AI Will Become a Purchasing Consideration, Though Plans Are Still Developing

GenAI Solutions Drive Cybersecurity Spending

It appears that GenAI cybersecurity technologies are viewed as a generational change. This conclusion is based on the fact that more than three-quarters (78%) of organizations plan on increasing spending for security solutions with generative AI capabilities. And while the bulk of new spending (73%) will focus on adding new generative AI products or features, CISOs will also dedicate budget dollars to security technologies to mitigate risks and enforce security policies specific to general GenAI initiatives. This spending balance will likely vary widely based on industry, regulations, and organizations' GenAI application usage. The more GenAI in use, the more organizations will need appropriate compensating controls for risk mitigation.

Impact of security solutions with GenAI capabilities on security budget.

21%

78%

■ We will increase spending for security solutions with generative AI capabilities

■ We will reallocate spending from somewhere else for security solutions with generative AI capabilities

Priorities for spending on GenAI over the next 12-24 months.

27%

73%

■ Adding generative AI products and/or features to security technologies

■ Adding security controls as guardrails to mitigate the risks associated with generative AI usage by my organization and/or cyber-adversaries
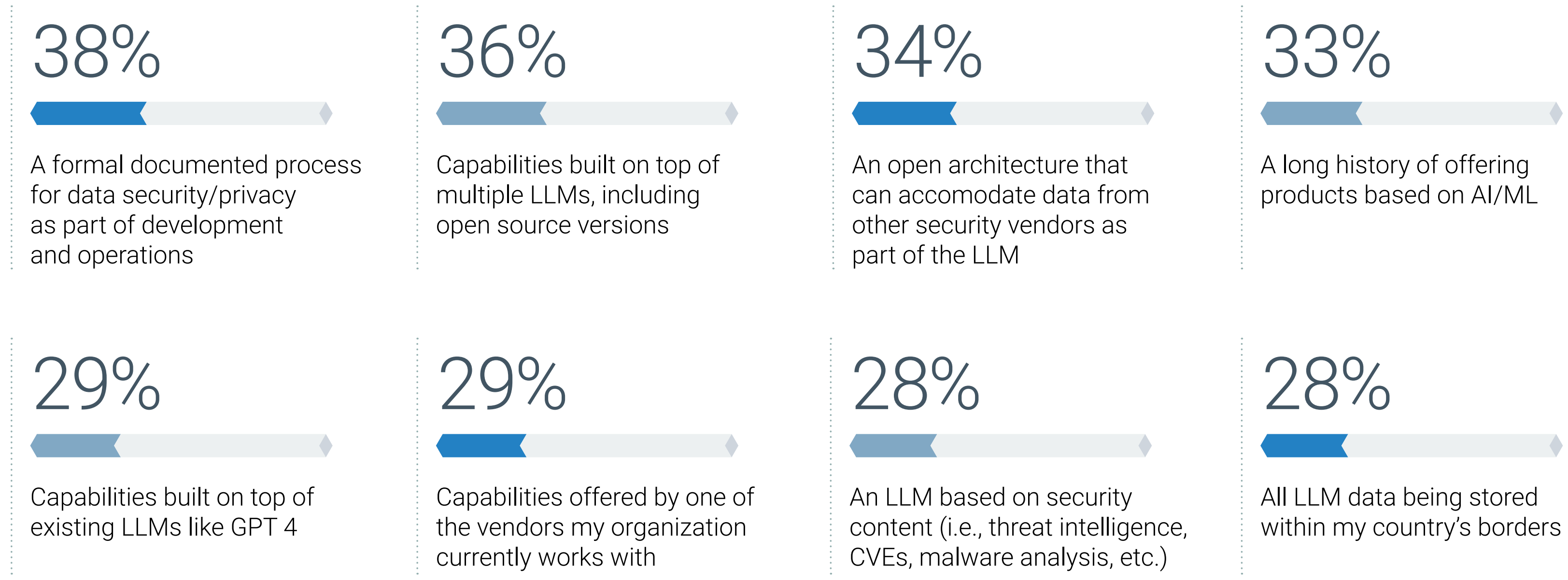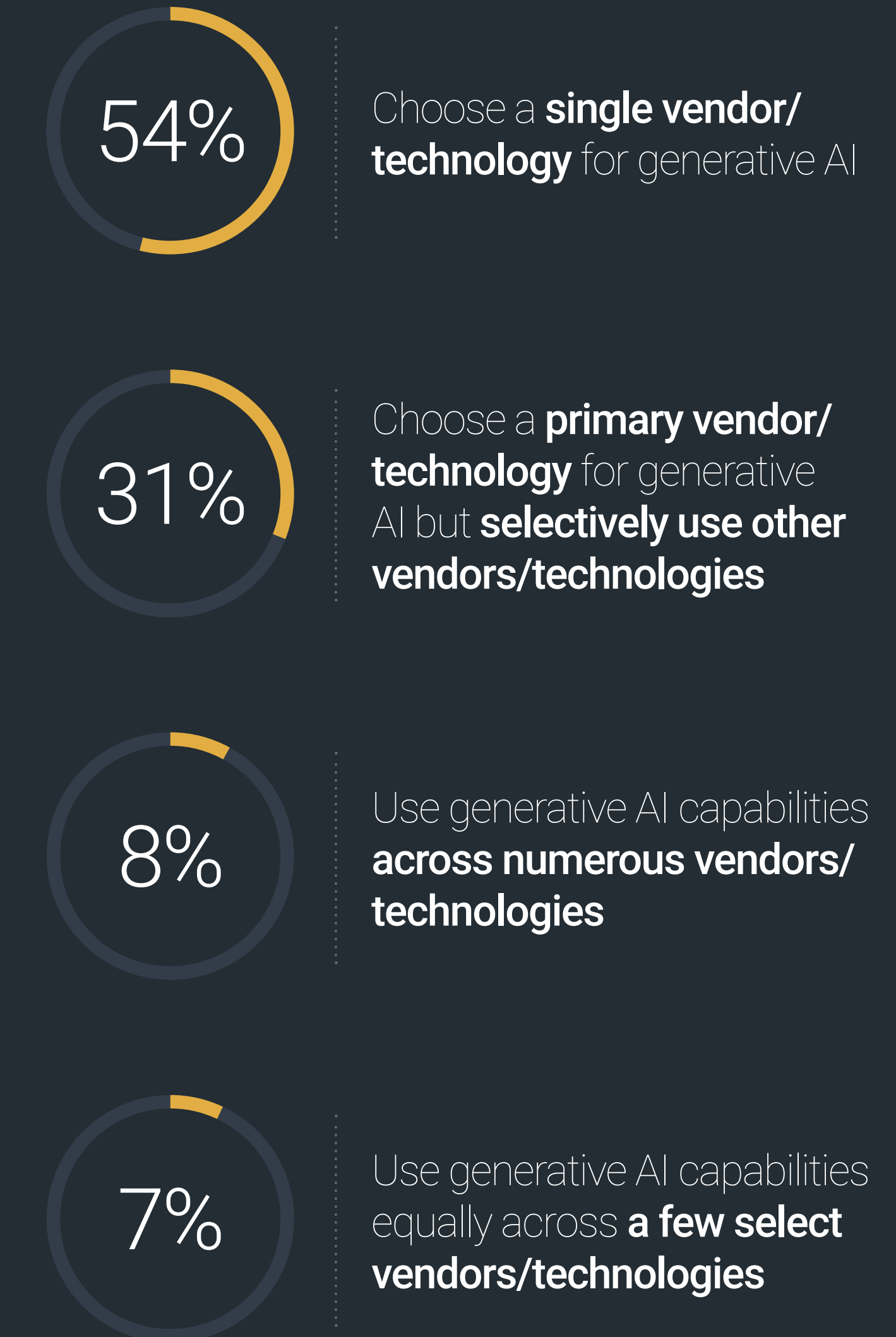
Generative AI and Security Vendor Selection

At this point, more than half (54%) of organizations are leaning toward choosing a single vendor and technology for generative AI security tools, but this strategy may change with time and rapid technology innovation. In fact, 31% of organizations will choose a primary GenAI vendor/technology but selectively use others, and 15% will use GenAI capabilities across numerous or a few select vendors/technologies.

Since GenAI-based security technologies are in their genesis phase, organizations will have to learn how to evaluate products and capabilities as part of their RFI/RFP processes. As of now, the top purchasing considerations include vendors having a formal documented process for data security/privacy as part of development and operations, capabilities built on top of multiple LLMs (including open source versions), an open architecture, and lots of experience with AI/ML-based products. As previously stated, CISOs will likely use the lessons learned from their previous experiences with machine learning to evaluate tools and set the right expectations within the organization.

Most important considerations for GenAI capabilities offered by security vendors.

38%
A formal documented process for data security/privacy as part of development and operations

36%
Capabilities built on top of multiple LLMs, including open source versions

34%
An open architecture that can accomodate data from other security vendors as part of the LLM

33%
A long history of offering products based on AI/ML

29%
Capabilities built on top of existing LLMs like GPT 4

29%
Capabilities offered by one of the vendors my organization currently works with

28%
An LLM based on security content (i.e., threat intelligence, CVEs, malware analysis, etc.)

28%
All LLM data being stored within my country's borders

Likely strategy for augmenting security tools with generative AI products and/or features.

54% Choose a **single vendor/ technology** for generative AI

31% Choose a **primary vendor/ technology** for generative AI but **selectively use other vendors/technologies**

8% Use generative AI capabilities **across numerous vendors/ technologies**

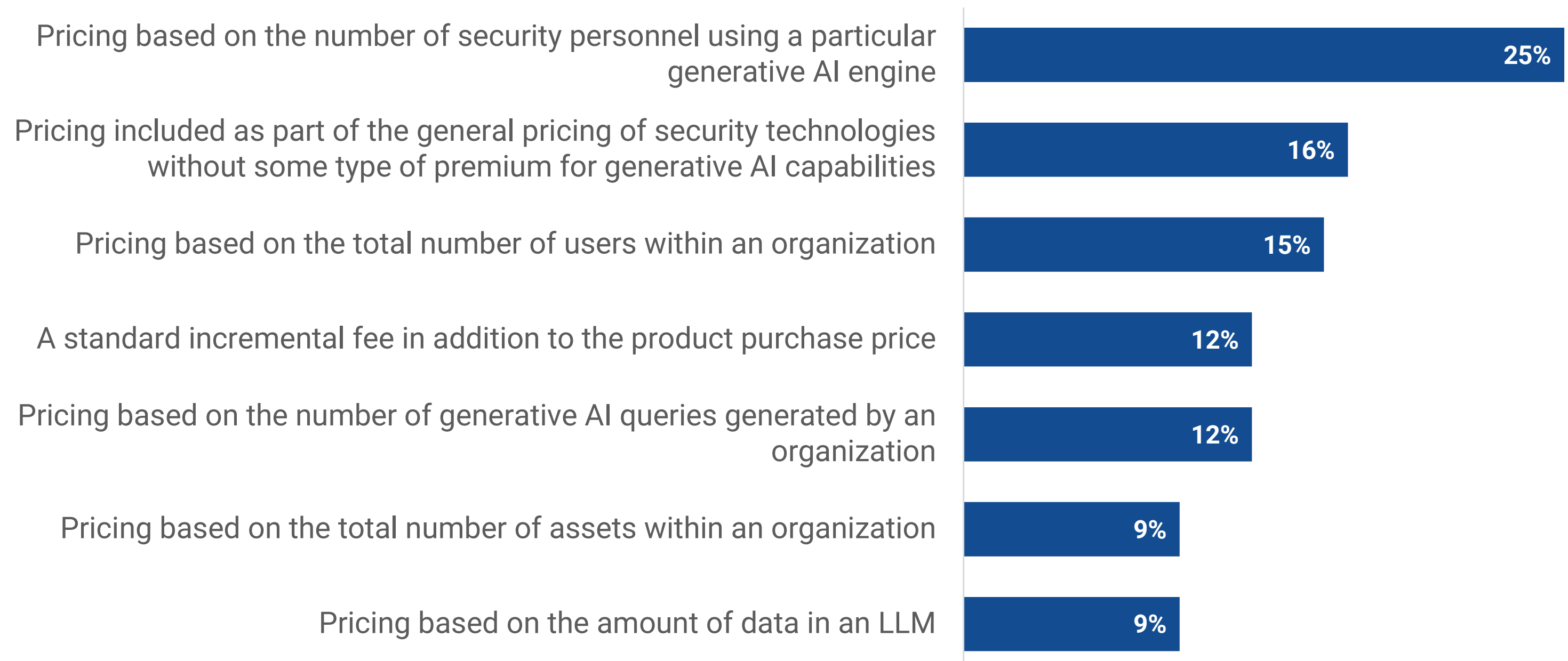**7%** Use generative AI capabilities equally across **a few select vendors/technologies**

Thoughts on GenAI Pricing for Cybersecurity

Generative AI capabilities will likely come as additional features in new cybersecurity product revisions. Vendors are expected to charge a premium for GenAI capabilities, so ESG asked security professionals which pricing models they preferred in this scenario. The data suggests a bit of uncertainty, which is expected for this type of new technology. Nevertheless, survey respondents' preferences range from pricing based on the number of security personnel using GenAI through pricing baked into product pricing to pricing based on the total number of users within an organization.

Despite these preferences, GenAI pricing is likely to be a quagmire for the foreseeable future as the market develops. Security and purchasing managers should monitor different pricing models and compare notes with other organizations in their industry as they negotiate with vendors.

Most appropriate pricing models for security technologies that include GenAI capabilities.

Pricing Model	Percentage
Pricing based on the number of security personnel using a particular generative AI engine	25%
Pricing included as part of the general pricing of security technologies without some type of premium for generative AI capabilities	16%
Pricing based on the total number of users within an organization	15%
A standard incremental fee in addition to the product purchase price	12%
Pricing based on the number of generative AI queries generated by an organization	12%
Pricing based on the total number of assets within an organization	9%
Pricing based on the amount of data in an LLM	9%

"GenAI pricing is **likely to be a quagmire for the foreseeable future** as the market develops."

elastic

ABOUT

Elastic Security modernizes SecOps by unifying the capabilities of SIEM, endpoint security, and cloud security, equipping practitioners to protect, investigate, and respond to complex attacks. With an open and transparent platform — and an agent that stops ransomware and advanced threats alike — it helps organizations reduce risk, advance SecOps maturity, and harden DevSecOps processes.
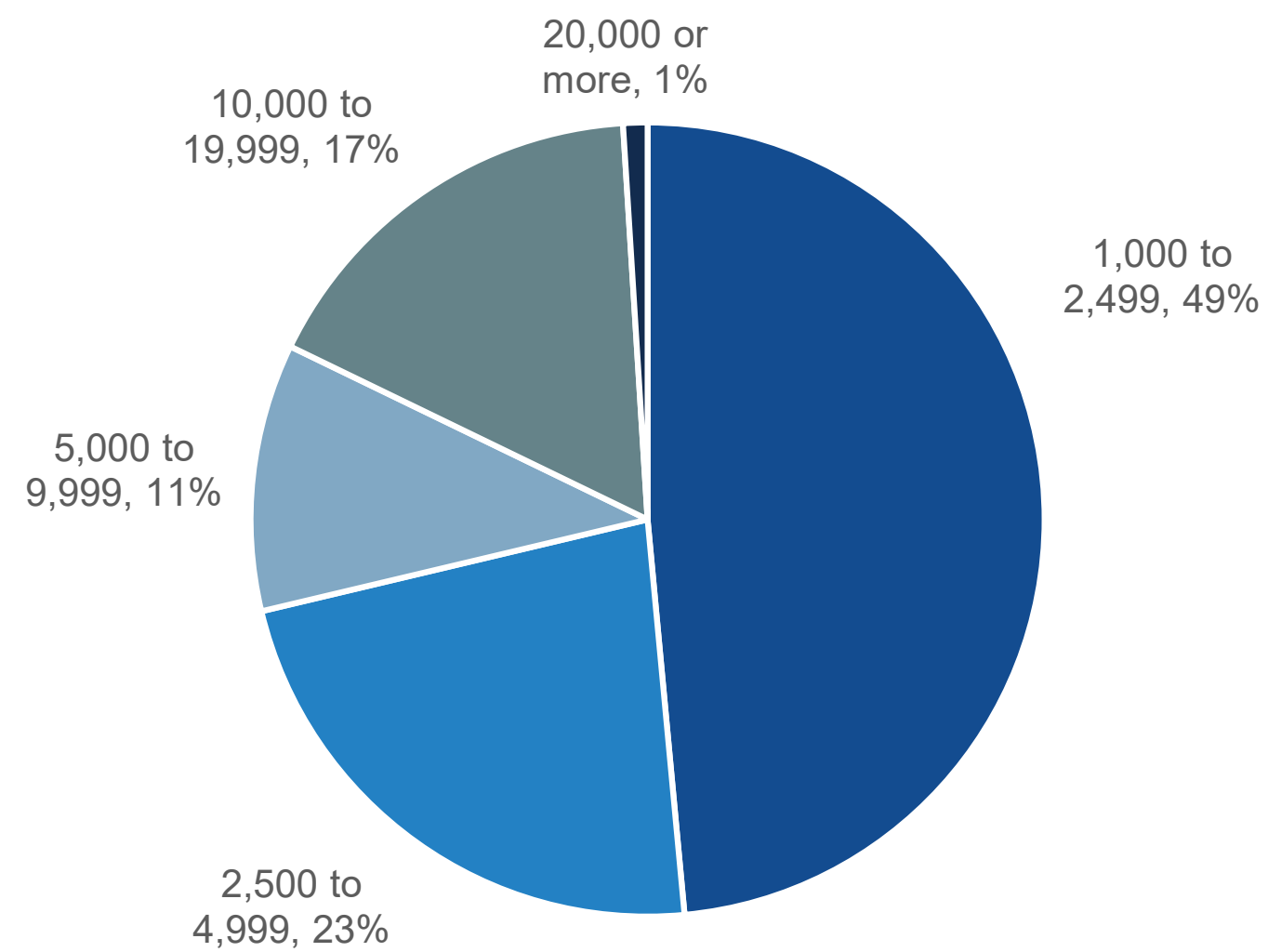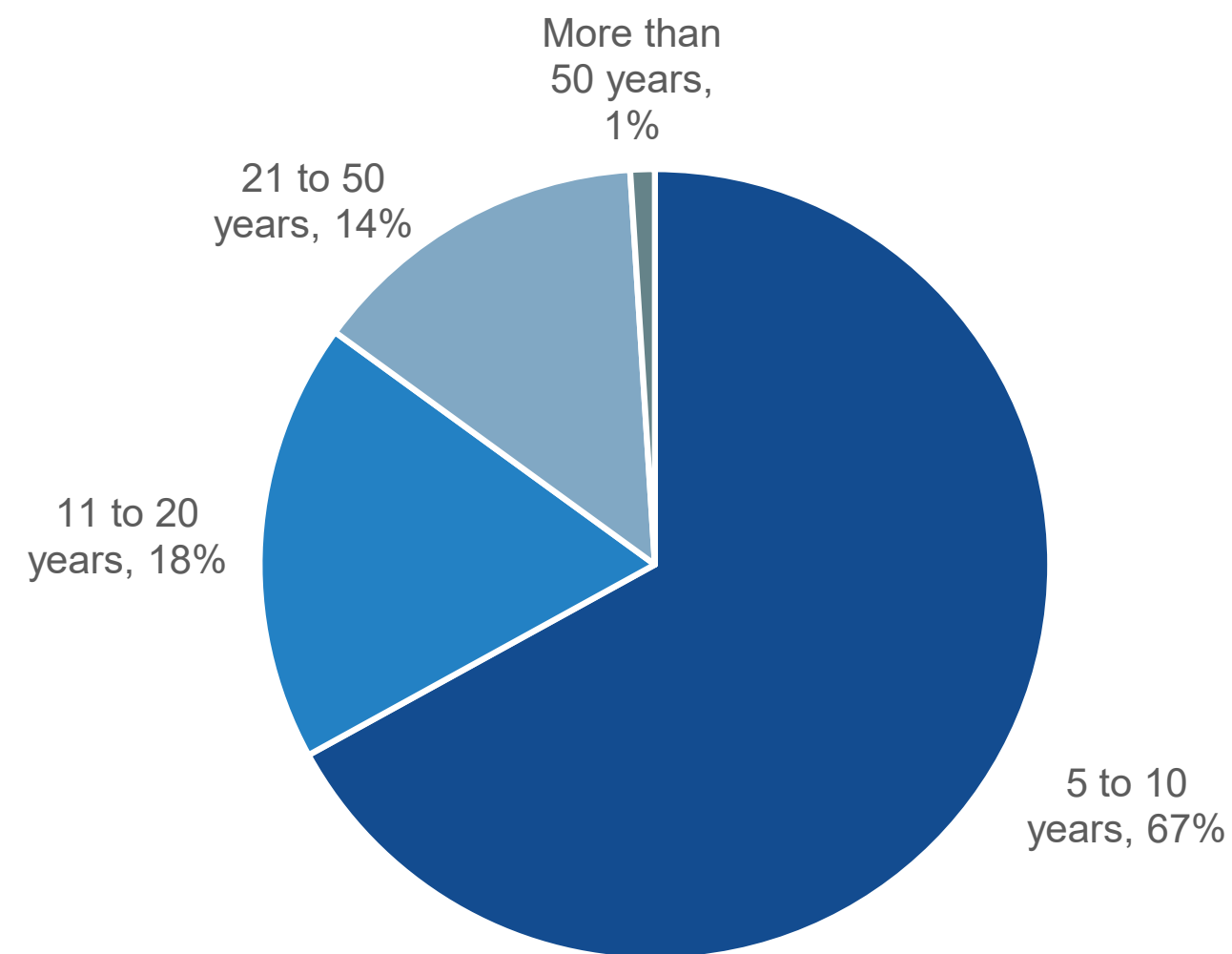
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between November 6, 2023 and November 21, 2023. To qualify for this survey, respondents were required to be involved with supporting and securing, as well as using, generative AI technologies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 370 IT and cybersecurity professionals.

Respondents by number of employees.

- 20,000 or more, 1%
- 10,000 to 19,999, 17%
- 1,000 to 2,499, 49%
- 5,000 to 9,999, 11%
- 2,500 to 4,999, 23%

Respondents by age of organization.

- More than 50 years, 1%
- 21 to 50 years, 14%
- 11 to 20 years, 18%
- 5 to 10 years, 67%

Respondents by industry.

- Business services **18%**
- Manufacturing **16%**
- Retail/wholesale **14%**
- Financial **14%**
- Communications and media **13%**
- Utilities **10%**
- Technology **7%**
- Healthcare **3%**
- Other **5%**

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.