Omdia
by informa techtarget

Next-generation Offensive Security Strategies Give Defenders the AI Advantage

Melinda Marks | *Practice Director*

May 2026

This Omdia research and eBook was commissioned by Cobalt and is distributed under license from Informa TechTarget, Inc.

Research objectives

The adoption of offensive security models and the rise of agentic AI are reshaping modern cybersecurity strategies. Teams are augmenting traditional human-led tests with a mix of automated platforms and crowdsourced talent. The next generation of this concept comes from agentic AI as a reaction to cyber-adversaries developing AI agents for autonomous attacks. Specifically, vendors are starting to offer autonomous offensive AI agents to continuously test defenses.

How are organizations building and budgeting for this modern approach to offensive cybersecurity, which includes automated tools, crowdsourced models, and human-scale security teams? Additionally, what is the impact of agentic AI on operationalizing and managing offensive security strategies?

To understand these trends and the resulting market dynamics, Omdia executed a survey of 400 IT and cybersecurity professionals at organizations in North America involved with or responsible for developing and managing offensive security strategies and capabilities.

This study sought to:

- **Assess** current drivers for offensive security tools, technologies, and services.
- **Analyze** strategies for programs to evolve, including using agentic AI and human cybersecurity talent.
- **Examine** key drivers for current programs and metrics for success.
- **Determine** future plans for investment in offensive security technologies and processes.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.

Key findings

Organizations need offensive security strategies to stay ahead of threats

Page 4

Security teams face challenges with current tools

Page 7

Organizations are looking to AI to evolve offensive security programs

Page 11

Roles and responsibilities will evolve with new technology usage

Page 15

Security metrics should be used to measure program success

Page 18

Most organizations will increase spending on offensive security programs

Page 21

Back to Contents

Organizations need offensive security strategies to stay ahead of threats

AI tops the list of key trends fueling the need for offensive security strategies

Security teams are boosting their offensive cybersecurity efforts to ensure they can stay ahead of threats and attacks, which are scaling rapidly. They face mounting pressure as attackers can increasingly launch automated attacks using AI and more quickly exploit vulnerabilities. Security teams need an effective strategy to ensure they can counteract attacker capabilities as they scale their methods and capabilities to penetrate defenses.

Other trends driving offensive security measures include supporting the expansion of digital assets across environments, dealing with cybersecurity skill shortages, and the need to meet regulatory requirements for continuous security validation.

Greatest influence on offensive security strategies over the past 12 months.

- **32%** The emergence of AI-powered automated attacks by adversaries
- **25%** Increased speed of vulnerability exploitation by threat actors
- **16%** The expansion of digital assets across multi-cloud and SaaS environments
- **14%** Shortage of skilled cybersecurity personnel as manual testing resources
- **14%** Regulatory requirements for continuous security validation (e.g., DORA and EU AI Act)

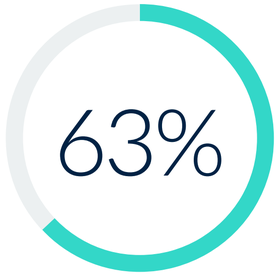
Back to Contents

Protection requires complete visibility

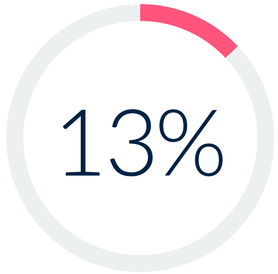
A big challenge for organizations is attack surface visibility, with only one-quarter feeling they have complete real-time visibility into their data and assets. The resulting gaps often drive the need for offensive security strategies to identify areas of vulnerability before attackers can find ways to penetrate. Security teams require a continuous approach that can be integrated with their security solutions to strengthen their overall security programs. This is where traditional offensive security strategies, such as manual, periodic penetration tests, fall short with static, periodic views that leave gaps. Organizations need continuous visibility with thorough ways to test the efficacy of security controls to ensure they can protect against real-world threats and attacks. They also need the context to drive needed remediation in time to prevent incidents, while optimizing efficiency and cost-effectiveness.

Current state of organizations' attack surface visibility.

Complete visibility: We can account for 100% of our data and assets in real time



High visibility: We can account for most assets but have gaps in shadow IT or third-party connections



Moderate visibility: We have a handle on core on-premises assets but struggle with cloud or SaaS

Where traditional offensive security strategies are currently falling short.

They provide a static view that is obsolete by the time the report is delivered

53%

They are too infrequent to capture risks compared with the pace of technology change and growth

48%

They fail to test the efficacy of security controls against real-world threats, tactics, and procedures

46%

The reports lack actionable context for remediation teams to execute against

41%

They are too expensive to scale across the entire technology portfolio

33%

They do not sufficiently cover non-human identities or service accounts

31%

Back to Contents


Security teams face challenges
with current tools

Teams must consider a variety of factors when deciding to leverage offensive security approaches

Teams are considering a variety of factors to determine their tools and approaches when it comes to offensive security. A quarter look at a mix of factors across asset classes, while another quarter consider compliance and regulatory mandates. Other organizations may apply offensive security tactics based on the criticality of the application or asset (21%), frequency of code changes (17%), or budget availability and project funding (12%). These are all important factors, but organizations need to consider how to optimize their program, including best usage of time, resources, and budget, to proactively mitigate their risk and prevent incidents.

How organizations primarily decide when to leverage different offensive security approaches.

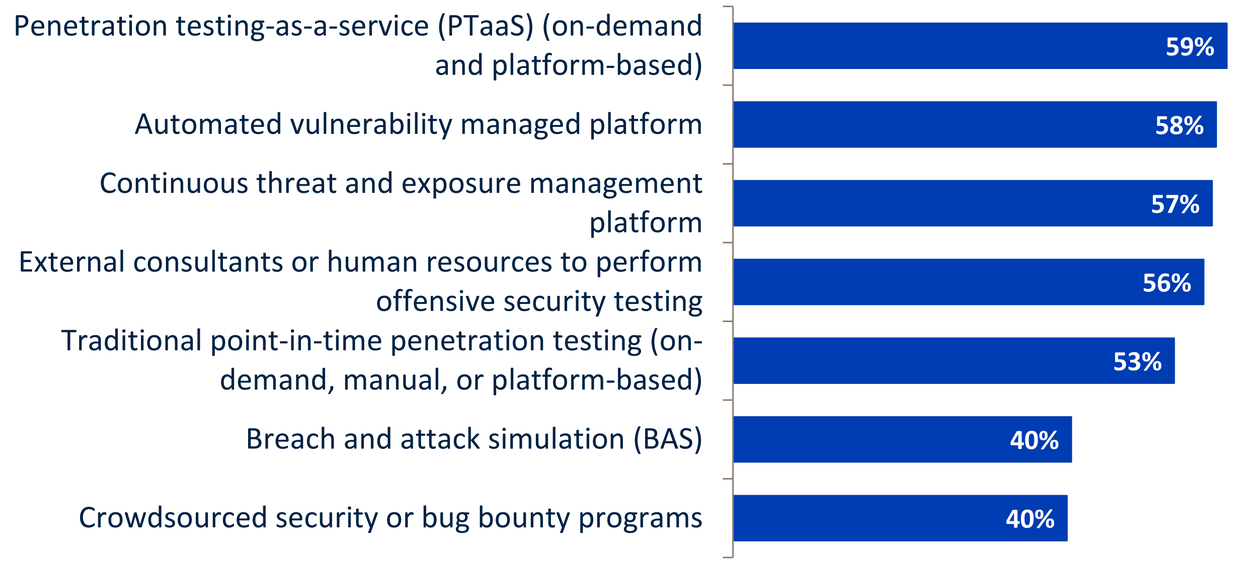
25%	A standardized mix of factors across all asset classes
25%	Compliance and regulatory mandates
21%	Criticality of the application or asset
17%	Frequency of code changes or deployments
12%	Budget availability and project-specific funding

Back to Contents

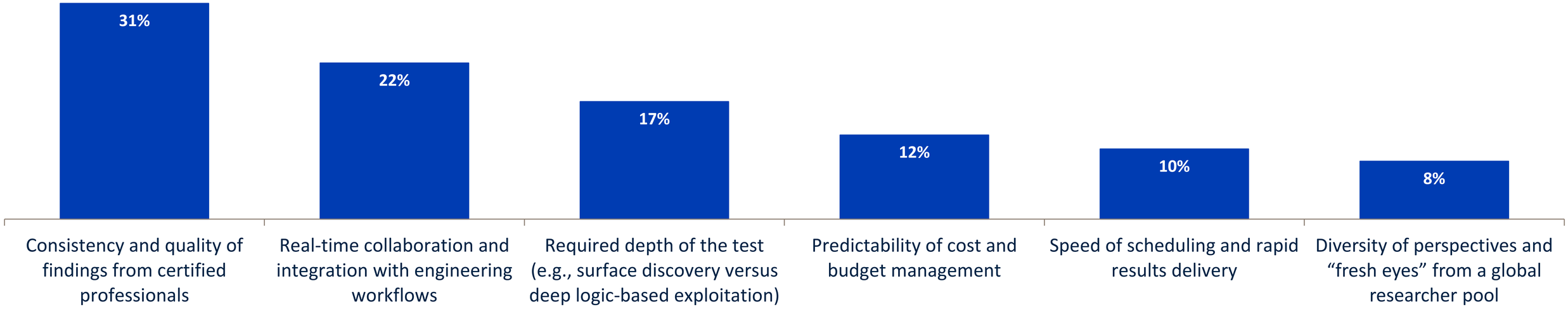
Organizations use a wide range of offensive security models, including penetration testing-as-a-service

When it comes to the offensive security models that organizations currently use, more than half cited penetration testing, both traditional and penetration testing-as-a-service (PTaaS), automated vulnerability management platforms, continuous threat and exposure management platforms, and external consultants. PTaaS platforms offer continuous manual and human penetration testing solutions, including security testing, policy setting, and reporting overall program results, and they often integrate with application security tools. Organizations sometimes consider PTaaS offerings instead of traditional crowdsourced penetration testing security approaches because they need to augment staff and the limitations of other security tools and processes in place. Key decision factors include the need for consistency and quality findings from certified professionals, real-time collaboration and integration with engineering workflows, and required depth of the tests.

Offensive security models currently utilized.



Most influential factor when considering PTaaS versus crowdsourced security.



Back to Contents

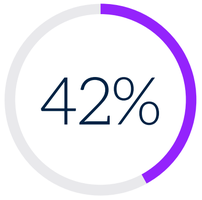
Offensive security strategies strengthen defensive operations

Organizations are utilizing offensive security findings to strengthen their defensive capabilities. Whereas offensive security measures traditionally included crowdsourcing, penetration testing, and programs such as bug bounties that ran separately from application security tools such as testing tools and scanners, organizations are now looking for offensive security solutions that can integrate with defensive security tools and processes. As a result, security teams are more effectively integrating offensive security findings into a wide variety of defensive operations. The value of offensive security solutions should be proven by how much they strengthen the overall security programs instead of their capabilities in identifying weaknesses and collecting fees for what they find.

How offensive security findings are integrated into defensive operations.

Directly into the SOC's detection engineering and rule-tuning process

Used to set policies and guardrails for application development



Used exclusively for compliance reporting and audit evidence

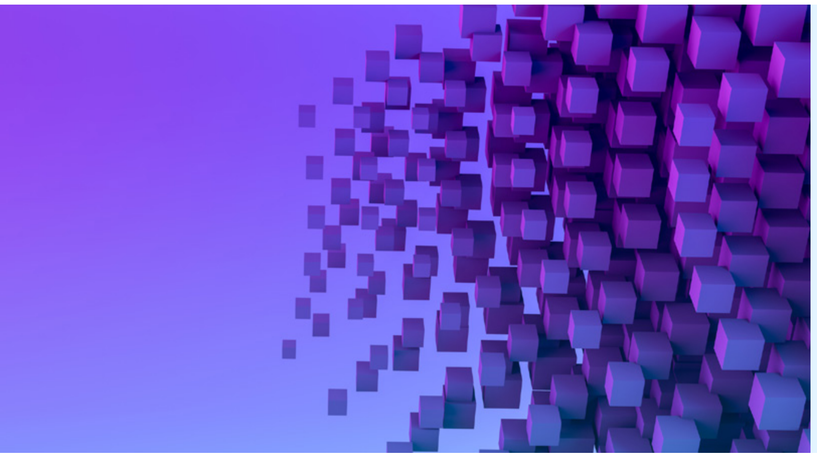
Directly into a centralized risk-based exposure management platform

Used to adjust application development processes or roadmap

Manually reviewed and prioritized by security leadership on a quarterly basis

Back to Contents

Organizations are looking to AI to evolve offensive security programs



AI agents are the likeliest technology to evolve offensive security strategies

More than four in ten (42%) organizations cite autonomous AI security agents as having the greatest potential for evolving offensive security strategies. Attack surface management (24%) is also well-positioned to advance programs, followed by identity threat detection and response (14%), adversarial exposure validation platforms (10%), and risk-based vulnerability management (RBVM) to help security teams stay ahead of attackers (10%).

Technology that organizations anticipate being most foundational to the evolution of offensive security strategies.

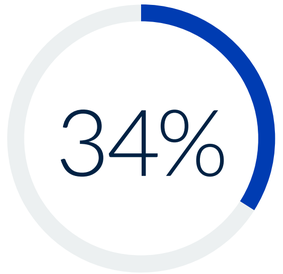
- **42%** Autonomous AI security agents (i.e., agentic PTaaS or agentic penetration testing)
- **24%** Cloud-native attack surface management (EASM, ASM, or CAASM)
- **14%** Identity threat detection and response (ITDR)
- **10%** Adversarial exposure validation (AEV) platforms
- **10%** Risk-based vulnerability management (RBVM)

Back to Contents

Agentic AI is vital to bolstering offensive security, though full autonomy is still developing

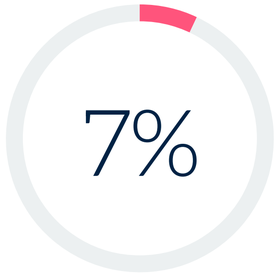
When asked how important agentic AI will be to bolstering their organization's offensive security posture in the next 24 months, the majority of respondents stated that it is either very important (60%) or critical (34%). Although most organizations see agentic AI as vital to bolstering offensive security, only a small percentage (7%) use it with full autonomy, with capabilities to operate independently within preset policy boundaries, at this point. For now, the balance of organizations involve human oversight in the form of humans staying adjacent (27%), humans in the loop (34%), or humans utilizing AI recommendations (33%). This is likely to shift as AI technology evolves and there is more trust in the accuracy and efficacy of the AI agents.

Importance of agentic AI to bolstering offensive security posture in the next 24 months.



Critical:
It will be the foundation of our security strategy

Very important:
It will be a core component of our security strategy, but other tools are more valuable



Somewhat important:
It will play a supporting role in our security program

Current level of autonomy of the AI agents used for offensive security tasks.

7% **Full autonomy:** AI operates independently within preset policy boundaries

27% **Human adjacent:** AI operates autonomously but allows for human intervention and oversight

34% **Human in the loop:** AI executes tasks but requires human approval for every action

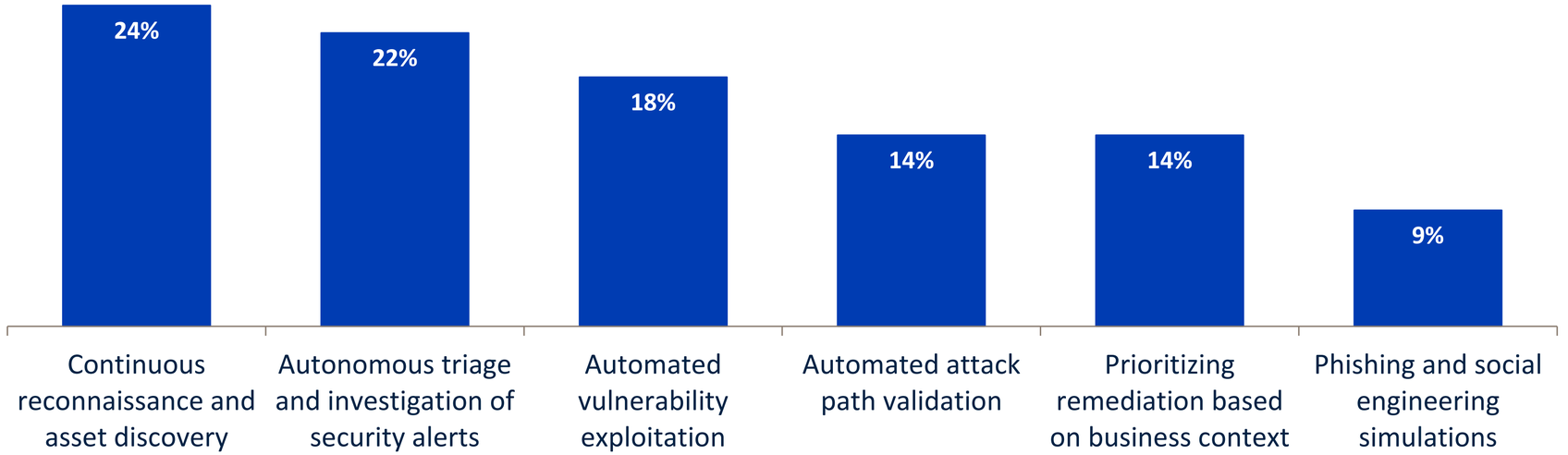
33% **Advisory:** AI provides recommendations that are manually reviewed and executed

Back to Contents

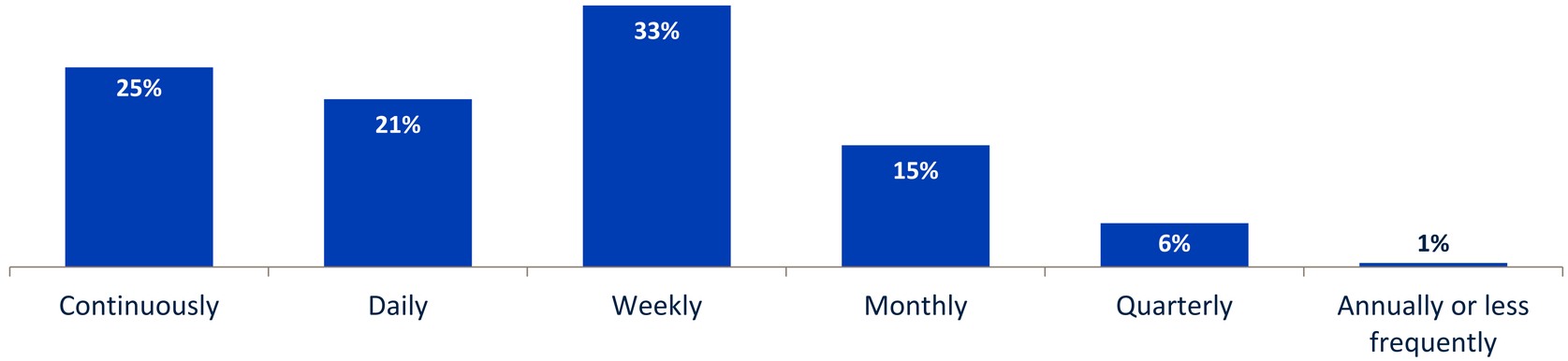
Organizations need continuous attack surface discovery

Agentic AI is most promising in areas such as continuous asset discovery, autonomous triage and investigation of alerts, and automated vulnerability exploitation. As attack surfaces scale and change, attack surface visibility and monitoring are important. The plurality is performing attack surface discovery weekly, with a quarter performing it continuously. Organizations can evolve their programs by continuously performing external attack surface discovery, which the highest percentage of respondents saw as a good use case for agentic AI. This appears to be another promising area to which organizations can apply agentic AI to evolve their programs.

Tasks AI agents are best suited to handle in an offensive security context.



Frequency with which organizations perform external attack surface discovery.



Back to Contents

Roles and responsibilities will evolve with new technology usage

Primary offensive security strategy stakeholder is most often the chief information security officer

Who is the primary stakeholder for the development and management of organizations' offensive security strategies? That is most often the chief information security officer (CISO), but the chief information officer (CIO) can also often take up that role.

Primary stakeholder for the development and management of offensive security strategies.

45%	Chief information security officer (CISO)
30%	Chief information officer (CIO)
12%	Head of security operations (SecOps)
7%	Head of application security or DevSecOps
6%	Cyber-risk or audit leader

Back to Contents

AI *and* humans are important in offensive security programs

While security teams are investing in AI technologies to automate tasks that are difficult, time consuming, or tedious for humans, they are also addressing the importance of humans and their roles. Half are investing in technologies while recognizing the importance of humans in the loop, with 44% viewing humans as central to offensive operations and the success of the program. Only 6% are striving to rely on technologies and aspire to remove humans from the loop. So, while AI adoption is rampant, human experience and skills are still seen as valuable, and human roles can evolve with AI agent deployment. Indeed, security teams will need to adapt their skill sets and responsibilities as they increasingly utilize AI. While it will help them more efficiently do their jobs of proactive threat hunting and strategic defense, practitioners will need to shift their skills to supervising autonomous workflows as well as increase their architectural and governance proficiency.

View on the role of the expert human offensive practitioners in security programs.

50%

We need humans in the loop but are investing in technologies to ensure the success of our program

44%

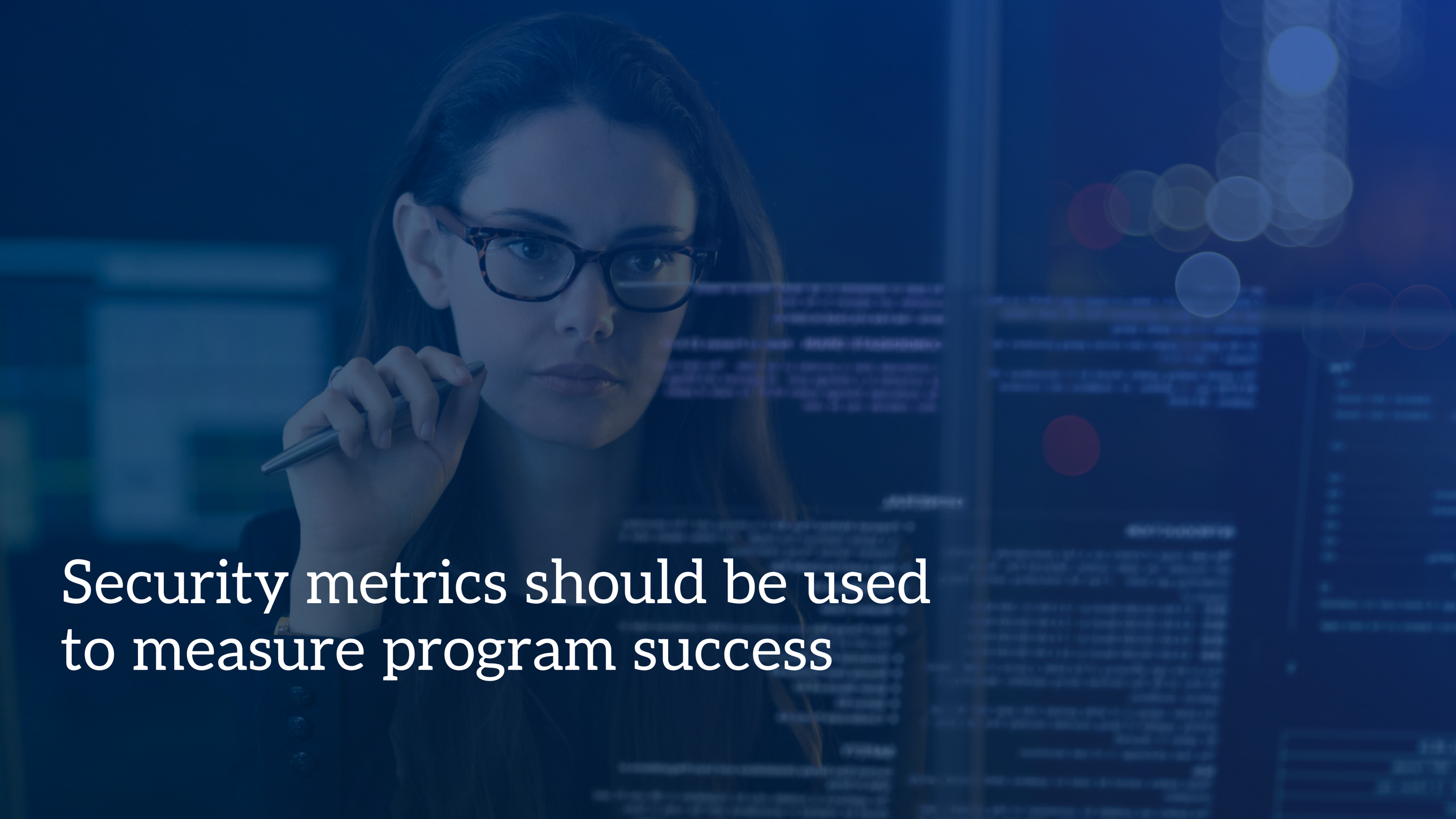
Humans and their expertise are central to offensive operations and the success of our program

6%

We are striving to rely on technologies and solutions for offensive security so we will not need humans in the loop for our programs

Change that the adoption of agentic AI is expected to have on the day-to-day workflow of security teams focused on offensive security capabilities.

Back to Contents



Security metrics should be used to measure program success

Teams use a range of metrics to evaluate offensive security

The need to integrate offensive security measures into overall programs is also apparent in how organizations are measuring their effectiveness and positive results. One-third of security teams use a vendor exposure management platform to accomplish this, while another 28% leverage their own business or risk formula and systems. Only 22% use the offensive security vendor's platform to measure offensive security results, which demonstrates the need to use the offensive security tools with other tools in place to make the case for overall value to the security and risk management program.

Technology used to produce the metrics and scores for measuring offensive security results.

33% A vendor exposure management platform

28% Our own business or risk formula and systems

22% A vendor offensive security platform

16% A vendor risk quantification platform

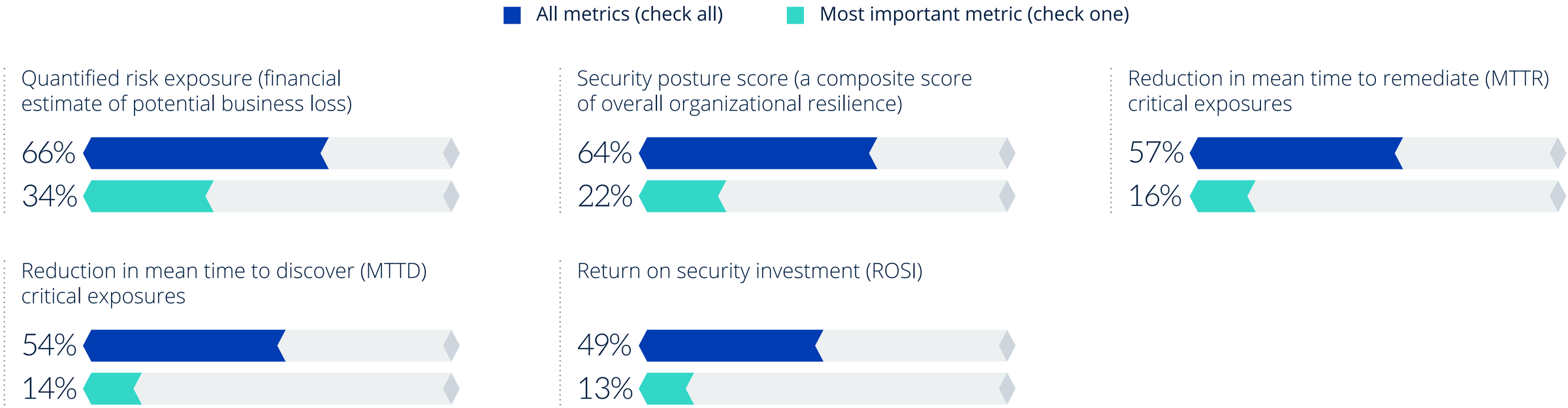
Back to Contents

Offensive security programs must quantifiably reduce risk

Organizations should utilize key security risk metrics to measure the effectiveness of their solutions and to communicate benefits and positive results from successful programs. This is valuable for demonstrating overall security program effectiveness and is relevant to business leaders and boards.

Key metrics used today include quantified risk exposure, security posture scores, reduction in mean time to remediate (MTTR) critical exposures, reduction in mean time to discover (MTTD) critical exposures, and return on security investment (ROSI).

Metrics tracked to communicate the risk reduction impact of offensive security to the board or executive leadership.



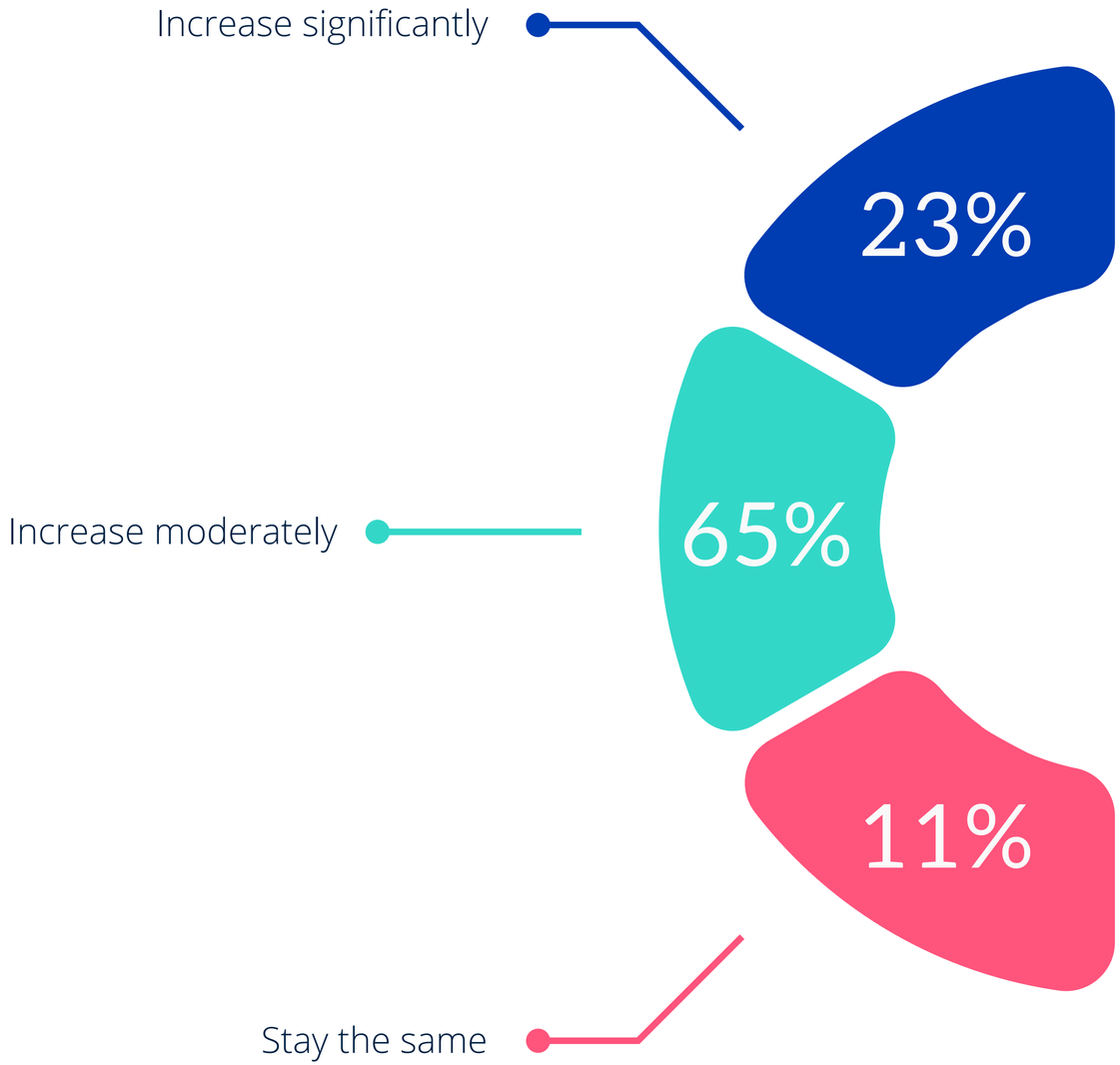
Back to Contents

Most organizations will increase spending on offensive security programs

Most plan to increase investments in offensive security technologies

The majority of respondents (88%) are increasing their budget for offensive security technologies, including 23% planning to increase spending *significantly*. This is likely due to challenges and concerns like attackers' abilities to utilize AI, the increased speed of exploitation of vulnerabilities, and the need to manage attack surface growth.

Expected change in budget for offensive security technologies over the next 12 months.



Back to Contents

Organizations reported a slew of key factors for selecting offensive security technology

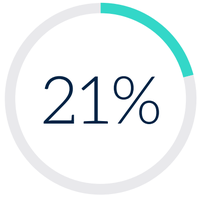
Organizations are looking for demonstrable improvements to their overall security programs. When asked about the top factor for selecting an offensive security vendor or technology, the most commonly cited were a proven ability to reduce risk, the ability to provide a unified view across environments, and ease of integration with existing SOC tools. Another key aspect of developing offensive security programs is simulating possible attacks to validate the security of applications and systems. When asked about top goals for addressing adversarial behavior, the most cited was resilience and response to security incidents. However, organizations also seek better capabilities to identify and remediate exposures, prevent attackers from exfiltrating data, and stop lateral movement. While the least-cited goal is preventing an attacker from finding an initial entry point, that is an important benefit of an effective offensive security program. These are all key areas for offensive security solutions to address.

Single most important factor when selecting an offensive security vendor or technology.

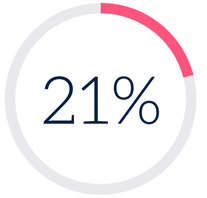
- 26% — Proven ability to reduce measurable risk
- 26% — Ability to provide a unified view across IT, cloud, and OT environments
- 21% — Ease of integration with existing SOC tools (SIEM, SOAR, and EDR)
- 11% — Depth of automation and autonomous (agentic) capabilities
- 10% — Proven ability to improve compliance posture
- 8% — Total cost of ownership and pricing model

Aspects of adversarial behavior that organizations are most focused on when selecting an offensive security technology.

Resilience and response: Using detection capabilities to find and contain an attack before it achieves its objective

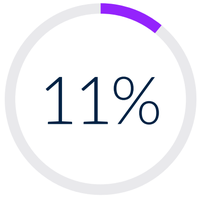


Vulnerability breadth: Discovering all CVEs or misconfiguration exposures across the technology environment



Data exfiltration: Preventing an attacker from bypassing data loss prevention technologies and egress controls to move sensitive data out

Lateral movement: Preventing an attacker from pivoting from a low-privilege account to the “crown jewel” assets



Initial access: Preventing an attacker from finding an entry point into the technology environment

Back to Contents

Cobalt

About

Cobalt is the pioneer in Pentesting as a Service (PTaaS) and a leader in autonomous offensive security testing grounded in human expertise. The Cobalt Offensive Security Platform spans the full spectrum of offensive security, from targeted, human-led pentesting to high-frequency, AI-driven autonomous security testing. Only Cobalt brings together the four critical elements of modern offensive security: elite security expertise, a purpose-built platform, proprietary pentesting intelligence, and AI-driven orchestration. Thousands of customers and hundreds of partners rely on Cobalt and its global network of 500+ vetted security experts to continuously identify, prioritize, and remediate exploitable risk with the speed, flexibility, and precision modern organizations demand.

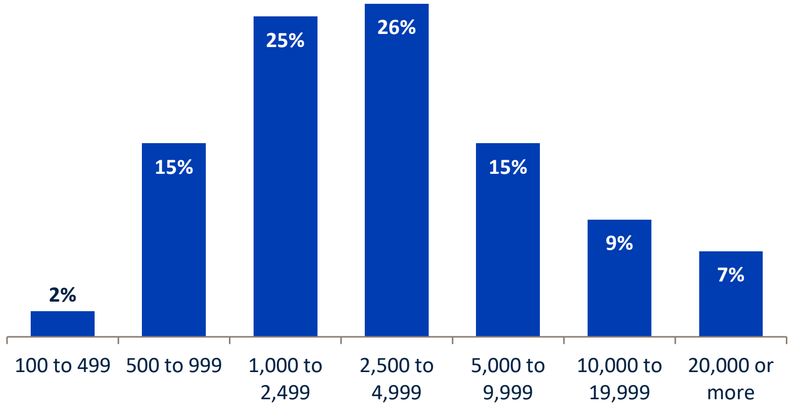
Learn more

Research methodology and demographics

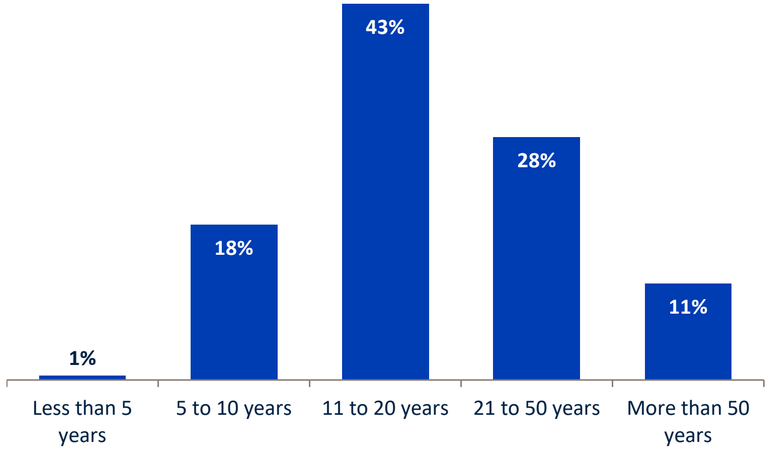
To gather data for this report, Omdia conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between March 9, 2026, and March 13, 2026. To qualify for this survey, respondents were required to be involved with or responsible for developing and managing offensive security strategies and capabilities. 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 several criteria) for data integrity, we were left with a final total sample of 400 IT and cybersecurity professionals.

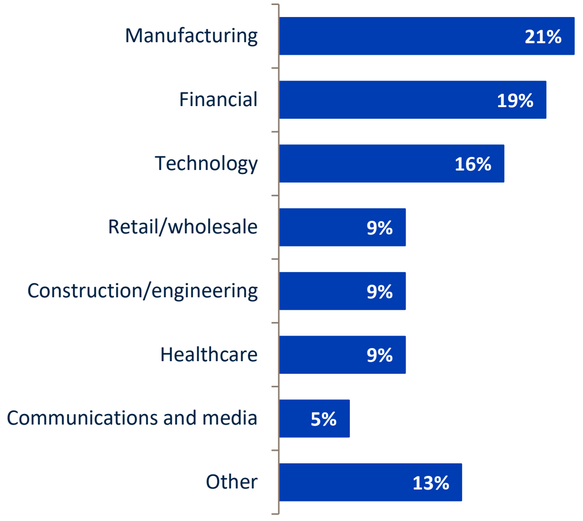
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



Back to Contents

Omdia provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.