May 2026

REPORT

Securing the Expanding Attack Surface in the Age of AI

infoblox®

Table of Contents

Introduction and Key Research Findings: A Problem of Exposure

EXTERNAL RISK IN THE AGE OF AI

The attack surface is expanding faster than ever. AI-driven applications, cloud services, software as a service (SaaS) platforms and distributed work models are introducing new exposures at a pace traditional security approaches were never designed to handle. Risk is no longer static or confined to the enterprise—it is dynamic, external and constantly shifting.

At the same time, attackers are moving faster. AI-driven phishing, deepfakes, automated malware creation and rapidly shifting infrastructure have compressed the window between exposure and impact. In this environment, detection alone is no longer sufficient. Organizations must understand which exposures matter most, why they matter and how to reduce risk before compromise occurs.

To understand how security leaders are responding to this reality, Infoblox commissioned independent research to examine digital risk, exposure and attack surface management, and threat detection in the age of AI. The executive summary that follows highlights the key findings.

96% of organizations report challenges managing threat exposure

87% have suffered AI-driven attacks

34% cannot link vulnerabilities to real-world exploitation

>50% prioritize phishing takedown and credential exposure

EXECUTIVE SUMMARY: KEY FINDINGS

1. Attack Surface Expansion Is Overwhelming Security

The attack surface is growing faster than organizations can manage it. Of the organizations surveyed, 96% report challenges managing threat exposure, driven by rapid expansion of cloud services, SaaS applications, IoT/OT systems and shadow IT. Cloud exposure alone is the top priority for more than half of security teams, reflecting how quickly risk is shifting beyond traditional enterprise boundaries.

2. AI-Driven Attacks Are Already the Norm

AI has compressed the time between exposure and impact. The vast majority of organizations (87%) have already experienced adversarial AI-driven attacks, most commonly AI-driven phishing and automated malware. As a result, AI-driven threats such as deepfakes and AI-generated phishing are now the leading security concern, surpassing ransomware and other traditional risks.

3. Knowledge of Real World Exploitability Remains the Biggest Gap

The biggest challenge with managing threat exposure is determining which vulnerabilities are actually exploitable, highlighting a persistent gap between knowing about exposures and risks, and prioritizing which ones to focus on.

4. Phishing and Credential Leaks Are Primary Concerns

Security leaders increasingly recognize that attacks often begin outside the enterprise. More than half of organizations prioritize phishing infrastructure takedown and credential leak detection. These findings show that external digital risks are central to modern attack paths, not peripheral issues.

67% reported DNS hygiene as a concern

82% increased the use of preemptive security tools year over year

5. Poor DNS Hygiene Leads to Additional Exposure Concerns

Almost two-thirds of organizations (67%) reported DNS hygiene as a concern, and 88% report additional exposure concerns driven by poor DNS practices. Unmanaged or misconfigured DNS infrastructure creates blind spots that attackers exploit to establish malicious domains, redirect traffic and evade detection.

6. Security Strategy Is Shifting toward Preemptive, Intelligence-Driven Control

In response to accelerating threats, organizations are rebalancing their security investments. Nearly half expect to allocate security tools toward preemptive controls over the next 12 months, and 82% report increasing their use of preemptive security tools year over year. Prevention and predictive threat intelligence resonate most strongly, signaling a clear move beyond detection-only security models.

Digital Risk, Exposure and Attack Surface Management

As digital environments grow more complex, exposure and digital risk management have become some of the most difficult challenges facing security teams. Cloud services, SaaS applications, IoT and OT systems, third-party dependencies and externally exposed digital assets continuously expand the attack surface, often faster than organizations can inventory, assess or secure them.

While many organizations report gaining end-to-end visibility into assets and exposures relatively quickly, research shows that visibility alone does not guarantee meaningful risk reduction. The most significant challenge remains prioritization: determining which vulnerabilities, misconfigurations and external digital risks are most likely to be exploited by real attackers.

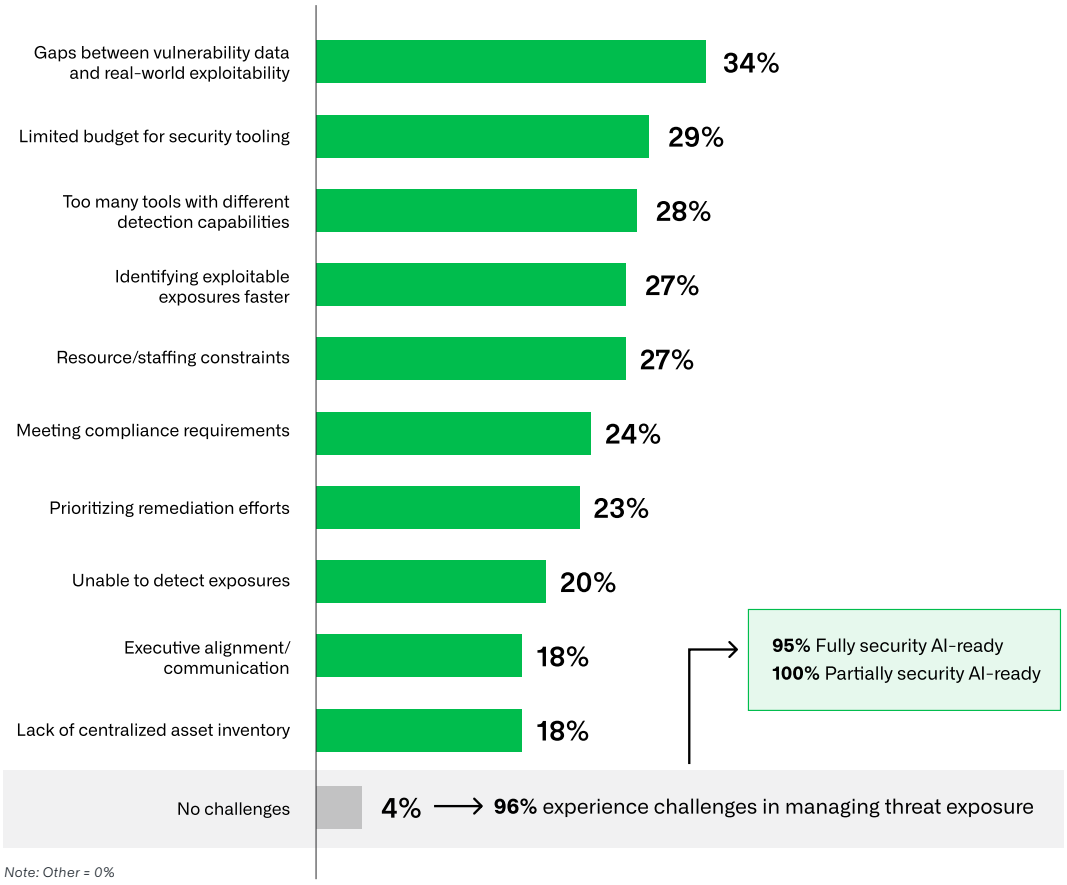
Budget constraints, fragmented tooling and limited integration between exposure management, digital risk protection and threat intelligence continue to slow progress. As a result, organizations struggle to align remediation and disruption efforts with actual attacker behavior, particularly for threats that originate outside the enterprise, such as phishing infrastructure, impersonation campaigns and brand abuse.

These findings underscore the need for continuous, intelligence-driven approaches that connect internal exposures with external digital risk, linking assets, vulnerabilities and attacker activity into a single operational view, rather than treating them as separate disciplines.

TOP CHALLENGES IN MANAGING THREAT EXPOSURE

With 96% of organizations facing challenges in managing threat exposure, the biggest hurdles stem from bridging the gap between vulnerabilities and real-world exploitability (34%), compounded by budget constraints (29%) and overly fragmented tooling (28%).

What are your biggest challenges in managing threat exposure today? Select up to three:



Note: Other = 0%

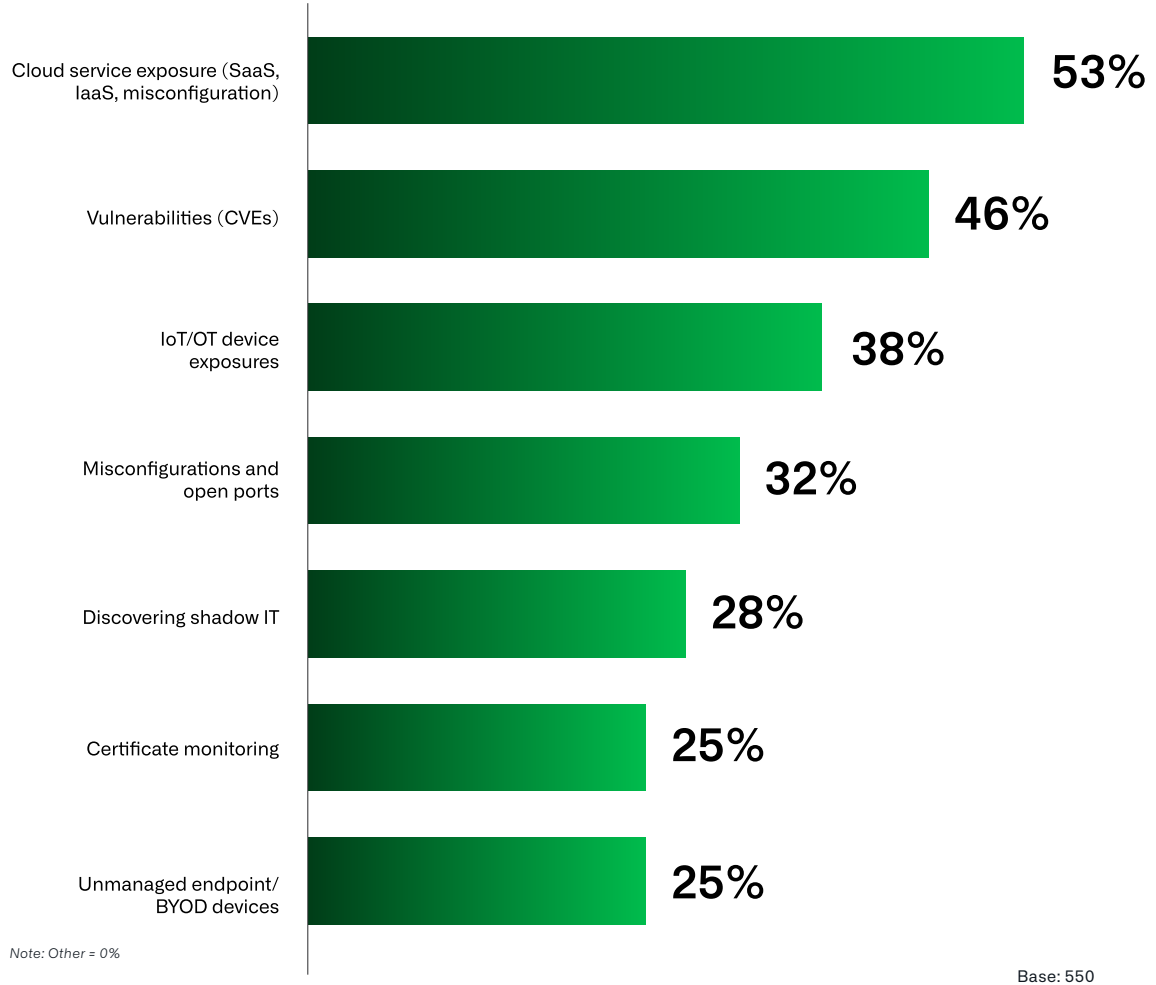
Base: 550

Organizations that are not fully ready to secure their AI systems are highly likely to face challenges in managing threat exposure, showing that gaps in AI security readiness directly translate into threat exposure challenges.

ATTACK SURFACE EXPOSURE PRIORITIES

Cloud service exposure is the top priority for security teams (53%), followed by vulnerabilities (46%) and IoT/OT device risks (38%).

Which attack surface exposures are most important for you to address? Select up to three:



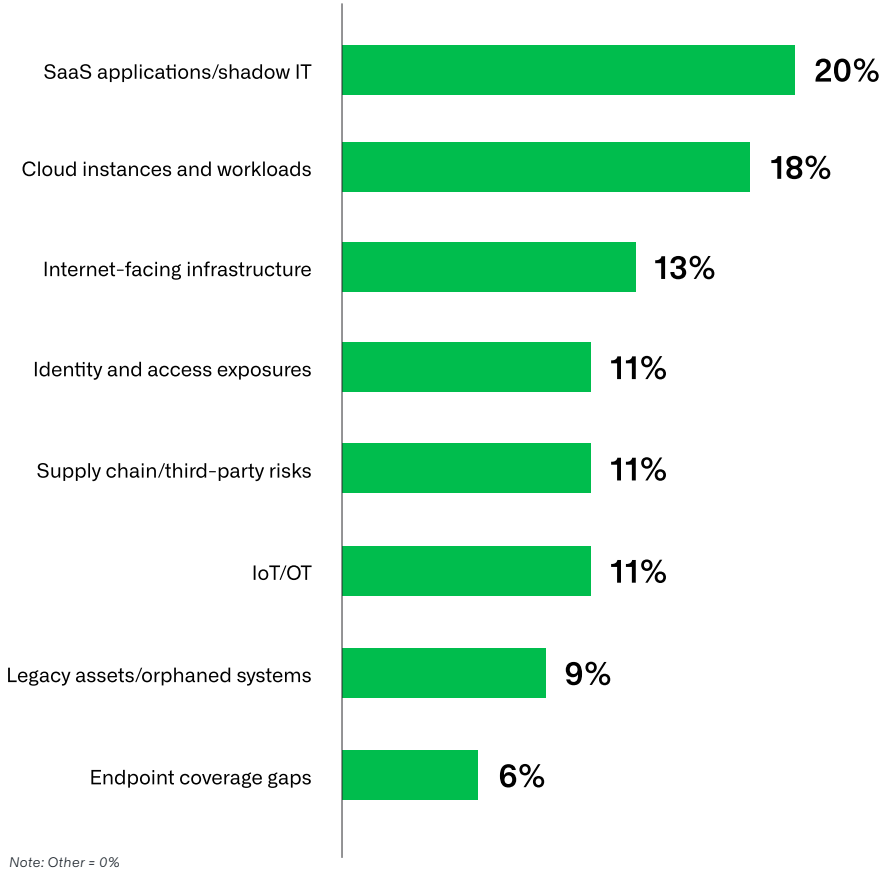
Note: Other = 0%

Base: 550

THE ASSETS THAT ARE HARDEST TO MANAGE FOR EXPOSURE

The assets that are hardest to manage exposures on are diverse, with SaaS applications and shadow IT topping the list (20%), closely followed by cloud instances and workloads (18%).

Which type of asset is hardest for your organization to manage exposures on? Select one:



Note: Other = 0%

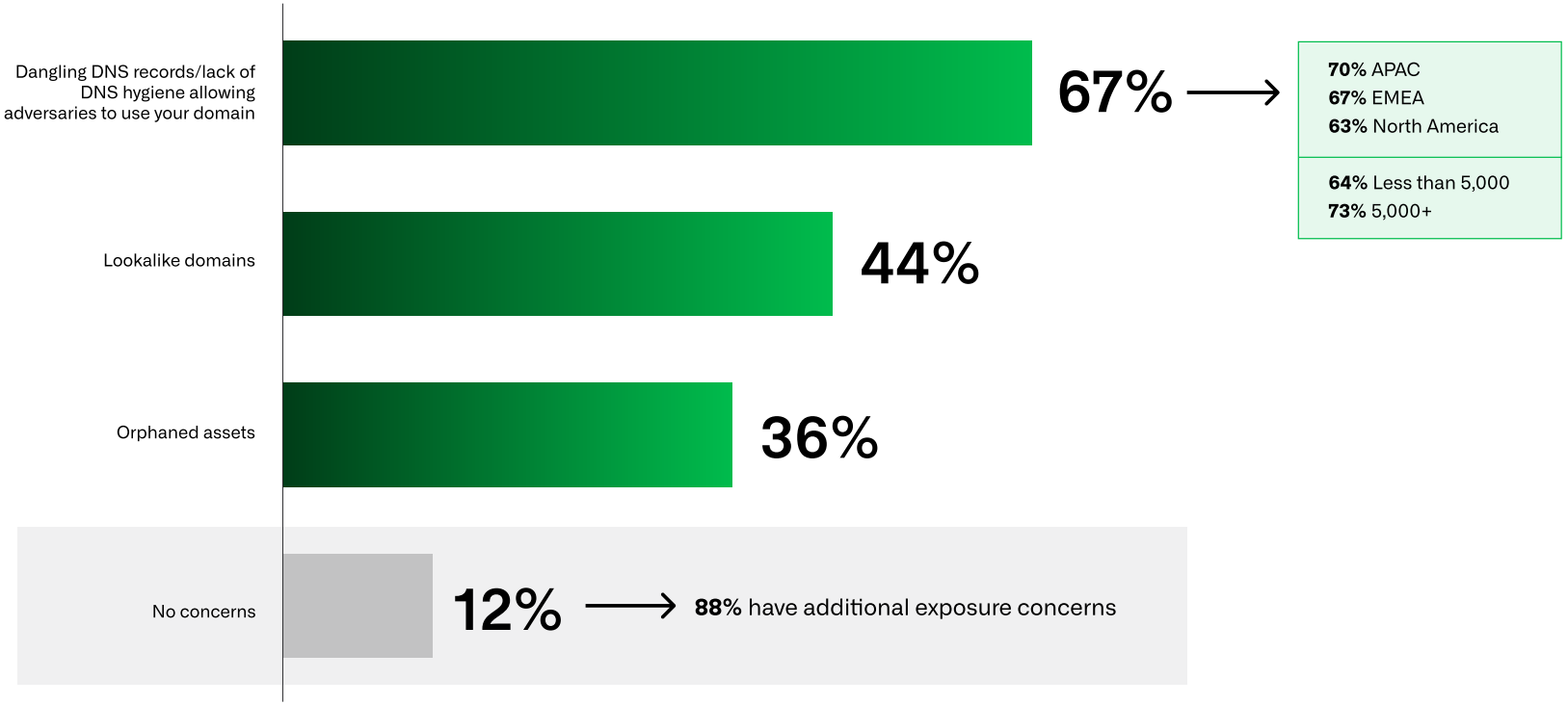
Base: 550

The fact that no single asset category dominates suggests exposure management is a widespread challenge.

OTHER EXPOSURE CONCERNS

Nearly all organizations (88%) report additional exposure concerns, with poor DNS hygiene leading the pack (67%). Poor DNS hygiene often reflects deeper visibility and ownership gaps across distributed environments.

What other exposures, if any, are you concerned about? Select all that apply:



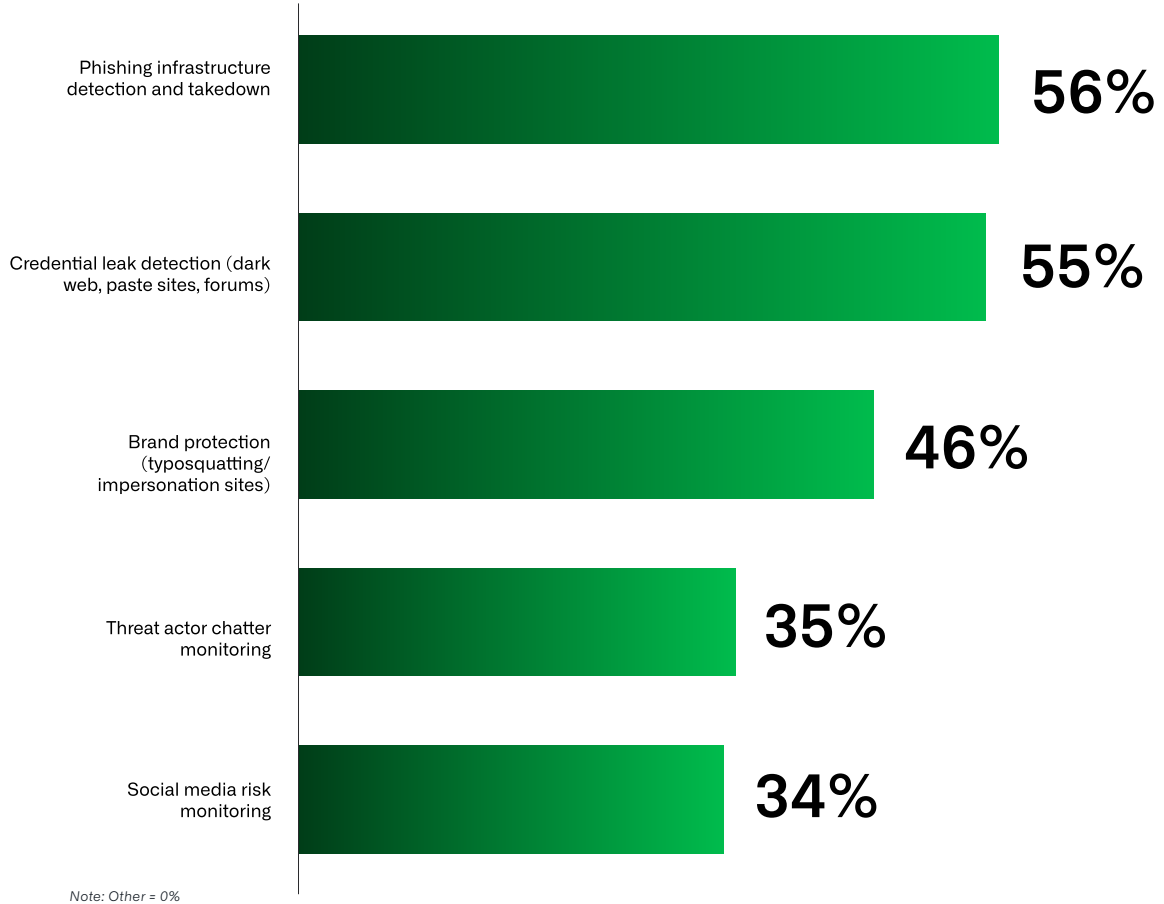
Note: Other = 0%

Base: 550

MOST CRITICAL DIGITAL RISK PROTECTION USE CASES

Organizations are prioritizing threats that directly enable or amplify attacks, with phishing infrastructure takedown (56%) and credential leak detection (55%) emerging as the most critical digital risk protection needs, and brand protection close behind (46%).

Which digital risk protection use cases are most critical for your organization? Select up to three:



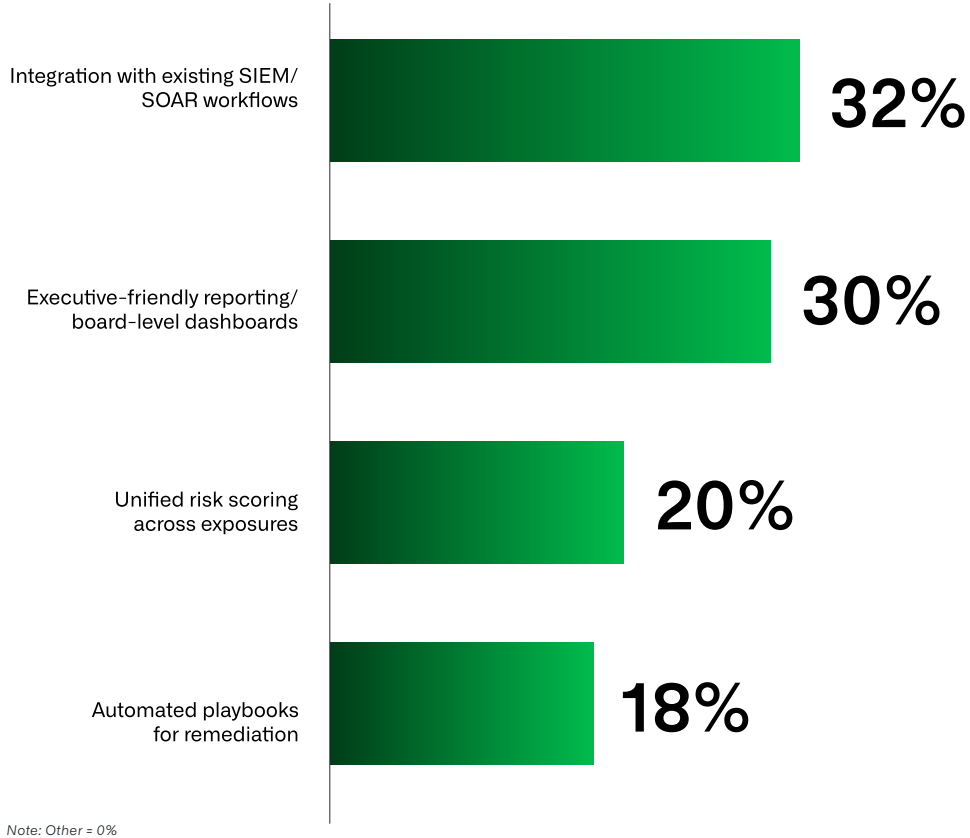
Note: Other = 0%

Base: 550

VALUE DRIVERS FOR SECURITY TOOL INTEGRATION

Integration with existing security information and event management (SIEM)/security orchestration, automation and response (SOAR) workflows (32%) and executive-friendly reporting (30%) are seen as the highest-value additions when connecting digital risk and exposure management solutions.

Which of the following would add the most value if integrated across digital risk and exposure management solutions? Select one:



Note: Other = 0%

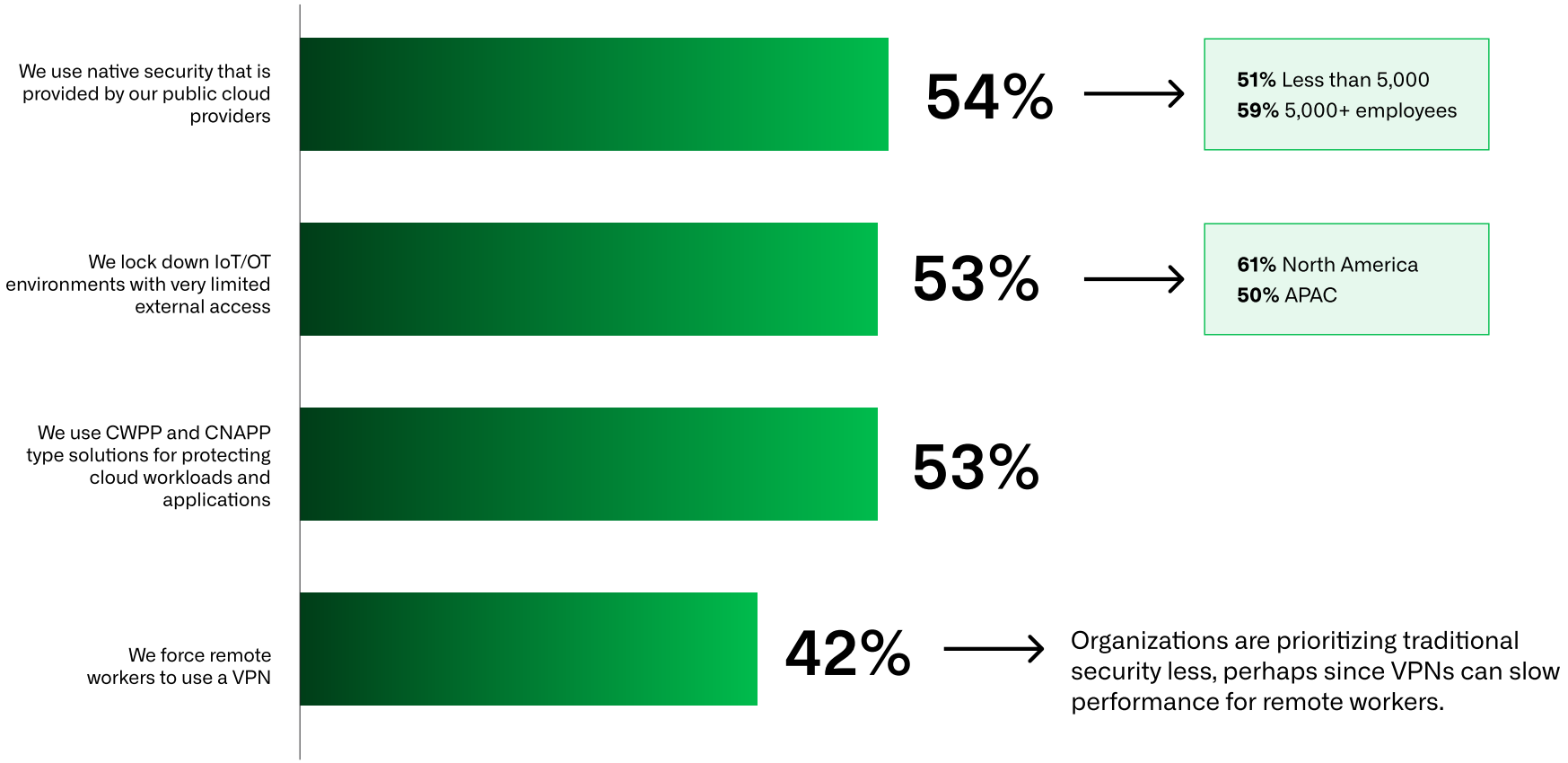
Base: 550

Security teams value integrations that streamline existing workflows and make risk visible to leadership, suggesting a focus on both operational efficiency and clear executive communication.

PROTECTING ATTACK SURFACES

No single approach dominates, and most rely on layered protection, with organizations using a mix of native cloud provider security (54%), locked-down IoT/OT environments (53%) and cloud workload protection platform (CWPP)/cloud-native application protection platform (CNAPP) solutions (53%) to secure their expanding attack surface.

How are you protecting all of your attack surface, including hybrid users, BYOD, IoT/OT and cloud workloads? Select all that apply:



Note: Other = 0%, Not sure = 2%

Base: 550

Threat Detection in the Age of AI

AI has fundamentally altered both sides of the security equation. Threat actors are using AI to generate highly convincing phishing campaigns, automate reconnaissance and rapidly generate targeted single-use attacks. In response, security teams are increasingly relying on AI-assisted detection to keep pace with volume and speed.

Nearly all organizations are already using AI within their security operations. However, many teams report ongoing challenges with real-time detection, intelligence gaps and skills shortages that limit their ability to respond effectively as attacks evolve.

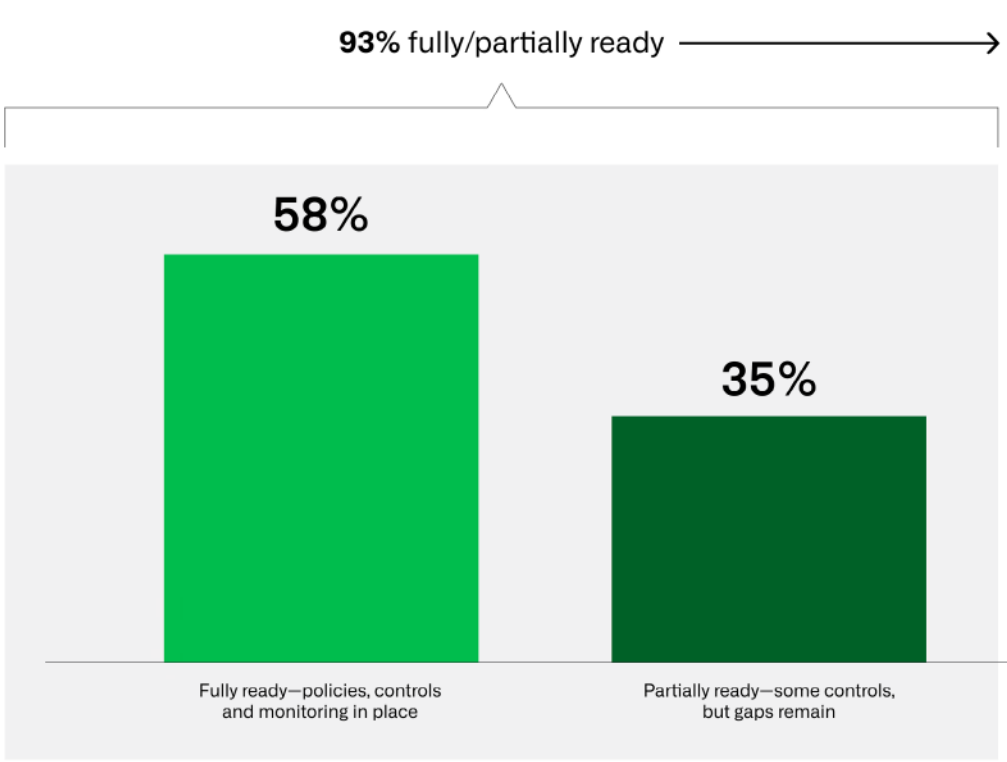
As attacks become more targeted and infrastructure more disposable, organizations need preemptive strategies that are capable of getting ahead of AI-driven attacks, reducing reliance on downstream response after compromise has already begun.

The survey data clearly shows that organizations are balancing their investments between preemptive and traditional detection/response solutions. Over half of organizations (52%) are also looking at technologies such as predictive threat intelligence to combat AI-driven threat actors.

AI SECURITY READINESS

Confidence appears high, with 93% of organizations claiming at least some readiness to secure AI systems, but with only 58% feeling fully prepared, there is still a clear gap to achieving true AI security maturity.

How ready is your organization to secure AI systems, tools and AI-driven applications? Select one:

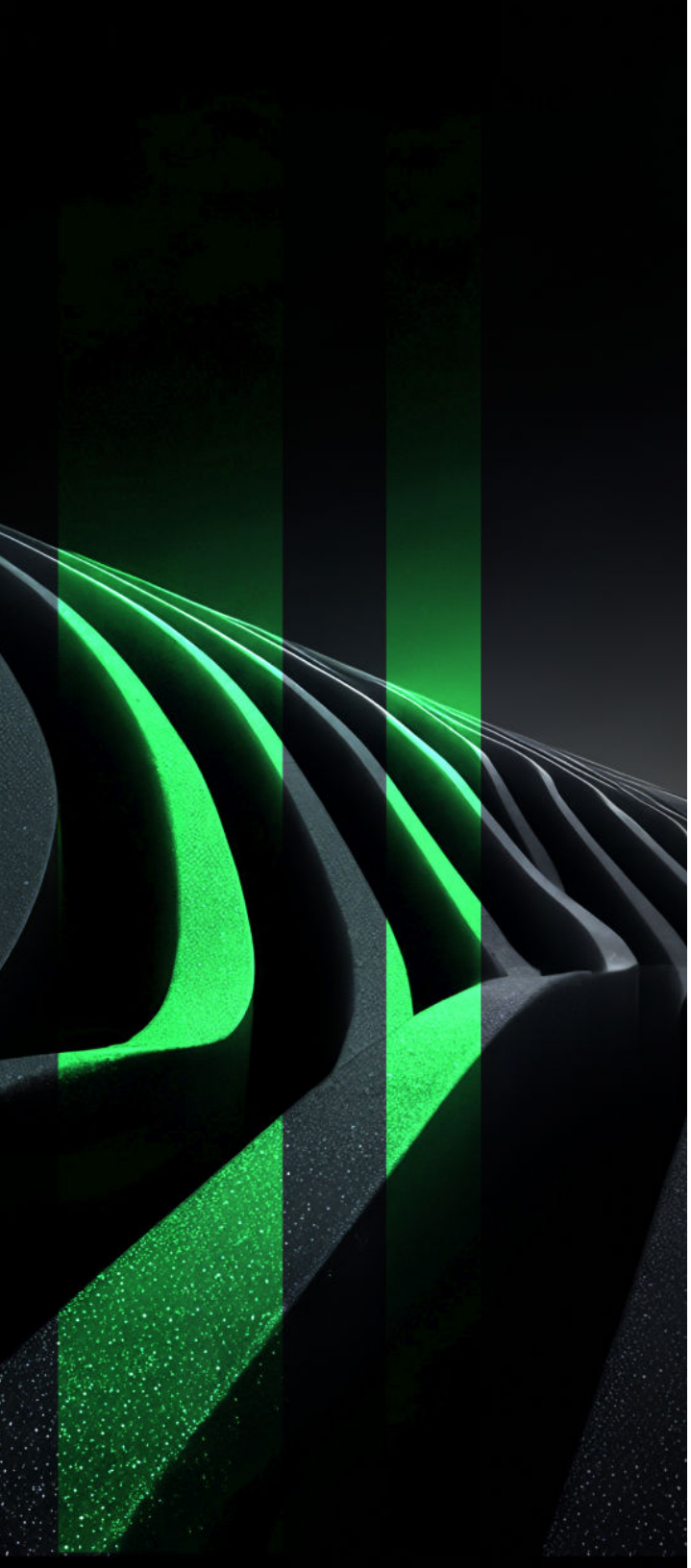


Company size	1–199	200–499	500–999	1,000–4,999	5,000+
%	80%	92%	94%	96%	97%

AI readiness increases with company size, indicating that bigger organizations are better positioned to build the infrastructure needed for robust AI security.

Note: Not sure = 1%

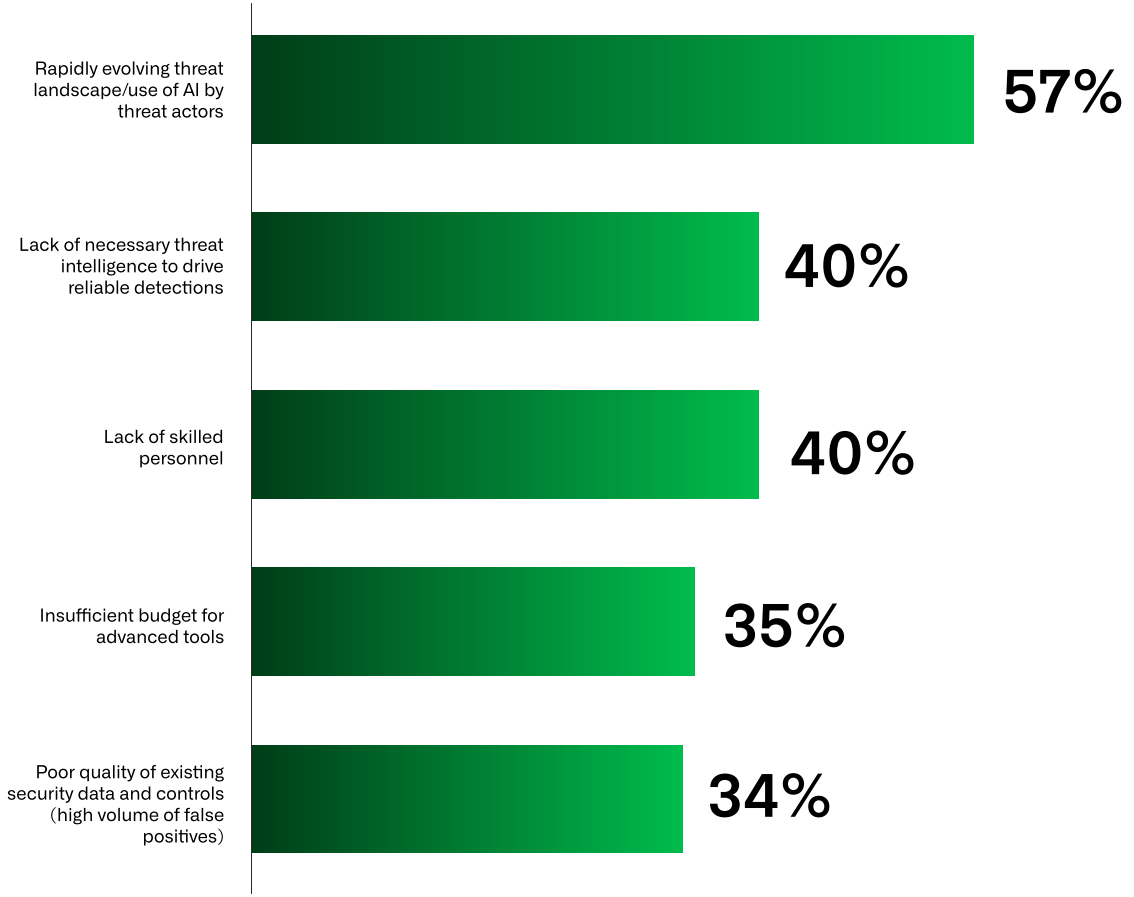
Base: 550



CHALLENGES IN REAL-TIME DETECTION

Real-time detection is a significant struggle, with over half of organizations (57%) overwhelmed by a rapidly evolving, AI-driven threat landscape, and many also held back by gaps in intelligence (40%), skills (40%) and tooling (35%).

What challenges does your organization face in detecting advanced threats in real time? Select all that apply:



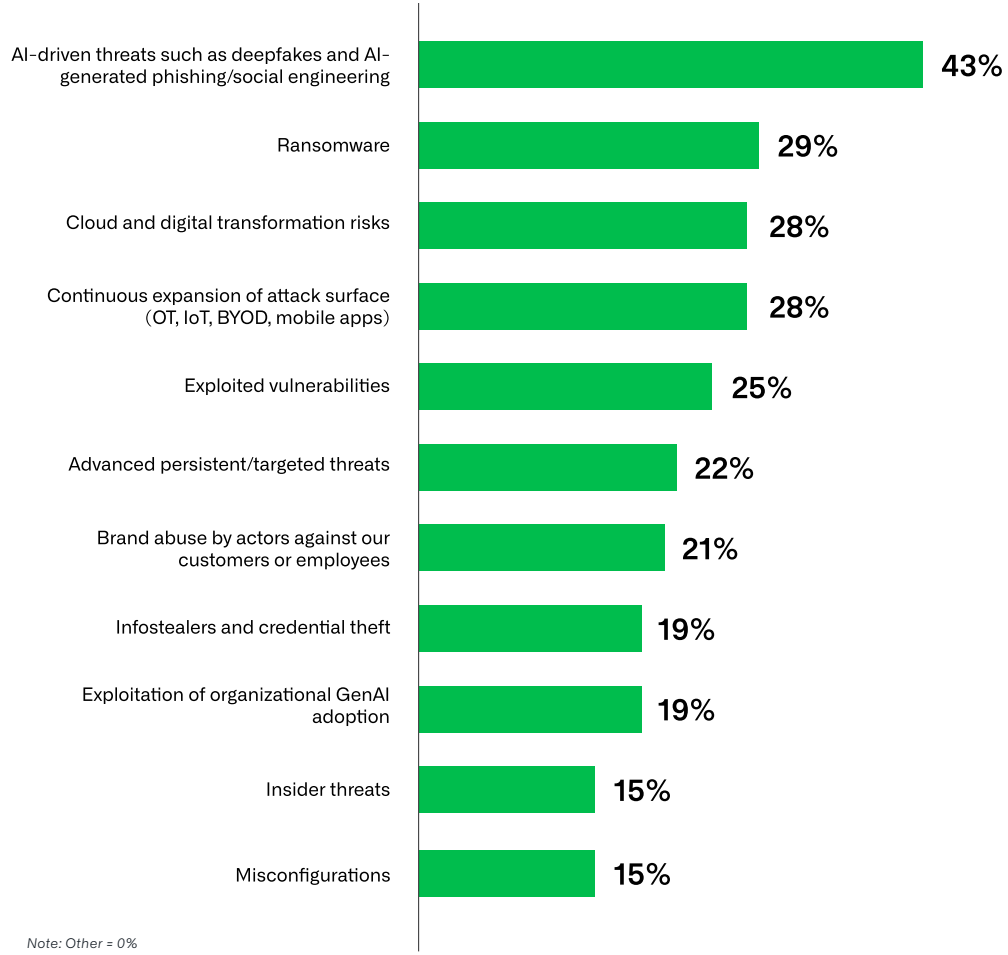
Note: Other = 2%

Base: 550

TOP THREAT CONCERNS

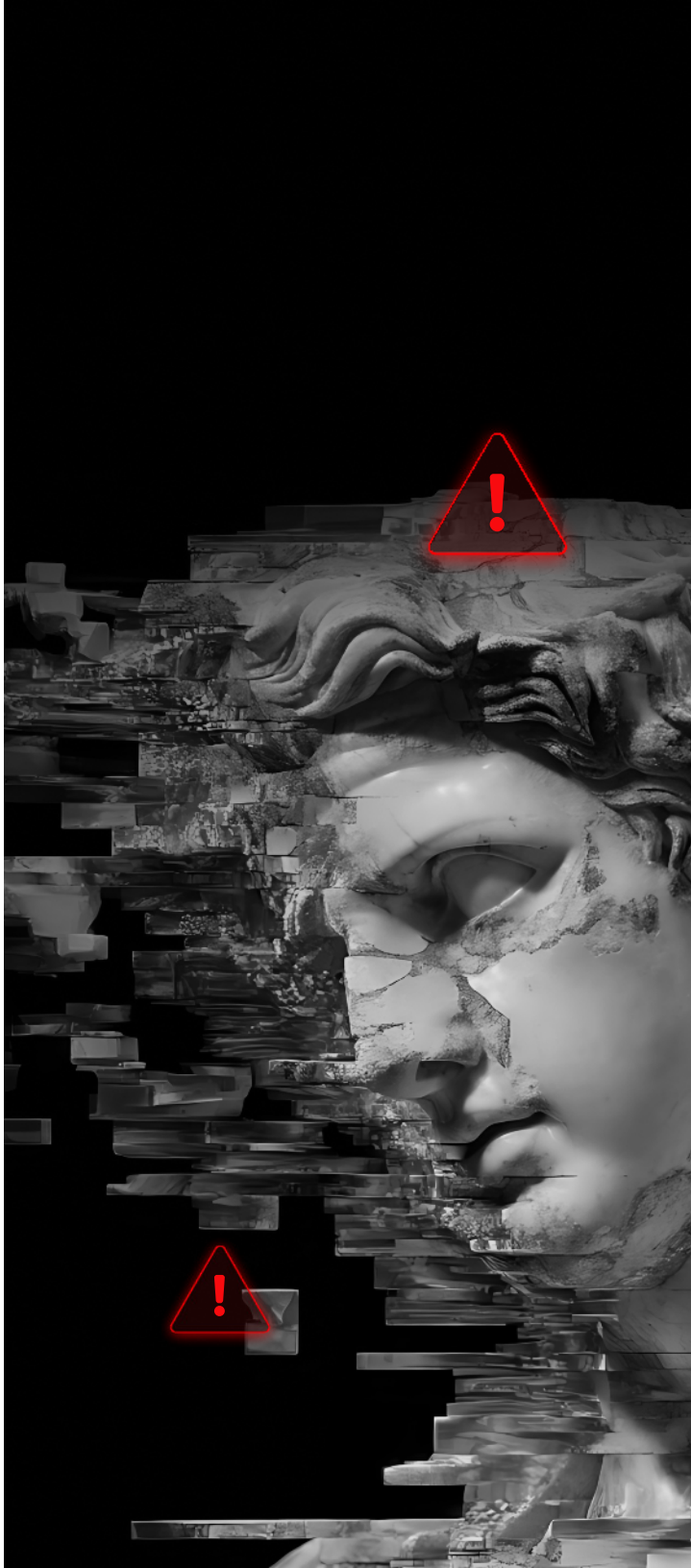
AI-driven attacks are now the leading worry for organizations, with 43% most concerned about deepfakes and AI-generated phishing, far surpassing more traditional threats like ransomware (29%) and cloud or attack-surface risks (both 28%).

What threats/risks are you most concerned about? Select up to three:



Note: Other = 0%

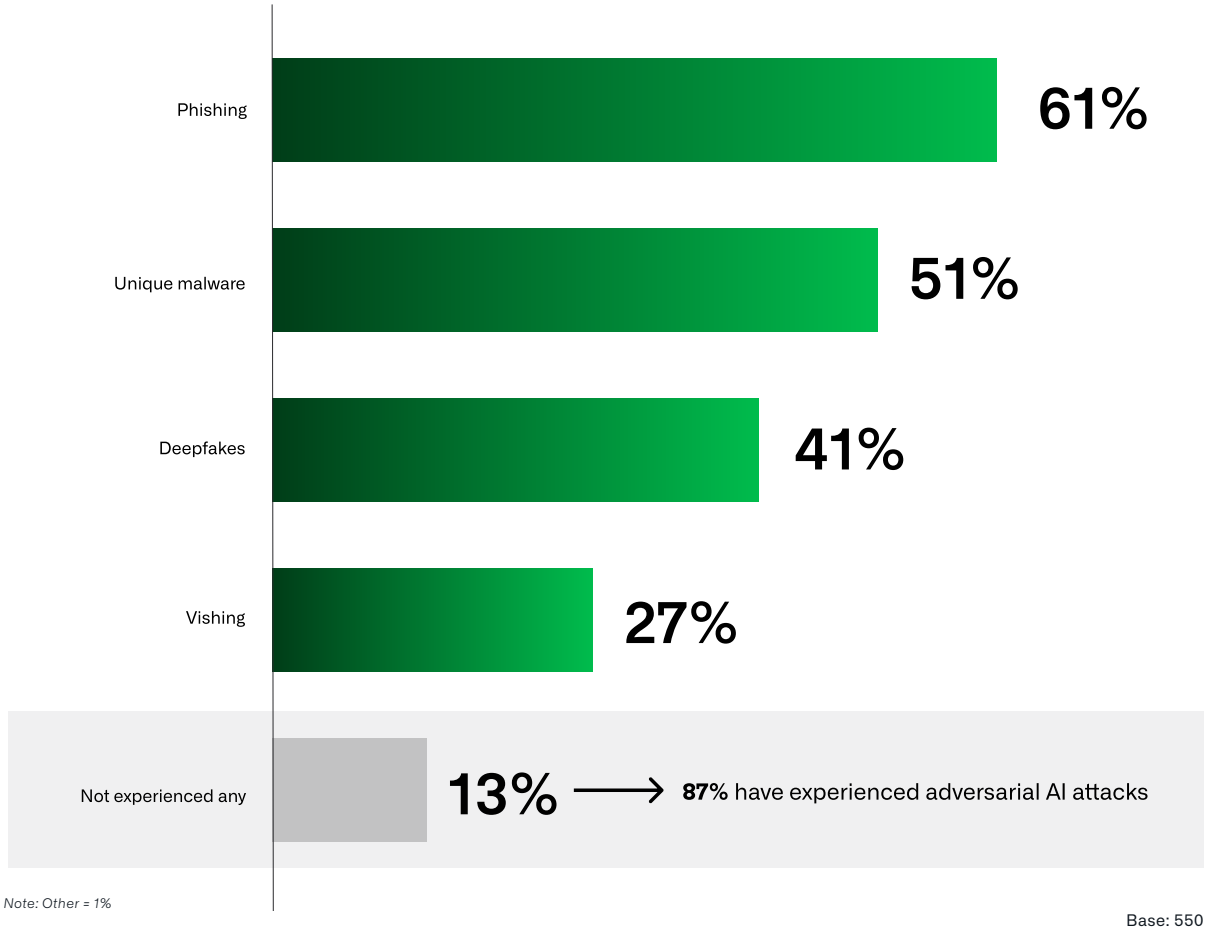
Base: 550



EXPERIENCE WITH ADVERSARIAL AI ATTACKS

The majority of organizations (87%) have already faced adversarial AI–driven attacks, with phishing (61%) and AI-crafted malware (51%) emerging as the most widespread threats.

Which of the following types of attacks (or attempted attacks) that use adversarial AI (cyberattacks that use AI and ML to get more targeted) have you/your organization experienced? Select all that apply:



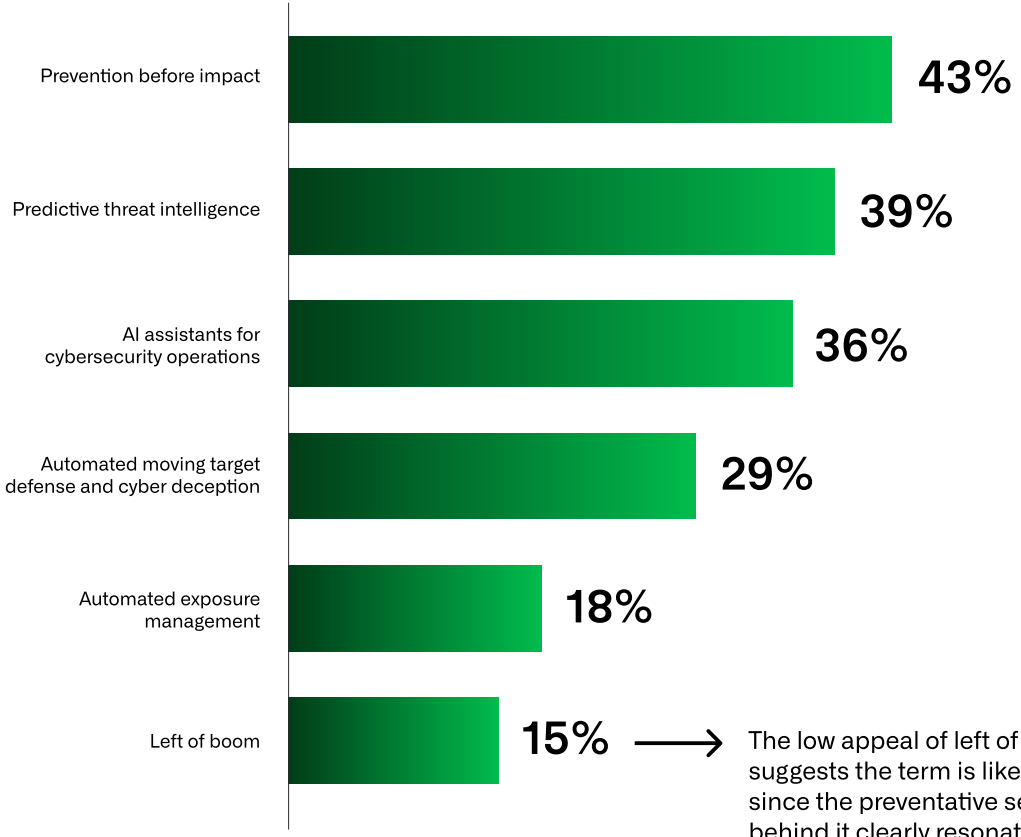
Note: Other = 1%

Base: 550

APPEAL OF PREEMPTIVE SECURITY CONCEPTS

In this report, preemptive security is defined as stopping malicious activity before impact, rather than responding after compromise. Viewed through this lens, prevention (43%) and predictive threat intelligence (39%) emerge as the most compelling aspects of a preemptive security strategy.

When you hear the term preemptive security, which phrase(s) most appeal(s) to you? Select up to two:

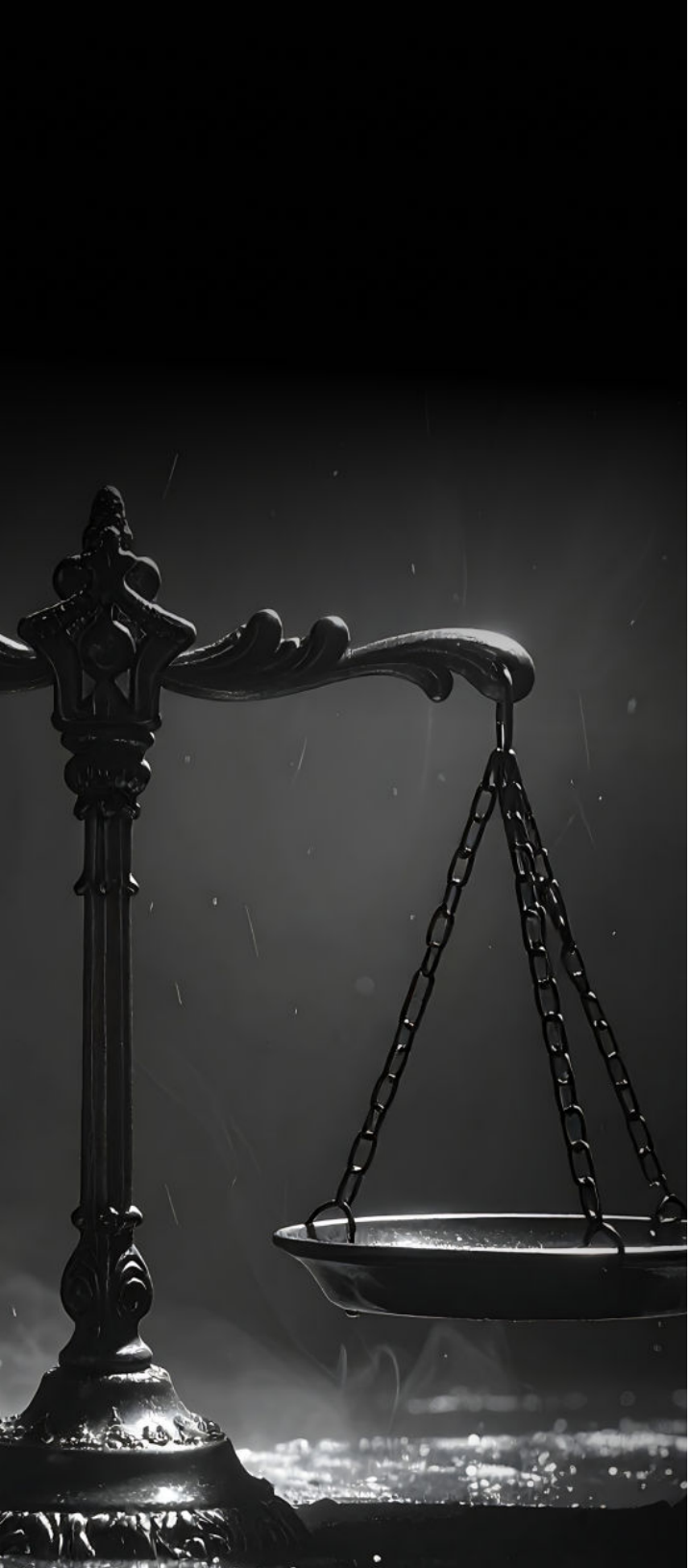


The low appeal of left of boom (15%) suggests the term is likely less understood, since the preventative security mindset behind it clearly resonates.

Note: Other = 0%

Base: 550

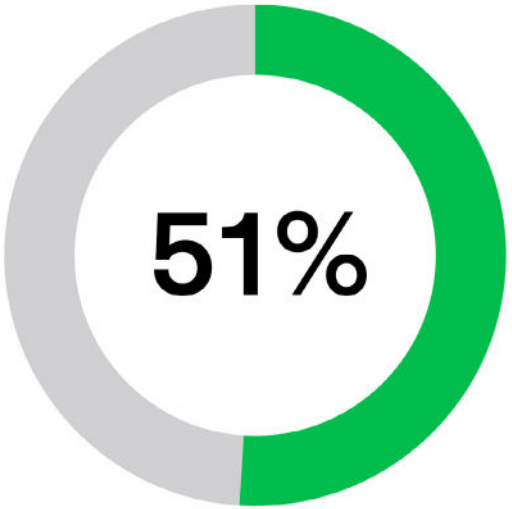
Security leaders show a clear preference for proactive, intelligence-driven approaches over more technical or niche concepts. AI-assisted security operations also resonates strongly (36%), signaling growing confidence in AI for defense.



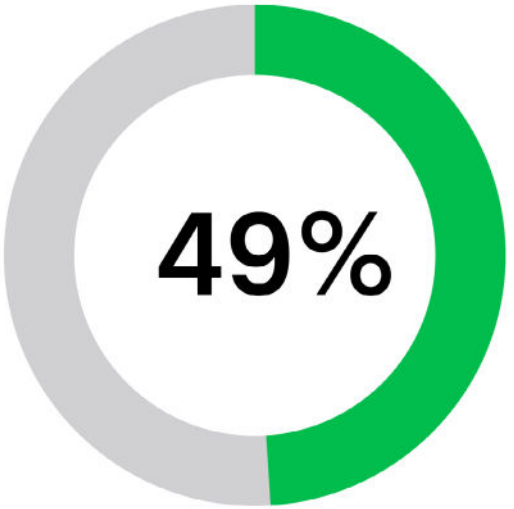
BALANCING PREEMPTIVE SECURITY WITH TRADITIONAL DETECTION

Organizations expect an almost even split between preemptive security (49%) and traditional detection/response (51%) in the next 12 months.

In the next 12 months, how do you expect your security tools to distribute between preemptive security versus traditional detection/ response? Totalizer—please write in %.



% Traditional Detection/Response



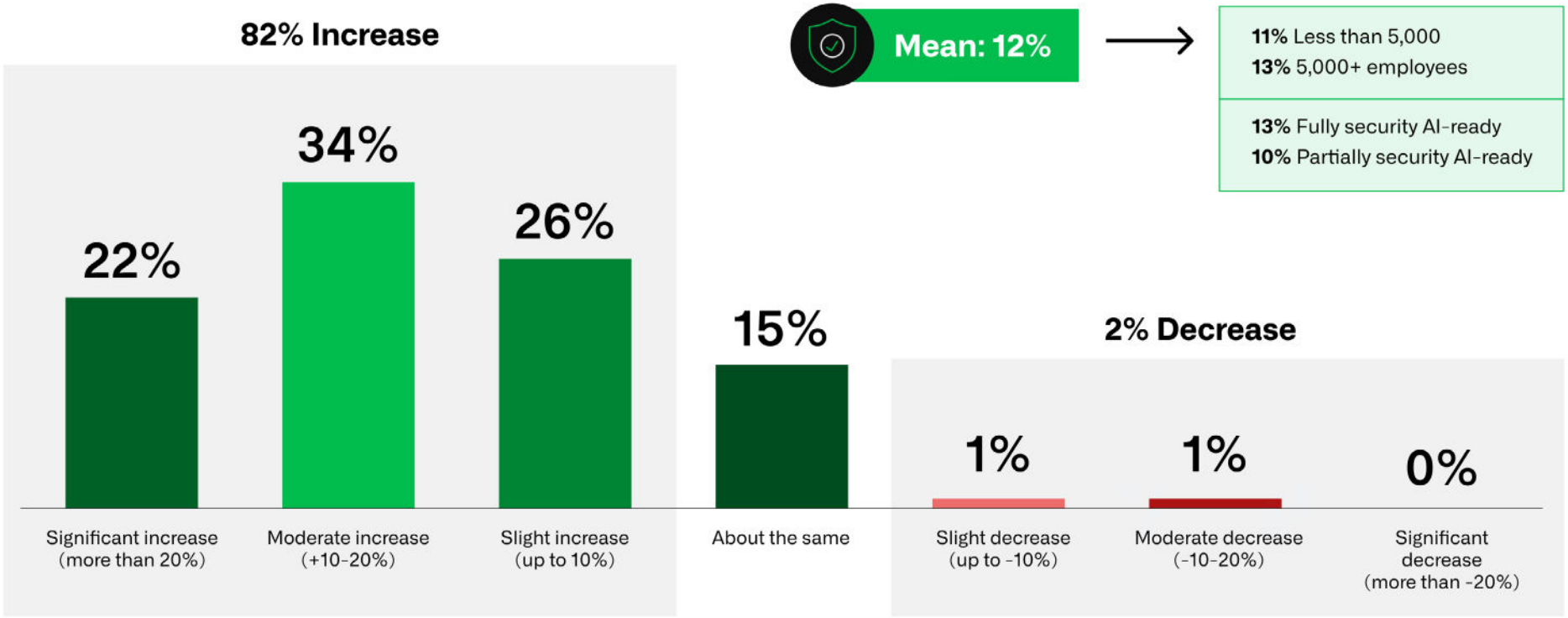
% Preemptive Security

Base: 550

CHANGE IN PREEMPTIVE SECURITY TOOL USAGE

Compared with the past year, the share of preemptive tools has risen by an average of 12%, signaling clear momentum toward more proactive security approaches despite the near-50:50 balance.

Compared to the past 12 months, how does this expected focus on preemptive security tools change?* Select one:



Note: Don't know = 1%

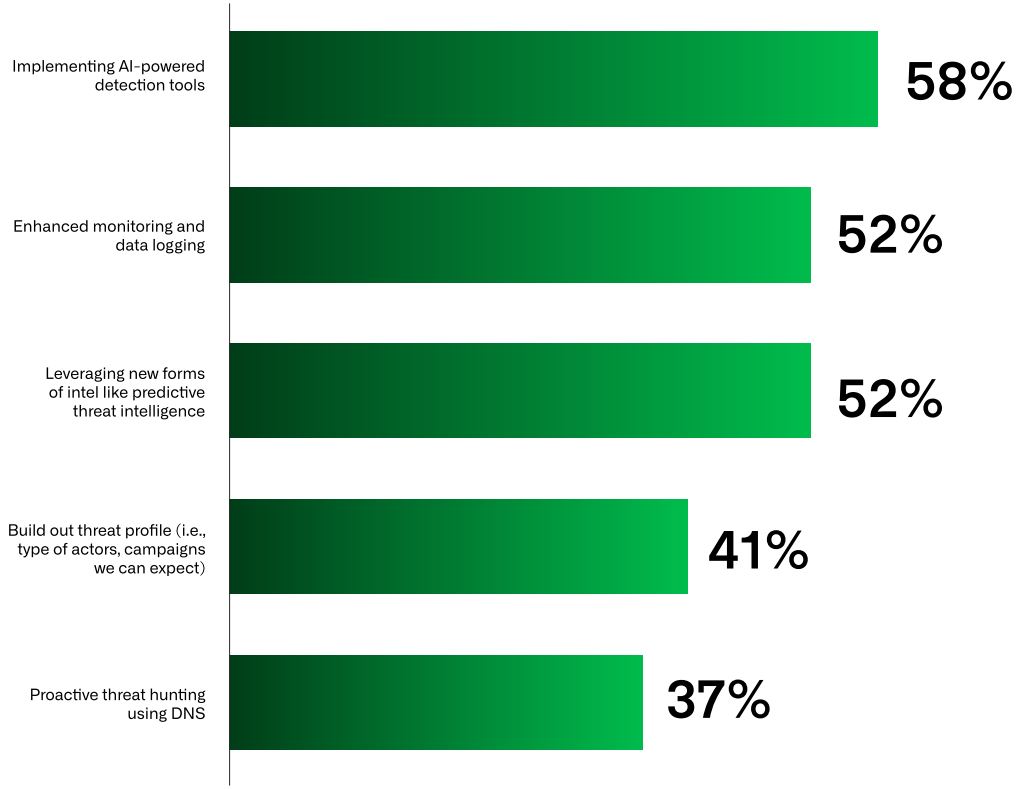
**Asked those who selected 1% or more for preemptive security*

Base: 550

COMBATTING AI-DRIVEN THREAT ACTORS

A wide range of threat detection methods are used to combat AI-driven threat actors, with the top three approaches being implementing AI-powered detection tools (58%), enhancing monitoring and data logging (52%), and leveraging newer forms of intelligence (52%).

What are you doing differently or plan to do differently for threat detection to combat the use of AI by threat actors? Select all that apply:



Note: Other = 1%

Base: 550

The lack of a single dominant strategy suggests that organizations are relying on a layered, multi-method defense, recognizing that no single solution is sufficient to stay ahead of increasingly evasive attacks.

Conclusion: Preemptive Security, Digital Risk and External Exposures

PREEMPTIVE SECURITY AS THE FOUNDATION OF EXPOSURE AND DIGITAL RISK MANAGEMENT

Taken together, the findings point to a clear evolution in security strategy. Organizations are no longer choosing between detection and prevention. They are seeking ways to connect digital risk intelligence, exposure management and foundational controls into a more continuous, proactive approach.

Preemptive security reflects this shift. Rather than waiting for compromise, it focuses on reducing attacker opportunity by identifying externally exposed and high-risk digital assets, prioritizing exposures based on real-world threat activity and disrupting malicious infrastructure earlier in the attack lifecycle.

The research suggests that organizations see the greatest value when digital risk protection, exposure management and preemptive controls complement existing detection and response capabilities. Together, these approaches help security teams concentrate effort where it matters most, reducing digital risk and preventing impact before attacks reach users, customers or the enterprise.

Research Overview and Methodology

CONTEXT AND BACKGROUND

To ensure statistically valid insights, research was conducted across a global sample of cybersecurity professionals using a rigorous survey methodology.

At an overall level, results are accurate to ± 4.2% at 95% confidence limits assuming a result of 50%.

The interviews were conducted online by Sapio Research in October 2025 using an email invitation and an online survey.

Respondents

- N = 550 panel respondents
- Cybersecurity professionals
- Based in Australia, France, Germany, India, Japan, Singapore, South Africa, United Arab Emirates, the United Kingdom and the United States
- **Focus sectors:** Education, financial services, government, healthcare, manufacturing and retail

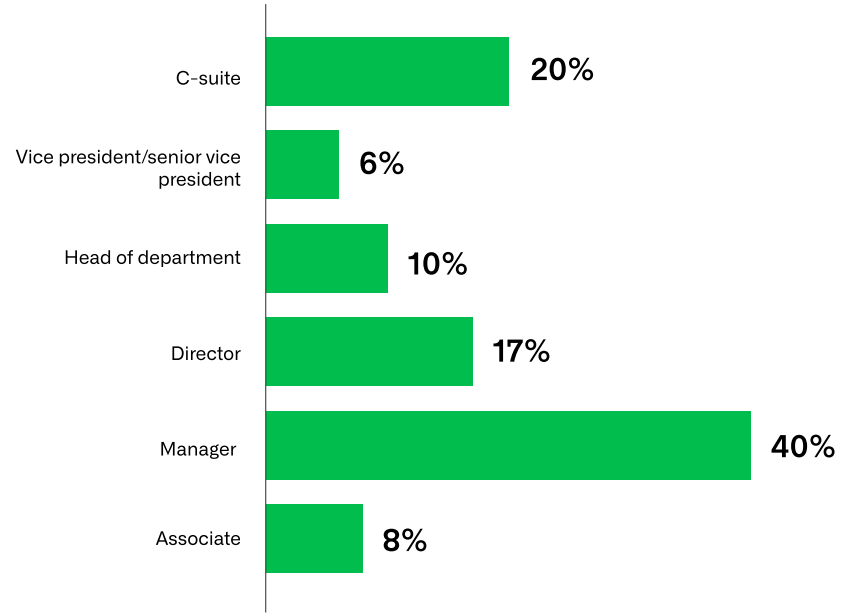
RESPONDENT DEMOGRAPHICS SUMMARY

Country of Residence

Business Size

Number of Employees	Number of Respondents
1–199	15%
200–499	25%
500–999	24%
1,000–4,999	19%
5,000+	18%

Job Role



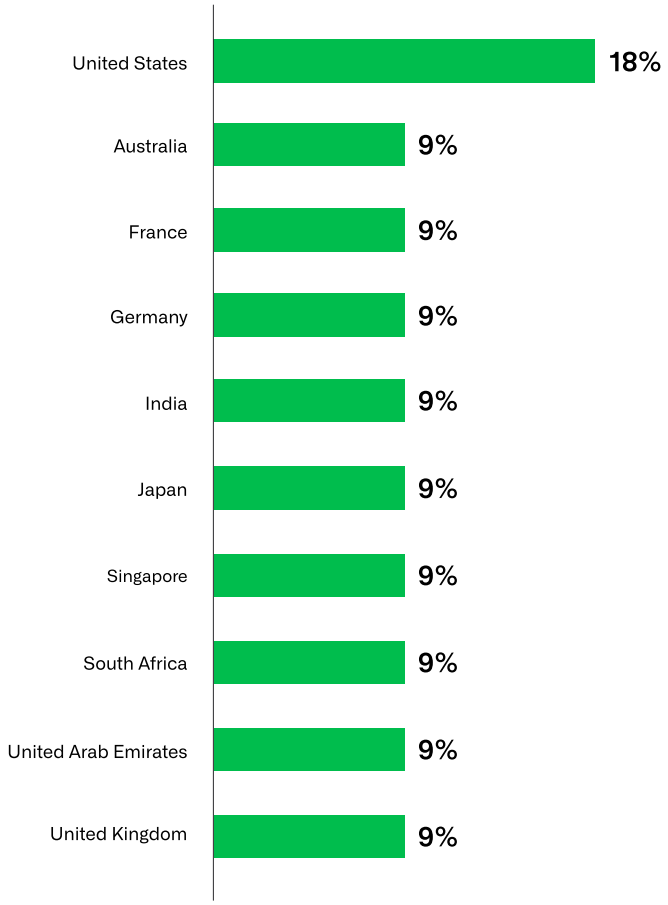
Top Sector

1	Manufacturing	14%
2	Financial services	14%
3	Government	10%
4	Healthcare	10%
5	Education	10%
6	Retail	10%

COUNTRY AND INDUSTRY

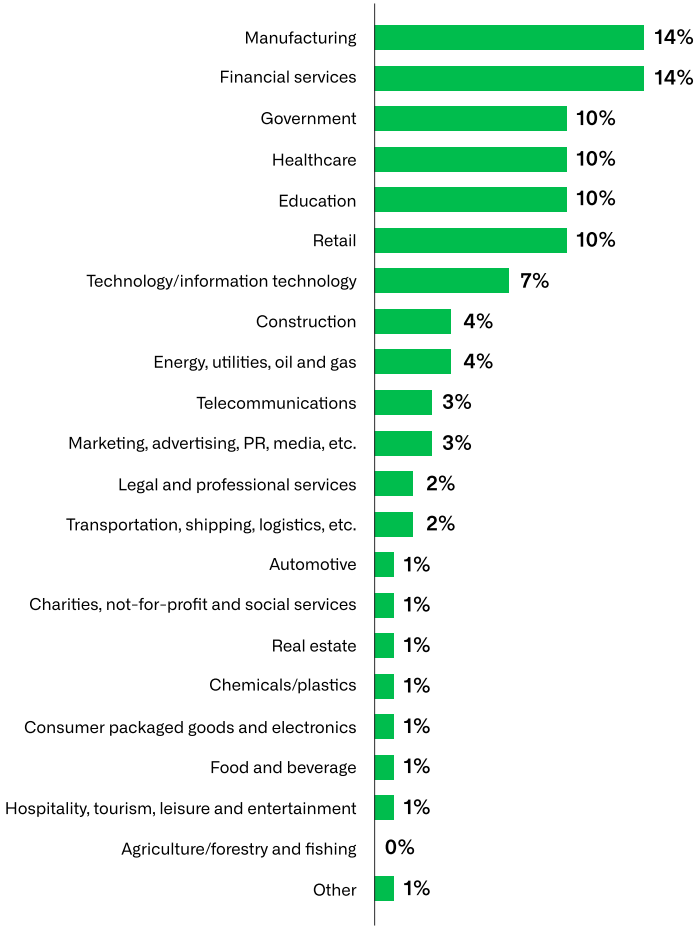
Country

Which country do you live in? Select one.



Industry

What industry sector is your organization in? Select one.

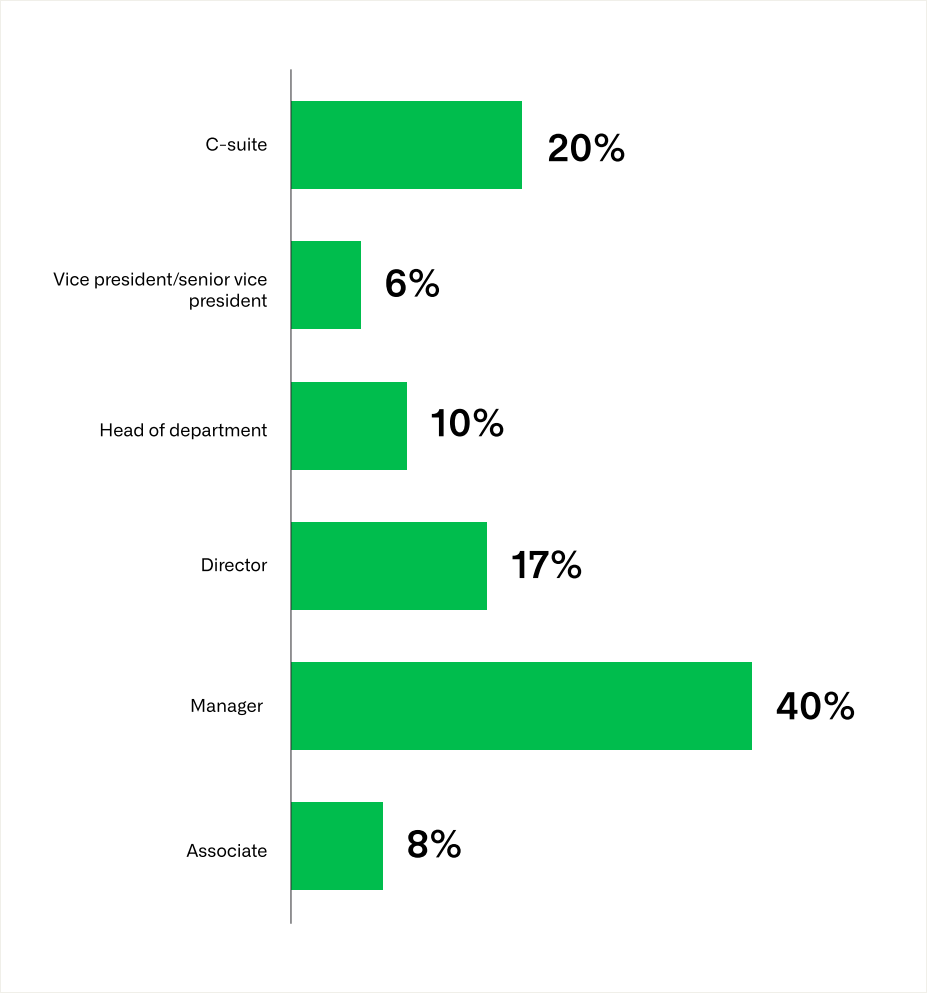


Base: 550

JOB ROLE

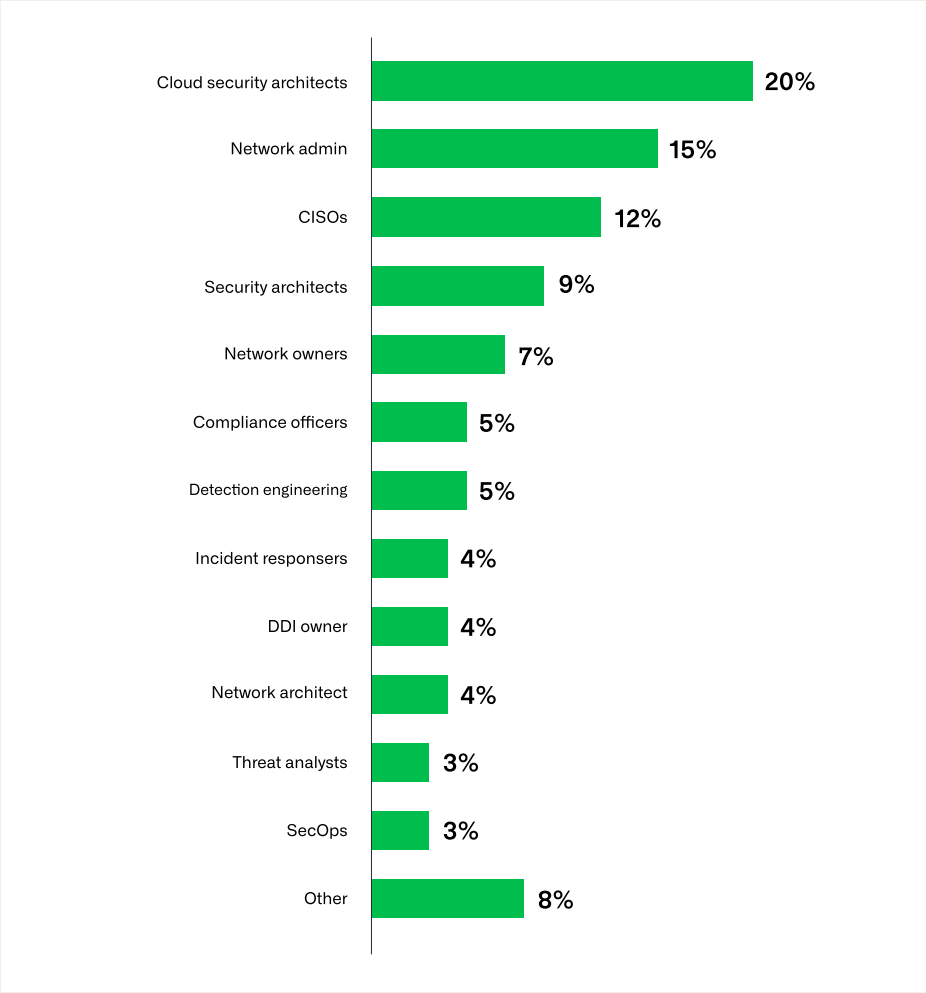
Job Role

Which of the following best describes your job role? Select one.



Functional Role

Which of the following best describes your job role? Select one.

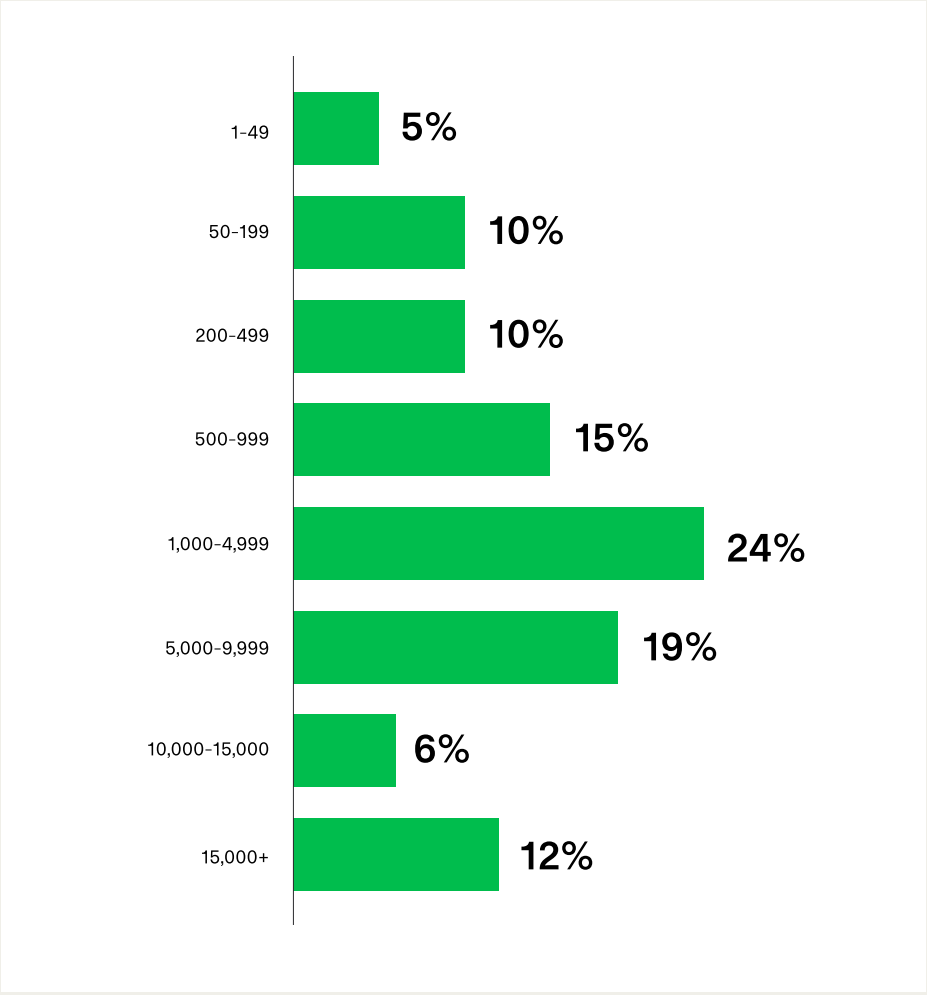


Base: 550

COMPANY SIZE AND DEPARTMENT

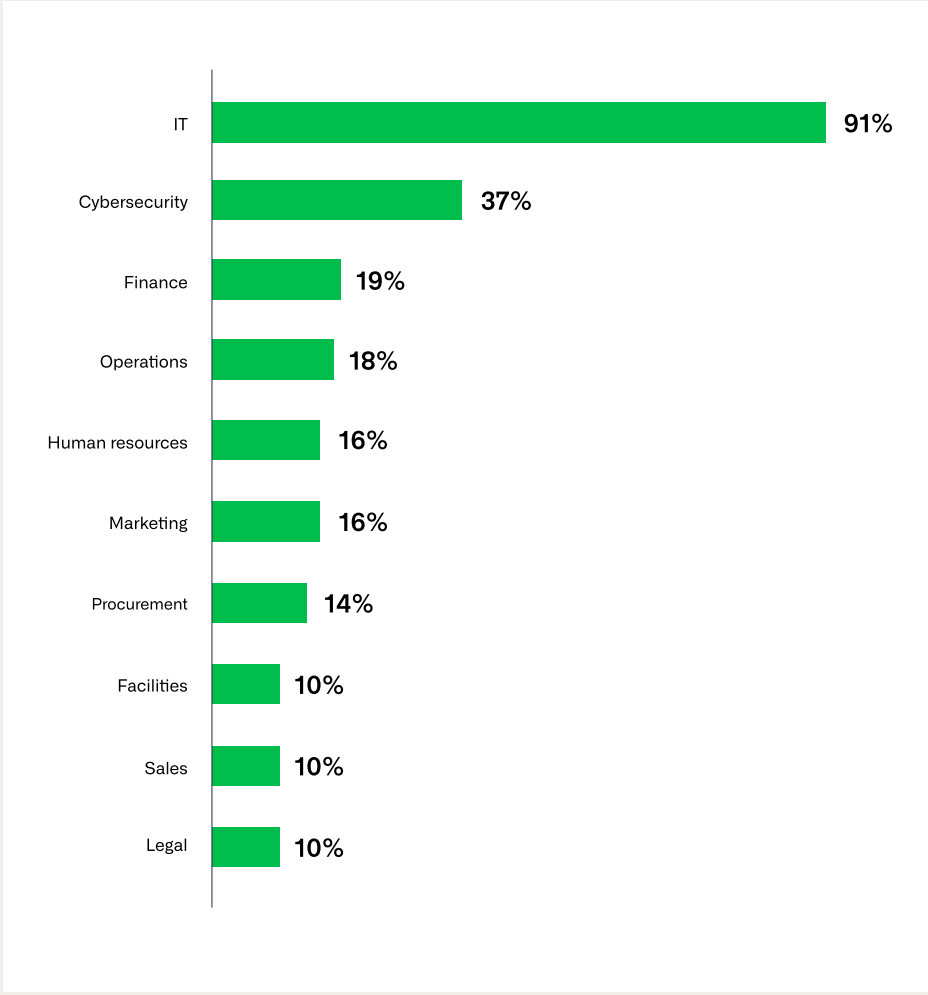
Company Size

How many people work in your organization? Select one.



Department

Which of the following departments do you work in or are responsible for? Select all that apply.



Base: 550

ABOUT INFOBLOX

Infoblox unites networking and security with a protective DDI platform. We combine market-leading DNS, DHCP and IP address management (DDI) with Protective DNS and deep asset visibility so organizations can secure, automate and scale hybrid, multi-cloud environments.

Our platform brings together:

- **Infoblox Universal DDI™** to unify DNS, DHCP and IP address management across data centers, clouds and edge locations
- **Infoblox Threat Defense™** Protective DNS to stop threats at the DNS layer before they reach users, devices or workloads
- **Infoblox Universal Asset Insights™** for real-time context on which users, devices and workloads are behind DNS activity
- **Digital Risk Protection Services** (**DRPS**), part of Infoblox Exposure Management, to detect and disrupt phishing, brand abuse, credential exposure and fraud across external attack surfaces; built on technology acquired from Axur

Explore how Infoblox supports Exposure Management and Protective DNS with its protective DDI platform at infoblox.com. To discuss this research or see a tailored demonstration, visit infoblox.com/contact or reach out to your local Infoblox representative.

Research conducted with assistance from Sapio Research.

team@sapioresearch.com | sapioresearch.com

infoblox.

Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business, providing the visibility and context needed to move fast without compromise.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com