cynet



Global AI Security Readiness Report

How MSPs and in-house security teams are preparing their people, processes, and products for AI-driven threats

www.cynet.com

cynet

Table of Contents

Introduction 3

Key Findings and Methodology 4

Section One: The AI Impact 5

1. AI-Powered Threats Are Top of Defense Priority List 6
2. MSPs Embrace the AI Future 7
3. In-House Teams and MSPs Are Aligned on the Top Priority Capabilities 8
4. 59% Want to Involve MSPs When Adopting New Security Tools 9
5. Over 80% Plan to Spend More in Pursuit of Faster Detection and Response 10
6. AI Adoption Is No Longer Optional, but Hesitation Remains 11

Section Two: The Current Threat Landscape 12

1. MSPs Report Fewer Incidents Among Their Customers Than In-House Teams 13
2. MSPs Benefit From Experience With Diverse Threats and a Deeper Security Bench 14
3. Incidents Add Pressure for Internal Resources 15
4. MSPs Manage 60% More Cybersecurity Tools Than In-House Teams 16

Key Takeaways 17

INTRODUCTION

Advances in AI Have Changed the Rules for Attackers and Defenders

Modern attacks are now comprised of coordinated chains of strikes, engineered to find the path of least resistance across an ever-expanding attack surface.

Every device, every credential, every misconfiguration is a potential entry point, and while defenders may cautiously embrace some AI tooling, attackers with little to lose are using cutting edge technology to find and exploit gaps whenever they exist.

We surveyed:

800
Managed Service Providers (MSPs)

800
in-house security representatives

to understand how small-to-medium-sized businesses (SMBs) are responding to the new AI-led chapter of cybersecurity. Respondents were based in Australia, Canada, Ireland, Italy, New Zealand, Portugal, Spain, UK and US. Interviews were conducted by Sapio Research in March 2026 using an email invitation and an online survey.

Throughout the report we use **blue to represent MSPs** and **magenta to represent in-house security teams**. This visual differentiation will help you easily follow the data and see how perspectives vary between these two groups.

Among insights on cybersecurity budgets, tools, and the threat landscape, we identified how MSPs are uniquely positioned to educate and guide internal security teams through deeper, earlier AI adoption. Our findings demonstrate a strong alignment between MSP offerings and the capabilities most valued by SMBs.

Furthermore, the network benefits and deep expertise provided by MSPs make them ideal partners for in-house teams evaluating new security tools.



The findings in this report will help you position your business for success against the backdrop of AI-powered cybersecurity threats and opportunities, now and into the future.

Key Findings

Security Budgets

89%

MSPs

are increasing their security budgets

78%

IN-HOUSE SECURITY TEAMS

are increasing their security budgets

Top Priorities

MOST URGENT THREATS

Defending against AI-enabled social engineering & phishing campaigns

IMPACTS OF SECURITY INCIDENTS

Increased strain on internal resources and data exposure

MSP Adoption

59%

IN-HOUSE SECURITY TEAMS

want to involve MSPs when adopting new cybersecurity capabilities

Incident Exposure

22%

MSPs

Number of MSP clients on average that experienced or suspected a security incident

60%

IN-HOUSE SECURITY TEAMS

experienced or suspected incidents

cynet



Section 1:

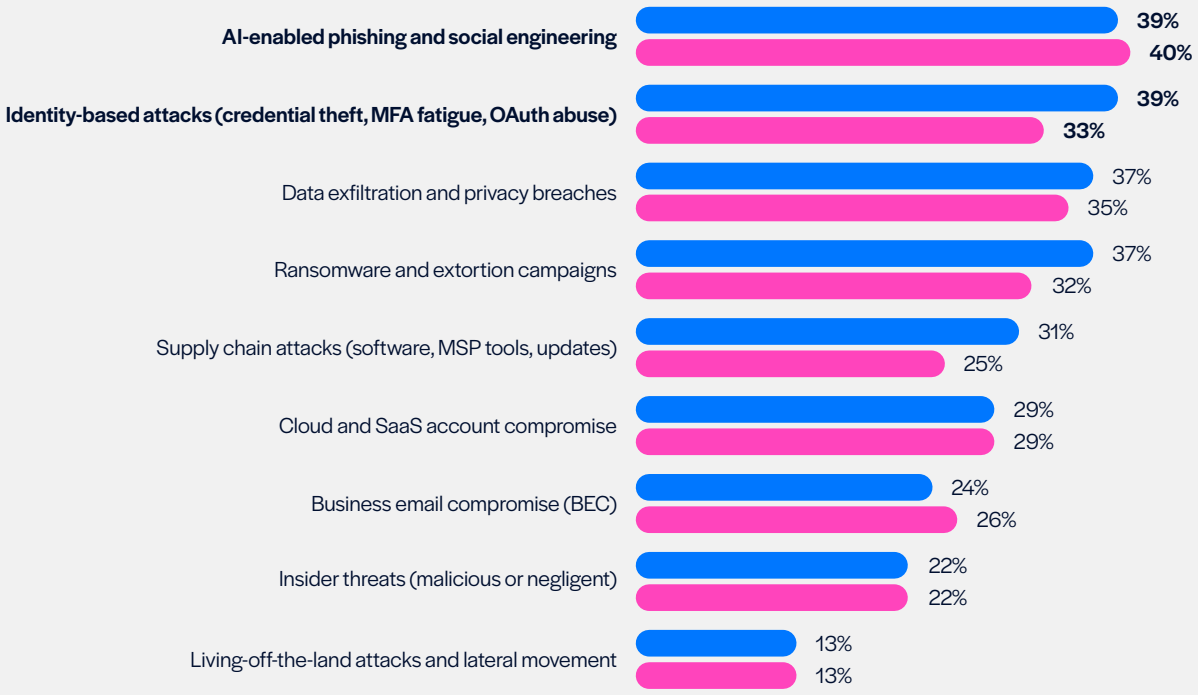
The AI Impact

How AI is influencing cybersecurity strategies and spending plans.

AI-Powered Threats Are Top of Defense Priority List

Defending against AI-enabled phishing and social engineering is the highest priority for MSPs and in-house teams, along with identity-based attacks – which are exacerbated by agentic AI in the hands of bad actors.

Respondents were asked which security threats are the highest priority for them to defend against in 2026.



AI is at the core of the modern SOC

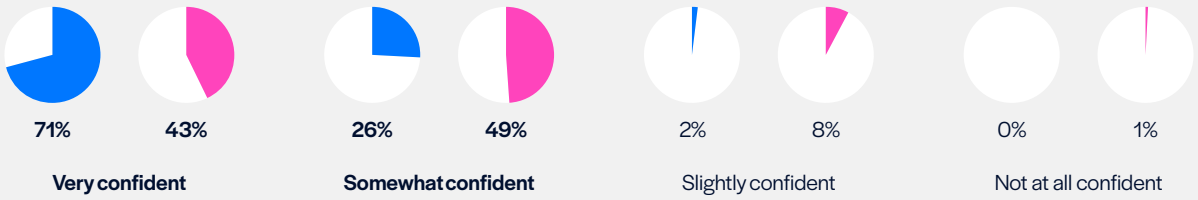
The integration of AI into cybersecurity operations is becoming increasingly pivotal for both MSPs and in-house teams. In particular, agentic AI enables autonomous threat detection and response at a speed and scale no human team can match. This shifts security operations from reactive to proactive, where AI agents – overseen by humans – continuously hunt threats, adapt to evolving attacker tactics, and multiply the capacity of lean security teams. However, as organizations strive to strengthen their security measures, AI technologies are being adopted at varying rates across different sectors. In a threat landscape subject to constant change, MSPs are uniquely positioned to lead the charge in bringing their customers into the AI era.

MSPs Embrace the AI Future

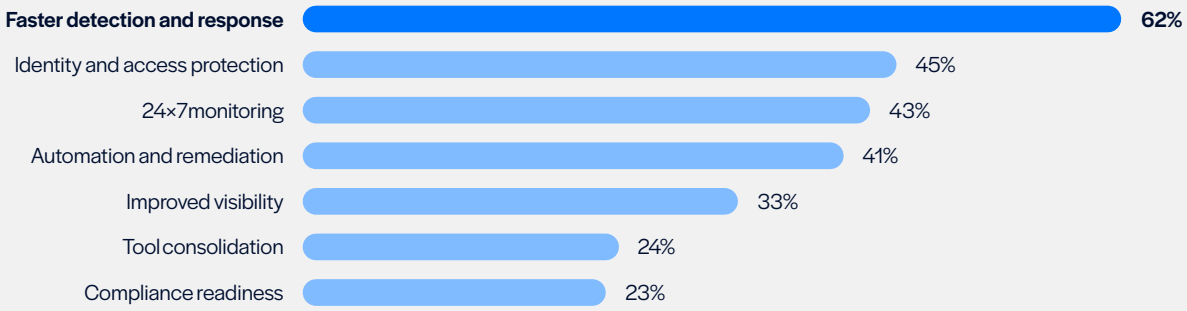
71% of MSPs are very confident in their ability to detect and respond to customer incidents. This confidence can be attributed to the integration of AI tools which bolster their operational efficiency and effectiveness. Added to which, 62% plan to make significant improvements in detection and response times in customer security postures this year – an area AI is ideally positioned to support.

In contrast, **in-house teams, while confident in their ability to detect and respond to incidents, are still catching up. 43% are very confident and 49% are somewhat confident,** indicating room for growth in AI adoption.

MSP respondents were asked how confident they are in their ability to detect and respond to customer incidents.
In-house team respondents were asked how confident they are in their ability to detect and respond to security incidents.



MSP respondents were asked where they expect to make the biggest improvements to customer security postures in 2026.



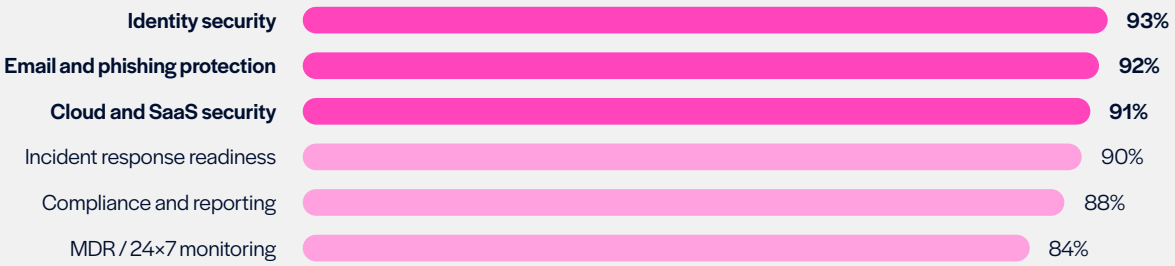
MSPs bridge the AI adoption gap

As MSPs continue to advance their AI capabilities, they are uniquely positioned to assist in-house teams in getting to grips with AI in cybersecurity, offering expertise which bridges the gap in AI adoption rates.

In-House Teams and MSPs Are Aligned on the Top Priority Capabilities

Capabilities sought by in-house teams are strongly reflected in MSPs' offerings, with identity security, email and phishing protection, and cloud and SaaS security featuring in the top three for both groups.

In-house team respondents were asked to what extent the listed security capabilities are important to their organization today.



MSP respondents were asked which security capabilities they currently offer their customers.



Regions vary on agentic AI

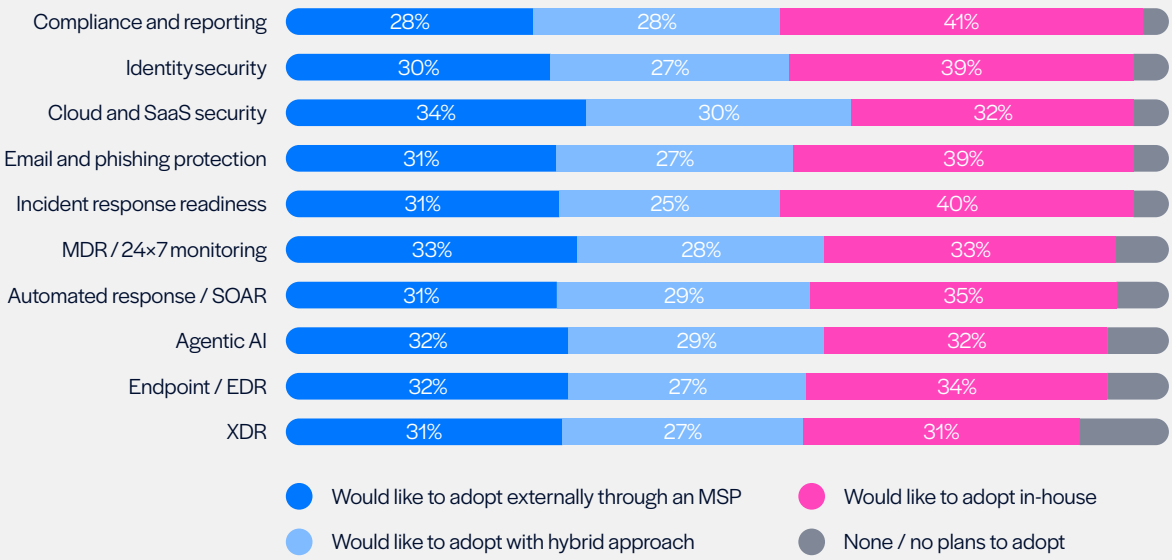
Over half (53%) of in-house teams in Australia and New Zealand rate agentic AI as very important. Only 35% of their counterparts in Southern Europe (the region least likely to detect incidents using their own security tools) agree. MSPs in southern Europe have an opportunity to engage customers who are hesitant to adopt agentic AI in-house, and pair it with their human-in-the-loop AI strategy.

59% Want to Involve MSPs When Adopting New Security Tools

The preference for adopting new tools through either a hybrid approach or MSPs is becoming more pronounced, reflecting a strategic shift in how organizations manage their cybersecurity needs. For instance, 27% of in-house teams want to adopt EDR using a hybrid approach, while 32% prefer to adopt it externally through an MSP.

Cloud and SaaS security sees 34% of in-house teams looking to MSPs for help and 30% considering a hybrid approach. For MDR and 24/7 monitoring, 33% of in-house teams are considering MSPs, while 28% are interested in a hybrid approach. Nearly a third (32%) of in-house teams want MSPs to help them introduce agentic AI, while 29% are considering a hybrid adoption approach.

In-house team respondents were asked how they would ideally implement the listed capabilities.



MSPs have an AI leadership role

14% of in-house teams say AI assistants, AI SOC agents and other agentic AI are not very or not at all important security capabilities. A further 7% of organizations have no plans to adopt agentic AI in this area. But the reality is that AI-driven zero-day attacks underscore the futility of resisting AI implementation. Threat actors have already embraced the potential of artificial intelligence, and organizations who fail to adopt AI-powered solutions face an uncertain future. MSPs, with their early and effective adoption of the technology, can help lead reticent clients on the need and means to embrace it.

Over 80% Plan to Spend More in Pursuit of Faster Detection and Response

The vast majority of in-house teams (78%) and MSPs (89%) plan to spend more on security tools this year than last year.

Respondents were asked what best describes their security tools budget outlook for 2026 compared to last year.



Driving this spend is a desire to speed up detection and response and operate more efficiently in the face of an increase in zero-day attacks and vanishingly small TTE window. For instance, 42% of in-house teams consider faster detection and response as a critical outcome when evaluating security investments for 2026, indicating a growing recognition of AI's potential.

Respondents were asked which outcomes matter most when evaluating security investments in 2026.



Top 3 investment areas for in-house teams in 2026

01 **Cloud security**

02 **Securing AI agents and LLMs**

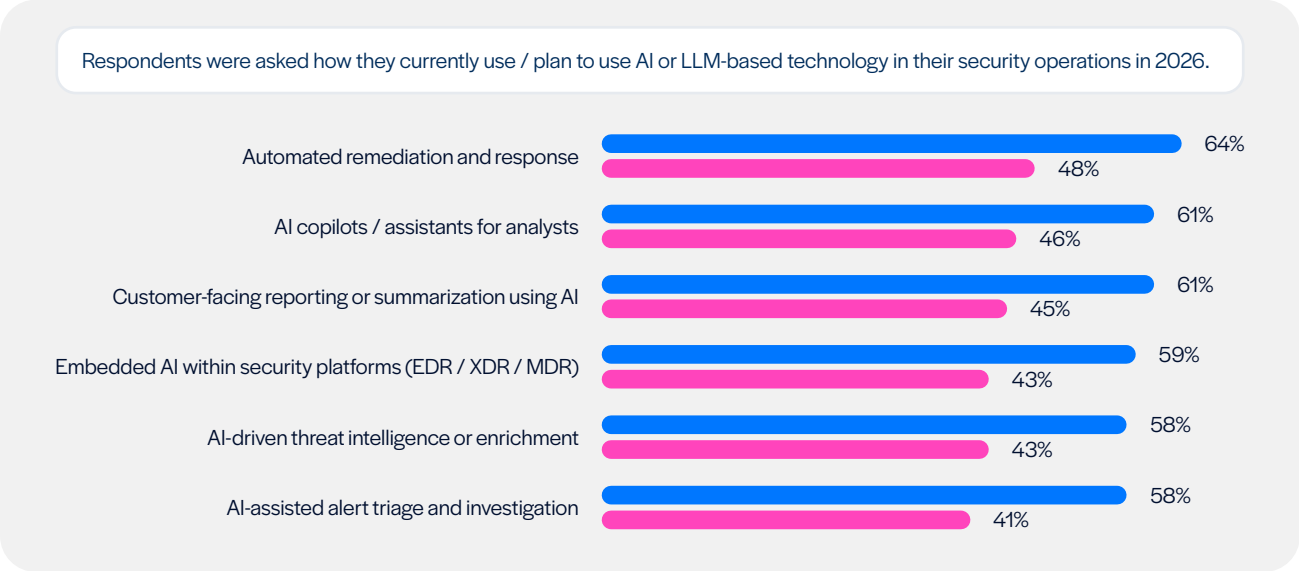
03 **Identity security**

AI Adoption Is No Longer Optional, but Hesitation Remains

The disparity in AI adoption rates between MSPs and in-house teams is notable. MSPs have higher rates of AI usage (60% on average) across every area compared to in-house teams (44% on average).

MSPs are at the forefront of AI adoption, with a significant portion already integrating AI technologies into their security operations. 51% have embedded AI within security platforms such as EDR, XDR, and MDR, 49% are using AI-assisted alert triage and investigation, and 56% have implemented automated remediation and response systems.

In-house teams are also making strides, but more slowly. While 53% of MSPs have already adopted AI copilots or assistants for analysts, in-house teams are still in the planning stages, with many expressing a desire to adopt these technologies in the near future.



No time to wait for AI adoption

Governments are issuing urgnet calls for AI adoption in both public and private sectors. In June 2026, the US government issued an executive order on AI innovation and security that leans on public-private collaboration to widen access to AI-enabled defensive tools and harden systems against fast-moving threats.[1]

Days later, the Five Eyes cyber agencies (the US, UK, Canada, Australia, and New Zealand) warned that frontier AI models are set to fundamentally transform both offensive and defensive cyber capabilities on a timeline of months, not years. Their message to private-sector leaders echoes our own data: success won't come from deploying more tools, but from integrating AI into security operations and getting the fundamentals right.[2]

1. https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/
2. https://www.cisa.gov/news-events/news/five-eyes-cyber-security-agencies-statement



Section 2:

The Current Threat Landscape

The most common incidents and their impact on MSPs and in-house teams.

MSPs Report Fewer Incidents Among Their Customers Than In-House Teams

Respondents from in-house teams were far more likely (60%) to experience or suspect incidents than MSPs noted among their customers (22% on average). This could suggest that those working with MSPs are better able to proactively prevent attacks before they occur. The in-house teams surveyed for this report include those who manage security themselves (29%), use a managed service provider (27%), and who operate a mixture of both (44%).

MSP respondents were asked what proportion of their customers, if any, have experienced a security or ransomware incident in the past 24 months.



In-house respondents were asked if their organization had experienced a security or ransomware incident in the past 24 months.



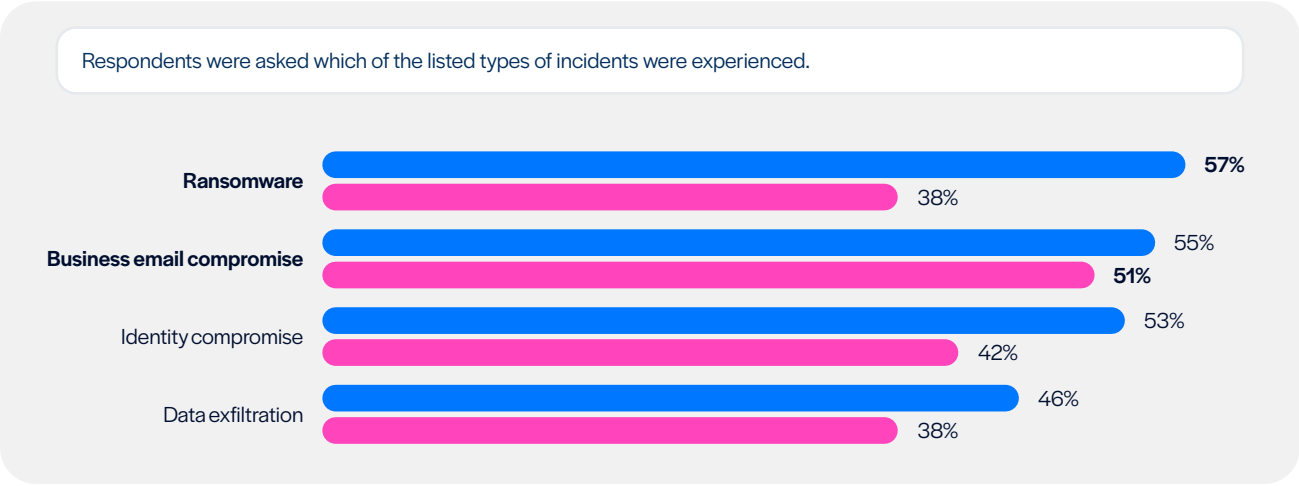
Spain, Italy, and Portugal see fewer incidents

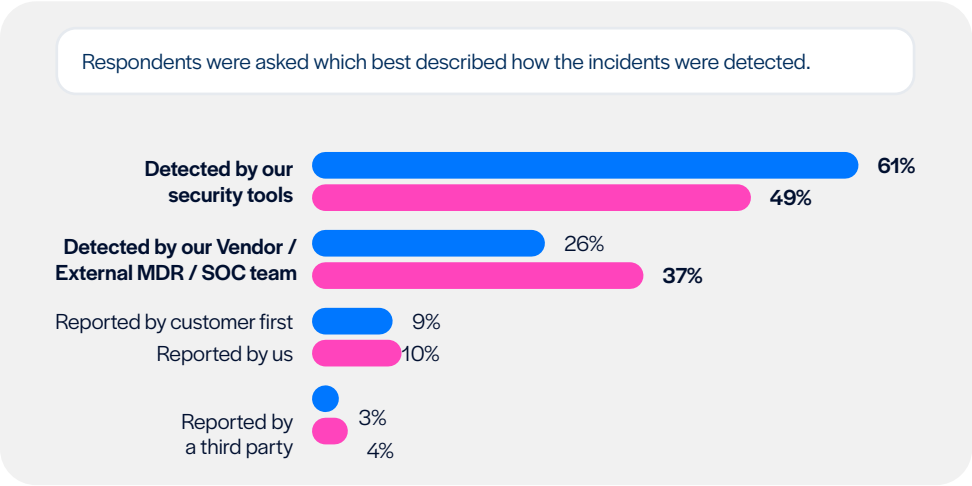
Southern Europe reports the fewest security incidents, across both in-house teams and MSPs. In-house teams in this region also report lower detection rates than others using their own security tools, suggesting reporting rates may not accurately reflect actual incident levels.

%	of in-house teams experiencing or suspecting incidents	%	of MSPs' customers experiencing incidents on average
69%	UK & Ireland	26%	North America
61%	North America	25%	Australia & New Zealand
58%	Australia & New Zealand	21%	UK & Ireland
49%	Southern Europe	16%	Southern Europe

MSPs Benefit From Experience With Diverse Threats and a Deeper Security Bench

MSPs, with their range of clients, breadth of services, and sector coverage, see a wider variety of incidents than in-house teams. **Ransomware is the most common incident MSPs deal with, versus business email compromise (BEC) for in-house teams.**





Nearly two-thirds (61%) of MSPs detected threats using their own security tools, compared to under half (49%) of in-house teams. Around a third (37%) of in-house teams were alerted to incidents by external cybersecurity partners.

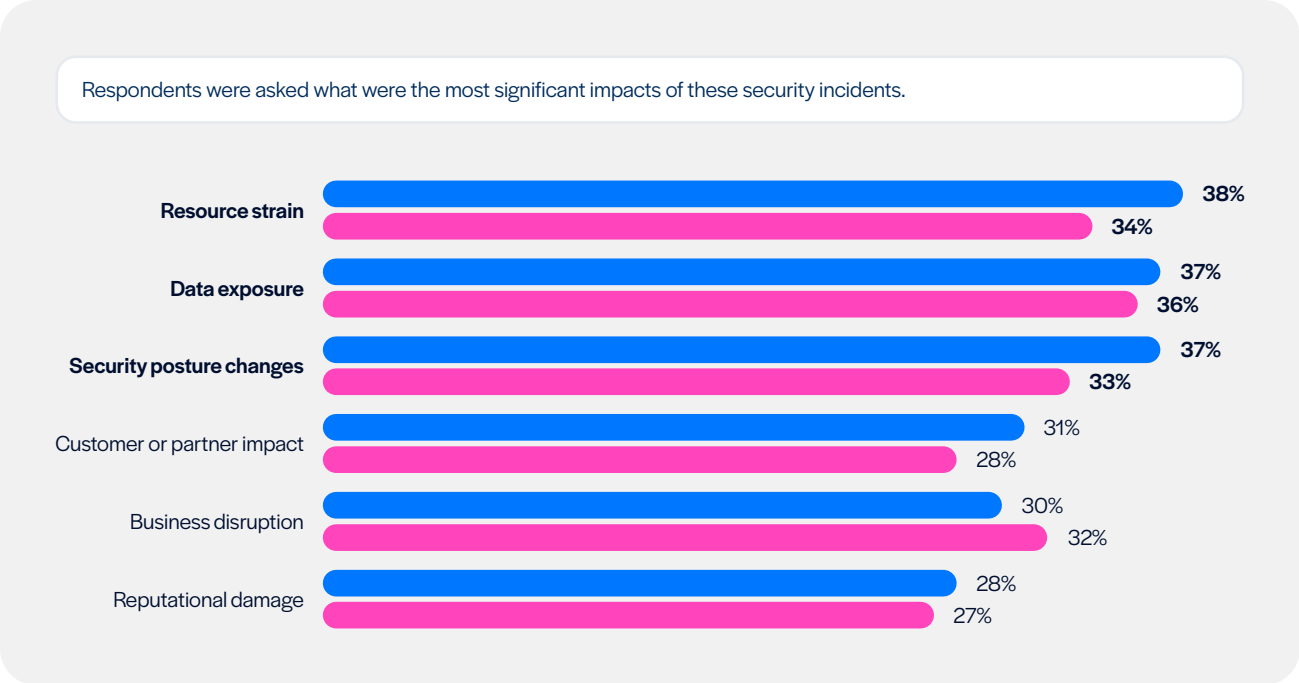
IT outpaces energy and utilities in cybersecurity capability

67% of those working in high-tech, IT or software firms were able to detect incidents using their own security tools. In contrast, only 34% of those working in retail, trade and eCommerce could say the same. Similarly, 57% of high-tech, IT or software companies describe their cybersecurity capability as mature, compared to just 30% in transportation and warehousing.

Incidents Add Pressure for Internal Resources

Strain on resources is one of the top impacts of security incidents both on MSPs and in-house teams. While in-house teams are constrained by fixed resources, MSPs can scale capacity up or down with more agility depending on client needs.

Both groups agree that data being exposed (#2) and changes in security postures (#3) are significant issues. For in-house teams, with internal resources already under pressure, the need to investigate and implement new tools or systems as security postures adapt to changing threats only compounds the problem.



44%

IN-HOUSE SECURITY TEAMS

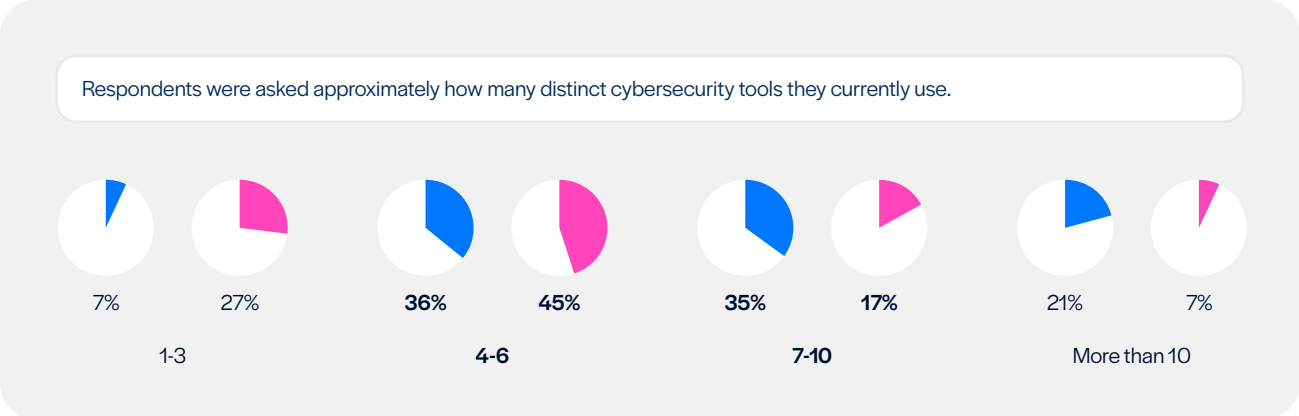
have 15+ members of dedicated cybersecurity staff, compared to just 14% of in-house teams

More incidents leads to higher security spend

Organizations that increased their security budget this year versus last year reported more security incidents than those that didn't.

MSPs Manage 60% More Cybersecurity Tools Than In-House Teams

In their efforts to handle a broad and growing range of incident types, **MSPs are using 8 security tools on average, compared to 5 used by in-house teams.**



Tackling the tools explosion

MSPs are deploying more tools in response to the variety of incidents faced by their customers. Paradoxically, however, more tools lead to more (often false) alerts, more fatigue, and more integration complexity. What's more, in the context of today's style of attacks – which are coordinated paths, rather than isolated events – point tools only see pieces while unified platforms see the entire attack chain. Unified security platforms support both efficiency and effectiveness – meaning MSPs no longer have to choose between breadth of coverage and depth of visibility.

78%

of organizations say tool sprawl hinders threat mitigation[1]

1. 2025 Barracuda Networks Survey

Key Takeaways

AI adoption as part of comprehensive security strategy is not optional, despite hesitation to adopt it. While internal teams negotiate with legal and GRC on policies and use cases, threat actors already leverage AI to create and accelerate attacks.

MSPs are uniquely positioned to help in-house IT and security teams prepare and respond to the explosion in AI-powered threats:

Nearly two-thirds (61%)

IN-HOUSE SECURITY TEAMS

will deliver agentic AI through an MSP or a hybrid model

57%

MSPs

are rolling out agentic AI as their top priority capability this year

71%

SMALL AND MID-SIZED BUSINESSES

already manage their cybersecurity through an MSP model

While running AI security in-house at an SMB will technically be possible in 2026 and beyond, strategically it will be hard to defend. MSPs have the delivery channel, are 13-16 percentage points ahead on every AI capability, and have the scale which most in-house teams lack.

The AI future of security is already here. The organizations that embrace it will own what comes next.

About Cynet

Cynet manages attack paths with AI. Our unified, AI-powered cybersecurity platform — purpose-built for security teams and delivered through a global partner network — predicts, sees, and disrupts the full attack chain across endpoints, identity, networks, email, cloud, mobile, and SaaS. Backed 24x7 by CyOps, our integrated AI SOC, Cynet reduces tool sprawl, alert fatigue, and response times so teams can focus on what matters most.

Learn more at **cynet.com**

About Sapio Research

Sapio Research is a Certified B Corp™ full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions. Their team of expert researchers deliver valuable insights to support their clients understand their audience, build powerful brands, and cut through the noise with compelling data-driven content.

For more information, visit **sapioresearch.com**