November 2025
White Paper
Sponsored by Microsoft Security

Using Agentic AI to Solve the Core Cybersecurity Problem: Time

Michelle Abraham
Senior Research Director,
Security and Trust, IDC

Frank Dickson
Group Vice President,
Security and Trust, IDC

Table of contents

Click any title to navigate directly to that page.

Introduction

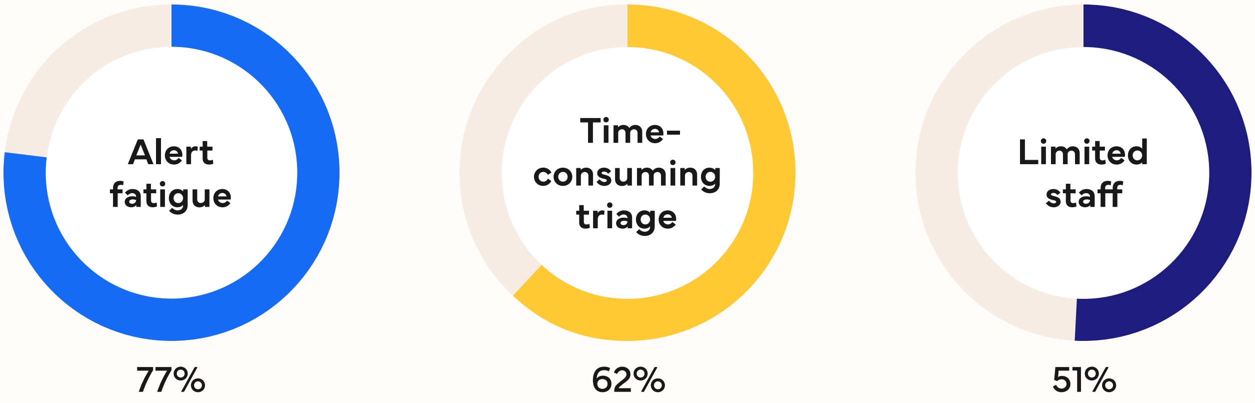
Building a resilient organization in today's digital landscape is a formidable challenge, shaped by a convergence of complex factors. Modern IT environments are increasingly hybrid and heterogeneous, introducing layers of complexity that can be difficult to manage. Organizations also face persistent staff shortages, an ever-expanding threat landscape, and a growing array of compliance regulations. Compounding these issues is the elevation of cyber-risk to a core business risk, making resilience not just a security and IT concern but a strategic imperative for the entire enterprise.

On a tactical level, those responsible for cybersecurity encounter a range of operational hurdles that complicate the task of securing digital assets. Common challenges include gaps in internal policies, the risk of missing emerging threats, and the repetition of manual tasks that strain limited human resources. Security teams often struggle with a lack of context in alerts, time-consuming triage processes, and alert fatigue, all of which can undermine their ability to respond effectively to incidents. These obstacles highlight the need for organizations to adopt more integrated and efficient approaches to cybersecurity to achieve true resilience. **Figure 1 (below)** presents the key cybersecurity challenges that respondents in a recent Microsoft-sponsored IDC survey reported.

Figure 1

Cybersecurity challenges

Across all security and IT workflows, what are your top challenges?



n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Although the specific challenges organizations face may differ, each is directly or indirectly connected to time constraints, the repetitive nature of cybersecurity tasks, and the limited temporal bandwidth of security teams. For example, alert fatigue becomes a significant problem only when there are not enough personnel available to address the volume of alerts generated. Similarly, time-consuming tasks pose a substantial issue when organizations lack the necessary headcount to efficiently perform the required work. These factors underscore how resource limitations amplify the impact of otherwise manageable operational challenges, making it essential for organizations to consider both staffing and process efficiency in their approaches to cybersecurity.

Time contraints that organizations face:

Phishing alert triage

13 mins. per alert

Insider risk alert investigations

18 mins. per investigation

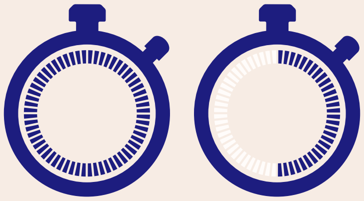
Sensitive data exposure alert research

22 mins. each

Conditional access reviews

35 mins. per request

Addressing vulnerabilities on Windows devices



90 mins. per patch

Notes: 363 respondents indicated user-reported phishing alerts are triaged, 277 respondents indicated insider risk alerts are reviewed, 288 respondents indicated sensitive data exposure alerts are triaged, 293 respondents indicated conditional access alerts are triaged, and 331 respondents indicated that vulnerabilities are patched by internal staff.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

Realistically, no organization is going to see dramatic increases in headcount. Even fully staffed organizations suffer from fatigue and burnout from the tedium of highly repetitive manual effort, which results in staff turnover and missed threats from high-volume tasks. The best-funded organizations struggle to keep pace with the growth of security tasks resulting from IT complexity and a changing threat environment. It is difficult to scale the number of people, so technology is necessary to scale the amount of work for which each person is responsible and the nature of the work. People are best suited for complex tasks, while AI is best suited for repetitive and mundane work.

The purpose of this paper is to show the average amount of time it takes for IT and security professionals to perform several highly repetitive yet important cybersecurity-oriented tasks, as well as how the automation of those tasks using agentic AI will dramatically increase the productivity of cybersecurity teams.

Methodology

Microsoft engaged IDC to survey IT and security professionals in the following countries:

Canada
U.S.
Norway
Sweden
Finland
U.K.
Denmark
Germany
France
U.A.E.
Saudi Arabia
India
Japan
Singapore
Australia
New Zealand

- Respondents were required to work for organizations with more than 500 employees.

- **Industries:**

Software and IT	15%
Energy	12%
Healthcare	11%
Financial services	10%
Retail	18%

with the remainder working across industries

- **Areas:**

IT management	26%
Cybersecurity	74%

- **Roles:**

Directors	38%
Managers	24%
Executives	20%

with some other middle management and C-level workers

The tactical and manual weight on cybersecurity team productivity

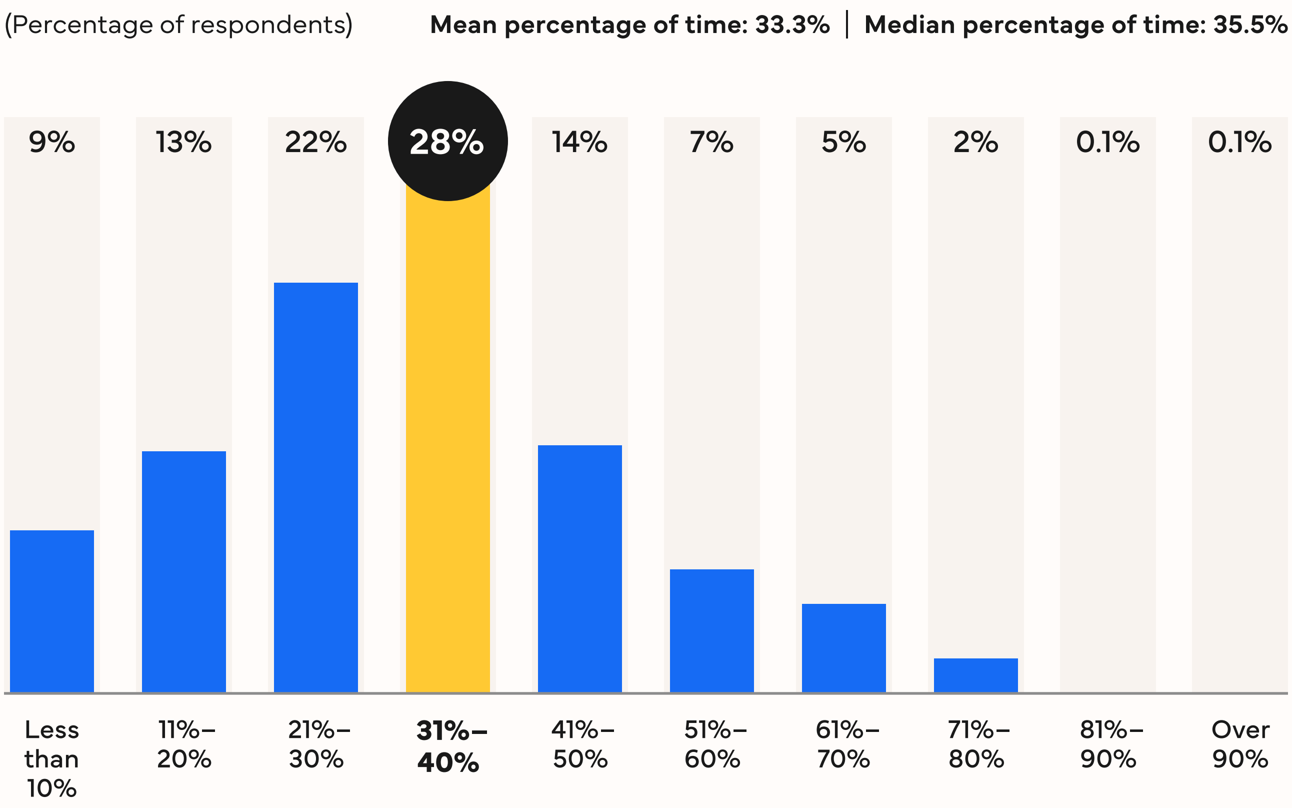
The struggle over time in cybersecurity continues to come back to people. Despite the sophistication of cybersecurity tools, IT and security professionals report that repetitive tasks require a large percentage of their time, 33% on average **(Figure 2, next page).**

Workers generally dislike repetitive, mundane tasks because these activities lack intellectual stimulation, which can lead to disengagement, fatigue, and burnout. The repetition of triaging alerts and the performance of routine compliance checks is often frustrating, especially when limited staffing means these tasks consume valuable time that could be spent on more strategic work. Organizations then don't have time to address complex challenges, making it important for organizations to automate or streamline these processes to maintain employee engagement and efficiency.

Figure 2

Time on repetitive tasks

What percentage of your time or your team's time is spent on repetitive tasks?



n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

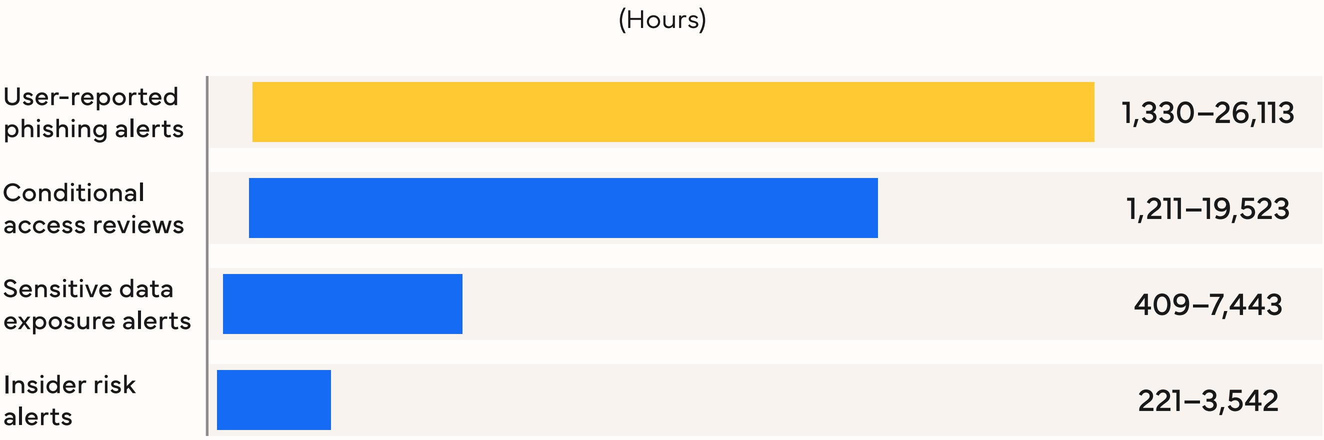
Over a year, the repetitive tasks add up to very real-time commitments. IDC asked the survey respondents about the time and resources spent on several cybersecurity tasks.

The number of alerts varied greatly by the size of the organization. Those with 500 to 999 employees were on the lower end of each of these figures, while those with over 10,000 employees were on the high end.

Figure 3

Hours spent per year

How much time does it take an internal person to review an alert?



Notes: 363 respondents indicated user-reported phishing alerts are triaged, 293 respondents indicated conditional access alerts, 288 respondents indicated sensitive data exposure alerts, and 277 respondents indicated insider risk alerts.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Respondents spent **1,330 to 26,113 hours** per year on phishing triage.

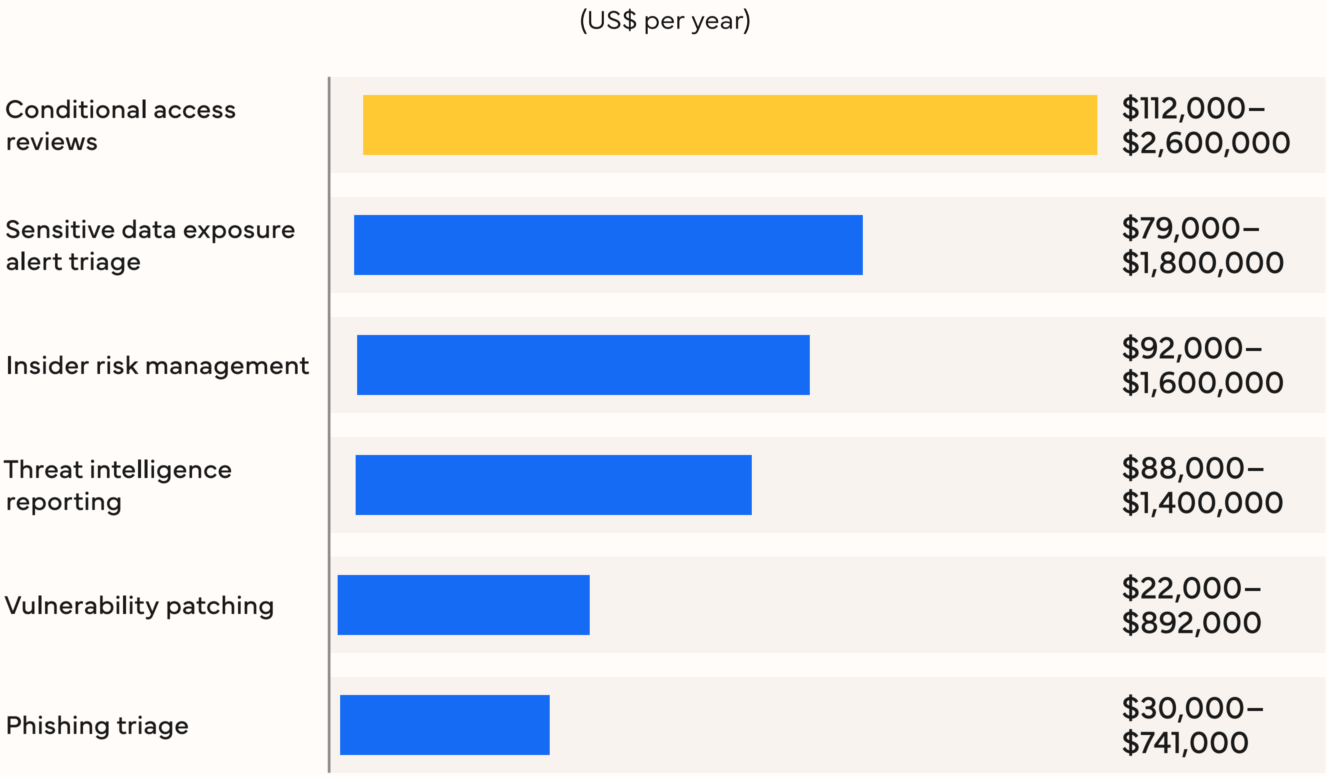
In many organizations, threat intelligence compilation must take place daily at a minimum, and 31.6% of organizations perform the task more than once a day.

Outsourcing can eliminate the time that internal human resources spend on tasks, but it requires spending on the external service, which can create large financial burdens, even if justified. **Figure 4 (below)** shows the amount that respondents reported spending on outsourcing these tasks.

Figure 4

Amount spent per year if tasks are outsourced

How much does an external third-party charge for alert review per month?



Notes: 177 respondents indicated conditional access alerts, 176 respondents indicated sensitive data exposure alerts, 174 respondents indicated insider risk alerts, 176 respondents indicated that organization specific threat reports need to be compiled, 167 respondents indicated that vulnerabilities are patched, and 177 respondents indicated user-reported phishing alerts are triaged by an external third party.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Dangerous gaps in security coverage

Time constraints often force staff to prioritize urgent tasks over strategic improvements, leaving gaps in defenses and compliance. As a result, organizations become more vulnerable to attacks and struggle to maintain effective, proactive cybersecurity programs.

Not having enough time limits cybersecurity teams' ability to thoroughly investigate alerts, patch vulnerabilities, and implement robust security measures, increasing the risk of missed threats and breaches. About one-third of alerts in the following categories go uninvestigated **(Figure 5, next page).**

Figure 5

Alerts investigated and uninvestigated per week

How many alerts does your team investigate each week, and how many go uninvestigated, regardless of the severity?

Alert types	Total alerts	Percentage left uninvestigated
User-reported phishing alerts	1,460	31%
Sensitive data exposure alerts	217	36%
Insider risk alerts	157	38%

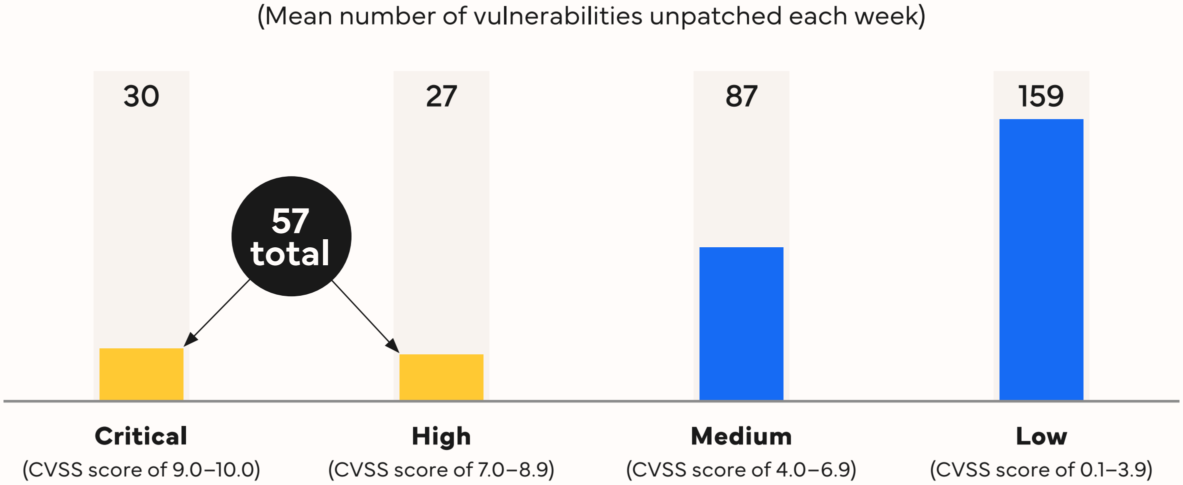
Notes: 436 respondents indicated user-reported phishing alerts are triaged, 403 respondents indicated sensitive data exposure alerts are triaged, and 381 respondents indicated insider risk alerts are triaged.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

The situation is similar with regard to patching vulnerabilities. On average, 57 critical and high vulnerabilities remain unpatched each week, with the widest variation on critical vulnerabilities depending on the size of the organization **(Figure 6, below).**

Figure 6

Unpatched vulnerabilities

How many vulnerabilities on your actively managed Windows devices go unpatched each week?



n = 498, respondents indicated that vulnerabilities are patched by internal staff/external third party;
Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

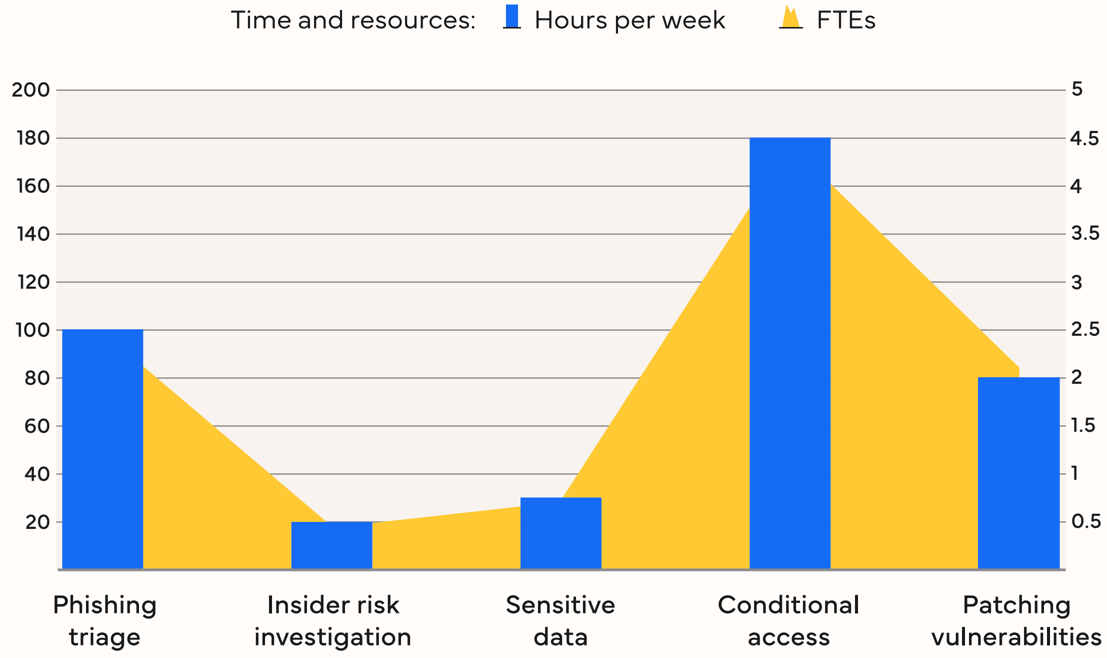
The cost of addressing 100% of these issues is exorbitant for many organizations and would require many more hours. Completing it would only be possible with additional FTEs **(Figure 7, below).**

Figure 7

Time and resources to do the work left undone

How much time does it take an internal person to review an alert?

See the figure data in an accessible table format.



Notes: 363 respondents indicated user-reported phishing alerts are triaged, 277 respondents indicated insider risk alerts are investigated, 288 respondents indicated sensitive data exposure alerts are triaged, 293 respondents indicated conditional access alerts are reviewed, and 331 respondents indicated that vulnerabilities are patched by internal staff.
FTE calculated based on number of hours. 1 FTE = 8 hours.
n = 711 ; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Concern over the impact of these gaps

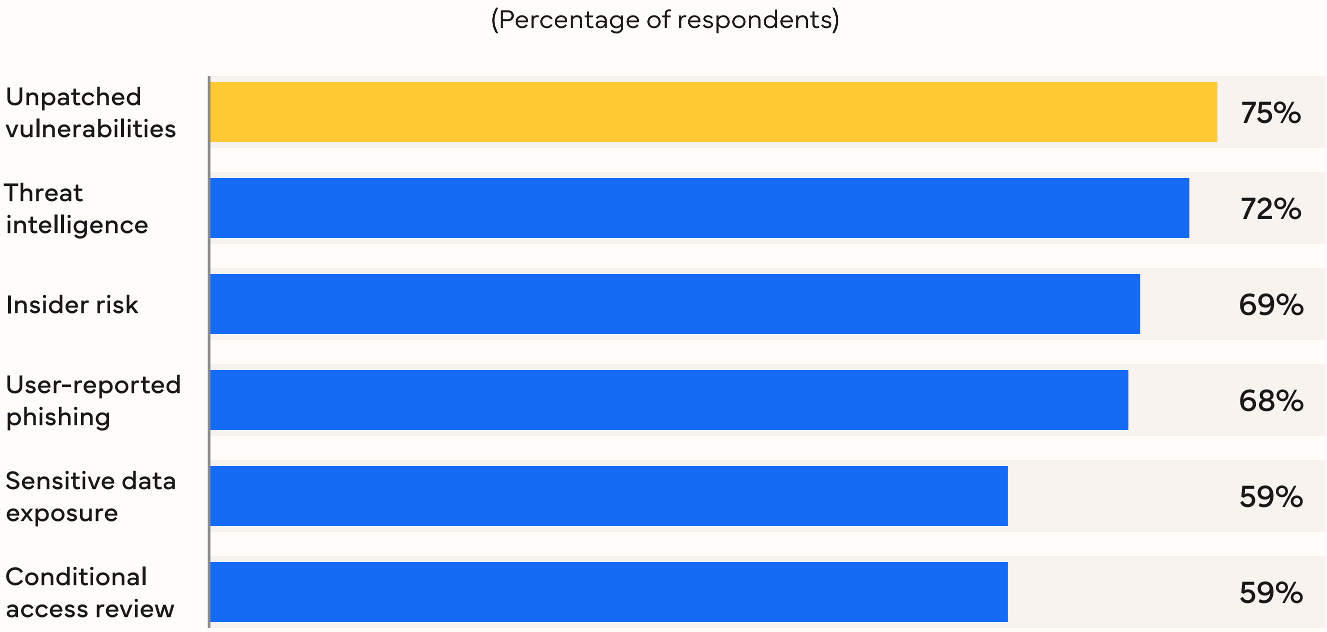
IT and security professionals are deeply concerned about gaps in their defenses because missed alerts and unpatched vulnerabilities can expose organizations to significant risks and operational disruptions.

The rapid expansion of attack surfaces and shortages of skilled security talent compound these issues. Many organizations also struggle with limited visibility, which hinders their ability to detect and respond to threats effectively. These gaps are not just technical issues; they represent business risks that can lead to data loss, reputational damage, and financial impact if attackers exploit them. The complexity of modern IT environments, especially with the integration of operational technology, the Internet of Things, and legacy systems, increases the likelihood of gaps in security protocols and compliance, making organizations more susceptible to targeted attacks such as ransomware and data manipulation.

Figure 8

Worry over the undone work

How worried are you about the risk of a breach from these unaddressed threats?



Notes: 498 respondents indicated that vulnerabilities are patched by internal staff/external third party, 384 respondents indicated specific threat reports are compiled, 451 respondents indicated insider risk alerts, 540 respondents indicated user-reported phishing alerts are triaged, 464 respondents indicated sensitive data exposure alerts, and 470 respondents indicated conditional access alerts.
The chart shows the percentage of those who were somewhat worried (1) and very worried (2).
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

According to the survey data, the greatest worry concerns unpatched vulnerabilities — 72% of respondents reported being worried that they are missing important threat intelligence that should be used to underpin the prioritization of tasks that IT and security teams perform. Respondents also reported being somewhat or very worried that the current frequency/thoroughness of their conditional access reviews is creating deficiencies that will need to be dealt with during the next audit.

> “The conditional access policies are the fundamentals of our security backbone.”

The concern over gaps in defenses is also reflected in the need for the continuous assessment and improvement of cybersecurity programs. Simply installing the latest security tools is not enough; organizations must conduct deeper inspections and regular risk or compliance assessments to uncover unknown exposures and noncompliance that attackers can exploit. The ongoing race between attackers and defenders means that organizations must maintain a consistent, methodical approach to inspecting the depth and breadth of their cybersecurity controls. Ultimately, security and IT professionals recognize that these gaps are not just technical shortcomings but strategic vulnerabilities that require a combination of skilled staff, effective processes, and advanced technologies to address. However, finding the time to think through and make adjustments to their strategies takes a back seat to alert triage.

Agentic AI: A new model for cybersecurity automation

With the emergence of generative AI, AI chatbots and AI assistants have become prevalent in cybersecurity products.

These AI assistants are very useful for asking questions in natural language and summarizing information, which saves time and avoids the need to perform mundane tasks. Now the industry is looking to use AI for more complex workflows with AI agents that can make decisions dynamically.

Unlike traditional security tools, AI agents can analyze vast amounts of data in real time, identifying patterns and anomalies that may indicate cyberthreats such as malware, phishing, or insider attacks. Their ability to learn from historical incidents and adapt to evolving attack techniques enables organizations to detect sophisticated threats that might otherwise go unnoticed. By automating routine tasks such as alert triage, vulnerability scanning, and incident response, AI agents reduce the burden on human analysts, allowing them to focus on more complex and strategic security challenges.

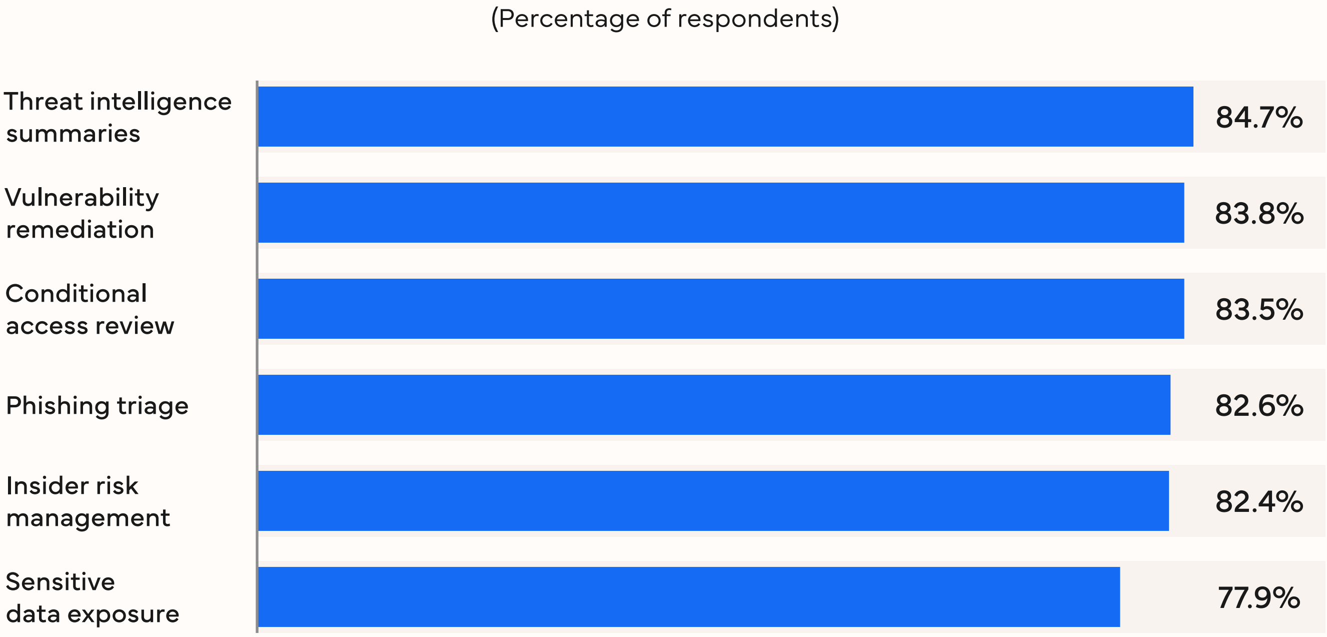
Additionally, AI agents improve the speed and accuracy of cybersecurity operations, helping organizations respond to threats faster and with greater precision. They can correlate data from multiple sources, including network traffic, endpoint activity, and user behavior, to provide contextual insights and prioritize risks based on potential impact. This not only minimizes false positives and alert fatigue but also supports compliance efforts by continuously monitoring for policy violations and unauthorized access. As cyberthreats become more advanced and attack surfaces expand, the scalability and adaptability of AI agents make them essential for maintaining robust, proactive security in dynamic digital environments. IT and security professionals see the benefits of AI agents for some of their most common and boring tasks **(Figure 9, below).**

> “The job is less tiring. That’s what I would say.”

Figure 9

The appeal of AI agents for specific tasks

Please rate the appeal of having AI agents address the following use cases with supervised autonomy.



Note: The chart shows the percentage of those who found AI very appealing (1) and appealing (2).
n = 711; Source: IDC’s *Agentic AI Cybersecurity Use Case Survey*, August 2025

Measurable impact of agentic AI

Cybersecurity organizations that use agentic AI in their daily operations have found measurable improvements with clear time savings by automating and accelerating critical security processes.

AI agents now efficiently handle tasks that once consumed significant resources, such as phishing triage, which can be reduced from 30 minutes to just three, and the instant generation of threat reports. These technologies also automatically detect conditional access gaps, allowing security teams to focus on higher-value activities rather than routine monitoring and manual analysis.

> “It’s like insurance. You don’t know how much it saves until it saves you.”

Regarding phishing triage, *"...an analyst ends up spending at least 30 minutes to see what is going on ... That's the minimum I'm talking about ... go through the Microsoft security portal, go to the threat explorer, search for that email, and then you know and also look at the headers, look at the verdicts ... and then after that, how many people have received, you run the report, how many people have clicked and open you run that report. It takes around 30 minutes at least per email."*

> With regard to the agent, "...all that runs around two to three minutes; it depends on how many people have received it."

> Agentic AI is as bad as it's ever going to be today. It's only going to get better."

Beyond efficiency, AI enhances security outcomes and workforce enablement. Organizations benefit from faster patching of zero-day vulnerabilities, reduced human error, and improved policy coverage, which collectively increase confidence in system configurations and audit readiness. AI also improves job satisfaction and reduces cognitive load for security and IT professionals, enabling junior staff to perform better under senior oversight and empowering non-security IT professionals to triage simple security tasks. This broadens the organization's security capabilities and fosters a more resilient, collaborative approach to cyberdefense.

Agentic AI is as bad as it's ever going to be today. It's only going to get better."

Return to table of contents

Trust, oversight, and governance

User trust in agentic AI is evolving, but it remains a complex and nuanced issue shaped by concerns over security, transparency, compliance, and operational reliability. Trust is not automatic.

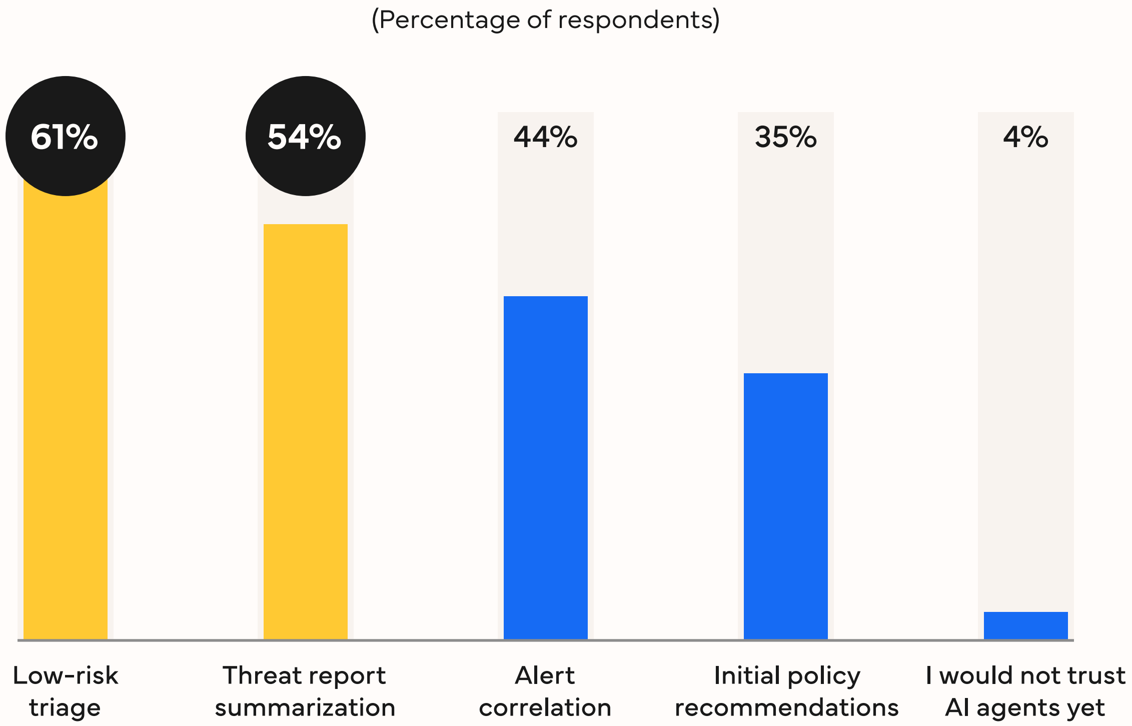
The top concerns include security issues resulting from autonomous actions, data privacy breaches, lack of transparency, and the risk of unintended consequences. While most respondents trust AI for low-risk tasks such as threat report summarization and low-risk triage, alert correlation and policy recommendations received lower marks **(Figure 10, next page).** Implementing policies incorrectly can cause systems to shut down because they cannot talk to each other.

> “I would trust a junior person to use it — but we still need the seniors.”

Figure 10

Trusted tasks for AI agents

In which areas would you trust (or find value in) an AI agent to handle the tasks autonomously?



Note: Multiple dichotomous table — total will not sum to 100%.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

These worries around agents are reflected in procurement criteria: Buyers prioritize security, compliance, and integration capabilities above speed or technical features, and demand auditability, explainability, and human override are core requirements. They are emphasizing the embedding of responsible AI frameworks, continuous monitoring, and human-in-the-loop mechanisms to ensure oversight.

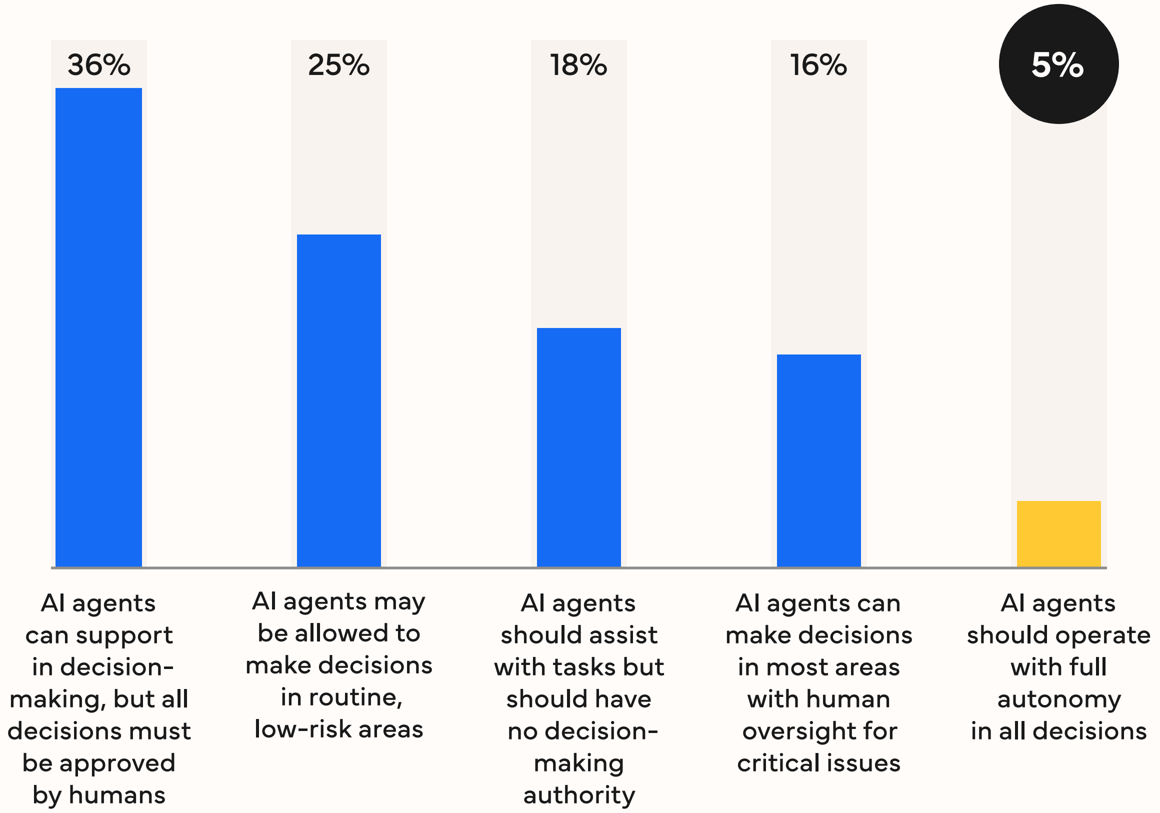
While trust for some tasks is high **(Figure 9, next page),** only 5.2% believe that AI agents should have full autonomy. The greatest number of respondents, 36%, support supervised autonomy in all areas, while 25% trust agents in low-risk or routine decisions only.

Figure 11

Views of AI agent autonomy

Which best represents your view of using agentic AI for cybersecurity use cases within your organization?

(Percentage of respondents)



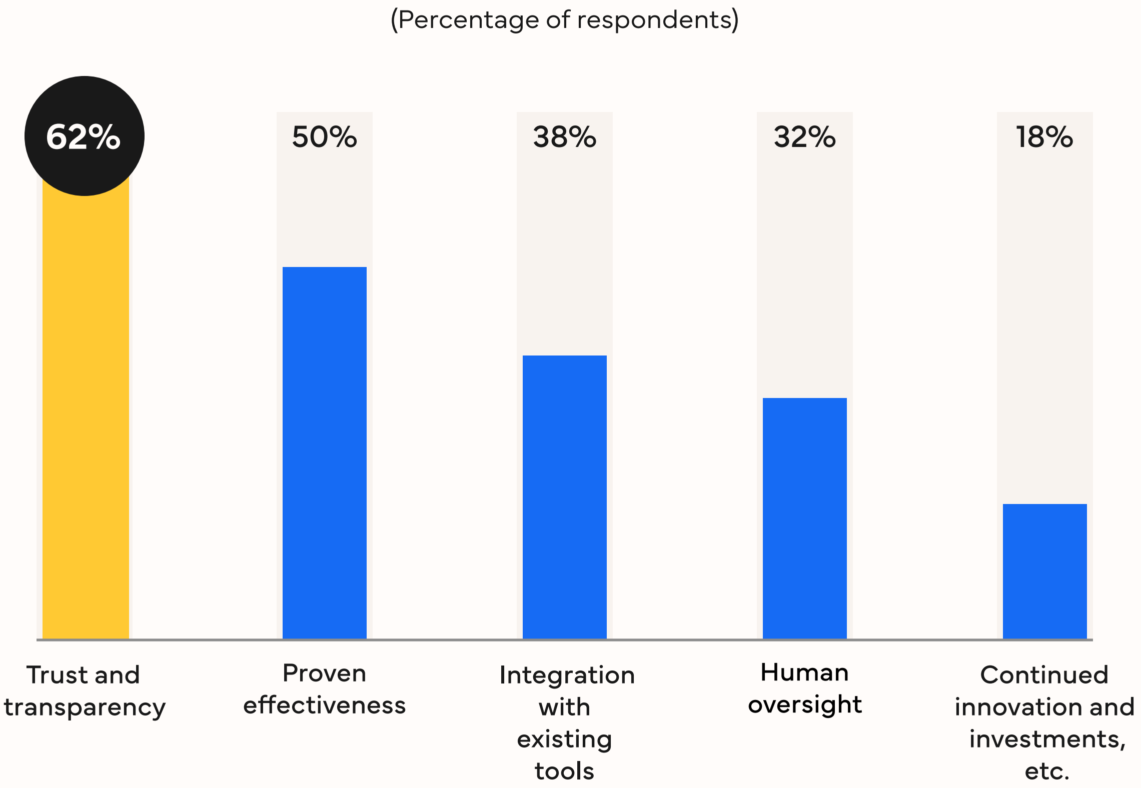
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

Unsurprisingly, trust and transparency lead the list of considerations when selecting AI agents, followed by proven effectiveness **(Figure 12, next page).** Autonomous systems can make impactful decisions that affect business operations, regulatory compliance, and ethical standards. Trust ensures that AI agents act reliably and securely, while transparency allows organizations to understand and oversee decision-making, reducing fears of "black box" outcomes and unintended risks. Proven effectiveness, demonstrated through rigorous validation and real-world success, reassures users that AI agents will deliver accurate and fair results.

Figure 12

Most important items for an AI security agent

Which qualities are most important when evaluating AI security agents?



n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Strategic recommendations

Prioritize high-impact use cases such as phishing triage and conditional access reviews, focusing on areas with significant time and cost burdens to maximize the benefits of AI agents in cybersecurity.

Building robust governance frameworks is essential, including clearly defining agent roles, permissions, and approval workflows, as well as ensuring auditability and transparency.

Monitor and measure ROI by tracking metrics such as time saved, alerts investigated, and breach prevention, using these data points to justify further expansion and investment in AI-driven security solutions.

Return to table of contents

Conclusion

In today's cybersecurity environment, organizations face a range of persistent challenges, including the complexity of hybrid IT infrastructures, expanding threat landscapes, staff shortages, and the elevation of cyber-risk to a core business concern.

These issues are closely linked to time constraints and the limited temporal bandwidth of security teams, which can lead to gaps in defenses, alert fatigue, and operational inefficiencies. The repetitive nature of many cybersecurity tasks compounds these problems, reducing productivity and hindering the ability to address complex threats and compliance requirements.

IT and security professionals spend an average of 33% of their time on manual, low-value activities. Critical tasks such as phishing triage, insider risk investigations, and vulnerability patching consume thousands of hours annually, and significant portions of alerts — up to 51% in some categories — go uninvestigated due to resource limitations, while outsourcing these tasks is costly.

33%
of IT and security professionals' time, on average, is spent on manual, low-value activities.

Time and resource constraints create dangerous gaps in security coverage, increasing the risk of breaches, data loss, and compliance failures. Most respondents express deep concern over unpatched vulnerabilities and uninvestigated alerts, recognizing these as strategic business risks rather than mere technical issues.

Agentic AI offers a scalable and transformative solution to these challenges by automating routine processes, accelerating threat detection and response, and enabling more effective use of limited human resources. Unlike traditional tools or basic AI assistants, agentic AI can handle complex, repetitive tasks with supervised autonomy, dramatically reducing the time required for activities such as phishing triage and threat intelligence reporting. Early adopters report measurable improvements in productivity, faster incident response, and enhanced job satisfaction among security staff. AI agents also enable organizations to scale their security operations without proportional increases in headcount, empowering teams to focus on higher-value, strategic work.

By strategically prioritizing high-impact use cases such as phishing triage and conditional access reviews, organizations can target areas with the greatest time and cost burdens. Building robust governance frameworks, clearly defining agent roles and permissions, and ensuring auditability and transparency are essential steps for successful adoption. Integration with existing security tools and cross-agent orchestration further enhance the effectiveness of AI-driven security operations.

However, trust, oversight, and governance remain paramount. While there is strong support for supervised autonomy, only a small minority favors full AI autonomy. Security, compliance, transparency, and human-in-the-loop controls are top priorities for organizations evaluating AI agents. Responsible AI frameworks, continuous monitoring, and robust integration with existing security infrastructure are essential for successful adoption.

Ultimately, organizations that embrace agentic AI and monitor its impact through metrics such as time saved, alerts investigated, and breach prevention will be better positioned to reduce risk and empower their teams. This approach not only strengthens security outcomes but also improves job satisfaction and enables junior and non-security staff to contribute more effectively. As cyberthreats continue to evolve, scaling security with agentic AI allows organizations to reclaim valuable time, adapt to new challenges, and build resilience in an increasingly digital and dynamic landscape. ●

Appendix A: Supplemental data

Respondents spent 1,330 to 26,113 hours per year on phishing triage **(Table 1, below).**

Table 1

Time taken to triage user-reported phishing

Phishing triage	Amount
Alerts per week	117–2,300 alerts
Triage time per alert	13.1 minutes
Total hours per week	**26–502 hours**

Note: 363 respondents indicated user-reported phishing alerts are triaged.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Respondents spend 221 to 3,542 hours per year on insider risk alert triage **(Table 2, below).**

Table 2

Time taken to triage insider risk

Risk alert triage	Amount
Alerts per week	14–225 alerts
Triage time per alert	18.2 minutes
Total hours per week	**4–68 hours**

Note: 277 respondents indicated insider risk alerts.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Appendix A: Supplemental data (continued)

Alerts about sensitive data exposure take between 409 and 7,443 hours per year to triage **(Table 3, below).**

Table 3

Time taken to review sensitive data exposure alerts

Sensitive data exposure triage	Amount
Alerts per week	21–394 alerts
Triage time per alert	21.8 minutes
Total hours per week	**8–143 hours**

Note: 288 respondents indicated sensitive data exposure alerts are triaged.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

Conditional access reviews take organizations between 1,211 and 19,523 hours per year, according to respondents **(Table 4, below).**

Table 4

Time taken to review conditional access alerts

Condition access reviews	Amount
Reviewed per week	40–642 reviews
Time per review	35.1 minutes
Total hours per week	**23–375 hours**

Note: 293 respondents indicated conditional access alerts are reviewed.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

Appendix A: Supplemental data (continued)

Table 5

Frequency of compiling and disseminating threat intelligence reports

Threat intelligence compilation	Percentage
More than once per day	31.6%
Daily	36.2%
Every other day	12.2%
Weekly	19.8%
Monthly or longer	9.9%

Note: 384 respondents indicated conditional access alert.
n = 711; Source: IDC's *Agentic AI Cybersecurity Use Case Survey*, August 2025

Return to table of contents

Appendix B: Accessible data tables

This appendix provides an accessible version of the data for any complex figures in this document. Click "Return to figure" to get back to the original figure.

Figure 7
Time and resources to do the work left undone

Alerts	Hours per week	FTEs
Phishing triage	99	2.50
Insider risk investigation	18	0.50
Sensitive data	29	0.75
Conditional access	177	4.50
Patching vulnerabilities	84	2.00

Notes: 363 respondents indicated user-reported phishing alerts are triaged, 277 respondents indicated insider risk alerts are reviewed, 288 respondents indicated sensitive data exposure alerts are triaged, 293 respondents indicated conditional access alerts are reviewed, and 331 respondents indicated that vulnerabilities are patched by internal staff.
FTE calculated based on number of hours. 1 FTE = 8 hours;
n = 711 ; Source: IDC's *Agentic AI Cybersecurity Use Case Survey,* August 2025

Return to figure

About the IDC analysts

Michelle Abraham

Senior Research Director, Security and Trust, IDC

Michelle Abraham is a senior research director in IDC's Security and Trust Group and is responsible for the Security Information and Event Management, Exposure Management, and Related Artificial Intelligence Technologies practice. Abraham's core research coverage includes SIEM platforms, exposure management platforms, attack surface management, breach-and-attack simulation, cybersecurity asset management, and device vulnerability management alongside AI-related security topics.

More about Michelle Abraham →

Frank Dickson

Group Vice President, Security and Trust, IDC

Frank Dickson is the group vice president for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of AI security; cybersecurity services; information and data security; endpoint security; trust; governance, risk, and compliance; identity and digital trust; network security; privacy and legal tech; and application security and fraud. Topically, he provides thought leadership and guidance for clients on a wide range of security topics, including ransomware and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson →

Message from the sponsor

Microsoft Security

Microsoft Security provides an AI-first, end-to-end security platform designed to protect people, data, and infrastructure.

Built on decades of threat intelligence and global scale, the platform delivers comprehensive protection across identity, endpoints, cloud, and data. Security Copilot brings generative AI into the workflow, helping defenders investigate incidents faster, reduce response times, and strengthen resilience. With integrated solutions and continuous innovation, Microsoft Security enables organizations to manage complexity and stay ahead of evolving threats.

Learn more about how Microsoft Security and Copilot can help your organization strengthen its security posture.

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies.

This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC

idc.com | in @idc | 𝕏 @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.