Voice of Security

2026 REPORT

THE INTELLIGENT WORKFLOW PLATFORM

2026 Report

Voice of Security

Contents

3 Introduction

4 Key findings

5 Methodology

7 Security's rising influence

14 AI and governance become core

20 Manual work persists

26 Optimisim about AI's impact on security careers

34 The intelligent workflow gap

40 2026 strategy checklist

42 The future of security

Thomas Kinsella

Co-Founder and CCO, Tines

Security is entering a new chapter. AI and automation are reshaping how security teams operate, but the core pressures of the job haven't gone away. Even as AI adoption grows, risk is rising, workloads continue to climb, and teams still lose time to manual, repetitive tasks that could be spent on more strategic work.

AI is also expanding the threat landscape. Data leakage, shadow AI, and prompt injection are top concerns, and emerging policies and regulations are making governance more complex.

What I'm most excited about is the momentum. AI is already supporting key security use cases, from threat detection to compliance and identity and access monitoring. Half of organizations now have formal and active AI policies, with many more making steady progress. 86% of respondents are optimistic about the impact AI will have on their careers, and 87% say board-level attention to cybersecurity is rising.

At the same time, the skills required to thrive are shifting fast. AI literacy and prompt engineering now rank as the most important skills for security teams, a requirement that barely existed two years ago.

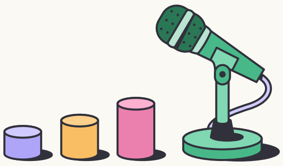
But there are still barriers to unlocking real value from AI and automation. Security and compliance concerns top the list, followed by budget constraints, integration gaps, and legacy systems. These realities help explain why AI adoption hasn't yet translated into meaningful reductions in manual work. It's perhaps no surprise that 92% of respondents say an intelligent workflow platform would be very or extremely valuable in helping them manage this complexity.

Before Tines, I spent more than a decade as a security operator. I know how hard it is to balance limited resources with rising risk and expectations. That's why this research matters to me. This is our largest survey to date, with responses from more than 1,800 security leaders and practitioners worldwide. It explores how teams are adapting to AI, where they feel pressure, and how their roles are evolving.

The opportunity ahead is significant for teams willing to move fast and responsibly. I hope these findings give you the clarity and confidence to navigate the year ahead.

Key findings

Here are a few of the insights we learned from the 1,800+ security professionals we surveyed:



#1

Security's strategic influence is growing, but there's still work to do

43% of respondents view their security function as a strategic enabler, and 87% report increased board-level attention to cybersecurity in the last year. But despite their increasing influence, 51% say it's extremely or very challenging to align security initiatives with broader business objectives, which may hinder their ability to deliver strategic impact.

#2

AI and AI governance have become foundational to security work

99% of SOCs are now using AI. Half of organizations have formalized and active AI policies in place, with another 42% making progress. AI is viewed as "highly effective" for many critical tasks. But concerns about security and compliance remain the biggest barriers to effective automation, limiting teams' ability to scale impact.

#3

Manual work remains high, even as AI adoption accelerates

81% say security workloads increased in 2025. Despite the rise of AI and automation, teams still spend on average 44% of their time on manual or repetitive work that could be automated. 76% experienced burnout, with heavy workloads cited as the main cause.

#4

Security teams feel optimistic about AI's impact on their careers

86% feel optimistic that AI will create new opportunities in the security job market, and 81% say their team is prepared to hire or reskill for new AI-related roles. AI literacy and prompt engineering are the top new skills for security professionals in 2026, underlining a fundamental shift towards AI-driven ways of working.

#5

Security teams want intelligent workflows to close the gap

92% rate an intelligent workflow platform as extremely or very valuable. Security teams anticipate a range of advantages from intelligent workflows, including higher productivity (48%), faster response times (41%), and better data accuracy (40%), which will help them overcome resource constraints and scale their operations securely, reliably, and effectively.

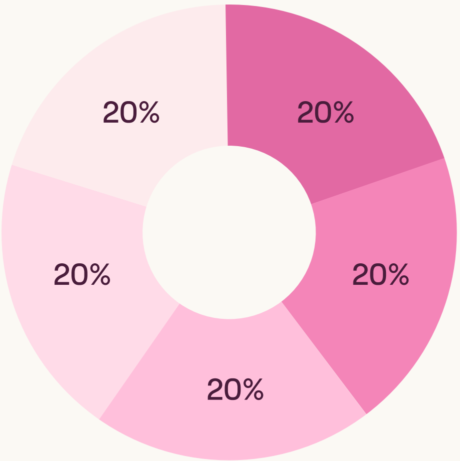
Methodology and participant demographics

Tines commissioned an independent research agency, Sapio Research, to survey 1,813 IT security and cybersecurity professionals across a range of sectors and global locations. At an overall level, results are accurate to ± 2.3% at 95% confidence limits assuming a result of 50%.

Note: Due to rounding, percentages may not add up to 100% throughout.

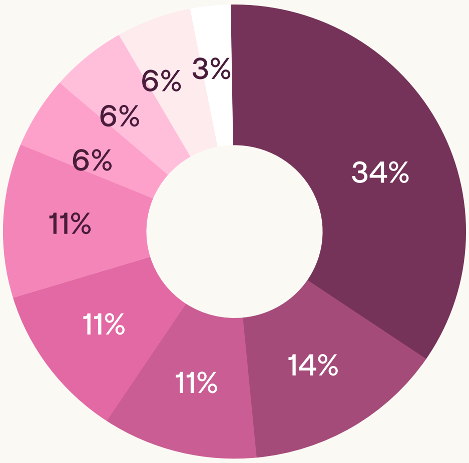
Business size (number of employees)

- ● 250–499
- ● 500–999
- ● 1,000–4,999
- ● 5,000–9,999
- ● 10,000+

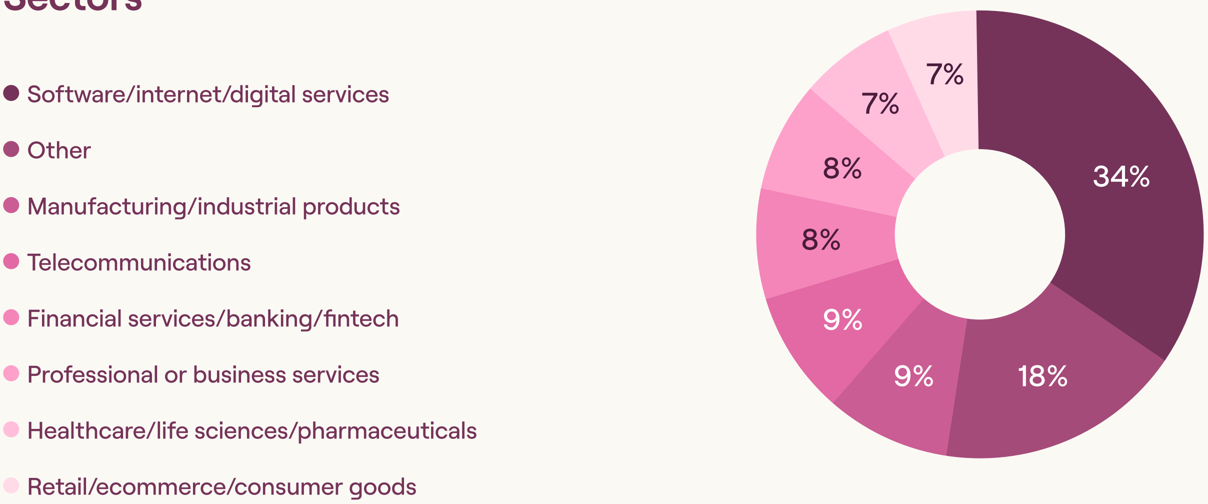


Location

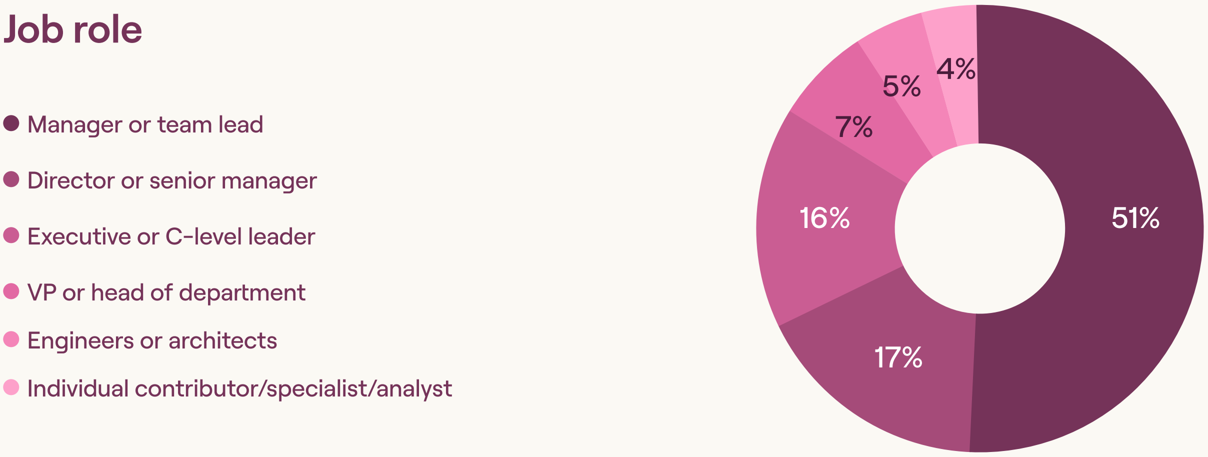
- ● US
- ● UK
- ● Germany
- ● Australia and New Zealand
- ● Sweden
- ● Canada
- ● Belgium
- ● Netherlands
- ● Ireland



Sectors



Job role



- 50% of respondents focus mainly on strategy, governance, and leadership across security or risk functions (leaders)
- 50% of respondents focus mainly on operational, analytical, or technical execution (practitioners)

1

Security's rising influence

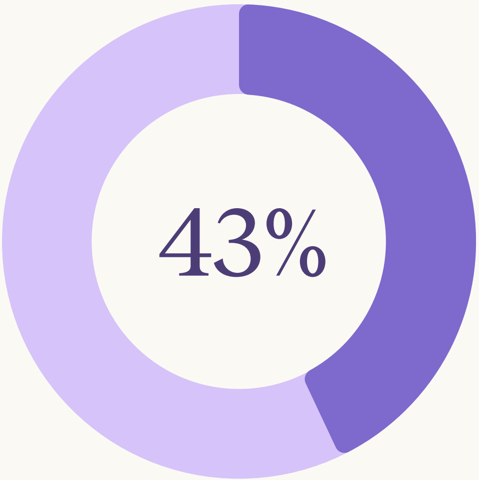
Security has long been treated as an operational necessity rather than a strategic capability. That's starting to change, but there's still work to do. Organizations increasingly recognize security's role in protecting customer trust and fostering business resilience, yet several barriers continue to limit its strategic influence.

Today, almost half of security teams say their function is viewed as a strategic enabler.

Execs are paying attention, with the vast majority of respondents (87%) reporting that board-level attention to cybersecurity has increased over the past year. This is especially notable in the US, where almost half (48%) say board-level attention has increased significantly.

43% of respondents say their security function is viewed as a strategic enabler within their organization

- ● 37% say they're viewed as a support function
- ● 19% say they're viewed as a cost center



87%

of respondents say board-level attention to cybersecurity has increased over the past 12 months

48%

of respondents in the US say board-level attention has increased significantly – the highest globally

Greater visibility hasn’t translated into alignment

Increased board-level attention reflects a rapidly intensifying risk environment. Almost three-quarters of respondents (73%) believe a significant cybersecurity incident is likely in the next 12 months, with 52% of US-based respondents believing it’s highly likely.

Increased attention doesn’t automatically translate to alignment, however. Many teams still struggle to connect security priorities to broader business objectives, with 52% rating it as highly challenging.

Senior decision-makers point to barriers like competing business versus risk goals, difficulty communicating value, limited visibility into risk or impact, resource constraints, and shifting business priorities. Worryingly, more than one in four (28%) security leaders feel like leadership sees security as a blocker.

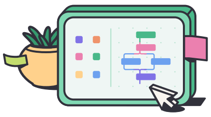
What are the biggest barriers preventing stronger alignment between security and business leadership, according to senior security leaders?

34%	Competing business vs. risk goals
32%	Hard to communicate security value
32%	Limited visibility into risk or impact
31%	Resource constraints
31%	Changing business priorities

Practitioners say they're held back from aligning with broader business goals by frequent priority changes and slow or rigid processes. They also point to burnout and too much manual work as obstacles.

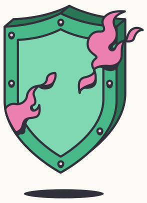
What are the biggest challenges that make it harder for their team's work to align with wider business goals, according to practitioners?

35%	Frequent priority changes
29%	Slow or rigid processes
29%	Hard to explain technical work
27%	Team burnout or low morale
26%	Limited visibility into business goals



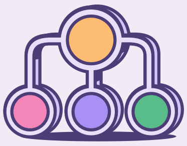
24% of security practitioners say too much manual work prevents them from aligning with wider business goals

Lean security teams are expected to focus on a wide range of issues, with priorities spread equally across multiple infosec domains. The flat distribution of senior security leader priorities for 2026 reinforces this tension.



What are senior security leaders' top priorities for 2026?

41%	Strengthen cloud and data security
33%	Enhance data privacy and protection (e.g. GDPR, CCPA)
32%	Enhance threat detection and response capabilities
31%	Establish clear AI policy and governance frameworks
25%	Improve incident response and recovery readiness



1 in 5 senior security leaders say increasing automation and orchestration is a top priority for 2026

Juggling multiple equally important demands, rather than executing a narrow roadmap, also makes it harder for security teams to prove impact.

Currently, security performance is evaluated through a mix of budget management, compliance outcomes, training effectiveness, and incident-related measurements.

Top metrics tracked to measure the performance of their security program

Leaders say:

- Security spend as a % of IT budget: 56%
- Regulatory compliance score: 53%
- Security training completion rate: 53%
- Estimated costs of incidents or breaches: 47%
- Customer or stakeholder trust scores: 45%

Practitioners say:

- Number of security incidents: 51%
- Security training completion rate: 42%
- % of systems with critical vulnerabilities: 41%
- Regulatory compliance score: 41%
- Mean time to detect: 41%

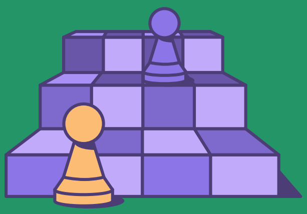
These KPIs paint a picture of a function that's expected to do it all. Security teams must deliver operational assurance and business accountability, respond to existing threats and proactively mitigate emerging ones, and stay ahead of evolving regulatory requirements – all while keeping costs low and without burning out their small teams.

Security is already playing a strategic role, but a lack of visibility and communication can cause its impact to go overlooked. To further strengthen their influence, teams must connect their KPIs more clearly to business objectives (such as business resilience and operational efficiency) to emphasize the value they bring and solidify their seat at the strategy table.

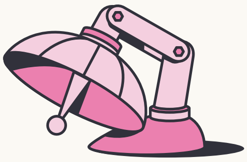
> "To move more strategically, internal teams need to work to solve problems before they occur. A cultural shift is the first thing needed, with metrics and rewards focused on avoidance of issues not quickly rectifying the ones your department creates."
>
> MATTHEW ARSENAULT, VP OF STRATEGIC ALLIANCES, JAMF SOFTWARE

AI and governance become core

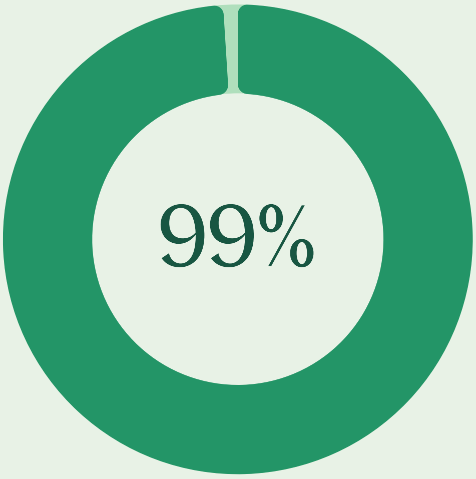
AI has become a fundamental part of security operations. Almost all (99%) of SOCs already use AI in some capacity, with 77% of respondents saying they regularly use AI, automation, or workflow tools as part of their everyday work.



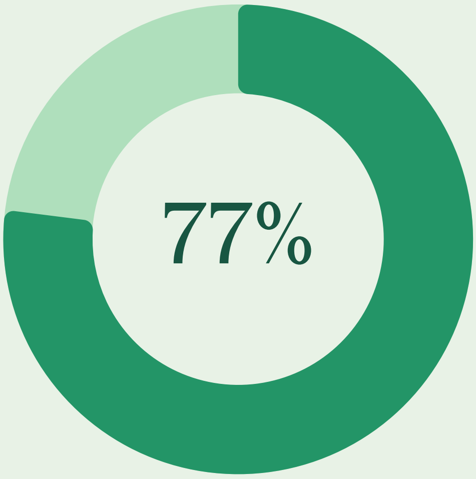
AI and AI governance have become foundational to security work.



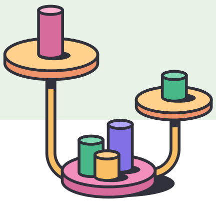
99% of SOC respondents use AI in some capacity



77% of all respondents regularly use AI, automation, or workflow tools as part of daily work



Both leaders and practitioners feel positive about the impact of AI, highlighting its effectiveness across key capabilities such as threat detection, identity and access monitoring, compliance and policy writing, and ticket triage and workflow automation.



What security jobs does AI excel at?

61%	Threat intelligence and detection
56%	Identity and access monitoring
56%	Compliance and policy writing
55%	Phishing or email analysis
53%	Ticket triage and workflow automation
53%	Reporting and communication
53%	Log analysis
53%	Developer support and code review
48%	Security and awareness training
47%	Vulnerability management

In addition to the huge benefits and opportunities it brings, AI is also a core part of the 2026 risk landscape. Three of the top five cybersecurity challenges security leaders expect to face this year explicitly center on AI. Data leakage through AI copilots and agents takes the number-one spot, closely followed by shadow AI and prompt injection attacks. Interestingly, the data reveals that internal AI use cases are considered a bigger risk than external attackers.

What's the biggest cybersecurity challenge your organization will face in 2026?

22%	Data leakage through AI copilots and agents
21%	Third-party and supply chain risks
20%	Evolving regulations and governance requirements
18%	Shadow AI (unauthorized or unmanaged AI use)
18%	Prompt injection and other AI manipulation attacks

Even the remaining two challenges (third-party risks and evolving regulations) are being reshaped by AI. These aren't new problem areas, but AI introduces new layers of complexity. Security teams need visibility into how third parties use and manage AI, and must ensure their own AI practices align with rapidly emerging regulations across industries and markets.

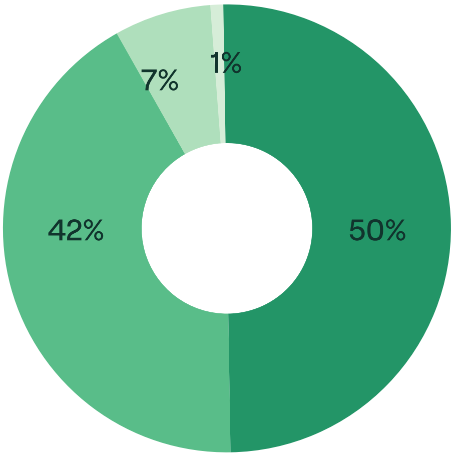
It's clear that AI isn't a fringe threat vector. It cuts across data protection, governance, and day-to-day operations. Once again, there's no clear individual challenge that leaders must prepare for. Instead, they need to be ready for a broad mix of AI-driven pressure points landing at once.

That's why AI governance is quickly becoming a core competency for modern security teams – particularly when many AI risks are coming from within. AI governance sets the policies, controls, and workflows to keep AI adoption safe, compliant, and predictable throughout the organization. It reduces risks of non-compliance, data leakage, and shadow AI, enabling teams to securely and confidently leverage AI and unlock its effectiveness.

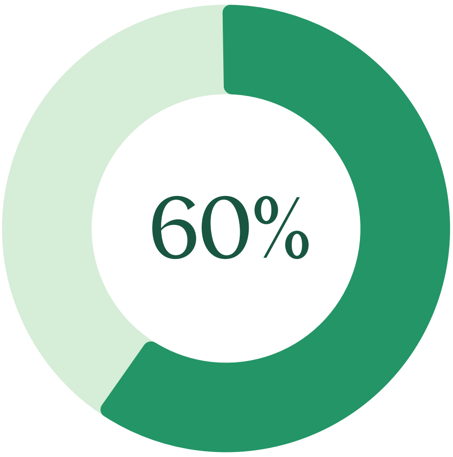
To do this, teams are pairing AI adoption with guardrails and policies. Larger organizations are more likely to have a formal AI policy or framework already, while SMEs are less likely but working to catch up.

Has your organization established a formal AI policy or framework?

- ● Yes, formalized and active
- ● In progress
- ● Discussed but not started
- ● No policy yet



60% of organizations with 5,000–9,999 employees have a formal AI policy in place compared to only 38% of organizations with 250–499 employees



Currently, 45% of respondents overall are "very confident" that AI outputs are subject to human-in-the-loop checks or other guardrails before being used in security decisions or actions. This rises to 65% for teams with formalized, active AI policies in place, highlighting the impact of a strong framework on essential governance touchpoints and critical decision-making.

Likewise, teams without these policies in place simply don't have the same confidence levels, suggesting they may be at risk of using unverified outputs for business decisions

Despite their importance, governance and compliance are still seen as blockers. Over a third of respondents (35%) cite it as the top barrier to effective automation, ahead of budget constraints and resource limitations. This could signal that governance maturity is lagging behind enthusiasm for AI adoption.

As we saw in the previous section, improving AI and governance policies are key priorities for security leaders and teams in 2026. Without these systems in place, however, teams will likely find it difficult to make progress and utilize AI to its full potential.

With AI firmly at the center of security work, security leaders and practitioners must champion governance as an enabler, not a blocker. A strong governance foundation, including clear policies and guardrails, empowers teams to scale AI safely and effectively, supporting business agility, responsiveness, and innovation while protecting against threats.

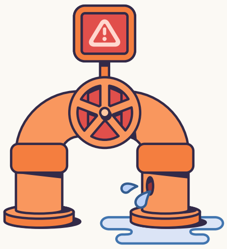
> “When you think of AI governance, a vast majority of it is data governance. But AI touches new areas like ethics, transparency, and model lifecycle management, so the old playbook around data governance or overall corporate governance only gets you part of the way. This new layer requires a task force of leaders to really rethink what it means, but the idea is really, really simple. Governance shouldn’t slow down innovation. It should make it safer to innovate.”
>
> TREVOR SCHULZE, CIO, GENESYS

3

Manual work persists

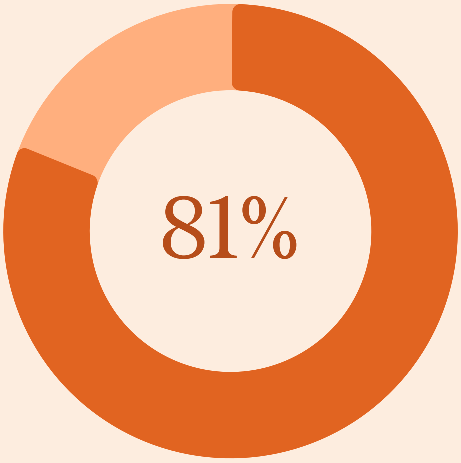
Even with AI in active use, manual work remains a major drain on time and energy. More than four out of five respondents (81%) say their security team's workloads have increased in the last 12 months. This means many teams are spending a huge percentage of their valuable time on tasks that could be taken off their hands – and out of their backlog – by AI and automation.

On average, **security teams still spend 44% of their time on manual or repetitive work** that could be automated.



This would be equivalent to roughly 3.5 hours in an 8-hour workday, if distributed daily. For a small but significant number of teams (14%), this rises to 60% to 80%. This means many teams are spending a huge percentage of their valuable time on tasks that could be taken off their hands – and out of their backlog – by AI and automation.

81% of respondents say their security team's workloads have increased in the last 12 months



Burnout follows

Three-quarters (76%) of security professionals say they experience emotional exhaustion, reduced motivation, or mental fatigue frequently or occasionally. Heavy workloads are the biggest culprit, followed by constant pressure, repetitive tasks, and limited resources.

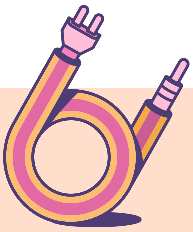
We also see that the more tools a team uses, the higher the likelihood of burnout. Almost half (47%) of all teams that use between 75 and 99 security tools daily say they frequently experience burnout, compared to the overall average of 26%.

Senior leaders recognize the negative impact of manual work on their teams. They rank modern tools and automation that reduce manual workloads as the top way to retain talent, even above competitive compensation packages and regular recognition.

Removing repetitive tasks helps to restore a good work-life balance, which practitioners cite as the most important factor impacting their decision to stay in their role.

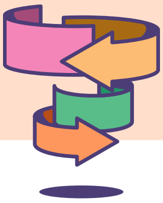
What are the main causes of burnout in your team?

39%	Heavy workloads
26%	Stress of incident response
26%	Repetitive tasks
25%	Incident staffing or resources



But it's not just a morale issue. Manual work creates more risk, from the compounding effects of human errors to reduced capacity that leaves teams unable to scale their response fast enough when threats arise. When used correctly, AI and automation can address these challenges, reducing heavy workloads and helping teams orchestrate workflows to free up time for high-impact, high-stakes work without requiring additional headcount. But it's clear that while AI is present in most organizations, many teams aren't yet using it to reshape their operational foundations.

This isn't due to a lack of interest or resistance to automation. In fact, only 19% of respondents say the ROI or business case for automation is unclear. The real blockers are foundational. Security and compliance concerns, limited resources, and technical challenges (such as integration gaps, legacy systems, and staff training) make it difficult to implement new ways of working, even when teams are optimistic about the potential.

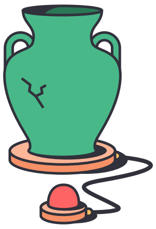


What are the main barriers to effective automation in your environment?

35%	Security or compliance concerns
32%	Budget or resource constraints
31%	Integration gaps between tools
30%	Legacy or outdated systems
29%	Insufficient skills or training

This could explain why AI adoption hasn't yet translated into meaningful reductions in manual work. When workflows are fragmented, processes depend on manual handoffs, and teams must constantly switch between disconnected tools and outdated systems, adding AI doesn't fix the problem. It just slots into the same broken structure, becoming another tool to manage instead of a force multiplier.

The signal is clear. AI alone is not enough. The potential to improve workloads is enormous, with massive time savings and morale improvements just within reach. But it can't solve underlying operational issues on its own.



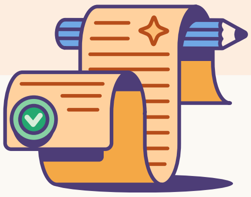
What are intelligent workflows?

Intelligent workflows unite AI, automation, integration, and humans to move work smoothly across systems and people. They combine three core types of workflows: rules-based automation, agentic AI, and humans-in-the-loop. This gives teams the flexibility to apply the right approach to each task, so they can scale operations securely and reliably.

To reduce workloads, eliminate repetitive muckwork, and create sustainable capacity, teams must rethink the foundation of how work gets done. This is where intelligent workflows come in.

Intelligent workflows gives teams the visibility, guardrails, and security required to scale their resources effectively and reliably. Only then can they break out of the cycle of rising workloads and turn AI from isolated wins into real impact.

> “Security teams now play a strategic role: enabling growth, managing risk, and aligning with business objectives. Yet repetitive low-value tasks keep them reactive. Automating these tasks frees analysts to focus on trends, control effectiveness, and risks tied to organizational goals. That shift transforms security operations from alert-driven responses to proactive strategies that demonstrate measurable business value and strengthen overall resilience.”
>
> SAM HARRIS, SR. DIRECTOR OF MANAGED SERVICES, STRATASCALE (SHI COMPANY)



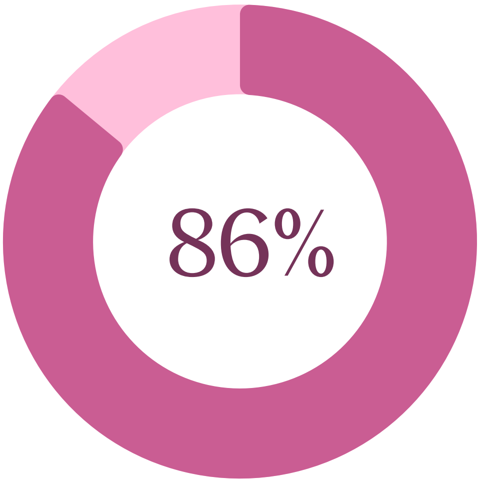
4

Optimism about AI’s impact on security careers

Security roles are shifting fast. AI is changing expectations, expanding responsibilities, and reshaping skillsets, and leaders and practitioners alike are excited about what this means for the future of their work.

Sentiment is overwhelmingly positive, with 86% of respondents expressing optimism that AI will create new opportunities in the job market. Of these, almost half (48% of leaders and 45% of practitioners) describe themselves as very optimistic.

86% of respondents are optimistic that AI will create new opportunities in the security job market



Exposure to AI further increases this confidence. More than half (52%) of teams that already use AI, automation, and workflow tools in their daily work say they're very optimistic. Significantly, two-thirds of respondents (66%) with a formalized and active AI policy or framework are very optimistic.

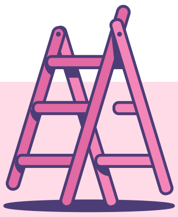
Confidence grows with AI maturity

This data suggests that the more experience teams have with AI and the more mature their adoption is, the more confidence they have that it will positively transform the job market. This may be because they're already seeing the benefits and impact of AI, automation, and orchestration in their everyday work.

Teams currently feeling the effects of manual work and frequently experiencing burnout also express higher-than-average levels of optimism, suggesting they're aware of the weaknesses in their current processes and recognize how AI could make their roles less repetitive and more strategic going forward.

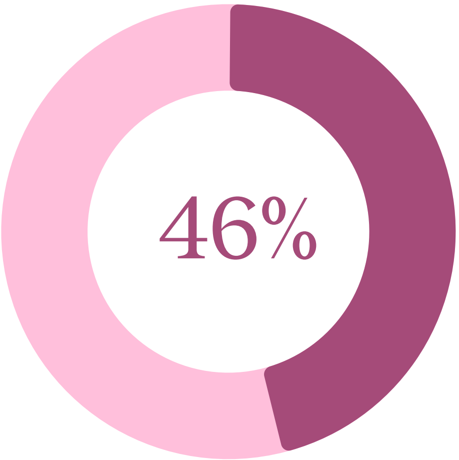
% of respondents who are very optimistic that AI will create new opportunities in the security job market

52%	Teams that regularly use AI, automation, and workflow tools as part of daily work
66%	Teams with a formalized and active AI policy in place
56%	Teams that spend 60% or more of their time on manual work
65%	Respondents who frequently experience burnout



However, some regions are more positive than others. The US, Australia and New Zealand, and the UK report the most optimism about the AI job market, while Europe remains more measured.

Global average: 46% of respondents are very optimistic that AI will create new opportunities in the security job market



This trend may reflect differences in these geographies' regulatory approaches to AI. For example, the EU's AI Act outlines a rigorous framework for how businesses use and report on AI, which could contribute to more measured expectations in those countries. It's worth noting, however, that even in these more cautious regions, overall optimism is still high, with only 3% of respondents globally saying they're "unoptimistic".

Skills needed to thrive

Looking forward, AI literacy and prompt engineering top the list of new skills deemed most important for security professionals as we enter 2026, closely followed by cloud and infrastructure security. The next generation of security professionals must also be skilled at security automation and threat intelligence, with data governance and ethics rounding out the top five.

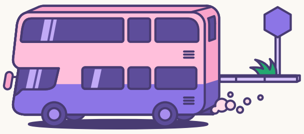
Which new skills do you think will be the most important for security professionals by 2026?

36%	AI literacy and prompt engineering
34%	Cloud and infrastructure security
28%	Security automation and scripting
28%	Threat intelligence and analysis
25%	Data governance and data ethics

Together, this skillset paints a clear picture of where security roles are headed. AI-driven, cloud-native, and compliance-first security will become the norm. Intelligent workflows mean that automation will handle repetitive tasks and data-intensive work, AI will provide explainable insights, and human analysts will focus on judgment and governance.

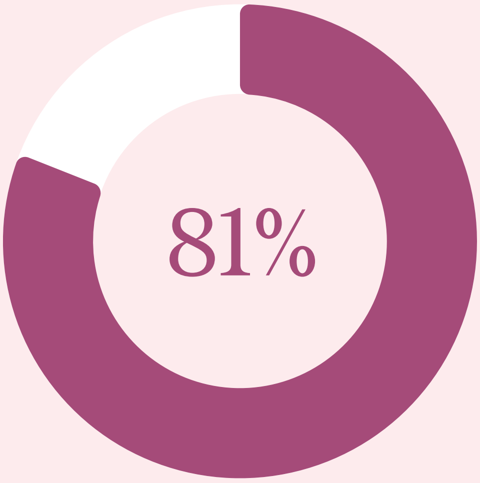
Teams are in a good position to reskill or hire for AI-related security roles, with 81% reporting that they're mostly or very prepared.

Once again, teams with a formal AI policy in place have an advantage. Over half (59%) say they're "very prepared" to reskill or hire for these roles, possibly because they're more familiar with the requirements for candidates. Teams without these frameworks in place (or at least underway) are at risk of falling behind, with only 48% believing they're prepared to fill these roles.



81% of respondents feel their team is mostly or very prepared to reskill or hire for AI-related roles

- ● 39% very prepared
- ● 42% mostly prepared



Percentage of respondents who say their team is prepared to reskill or hire for AI-related roles, by AI policy status

92%	Formalized and active	
74%	In progress	
48%	Discussed but not started/no policy yet	

When it comes to retaining top security talent, leaders and practitioners are relatively aligned – with one notable exception. As we saw in the previous section, practitioners rate a good work-life balance above all else. This is closely followed by fair compensation and flexible working options, with value-based factors (such as having an impact, positive team relationships, and opportunities to learn and grow) also ranking highly.

Senior decision-makers say reducing manual work via modern tools and automation is the most effective way to keep their employees happy, which maps neatly to practitioners' desire for a good work-life balance. But while leaders believe career growth opportunities and clear promotion paths are the second-best way to retain talent, practitioners are far less motivated by advancement than leaders realize, revealing a clear perception gap.

What actions are most effective for retaining security talent?

Leaders say:

- Modern tools and automation to reduce manual work: 40%
- Career growth opportunities and clear promotion paths: 40%
- Flexible or hybrid working options: 39%
- Competitive pay and benefits: 38%
- Investment in training and skills development: 38%

Practitioners say:

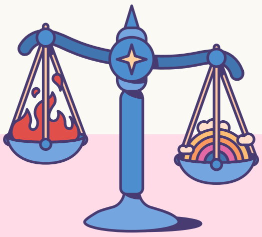
- Good work-life balance: 38%
- Fair pay benefits: 34%
- Flexibility to work remotely or hybrid: 33%
- Feeling that my work has impact: 33%
- Supportive team and culture: 33%

In fact, practitioners are more interested in having an impact (33%) than in clear career progression (29%). This is true across all lengths of service, even for early career professionals with only 1–3 years in security, risk, or process roles.

Overall, security professionals feel energized by the career possibilities AI is creating. For practitioners, AI feeds into their core priorities and long-term goals: it cuts out time-consuming, low-value tasks and enables them to focus on fulfilling, meaningful work that inspires them.

To keep top talent engaged and future-ready, leaders and organizations must invest in emerging skills, listen to what practitioners really want, and give teams the tools and workflows they need to win back time for impactful work.

> "In an era of tool sprawl, true efficiency requires intelligent workflows that unite human expertise, automation, and AI. This synergy is critical for continuous Zero Trust. We are seeing SOC teams use GenAI to operationalize adaptive trust – transforming real-time telemetry into immediate action and moving far beyond static policy enforcement."
>
> DAVID WILLIS, VICE PRESIDENT, TECHNOLOGY ALLIANCES, NETSKOPE



5

The intelligent workflow gap

Security tech stacks are growing, but their ecosystems are still far from optimal. Teams continue to face challenges, like high maintenance costs, limited automation, and operational blockers such as a lack of visibility, difficult reporting, siloed data, and poor UX.

Lack of integration remains a top challenge, particularly for companies with between 1,000 and 4,999 employees. This has significant effects. As we've already seen, integration gaps between tools is a major blocker to effective automation, especially for organizations with between 500 and 4,999 employees where it's ranked as the second-biggest barrier.

What challenges do your current tools create?

42%	High maintenance cost
34%	Limited automation
33%	Overlapping functionality
31%	Lack of integration

In 2026, businesses are leaning into interoperability. Some 62% of organizations are using or considering the OpenAI API or plugin framework for security work, while 44% are using or considering Model Context Protocol (MCP).

This suggests that teams are thinking strategically about AI adoption and moving beyond isolated AI pilots toward embedded, operational AI workflows.

Which interoperability protocols or frameworks is your organization using or considering to support AI adoption in security?

62%	OpenAI API or plugin framework
44%	Model Context Protocol (MCP)
43%	In-house proprietary protocol
39%	LangChain or similar orchestration frameworks
3%	Not using any interoperability protocol

MCP is gaining traction because it gives AI a standardized way to interact with tools and systems. While MCP accelerates the operationalization of AI, the inherent concerns around access control, auditability, and governance still exist. An intelligent workflow platform helps teams tightly scope tool actions, enforce deterministic checks around LLM behavior, and include human review where needed, all while integrating cleanly with the systems you already use. It gives you a safer, more controlled foundation to orchestrate AI.

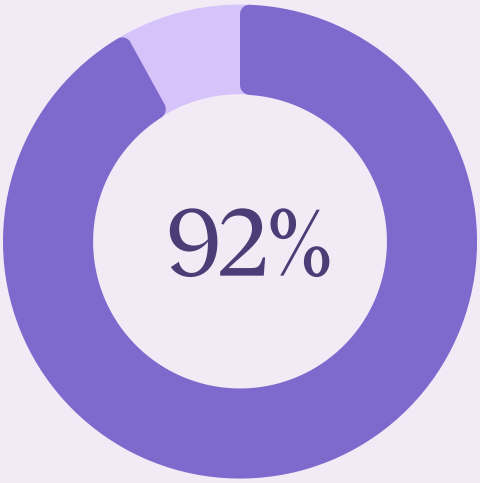
Rather than consolidating their tools, most respondents (73%) expect their security tech stack to expand in the coming year – particularly organizations that use over 50 tools. Even large tech stacks are only continuing to grow, highlighting the need for vendor-agnostic platforms that flexibly adapt to teams' tools rather than locking them into specific systems or ways of working.

If done poorly, however, these additional tools risk increasing pressure on already stretched teams and workflows. We've already seen how simply bolting on additional tools to existing workflows can contribute to burnout, adding to manual workloads and increasing context switching for practitioners.

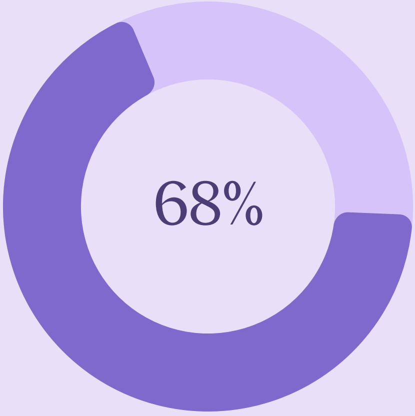
Intelligent workflows can relieve the pressures teams face on a daily basis.

92% of security professionals say an intelligent workflow platform is extremely or very valuable

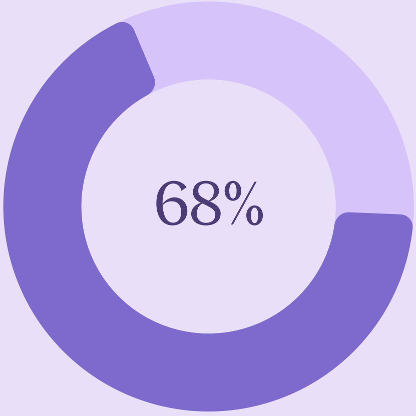
- ● 49% extremely valuable
- ● 43% very valuable



68% of respondents who frequently experience burnout say it would be "extremely" valuable



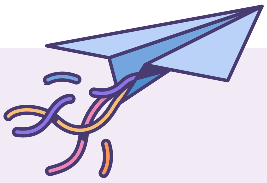
68% of respondents who use between 75 and 99 tools daily say it would be "extremely" valuable



Teams see strong potential for intelligent workflows to boost productivity, accelerate response times, and improve data accuracy. Respondents also expect them to strengthen compliance and facilitate faster decision-making, better visibility, and smoother collaboration.

What benefits would you expect from more connected, automated workflows?

48%	Higher productivity
41%	Faster response times
40%	Better data accuracy
34%	Stronger compliance
33%	Quicker decision-making
33%	Better team visibility
33%	Smoother collaboration

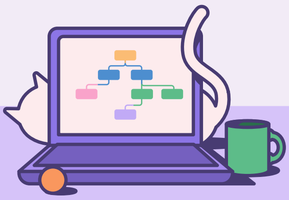


An intelligent workflow platform gives security teams the foundation to build, adapt, and scale their processes. The right platform unites automation, AI, and integrations so work can move seamlessly across systems and people in a secure, reliable way.

As workloads rise, AI adoption increases, and tech stacks expand, intelligent workflows will be the differentiator that enables security teams to orchestrate their work across even the most complex processes and systems without introducing risk.

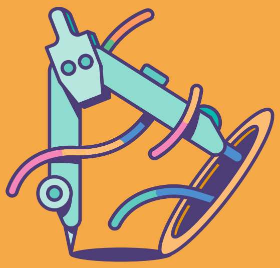
“Security teams have added tool after tool in search of clarity – but ended up with more alerts, more dashboards, and even more manual work. Intelligent workflows flip that equation. They streamline processes, pull context from integrated tools, and involve people only when human judgment is truly needed. The result: less fatigue, sharper focus, and a security program that scales and adapts to how modern organizations actually operate.”

ORON NOAH, VP OF PRODUCT EXTENSIBILITY & PARTNERSHIPS, WIZ



2026 strategy checklist

The insights in this report highlight the pressures security teams are facing and where change is needed. Where should security teams prioritize their efforts in 2026? This checklist outlines the focus areas that will matter most.



Align security priorities to business goals. Connect team metrics to broader business objectives so it's clear how security drives resilience, customer trust, and operational efficiency.

Treat AI as a foundational capability and build guardrails early. Adding AI to broken processes won't fix them. Reevaluate underlying workflows to understand where AI can provide real impact, and pair adoption with strong governance and clear guardrails from the start.

Reduce manual work to protect team capacity and reduce burnout. Look for opportunities to automate time-consuming tasks, such as evidence collection, triage, or case management, so practitioners can focus on higher-impact work.

Build AI literacy and automation skills across the team. Security skillsets must evolve to meet new AI-driven demands. Strengthen AI and automation literacy so practitioners can interpret, analyze, and challenge AI outputs with confidence.

Strengthen cross-team processes to reduce friction and improve alignment. Define clear workflows and communication pathways between key functions, like security and IT, for stronger collaboration and increased decision velocity.

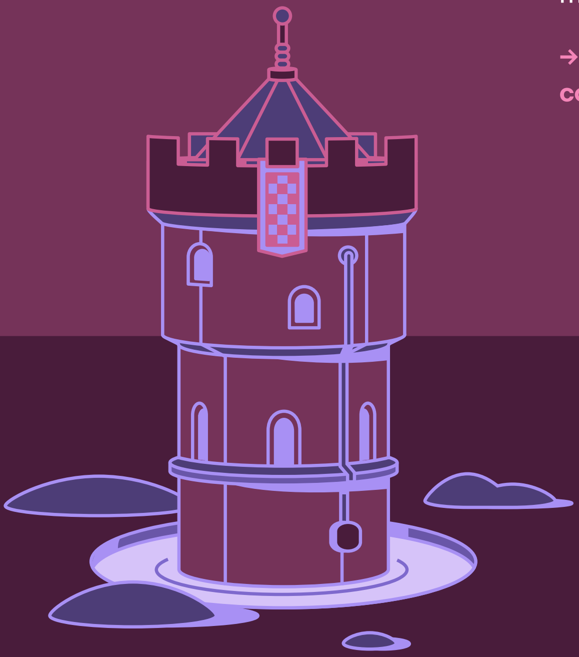
Modernize tooling and workflows to connect systems and enforce governance. Fragmented tools create risks, data silos, and manual work. Integrate tools and systems to keep data flowing and enhance governance with stronger reporting and auditability.

Use intelligent workflows to scale impact responsibly and maximize your resources. Combine deterministic automation, AI, and human judgment within a single orchestrated system. This gives teams the flexibility to respond to each use case based on risk and comfort level. Start with pre-built templates from the Tines Story Library to accelerate results.

The future of security

Modern security teams are expected to handle a wide range of priorities. But when everything is deemed equally important, it's hard to cut through the noise and understand where to devote limited time and resources.

To get (and stay) ahead in 2026, security teams need to rethink their underlying processes and win back time for high-value work. By using intelligent workflows to automate repetitive tasks and use cases, leverage AI responsibly, and maintain human judgment and oversight where it's most critical, security teams can multiply their strategic reach and impact to truly transform business operations.



→ Want to dig deeper into the data and discover how industry-leading security teams are preparing for 2026 and beyond? **Watch the webinar now.**

Tines is an intelligent workflow platform trusted by security and IT teams worldwide to power their most critical operations. From Fortune 50 enterprises to startups, teams rely on Tines for everything from phishing response and patch management to software and employee lifecycle workflows. Industry leaders like Canva, Databricks, Elastic, Kayak, Intercom, and McKesson use Tines' AI-powered workflows to improve efficiency, reduce risk, cut tech debt, and focus on what matters most.

→ Ready to get started? **Sign up for our community edition for free.**