zscaler™

Security Operations Trends Report

Summary of insights from a global survey of 550 security leaders, regarding their priorities, resources, and overall experiences

What's inside

Introduction 03

Key findings 04

The state of security operations 05

Cracks in the SOC: Skill gaps and operational strain 07

The future of security operations: AI agility and adaptive defense 12

Final thoughts 15

Methodology 16

Introduction

Security leaders struggle to keep up as threats outpace spending

Despite rising investment in tools and technologies, security leaders admit they are struggling to stay ahead of threats. Four out of five say they are spending more than ever on security, yet breaches and threats keep growing. Skills shortages, evolving adversary tactics, tool sprawl, and external pressures are pushing SOC teams into survival mode, leaving the future of cybersecurity in need of bold rethinking and accelerated adaptation.

Security leaders estimate that, on average, cyber incidents cost their organization

$3.7M

in the past year.

It's time for the SOC to adapt to survive

The solution, however, is not simply adding resources or throwing money at the problem. The future of security operations will be defined by how effectively teams can simplify workflows, streamline intelligence, and harness emerging technologies like AI — both to cut through overwhelming data and to anticipate new forms of attacks. This report reveals how security leaders are grappling with these trends and outlines the strategies they'll need to turn the tide.

Key findings

Security leaders are struggling with widespread skills shortages, the growing cost of cyber incidents, the complexity of defenses, tool sprawl, and AI's mixed role as both a help and a risk in security operations.

Budgets are still increasing, but throwing money at the problem isn't helping

On average, security budgets have increased by 12% in the past year, but 54% of security leaders say throwing money at cyber risk doesn't guarantee protection — it just buys more complexity.

Organizations are consolidating tools to streamline their workflows, but are still struggling to stop attacks quickly enough to prevent damage

Consolidation has been a focus over the past 12 months, as organizations now use 65 security tools on average, compared to 91 in 2024; but 73% of security leaders say the time from detecting an attack to resolution has increased.

The AI security threat is real, just a little different than what many might have expected

78% of security leaders say the talk of AI releasing a tidal wave of novel attacks is fearmongering, but 43% have already experienced an incident relating to their own AI tools, highlighting that internal policies are the most immediate priority for SOC teams.

The business impact of cyber attacks is heavily felt

Security leaders estimate that, on average, cyber incidents cost their organization $3.7M in the past year, with 46% suffering from an outage or disruption to service resulting from attacks.

Organizations are already widely adopting AI in security workflows to improve SOC team productivity

The top three security workflows that organizations are already using AI in are: detection analytics, intrusion detection, and SIEM data management.

Skills shortages continue to affect critical areas

75% of organizations have skills shortages around intrusion detection and 72% around incident response, making prioritizing and responding to threats quickly enough a top challenge for SOC teams.

With internal SOC teams already overwhelmed by skills gaps and finite resources, organizations need to find ways to take some of the burden of security off their shoulders, so that they're not solving every alert, vulnerability, or problem alone. Partnering with outside experts remains one of the most effective ways to bring in timely intelligence and handle routine threats to narrow the window of exposure.

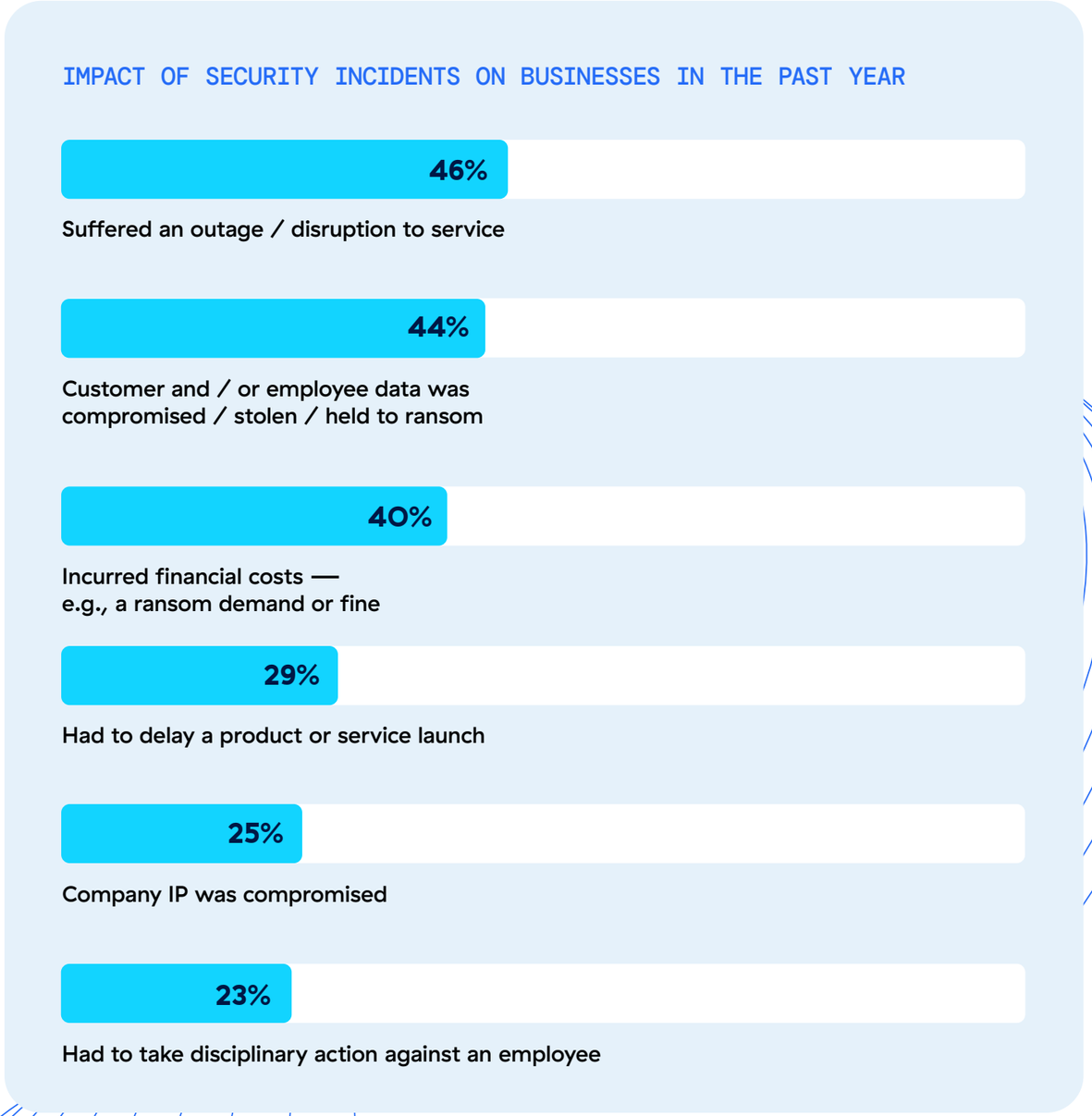
The state of security operations

Security budgets have increased by 12% in the past 12 months, but the pressure on SOC teams continues to rise as threats keep growing. Security leaders need to find a new approach and adopt more intelligent solutions to deal with rising attacks, as 54% say that throwing money at cyber risk doesn't guarantee protection; it just buys more complexity.

> **80% of security leaders** say that they're spending more than ever on security — yet breaches and threats keep growing.

SOC teams are also struggling to keep pace with the rapid expansion of the attack surface, which has risen by 41% in the past 12 months alone.

> **73% of security leaders** say that the time from detecting an attack to resolution has increased over the past 12 months, and 35% say there has been a significant increase.

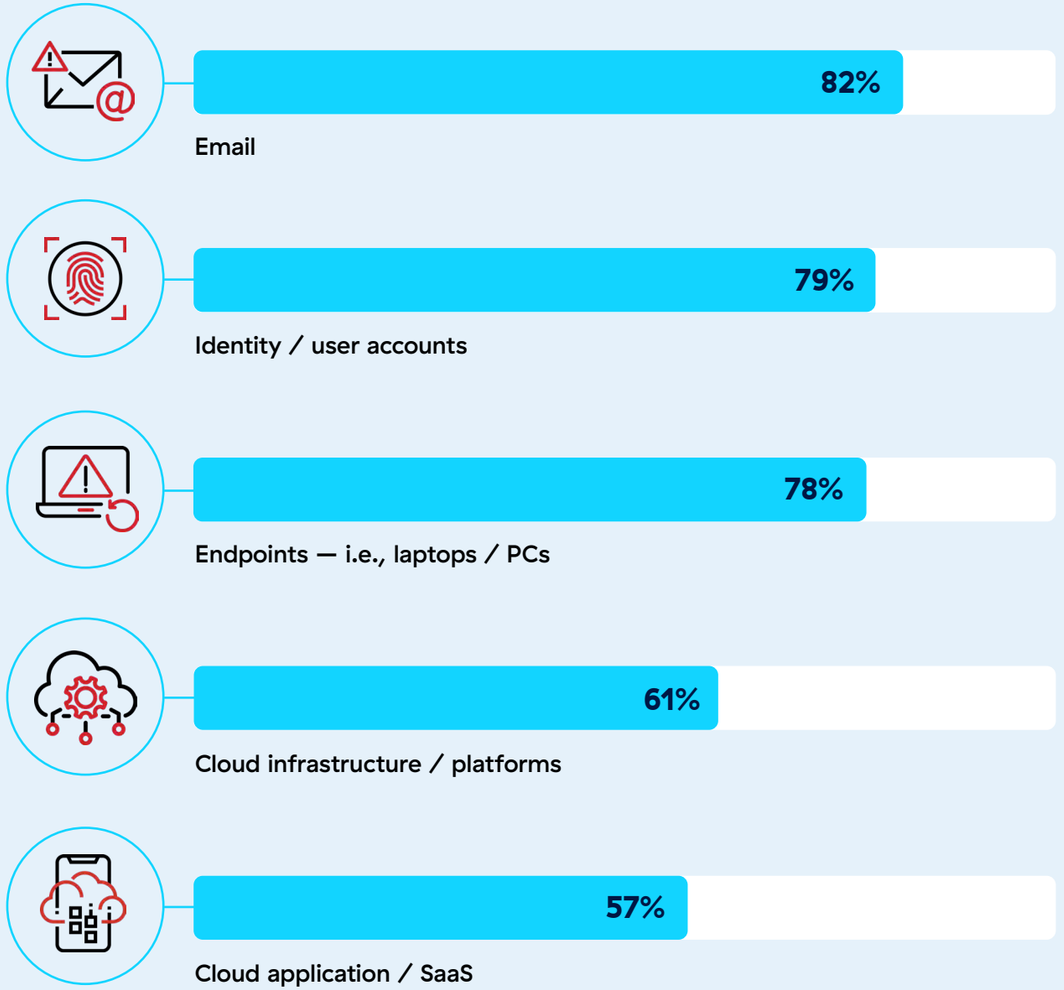


This hesitancy and sense of confusion means that successful cyber attacks are having an even greater business impact, **costing organizations an average of $3.7 million in the past year.** Email and identity are prime targets because adversaries can masquerade as legitimate users and remain undetected, using stolen credentials or hidden mailbox rules to quietly gain access to an organization's environment.

Today's threats increasingly target the fundamental tools and channels that keep organizations running, making their impact faster and more far-reaching. To counter this, security leaders should prioritize AI-enabled defenses that can spot subtle anomalies at scale and help security teams stay ahead of fast-moving adversaries.

> **83% of security leaders** say today's attackers don't break in — they log in — and they're harder to stop than ever.

CYBER INCIDENTS ORGANIZATIONS HAVE EXPERIENCED OVER THE PAST 12 MONTHS



Cracks in the SOC: Skill gaps and operational strain

Skills shortages in core areas mean many SOC teams struggle to move past alert-watching to active detection and response, leaving blind spots that adversaries can take advantage of. These gaps widen the "detection deficit" and raise the risk of serious incidents going unnoticed.

THE MOST COMMON SKILLS SHORTAGES WITHIN INTERNAL SOC TEAMS





With SOC skills shortages unlikely to improve, security leaders need different strategies to overcome their many challenges. Streamlining processes, consolidating tools, and partnering with third-party experts all have a role to play in helping teams to focus on the most critical threats rather than being overwhelmed by day-to-day noise.

Increasingly, this also means finding ways to integrate AI capabilities into routine workflows to automate investigation, reduce false positives, and give analysts the time to concentrate on high-value defense.

TOP CHALLENGES FOR SOC TEAMS



Prioritizing and responding to threats quickly enough to mitigate the impact



The amount of time needed to configure controls and policies in security tools



Managing SIEM data and making it useful for analytics and investigation



Securing multicloud environments



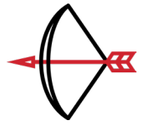
Attracting, recruiting, and retaining skilled security staff



Investigating incidents to meet strict regulatory reporting deadlines



Keeping the workforce trained on the latest threats to prevent issues such as phishing attacks



Threat hunting in a targeted and effective manner

As organizations work to overcome these challenges, they are implementing a range of practices and initiatives to reinforce security awareness across the business.

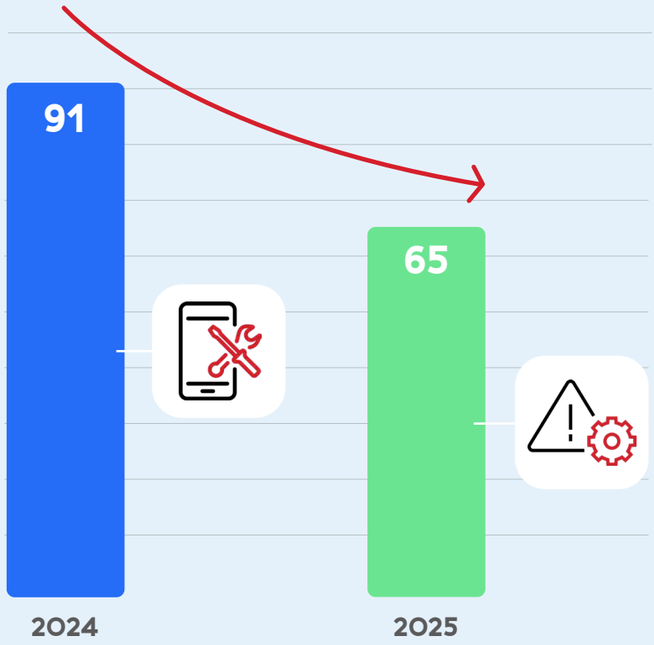
These initiatives must go beyond a tick-box exercise — every employee needs to be engaged in spotting risks and taking responsibility for security, because the SOC cannot defend the organization alone.

ACTIVE OR PLANNED EFFORTS TO INCREASE SECURITY AWARENESS IN THE WORKFORCE

Security awareness practices	Currently do	Planning to
Include cybersecurity training as part of employee onboarding	75%	19%
Discuss real-world cyber incidents and how they could have been avoided	67%	24%
Engage employees at all levels, from junior to senior roles	64%	26%
Mark Cybersecurity Awareness Month in October with activities	58%	31%
Recognize and reward good security behaviors amongst staff	50%	35%
Reward employees for flagging suspicious activity or emails	43%	39%
Gamify security awareness training to make it fun and more engaging	35%	43%

With SOC teams already stretched, fragmented tools and constant alerts only make skills shortages more difficult to manage. Consolidation isn't just about cutting costs — it's about reducing complexity and noise so security analysts can spot the threats that matter most and respond faster.

AVERAGE NUMBER OF SECURITY TOOLS ORGANIZATIONS USE



TOP SECURITY TOOLS OR SERVICES SECURITY LEADERS ARE LOOKING TO REMOVE OR CONSOLIDATE

Cloud security
46%

SIEM
42%

Application security
40%

Reducing complexity also extends to the way organizations balance their security operations between internal and external teams. By outsourcing routine monitoring and intelligence tasks, security teams can lean on trusted partners to absorb noise and tackle commodity threats — freeing themselves to focus on business-specific risks and improving their longer-term security posture.

THE EXTENT TO WHICH ORGANIZATIONS OUTSOURCE SECURITY FUNCTIONS

57% Day-to-day management and monitoring of SIEM

54% Incident response

50% Threat intelligence

49% Detection and response

47% Security awareness training

Security leaders need real-time insights into the performance of their teams and the effectiveness of the tools they rely on to make accurate decisions about where they can streamline and improve their workflows. Without this level of visibility, security leaders risk worsening skills gaps or making investments that don't deliver a valuable impact.

METRICS USED TO MEASURE THE PERFORMANCE OF SOC TEAMS AND TECHNOLOGY INVESTMENTS

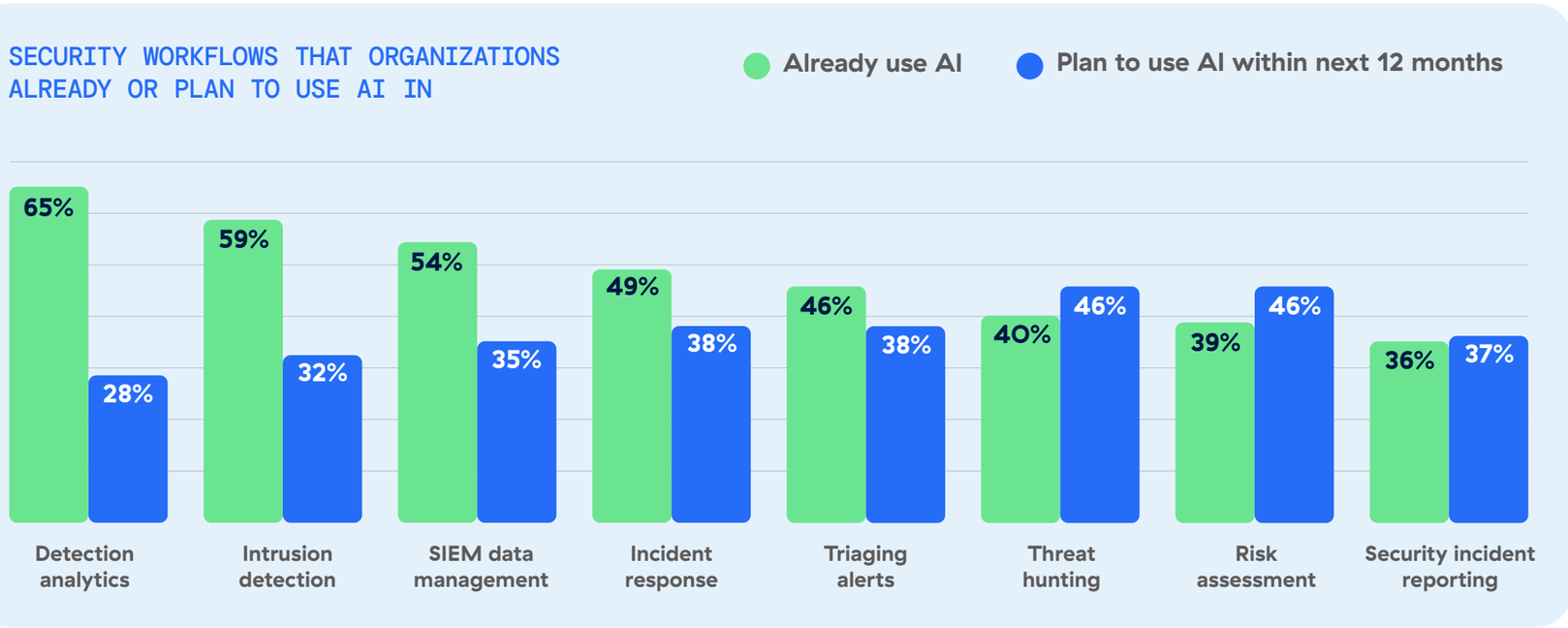
- Time to detect incidents/threats **47%**
- Mean time to resolution on threats **41%**
- Time to investigate incidents/threats **37%**
- Volume of incidents handled per analyst/team **35%**
- Cost per incident **31%**
- Percentage of incidents detected internally vs. externally **28%**
- False positive rates **24%**
- Percentage of automated vs. manual responses **22%**
- Dwell time (i.e., time threats remain undetected) **18%**

The future of security operations: AI agility and adaptive defense

AI is no longer an emerging technology — it's already transforming security operations, with many organizations and partners using it today to drive faster, smarter defense. The benefits are clear and will only continue to grow. The productivity and efficiency gains of AI are already reshaping how SOC teams work, making it one of the most important areas of investment for security leaders.

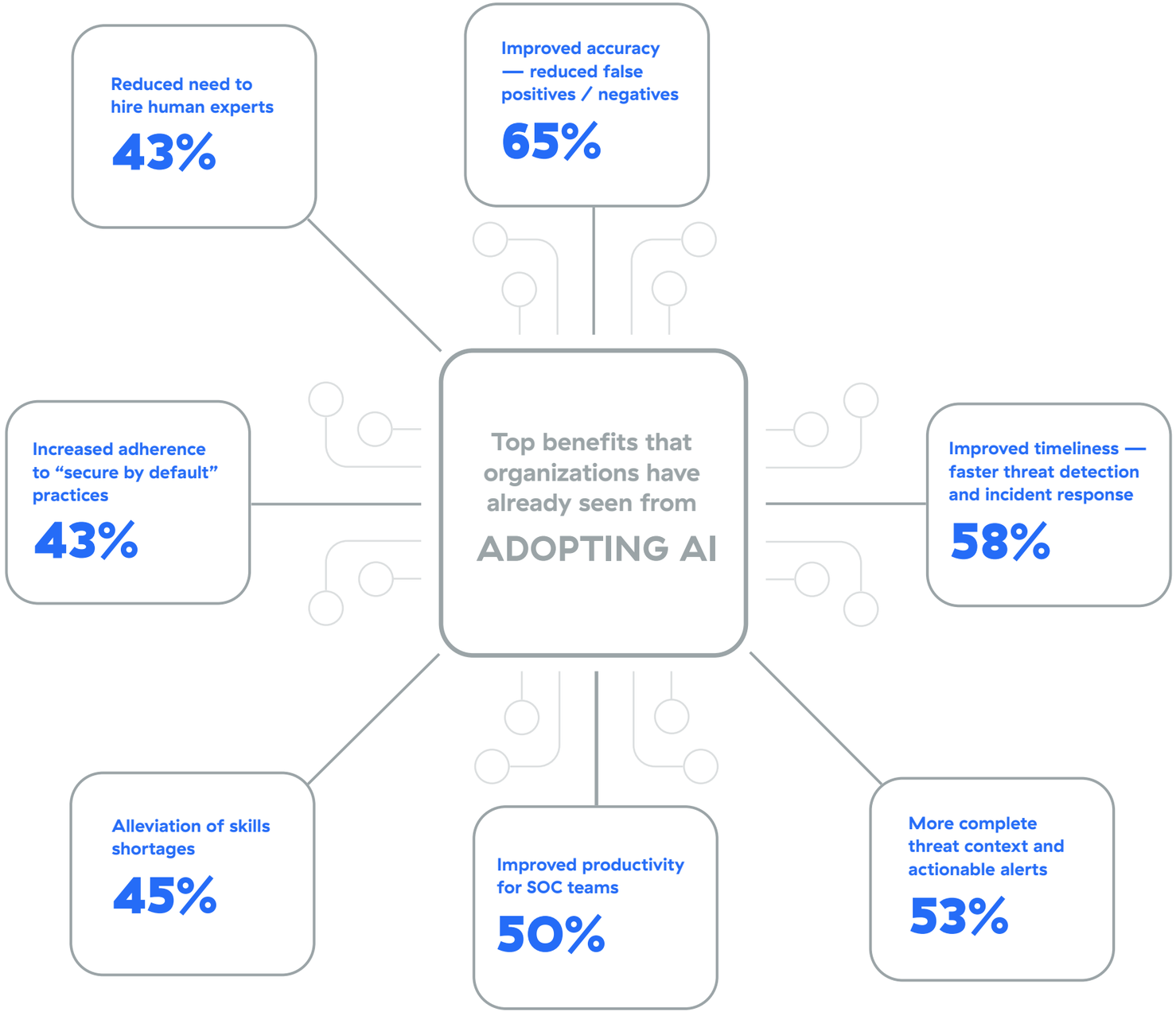
In fact, **80% of security leaders say that without AI, defenders are drowning in noise while adversaries sail right past them.** While some remain cautious about overreliance on AI, most recognize that thoughtful adoption is key. Security leaders must focus their efforts on applying AI where it delivers the most value: augmenting human judgment, accelerating detection, and enhancing defenders' ability to counter evolving threats.

SECURITY WORKFLOWS THAT ORGANIZATIONS ALREADY OR PLAN TO USE AI IN



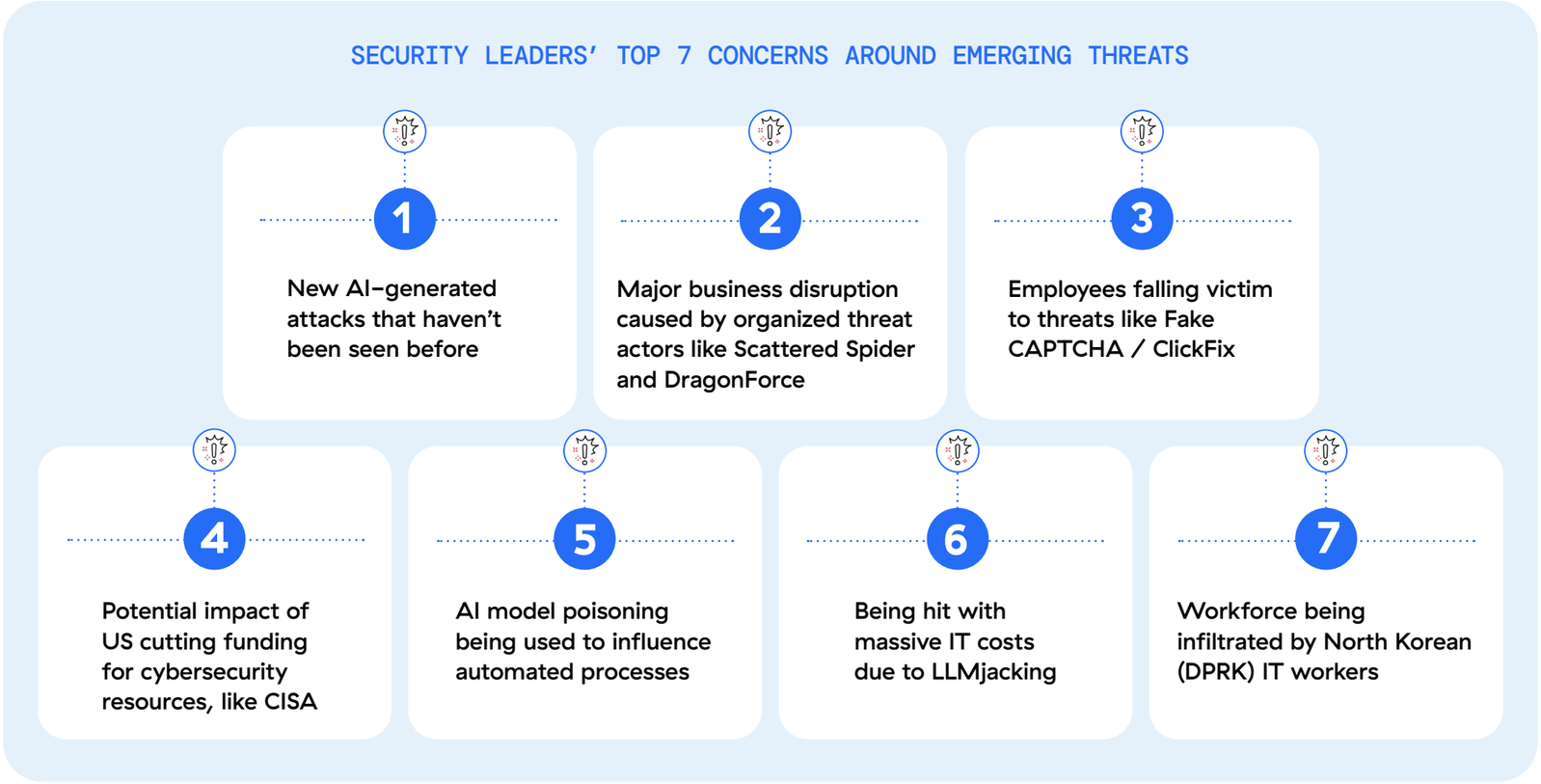
85%

of security leaders say forget the AI apocalypse — the real risk is being overwhelmed by the thousand missed threats that will get through if we don't automate more



As AI becomes central to modern defense, security leaders are also weighing its risks, recognizing that the same technology helping SOCs today can equally be used by adversaries. Their top concern is the rise of AI-generated attacks that haven't been seen before, highlighting that while AI brings significant benefits, it also gives adversaries new tools to scale their operations.

Now is the moment for security leaders to develop actionable plans for the future, identifying which threats are likely to have the biggest impact and where they'll originate. As organizations consider the solutions they want to invest in, they need to be prepared for a threat landscape that will no longer be defined only by familiar risks. By continuing to invest in intelligent, AI-driven solutions, security teams can better anticipate these shifts, detect subtle anomalies, and respond at the speed adversaries move. Rather than being defined by disruption, the future of security operations will be shaped by how effectively leaders use these tools to stay ahead.



While AI-generated attacks are a top concern for security leaders, much of the hype around how adversaries will use these technologies to supercharge their attacks has not materialized. The reality is that AI — for now at least — is simply a productivity tool.

78%

of security leaders say that the talk of AI releasing a tidal wave of novel attacks is fearmongering — it just helps adversaries move faster and smarter.

Final thoughts

The old model of throwing more tools, people, and budget at security operations is no longer viable — defenders need an approach that is leaner, smarter, and built to adapt.

WE RECOMMEND FIVE KEY STEPS:

1

Concentrate on what is unique to your business

Roughly 80% of threats stem from common technologies rather than business-specific systems. If a Windows flaw is exploited, it impacts every Windows user. That's why collective protection — gained by working with trusted security partners that monitor across hundreds of organizations — is more effective than going it alone. Internal teams should reserve their energy for defending the assets and applications that are truly unique to them.

2

Invest with precision

Security leaders need to regularly assess their people, tools, and processes to identify where resources are being wasted and where they are making the most difference. By measuring real outcomes, teams can decide which tools are worth keeping, which can be consolidated, and how to balance headcount, training, and outsourcing to get the best return.

3

Harness AI to scale your defenses

The benefits of AI for defenders far outweigh the risks. SOC teams drowning in alerts need technology that can turn raw data into actionable insight. AI can act as a powerful teammate — analyzing vast data sets, connecting dots across disparate systems, and surfacing what matters most. It won't be perfect, but AI gives analysts a faster, sharper starting point to act on.

4

Move from reactive to proactive defense

Adversaries are moving through intrusion chains faster than ever, shrinking the time defenders have to act. To stay ahead, organizations must detect threats earlier, anticipate what's coming, and shift resources into proactive defense. That means turning intelligence into concrete action, backed by 24/7 monitoring and hybrid security models that give stretched SOCs the coverage they need.

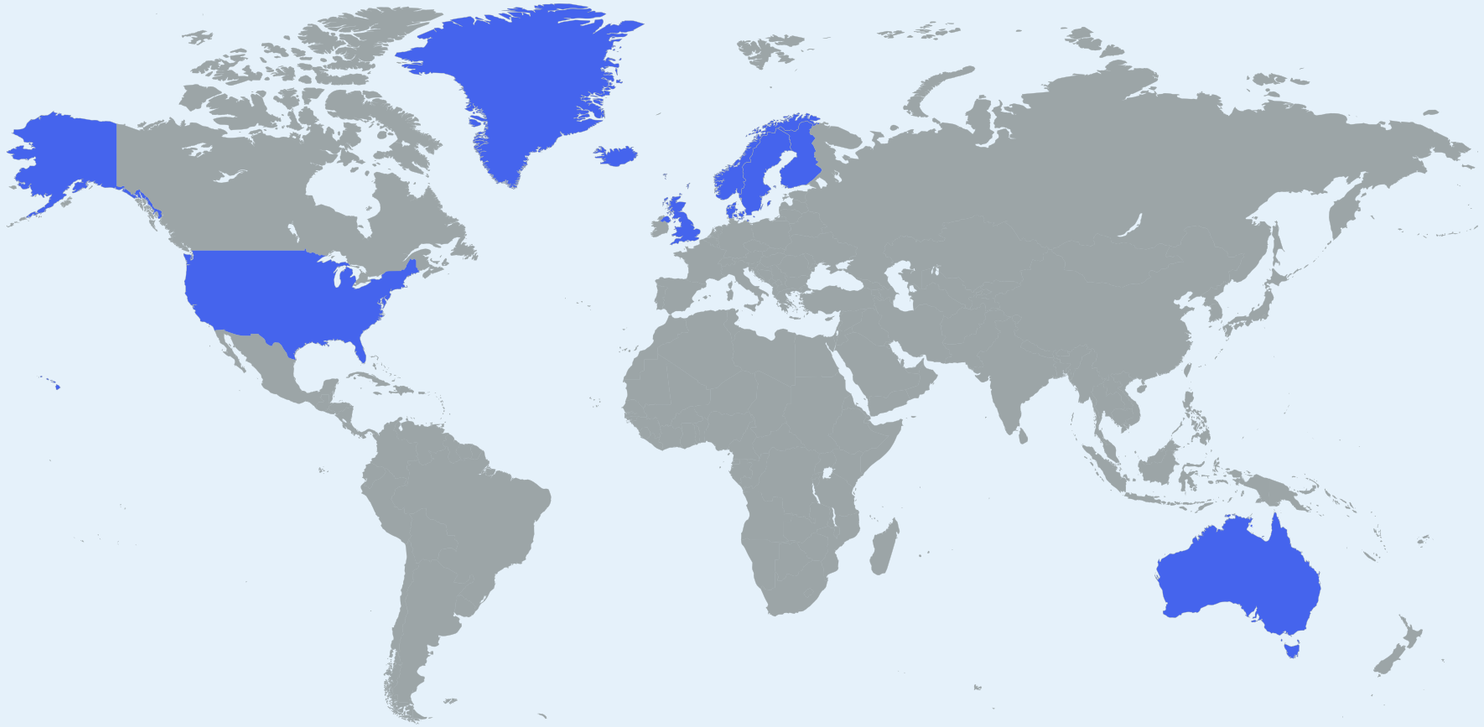
5

Enable your internal team to do what matters most

New technologies like cloud have widened the skills gap, leaving internal teams unable to master every system while also keeping pace with innovation. Leaders need to bridge this gap by reallocating resources away from repetitive operational tasks toward higher-value initiatives, supported by the right mix of automation and external expertise. This not only reduces risk but also ensures in-house teams are focused on the areas where they can deliver the greatest impact.

Methodology

This research was conducted by Coleman Parkes as an online survey of individuals with decision-making responsibility for data tooling for cybersecurity solutions. Coleman Parkes surveyed 300 respondents in the US, 100 in the UK, 100 in Australia and New Zealand, and 50 in the Nordics, from a cross-section of organizations with more than 1,000 employees.



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

Act Fast.
Stay Secure.™