seceon
SECURITY FOR EONS

The Global MSSP AI Threat Readiness Pulse 2026

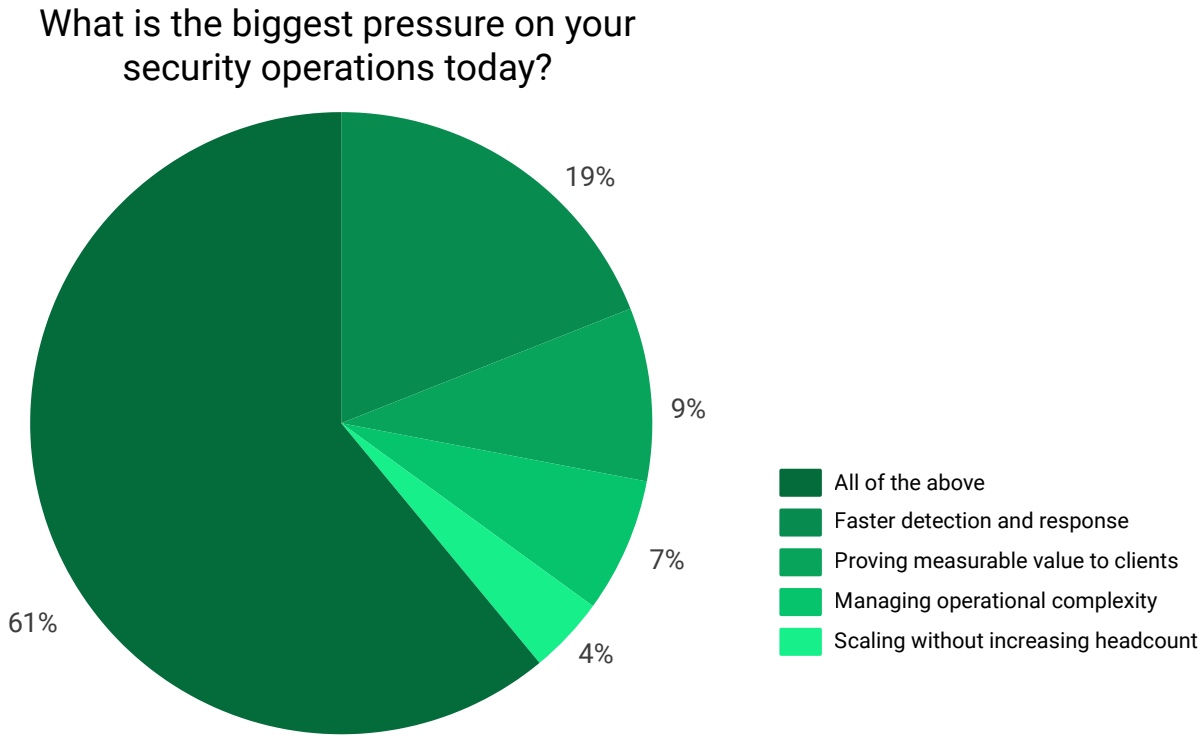
Bridging the Gap Between Emerging AI Threats and Operational Reality

Overview: Why This Pulse Matters Now

Between Q2 and Q3 2026, Seceon expanded its live channel polling program to reach a respondent base five times larger than the original program, capturing real-time reactions from MSPs, MSSPs, and security operations professionals across a significantly broader footprint of global channel and industry events. Individual polls drew up to 1,430 respondents, reflecting the deeper live-audience engagement generated as the program grew, reflecting the deeper live-audience engagement generated as the program grew and giving this edition of the Pulse Report a substantially larger statistical base than the original Q2–Q3 2026 run.

The picture that emerges is consistent, and arguably sharper at this scale: AI has moved from a future threat to a present one, identity has become the fastest-moving battleground on both offense and defense, and operational drag from too many dashboards and too much manual work continues to slow providers down even as client expectations rise.

When asked directly what pressures their security operations most, 61% of respondents polled on this question chose "all of the above" over any single factor: faster detection, proving value, managing complexity, or scaling without headcount growth. That result frames everything that follows: providers are not fighting one battle in 2026; they are fighting all of them simultaneously.

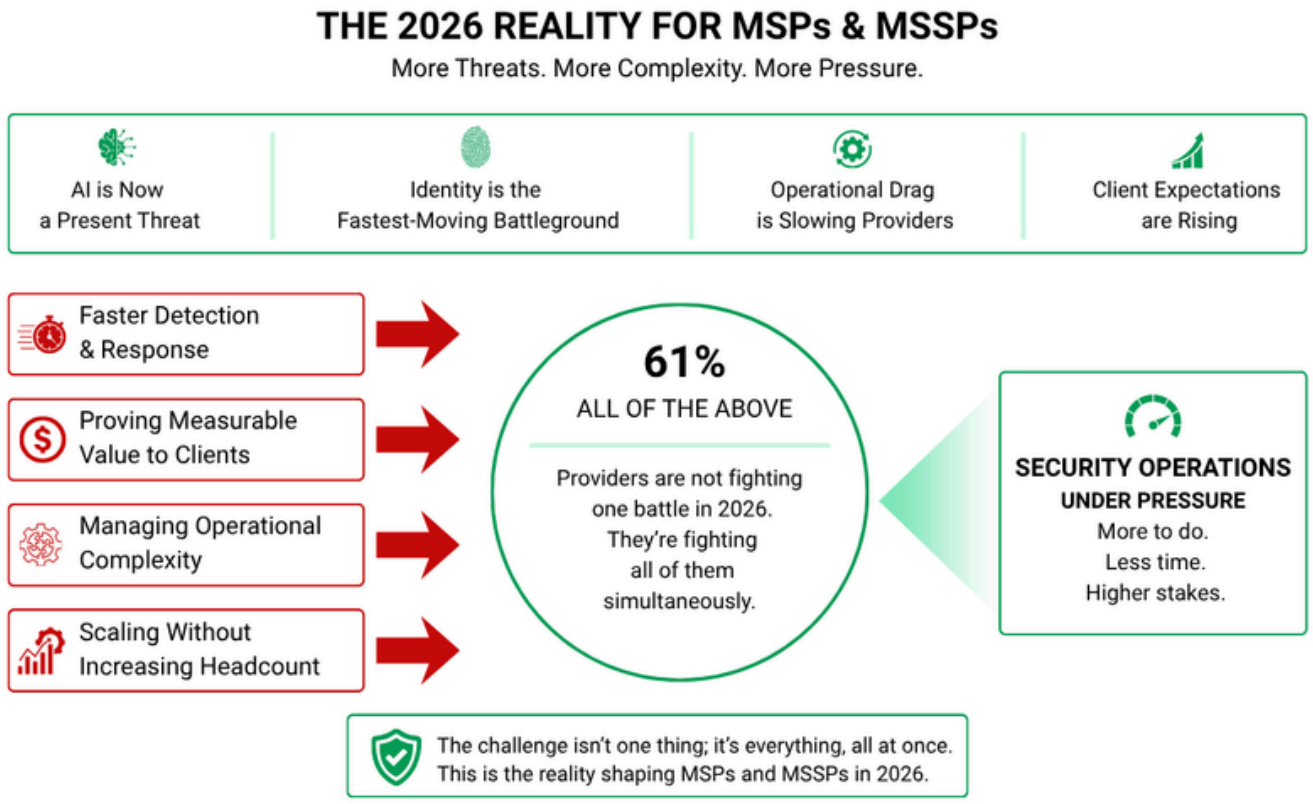


Why This Matters for MSPs and MSSPs Right Now

Today's threat landscape is defined less by any single exploit than by scale and speed: AI-generated phishing has become commoditized, nation-state operators (Salt Typhoon, Volt Typhoon) have shown a willingness to live inside telecom and critical-infrastructure networks for months at a time, and campaigns like APT10's historic 'Cloud Hopper' operation remain the clearest reminder that MSPs and MSSPs themselves are a preferred path into hundreds of downstream customers at once. A single compromised provider can become the blast radius for an entire client base which is exactly why this report's findings on identity, tool sprawl, and AI-readiness matter as much to a provider's own security posture as to what it sells.

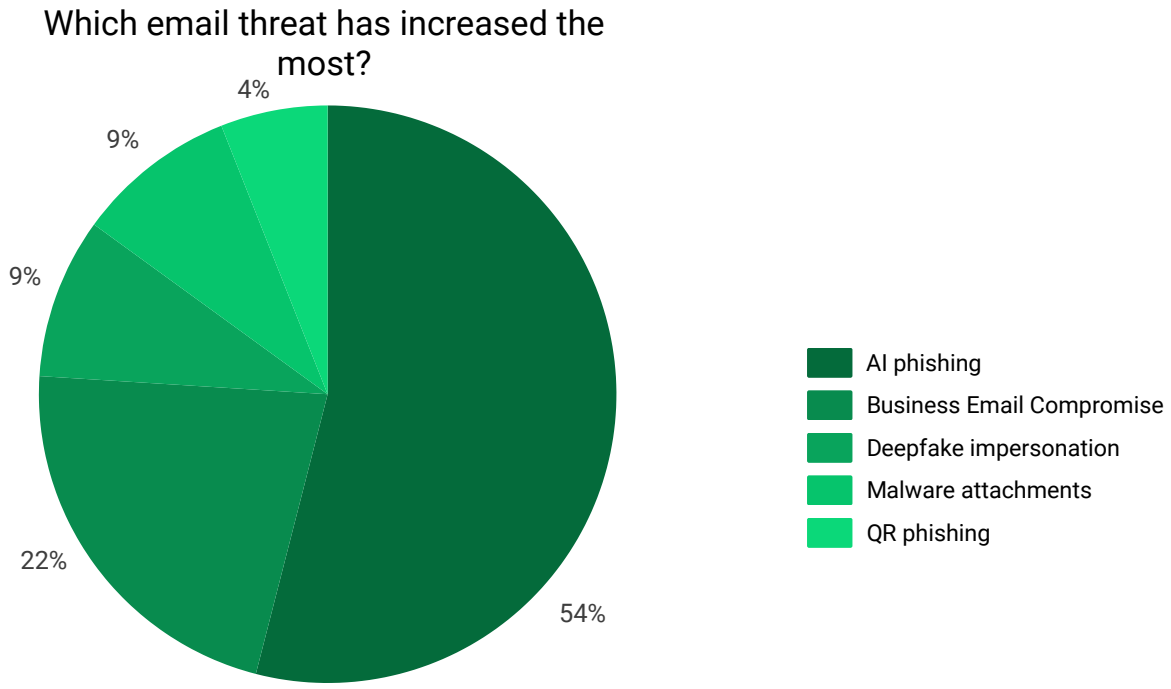
"This journey has fundamentally changed our business from delivering projects to delivering continuous business outcomes.
Today, with Seceon's AI-driven platform, we get unified visibility, intelligent threat detection, automated correlation, and faster incident response."

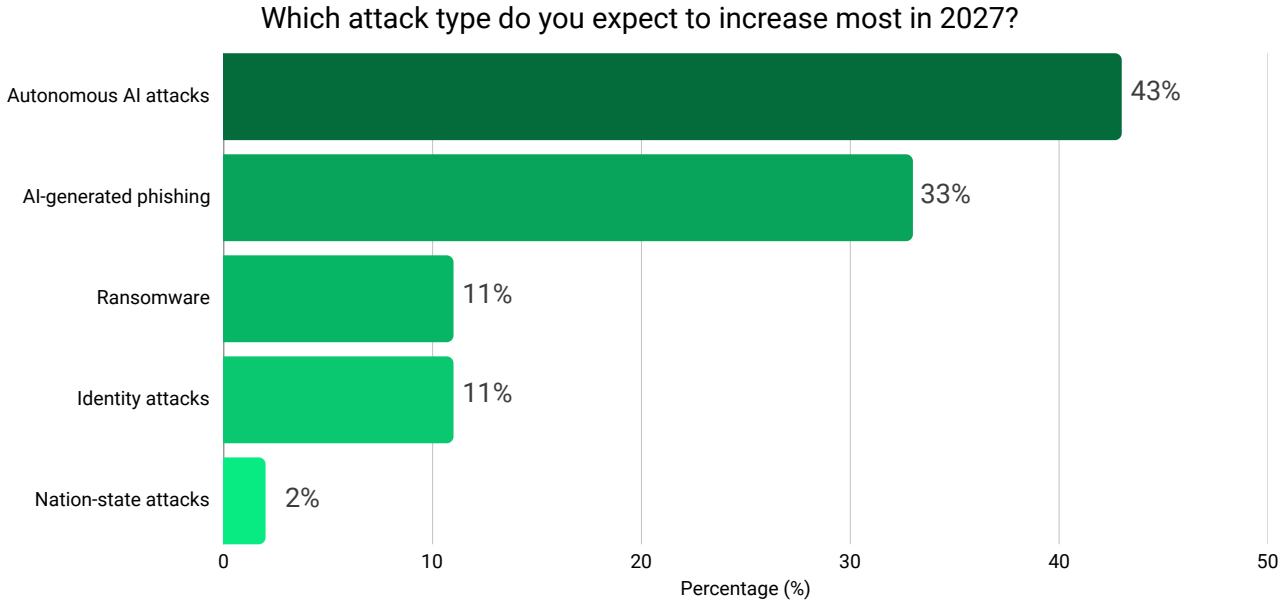
— **Atul Gosar (Network Tech Labs)**



Finding 1: AI Phishing Leads Today: Autonomous AI Attacks Are the Threat of Tomorrow

54% of respondents said AI-generated phishing is the email threat that has increased the most this year, more than double the next closest category (Business Email Compromise, 22%). But looking ahead, the picture shifts: 43% expect autonomous AI attacks, not phishing to be the fastest-growing attack type in 2027, with AI-generated phishing dropping to second place at 33%.





Context: Phishing has always been the entry point providers watch most closely, and AI has clearly supercharged it with more convincing language, faster targeting, and higher volume. The open question has been whether that trend continues, or whether something more advanced takes over.

Survey result: Respondents believe the threat landscape is about to shift categories entirely. Today's dominant threat (AI phishing) is expected to be overtaken by a fundamentally different one: autonomous, self-directed AI attacks that don't rely on a human clicking a link.

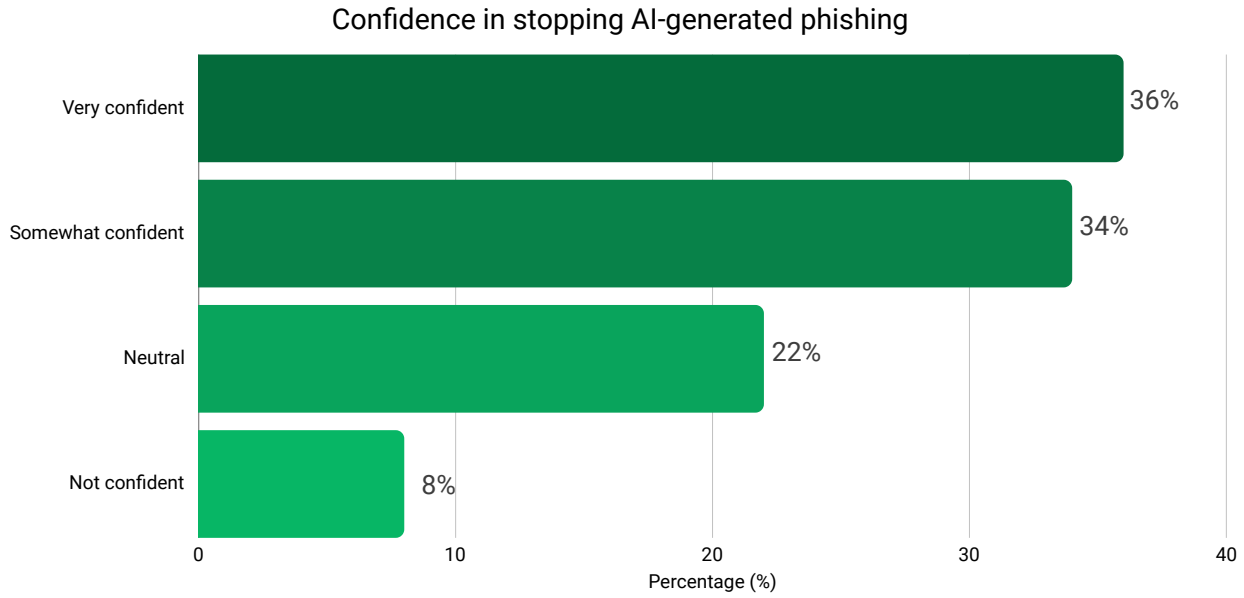
What this suggests globally: Providers who build their 2026 roadmap purely around better phishing filters and email security may already be building for the wrong fight by 2027. The channel is signaling a transition from AI-assisted attacks (a human using AI as a tool) to AI-driven attacks (an AI acting with limited human involvement).

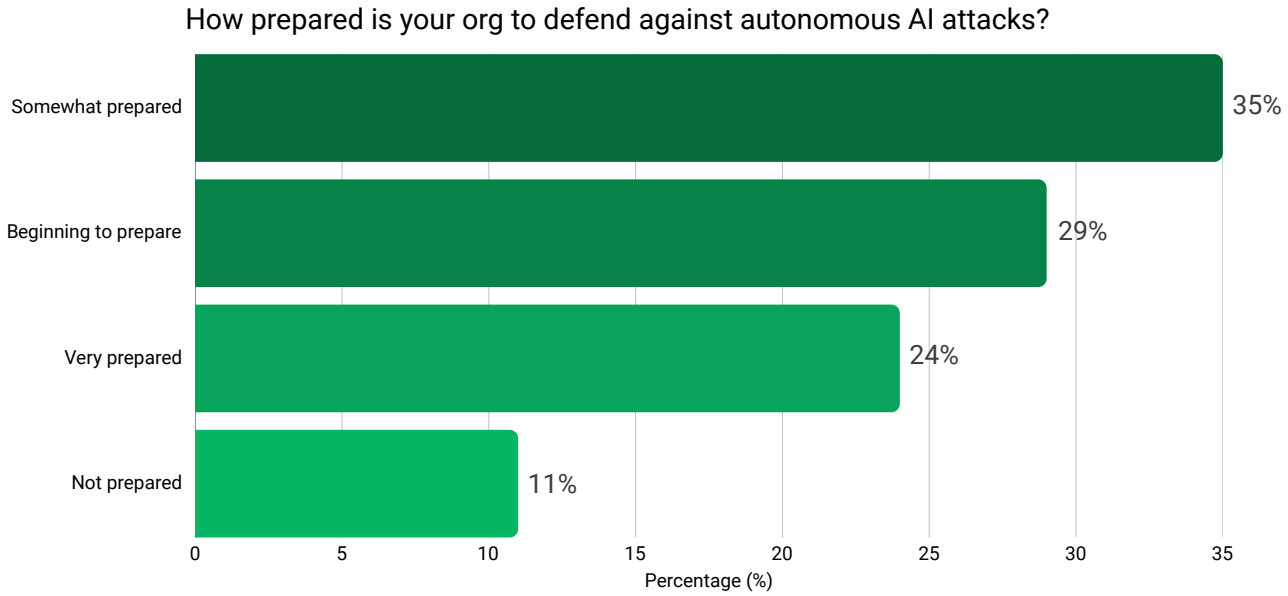
How providers can win: Treat phishing defense as table stakes, not the finish line. Seceon's Dynamic Threat Models (DTM), the self-adjusting AI/ML correlation engine at the core of aiSIEM and aiXDR-PMax, already build the behavioral baselining and 30-day stateful risk memory that autonomous, non-signature attacks require. Pairing DTM's machine-speed correlation with aiSOAR 4.0's sub-90-second automated response gives providers a head start on autonomous threat detection now, while attack volume is still low enough to build and test against.

> *"If you have an attacker which is AI-driven, we should have a detection that is intelligent as well, and that's where Seceon stands out. The Seceon detection and correlation engine is actually utilizing a dynamic threat model powered by ML, which can help not only to detect well-known attacks but also advanced attacks, zero-day attacks, including ransomware attacks where attacker methods keep changing.*
>
> — **Pratik Patil (TechFirst Gulf)**

Finding 2: Confidence Against Known Threats Doesn't Extend to What's Coming Next

70% of respondents said they are very or somewhat confident in stopping AI-generated phishing (36% very confident, 34% somewhat confident). But when asked about a related, forward-looking threat autonomous AI attacks only 24% said they are "very prepared," while 29% are still "beginning to prepare" and 11% report not being prepared at all.





Context: Confidence and preparedness are often treated as the same thing in vendor conversations, but this data shows they diverge sharply once the threat moves from something familiar (phishing) to something newer (autonomous attacks).

Survey result: Providers are meaningfully more confident about threats they've already spent years defending against than about the threat category they themselves expect to dominate by 2027.

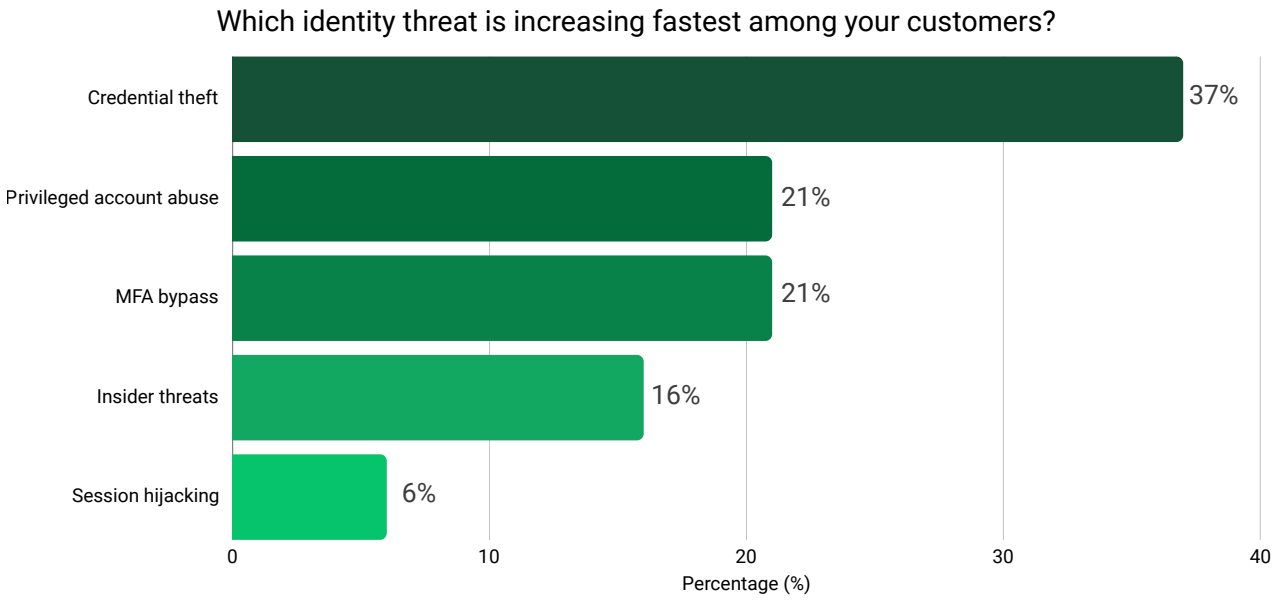
What this suggests globally: This is a readiness gap, not a confidence problem. Teams aren't in denial about autonomous AI attacks; they picked it as the top 2027 threat in Finding 1 but their operational preparation hasn't caught up to their own risk assessment yet.

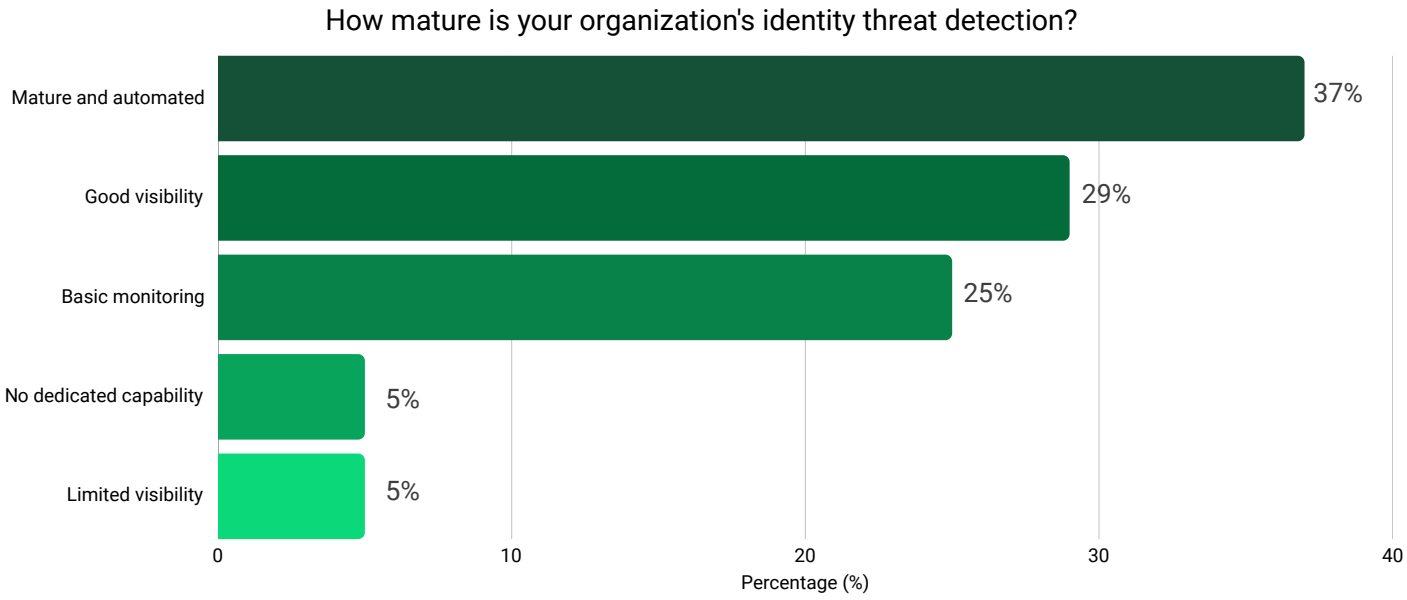
How providers can win: Close the gap before the threat matures. aiSOAR 4.0's GenAI playbook engine can stand up an autonomous-attack tabletop scenario from a natural-language prompt in about 30 seconds, and Dynamic Threat Models' Explainable AI (XAI) gives line-by-line, plain-language justification for every confidence score evidence a provider can put directly in front of a client during a QBR. Making "autonomous-attack readiness" a named, XAI-backed line item in roadmaps closes the credibility gap along with the technical one.

> *"The organizations that are going to win from a cybersecurity perspective are not going to be the ones that have the most AI on the slide when they present it to customers. It's going to be the ones that think about pairing AI with governance, telemetry, and response."*
>
> — **Joshua Skeens (CEO, Logically)**

Finding 3: Identity Is the Fastest-Growing Risk and the Fastest-Growing Defense

37% of respondents say credential theft is the identity threat increasing fastest among their customers, ahead of MFA bypass and privileged account abuse (21% each). Meanwhile, 66% describe their identity threat detection as either "mature and automated" (37%) or having "good visibility" (29%).





Context: Identity has been called the "new perimeter" for several years now. This data tests whether that's still marketing language or an operational reality reflected in where attacks and investment are actually concentrated.

Survey result: Identity shows up as a major area of concern and investment, with credential theft identified as the fastest-growing identity threat and a majority of providers reporting real maturity in identity threat detection, not just intent.

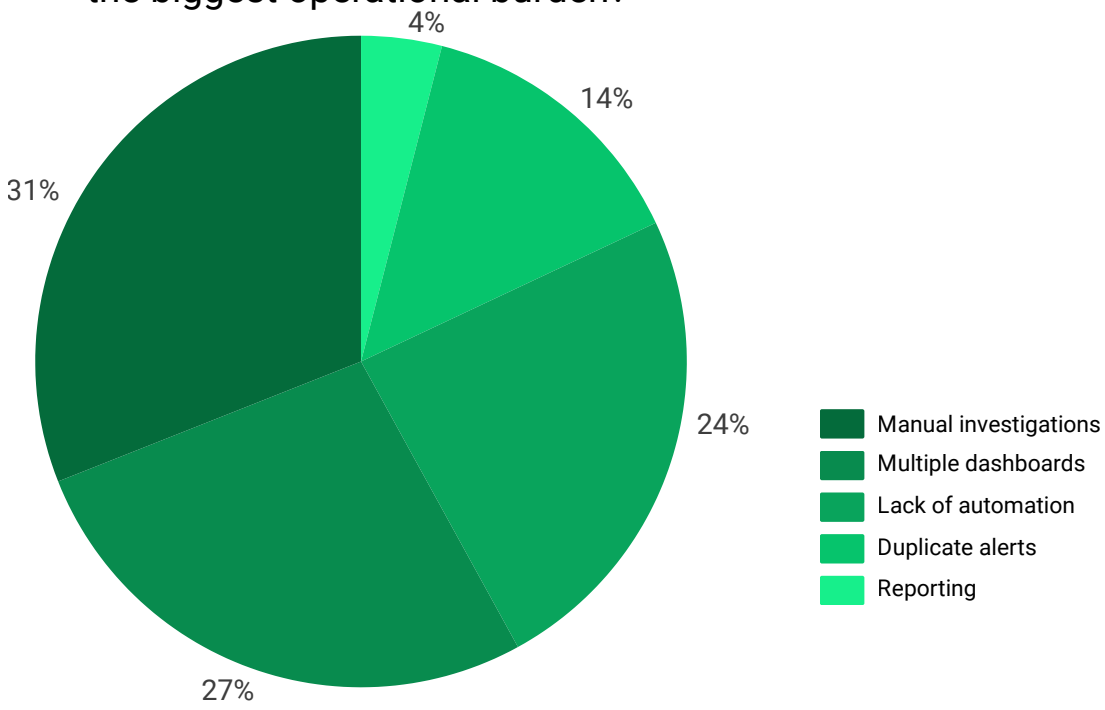
What this suggests globally: The market has largely absorbed the "identity is the new perimeter" message and is acting on it. The next differentiator won't be whether a provider covers identity at all, but whether identity telemetry is correlated with endpoint, cloud, and network signals or sitting in its own silo. As 2026 closes, that question increasingly extends beyond human identities to machine and AI-agent identities as well, which now need the same lifecycle governance as a human user account.

How providers can win: Don't sell identity security as a standalone module. Seceon's aiIDGuard/aiITDR module feeds directly into aiTRiSM360's Unified Identity Intelligence Graph, correlating credential, privilege, and behavioral signals for human, machine, and increasingly relevant AI-agent identities directly into aiSIEM and aiXDR detection and aiSOAR response workflows, so identity events trigger action, not just alerts.

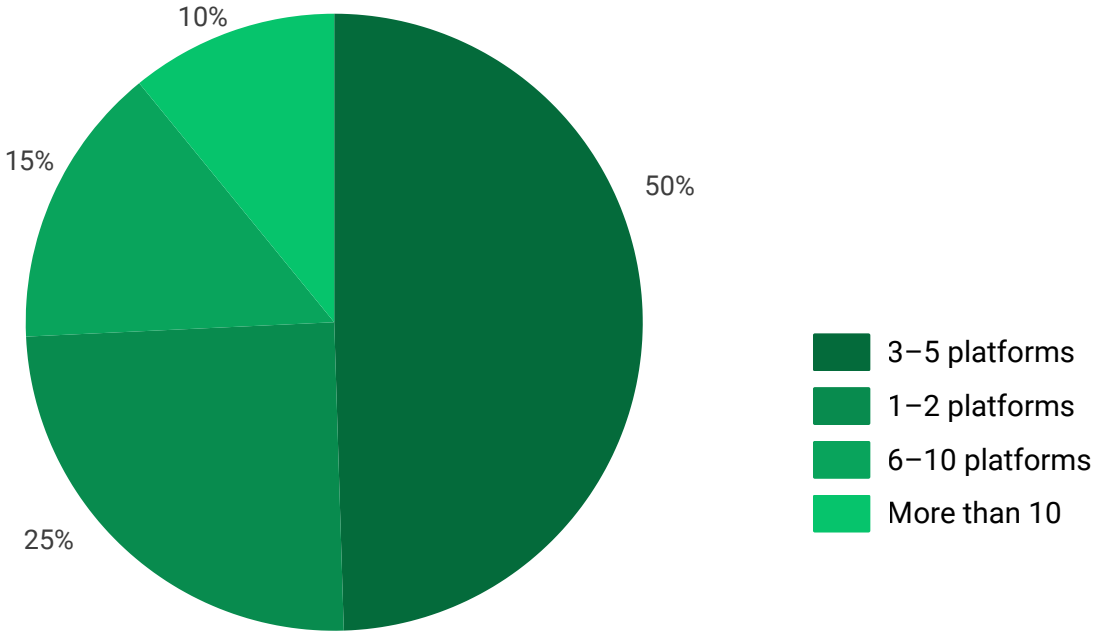
Finding 4: Tool Sprawl Still Defines the Operational Burden

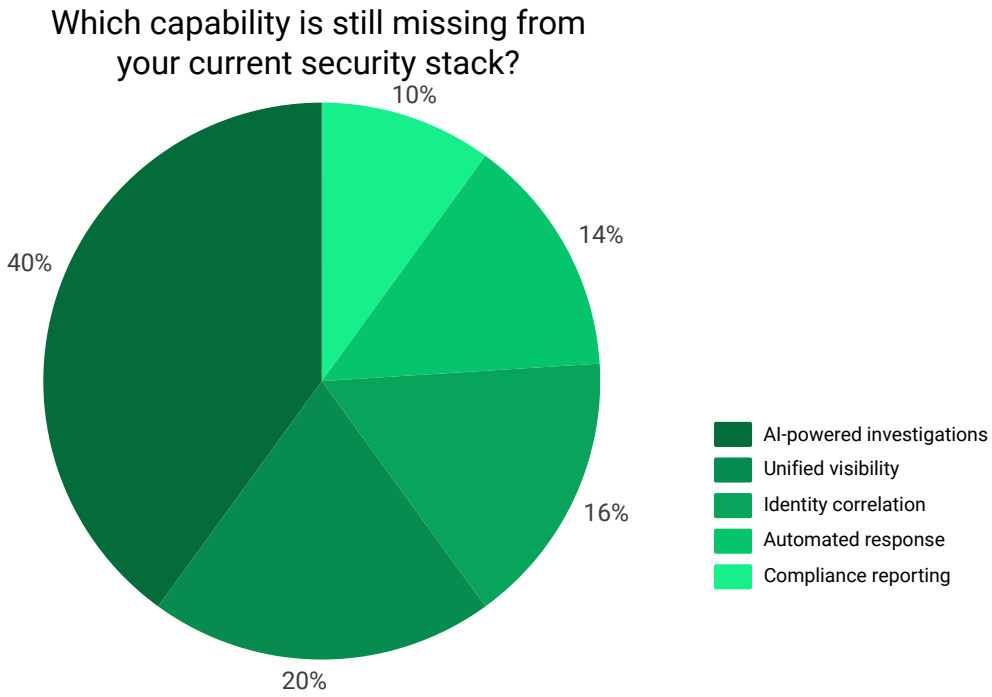
31% of respondents point to manual investigations as the integration challenge causing the biggest operational burden, followed closely by multiple dashboards (27%) and lack of automation (24%). Consistent with that, 50% of SOCs run 3–5 primary security platforms, and 25% run 6 or more. When asked what is still missing from their stack, 40% said AI-powered investigations, making it the largest response by far.

Which integration challenge causes the biggest operational burden?



How many primary security platforms does your SOC rely on today?





Context: Tool sprawl has been a known problem in the MSP/MSSP world for years, but this data pinpoints exactly where the pain shows up day-to-day: not in buying too many tools, but in the manual work required to stitch their outputs together.

Survey result: The complaint isn't platform count in isolation; it's what platform count forces analysts to do manually. "AI-powered investigations" being the single largest capability gap confirms the bottleneck sits at correlation and analysis, not data collection.

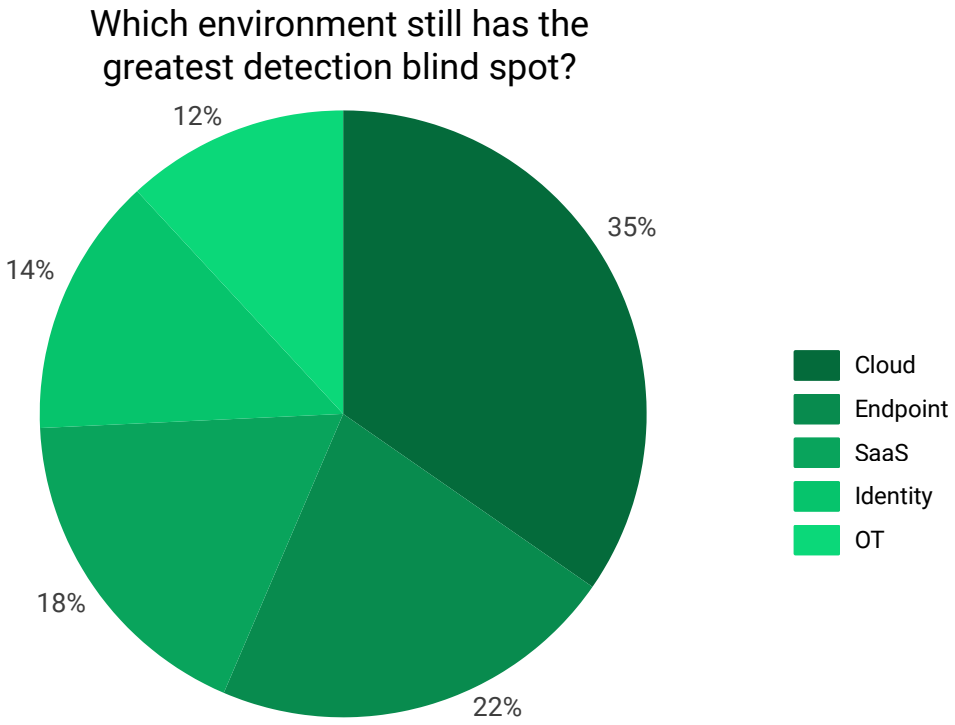
What this suggests globally: Providers have largely solved the "can we collect the telemetry" problem. What they haven't solved is turning that telemetry into a conclusion an analyst can act on without manually cross-referencing multiple dashboards.

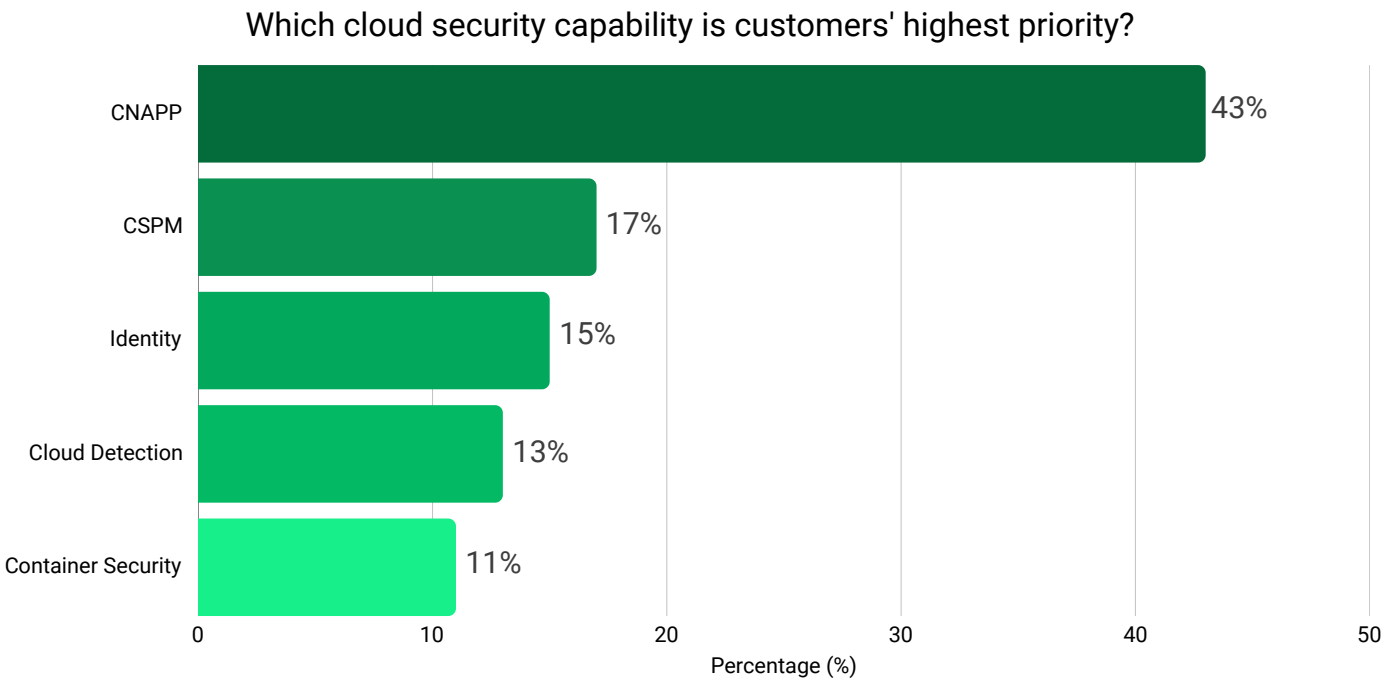
How providers can win: Prioritize AI-assisted investigation and correlation over adding another point solution. This is precisely what Seceon's unified Seceon Event Format (SEF) and SeraAI co-pilot are built for: because every data source normalizes into one schema instead of being reconciled after the fact across siloed tools, SeraAI can reason across identity, endpoint, cloud, and network telemetry in a single workflow, collapsing five dashboards' worth of manual cross-referencing into one AI-assisted investigation, drawing on Seceon's library of 4,000+ pre-trained ML models rather than a single generic model.

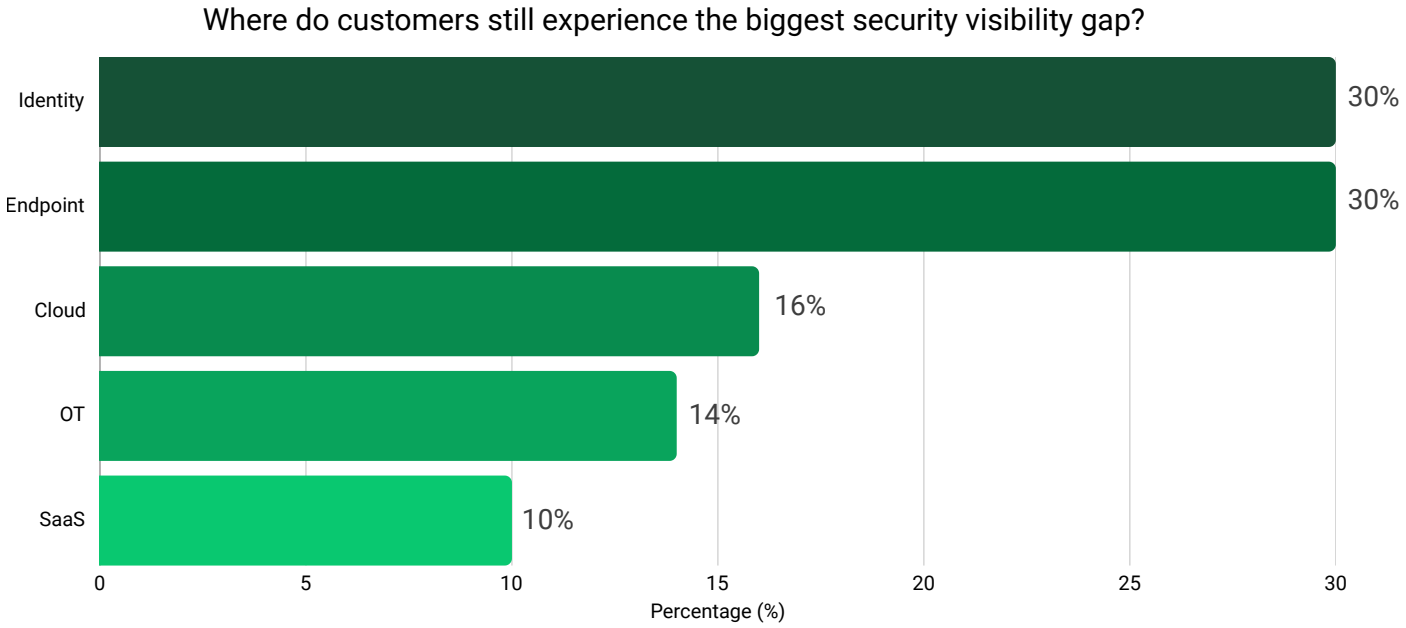
> *"One solution, one vision, one output. Output is continuous, comprehensive cyber resilience. This is the uniqueness of Seceon, wherein they come up with everything everything together."*
>
> — **Gitesh Shah (Samay Infosolutions)**

Finding 5: Cloud Remains the Most Persistent Detection Blind Spot

35% of respondents identify cloud as the environment with the greatest detection blind spot, ahead of endpoint (22%), SaaS (18%), identity (14%), and OT (12%). On priorities within cloud security specifically, CNAPP leads decisively at 43%. Interestingly, when asked where customers themselves report the biggest visibility gap, endpoint and identity tie for the top spot (30% each), with cloud lower at 16%.




Which cloud security capability is customers' highest priority?
CNAPP
CSPM
Identity
Cloud Detection
Container Security
43%
17%
15%
13%
11%
0
10
20
30
40
50
Percentage (%)


Where do customers still experience the biggest security visibility gap?
Identity
Endpoint
Cloud
OT
SaaS
30%
30%
16%
14%
10%
0
5
10
15
20
25
30
Percentage (%)

Context: Detection blind spots and customer-reported visibility gaps are two different lenses on the same problem; one is the provider's technical assessment, and the other is what customers say out loud. Comparing them surfaces where perception and reality diverge.

Survey result: Providers rate cloud as their toughest detection blind spot by a wide margin, but customers themselves are more vocal about endpoint and identity gaps. That gap between technical assessment and customer perception is itself a finding.

What this suggests globally: Customers may not yet perceive cloud exposure as their most urgent visibility gap, since it does not appear in their day-to-day complaints as often as endpoint or identity issues.

How providers can win: Don't wait for customers to ask about cloud visibility; they largely aren't. Lead QBR conversations with cloud detection findings proactively. Seceon's CNAPP suite includes CSPM and Cloud Detection & Response, which are available today, while KSPM, CWPP, CIEM, and DSPM are rolling out through the remainder of 2026. Together, these capabilities feed cloud posture and runtime findings directly into aiSIEM, so cloud risk shows up alongside identity and endpoint risk in the same console rather than requiring a separate cloud-security conversation.

"Cybersecurity is not just solving IT problems; it's a business resilience challenge. Working with a lot of partners, such as Seceon, has been a great partner over the past couple of months... We have actually onboarded Seceon as a strategic partner."

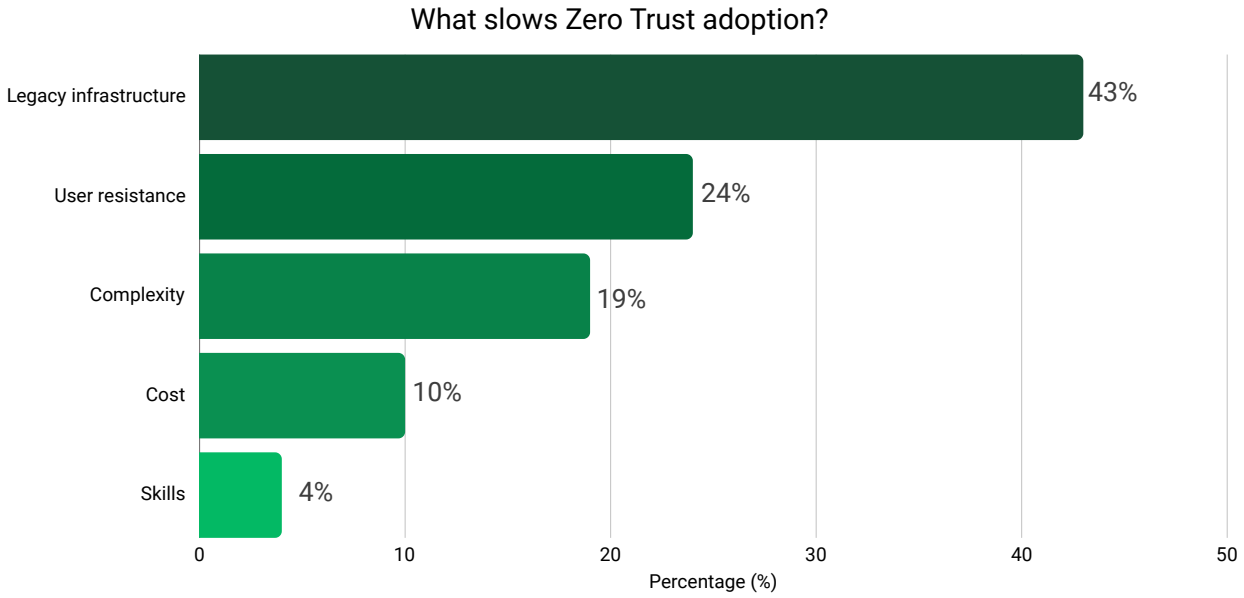
— **Atul Gupta (BlackBox)**

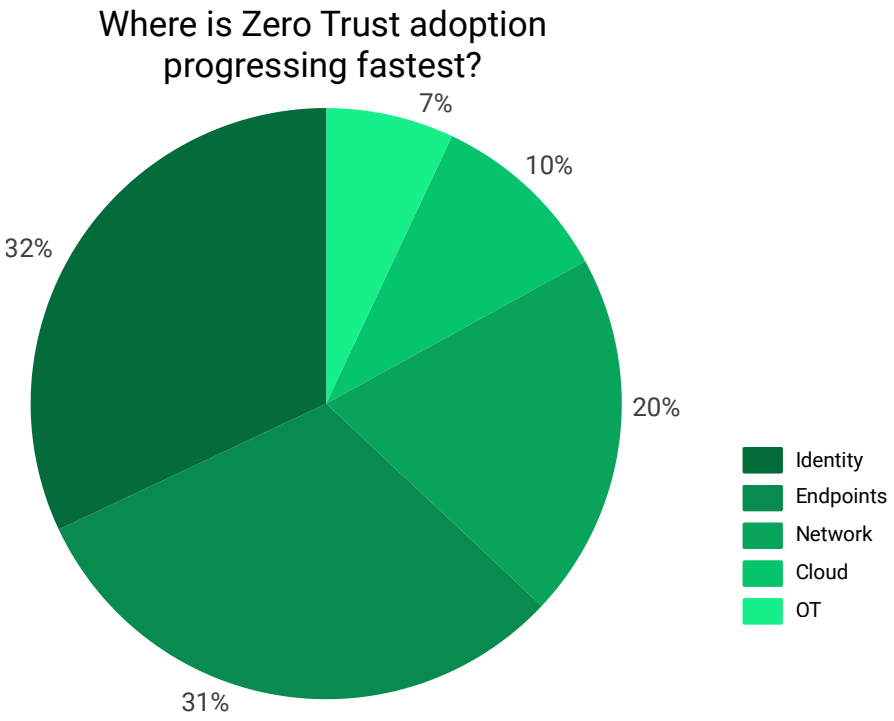
"If someone asks me, what is that one thing that you find in Seceon that you stick to Seceon over the years... one thing tops the charts. Second is innovative. Seceon is a company that you can reach out to, that you need this feature."

— **Sunday McDickson Samuel (SMSAM System Ltd.)**

Finding 6: Zero Trust Is Advancing in Identity, Stalling on Legacy Infrastructure

43% of respondents say legacy infrastructure is what slows Zero Trust adoption the most, more than double the next factor, user resistance (24%). At the same time, 32% say Zero Trust adoption is progressing fastest in identity. Together, these results reveal a clear pattern: Zero Trust is advancing most quickly in identity while legacy infrastructure remains its biggest barrier.





Context: Zero Trust is frequently discussed as a strategy or philosophy, but adoption is ultimately gated by concrete technical and organizational constraints, not willingness.

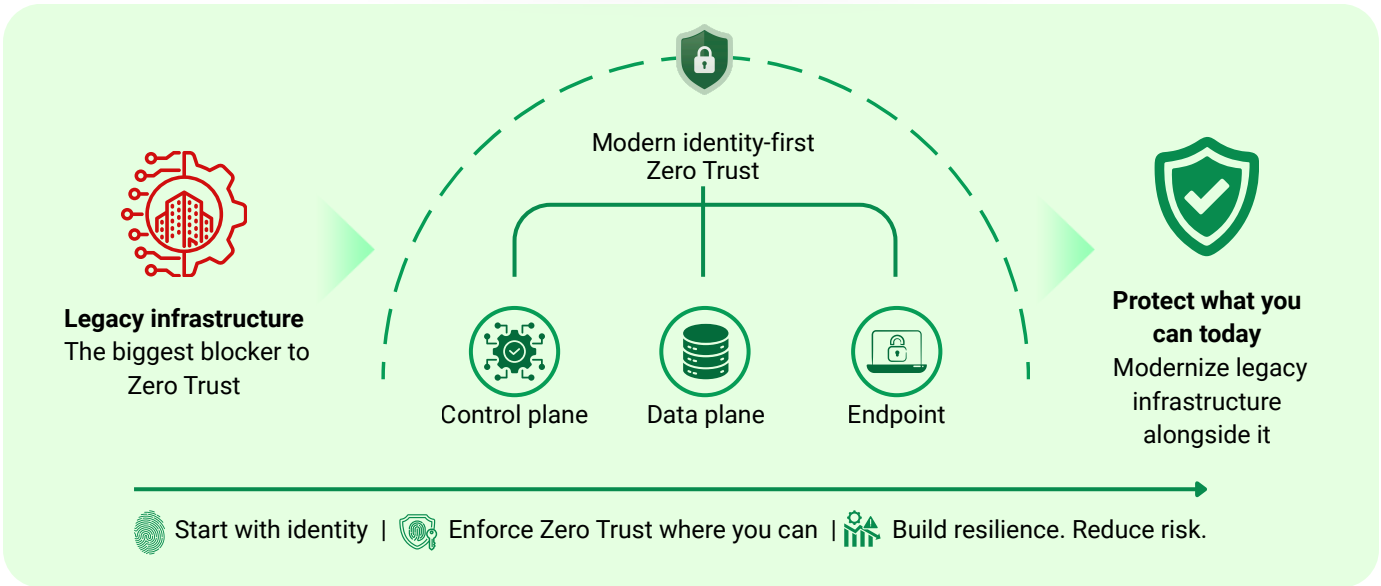
Survey result: Legacy infrastructure is, by a wide margin, the single biggest drag on Zero Trust adoption, well ahead of cost, skills, or complexity, which are often assumed to be the bigger barriers.

What this suggests globally: Zero Trust roadmaps that assume a greenfield environment will keep underdelivering. The real project for most providers is running a modern identity-first Zero Trust model alongside infrastructure that wasn't built for it.

How providers can win: Sequence Zero Trust rollouts around what's achievable now. Seceon's Zero Trust Access architecture separates policy decisions (Control Plane) from local enforcement (Data Plane and Endpoint Agent) so that no traffic is ever hairpinned through a cloud point of presence, meaning providers can extend risk-adaptive access control to identity and endpoints today, while building an explicit, funded plan for legacy infrastructure modernization rather than treating it as a blocker to work around indefinitely.

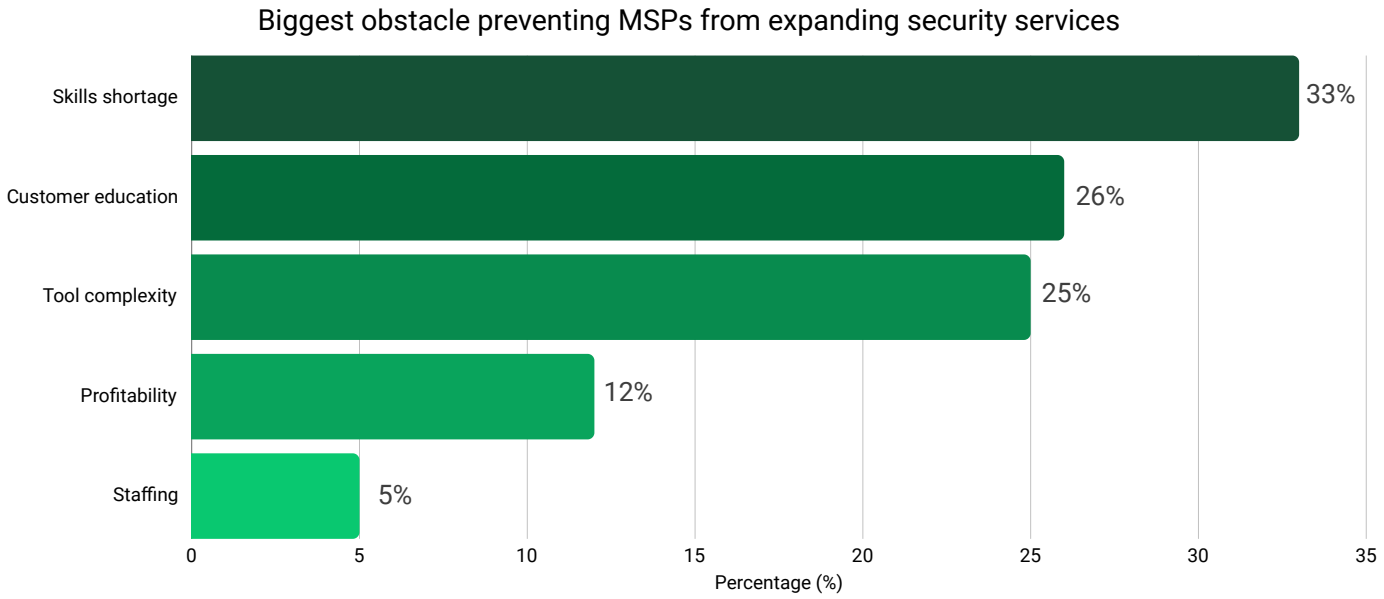
"Most players can give you a platform, but creating multiple playbooks user-friendly playbooks where anyone can create one without deep cybersecurity experience is where most people face the challenge. And this is the differentiator from the Seceon side: how we are supporting those customers."

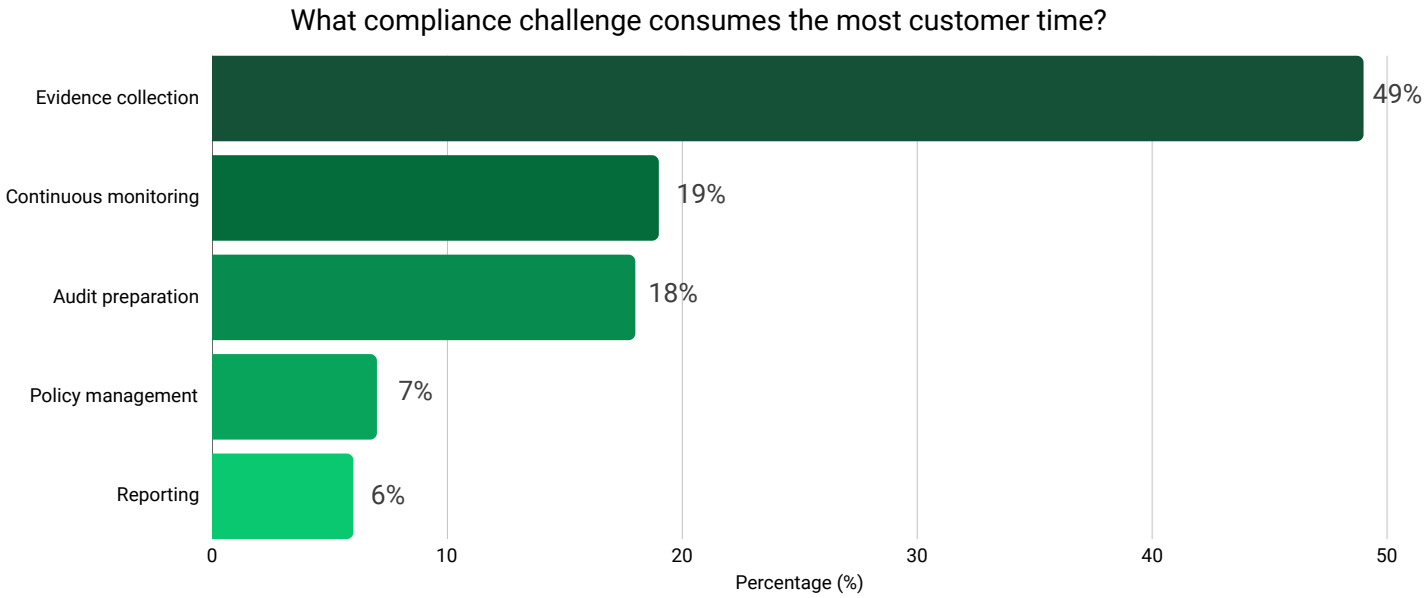
— **Kunal Panchamia (eProtect 360)**

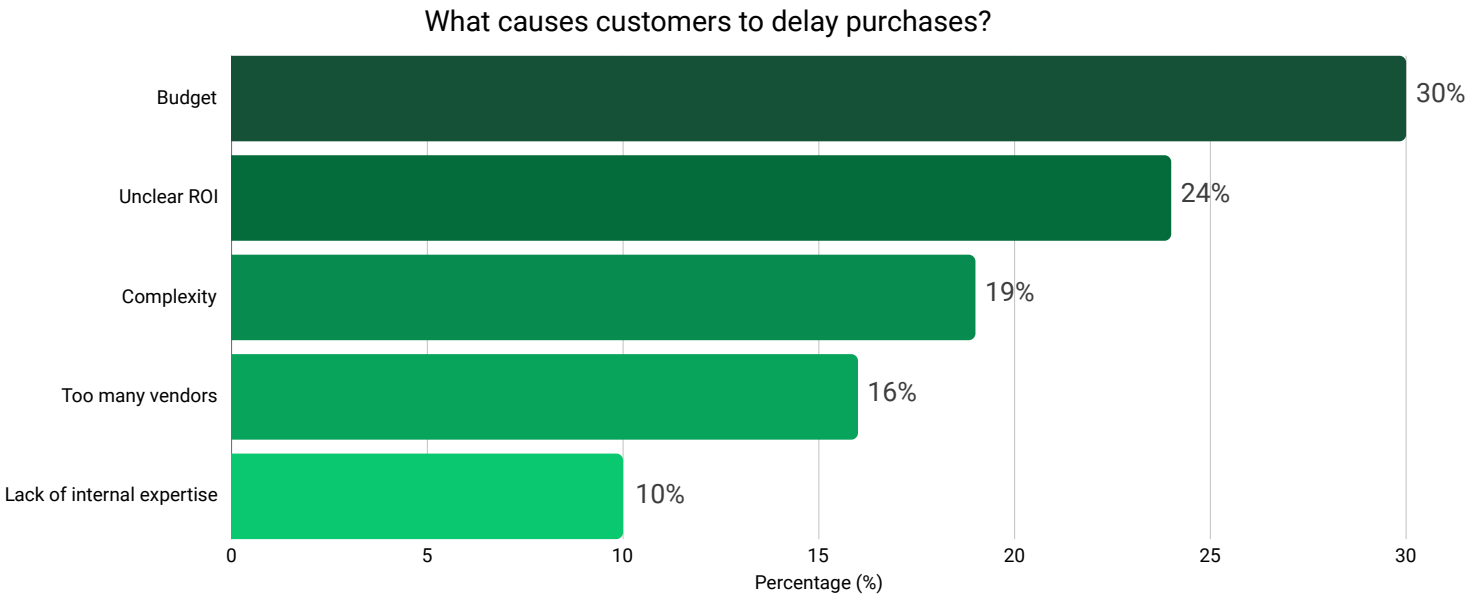


Finding 7: Compliance and Growth Friction: What Actually Slows MSPs Down

33% cite skills shortage as the biggest obstacle preventing MSPs from expanding security services, with customer education (26%) and tool complexity (25%) close behind. Within compliance work specifically, 49% say evidence collection consumes the most customer time far more than reporting or audit preparation. And on the sales side, budget (30%) and unclear ROI (24%) are the top reasons customers delay purchases.







Context: Growth friction shows up in three places for most providers: internal capacity (skills), operational drag (compliance busywork), and the sales cycle itself (why deals stall). This finding looks at all three together.

Survey result: Evidence collection alone eats up roughly half of the time customers spend on compliance — a manual, repetitive task that's a natural automation target. Meanwhile, unclear ROI is nearly as large a purchase blocker as budget itself.

What this suggests globally: A meaningful share of "we don't have budget" objections are really "we don't yet see the ROI clearly enough to prioritize budget for it" objections. Fixing the ROI story may unlock more deals than fixing the price.

How providers can win: Automate evidence collection first among compliance tasks; it's the single biggest time sink and the easiest to quantify in a business case. Seceon's CMX360 compliance module automates evidence gathering across 40+ regulatory frameworks. This kind of workflow has taken audit preparation from two to four weeks down to a couple of hours in Seceon deployments, creating a concrete, numbers-based ROI narrative to pair with every proposal.

"In the third year with Seceon, we've managed to achieve the highest level in the private sector a 100% successful certification with the National Cybersecurity Authority. The audit didn't only test the solution as a technology or the SOC as operations, but rather the whole process and concept of a security operations center."

— Yazeed Alshehri (TopNet, Saudi Arabia)

"CMX360 can be viewed as a force multiplier, not a replacement for governance. Its value comes from reducing low-value manual effort while making evidence, ownership, exceptions, and compliance decisions more transparent."

— Joshua A. Ward (Obviam)

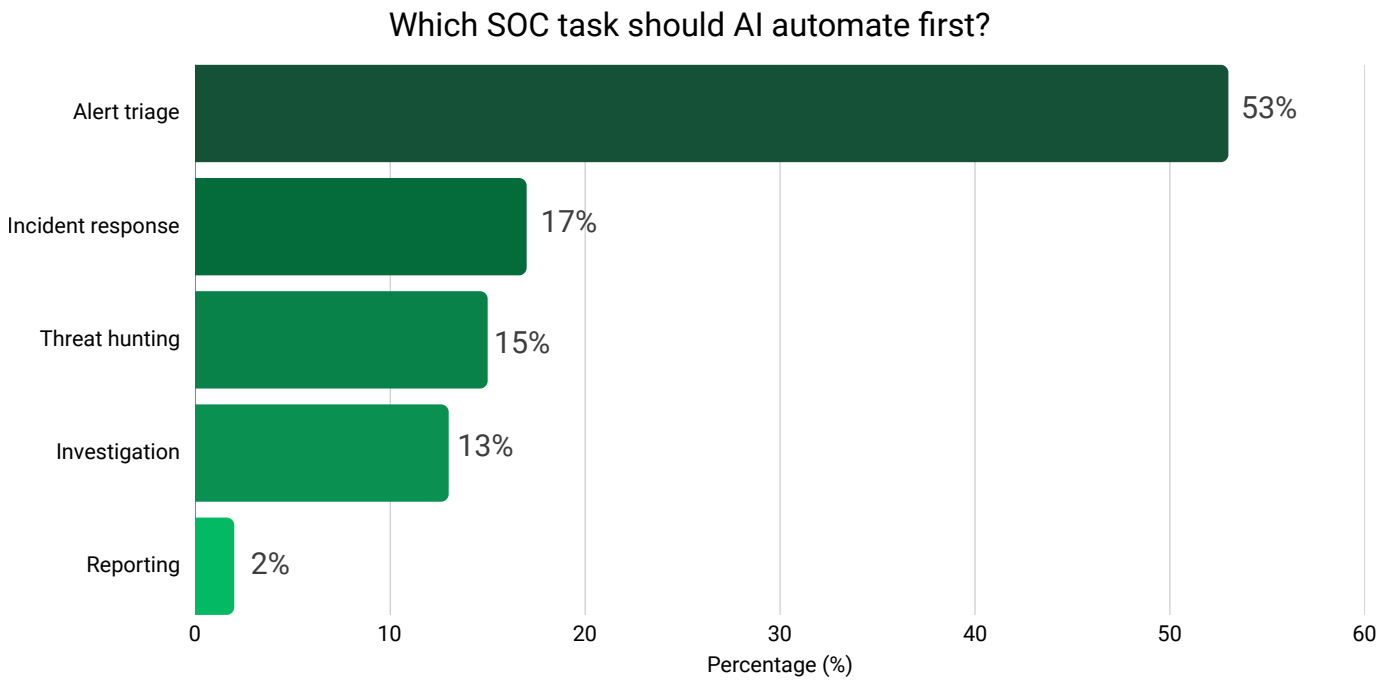
Finding 8: AI Is Now Both the Automation Priority and a New Security Risk

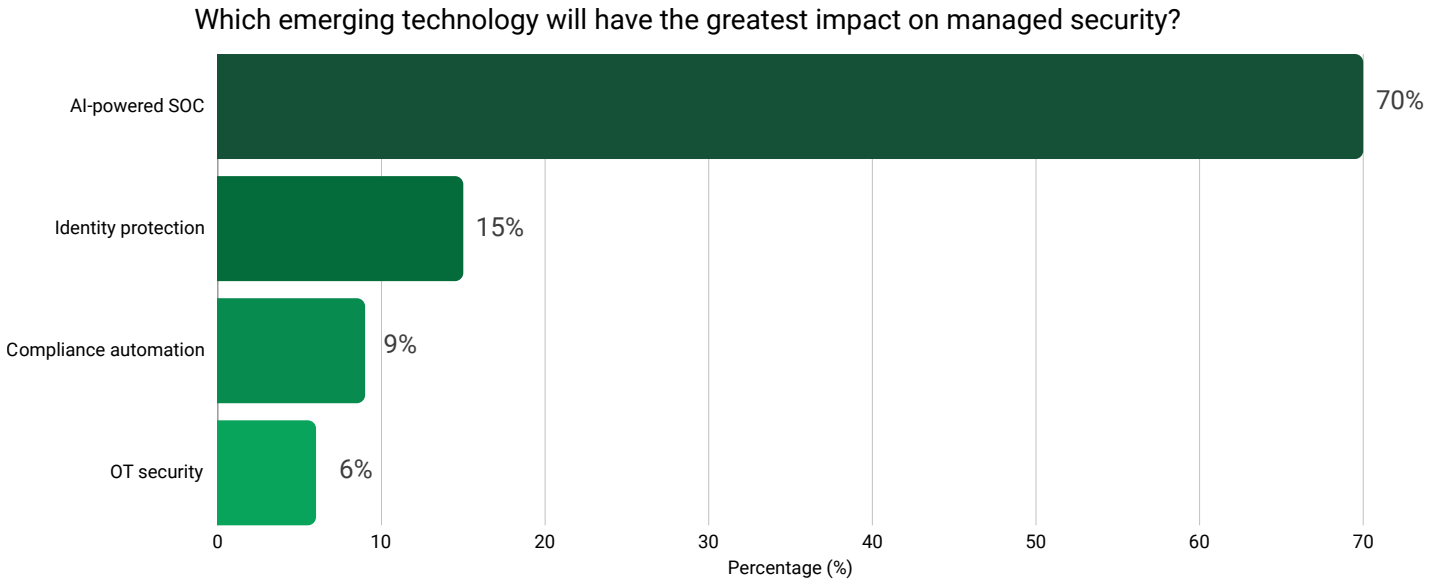
53% of respondents say alert triage is the SOC task AI should automate first, well ahead of incident response (17%) and threat hunting (15%). 70% believe an AI-powered SOC will be the emerging technology with the greatest impact on managed security, while 73% say customers will invest first in AI-powered detection and response over the next 12 months.

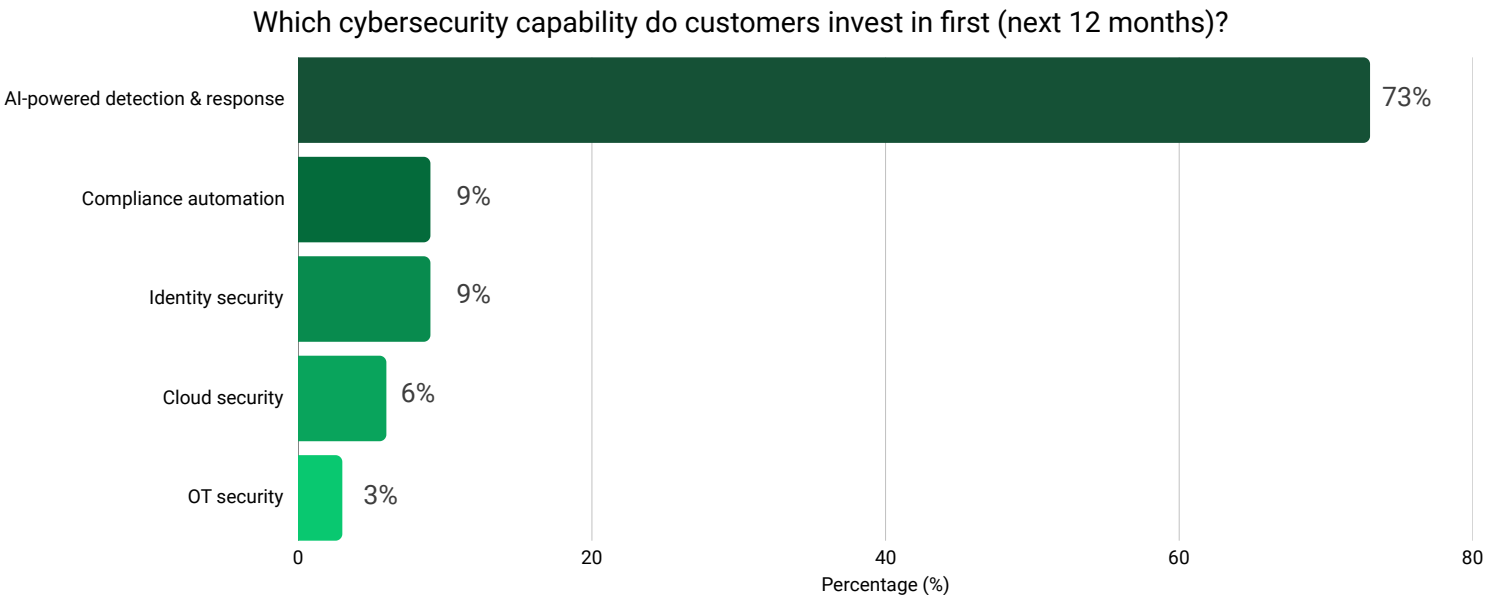
But the AI shift is not only about using AI to improve security operations. AI itself is becoming a new attack surface. Shadow AI, AI-based attacks, and techniques such as prompt injection against AI systems and AI modules are creating security risks that traditional security controls were not designed to address.

This makes AI trust, risk, and security management an increasingly critical part of the security stack. As organizations deploy more AI across their environments, providers need visibility into what AI is being used, how it is behaving, what data it can access, and whether it can be manipulated or abused.

This is the shift behind **aiTRiSM**: security cannot simply use AI to defend the organization; it must also secure the AI itself.







Context: By Q3 2026, the question for most providers isn't whether to invest in AI-driven security operations; it's where to point that investment first for the fastest return.

Survey result: The consensus is unusually strong across three separate questions: alert triage as the first automation target, AI-powered SOC as the biggest technology shift, and AI-powered detection & response as customers' top investment priority. Three different angles on the same question, and the same answer wins every time.

What this suggests globally: AI in the SOC has moved past the differentiation stage into the expectation stage, consistent with the broader 2026 finding that AI-driven operations are now assumed by buyers, not evaluated as optional add-ons.

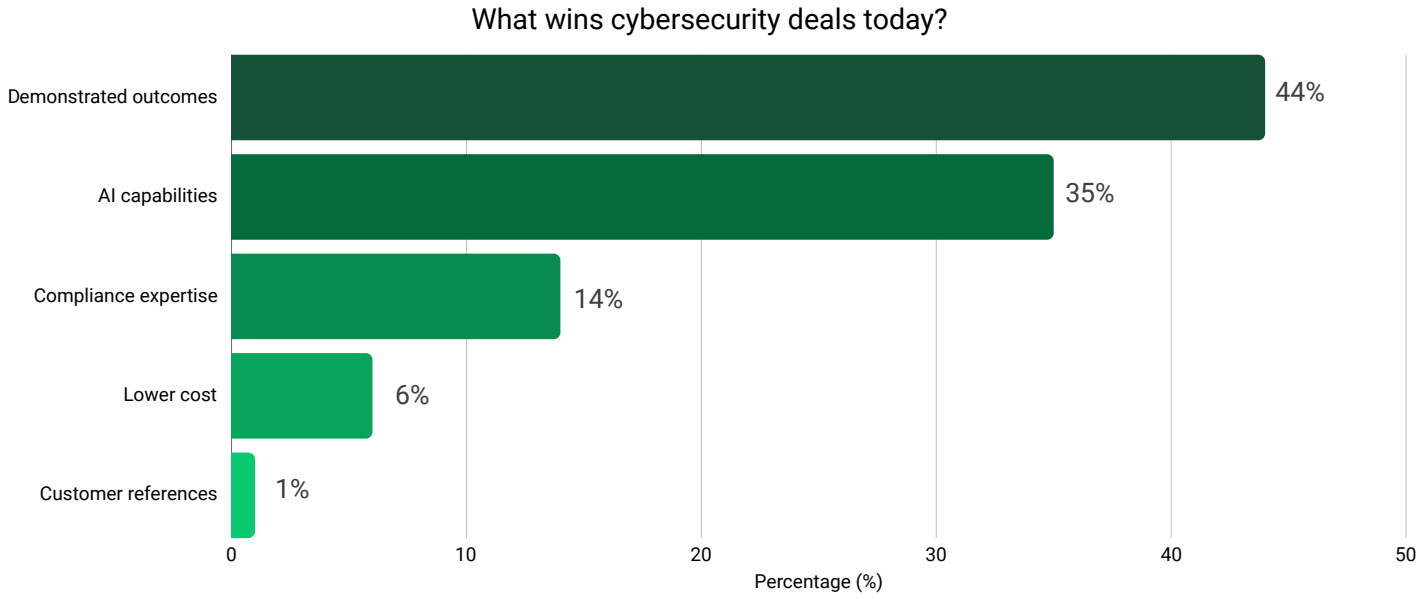
How providers can win: Start automation investment at alert triage, the task with the clearest consensus and the most immediate workload relief for analysts. Seceon's aiSOAR 4.0 already resolves more than 70% of incidents without analyst intervention and can generate a new automated playbook from a natural-language description in about 30 seconds, then build outward toward investigation and response rather than trying to automate everything simultaneously.

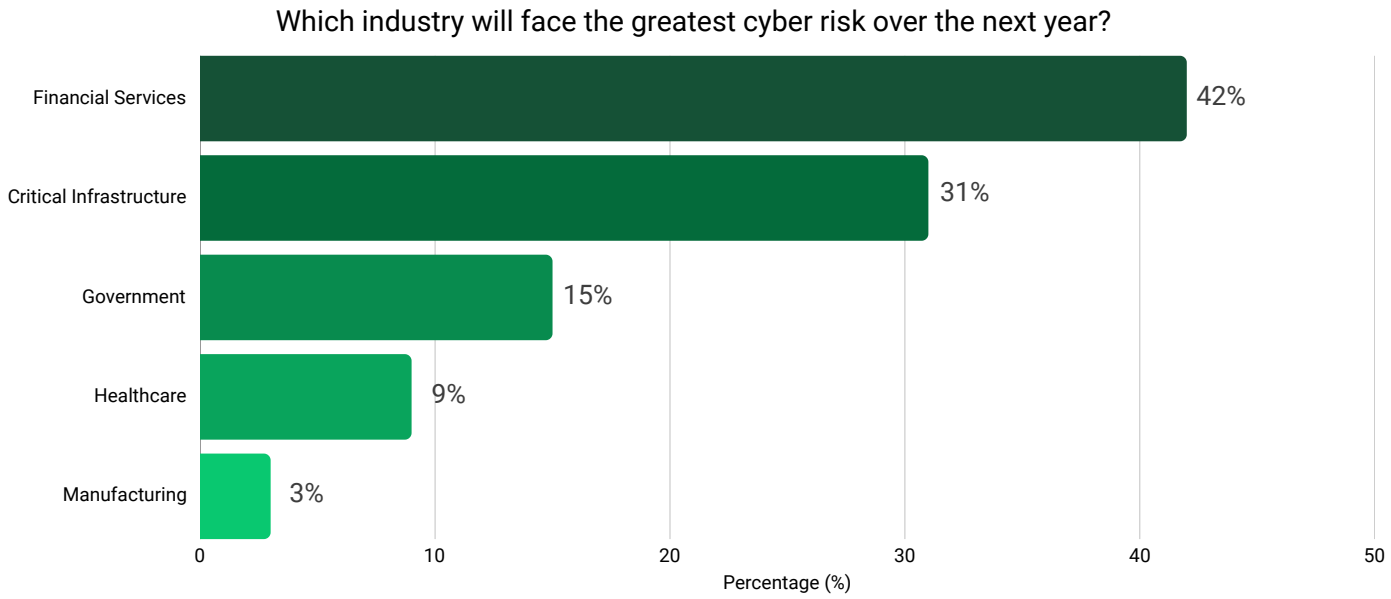
"It's a joint decision between the electrical teams, the instrumentation teams, the multiple device owners, and the multiple OEMs; somebody has to really sit down and take a conscious call. I think Seceon is able to read those protocols well, parse those protocols well, and make meaningful outcomes."

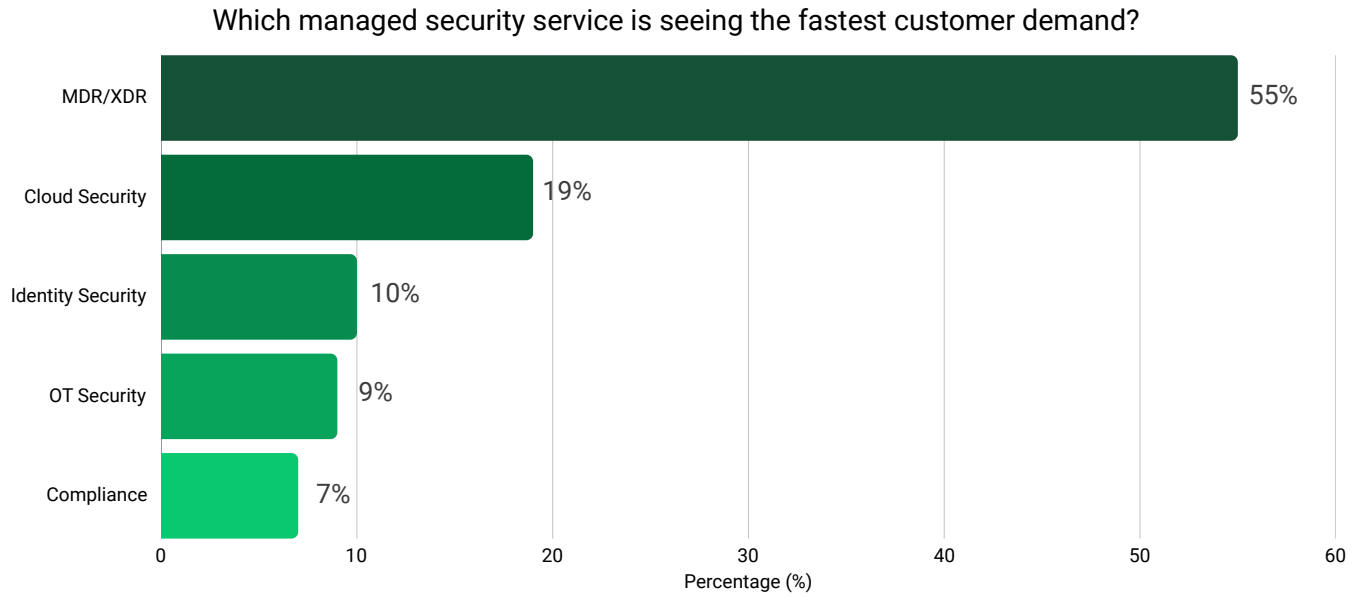
— **Prianshu Khandwala (Nayara Energy)**

Finding 9: What Wins Deals and Where the Risk Concentrates

44% say demonstrated outcomes are what wins cybersecurity deals today, with AI capabilities close behind at 35%, together accounting for nearly 8 in 10 answers, well ahead of lower cost (6%) or compliance expertise (14%). On risk concentration, 42% believe financial services will face the greatest cyber risk over the next year, followed by critical infrastructure (31%). And on service demand, MDR/XDR leads decisively at 55%, more than all other managed services combined.




Which industry will face the greatest cyber risk over the next year?
Financial Services
Critical Infrastructure
Government
Healthcare
Manufacturing
42%
31%
15%
9%
3%
0
10
20
30
40
50
Percentage (%)


Which managed security service is seeing the fastest customer demand?
MDR/XDR
Cloud Security
Identity Security
OT Security
Compliance
55%
19%
10%
9%
7%
0
10
20
30
40
50
60
Percentage (%)

Context: Understanding what wins deals, where risk is concentrated, and which services are in demand together shape where a provider should focus go-to-market energy in the second half of 2026.

Survey result: The data shows that demonstrated outcomes beat price as a deal-winner by a wide margin, echoing the broader market shift from tool-count selling to outcome-based selling. MDR/XDR's dominance in service demand confirms buyers want a managed outcome, not just a monitoring layer.

What this suggests globally: Financial services and critical infrastructure account for nearly three-quarters of perceived risk concentration between them, suggesting providers serving those verticals should expect the highest scrutiny and can justify the strongest outcome-based pricing.

How providers can win: Lead sales conversations with proof, not price. Case studies, live demos, and quantified outcomes outperform cost arguments by a wide margin. For providers serving financial services or critical infrastructure clients, Seceon's aiMSSP tooling and Master–Tenant multi-tenant (MT-MT) architecture position MDR/XDR as the anchor service, with purpose-built SWIFT/wire-fraud detection for banking and native OT/ICS protocol monitoring (aiSecOT360) for critical infrastructure both fast-growing categories and strong fits for the highest-risk verticals.

> *"With Seceon, we are getting all the automation automatic event correlation, behavior analysis, significant reduction of false positives, and the automation response capability. These things are very, very important for us. That's where Seceon is doing very, very well, and we are really proud to be part of this partnership."*
>
> — **Seydou Sidibe (3R Technologie)**

Conclusion: What This Expanded Pulse Tells Us

Taken together, these nine findings, now drawn from a live-polling base five times larger than the original Q2–Q3 2026 run, describe a market in a fast transition, not a stable one. AI has already reshaped the threat that dominates today (phishing) and is expected to reshape it again within a year (autonomous attacks). Identity is simultaneously one of the fastest-growing threat areas and the biggest Zero Trust success story. And the operational bottleneck for most providers has shifted from "can we see the data" to "can we act on the data fast enough."

A few clear priorities emerge for the second half of 2026:

- Build autonomous-attack readiness now, before it becomes the dominant threat category that respondents already forecast it will be, using behavioral baselining and Explainable AI, not just phishing filters.
- Correlate identity signals, including machine and AI-agent identities, into detection and response workflows rather than treating it as a standalone product.
- Automate investigation and alert triage first; this is where AI investment shows the fastest, most consensus-backed payoff.
- Lead with cloud visibility proactively, since customers report it less often than providers identify it as a major detection blind spot.
- Sell outcomes and proof over price. By a wide margin, that is what actually wins deals in this market.

Seceon's Open Threat Management (OTM) Platform is built for exactly this shift. Rather than a stack assembled through acquisition, OTM natively unifies aiSIEM, aiXDR-PMax, aiSOAR 4.0, aiIDGuard/aiITDR, aiTRiSM360, the emerging CNAPP suite, Zero Trust Access, CMX360 compliance automation, TI360 threat intelligence, aiSecOT360 for OT/ICS, and the SeraAI co-pilot, all sharing one data format (SEF) and one AI/ML correlation core (Dynamic Threat Models). For MSPs and MSSPs navigating a threat landscape that is moving from AI-assisted to AI-driven, that native unification, rather than another point tool, is what turns manual investigation into automated, provable outcomes.

"We succeed only when our partners grow, because their growth is our growth. Our partners' confidence inspires us to push the boundaries of what's possible, and enables us to empower organizations to always stay one step ahead of threats."

— **Chandra Pandey, CEO, Seceon**

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI- and ML-powered aiSIEM and aiXDR platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

A Note on Methodology

This expanded edition reflects live polling conducted across Seceon's Q2 and Q3 2026 channel engagements, expanded to five times the original respondent base to reflect the program's expansion across a broader footprint of global MSP/MSSP channel and industry events during the same period. Percentages are drawn directly from the underlying live-polling data, rounded to the nearest whole number, and may not sum to exactly 100% in all cases.

As with the original release, this report is intended to give MSPs, MSSPs, and security operations leaders a directional read on where the channel's attention, confidence, and investment are heading, not a substitute for organization-specific risk assessment.