seceon
SECURITY FOR EONS

Global MSP & MSSP Security Operations Outlook for 2026

What Partners Are Seeing in the Market — and How Providers Can Win



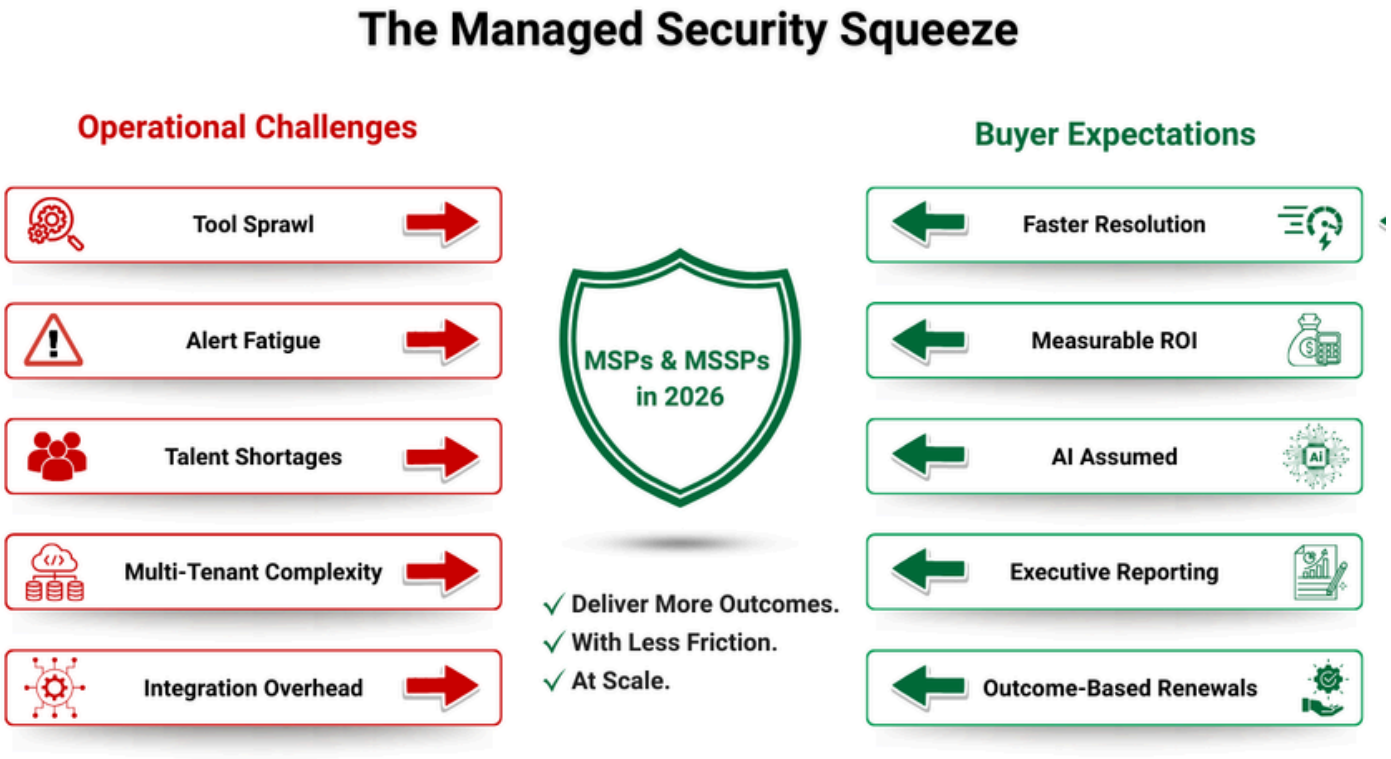
Overview: Why This Report Matters Now

Across regions and industries, MSPs and MSSPs are being asked to do more than ever before: respond faster, prove value more clearly, support increasingly complex environments, and scale services without burning out teams or margins. At the same time, buyers are more informed, more demanding, and less patient with security programs that can't clearly demonstrate impact.

A growing body of channel research has pointed to tool sprawl and alert fatigue as a structural problem for MSPs. One 2025 channel report summarized it bluntly: "Survey finds tool sprawl, false positives, and poor integration are exhausting MSP teams and increasing the risk of missed threats."[1]

Analyst research also shows that the managed security model itself is evolving toward outcomes and flexibility. An HFS Research excerpt on cybersecurity services describes a shift away from traditional SOC delivery toward "flexible, outcome-aligned MSSP delivery."[2]

Taken together, these signals reflect a market under pressure from both sides. On one end, operational complexity is straining SOC teams. On the other hand, buyers are raising expectations around measurable value, responsiveness, and business alignment. Providers are being asked not just to secure environments but to simplify them, scale them, and prove their impact.



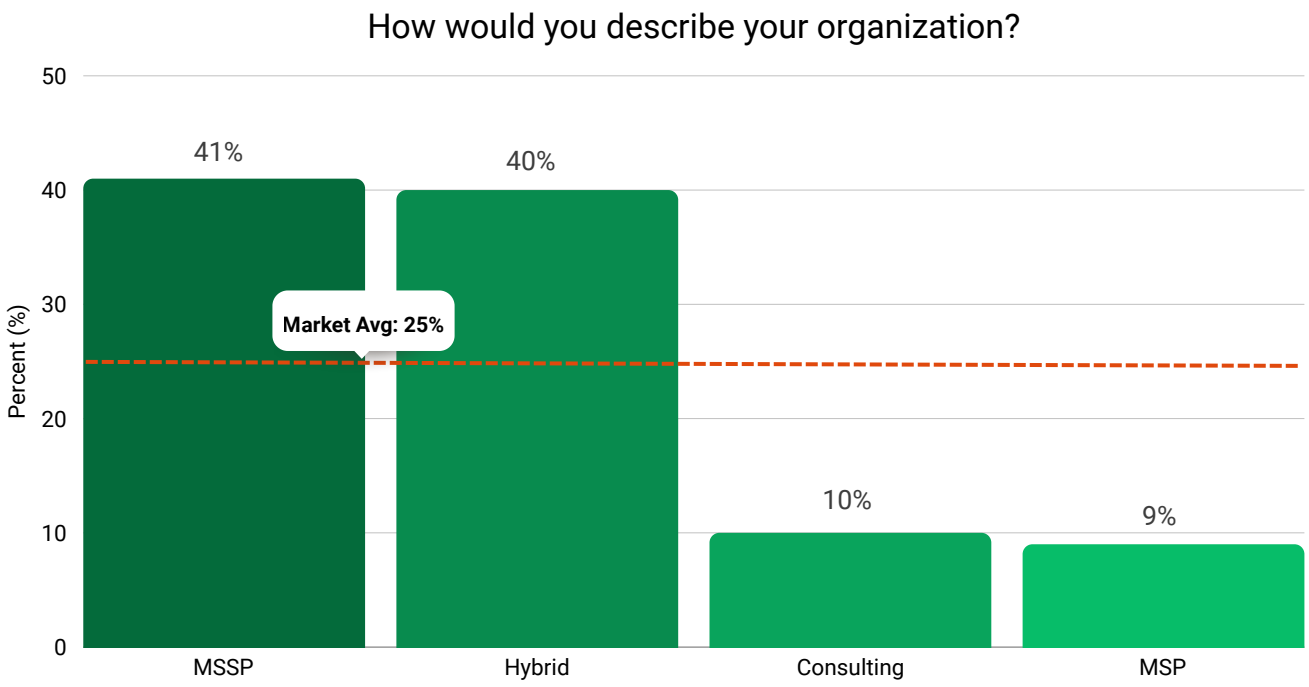
Against this backdrop, Seceon surveyed MSPs, MSSPs, and hybrid providers actively delivering managed security services around the world. The data reflects what operators, service leaders, and security teams are seeing firsthand in client conversations, not theory, not vendor positioning, but real expectations shaping buying, renewal, and expansion decisions.

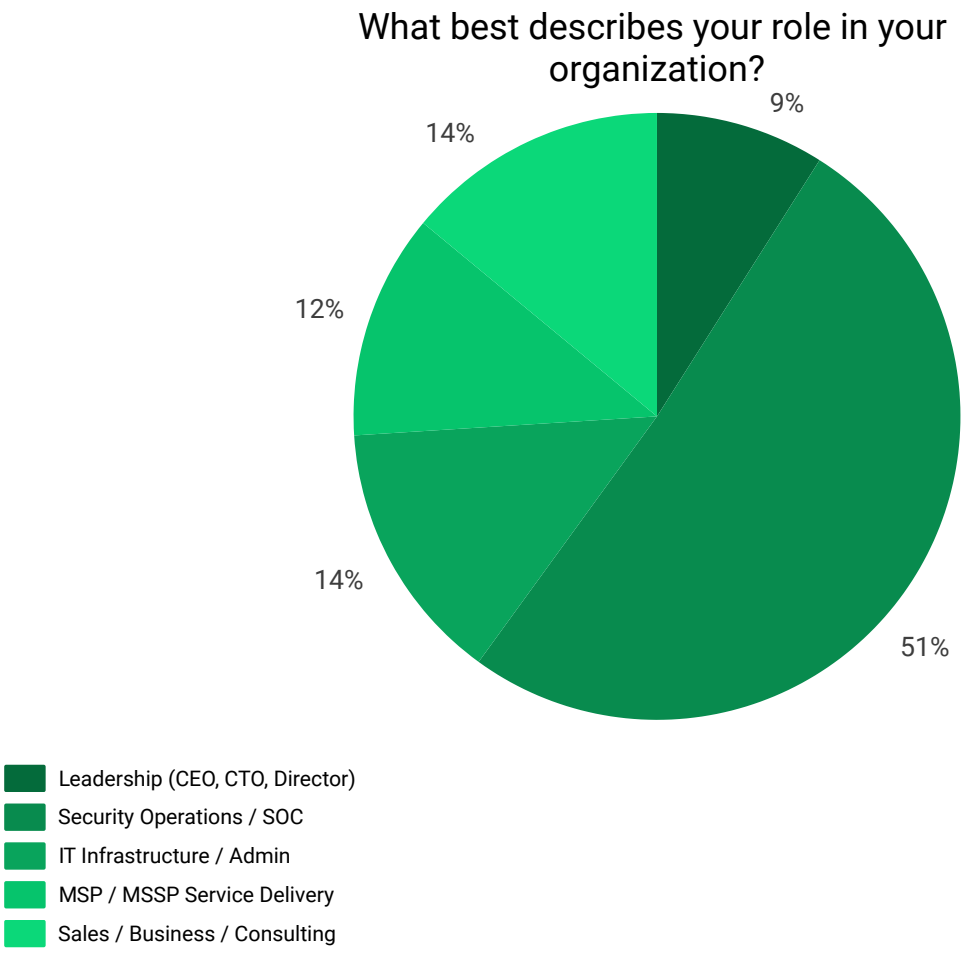
The findings point to several hard truths:

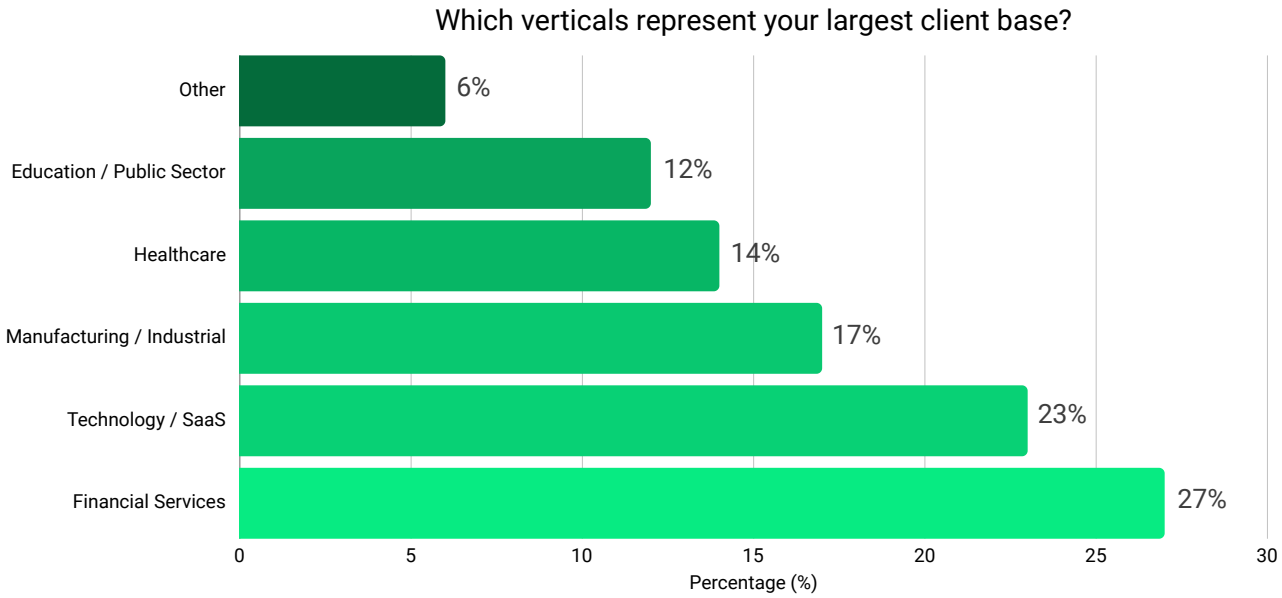
- AI and automation are no longer differentiators; they are assumed.
- Faster detection and response matter more to clients than tool lists or compliance checkboxes.
- Operational complexity and staffing pressure are hitting providers earlier than expected.
- Trust keeps clients loyal — but measurable outcomes drive growth.

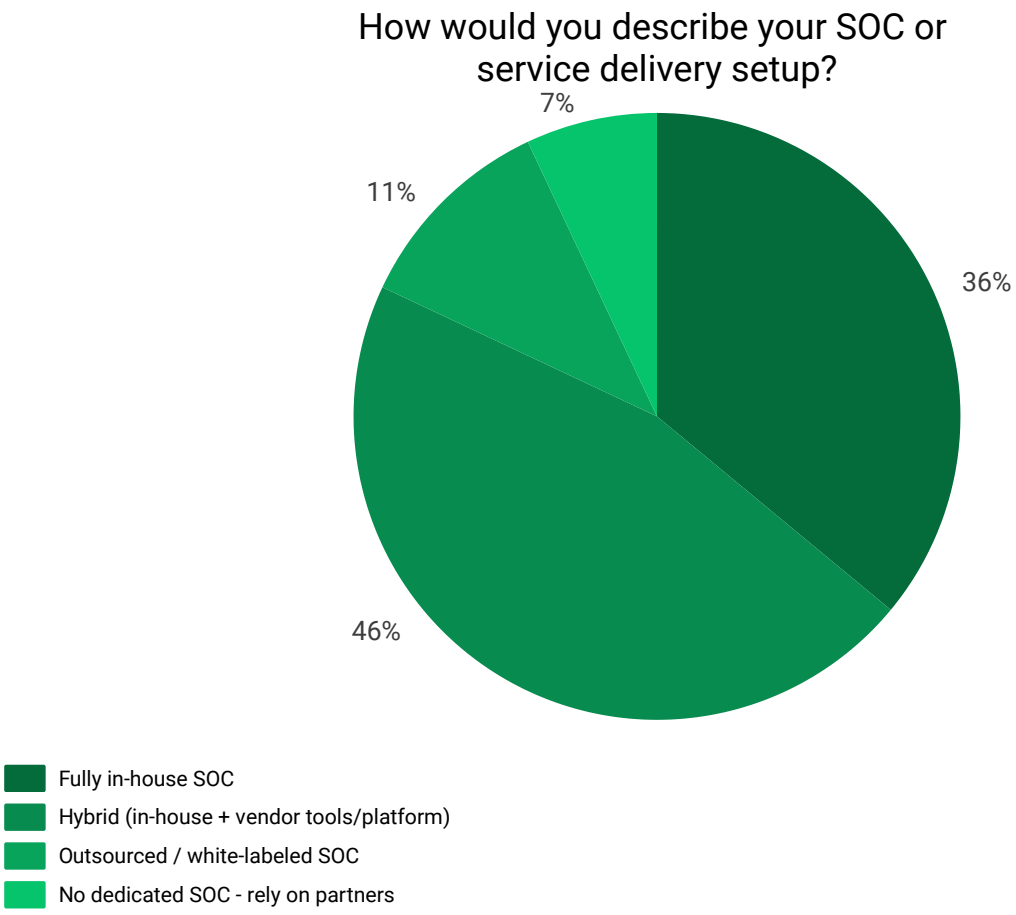
Rather than presenting survey results in isolation, this study connects practitioner insight to the broader market picture — what MSPs and MSSPs are experiencing globally, how buyer behavior is changing, and where providers should focus to deliver stronger outcomes and more scalable security services in 2026 and beyond.

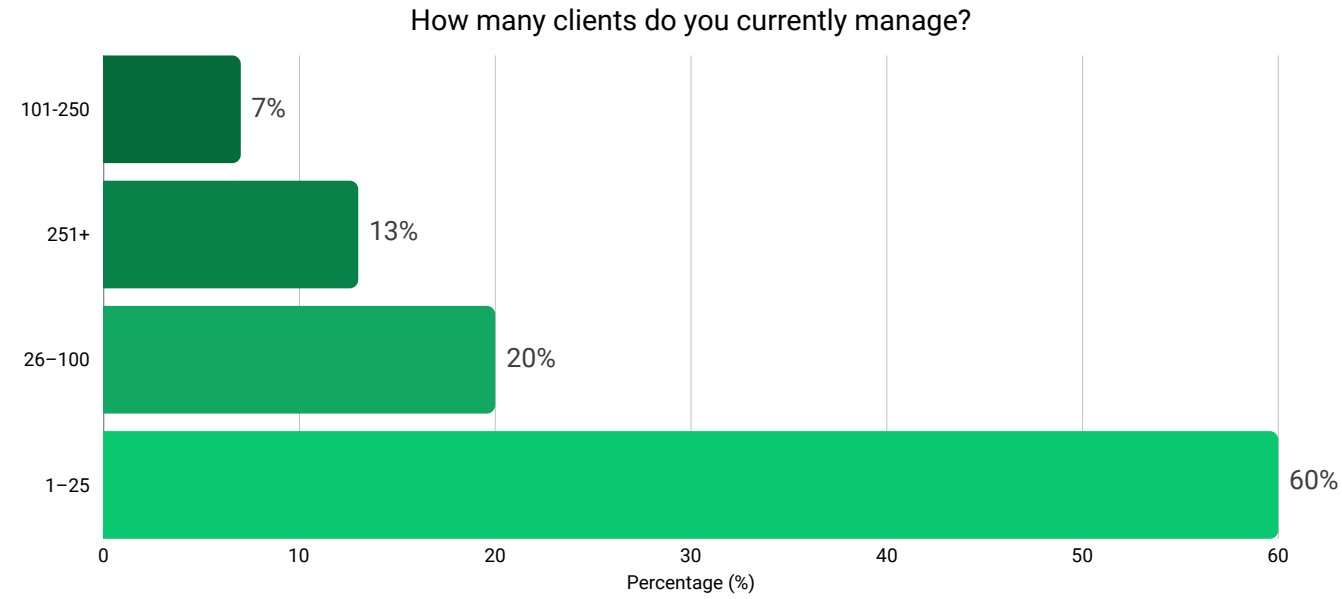
Survey Snapshot: Who This Data Represents




What best describes your role in your organization?
9%
14%
12%
14%
51%
Leadership (CEO, CTO, Director)
Security Operations / SOC
IT Infrastructure / Admin
MSP / MSSP Service Delivery
Sales / Business / Consulting


Which verticals represent your largest client base?
Other
6%
Education / Public Sector
12%
Healthcare
14%
Manufacturing / Industrial
17%
Technology / SaaS
23%
Financial Services
27%
0
5
10
15
20
25
30
Percentage (%)


How would you describe your SOC or service delivery setup?
7%
11%
36%
46%
Fully in-house SOC
Hybrid (in-house + vendor tools/platform)
Outsourced / white-labeled SOC
No dedicated SOC - rely on partners


How many clients do you currently manage?
101-250
7%
251+
13%
26–100
20%
1–25
60%
0
10
20
30
40
50
60
Percentage (%)

The insights in this report are drawn from responses across a global community of MSPs, MSSPs, and hybrid service providers actively delivering managed security services today. The audience reflects **hands-on operators and decision-makers**, not abstract respondents — people responsible for running SOCs, serving clients, and scaling security offerings in real-world environments.

Provider profiles

- **82%** of respondents identify as **MSSPs or hybrid IT + security providers**, underscoring a strong security-first perspective
- The remainder includes **consulting/advisory firms and MSPs**, offering insight into earlier-stage and transitional service models

Roles and responsibilities

- **Over half** of the respondents work directly in **Security Operations or SOC roles**
- Additional perspectives come from **IT/cloud teams, service delivery leaders, business roles, and executive leadership**
- This ensures the data reflects both **technical execution and business decision-making**

Client environments

- The majority of providers support **SMB and mid-market organizations**, with additional representation from enterprise and mixed portfolios
- **Financial services, technology/SaaS, manufacturing, healthcare, and public sector** are the most common client verticals

Service delivery models

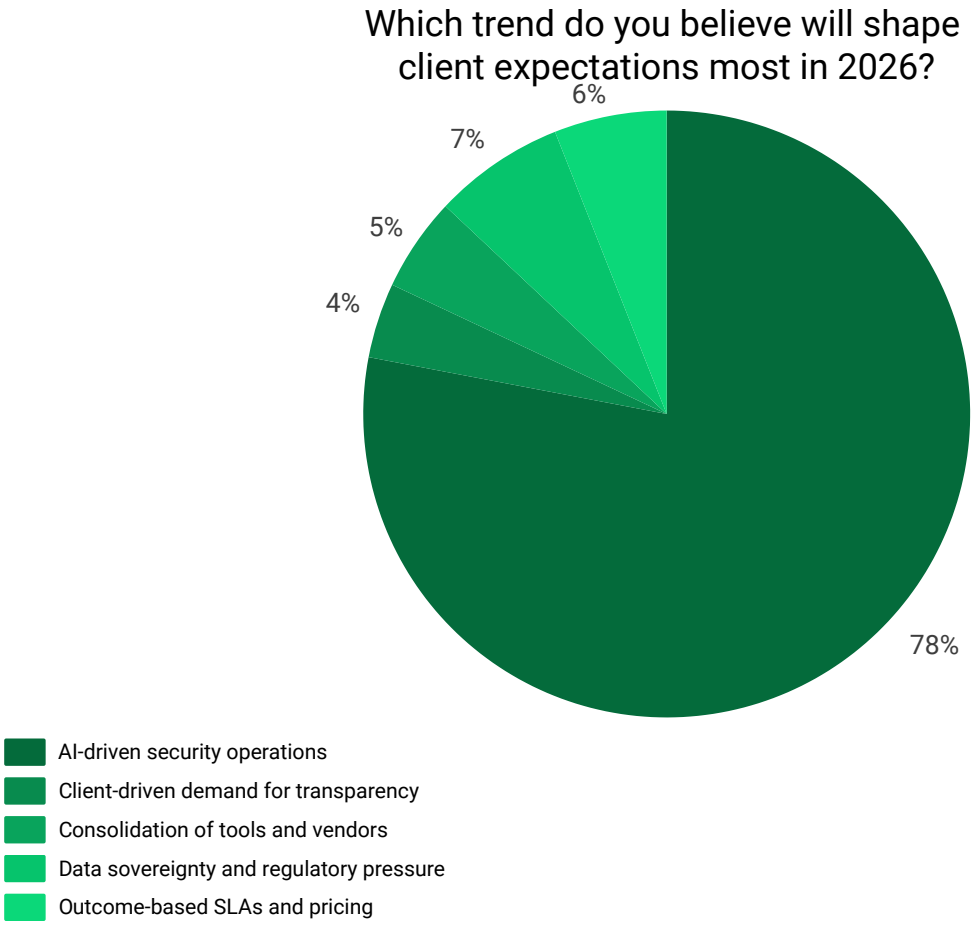
- **Hybrid SOC models** (combining in-house teams with external platforms and tools) are the most common approach
- Fully in-house SOCs and outsourced/white-labeled models remain in use, highlighting diverse operating strategies across the market

Why this matters

Together, this snapshot shows that the findings reflect the realities of **modern managed security delivery**: multi-tenant environments, constrained resources, diverse client needs, and increasing pressure to deliver measurable outcomes at scale. The perspectives captured here are directly relevant to providers navigating growth, modernization, and competitive differentiation in today’s security services market.

Finding 1: AI Has Moved from “Differentiator” to “Baseline Expectation”

Based on the data, **78% of respondents** said **AI-driven security operations** will shape client expectations most in 2026 (254/326). In addition, **72%** said clients are **actively asking and evaluating AI or automation options** (125/174), and **53%** reported that the biggest shift versus last year is **increased interest in automation and AI assistance** (58/109).



Context: For years, AI has been discussed as an innovation theme. The practical question for MSPs and MSSPs is whether AI is still “nice-to-have” or whether it has become a buyer expectation that affects renewals, win rates, and competitive positioning.

Survey result: The strongest signal is not just the top-line 78% selection for 2026 expectations—it’s the consistency across questions: clients are actively evaluating AI today, and interest has accelerated versus last year.

What this suggests globally: MSPs and MSSPs are entering a market where many buyers assume some level of automation exists behind the service. The competitive battleground shifts from “do you use AI?” to “what outcomes does it enable, and can you prove it?”

How providers can win: Providers that do best in 2026 will treat AI as an **operational capability** (speed, accuracy, workload reduction), not a marketing claim. The win is delivering repeatable improvements in detection and response while keeping service delivery sustainable.





Image 1 —Gitesh Shah (Samay Infosolutions Pvt. Ltd.) met with Chandra Pandey (Seceon) during his India tour.
Image 2 — Gitesh Shah with Team Seceon at the SCB & DCCB Ingenious Leadership Summit, Goa.

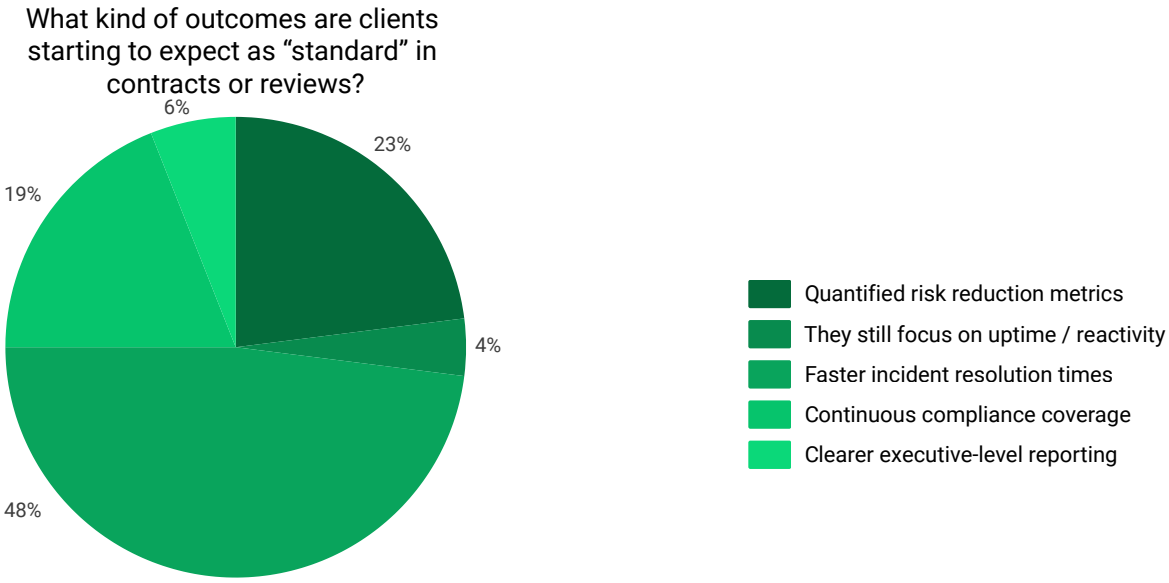
“We’re entering an era where cyber risk is inseparable from geopolitical risk. Nation-state activity and crisis-level attack scenarios are no longer theoretical — they’re shaping how organizations think about resilience. In this environment, cybersecurity isn’t just an IT decision; it’s a strategic one that affects long-term stability and growth.”

— Gitesh Shah, CEO & Founder, Samay Infosolutions Private Limited



Finding 2: Clients Are Raising the Bar on Outcomes — Especially Speed

Based on the data, **49% of respondents** said clients now expect **faster incident resolution times** as a standard contract or review outcome (153/314). A further **23%** report clients expect **quantified risk reduction metrics** (72/314), and **19%** cite **continuous compliance coverage** (59/314). Only **4%** said clients still focus on uptime/reactivity (11/314).



Context: Many providers still position security services around coverage ("we monitor X, Y, Z") or compliance ("we help you pass audits"). Increasingly, buyers want security to be expressed as measurable outcomes.

Survey result: "Faster resolution" is the dominant expectation—more than any reporting or compliance outcome. Risk reduction metrics are meaningful but still secondary to speed. **What this suggests globally:** Buyers increasingly evaluate providers on **time-to-detect and time-to-respond** narratives, not just tooling or checklists. This aligns with the rise of executive scrutiny: leadership teams want assurance that incidents are contained quickly and consistently.

How providers can win: Providers should package and report services around **response speed and measurable containment**, then build toward quantified risk reduction over time. The near-term win is operational credibility: "when something happens, we resolve it faster."

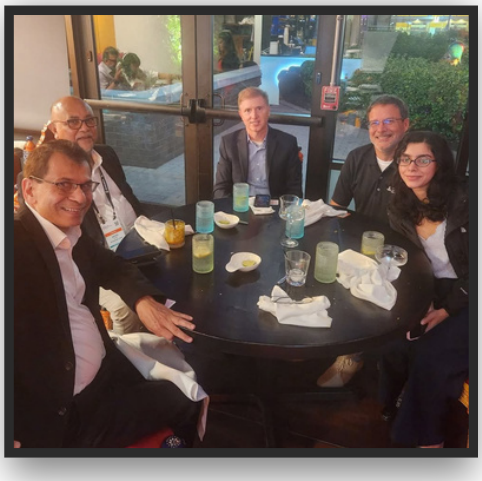




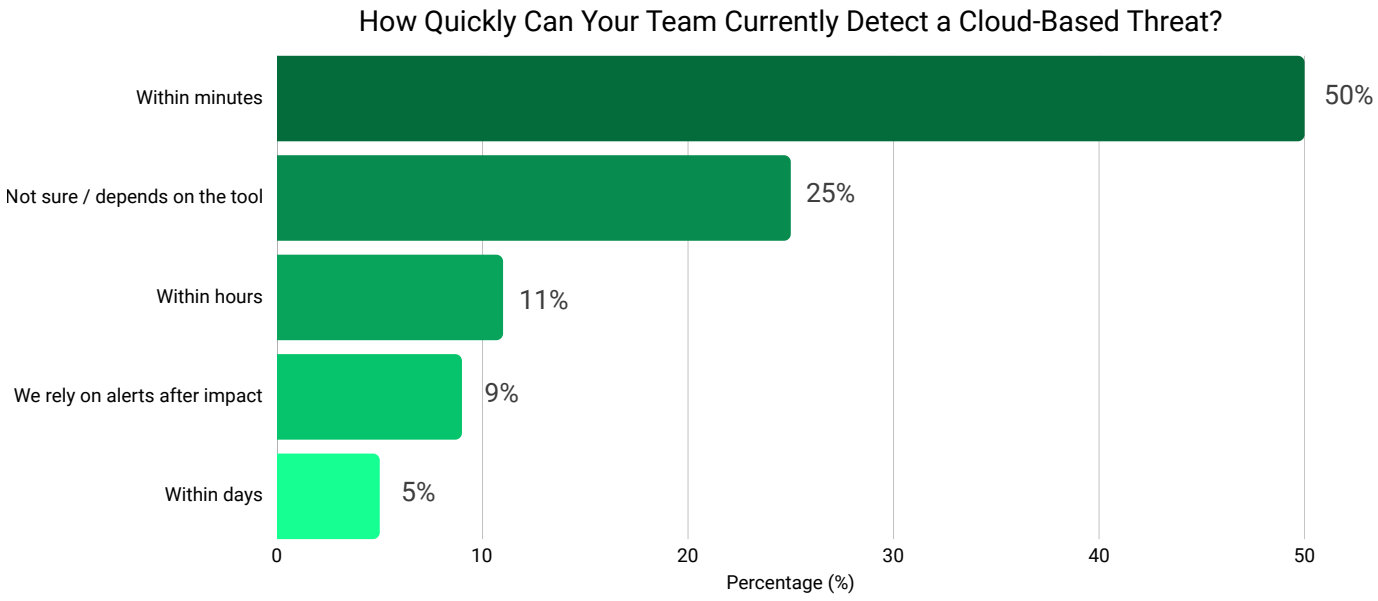
Image 1 — Team dinner with Keith Johnson, during the Gartner Security Conference.
Image 2 — Seceon leadership with Keith Johnson Jr. of Obviam at Black Hat USA 2025.

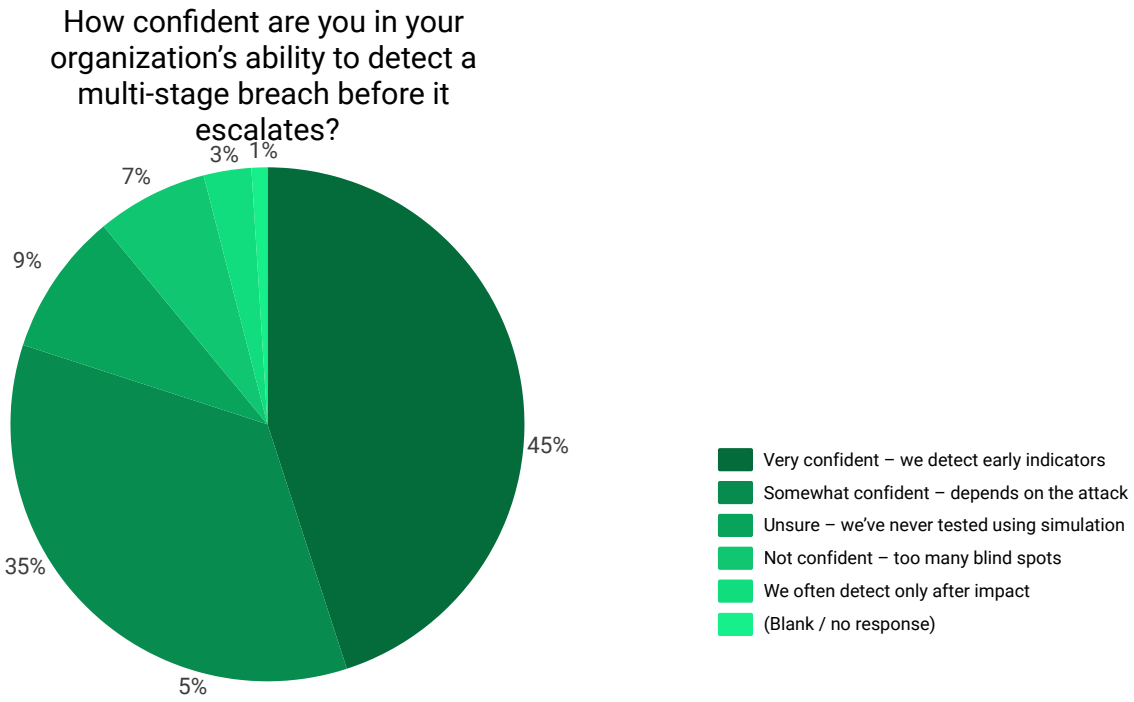
> *"You can deploy the best technology in the world, but without strong customer service, long-term relationships are hard to sustain. Technology is the enabler — trust, responsiveness, and accountability are what keep clients with you. At the end of the day, customers want to know you'll be there when something goes wrong."*
>
> **— Keith Johnson, Executive Vice President, Obviam**



Finding 3: Detection Confidence Is High, But Consistency Is Not Guaranteed

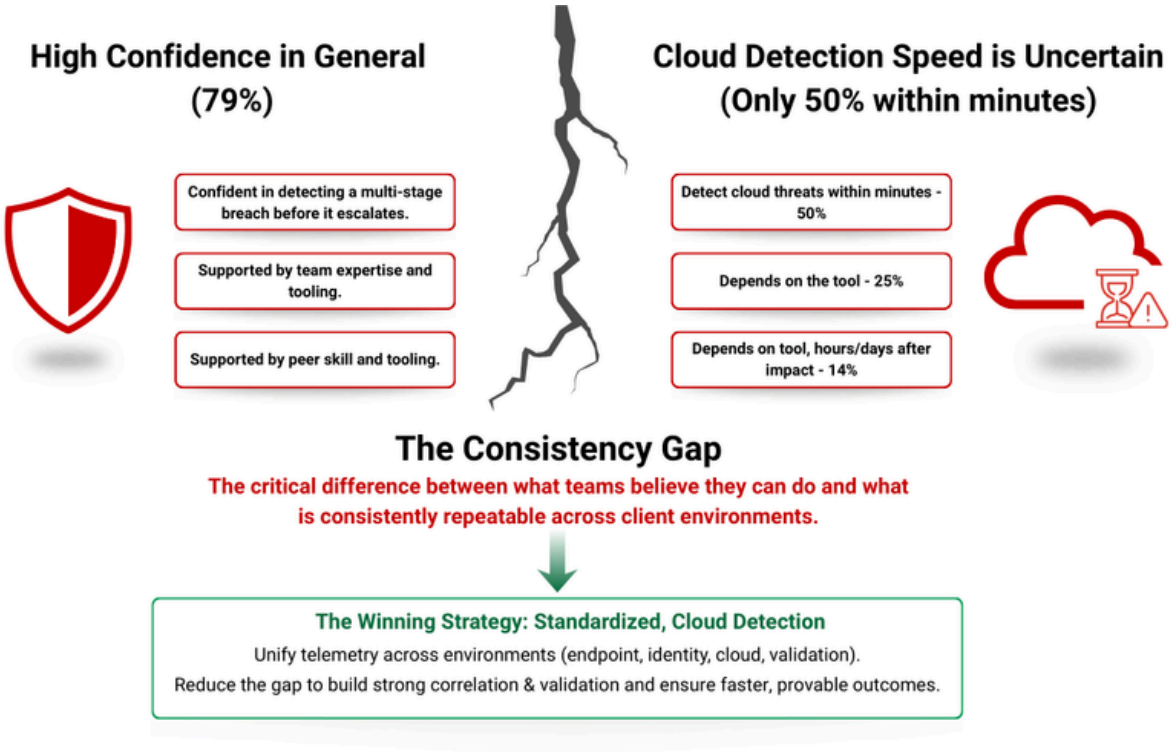
Based on the data, **79%** report being **very or somewhat confident** in detecting a multi-stage breach before it escalates (44% very confident = 71/161; 35% somewhat confident = 57/161). At the same time, cloud detection speed shows uncertainty: only **50%** say they detect cloud-based threats **within minutes** (128/255), while **25%** say "**it depends on the tool**" (64/255), and **14%** report detection only after hours/days or after impact (27+13+23 = 63/255).





Context: Confidence is important, but buyers increasingly care about reliability across environments—especially cloud, identity, and endpoint—where modern attacks move laterally.

Survey result: Respondents feel confident in principle, but a meaningful portion cannot guarantee consistent performance in cloud scenarios and tool-dependent setups.



What this suggests globally: Many providers are operating with a "confidence gap" between **what teams believe they can do** and **what is consistently repeatable across client environments**. This is especially relevant for hybrid SOC models and multi-tenant environments where tooling and telemetry vary.

How providers can win: The winners will standardize detection across environments and reduce tool-dependency through consistent telemetry, correlation, and validation (including simulation/testing where feasible). Consistency becomes a differentiator even when "AI" is table stakes.



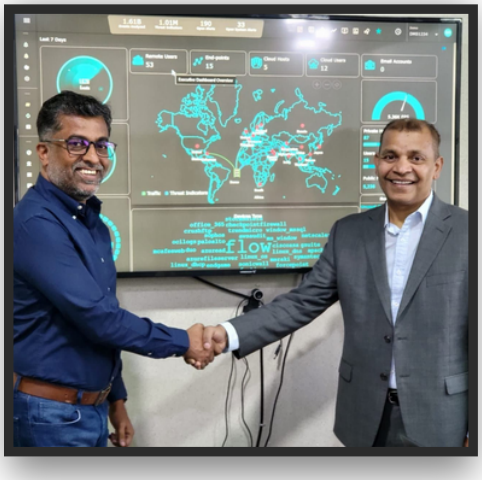


Image 1 — Seceon leadership and partners aligning on the 2026 MEA growth strategy and channel-first expansion.
Image 2 — Jibu John of CyberDisti with Chandra Shekhar Pandey of Seceon discussing MEA channel growth.

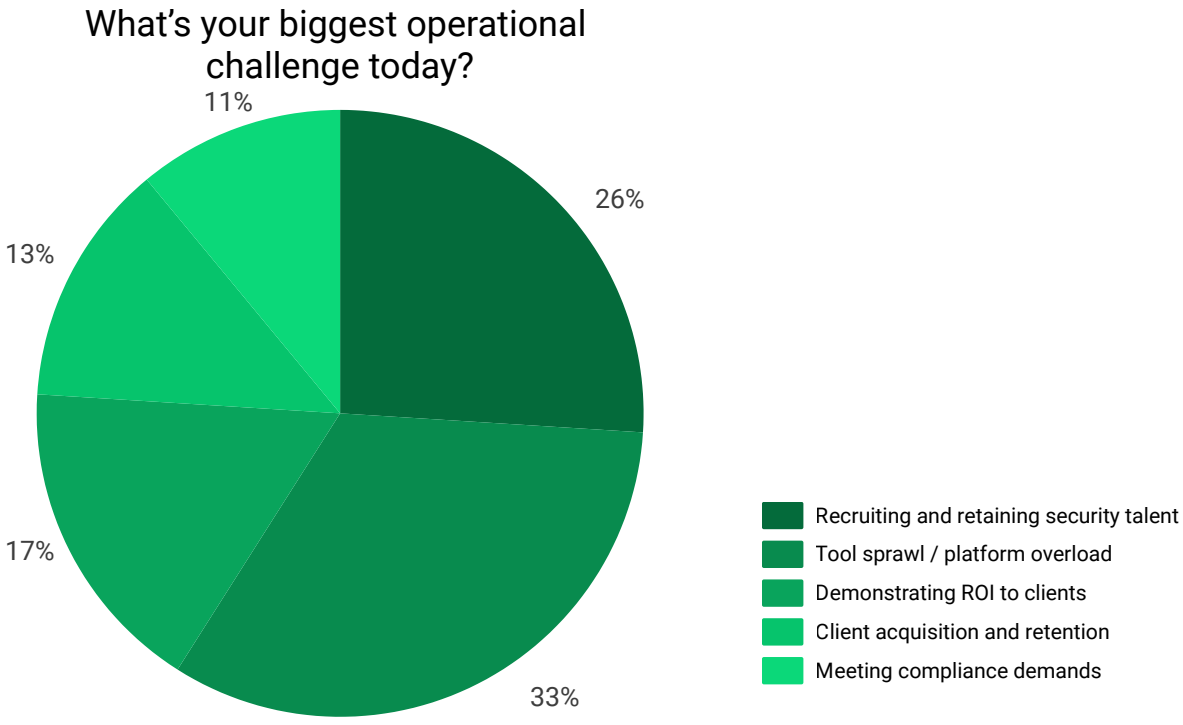
"From a SOC perspective, one of the biggest challenges is running multiple siloed solutions — SIEM for monitoring, SOAR for remediation, UEBA, EDR, vulnerability tools from different vendors. Because of this fragmented approach, it not only affects overall CAPEX, with separate licensing and infrastructure for each solution, but it also impacts SOC efficiency. Analysts end up juggling different platforms to investigate a single alert — and that's where the real challenge comes in, finding that needle from that haystack."

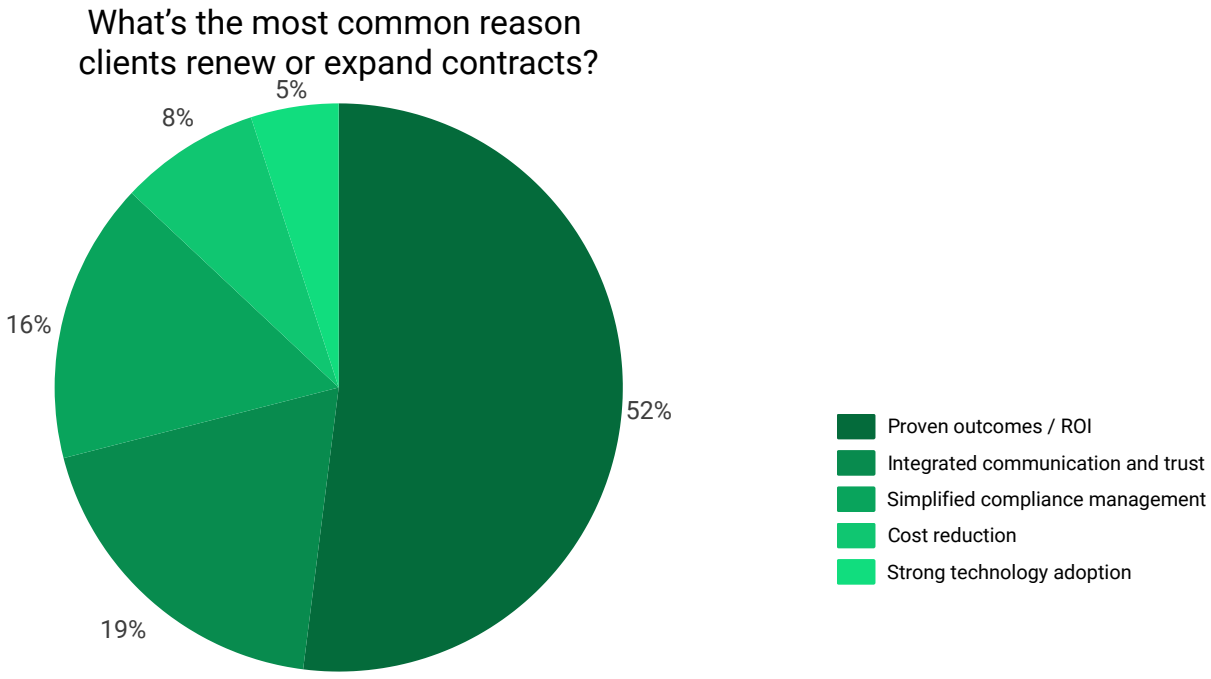


— Pratik Patel, Cybersecurity Division Leader, Tech First Gulf

Finding 4: Tool Sprawl and Talent Constraints Are the Top Operational Headwinds

Based on the data, **32%** cite **tool sprawl/platform overload** as their biggest operational challenge (40/126). **26%** cite **recruiting and retaining security talent** (33/126). ROI proof (17%), client acquisition/retention (13%), and compliance demands (11%) follow.





Context: MSPs and MSSPs are being asked to deliver more outcomes (speed, reporting, risk reduction) while maintaining margins. Tool sprawl increases complexity and labor; talent shortages make that labor expensive and hard to scale.

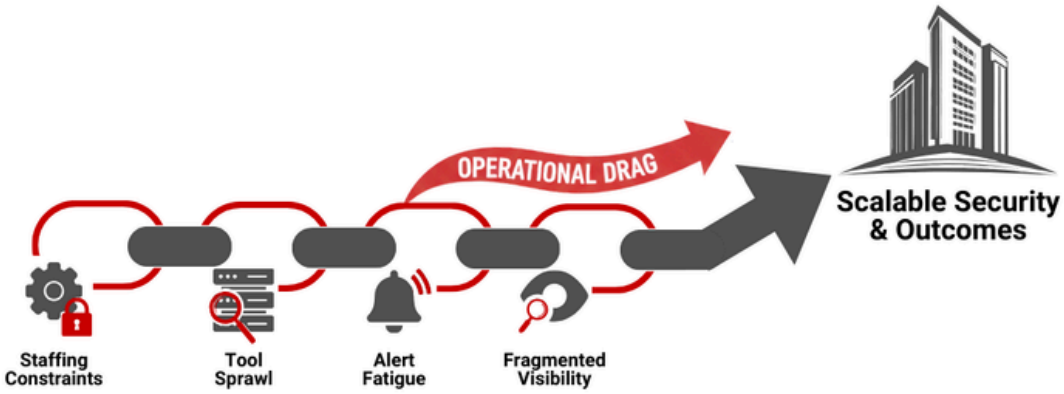
Survey result: Tool sprawl edges out talent constraints as the top pain point, suggesting that operational friction is driven as much by **system complexity** as by headcount.

What this suggests globally: Providers are being squeezed between expanding scope and operational reality. Many are likely accumulating tools to close gaps, then paying the price in integration overhead, alert fatigue, and training burden—especially in SOC-heavy organizations.

How providers can win: Focus on reducing operational drag: consolidate workflows, standardize playbooks, and prioritize capabilities that reduce analyst workload and improve signal quality. The win is "scale without proportional headcount."

The Operational Drag

Complexity & Talent Headwiids Slot MSP/MSSP Growth



The Problem: Too many tools, nought people, equals slow, inconsistent security.
The Goal: Simplify to scale





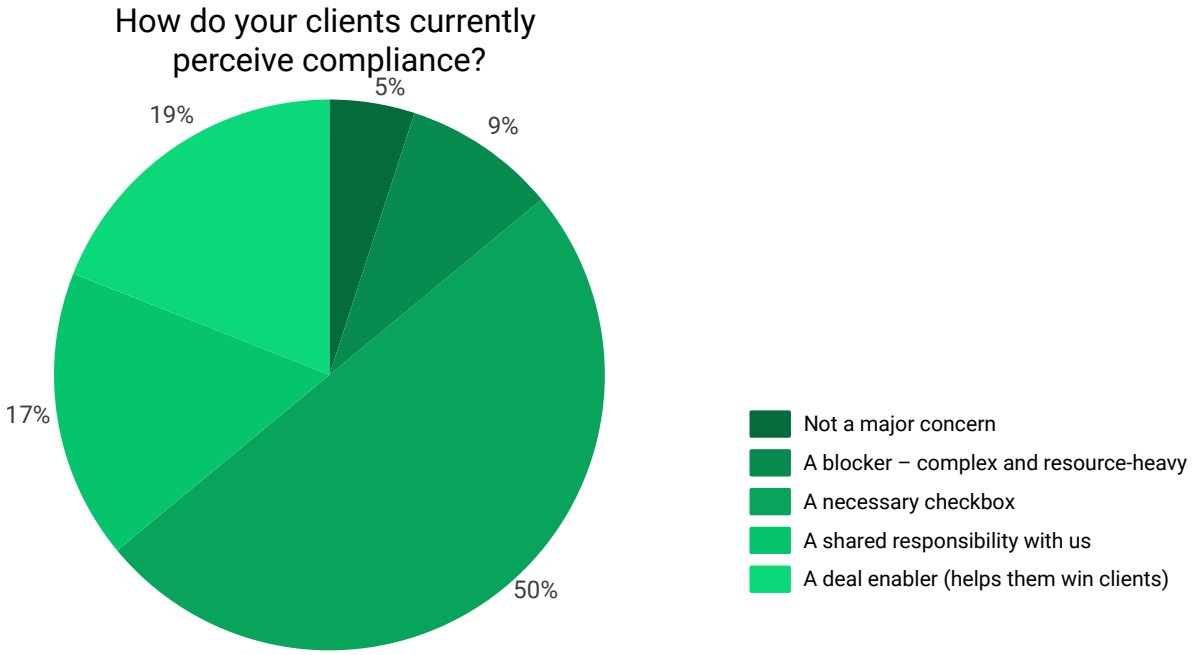
Image 1 — Seceon and Corr-Serve strengthening their strategic cybersecurity partnership.
Image 2 — Seceon leadership connecting with cybersecurity leaders during the ICT Summit gala evening.

> *"Organizations haven't ignored security — they've invested heavily. The real problem is fragmentation: too many tools, broken visibility, and human-led correlation that simply doesn't scale."*
>
> **— Mark Van Vuuren, Product Director, Corr-Serve**



Finding 5: Compliance Is Necessary, But Rarely the Primary Growth Engine

Based on the data, **49%** say clients see compliance as a **necessary checkbox** (49/99). **19%** say it is a **deal enabler** (19/99), while **17%** view it as a shared responsibility (17/99), and **9%** see it as a blocker (9/99).



Context: Many providers invest heavily in compliance messaging. But if buyers treat compliance as baseline, compliance alone may not differentiate providers unless paired with outcomes and reporting.

Survey result: Compliance is primarily “table stakes,” with a smaller portion viewing it as a commercial enabler.

What this suggests globally: Compliance may be essential for entry into certain industries and regions, but growth and expansion depend more on outcomes and operational performance. Providers should still deliver compliance well, but not mistake it for the main reason clients expand services.

How providers can win: Treat compliance as part of a broader value story: combine continuous compliance posture with measurable outcomes (speed, incident reduction) and executive-ready reporting. The win is “compliance + impact,” not compliance alone.





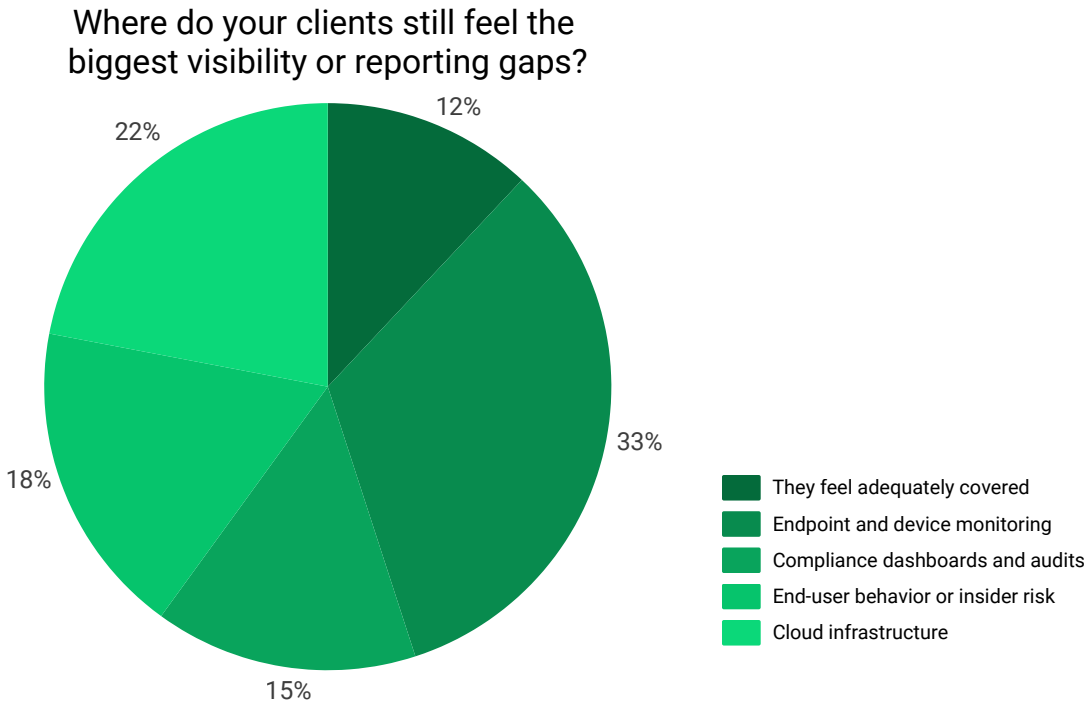
Image 1: Strengthening partnerships to drive the future of cybersecurity innovation.
Image 2: Seceon team with Colin Carhart of Logically during Blackhat USA 2025

> *"The launch of aiCompliance CMX360 represents a game-changer for our 500+ customers across financial services, healthcare, state and local government, education, and retail."*
>
> — **Joshua Skeens, CEO, Logically**



Finding 6: Visibility Gaps Persist—Especially on Endpoint, Cloud, and Insider Risk

Based on the data, only **12%** say clients feel "adequately covered" on visibility and reporting (9/74). The top gaps are **endpoint and device monitoring (34%)** (25/74), followed by **cloud infrastructure (22%)** (16/74), and **end-user behavior/insider risk (18%)** (13/74). Compliance dashboards are also a gap for **15%** (11/74).



Context: Visibility gaps drive slow investigations and inconsistent outcomes—exactly the opposite of what clients are now demanding (speed and measurable impact).

Survey result: Most providers have at least one meaningful gap area, with endpoint leading.

What this suggests globally: Providers are still dealing with fragmented telemetry across endpoint, cloud, identity, and user behavior. These gaps often show up when a real incident crosses boundaries (e.g., compromised identity → cloud access → endpoint persistence).

How providers can win: Providers should prioritize unified visibility and correlation across endpoint, cloud, identity, and user behavior—not just collecting logs, but making them usable for fast triage and response. The win is reducing time lost to correlation and escalating only what matters.





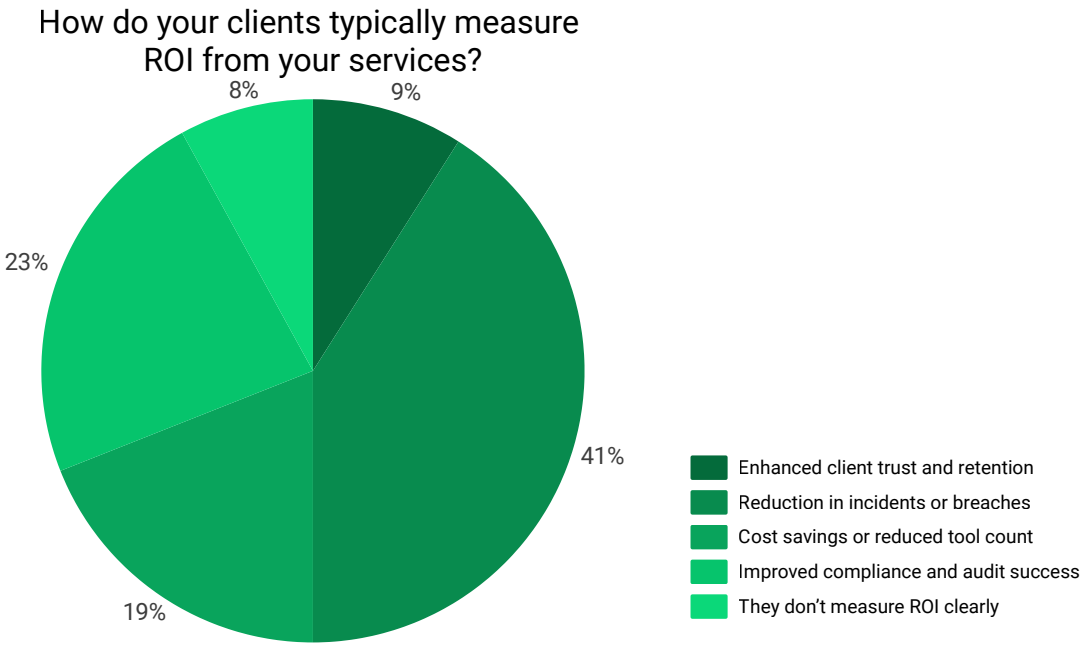
Image 1: Seceon leadership engaging with teams from Airtel, Airtel Business, Inventum, and GMR Group to advance cybersecurity for critical infrastructure.
Image 2: Leadership conversations shaping cybersecurity with Chandra Shekhar Pandey and Bithal Bhardwaj.

> *"Every digital touchpoint is a potential entry point for adversaries. Security cannot be just perimeter-based. The models must evolve toward continuous validation of every device, every entity, and every interaction."*
>
> — **Bithal Bhardwaj, Chief Executive Officer, Gramax (GMR Group)**



Finding 7: Retention Runs on Trust; Expansion Runs on Outcomes

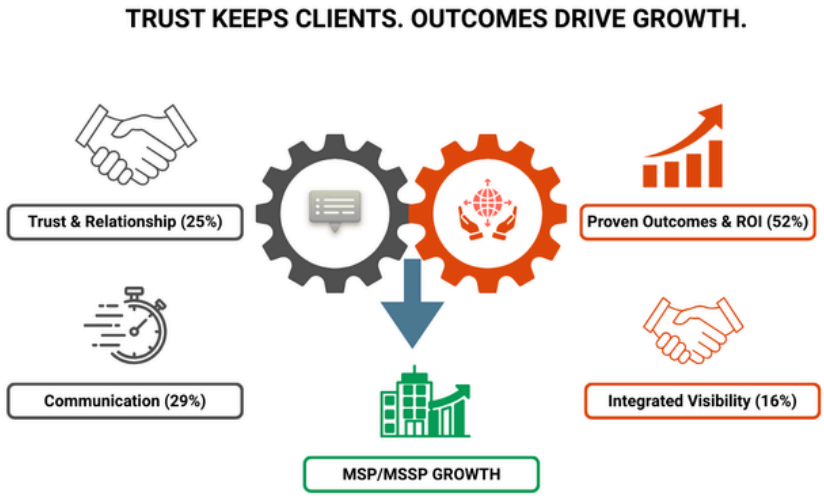
Based on the data, the most cited reason clients stay long-term is **consistent communication and transparency (29%)** (44/150), followed by **relationship and trust (25%)** (37/150) and **fast response (24%)** (36/150). Meanwhile, the most common reason clients renew or expand contracts is **proven outcomes/ROI (52%)** (83/159), with trust/communication secondary (19%) (31/159) and integrated visibility/reporting at 16% (25/159).



Context: MSPs and MSSPs often treat retention and expansion as the same problem. The data suggests they are related but distinct.

Survey result: What keeps clients satisfied day-to-day (communication, trust, responsiveness) is not always what drives budget expansion (proven ROI).

What this suggests globally: Providers who "feel good to work with" will retain accounts, but those who can **prove measurable impact** will expand them. In a competitive market, both are required.



The Two-Speed Model: Keep clients with service, grow them with proof.

How providers can win: Invest in two motions: (1) a strong communication cadence (clear, transparent updates), and (2) a measurable outcomes model (metrics tied to incident reduction, response speed, and risk reduction). The win is being trusted *and* being provably effective.





Image 1 — Strategic discussions on cybersecurity innovation during Kunal Panchamia's visit to Seceon HQ, Westford, MA.
Image 2 — Seceon recognizing eProtect 360 as the "Next-Gen MSSP Growth Partner" during a special award presentation in New Delhi.

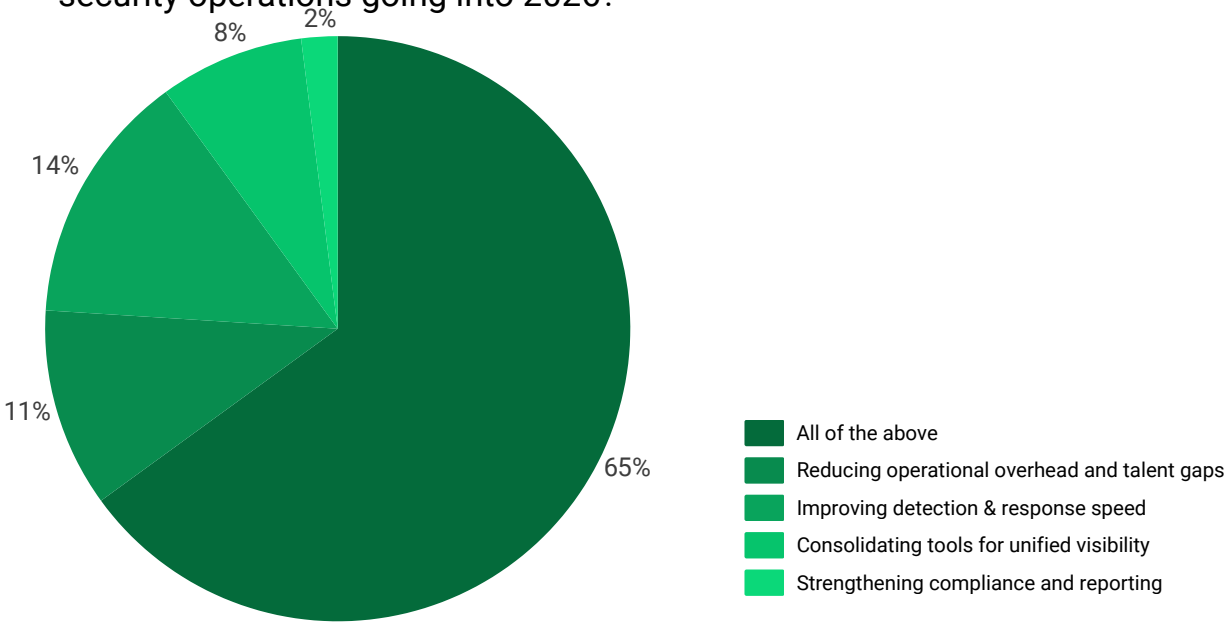
> *"What keeps clients with us long term isn't just coverage — it's integrity, transparency, responsiveness, and the ability to show measurable outcomes over time. When you combine strong delivery with continuous investment in people, process, and AI, security becomes an enabler of growth rather than a constant firefight."*
>
> **— Kunal Panchamia, Founder and CEO, ePROTECT 360 Solutions Pvt. Ltd.**



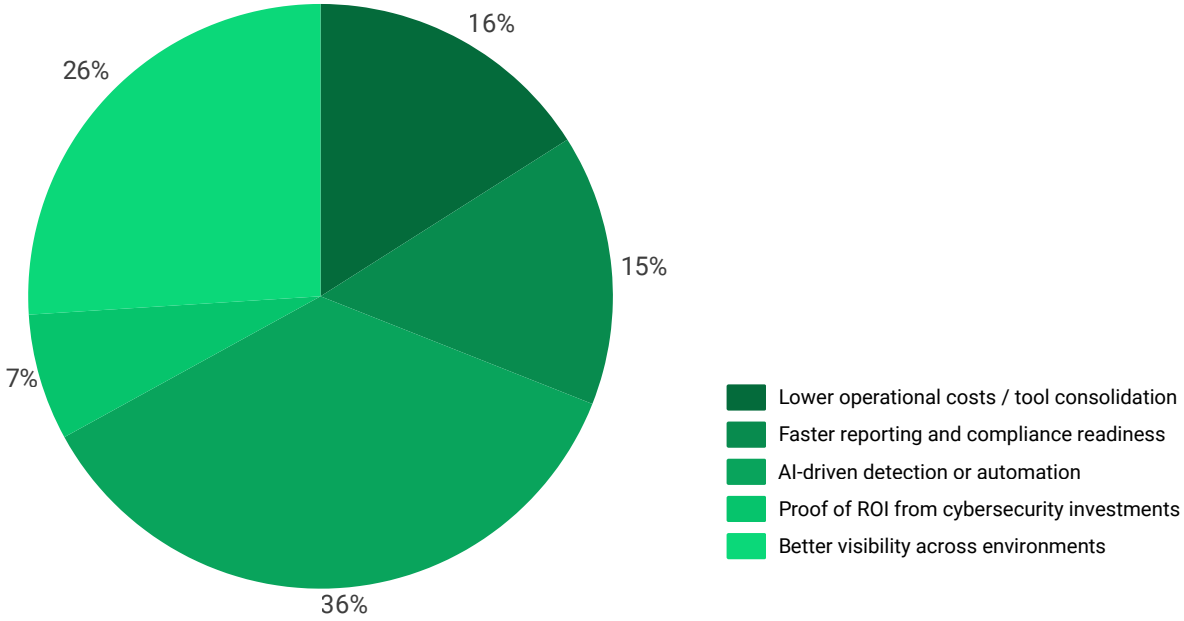
Finding 8: The 2026 Service Model Is "All of the Above"—But AI Automation Leads the Pack

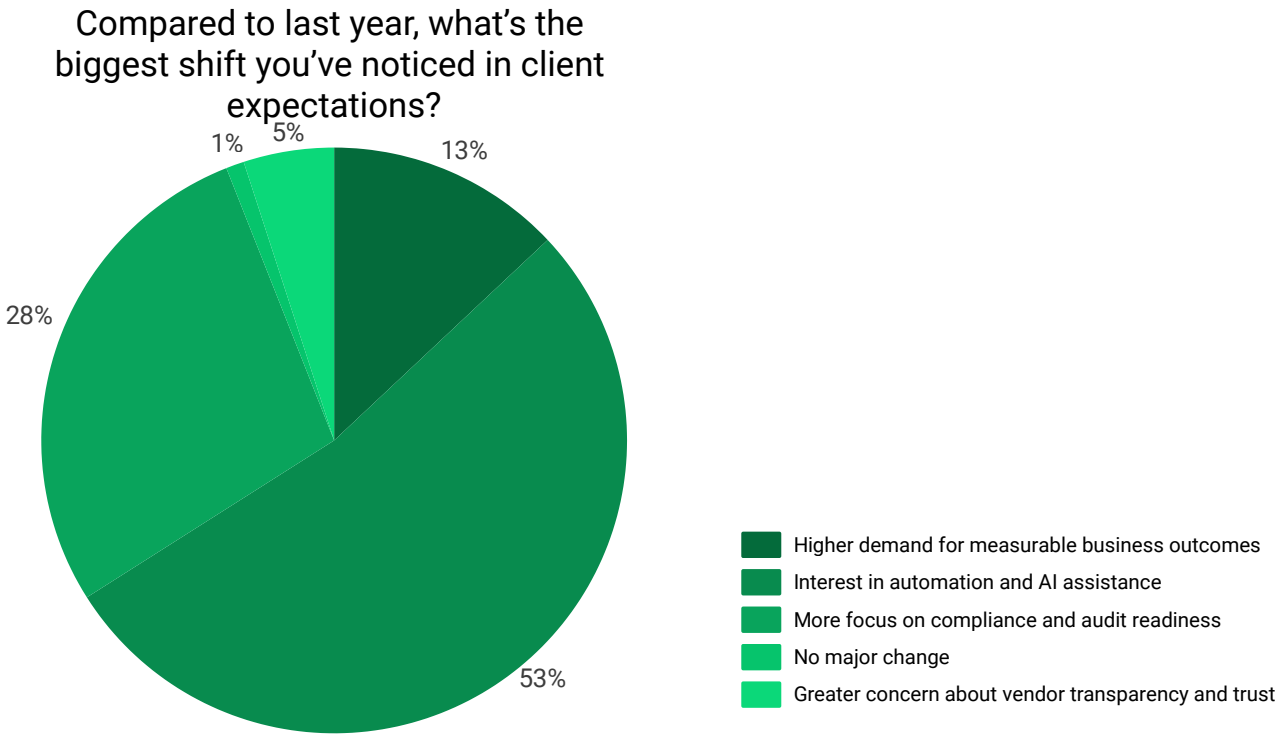
Based on the data, **64%** selected "all of the above" as their biggest 2026 security operations priority (62/97). Similarly, for expected shifts in service offerings, **54%** selected "all of the above" (55/101), while **31%** specifically selected adding **AI-driven automation** (31/101). When asked where AI/automation will have the biggest client impact, **56%** selected faster detection/response (87/155), and **28%** selected improved accuracy/reduced false positives (44/155).

What is the biggest priority for your security operations going into 2026?



What are your clients asking for most often this year?





Context: Providers are being pushed to modernize on multiple fronts simultaneously: operations, detection speed, compliance, reporting, and tool consolidation.

Survey result: Respondents don't see a single priority—they see a compound challenge. However, AI automation emerges as the most distinct single lever when forced to choose.

What this suggests globally: Many MSPs and MSSPs are moving toward service models that blend automation with unified operations—primarily to improve speed and accuracy while managing workload.

How providers can win: Treat AI automation as the foundation for delivering multiple outcomes at once: faster response, better signal quality, improved reporting, and reduced operational overhead. The win is "multi-outcome delivery" without burning out the SOC.





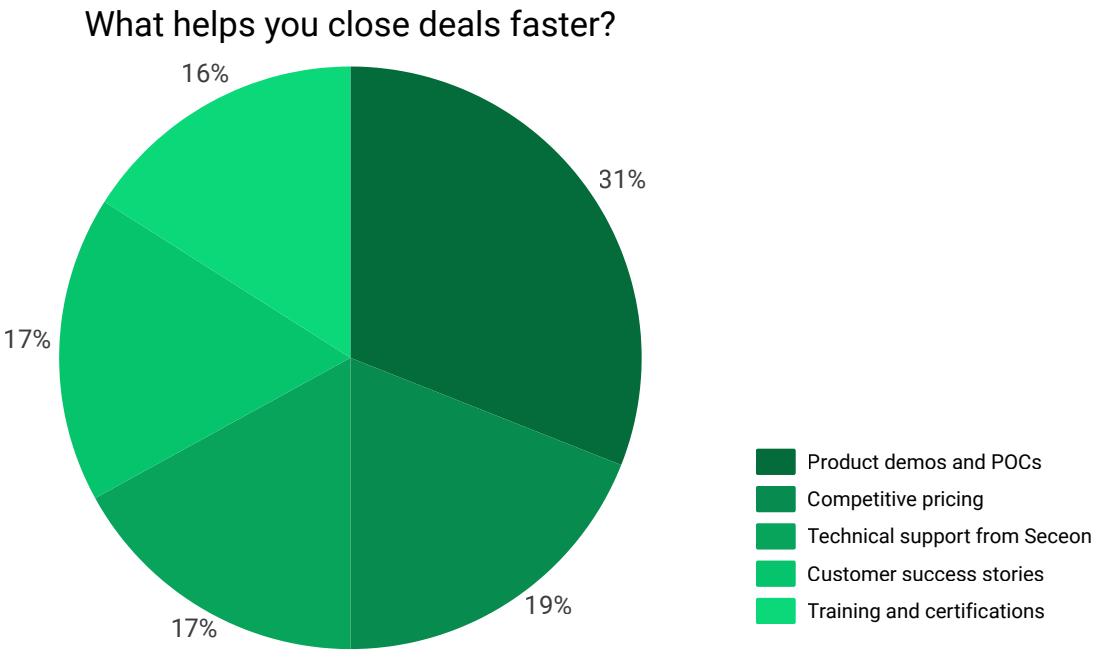
Image 1: Seceon and Exertis Enterprise strengthen their partnership to advance AI-driven cybersecurity services across the UK and EMEA.
Image 2: Chandra Shekhar Pandey with Geoff Towns discussing cybersecurity innovation.

> *"The use of AI and machine learning enables us to automate at scale and deliver very precise, proactive threat detection and response — preventing breaches before they can cause damage."*
>
> — **Dominic Ryles, Director of Cloud & Cybersecurity, Hammer (formerly Exertis)**



Finding 9: What Helps Providers Close Deals Faster

Based on the data, the top factor that helps close deals faster is **product demos and POCs (30%)** (103/343). Other accelerators include **competitive pricing (19%)**, **technical support (17%)**, **customer success stories (17%)**, and **training/certifications (16%)**.



Context: As buyer expectations rise, sales cycles often require proof—not just promises. Providers need repeatable ways to build confidence quickly.

Survey result: Demos/POCs lead, but the spread across factors indicates that faster deals often require a complete enablement motion: proof + support + credibility + readiness.

What this suggests globally: Providers are in an environment where trust must be earned quickly. Buyers want to see capabilities in action and want confidence that implementation and service delivery will be supported.

How providers can win: Build a “proof + confidence” motion: show capability (POC), prove outcomes (case stories), ensure delivery confidence (support), and reduce adoption friction (training). The win is shortening time-to-trust.





Image 1: Seceon leadership with Sunday McDickson Samuel, CEO of SMSAM Systems LTD, at Seceon's USA headquarters.
Image 2: Seceon leadership with Sunday McDickson Samuel, CEO of SMSAM Systems LTD, during Black Hat USA 2025

> *"Our growth came from proving security works in real environments, not from hype or market noise. We didn't win large financial institutions overnight — trust was built steadily as clients saw the capability in action. Once they experienced it firsthand, the value became clear."*
>
> **— Sunday McDickson Samuel, CEO, SMSAM Systems LTD**



Conclusion: What This Data Tells Us — and How MSPs & MSSPs Can Win

Taken together, the findings in this study point to a market that has already changed — even if many service models have not fully caught up.

Across regions, verticals, and provider types, the data shows a consistent shift in how managed security services are evaluated. Clients are no longer impressed by tool counts or abstract promises of protection. They are asking tougher questions: *How fast can you detect? How quickly can you respond? What measurable difference does this make to my risk and my business?*

That shift mirrors broader channel commentary. As IT Pro noted in 2025, “The MSPs that are going to stand out in the future are certainly going to be the MSPs that simplify the complex.”[3] In many ways, that sentence captures the core tension revealed in this research. Security environments are expanding. Threats are accelerating. Tool ecosystems are multiplying. And yet buyers increasingly expect clarity, speed, and measurable value.

Several themes stand out clearly from the data:
AI and automation are no longer differentiators. They are assumed. Clients increasingly expect intelligent, automated security operations to sit beneath the service — not as a feature, but as the engine that enables speed, accuracy, and scale.

Outcomes now matter more than coverage. Faster incident resolution, reduced impact, and clear evidence of improvement are becoming the standard by which providers are judged. Compliance remains necessary, but it is rarely the reason clients expand relationships or increase spend.

Operational pressure is arriving earlier than expected. Tool sprawl, staffing constraints, and fragmented visibility are straining SOC teams even at relatively small scales. Providers are feeling enterprise-level complexity long before they achieve enterprise-level margins.

Trust sustains relationships — but results drive growth. Consistent communication and transparency keep clients loyal, while proven outcomes and ROI unlock renewals and expansion.

For MSPs and MSSPs, the takeaway is not that everything must change at once. The data points to a focused set of priorities:

- Invest in capabilities that improve speed, consistency, and accuracy across environments
- Reduce operational friction so teams can scale without linear headcount growth
- Translate security activity into clear, outcome-based metrics that clients understand
- Pair strong communication with measurable results to build trust and justify expansion

Providers who align their operations, reporting, and service models around these principles will be better positioned to compete — not just on technology, but on impact.

For organizations seeking to modernize their security operations, the path forward requires more than additional tools. It requires unification, automation, measurable outcomes, and the ability to scale without overwhelming teams. Platforms built specifically to consolidate detection, response, compliance, and visibility into a unified operational model, such as those delivered by Seceon, are designed to help MSPs and MSSPs simplify complexity while delivering the measurable impact today's buyers expect.

The managed security market is not slowing down. Expectations are rising globally. The providers who win will be those who can consistently deliver outcomes, simplify operations, and clearly demonstrate value in an increasingly complex world.

The opportunity now is to act on it.

> *"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 750 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,300 clients.

Citations:

This Report is based on research and data from:

- Okeke, F. (2025, August 14). *75% of MSPs suffer alert fatigue from security tool sprawl, survey finds.* Channel Insider. https://www.channelinsider.com/channel-business/running-an-msp/heimdal-security-fatigue-report-2025/
- HFS Research. (2025, July 30). *Excerpt for EY: HFS Horizons—Cybersecurity Services, 2025.* Ernst & Young Global Limited. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/about-us/analyst-relations/documents/ey-gl-hfs-horizons-cybersecurity-services-report-07-2025.pdf
- Horton, C. (2025, October 15). *Channel leaders: Complexity is an opportunity.* IT Pro. https://www.itpro.com/business/business-strategy/channel-leaders-complexity-is-an-opportunity

© 2026 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.