

Report



# The MSP AI Burning Questions Report: **What MSPs Are Actually Asking About AI**

Straight from the forums, Slack threads, and late-night Reddit posts.  
Unfiltered, peer-sourced, and answered by the people living it 24/7.

## Introduction

Artificial Intelligence has quickly shifted from a future concern to an immediate operational reality for MSPs, MSSPs, and vCISO firms. Over the past year, the conversation has moved beyond curiosity into practical questions about governance, risk, tooling, and long-term relevance.

To better understand what service providers are actually dealing with, not just what vendors assume, Cynomi analyzed a combination of sources: direct input from Cynomi partners and community members, as well as public discussions across forums like r/MSP, r/sysadmin, r/cybersecurity, and related communities.

Rather than relying on surveys alone, this approach reflects real-world, unfiltered operator concerns: what practitioners are asking peers when facing decisions in real time. While these signals are directional, clear patterns emerged across hundreds of discussions.

From all that research, five core questions consistently surfaced. Below, we've paired each with perspective from our Cynomi community with specific call outs from our experts and partners who are actively working through these challenges with clients today.

### The five questions

- 1 How do we say "no" to client AI requests, without losing the account?
- 2 Are clients actually leaking sensitive data into AI tools?
- 3 Where does AI actually deliver value in the service desk?
- 4 Is Microsoft Copilot actually good — and do I sell it, give it away, or steer clients to Claude/ChatGPT?
- 5 Will AI replace MSPs, or change what clients need from us?

## Contributors

This report combines a synthesized Cynomi point of view on each question with on-the-record opinions from Cynomi experts and guest contributors from the partner community.

### Cynomi Experts



**David Primor** • [CEO and Co-Founder, Cynomi](#)

David co-founded Cynomi to put CISO-level decision-making in reach of every service provider, not just enterprises with in-house security leadership. He works closely with MSP and MSSP leaders on where AI changes the economics of delivering security services, and is a frequent voice on building advisory practices that scale.



**Roy Azoulay** • [CIO and Co-Founder, Cynomi](#)

Roy co-founded Cynomi and leads the thinking on how CISO Intelligence is built into the platform. He spends his time at the intersection of AI capability and security risk, advising partners on safe, structured AI adoption and on the technical controls that actually hold up in production.



**Tim Coach** • [Chief Evangelist, Cynomi](#)

A well-known voice in the MSP and MSSP community, Tim works hands-on with Cynomi partners on how agentic tools are reshaping day-to-day service delivery. He brings a practitioner's read on where AI creates leverage and where it quietly introduces new risk.

### Guest Contributors



**Andrew Morgan** • [Founder, Right of Boom](#)

Andrew is the founder of Right of Boom, one of the most respected security-focused communities and events for MSPs. He advises providers on turning AI and security conversations into strategic, revenue-generating client relationships rather than reactive support tickets.



**Dara Gibson** • [CEO and Owner, Cyber Ready](#)

Dara leads Cyber Ready and works at the intersection of cybersecurity and cyber insurance. She helps service providers and their clients adopt AI without opening governance gaps, with a focus on doing integrations properly to prevent data leaks and tool sprawl.



**Thomas Bergman** • [vCISO, Proven IT](#)

A practicing vCISO at Proven IT, Thomas works hands-on with clients from small business to mid-market. He is focused on translating AI from buzzword into measurable, governed value on the front line of service delivery, from the service desk to the boardroom.



**Don Monistere** • [CEO, General Informatics](#)

Don has operationalized agentic AI inside his own MSSP, from sandboxing AI deployments before client conversations to running AI-assisted triage across thousands of tickets. He brings a hard-earned, in-the-trenches view of what works and what goes wrong at scale.

# 1. How do we say "no" to client AI requests, **without losing the account?**

## CYNOMI COMMUNITY PERSPECTIVE

**The most effective providers are not positioning themselves as blockers, but as enablers with guardrails.**

Outright banning tools like ChatGPT or Claude often drives usage underground. Instead, leading MSPs are reframing the conversation around responsible adoption. That starts with defining what safe usage looks like, what data can and cannot be used, which tools are approved, and where human oversight is required.

The shift is subtle but important: from "no" to "not like that, here's how we can do it safely."

In practice, this often includes establishing approved AI tools, setting data-handling rules, and helping clients understand the risks of unsanctioned usage. Providers who take this approach are finding they can maintain trust while still reducing exposure.

## WHAT THE EXPERTS SAY

**David Primor** • [CEO and Co-Founder, Cynomi](#)

The short answer is: don't start with "no". When a customer asks for an AI capability, the first step is to understand the underlying need. What problem are they trying to solve? What outcome are they looking for? Often, the request itself is not the real requirement.

Once you understand the business need, have an open conversation about the challenges, risks, and constraints, especially with AI, where security, privacy, accuracy, compliance, and governance can have significant implications. If you already have a solution that can address the need, adapt it to the customer's use case rather than focusing on why their original request isn't possible. If you don't, treat it as valuable market feedback that may influence your roadmap.

The companies that win with AI are not the ones that say "no" the most — they are the ones that help customers achieve their goals safely and responsibly.

**Andrew Morgan** • [Founder, Right of Boom](#)

Don't say no. Get curious. "That's really interesting...what are you trying to accomplish? What inspired this idea? If you could have the perfect outcome, what would it look like?" Nine times out of ten, those three questions surface the real business outcome. Then find a way to deliver it with guardrails around data, privacy, and IP. You haven't said no, you've turned a procurement request into a strategic conversation, which is exactly the seat MSPs should be fighting for right now.

**Thomas Bergman** • [vCISO, Proven IT](#)

The framing of the answer is key. When working with clients ranging from small business owners to mid-market executives, the CISO must naturally shift the conversation toward the specific business objective AI is meant to solve. More often than not, this surfaces a non-tangible desire to simply "use AI" without a defined problem or outcome. It becomes the MSP's responsibility to educate the client and provide concrete examples of how AI can drive value, while simultaneously reviewing the controls that must be in place to do so safely.

The MSP should already have enough familiarity with the client to identify a relevant business process and demonstrate value directly. Once value is established through a targeted demo, the client is far more likely to invest in the required controls which, in turn, represents incremental revenue for the MSP.

**Don Monistere** • [CEO, General Informatics](#)

You can't say no to AI and you shouldn't try. What you can do is make the risk tangible. At General Informatics, we built a sandbox to test agentic AI deployments before any client conversation, so that when an executive comes to us excited about standing up an AI agent, we can show them real data of what happens when it goes rogue. The conversation shifts immediately: from "you're slowing me down" to "I didn't know that could happen."

My framing to clients: I'm not telling you no. I'm showing you what the risk is. If you want to take it, that's on you. But my responsibility is to show you how these decisions impact your overall risk posture. That approach keeps the relationship intact, respects the client's autonomy, and positions us as advisors, not gatekeepers.

## 2. Are clients actually **leaking sensitive data into AI tools**?

### CYNOMI COMMUNITY PERSPECTIVE

**This is no longer theoretical, it is already happening in day-to-day workflows.**

Across both community discussions and partner anecdotes, there are repeated examples of employees pasting sensitive information: legal documents, medical records, internal communications, into public AI tools for convenience. The issue is rarely malicious; it is driven by ease of use and lack of awareness.

Traditional controls like DLP and web filtering are not well-suited to this problem, particularly when prompt content is invisible. As a result, providers are shifting toward data-centric policies rather than tool-centric restrictions: clearly defining what types of data can be used with AI, encouraging enterprise-grade tools where appropriate, and embedding practical guidance into user behavior.

Education plays a significant role here. Simple, relatable rules, paired with real-world examples, are proving more effective than static policy documents.

### WHAT THE EXPERTS SAY

**Tim Coach** • [Chief Evangelist, Cynomi](#)

Without a doubt. With the new wave of agentic tools: Claude Code, Cowork, and others, our partners and their people are throwing everything, including the proverbial kitchen sink, at these tools to achieve a wide range of outcomes.

The biggest issue is the people who pay their \$20 a month to make their lives easier. They aren't thinking about what data they're putting in, what they're leaking, or the legal risk they're taking on – it doesn't even register. They just want it faster, and they've thrown caution to the wind. As a result, service providers are having to start back at the beginning, working to protect their partners and their partners' partners.

**Roy Azoulay** • [CIO & Co-Founder, Cynomi](#)

Yes, if your clients aren't actively managing it, they're almost certainly leaking sensitive data into AI tools. The behavior is convenience-driven: employees paste contracts, client emails, HR records, and source code into public AI tools because it gets them a better answer. A written policy saying "don't do this" is not a control.

Leakage is structural. Employees can reach public AI tools from any browser without IT involvement, and useful prompts require real business context. You can't write a good AI prompt about a client contract without including the contract.

#### **My recommendations for MSPs:**

- Discover before you govern. Find out what tools are actually in use including personal accounts and browser extensions IT doesn't manage. Shadow AI is the norm, not the exception.
- Define an approved toolset. Enterprise and business plans include data privacy commitments, admin controls, SSO, and no training on customer data. Give employees a sanctioned option so compliance isn't a productivity penalty.

- Build technical controls. Prompt inspection and DLP at the point of submission are far more effective than after-the-fact detection. Intercept risky behavior before data leaves.
- Fix permissions before deploying connected AI. Tools like Copilot surface whatever the user already has access to. If SharePoint and Teams have broad “everyone” permissions, which most SMB environments do, connected AI amplifies that exposure immediately.
- Train at the point of risk. In-line coaching triggered when a user is about to paste sensitive content changes behavior. Annual awareness training doesn't.

**Don Monistere** • [CEO, General Informatics](#)

What's coming next is giving AI systems authority to act: to make decisions, execute tasks, interact with vendors. That's a different risk profile entirely, and most clients have no framework for it. Zero trust, which enterprises have been discussing for years, is quickly becoming a practical necessity for SMBs, because AI agents sitting inside the network and communicating externally are exactly the threat model zero trust was designed to address. You've also got vibe-coded applications built with unvetted libraries sitting inside the firewall. The normalized-traffic visibility that zero trust networking provides is increasingly the only reliable way to know what's actually happening.

### 3. Where does AI actually deliver value in the service desk?

#### CYNOMI COMMUNITY PERSPECTIVE

**Despite the hype, the strongest returns are coming from focused, assistive use cases, not full automation**

High-performing teams are using AI to augment, not replace, their service desk workflows: summarizing tickets, suggesting responses, improving documentation access, and accelerating routine communication.

Attempts to fully automate complex workflows, especially those involving system changes or sensitive actions, often introduce risk and rework. As a result, many providers intentionally limit AI to “copilot” roles, where humans remain in control of execution.

Tooling strategies vary. Some MSPs adopt commercial platforms for speed, others build custom workflows for flexibility, and many land in between. Across all approaches, the common thread is iterative deployment, starting small, measuring impact, and expanding based on what actually works.

#### WHAT THE EXPERTS SAY

**Andrew Morgan** • [Founder, Right of Boom](#)

AI delivers value in the service desk in three specific areas, and almost nowhere else. First, ticket triage and classification, the most boring use case and the highest-leverage one. AI is genuinely good at reading a ticket, categorizing it, routing it to the right tier, and tagging it for trend analysis. Three months of clean categorization gives you the trend reports you’ve been promising clients for years.

Second, knowledge base search and response drafting, not autonomous resolution, drafting. AI finds the relevant KB article and surfaces a suggested response that the tech reviews, edits, and sends. It compresses tier-one resolution time without taking the human out of the loop; the tech is still accountable for what gets sent, and that accountability is the whole point. Third, post-incident documentation, writing up the resolution, updating the KB, closing the loop. Most service desks recover an hour per tech per day just by automating this step.

**Roy Azoulay** • [CIO & Co-Founder, Cynomi](#)

AI delivers real service desk value when it improves how work flows, not just how fast tickets close. The highest-impact use cases are structural: turning vague intake (“VPN broken”) into structured, enriched data before it hits a technician; giving L1 access to prior resolutions and diagnostics at the point of work; keeping the knowledge base current by drafting articles from resolved tickets automatically; and surfacing patterns across tickets before they become incidents. AI also reduces the administrative drag of cross-tool summarization, client communication drafting, and management reporting. The catch is that AI accelerates whatever system it’s placed into weak categories, stale knowledge, and poor permissions produce unreliable automation, not efficiency. Start with low-risk, assistive use cases like triage, enrichment, and article drafting, and expand as process maturity improves. The goal is a service desk where routine work is assisted, complex work is better supported, and recurring demand is systematically reduced, not just a faster queue.

**Dara Gibson** • CEO & Owner, Cyber Ready

In the cyber insurance industry, customer-service chatbots and automating underwriting and claims are the top use cases for AI increasing value. For cybersecurity service, first-tier triage of alerts provides clear value to the cyber team.

**Thomas Bergman** • vCISO, Proven IT

The largest value I see in practice is the ability to structure unstructured thoughts and produce better documentation, faster. As a Tier 1 technician works through a troubleshooting sequence, they may keep a running bullet list of attempted steps that is perfectly clear to them, but largely unreadable to the next technician picking up the ticket. By leveraging AI, that same technician can quickly transform their notes into structured documentation, either to resolve the ticket cleanly or to escalate with a level of clarity that historically required a more senior hand.

A common example is a mobile email delivery failure. A Tier 1's working notes might be: restarted the phone; logged out/into Outlook; checked CA policies; reviewed M365 service health; user still unable to retrieve email, in HQ, on guest Wi-Fi. The prompt I would use to convert those notes into a ticket-ready entry is:

*"Take the following unstructured troubleshooting notes and document them inside the ticket prior to escalating to Tier 2. Additionally, suggest any further steps I may not have taken yet."*

The result is a clean, escalation-ready entry, environment captured (Corporate HQ, guest Wi-Fi / untrusted segment, Outlook client to confirm at T2), each Tier 1 step written up with its outcome (full power cycle, Outlook session reset, Conditional Access review with no confirmed policy match, M365 Service Health clear), and a clear current status of unresolved, turning a senior-level write-up into something a Tier 1 can produce in seconds.

**Don Monistere** • CEO, General Informatics

We deployed AI triage at our service desk about 90 days ago, and the results have been concrete. Every ticket that comes in gets triaged by AI before it hits a level-one technician, it doesn't matter if there are 2,000 in the queue, they're processed in seconds. What we've seen is that L1 engineers are now capable of handling tickets they couldn't handle before, because the work of categorizing, prioritizing, and creating an instruction set has already been done for them.

## 4. Is Microsoft Copilot actually good — and do I sell it, give it away, or steer clients to Claude/ChatGPT?

### CYNOMI COMMUNITY PERSPECTIVE

#### Copilot's value is highly dependent on the environment it operates in.

In well-structured Microsoft 365 environments with clean permissions, organized data, and consistent usage, Copilot can significantly improve productivity within familiar workflows. In less mature environments, results are often inconsistent, leading to user frustration.

This has led many providers to position Copilot not as a standalone solution, but as part of a broader AI ecosystem, often paired with tools like ChatGPT or Claude that may perform better for complex reasoning or cross-domain tasks.

A key lesson from the field: preparation matters as much as licensing. Providers who invest in tenant readiness – data hygiene, access control, and content structure, see much stronger outcomes and adoption.

### WHAT THE EXPERTS SAY

#### Roy Azoulay • CIO & Co-Founder, Cynomi

Microsoft Copilot is still worth considering, but it should not be treated as the default AI choice for every client. Its real value is not that it is the “best AI”, in many cases it is not. ChatGPT and Claude are often stronger for high-quality writing, reasoning, research, analysis, and flexible workflows, and advanced teams will naturally prefer them.

Copilot's value is different: it is the most practical option for organisations that already run their business in Microsoft 365. If a client lives in Outlook, Teams, Word, Excel, SharePoint, and OneDrive, Copilot reduces friction where work already happens, meeting summaries, email drafting, document creation, finding internal information, and helping less technical users start using AI without changing how they work.

The mistake is selling Copilot as a revolutionary AI assistant; it's better positioned as a Microsoft 365 productivity layer. So: don't push it blindly, and don't give it away. Assess workflows first. If their work is Microsoft-centric, sell Copilot with readiness, permissions review, training, and governance. If they need stronger general-purpose AI, recommend ChatGPT or Claude. The MSP's value is not reselling whichever licence is fashionable, it's helping clients choose the right tools, avoid data leakage, clean up permissions, and turn AI into measurable productivity. The winning position is trusted AI advisor, not Copilot reseller.

#### Thomas Bergman • vCISO, Proven IT

This is highly subjective, and will often depend on what the business objective is. Copilot is an excellent choice for working with native M365 data, and is particularly well-suited for users who are newer to AI tools or have not yet developed a working relationship with a competing platform. For users who have already built a cadence with another tool, where the AI has learned their communication style, preferred format, and terminology, Copilot will initially feel like a step backward, because they are starting from zero.

Where Copilot genuinely wins: summarizing meetings in Teams, drafting emails in Outlook with full thread context, and working against SharePoint or OneDrive data without a manual paste. Where it loses ground: open-ended strategic thinking, long-form content generation, and any workflow already optimized around another model's behavior.

A prompt I've saved and shared with clients when onboarding Copilot:

*"I am going to help you understand how I work so you can assist me more effectively over time. Ask me questions — one at a time — to learn my role and primary responsibilities, the types of tasks I use AI for most, my preferred communication style (formal vs. conversational, concise vs. detailed), the industries or subject matter I work in, and any specific terminology or context that would help you respond more accurately. Once we've worked through these, summarize what you've learned about me in a structured profile I can reference and build on in future sessions."*

## 5. Will AI replace MSPs, or **change what clients need from us?**

### CYNOMI COMMUNITY PERSPECTIVE

**AI is not eliminating the need for MSPs, but it is redefining where value is delivered.**

Routine repetitive tasks are becoming faster and, in some cases, automated. At the same time, clients face new challenges: AI governance, data exposure risks, tool sprawl, that they are not equipped to handle alone.

This is shifting the role of providers upward. The most successful firms are leaning into advisory, risk management, and strategic guidance rather than purely operational support.

There is also a growing divide between providers integrating AI into their own operations and those who are not. Increasingly, the competitive pressure is not AI replacing MSPs directly, but AI-enabled providers outperforming traditional ones. When clients attempt to fully replace providers with DIY AI, they often expose gaps in security, reliability, and oversight, ultimately reinforcing the need for experienced partners.

### WHAT THE EXPERTS SAY

**David Primor** • [CEO & Co-Founder, Cynomi](#)

AI won't replace MSPs, but it will replace the idea that reactive IT support is enough. Clients now face two converging challenges: employees using unapproved AI tools and leaking sensitive data without realizing it, and executives who want a practical AI roadmap and don't know where to start. Both problems land on the MSP's desk, and neither gets solved by keeping systems running. The MSPs that win will move up the value chain, offering AI readiness assessments, permission reviews, governance, secure adoption plans, and ongoing advisory. That relationship is hard for AI to replace. It understands tasks; it doesn't understand a client's environment, risk appetite, legacy constraints, and people the way a good MSP does.

**Tim Coach** • [Chief Evangelist, Cynomi](#)

This question comes up every few years as technology changes, and every time the MSP rises to meet the new version. No more on-prem Outlook; it moved to the cloud – how do we manage it and make money? We found a way. No more tape backups; everything moved to the cloud – we found a way. On-prem servers gone, everyone working from home, all data in the cloud – you get it.

Technology is perhaps the fastest-changing industry out there, and we always find a way. SMB, mid-market, and even some enterprises outsource IT because they don't understand it and don't want the overhead, for the weighted cost of a single FTE or less, they get an entire team. Security is no different: as attackers get smarter, so do we. The difference now is we need a CISO overwatching and guiding security strategy for the future, and the easiest way for any company to do that is through their MSP.

**Dara Gibson** • CEO & Owner, Cyber Ready

AI is a tool. It cannot replace the human in the MSSP. It will, however, change what clients expect from the service provider, increasing the need for governance partners and ensuring AI integrations are done properly to prevent leaks and tech sprawl.

**Thomas Bergman** • vCISO, Proven IT

AI will not replace the MSP, but like every major technology shift before it, it will raise the bar for what clients expect from us. Clients engage MSPs because they've made a strategic choice to outsource technology leadership, or because they recognize a gap in their own technical proficiency. Neither means the client is unaware of AI. The opposite is increasingly true – clients arrive already curious, expecting their MSP to have answers.

This is not a new pattern. Cloud adoption created the same pressure a decade ago: the question was not whether to move workloads off-premise, but how, when, and at what risk. MSPs that had already been through that journey internally could lead clients through it with confidence; those still catching up were playing defense.

AI follows the same arc. The differentiator today is the MSPs genuinely integrating AI into their own operations, not just reselling it. Being Customer Zero matters here. When an MSP has already lived the implementation, absorbed the failure modes, and built repeatable processes around the tools, that lived experience becomes a competitive asset. Clients aren't looking for a vendor that can explain what Copilot does, they're looking for a partner who can tell them whether it belongs in their environment, and what it will actually take to get there. The MSPs that treat AI as just another product line will find margin compression; the ones that internalize it as an operational capability will find themselves positioned exactly where clients need them – out in front.

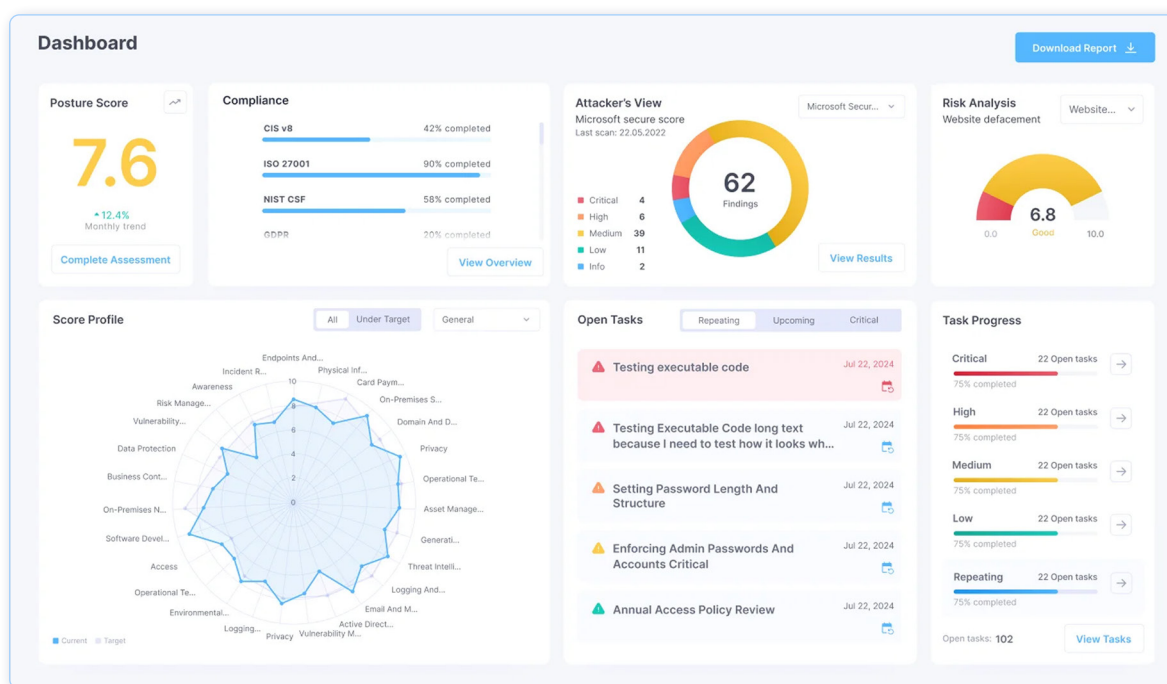
## The bigger shift

This set of questions reflects a broader transition underway across the industry. AI is no longer a future capability to plan for, it is an active variable in how services are delivered, secured, and valued today.

The service providers navigating this shift most effectively are not chasing every new tool or trend. They are focusing on structure: governance, controlled adoption, practical use cases, and clear client guidance. Across all five questions, one theme dominates, **the winning providers are moving from reactive operations toward governance, advisory, and strategic guidance.**

## Where Cynomi fits: the **CISO Intelligence** advantage

That shift, from operator to trusted advisor, is exactly what Cynomi was built to enable. And it starts with a simple truth the market is catching up to: AI assistants are dead. Service providers don't need another chatbot that asks you to write the prompt, review the draft, and paste the result somewhere useful. That is more work in a new wrapper.



Cynomi takes a different path. As the agentic Security Growth Platform for service providers, powered by CISO Intelligence, Cynomi embeds the decision-making logic of an experienced security leader directly into the workflow. Our AI Co-Workers read each client's posture and produce the policy, plan, assessment, or report your team would otherwise build by hand, with the reasoning shown so you can trust and explain every recommendation. That is the difference between an assistant and a security force multiplier.

It maps to three outcomes, the promise at the heart of the platform:

#### Know more.

Senior-level context, explainability, and portfolio-wide visibility into risk, gaps, and client opportunity.

#### Do more.

Guided, agentic workflows that turn assessments into remediation programs and map 40+ compliance frameworks as a single continuous effort.

#### Grow more.

Security gaps surfaced as service and recurring-revenue opportunities, so security becomes a growth engine instead of a cost center.

The result is measurable. Partners report up to 60% security revenue growth, 70% faster assessments, and roughly 30% margin improvement, achieved by standardizing delivery rather than adding headcount. AI is raising client expectations fast. Cynomi is how providers meet them at scale, across every client and every maturity level.

## 60%

security revenue growth  
reported by partners

## 70%

faster assessments

## ~30%

margin improvement



**Ready to lead the AI conversation with your clients?**

[Learn more about the Cynomi Security Growth Platform](#)

[Book a demo for your team](#)

[Join our MSP Growth Community weekly — register here](#)

## About Cynomi

Cynomi is the agentic Security Growth Platform for service providers, powered by CISO Intelligence—with the decision-making logic of an experienced security leader embedded into every workflow. Purpose built for MSPs, MSSPs and consultancies, Cynomi helps service providers deliver, scale, and grow cybersecurity services across every client and every maturity level. By combining complete security program management with portfolio-level revenue insights, Cynomi turns cybersecurity into a repeatable, profitable growth engine that improves margins, standardizes delivery, strengthens client trust, and uncovers new recurring revenue opportunities. Partner with us at [www.cynomi.com](http://www.cynomi.com).