

FOR IMMEDIATE RELEASE

MEDIA CONTACT

Brandon Rhea · RYTHMz
bradon.rhea@rythmz.com

SCOUTz Comes Out of Stealth to Retire the “So, Tell Me About Your IT” Meeting

The security sales intelligence platform gives MSPs dated evidence before the first meeting, then keeps it attached through delivery and reassessment.

PHOENIX, Ariz. (September 9, 2026) — SCOUTz, a security sales intelligence platform for managed service providers, today came out of stealth and opened a 30-day open beta to any MSP that applies at scoutzsecurity.io. The platform is built for the part of the sales process that MSP tooling has skipped: everything between a booked first meeting and a signed client.

The channel has no shortage of tools and programs that get an MSP the first appointment. None of them let the MSP walk into that appointment with confidence and evidence, so the seller starts discovery from zero and opens with the line every business owner has heard before: so, tell me about your IT. The marketing company earns the meeting. The PSA and RMM earn their keep after the contract is signed. Everything in between has run on charm and a template.

SCOUTz owns the missing middle

Before the meeting, it pairs the prospect's public events, such as a new location or an IT hire, with its own dated external evidence, then prepares the questions to ask in the room, so the MSP arrives knowing why the account matters. In the meeting, an outside-in domain review covers email authentication, certificates, subdomains, and exposed services, drawing on a registry of 156 distinct check types that each carry an authored explanation and next step, with no agent, no install, and no login required. Those signals justify a better question; SCOUTz never presents them as proof of what sits inside the business.

After the meeting, one click of read-only consent lets SCOUTz review the Microsoft 365 tenant: identity, application, consent, security, and managed-device context, plus AI readiness views for Microsoft Copilot, ChatGPT, Claude, and Gemini built from the tenant's application access evidence. There is no agent, install, or configuration change. SCOUTz does not read mail, documents, files, chats, or prompts.

Every finding traces to a named check and the date it ran, and an unknown never scores as clean. Findings carry fix guides with prerequisites, steps, validation, and rollback, a work plan the MSP owns, and ticket-ready text for the PSA. A rescan compares new evidence against a pinned baseline, so the next quarterly review rests on what changed, and Studio builds a client-safe edition for the business owner and an operator edition for the MSP's technical team from the same evidence.

“There are a ton of tools, programs, and marketing companies that will get an MSP the first meeting. What none of them do is put the MSP in that room already knowing something true about the business,” said Steve Copeland, founder of SCOUTz and CEO of RYTHMz. “I built two MSPs, so I know what that meeting feels like when you walk in with a deck and a story and walk out with a follow-up. The guy selling solar and the woman selling roofing both have better tools for a first meeting than MSPs do. All service businesses sell the same way, and we have been woefully behind on that. Today that changed.”

Built around evidence, consent, and people

The platform's limits are deliberate. SCOUTz is read-only by design and never changes a client's environment, and it refuses to model dollar losses from hypothetical breaches. AI handles drafts and explanations; deterministic checks decide whether a finding exists, and people own the final claims. Every finding is a check that ran, on a date, not AI pretending a product exists.

“Everyone in this industry has seen the slide with an employee's stolen password on it. We refused to build that. Not because we can't find it, because it's not right,” Copeland said. “Fear gets you a meeting and costs you the relationship. Show a business owner what was checked, what was found, and when, and they can make a decision. That is the conversation that closes.”

Before opening the beta, SCOUTz ran a closed program with fifty MSPs drawn from three MSP peer communities. Their feedback was worked through the product in full, and the group remains the SCOUTz founders group. One of them ran it from his phone on the client he had just met with. “Man, I wish I had this in the meeting I just walked out of,” said Zach Kinder, President and Partner of Net-Tech Consulting, a managed IT and cybersecurity firm in El Paso, Texas.

Copeland started building SCOUTz nine months ago, right after finishing The 3AM Test for MSPs, for what he calls the people still in the seat. “I built it for a community that desperately needs tools that were not built by vendors, or by people who have never sat in the seat trying to close a deal so they could make payroll,” he said.

What's next

First, a portfolio view that shows everything that changed across an MSP's clients since the last login. Then Google Workspace review, built against CISA's Secure Cloud Business Applications baselines. Behind it, the same evidence model is planned for Apple devices through read-only connections to the MDM platforms MSPs already run, for framework mapping across NIST, CIS, and CMMC using NIST's machine-readable catalogs, and for an application and AI governance record spanning every connected platform.

Each addition has to help an MSP answer the same questions about an account: what needs attention, what changed, why it matters, what to do, and who to talk to. Whatever ships, a finding that maps to a framework is never presented as compliance, and no release will blend platforms into a single score.

Availability

SCOUTz opened this week as an open beta: 30 days at \$0, starting when the workspace is provisioned. Every application is reviewed before access is provisioned, and participants receive the price, effective date, and cancellation terms in writing before any charge. List price is \$279 per month. A free public domain score runs on the site with no signup.

About SCOUTz

SCOUTz is security sales intelligence for managed service providers. It hands the MSP account context and dated evidence before the first meeting and keeps that evidence attached through review, delivery, and reassessment, so the story the MSP sold is the story it proves. SCOUTz is self-funded, headquartered in Phoenix, Arizona, and built by RYTHMz for the channel. Learn more at scoutzsecurity.io.

About RYTHMz

RYTHMz is a channel-only 5G connectivity company serving more than 180 MSP partners and the 2025 ASCII Cup Vendor of the Year. Learn more at rythmz.com.

###