

EXECUTIVE PAPER · MSP PARTNERS

Put Senior Engineering Behind Your Brand

Managed service providers lose clients and deals to work their teams cannot staff. Owners should secure white-label senior engineering for escalations and projects, under a contract that fixes the handoff, the access and who owns the client.

AUTHOR

Chris Watkins

SERVICE

MSP Partners

FOR

CEO, COO, Owner · 12 min read

AT A GLANCE

The problem. Clients now ask their managed service provider for cloud migrations, disaster recovery design, security architecture and AI. Most MSPs staff for day-to-day support. In Kaseya's 2026 survey of more than 1,000 MSPs, 48% named AI and automation as clients' top need, and a third of new clients had left another MSP. ISC2's 2025 study found 59% of security teams reporting critical or significant skills gaps.

Why it persists. A senior architect costs more than most MSPs can keep busy, so owners decline the project or hand it to the best technician they have. Both choices put the client relationship at risk, and the second can put the client's systems at risk too.

The recommendation. Contract for senior engineering capacity that works under your brand, inside your ticketing system, through named and logged accounts. Put the handoff, the access rules and client ownership in writing before the first escalation. Track hours and outcomes so you know when to hire.

The Decision in Front of You

A client asks for something the team cannot do well: a migration off an aging virtualization platform, a disaster recovery design the auditors will accept, an incident that has beaten the level-two technicians for three days, or a first AI system connected to client data. The owner has four choices. Decline the work. Give it to a capable but junior engineer and hope. Hire a senior engineer. Or contract senior capacity that works behind the MSP's brand.

This paper argues for the fourth choice, with the contract written first. The stakes are the client relationship. In Kaseya's 2026 State of the MSP Report, 33% of new clients were switching from another MSP, and a Kaseya executive said clients leave providers that lack the skills, tools or technology they need [1]. A declined project often leaves with the client who asked for it.

The risk on the other side is real as well. A partner engineer with administrator rights to client systems becomes part of the client's supply chain. The terms that govern that access matter as much as the engineer's skill.

What's Happening

Clients are asking for more than MSPs staff

Kaseya's 2026 survey of more than 1,000 MSPs found 48% ranked AI and automation as their clients' top need for the year, ahead of cybersecurity and backup [1]. Only 13% said AI was a meaningful source of revenue for them [1]. Seventy-one percent named winning new customers as their top business

challenge [1]. In Kaseya's previous survey, 45% of MSPs in Europe, the Middle East and Africa named staffing as their top issue [2].

The wider talent market offers little relief. ISC2's 2025 Cybersecurity Workforce Study surveyed 16,029 professionals: 95% reported at least one skills need on their team and 59% called their gaps critical or significant, up from 44% in 2024 [4]. Eighty-eight percent had experienced at least one significant consequence from a skills shortage [4]. Thirty-three percent said they lacked the resources to staff their teams adequately, and 29% said they could not afford to hire people with the skills they needed [4]. AI and cloud security topped the list of skills in demand, at 41% and 36% [4].

Partnering is already normal

The channel has already moved toward shared capacity. CompTIA's IT Industry Outlook 2025 reported that 90% of channel firms partner with peers in response to the growing complexity of technology, and 81% said those relationships had been positive [3]. The open question for most owners is how to structure a partnership so the MSP keeps the client, controls the access and can prove what was done.

MSPs are an attack path, and regulators have noticed

Attackers target MSPs because one provider's tools reach many clients. In July 2021 the REvil group used Kaseya's VSA remote management software against Kaseya's own customers: by the company's count fewer than 60 of them, most providing IT services to other firms, were compromised directly, and the impact reached as many as 1,500 downstream businesses [11]. Five national cyber agencies, with the NSA and FBI, issued joint guidance in 2022 on protecting MSPs and their customers [5]. It tells customers to require, in the contract, who owns hardening, detection and incident response, how and when the MSP reports incidents, multifactor authentication on every MSP account, and disabling of MSP accounts when the relationship ends [5]. It also tells both sides to manage risk from subcontractors [5]. NIST SP 800-161 Rev. 1, updated in November 2024, sets out the same discipline for supply chain risk generally [12].

In the United Kingdom, the Cyber Security and Resilience Bill introduced on 12 November 2025 proposes bringing some MSPs under regulation [13]. Government research published with it counted 12,867 UK MSPs, employing about 343,762 people with an estimated £51 billion in revenue, and estimated that around 1,214 could fall in scope depending on final definitions [13].

Three cases from 2024 and 2025

ConnectWise ScreenConnect, 2024. On February 19, 2024, ConnectWise disclosed an authentication bypass in on-premises ScreenConnect, a remote access tool widely used by MSPs, rated 10 out of 10 for severity [6]. An anonymous attacker could create an administrator account and take over the server [6], and administrators could run code on the server with system rights [8]. Exploitation began about a day after disclosure, and the Shadowserver Foundation counted about 3,800 vulnerable servers [7].

ConnectWise patched its cloud instances itself, while on-premises customers had to upgrade [6]. The lesson for this paper: a remote access tool is the shared door to every client, and an MSP needs someone who can assess and close a flaw like this within hours.

SimpleHelp and DragonForce, 2025. In 2025 Sophos responded to an attack in which a threat actor likely exploited a chain of three SimpleHelp vulnerabilities, gained control of an MSP's remote management instance and used it to deploy DragonForce ransomware and steal data [10]. The attacker gathered information across multiple client environments; one client with managed detection and response stopped the attack, while the MSP and other clients were encrypted and had data stolen [10]. In June 2025 CISA warned that ransomware actors had used the same unpatched SimpleHelp software to reach the customers of a utility billing software provider [9]. The lesson: every account and tool a partner uses on your clients' systems widens this exposure, and the contract has to say how it is controlled.

Marks & Spencer and its IT service desk, 2025. In April 2025 the UK retailer Marks & Spencer suffered a cyberattack that halted online orders from April into June; the company later put the total cost at about £136 million [14], and trade press estimates ran as high as £300 million [15]. In October 2025 M&S said its contract with Tata Consultancy Services for its IT service desk had ended after a tender begun in January [15]. Both companies deny any link to the attack, and TCS said its review found the vulnerabilities did not originate in its networks [15]. The lesson for MSP owners: after a major incident, every provider in the client's access chain comes under the client board's scrutiny, and the one with clear records of what each person did and could do is in the strongest position.

SIDEBAR: WHAT "WHITE-LABEL" MEANS HERE

White-label senior engineering means a partner's engineers work under the MSP's name, in the MSP's ticketing system and client channels, while the MSP keeps the contract, the billing and the relationship. It differs from referral, where the client contracts the specialist directly, and from resale, where the MSP passes through a third party's service. Whether to disclose the partner to the client is a contract question covered below.

Why the Usual Approach Fails

Declining the work feels safe. The client goes elsewhere for the project, the other firm learns the environment, and at renewal it is the obvious alternative. Kaseya's switching figure shows how often that ends with the client moving [1].

Stretching junior staff fails more slowly. A level-two technician can follow a migration runbook. Writing one, with a rollback path and a tested recovery point, takes years of production experience. The ISC2 data shows what happens when teams run short of skills: most report significant consequences, and many report more than one [4]. In an MSP, those consequences land on a client.

Hiring a senior engineer is sound when there is enough work. Most MSPs have senior work in bursts: a migration this quarter, a hard escalation next month, a disaster recovery test twice a year. A full-time architect at a fully loaded salary sits underused between bursts, and leaves when the work gets repetitive.

An informal partnership is the fourth failure: a trusted contact's firm, a shared administrator login, no written terms. That arrangement creates exactly the risks the 2022 joint guidance warns about, from shared credentials to accounts nobody disables when the work ends [5].

The Framework: The Bench Contract

The Bench Contract treats outside senior engineering as part of the MSP's own service. It has four parts, and all four are agreed before the partner touches a client.

Exhibit 1. The Bench Contract: four parts agreed before the first ticket

Part	What it fixes	Minimum terms
Scope	Which work goes to the partner	Named tiers: level-three escalation, scoped projects, architecture review; response times per tier; what stays with the MSP
Handoff	How work enters and leaves	Tickets stay in the MSP's system; MSP engineer stays on every escalation; partner returns a fix, a root cause and a runbook the MSP can reuse
Access	What the partner can reach, and the record of it	Named individual accounts, multifactor authentication, least privilege, time-limited elevation, all sessions logged; no shared credentials; accounts disabled at the end of each engagement [5]
Ownership	Who owns the client and the work	MSP holds the client contract and billing; non-solicitation of clients and staff; documentation and code belong to the MSP or client; partner incident reporting within a set number of hours; insurance and liability limits stated

Source: author's framework, access and reporting terms drawn from the 2022 joint guidance on MSP security [5].

Two terms need care. The first is disclosure. Read each client contract for subcontracting and data-processing clauses before the partner works on that client, and disclose the arrangement wherever the contract or the law requires it. The second is the handoff back. The value of a senior partner compounds when each escalation leaves a runbook behind and the MSP's own engineer could handle the same problem next time.

In practice an escalation follows one path. The client raises a ticket with the MSP. The MSP's level-two engineer diagnoses it and escalates. The partner's senior engineer works it through a named, logged account, and records the fix, the root cause and a runbook in the MSP's ticket. The MSP reports the outcome to the client under its own brand.

What it costs against a hire

The figures below are the author's illustrative estimate. Assume a senior engineer costs $220,000 a year fully loaded and a partner bills $200 an hour for senior work.

Exhibit 2. Below about 1,100 hours a year, contracted capacity costs less than a hire (author's illustrative estimate)

Senior hours needed per year	Partner cost at $200 an hour	Full-time hire at $220,000
300 (escalations only)	$60,000	$220,000
600 (escalations plus two projects)	$120,000	$220,000
1,100 (break-even)	$220,000	$220,000

Source: author's illustrative estimate. Break-even hours = $220,000 ÷ $200. Excludes recruiting time, management overhead and the margin the MSP earns on project work.

The other side of the ledger is revenue. A $300,000 migration delivered through a partner whose cost is 65% of the price leaves the MSP $105,000 of gross margin it would not have earned by declining, and keeps the client away from a competitor. The owner should track partner hours by month. Once they run steadily near the break-even line, hire.

Costs, Risks, and Tradeoffs

Exhibit 3. What contracted senior capacity costs, and when it is wrong

Area	Cost or risk	Mitigation
Margin	Senior hourly rates cut project margin	Price projects with partner cost included; quote fixed scopes for repeatable work
Supply chain exposure	Another firm holds privileged access to client systems [9][10]	Named accounts, MFA, logging, time-limited elevation, account removal at engagement end [5]
Client relationship	The partner could approach clients directly	Non-solicitation clause; MSP holds the contract and all client communication
Knowledge drain	Skills stay with the partner and the MSP's team does not grow	Require runbooks on every ticket; pair an MSP engineer on every project
Disclosure	Client contracts or law may require naming subcontractors	Review contracts before assignment; disclose where required
Partner dependency	The partner's availability or failure becomes yours	Response times in contract; a second partner or a planned hire for critical skills
When this is wrong	The MSP has steady senior demand above the break-even line, sells a specialty that is its core identity, or has clients whose contracts or regulators forbid subcontracting	Hire, build the practice in house, or refer the client directly with a clear fee arrangement

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	List the projects declined and escalations that ran past their target in the last 12 months. Estimate annual senior hours. Review client contracts for subcontracting and data-processing terms.	MSP owner with service delivery manager	A written count of lost deals, overdue escalations and estimated senior hours
First 90 days	Select a partner. Sign a Bench Contract covering scope, handoff, access and ownership. Create named, logged partner accounts with MFA. Run the first escalation through the MSP's ticketing system.	Owner with security lead	Signed contract; zero shared credentials; first escalation closed with a runbook attached
First 90 days	Take one previously declined project type to market with partner capacity priced in.	Owner with sales lead	First partner-backed project signed at target margin
First 365 days	Review partner hours, response times, client satisfaction and runbook reuse each quarter. Audit partner accounts. Decide whether volume justifies a hire.	Owner with finance and security lead	No partner account active without an open engagement; hire-or-continue decision made on measured hours

Source: author's recommendation.

Questions to Ask Your Team

1. Which projects did we decline or lose in the last year because we lacked the skills, and what were they worth?
2. Which escalations stayed open longest, and who finally closed them?
3. How many senior engineering hours would we have used last year if we had them?
4. Which client contracts restrict subcontracting or require us to name subprocessors?
5. If a partner engineer worked on a client tonight, could we show every account they used and every action they took?
6. Who disables partner access when an engagement ends, and how do we check it was done?
7. How many of our level-two engineers could handle last quarter's hardest escalation if it recurred?

Closing

Clients expect their MSP to handle migrations, recovery, security architecture and now AI, and the senior engineers who do that work are scarce and expensive to keep busy. Contract that capacity under your own brand, run it through your own ticketing system and named accounts, and put the handoff, access and client ownership in writing before the first ticket. Measure the hours, keep the runbooks, and hire when the volume justifies it.

Sources

[1] ITPro. "AI demand soars as traditional deal sizes shrink, Kaseya reports." Coverage of Kaseya, "2026 State of the MSP Report." 2026. https://www.itpro.com/technology/artificial-intelligence/ai-demand-soars-as-traditional-deal-sizes-shrink-kaseya-reports.

[2] IT Europa. "MSPs Target Profitability Amid Competitive Pressures." Coverage of Kaseya, "2025 State of the MSP Industry" survey. 2025. https://iteuropa.com/news/msps-target-profitability-amid-competitive-pressures.

[3] CompTIA. "Optimism outweighs worries and uncertainties for tech pros and IT channel companies in CompTIA IT Industry Outlook 2025." Press release. 2024. https://www.comptia.org/en-us/about-us/news/press-releases/optimism-outweighs-worries-and-uncertainties-for-tech-pros-and-it-channel-companies-in-comptia-it-industry-forecast-2025/.

[4] ISC2. "ISC2 Publishes 2025 Cybersecurity Workforce Study." 2025. https://www.isc2.org/insights/2025/12/isc2-publishes-2025-cybersecurity-workforce-study.

[5] Cybersecurity and Infrastructure Security Agency, NSA, FBI, NCSC-UK, ACSC, CCCS and NCSC-NZ. "Protecting Against Cyber Threats to Managed Service Providers and their Customers." Alert AA22-131A. 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a.

[6] ConnectWise. "ConnectWise ScreenConnect 23.9.8 Security Fix." Security bulletin, CVE-2024-1709 and CVE-2024-1708. 2024. https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8.

[7] BleepingComputer. "ScreenConnect critical bug now under attack as exploit code emerges." 2024. https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/.

[8] Huntress. "A Catastrophe For Control: Understanding the ScreenConnect Authentication Bypass." 2024. https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass.

[9] Cybersecurity and Infrastructure Security Agency. "Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider." Alert AA25-163A. 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-163a.

[10] Sophos. "DragonForce actors target SimpleHelp vulnerabilities to attack MSP, customers." 2025. https://www.sophos.com/en-us/blog/dragonforce-actors-target-simplehelp-vulnerabilities-to-attack-msp-customers/.

[11] Kaseya. "Important Notice July 2nd, 2021." Incident updates for the VSA attack. 2021. https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-2nd-2021.

[12] National Institute of Standards and Technology. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." NIST SP 800-161 Rev. 1, Update 1. 2024. https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final.

[13] Department for Science, Innovation and Technology. "Research on managed service providers 2025." Published with the Cyber Security and Resilience Bill. 2025. https://www.gov.uk/government/publications/research-on-managed-service-providers-2025.

[14] The Register. "M&S pegs cyberattack cleanup costs." November 5, 2025. https://theregister.com/2025/11/05/ms_pegs_cyberattack_cleanup_costs/.

[15] Retail Gazette. "M&S terminates IT contract." 2025. https://www.retailgazette.co.uk/blog/2025/10/ms-terminates-it-contract/.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.