Propulsion

The MSP breakpoint

What it takes to lead in the age of AI, cybersecurity, and compliance

Contents

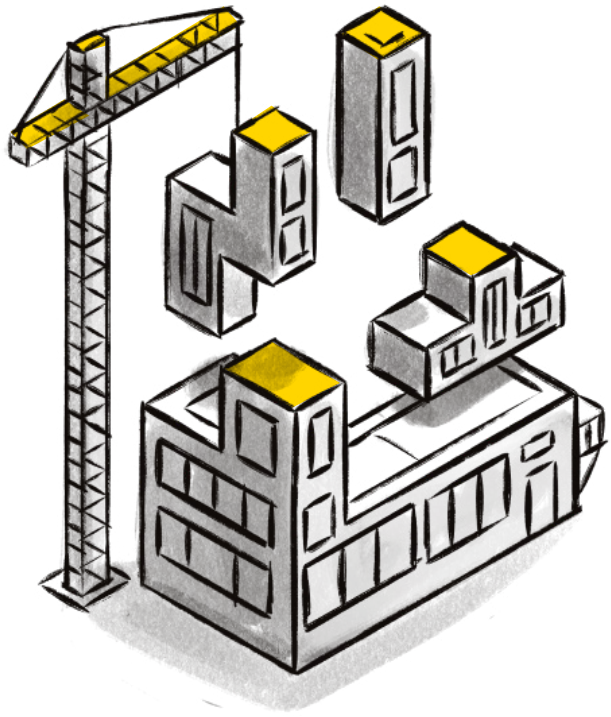
Introduction:

The MSP gap and the rise of the *next-gen provider*

Technology is rewriting the playbook for small and mid-sized businesses (SMBs) and their MSPs. SMBs aren't abandoning the help desk or the need for reliable IT support: those remain essential. But they're *also* facing a far broader set of challenges: navigating a wave of digital advancements, defending against escalating cybersecurity threats, and keeping pace with evolving compliance requirements—all at once, with limited resources and little margin for error.

The reality is, many SMBs are struggling to get a handle on it all. AI, advanced security, compliance, and automation now form the backbone of how companies operate, compete, and grow, but most lack the expertise or bandwidth to put them to work. The role of the modern MSP is to educate and empower SMBs to turn these demands into differentiation, growth, and efficiency. The next generation of providers delivers strategic value as true technology partners: fluent in client challenges, focused on outcomes, and equipped to move at the pace of change.

But most MSPs aren't built for *this moment*



Recent industry data shows that nearly 80% of managed service providers have hit a ceiling in their ability to advance their security and technology stacks.[1] Despite years of pressure to build out cybersecurity services, most MSPs still struggle to understand, staff, and deliver them effectively. Nearly 40% of MSP staff time is still spent on manual tasks, and 88% say this prevents them from innovating, ultimately stalling progress for both their clients and themselves.[2] Too often, security tooling is bolted on reactively (because customers ask for it, competitors offer it, or analysts recommend it) *without* the depth of expertise required to make it work.

That same pattern extends to industry specialization. Most MSPs still operate as generalists, even as demand grows for deeper vertical expertise in regulated and compliance-driven environments. This is especially true for government agencies, DoD contractors and subcontractors, finance, legal, healthcare, and manufacturers operating within regulated supply chains. Outdated toolsets, legacy business models, and shallow expertise in AI, security, and automation are leaving many MSPs flat-footed *just* as client needs are accelerating.

That gap is becoming impossible to ignore. SMB dissatisfaction with traditional MSPs is rising, and scrutiny is mounting. For example, while 84% of MSPs now manage cybersecurity for their clients, 77% report increased questioning of their security capabilities.[3] And while cyber risks are a top concern for nearly 60% of MSPs, only a small minority cite talent (3.7%) or compliance (2.1%) as major threats.[4] That's a dangerous disconnect between what clients expect and what many MSPs prioritize (or are equipped to deliver).

The MSP gap, by the numbers

80%
have hit a ceiling advancing their tech & security stacks

88%
say manual work blocks innovation

77%
report rising client scrutiny of their security capabilities

Just 3.7% cite talent & **2.1%** cite compliance
as major threats (& therefore as priorities)

Too many MSPs are still running yesterday's playbook... and it's showing

And it's not just technology that lags: talent is an equally pressing gap. Most MSPs still view technicians as interchangeable resources rather than investing in the specialized skills required to master AI, security, and compliance. Without building and continually developing a bench of highly trained people, providers will struggle to evolve their service models. As one industry leader puts it: "If we train people, they might leave, but if we *don't* train them, they might stay… and we don't want the people who don't want training."

At Propulsion, we recognize that MSPs are at an inflection point… and the stakes are high. Those that win won't stop at managing IT infrastructure and providing help desk services; they'll architect outcomes as business partners. With intelligent automation, embedded security, and built-in compliance at every layer of their offering, next-gen MSPs will help SMBs modernize operations, adopt AI responsibly, and stay ahead of regulatory, economic, and competitive pressure—from frameworks like NIST, CIS, CMMC, SOC 2, and PCI DSS to emerging AI governance standards. Just as importantly, they'll apply those same capabilities *internally*, using AI and automation to scale delivery, reduce manual work, and create more space for strategic engagement with customers.

Leaders like Canalys and Jay McBain predict that AI-native platforms will define "MSP 4.0."[5] But tech alone won't win the future. The next generation of MSPs will take accountability for measurable business impact (not just uptime). That means guiding SMBs through AI readiness, embedding cybersecurity as a foundation for automation, consolidating toolchains, and driving efficiency across sales, HR, and finance. It means navigating new AI regulations, anticipating compliance shifts, and leading the change management that keeps teams moving forward. The MSPs built for this moment won't act like vendors. They'll operate as long-term allies: focused not just on systems, but on shared success.

We wrote this for decision-makers on both sides of the table:

- SMB leaders asking "*Is our MSP still the right fit for where we're headed?*"
- CIOs & IT leaders looking to future-proof their tech partnerships
- MSP founders deciding whether to scale, specialize, or join a next-gen platform
- Execs navigating the shift from reactive support to strategic enablement
- Anyone evaluating what it means to be future-ready in the age of AI, automation, & cybersecurity

This whitepaper outlines the new bar for MSPs: what the market demands, how top performers are evolving, and what it takes to stay competitive in the AI era. It's written for SMBs reassessing whether their current provider is future-ready.

Through real-world data, analyst insights, and operator perspectives, we'll lay out the blueprint for choosing a modern MSP: one built for outcomes, grounded in trust, and ready to lead in an AI-powered, security-first world.

The evolution of the MSP (and the end of "*MSP 3.0*")

The managed services model has always evolved alongside technology, but today's inflection point is fundamentally different. Earlier shifts were largely about tools: moving from break/fix to IT infrastructure management, then cloud migration, then basic cybersecurity. Each phase focused on delivering efficiency, uptime, and cost savings.

Now, SMBs aren't just looking for technical support; they're looking for strategic enablement. They need partners who can help them adopt AI responsibly, embed cybersecurity into every layer of operations to reduce risks, navigate shifting compliance requirements, and automate business functions from finance to HR and Marketing. Meeting that need requires more than stacking new tech on top of old models. It demands a reimagined role for the MSP: not a service vendor, but as a business partner accountable for real business outcomes, resilience, and competitive advantage.

Let's take a look at how we got here (and what it'll take to move forward).

From reseller to risk partner:

a brief history of the MSP model

1 Value-added reseller (VAR): the product-centric origin

Before MSPs, enterprise IT needs were often met by centralized service bureaus. But as distributed computing gained traction in the 1980s, businesses shifted to on-premise infrastructure, opening the door for value-added resellers (VARs). These firms sold servers and networking equipment, bundling in installation and basic support.

But margins shrank as hardware became commoditized in the mid-1990s; and the transactional, project-based model became unsustainable. To stay viable, VARs needed new revenue streams and a more service-oriented identity. Many began offering support services, giving rise to the break/fix model.

Business model
Hardware/software sales

Service scope
Light implementation, often sold as an add-on

Key features
Product procurement, installation, & basic setup

Economics
One-time revenue driven by product resale margins, which steadily declined as hardware became commoditized

2 Break/fix: reactive services and unpredictable costs

The commoditization of hardware wasn't the only pressure point: growing complexity in SMB IT environments called for responsive support. That demand birthed the break/fix model. In the late 1990s and early 2000s, many VARs shifted to hourly IT support, charging to fix problems as they arose.

The model, however, created multiple pain points. It offered no incentive to prevent downtime, was entirely reactive, and left SMBs with unpredictable, often lumpy costs from month to month. A string of issues could send support bills soaring, even as the business absorbed the hit of lost productivity. (Even today, downtime for small businesses typically costs between $137 and $427 per minute, meaning a three-hour outage could total upwards of $75,000.)[6] As IT environments grew more complex, the reactive model proved inefficient, expensive, and unsustainable. The shift to proactive support was inevitable.

Business model
Billable hours plus hardware sales

Service scope
On-demand maintenance across hardware, software, & network infrastructure

Key features
Reactive troubleshooting, in-person fixes, limited SLAs

Economics
Unpredictable, lumpy revenue tied to outages and customer issues

3 MSP 1.0: the rise of proactive support and recurring revenue

Internet connectivity and remote monitoring tools in the early 2000s allowed MSPs to shift from reactive firefighting to proactive system management. As internet access improved in the early 2000s, tools like Kaseya and ConnectWise enabled MSPs to shift from reactive firefighting to proactive monitoring, management, and a new business model of contract-based recurring revenue.

This leap forward reduced downtime and smoothed out cash flow for both the MSP and SMBs. But MSPs were still focused on IT infrastructure uptime, and not aligned with broader business goals or outcomes.

Business model
Recurring revenue

Service scope
Provisioning & management of on-prem devices, infrastructure, telecom, & applications

Key features
Remote monitoring, ticketing, patching, preventive maintenance

Economics
Stabilized margins through standardized, packaged services

4 MSP 2.0: cloud enablement and security expansion

As AWS, Azure, and Google Cloud gained traction in the 2010s, cloud and SaaS adoption surged, prompting clients to demand more from MSPs: migration, integration, and protection across hybrid environments.

At the same time, the rapid increase and evolution of cyber threats created new levels of risk for SMBs, and a corresponding demand for stronger defenses. For MSPs, this represented both a revenue opportunity and a steep learning curve. Many added cybersecurity tools and services to their portfolios, but doing so required new training, expertise, and ongoing investment in talent. This phase marked a *shift toward* strategic partnership, but most MSPs still operated as system managers rather than enablers of business value.

Business model
Recurring revenue with upsell potential

Service scope
Remote management of hybrid infrastructure, telecom, cloud applications, & baseline cybersecurity

Key features
Cloud migration, endpoint antivirus, disaster recovery, first-generation security services

Economics
Higher margins driven by bundling cloud & security services, but added costs for staff training and expertise

5 MSP 3.0: basic automation, advanced security, and early compliance

As data moved to the cloud and attacks grew more sophisticated, cybersecurity became table stakes. COVID-19 only accelerated the shift toward remote-first operations and pressure to improve efficiency. By the late 2010s and early 2020s, rising cyber risk and regulatory complexity pushed MSPs to expand their security toolkits and experiment with automation.

But automation at this stage was limited. Most MSPs relied on scripts within their RMMs—useful for patching or device management, but far from the true workflow automation emerging today. Security was layered on in similar fashion: EDR, scripting, and remote monitoring often bolted onto existing stacks rather than integrated into cohesive systems. Despite the *appearance* of maturity, cybersecurity posture remained weak: by 2022, 60% of MSPs reported a security breach, and only 35% had access to the depth of security expertise, continuous monitoring, and incident response capabilities required to detect and contain threats effectively.[7] Compliance support was in its early stages, typically offered as checkbox-level services rather than meaningful risk mapping or audit readiness.

Business model
Premium recurring revenue model with incremental security & automation add-ons

Service scope
Remote management of hybrid cloud environments, devices, telecom, SaaS apps, & IT infrastructure

Key features
Basic scripting within RMMs, layered (but loosely integrated) security, early-stage compliance support

Economics
Stronger recurring revenue, some efficiency gains, but rising exposure due to weak integration and shallow expertise

As risks accelerate, bolt-on fixes are no longer enough. The next generation of MSPs will be defined by deep integration, intelligent automation, and risk-first design: built from the inside out. Closing these gaps isn't just about stacking new platforms or processes. It also requires investing in *people*—building the next generation of analysts, architects, and advisors who can translate technology into business impact. Without that human expertise, even the best tools fall short.

The evolution of the MSP model

Value-added reseller (VAR):
Hardware resale margins collapsed, pushing firms toward services

Break/fix:
Reactive support left SMBs with costly downtime and unpredictable bills

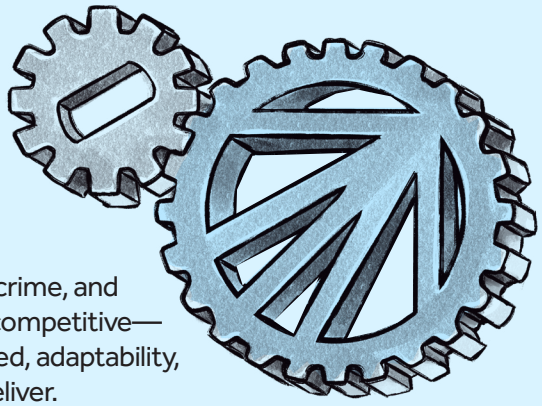
MSP 1.0:
Proactive monitoring stabilized IT uptime, but value stayed narrowly technical

MSP 2.0:
Cloud and security expansion exposed gaps in talent and integration

MSP 3.0:
Bolt-on automation and basic compliance proved insufficient against rising risk

Next-gen MSP: ?

Why MSP 3.0 is *no longer enough*



Today's SMBs are navigating increased costs, labor shortages, rising cybercrime, and generative AI all at once. They're expected to stay secure, compliant, and competitive—often without a full IT team. Meeting those demands requires a level of speed, adaptability, and strategic insight that yesterday's MSP model was never designed to deliver.

At the same time, MSPs face their own internal pressures. To scale effectively, they must adopt AI and automation in their own delivery models, reduce reliance on manual work, and harden their own security posture. They must also invest in talent, building and retaining teams with the advanced skills that modern security, compliance, and AI integration demand. Providers that fail to evolve on all three fronts (technology, process, and people) will fall behind.

For SMBs, that external pressure takes very real forms:

1 AI is making its way into every corner of the business

SMBs are using it for everything from prospecting emails to Support automation, but often without oversight. Nearly half (45%) report that employees are using generative tools without formal approval. They need partners who can help them deploy AI responsibly, with guardrails for security, ethical use, and business alignment.

2 Cyber threats have intensified

Sophisticated phishing, ransomware-as-a-service, and supply chain attacks now target SMBs at scale. 59% of organizations reported being hit by ransomware in the past year, and the average cost to recover from an attack (excluding the ransom payment) was $2.73 million in 2024.[8] SMBs need partners who can deliver real security maturity (not just basic tools) through 24x7 monitoring, layered defense, rapid detection, and strategic risk management.

3 Compliance is only getting more complex

Frameworks like NIST, CIS, CMMC, PCI DSS v4.0, HIPAA, SOC 2, and emerging AI guidance require SMBs to document controls, manage third-party risk, and prove due diligence—often without a dedicated compliance team. Only 22% of SMBs report having an advanced security posture.[9] Increasingly, these requirements are driven by customers, as large enterprises and government-adjacent organizations push security standards down the supply chain. SMBs need MSP partners who can simplify compliance through embedded controls, audit-ready reporting, and proactive risk management that scales with their business.

4 Automation is running into walls

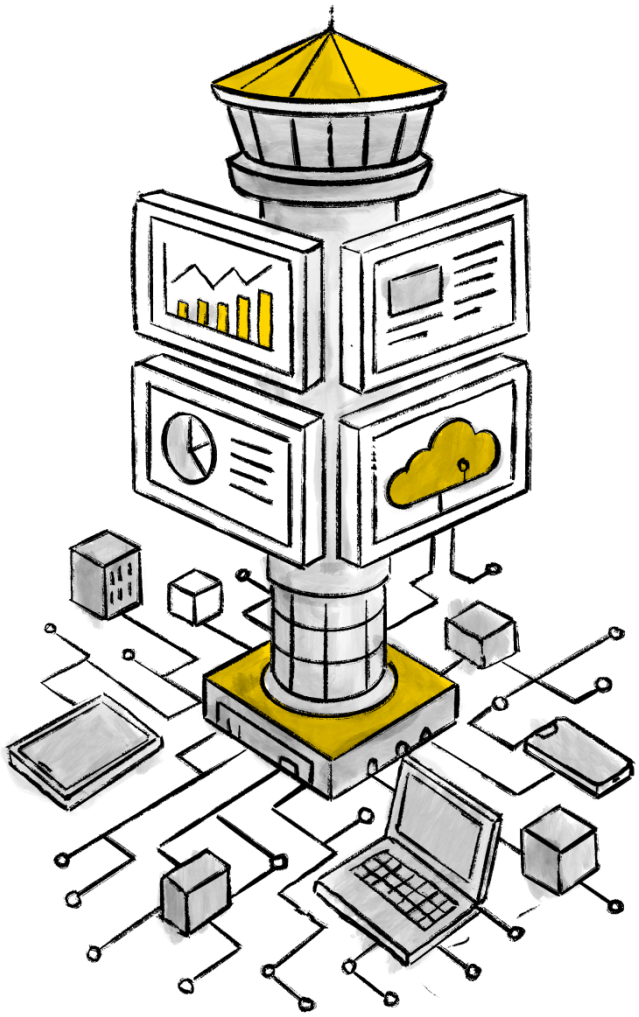
SMBs want to streamline hiring, invoicing, inventory, and support. Tools like Microsoft Power Automate, n8n, and UiPath are entering the stack, but results often fall short because most departments still operate in isolation, employees often lack the training or confidence to embrace automation fully, and SMBs rarely have the budget to hire the engineering talent required to build and maintain these systems. (Only 24% of SMBs have automated processes across more than two business functions.)[10] SMBs need MSPs who can break those silos: designing, integrating, and managing automation that connects systems, aligns teams, and drives real outcomes.

5 The stack is becoming unmanageable

In 2024, SMBs used an average of 58 different business applications.[11] As they adopt more tools across cybersecurity, automation, and compliance, integration becomes a bottleneck. Fragmented platforms increase overhead, introduce risk, and create operational blind spots. SMBs need MSPs who can *unify* (not just add to) their tech stacks, ensuring that new capabilities don't come at the cost of complexity.

6 Outcomes matter as much as uptime

SMBs are under pressure to make every investment count, and are expecting measurable results from their technology stacks. They're moving away from generic solutions toward vertical-specific, outcome-driven platforms that solve business-critical challenges out of the box. Yet 60% of SMBs struggle to measure the financial impact of automation.[12] They need MSPs who go beyond implementation to true enablement: tracking and accelerating ROI, driving operational efficiency, and helping leadership teams achieve long-term strategic impact. That level of enablement requires deeper specialization. The next generation of MSPs will organize around centers of excellence—building vertical expertise in industries like finance, legal, healthcare, and manufacturing—so they can align technology outcomes with the precise metrics and regulatory realities of each field.



⚠ These aren't just new tools or evolving checklists; they're a fundamental shift in what SMBs need from their technology partners. Sure, MSP 3.0 brought progress; but it wasn't built for this level of complexity, urgency, or strategic demand.

The case for next-gen MSP, in 7 data points

1. **45%**
of SMBs say employees are using gen AI tools without formal approval

2. **59%**
of organizations were hit by ransomware in the past year

3. **$2.73M**
the average cost to recover from a ransomware attack in 2024 (excluding ransom payments)

4. **Only 24%**
of SMBs have automated processes across more than two business functions

5. **Only 22%**
of SMBs report having an advanced security posture

6. **58**
business applications are used on average by SMBs in 2024

7. **60%**
of SMBs struggle to measure the financial impact of automation

What modern MSPs must own to stay relevant:

The new mandate *for tech partners*

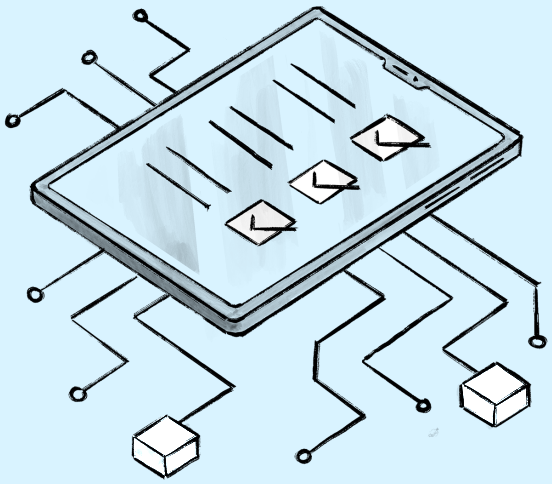
The bar hasn't merely been raised in recent years; it's been *redefined*. As SMBs face mounting complexity across AI, cybersecurity, automation, and compliance, the next generation of technology partners needs to do more than install tools or respond quickly. They must act as embedded, strategic enablers of growth, resilience, and efficiency. (That mandate extends *inward* too: next-gen MSPs need to invest in their own people, with programs that continually build the advanced skill sets required to deliver at this level.)

Rather than operating just at the infrastructure level, next-gen MSPs embed themselves in the *business* layer, where strategy, outcomes, and operations converge. They help clients move faster, spend smarter, and keep their systems secure and operations compliant. That requires moving beyond tools and tickets, and toward outcomes that actually shape the trajectory of a business.

The next-gen *MSP's scorecard*:

7 outcomes that matter

Today's SMBs expect their technology partners to help shape outcomes that drive performance, resilience, and long-term growth. The role of the next-gen MSP is to position technology as a strategic advantage, elevating it from a line-item expense to a driver of differentiation and growth.



That means contributing to:

Revenue growth

through AI-enabled sales workflows, faster lead response, and richer customer insights. MSPs must implement use case discovery, secure AI deployment, workflow integration, and ongoing model tuning across multiple departments.

Cost savings

via vendor consolidation, cloud spend optimization, and automated back-office operations. That means evaluating the full stack, eliminating redundancy, renegotiating vendor contracts, and redesigning processes from procurement to invoicing.

Operational efficiency

by connecting siloed systems and streamlining cross-functional workflows. That means building and maintaining integrations across CRMs, ERPs, ticketing platforms, and analytics tools, plus resolving data mismatches and access controls.

Risk reduction

through proactive cybersecurity, real-time detection, compliance alignment, and resilient architecture. MSPs must deliver layered security, 24/7 monitoring, mapped controls for CMMC, SOC 2, PCI DSS, and HIPAA, and simplify a growing maze of vendor tools.

Workforce productivity

by enabling automation, secure access, and collaborative tooling across teams. That means designing user-centric workflows, enforcing granular access policies, supporting hybrid environments, and providing tools employees actually adopt.

Customer experience gains

by eliminating friction in onboarding, support, and communications. That means reengineering support flows, integrating communications platforms, and accelerating time to resolution.

Smarter decision-making

via unified data pipelines, embedded analytics, and real-time visibility. That means integrating and normalizing data across business systems, building dashboards, and enabling leaders to act with confidence.

These expectations aren't abstract; they're fast becoming table stakes:

92% say they're willing to pay a premium for integrated solutions[13]

52% say they rely on MSPs to help them manage a spiraling number of disconnected security vendors & solutions[14]

45% say they'll switch providers if their MSP can't offer 24/7 monitoring or real-time incident response[15]

None of these outcomes lives in isolation. To deliver on this scorecard, MSPs must operate as architects, analysts, educators, and long-term advisors. They must also deepen their expertise by building centers of excellence in key industries like finance, legal, healthcare, and manufacturing, where client needs and compliance demands are most complex. And they must do it all securely, scalably, and repeatably… across industries, environments, and teams.

8 hats every modern MSP *must wear*

To deliver meaningful business outcomes in today's AI-powered, security-first world, modern MSPs must step into eight distinct roles (all at once!). This isn't an expanded services list; it's a redefinition of the role.

The Support Backbone

No matter *how* advanced the tech stack becomes, SMBs still need dependable day-to-day support. This role covers the help desk, troubleshooting, and responsive service that keeps operations running smoothly. It's the backbone of trust: solving problems quickly, minimizing downtime, and ensuring employees can stay productive. Without this foundation, none of the other hats can succeed.

The AI Readiness Coach

AI is showing up across every business function, but most SMBs lack a strategy for how to adopt it, or guardrails to manage the risk. Wearing this hat means helping clients assess readiness, identify and vet the right tools, create usage policies, and embed AI safely and ethically into real business workflows. Doing this well also requires training your own teams to stay ahead of fast-moving AI capabilities.

The Cyber Resilience Architect

The rise of cloud computing, connected devices, and a distributed workforce have erased the traditional perimeter and widened the attack surface, yet many SMBs still rely on outdated defenses. This role requires designing layered, proactive security architectures that include 24/7 monitoring, incident response, zero-trust frameworks, and compliance-aligned controls.

The Workflow Integrator

Automation isn't just for IT anymore. SMBs want to streamline processes across Sales, HR, Finance, and Customer Support. But siloed departments and scattered tools often stall progress. Modern MSPs must design, connect, and manage cross-functional workflows that boost productivity and eliminate manual work across departments.

The Compliance Navigator

Standards are evolving quickly, from NIST, CIS, HIPAA, and CMMC to the EU AI Act and new state-level AI laws. This hat calls for interpreting complex regulations, educating, conducting readiness assessments, mapping controls, maintaining audit readiness, and proactively advising SMBs on how to stay ahead of compliance risk.

The Tech Stack Strategist

SMBs are overwhelmed by redundant tools and fragmented systems. Wearing this hat means helping clients reduce sprawl, simplify integrations, eliminate cost centers, and build a tech stack that's scalable, secure, and fit for purpose.

The Change Management Partner

Even the best tools fall flat without adoption. Modern MSPs must guide teams through change, offering onboarding, enablement, support, and continual optimization to make sure systems are embraced and used effectively. That same commitment to enablement must apply internally: next-gen MSPs can't drive change for clients if they don't build a culture of continuous learning within their own teams.

The Trusted Business Advisor

Today's SMBs don't need another vendor; they need a partner who understands their goals and helps drive them forward. Wearing this hat means acting more like a true virtual CIO (vCIO) than a "virtual Captain Obvious." That means aligning technology with business priorities, embedding strategy into client conversations, and earning trust through measurable outcomes rather than ticket counts or SLAs. This role reframes technology from a cost center into a strategic advantage. It requires regular engagement with decision-makers and the ability to translate technical alignment into clear business impact.

The people factor

Technology and process only go so far. The next-gen MSP must also cultivate, train, and retain the skilled talent required to deliver advanced AI, cybersecurity, and compliance services. Just as important, it needs professionals who can consistently deliver exceptional customer experiences: account managers, support teams, and vCIOs who combine technical expertise with empathy, clarity, and strong communication. As AI becomes more prevalent, these human interactions matter more.

As one industry leader put it: "If we train people, they might leave. But if we *don't* train them, they might stay… and we don't want the people who don't want training."

The MSPs that thrive will be those that treat talent development as core infrastructure, not an afterthought.

These hats aren't optional; they're the uniform of the modern MSP. They demand strategic fluency, industry-specific specialization, and a commitment to continuous reinvention.

Next-gen MSPs must be equal parts technologist, strategist, and enabler. But operating at this level takes more than intent. It takes capital, technical depth, and organizational maturity that most teams weren't built to sustain. (And the market isn't slowing down to let them catch up.)

That's why many traditional providers—even those with great intentions—will struggle to level up.

The credibility gap:

Why most MSPs can't deliver what today's SMBs *need*

On paper, many MSPs (including those considered "MSP 3.0") claim to offer AI, cybersecurity, automation, and compliance services. They check all the right boxes on a capabilities list.

But in practice, most treat these as bolt-on add-ons: bundled tools, resold platforms, and shallow support that rarely connects to business outcomes. For example, in a recent Propulsion survey, 85% of SMB leaders said their MSP had recommended AI tools—but most described those recommendations as one-off mentions, not strategic guidance, and few saw evidence of the specialized talent required to make those tools work in practice.

The result? Checkbox compliance. Surface-level automation. Security in name only.

For SMBs, the risk is real. Partnering with an MSP that lists the right services but lacks the depth to implement them can lead to wasted spend, compliance failures, and preventable disruption.

The limits of legacy:

What's holding MSPs back

MSP 3.0 moved the needle, but it still can't meet the demands of today's SMBs. Here's why most providers aren't able to deliver:

1 Shallow specialization

Most MSPs remain IT infrastructure experts—skilled at keeping systems running, but not equipped for the new demands now emerging. Areas like AI, advanced automation, cybersecurity, and compliance are beginning to matter *most* to SMBs, yet few providers have the depth to deliver them effectively. Instead of offering integrated, business-aligned solutions, many bolt on lightly productized services, often reselling tools without the expertise to deploy them meaningfully. The result is siloed support and surface-level implementations that rarely deliver real outcomes. Few providers can:

- Tune AI models or implement usage guardrails
- Map controls to frameworks like NIST, CIS, CMMC, HIPAA, or PCI DSS
- Build end-to-end automations that span departments and systems

What this means for SMBs:

Without deep, cross-domain expertise, MSPs can't help SMBs deploy AI safely, automate strategically, or meet rising security and compliance demands. The result is more than inefficiency; it's exposure, wasted spend, and missed opportunities for transformation. In today's high-stakes environment, shallow specialization isn't just inadequate; it's dangerous.

---

2 Fragmented toolsets and no integration strategy

Many MSPs resell dozens of point solutions (one for email security, another for patching, another for backup, etc.) *without* a unifying architecture or integration plan. In most cases, the MSP bears the brunt of this complexity, managing an unwieldy stack across their client base. But the impact spills over to customers, too, who are often left unsure whether they're truly secure when their provider can't offer unified reporting or regular business/technical reviews.

In the security stack alone, the average MSP juggles four different tools from four separate vendors.[16] Some providers juggle 10, 20, or even 30 tools, creating environments that are inefficient for the MSP and nearly impossible to manage or secure at scale.[17] It's no surprise that 94% of MSPs say they're still searching for a unified platform to simplify delivery and reduce risk.[18] Choosing such platforms (and leveraging automation and AI to eliminate inefficiencies) is what sets the next-gen MSP apart.

What this means for SMBs:

Without centralized oversight or cohesive strategy, tool sprawl leads to blind spots, data silos, and integration failures. That means higher IT costs, overlapping features, lower ROI, and more risk. MSPs who can't connect the stack can't protect the business.

3 Internal AI use ≠ customer enablement

Most MSPs are using AI—but primarily for themselves, and often only in limited ways. While 75% report leveraging AI to streamline internal operations, in many cases that "usage" amounts to dabbling rather than deploying the technology to its full potential.[19] Nearly 90% also lack the knowledge to help clients do the same.[20]

That disconnect leaves SMBs flying solo. From AI-powered sales workflows to automated support, businesses are eager to adopt generative tools; but few receive the guidance, guardrails, or integration support they need from their MSP.

What this means for SMBs:

AI is reshaping how businesses operate, from sales and support to strategy and execution. But without expert guidance, SMBs risk deploying powerful tools with no guardrails: exposing sensitive data, overlooking compliance, and wasting time on poorly matched use cases. When MSPs keep AI expertise in-house, they leave clients vulnerable to costly missteps, and miss the chance to deliver real, transformative value.

4 Talent shortages and hiring constraints

Most MSPs are facing a talent crunch that limits their ability to evolve. A full two-thirds (66%) of technology providers report skills gaps on their IT teams, with AI/ML and cybersecurity tied as the top two areas of shortage (30%), followed by cloud computing (26%).[21] For many smaller or standalone MSPs, the challenge is compounded by cost: skilled resources are expensive, and hiring them at scale often isn't feasible while still running a profitable business. That leaves critical blind spots, especially when it comes to:

- Securing hybrid environments or build layered defenses
- Designing and govern safe, effective AI implementations
- Supporting automation strategies beyond basic IT workflows
- Delivering compliance-ready solutions with mapped controls

What this means for SMBs:

When MSPs can't attract or retain skilled engineers, SMBs are left with outdated strategies and overextended support. The consequence isn't just slower response times; it's missed innovation, higher risk exposure, and costly reliance on external consultants to fill the gaps. In today's environment, where specialized knowledge is key to transformation, staffing constraints translate into strategic stagnation.

5 Disconnected teams, no business translation

Most MSPs are still structured for *infrastructure*, not *outcomes*. Their teams operate in silos, with little collaboration across AI, cybersecurity, automation, and compliance. The result is no unified approach, no alignment on goals, and no clear accountability for long-term results. And without skilled people who can span these domains, even well-intentioned MSPs struggle to deliver real outcomes. Most MSPs lack:

- Shared workflows and handoffs across AI architects, security leads, and compliance advisors
- Clear ownership of business KPIs or transformation goals
- Post-deployment support, training, or lifecycle optimization
- The ability to translate technical outputs into real business outcomes (a gap that underscores the need for vCIO or vCISO engagements as part of the MSP experience)

What this means for SMBs:

Tools may get deployed, but impact is left to chance. No one owns adoption. No one aligns technology to business outcomes. And no one ensures systems are integrated, optimized, or actually used over time. Without a cross-functional delivery model and post-launch enablement, SMBs are forced to patch together fragmented solutions, and pay the price in lost efficiency, stalled progress, and unmet potential.

---

6 No vertical fluency

Many MSPs rely on a one-size-fits-all playbook, offering the same tools and templates to every client, regardless of industry. But the needs of a healthcare startup, a manufacturing firm, and a retail brand differ dramatically when it comes to workflows, data, compliance, automation, and the industry-specific applications that keep each business running. Today's vertical realities demand tailored solutions, and the next generation of MSPs will organize around centers of excellence: specialized teams built to go deep in key sectors like finance, legal, healthcare, and manufacturing, where compliance and operational complexity are highest:

- Healthcare workflows must support HIPAA compliance and secure onboarding
- Manufacturing systems must integrate MES, inventory, and asset management
- Retail tools must balance AI efficiency with PCI compliance and customer privacy
- SaaS environments must enforce SOC 2 controls and role-based access

What this means for SMBs:

Without vertical fluency, even best-in-class tools miss the mark. Compliance risks slip through the cracks, workflows break down, and teams are left wrestling with one-size-fits-none solutions that add friction instead of removing it. Ultimately, this means more gaps, more guesswork, and less return on every dollar spent.

7 Misaligned incentives

Many MSPs are still tethered to legacy business models that reward volume over value: charging based on tickets, endpoints, or vendor bundles. In this structure, reducing complexity, consolidating tools, or eliminating unnecessary software *actually shrinks* the MSP's revenue. In other words, even well-meaning providers are disincentivized from driving the very efficiency and innovation their clients expect.

What this means for SMBs:

Your MSP might know the right answer, but have no business reason to implement it. When incentives favor complexity over clarity, SMBs pay more for less value. Without a model that rewards simplification and transformation, even the most advanced tools won't translate to progress.

8 Limited financial resources

Building deep expertise across AI, cybersecurity, automation, and compliance doesn't come cheap. MSPs typically operate on thin margins: average service gross margins are around 50–60%, with best-in-class hitting 70%.[22] But 30–40% of that revenue goes to overhead, leaving limited room for large investments in talent, tools, or R&D.[23]

Few MSPs can absorb the cost of hiring specialized engineers, maintaining certifications, or building scalable services. Without scale or capital, they can't support full-stack security platforms, enterprise-grade automation, or compliance-heavy offerings such as CMMC.

What this means for SMBs:

When MSPs can't afford to invest, their clients pay the price. Underpowered security leaves doors open. Patchwork automation creates more friction than it solves. Compliance becomes a guessing game. Instead of driving growth, technology becomes a liability, holding SMBs back just when they need to move faster.

The result?

A widening credibility gap between the services MSPs say they offer and the outcomes SMBs actually need.

Bridging this gap requires more than rebranding or bolt-on tools. It calls for a new kind of MSP—one designed from the ground up for AI, automation, compliance, and security, with deep vertical expertise and centers of excellence that can deliver true business outcomes.

A new category emerges:

The AI-savvy, *security-first* MSP

The last section made one thing clear: even MSPs built for "3.0" can't support today's SMB needs. In a world in which AI is evolving weekly, last year's playbook is already legacy—and yesterday's infrastructure experts are scrambling to stay relevant.

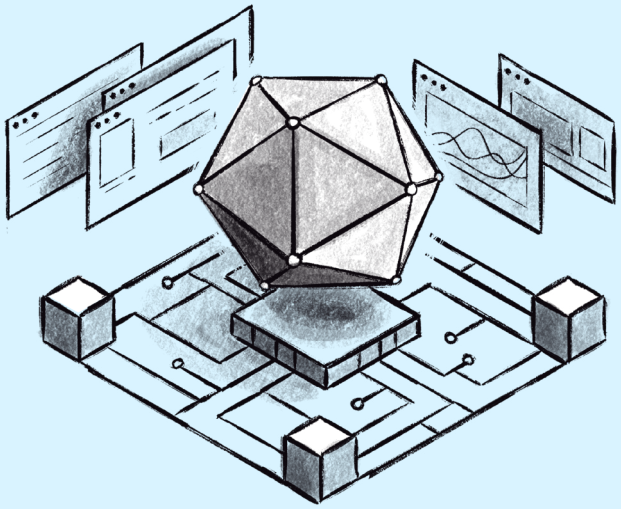
What's needed now is a different kind of MSP: one designed *from day one* for a world of connected tools, smarter threats, and higher stakes.

This full-stack model is AI-enabled, automation-first, security-led, and compliance-conscious… *not* because those features were tacked on later, but because they've been foundational from the start.

These next-gen MSPs align technical execution with business strategy at *every layer* of the stack: streamlining operations, reducing risk, and unlocking new opportunities for their SMB clients.

What defines the next-gen MSP?

The next generation of MSPs is built around intelligence and enablement.



That means:

1 AI-native at the core

Next-gen MSPs don't just recommend tools like Copilot or ChatGPT; they embed AI into clients' cross-functional workflows to automate HR onboarding, reconcile invoices, optimize sales sequences, and more. Where traditional MSPs stop at tool selection, next-gen partners drive adoption, integration, and measurable lift. *Internally*, they use AI and automation to streamline complete workflows, lowering costs, reducing manual effort, and creating more capacity for strategic interactions with customers. This requires talent who can bridge business workflows and technical systems: engineers, analysts, and trainers who understand both the tools and the organizational context.

2 Security-first by design

Not bundled antivirus. Not "we'll get to that later." These MSPs implement zero-trust architecture, 24/7 monitoring, and compliance-ready configurations from day one. They run risk assessments before rollout, map frameworks like NIST, CIS, SOC 2, HIPAA, CMMC, or PCI DSS to real infrastructure, and generate audit-ready reports as a baseline. This depth of protection is only possible with dedicated security specialists: people fluent in frameworks, adversary tactics, and continuous monitoring.

3 Compliance-aware by default

Offering "compliance as a service" isn't just about deploying software; it's about specialists who know how to interpret evolving requirements and translate them into day-to-day operations. Next-gen MSPs operationalize compliance: auto-logging HIPAA changes, flagging risks under emerging AI laws, and preparing clients for frameworks like NIST, CIS, CMMC 2.0, PCI DSS v4.0, or SOC 2.

4 Outcome-aligned by structure (not by exception)

Legacy MSPs might guarantee uptime (and that remains essential). *Next-gen* MSPs build on that foundation by pointing to outcomes: "Invoice time dropped 30% through automation"; "sales conversions up 12% thanks to AI-enabled workflows." They track the KPIs that actually move the business forward.

5 Embedded advisory at the executive level

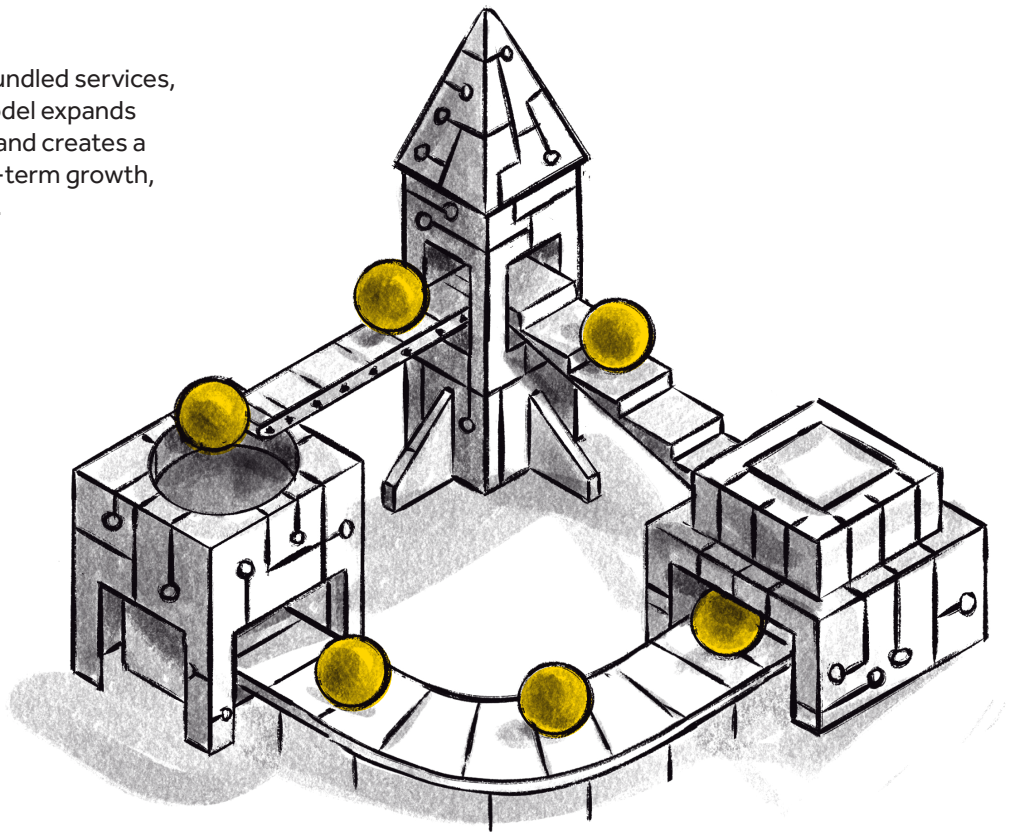
Next-gen MSPs aren't just "tech partners." They sit with your leadership team, lead quarterly business reviews, and guide strategic planning. They also put multi-year roadmaps in place to ensure budgets stay aligned to priorities. Advisory only works if the MSP fields leaders who've sat in both technical and executive seats—people fluent in strategy as well as in systems. From *that* position, they can say, "Here's what's slowing you down… and here's how to fix it."

6 End-to-end IT management

From provisioning and remote management of hybrid cloud environments, devices, SaaS applications, telecom, and cybersecurity systems to infrastructure monitoring and layered defenses, next-gen MSPs support the full stack with scalability and security in mind. Behind the platform are skilled engineers and operators who can adapt to new technologies and resolve issues that automation alone can't handle.

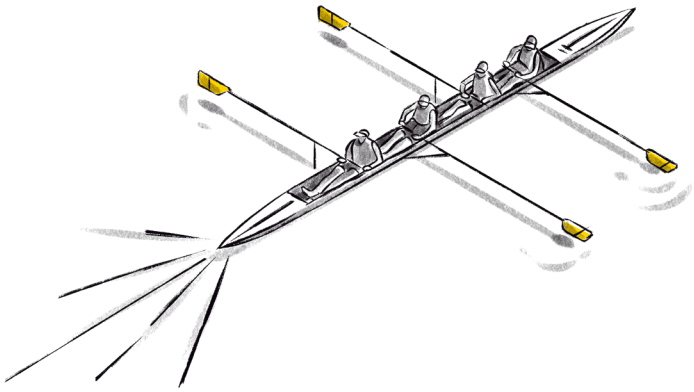
7 Built for scale

With automated delivery, bundled services, and recurring value, this model expands margins, boosts retention, and creates a sustainable engine for long-term growth, for both provider *and* client.



MSP 3.0 vs. next-gen MSP:

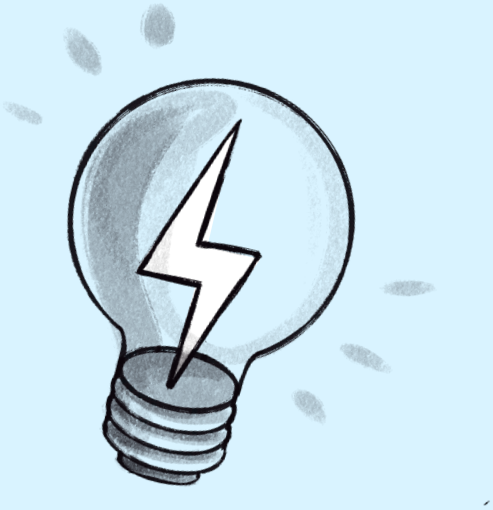
A side-by-side comparison



	MSP 3.0	Next-Gen MSP
AI & automation	“Copilot can streamline that workflow for you.”	“We’ve implemented Copilot securely, trained your employees, and can show you the productivity lift you’re seeing.”
Security	“We’ve bundled endpoint protection with your plan.”	“Your security stack, processes, and procedures now map directly to CIS. We’ll walk you through the audit-ready controls.”
Compliance	“We offer compliance reporting if you need it.”	“We proactively log changes, flag emerging risks, and keep you aligned to frameworks like CMMC, HIPAA, and PCI.”
Value measurement	“We guarantee 99.9% uptime.”	“Since we rolled out that automation, invoice time dropped 30%. Your sales conversions are up 12%.”
Strategic advisory	“Let’s review your tickets for the quarter.”	“Here’s what’s blocking your growth… and here’s how to solve it.”
IT management	“We can help manage your endpoints and servers.”	“We provision, manage, and secure your entire tech stack, from telecom to SaaS to hybrid cloud.”
Business model / growth	“Our model depends on ticket volume and reactive support.”	“We use automation to reduce overhead and drive long-term margins. That means more value for you, and a sustainable growth engine for us.”

From infrastructure to insight:

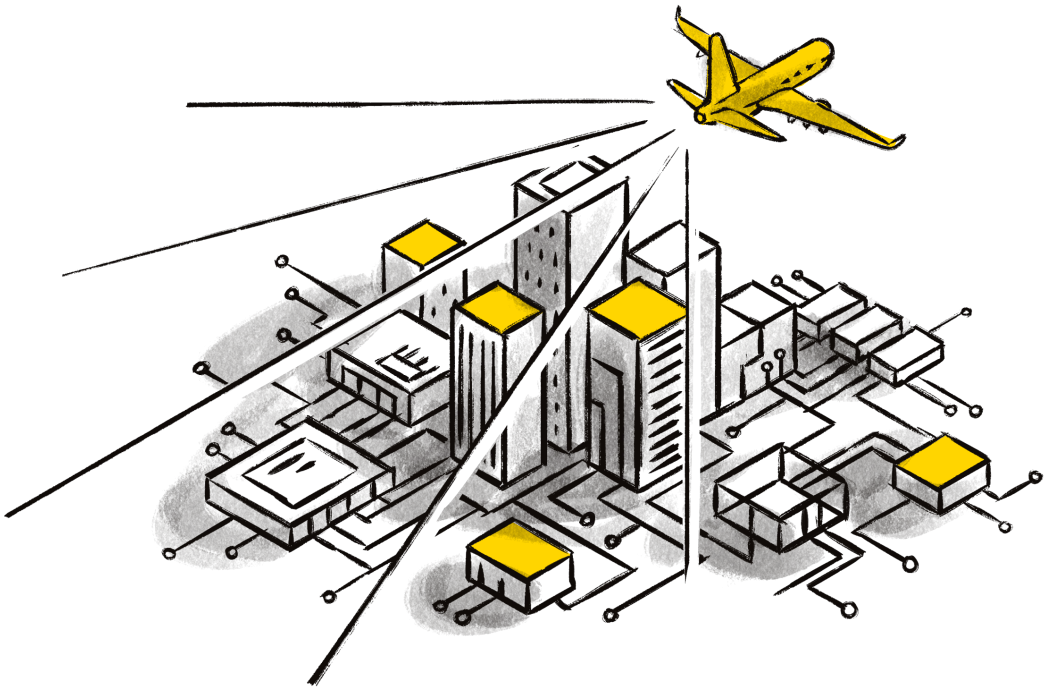
The evolution of MSP performance



Note: Each of these stages builds on the last. The core services, support, and metrics of Traditional and MSP 3.0 models remain essential, but the next-gen MSP adds new capabilities that elevate technology from baseline operations to strategic impact.

	Traditional MSP	MSP 3.0	Next-Gen MSP
Core focus	Infrastructure uptime, break/fix response	Proactive IT support, basic cloud & automation	Business outcomes via AI, cyber, compliance, automation
Primary metrics	Uptime %, ticket resolution time, endpoint count	Response SLAs, # of cloud migrations, # of automations	All of the metrics in "Traditional MSP" and "MSP 3.0," plus revenue lift, time-to-value, risk reduction, tech alignment score
Security approach	Basic antivirus, firewall	Layered security stack, some MDR/SIEM	Integrated security stack, 24/7 proactive monitoring, security-first design
Compliance	Ad-hoc or reactive support for HIPAA, PCI, etc.	Basic compliance offerings, bolt-on assessments, documentation support	Embedded compliance frameworks (NIST, CIS, CMMC, HIPAA, PCI, SOC 2) with mapped, continuously enforced controls
Automation	Minimal, mostly RMM scripting for MSP internal use	Some internal end-to-end workflow automation	Full-stack orchestration, including client workflow automation across departments & systems
Client communication	Reactive, ticket-based updates	Scheduled QBRs, improved reporting	Embedded vCIO/vCISO, strategic planning sessions, KPI dashboards

	Traditional MSP	MSP 3.0	Next-Gen MSP
Business alignment	Limited or no business goal integration	Some alignment via vCIO/vCISO-lite roles	Deep discovery of business goals & roadmap-driven engagement
Toolset strategy	Fragmented tools, little integration	Tool consolidation efforts underway	Platform-based toolset, unified data layer
Service model	Reactive, ticket-based	Proactive monitoring & some advisory	Full-stack delivery with measurable impact
AI readiness	None or vendor-focused only	Some awareness, low enablement	Client-specific enablement & workflow implementation
Pricing model	Per device, per ticket, volume-based	Flat-rate + value-added bundles	Recurring revenue tied to outcomes, compliance, & AI enablement
Talent model	Generalist technicians covering infrastructure basics	Small, siloed teams with some upskilled engineers	Access to specialized roles (AI architects, SOC analysts, compliance experts, workflow engineers) embedded into delivery



Next-gen MSP reporting metrics:

What SMBs actually want to see

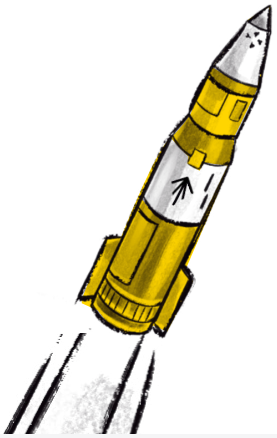
Next-gen MSPs don't just share ticket logs or uptime graphs. They surface the metrics that matter most to business leaders: alignment, adoption, resilience, and ROI. At Propulsion, this means delivering clear, structured reporting tied to client priorities. Every quarter, we share progress across operations, security, and strategic planning, so SMBs know exactly what they're getting and where they're headed.

	What to track	Why it matters
Strategic meetings	Number of vCIO/vCISO meetings, meeting notes, action item closure rate	Shows proactive alignment & accountability
Budgeting & planning	Number of budgets completed; % adherence to roadmap plans	Builds trust, avoids surprise costs, demonstrates long-term thinking
Support requests	Ticket volume trends; % auto-resolved vs. human intervention; top recurring issues	Indicates system stability, training opportunities, & behind-the-scenes value
Escalations	Number completed; % of recommended changes implemented	Tracks alignment progress, reduces risk, shows momentum
Tech reviews	Quarterly technology assessments completed; stack optimization recommendations; alignment to business roadmap	Ensures technology investments remain relevant and identifies opportunities for consolidation or improvement
Business impact	Estimated hours saved, downtime avoided, incidents mitigated	Connects tech work directly to business productivity and resilience
Roadmap progress	% of strategic projects completed on time/on budget	Reinforces MSP follow-through & business alignment
Adoption & engagement	Tool adoption rates; employee training participation; usage data (when available)	Demonstrates whether investments are being used & where enablement is needed
Security & compliance	# of mapped controls passed, incidents detected, risk items closed	Proves that security isn't just installed; it's actively managed
Business goal alignment	Short/long-term goals captured & tied to roadmap items	Shows that the MSP understands, & is helping to achieve, the client's big picture

When MSPs track and share metrics like these, they don't just support the business; they become part of it. It's a roadmap to deeper relationships, stronger retention, and long-term strategic relevance.

The business outcomes next-gen MSPs drive

By embedding themselves across workflows, security, and planning, next-gen MSPs drive meaningful (and powerful) results across the business. Common outcomes include:



Faster workflows, higher productivity

- HR onboarding (and offboarding) time cut from days to hours through AI-assisted workflows
- Invoice reconciliation and billing automation saves dozens of hours per month
- Sales teams improve conversion rates through personalized, AI-optimized sequences
- Fewer repetitive IT tickets thanks to proactive automation and system intelligence

Stronger security posture

- 24/7 monitoring and automated incident response reduce time-to-detection
- Zero-trust architecture and layered defenses lower exposure to ransomware, phishing, and insider threats
- Audit-ready compliance reduces legal, regulatory, and reputational risk

Access to scarce expertise

- Fractional AI engineers, security analysts, and compliance officers
- On-demand expertise without the overhead of full-time hires
- Bridges the talent gap that slows innovation and execution

Improved cost efficiency and budget clarity

- Predictable, recurring pricing models reduce surprise spend and budgeting gaps
- Automation lowers operational overhead, allowing teams to do more with fewer resources
- Consolidation of vendors and tooling cuts software waste and licensing bloat

Increased operational resilience

- Cloud migrations minimize downtime and allow for rapid scaling or recovery
- Remote device management ensures continuity across hybrid or distributed teams
- Backup and disaster recovery planning keeps critical systems online, even under stress

Stronger IT–business alignment

- vCIO/vCISO input turns technology planning into business strategy
- Executive dashboards and QBRs surface the metrics that matter most: ROI, risk, opportunity
- Budgets are mapped to outcomes, not just upgrades

Scalability and retention

- Infrastructure grows with the business—*without* constant reinvestment or rebuild
- Employees stay longer when tools actually help them work better
- A future-ready foundation that enables expansion, acquisitions, or transformation

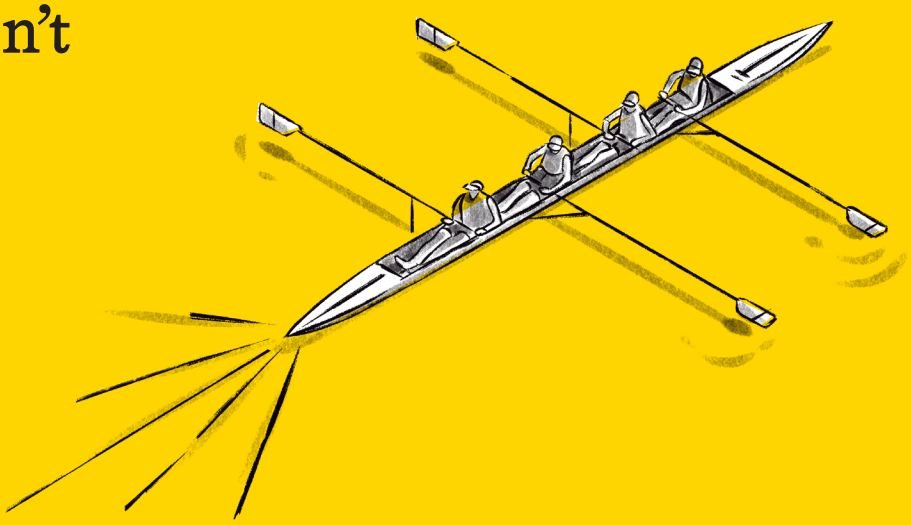
The result?

Less firefighting, more foresight, and a secure, scalable foundation for growth

Next-gen MSPs aren't just providers.

They create momentum and remove the friction that holds SMBs back.

Talk to the Propulsion team to learn more



Propulsion

Sources

1. *The State of MSP Security Maturity Report 2025*. Todyl.
2. Michael George. "*The Future of MSPs in 2025: Predictions and Trends*." Forbes Technology Council, February 11, 2025.
3. *The CyberSmart MSP Survey 2025*. CyberSmart.
4. *Managed Service Provider (MSP) Statistics: USA 2025*. Infrascale, March 3, 2025.
5. Michael Siggins. "*AI, Platforms, and the Future of MSPs: Exclusive Look Inside Channel Program's 2025 IT Management Software Report*." ChannelPro Network, June 26, 2025.
6. "*Incident Management for High-Velocity Teams*." Atlassian.
7. *Global State of the MSP Report: Trends and Forecasts for 2024*. Datto.
8. "*Ransomware Payments Increase 500% in the Last Year, Finds Sophos State of Ransomware Report*." Sophos, April 2024.
9. *State of IT Security in SMBs in 2024–2025: What 445 SMB IT Pros Told Us About Cybersecurity in 2024–2025*. Devolutions.
10. *State of the Automation Professional Report 2024*. UiPath.
11. "*SMBs at Work 2024: What Apps Make the SMB Stack?*" Okta.
12. *State of the Automation Professional Report 2024*. UiPath.
13. *The MSP Customer Insight Report 2025*. Australian Cyber Security Magazine.
14. Tilly Travers. "*The MSP Customer Insight Report 2025: Key Takeaways for Success*." SmarterMSP, July 15, 2025.
15. "*73% of Organizations with up to 2,000 Employees Rely on MSPs to Manage the Security Challenges of Growth.*" Barracuda Networks, press release, July 15, 2025.
16. Christopher Hutton. "*Cynet: Lack of MSP Automation Holding Clients Back*." Channel Futures, July 23, 2025.
17. Michael George. "*Too Many Tools, Too Many Threats: How MSPs Can Take Back Control*." Forbes Technology Council, June 16, 2025.
18. Christopher Hutton. "*Cynet: Lack of MSP Automation Holding Clients Back*." Channel Futures, July 23, 2025.
19. *2025 MSP Performance Report: 3 Secrets to Hyper-Growth from Industry Leaders*. JumpCloud.
20. Christopher Hutton. "*Vast Majority of MSPs Lack AI Knowledge to Serve Customers*." Channel Futures, June 6, 2024.
21. Mike Vizard. "*Opportunities Arise for MSPs Despite Skills Shortages*." SmarterMSP, January 18, 2024.
22. "*Gross Margin & Gross Profit: The MSP Playbook for Better Business Health*." Gradient MSP, September 16, 2024.
23. Matt Linn. "*MSP Profit Margins 101: Industry Averages & Ways to Improve*." Thread, August 7, 2024.
24. *2024 MSP Benchmark Survey Report*. Kaseya.
25. *2024 MSP Benchmark Survey Report*. Kaseya.
26. *Global MSP Preferences Survey*. AvePoint.
27. *2024 MSP Benchmark Survey Report*. Kaseya.
28. Christopher Hutton. "*MSPs Struggle to Add Customers in 2024*." Channel Futures, December 13, 2024.
29. "*Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists*." ISC2, September 11, 2024.
30. "*87% of MSPs Need to Know More About AI to Meet Customer Needs*." Barracuda Networks (PR Newswire), June 6, 2024.