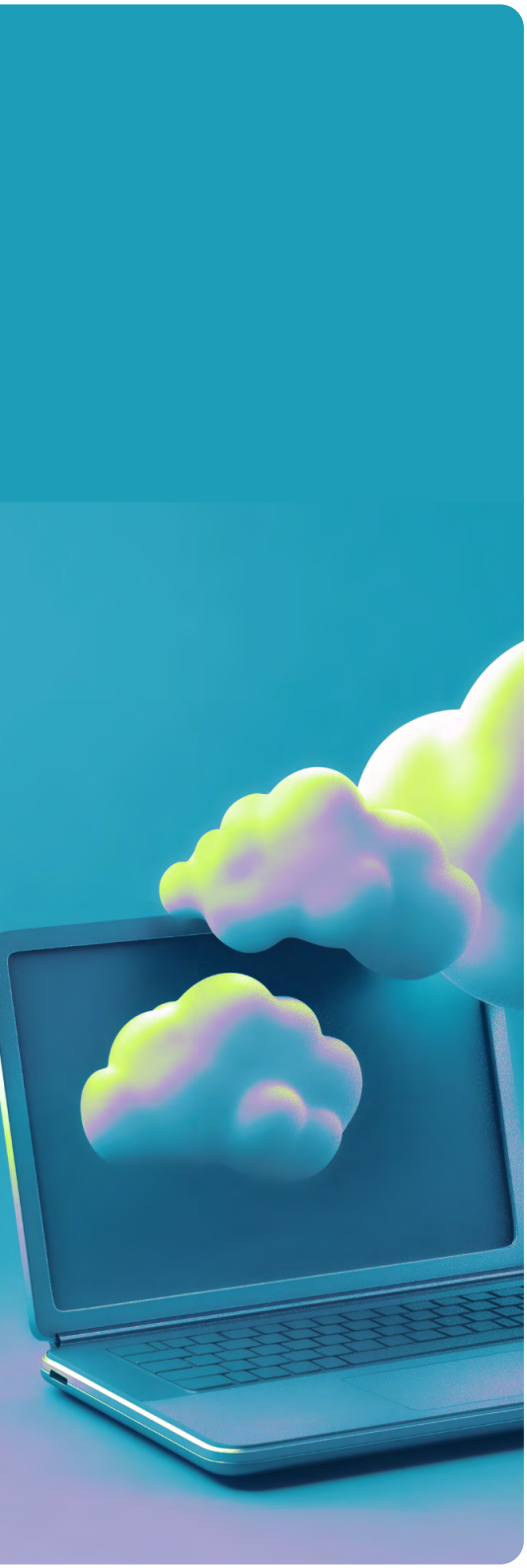
nerdio

The MSP guide to Microsoft 365 security at scale

How MSPs can unify cybersecurity management



Executive summary

Most small and medium-sized businesses still lack the tools and talent to manage cybersecurity on their own. As a result, they rely heavily on MSPs to deliver essential security services at a price they can afford.

But MSPs are hitting their own limits. Managing security across a growing customer base often means juggling five or more agents per user: EDR, identity security, RMM, device management, email protection, attack surface management… the list is endless. The operational overhead is significant, yet many MSPs hesitate to consolidate due to concerns about vendor lock-in, security gaps, limited MSP-specific coverage, or unpredictable pricing.

At the same time, Microsoft has rapidly matured its security stack, matching—and in some areas, surpassing—third-party tools across endpoints, identity, cloud workloads, and data. What's been missing is true multi-tenant management and MSP-friendly economics to make standardizing on Microsoft security viable at scale.

This guide walks through how to consolidate on Microsoft 365 Business Premium without compromising security or margins. You'll reduce endpoint agent sprawl, simplify security management, boost technician productivity, and eliminate unnecessary vendor costs, driving real operational efficiency and profitability with confidence.

nerdio

The hidden costs of a fragmented security stack

Any growing MSP has experienced the following scenario: You start with foundational security, like a next-generation antivirus (NGAV) or an EDR platform, and start offering more security as customers, cyber insurance providers, or compliance auditors begin requiring it. Years later, you're juggling multiple security tools, launching five different agents to diagnose and troubleshoot basic security issues, and dealing with sluggish environments as a result.

Before long, you're juggling dozens of logins, and your technicians are only relying on the security solutions they know like a crutch, impacting the effectivity of your security services and investigations.

This tool sprawl is a major operational liability. While the obvious answer to this problem would be for MSPs to centralize security operations on one platform, most best-in-class security solutions did not support multi-tenancy for MSPs. Additionally, most MSPs are wary of potential security and reliability risks that come with consolidating on one platform, regardless of any efficiency benefits. To an MSP, it feels like trading one set of problems for another.

After all, what happens if you consolidate and your MSP faces:

Unpredictable pricing: What if your consolidated platform raises prices next year? Will you be stuck, forced to absorb the cost, or start over again?

Security risks: If everything runs through one platform, what happens if that platform is compromised?

Downtime: Outages are inevitable. But when your entire operation relies on one tool, even a brief interruption can have big consequences. How will you handle that?

Loss of flexibility: What if you're locked into a platform that doesn't evolve with your business or forces you to give up specialized capabilities you depend on?

Missing features: Point solutions often go deep in specific areas. Can a unified platform really deliver what you need across the board?

These concerns are valid, and ignoring them is not an option. That's why MSPs need visibility that proactively addresses potential risks and keeps their security posture hardened.

Why consolidation on Microsoft Security is worth considering

When Microsoft reintroduced the Defender security portfolio in 2019, market reaction was mixed. At best, it was seen as "good enough." At worst, it was dismissed as a low-cost, checkbox solution.

That perception has changed. Microsoft has made security a top priority, investing more than $20 billion, employing over 34,000 security engineers, and building a robust partner ecosystem through initiatives like the Microsoft Intelligent Security Association (MISA). Today, Microsoft is a security leader in its own right.

More importantly, Microsoft recognized that the biggest security gaps don't exist in the Fortune 500; they exist in the other 99% of businesses. In response, it bundled core security capabilities into Microsoft 365 Business Premium, including Defender for Business, Entra ID, and Purview. MSPs can further extend coverage with advanced Defender and Entra plans, cloud app and identity protection, and Purview add-ons—often at up to a 65% per-license discount compared to standalone tools.

Consolidating on Microsoft's native security stack helps MSPs regain operational control. Fewer tools mean simpler training, higher efficiency, and reduced risk. Instead of managing dozens of portals, teams can operate from a single, standardized environment.

For technicians, consolidation means faster resolution times and fewer errors. Less context switching leads to better outcomes and more time spent solving real problems. Standardization also improves communication by aligning teams around shared tools and processes.

nerdio

Understanding how multi-tenant management can mitigate MSP security risks

For MSPs that are bought into Microsoft Security, the right Microsoft 365 multi-tenant management platform can offer the secure baselines and policy management MSPs need to address the risks they're really facing when they consolidate on any vendor, like security blind spots or a lack of consistency across tenants and environments. The right platform offers controlled architecture and centralized policies, enabling you to monitor access, manage permissions, and act quickly when needed.

Consolidating on Microsoft 365 will also enable MSPs to make their pricing clearer and more predictable. You won't have to reconcile five different invoices from separate security or compliance providers – it'll all be in your Microsoft invoice.

Flexibility doesn't vanish with a unified model. Many platforms support integrations or exports so you're not boxed in. When built for MSPs, core tools are built in from the start, not tacked on through plugins.

Important questions to ask your security partner

How do you know you're picking the right platform to help your MSP manage Microsoft 365 security at scale? Here are the questions you can ask to move beyond marketing claims and get to the facts that matter.

Start with security and compliance. How does the platform manage access? Are logs audit-ready? Has it passed third-party security reviews? A unified platform doesn't have to increase risk. If anything, it can improve your security posture by consolidating oversight.

Then, look at performance and uptime. Don't settle for vague promises. Are there real metrics, service-level agreements, and information about redundancy? Look for signs of a platform that's built for scale and resilience.

Evaluate cost transparency. Is pricing predictable? Are there surprise fees for support or overages? Does the vendor offer flexible licensing and caps on price increases?

Finally, assess migration and support. Does the vendor offer onboarding guidance, training materials, and hands-on assistance? What does support look like after go-live? Can you reach someone who understands your business?

Scoring vendors across these categories gives you a clearer picture of how they stack up—and whether they're truly ready to support your business at scale.

Transparency, trust, and moving forward with confidence

At Nerdio, we believe MSPs make the best decisions when they ask tough questions and get honest answers.

We know switching platforms impacts your team, clients, and business model. That's why Nerdio Manager for MSP is built to meet the real-world needs of MSPs managing Microsoft 365 tenants and software. From centralized control of Microsoft Defender, Intune, and other Business Premium solutions to proactive management of users, devices, security groups, and third-party applications, it's designed drastically to cut overhead and improve service delivery.

But features aren't enough. We back our platform with real reliability, including uptime that exceeds industry benchmarks, clear SLAs, transparent incident reporting, and a support team staffed by former MSPs who understand speed, empathy, and expertise matter.

Consolidation shouldn't mean compromising on security and efficiency. With the right questions, meaningful evaluation criteria, and a plan to validate your choice, you can replace tool sprawl with clarity and confidence.

Ready to get started? **Get in touch with a Microsoft 365 specialist at Nerdio** to see how you can streamline your MSP business.

About Nerdio

Nerdio is a leading provider of powerful, simplified cloud management solutions for businesses of all sizes. Trusted by managed service providers (MSPs) and enterprise IT departments alike, Nerdio equips organizations with seamless, cost-effective management tools for Azure Virtual Desktop (AVD), Windows 365, and comprehensive Modern Work solutions.

With thousands of customers worldwide, Nerdio accelerates cloud adoption, enabling companies to thrive in an era of hybrid work by providing modern, future-proof technology that adapts to evolving workplace needs.

For more information, please visit **www.getnerdio.com**.

nerdio

WEB www.getnerdio.com
EMAIL hello@getnerdio.com

WP020226000