opentext™ Cybersecurity

Microsoft Solutions Partner

Turn your Microsoft practice into a growth platform

How OpenText Cybersecurity sees the Microsoft opportunity evolving





The next evolution of the Microsoft MSP

The managed services market is changing. Microsoft continues to create significant opportunities for MSPs. The challenge is no longer attracting customers. It's building a business that can scale efficiently while protecting margins. For MSPs handling high volumes of singular Microsoft transactions, the question is no longer whether to evolve the model, it's how quickly you can do it.

This is OpenText Cybersecurity's perspective on where the Microsoft opportunity is heading, and what it takes to be on the right side of that shift.

Chapter 1

The hidden cost of growing your Microsoft practice

Microsoft 365 is the foundation of many successful MSP businesses. As practices grow, however, many MSPs add security, backup, identity, and compliance solutions from different vendors. Over time, managing those tools can become more complex than managing Microsoft itself.

This is exactly why many MSPs are moving toward platform consolidation. Rather than managing multiple security vendors, they are standardizing on a single platform that simplifies procurement, management, billing, and support.

The stack that grew without a plan

Every new vendor adds operational overhead, including different onboarding processes, admin portals, licensing models, support teams, and billing cycles. On their own, these don't seem like major issues, but together they create a hidden operational cost that chips away at your margins every day.

Today, protecting profitability has become just as important as winning new customers. That means finding new ways to make your business more efficient, rather than relying on constant cost-cutting, price increases, or simply doing more with the same resources.



85%

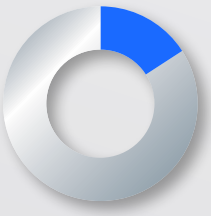
of interviewed partners bundled Microsoft with OpenText[1]

Managed services revenue growth is expected to slow to around 6–10% in 2026[2]

Invisible overhead, very visible margin impact

Vendor sprawl creates work that customers never see and rarely pay for. Engineers jump between consoles to troubleshoot issues, service desk teams work across multiple management interfaces, and operations teams reconcile invoices from different suppliers. Even a single support ticket can involve multiple vendor escalations.

It's easy to dismiss this as just a part of running an MSP, but the impact is measurable. Every additional vendor relationship consumes engineering time, increases administrative effort, and adds complexity across the business. Those costs don't appear on a customer invoice, but they show up in utilization rates, slower ticket resolution, and lower margins.



16%

rise in MSP mergers and acquisitions is expected in 2026[2]

The business case for simplification

The pressure is only increasing as larger providers continue to scale while smaller firms are expected to do more with fewer resources. The expectation is the same whether you're backed by private equity or running an independent business, and it makes operational efficiency less of a competitive advantage and more of a business necessity.

At the same time, you're facing growing customer budget pressure while also being expected to strengthen your own security posture and help customers stay compliant. With expectations rising on every front, there is little room for operational waste, which is why the right technology can play such an important role in improving efficiency.

Automation only works on a clean foundation

Automation delivers the biggest benefits when it's built on simple, consistent processes. If your team is still managing multiple disconnected platforms, automation can only take you so far. Simplify first, then automate.

Simplify the model, not the offering

This doesn't mean reducing customer choice or limiting the service you provide, as customers still expect a complete security and productivity solution. The opportunity is to rethink how those services are sourced, bundled, managed, and supported.

Reducing operational complexity allows engineers to spend more time delivering value instead of managing vendors, while also lowering administrative costs. It also helps simplify support processes and creates a business that's easier to scale without adding headcount.

The fix isn't fewer products, but a smarter way to bundle them so they work more efficiently. When this is done right, your margins change significantly.



Chapter 2

Why the most profitable MSPs are not the biggest resellers

License resale is often where MSPs start with Microsoft 365. It's simple, scalable, and creates predictable baseline revenue, but it's not where the margin is.

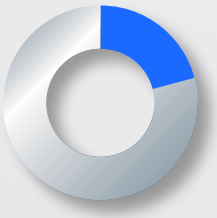
The real opportunity isn't selling another Microsoft licence. It's helping customers protect, secure, and manage the Microsoft environment they already depend on.

That shift is straightforward in concept and powerful in impact: attach security, backup, identity, and compliance services to an existing Microsoft 365 estate, and you grow monthly recurring revenue without the cost, time, or risk of acquiring a new customer.

You don't need new customers to grow

This change doesn't require replacing Microsoft. Instead, it means building complementary security, backup, identity, and compliance services around the Microsoft 365 environment customers already rely on. The platform remains the foundation, while the opportunity lies in delivering the ongoing management, protection, and expertise that customers increasingly need.

Cybersecurity and compliance are two of the fastest-expanding areas in the MSP portfolio right now, and the numbers make a compelling case for continued investment.



Compliance services are growing at

21%

year over year[2]

Cybersecurity managed services revenue is expected to grow by 14% in 2026, reaching $106bn[2]

This reflects a structural shift in customer demand. Security and compliance are no longer optional add-ons. They are core business requirements tied directly to risk.

Partners earn up to $6.73 in services revenue for every $1 of software sold[1]

This changes how you should think about value creation. The real margin is not in the license. It's in adoption, ongoing management, optimization, and expansion over time.

A broader portfolio builds a more valuable business

When you already have trusted Microsoft customer relationships, you have a natural opportunity to grow by offering complementary security, backup, and identity solutions. This expands your customers' value, increases recurring revenue, and reduces reliance on a single product, all without changing your business model or acquiring new customers.

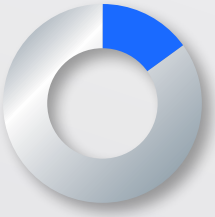
A broader, services-led portfolio makes your business more resilient, more scalable, and less dependent on vendor margins. Buyers typically place higher value on MSPs with predictable recurring revenue because these businesses are viewed as more stable and attractive long-term investments.

Chapter 3



95%

of organizations believe they can recover from a ransomware attack[3]



Only

15%

are actually able to recover successfully[3]

The next layer of profitable growth: Security and backup

Security and backup are not add-ons to a Microsoft 365 environment, they are the natural extension of it. When positioned correctly, selling additional solutions becomes much simpler because you're not introducing unfamiliar tools, you're completing the stack your customers already rely on and trust.

3 areas where additional coverage matters

Microsoft provides a strong foundation for productivity and endpoint management, but it doesn't eliminate risk exposure on its own. The gaps you're increasingly being asked to close sit in three areas: advanced email threat protection, endpoint detection and response, and cloud backup. And those gaps matter more today than they did even a few years ago.

The threat landscape has changed

Destructive attacks are increasingly being layered onto traditional ransomware, adding data theft and deliberate disruption of recovery, rather than replacing it. The objective is no longer just to lock data and demand payment, but to destroy recovery options entirely. In this environment, backup isn't just an IT utility, but a core part of security and resilience.

At the same time, cyber insurance providers are effectively becoming informal regulators. To secure coverage or maintain favorable premiums, customers are expected to demonstrate layered security controls where identity protection, endpoint detection, email security, and verified backup are not just best practice but baseline requirements. If you can demonstrate this stack is in place, you're in a strong position to help customers meet their cyber insurance needs.

$400,000 is the average cost of a ransomware payment[3]

A new risk hiding in plain sight

Compliance is shifting too. Shadow AI is rapidly expanding the attack surface inside most organizations. Your customers use AI tools that the business doesn't have oversight protocols in place for, which often exposes sensitive data without them realizing it. This creates an opportunity to get ahead of the conversation but also brings new responsibility. Data leakage is no longer only a user-behavior problem, but a risk you're expected to actively monitor and manage.





By helping customers gain visibility into shadow AI and put effective controls around its use, your service stack can turn an emerging data security risk into a proactive security and compliance opportunity.

Buying habits are changing fast

Microsoft processes an enormous volume of security signals every day. It's not only defenders operating at that scale, attackers are also constantly evolving to bypass those protections.

As a result, the way services are bought is changing, with more customers moving toward packaged, bundle-ready offerings through SaaS marketplaces.

Microsoft processes over 100 trillion security signals every day[2]

That shift matters, because it changes how services are sold and delivered. Customers no longer want multiple overlapping tools and separate invoices, they want clarity: one conversation, one bundle, one bill, and one support relationship.

This is where security, backup, and identity bundles become powerful. They reduce friction internally for you and externally for your customers, while also significantly simplifying the sales conversation.

The message to customers is simple: your Microsoft investment is already working hard. This adds the security layer that makes it complete.

Knowing what to offer is one thing. Making it happen consistently across every customer, and every renewal is where tangible scale comes from.



Over

60%

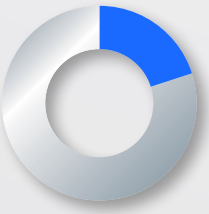
of MSPs are now purchasing regularly through SaaS marketplaces[2]

Chapter 4



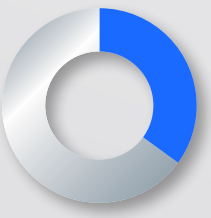
40%

gross margin.[1]
The target to aim for on your standard bundle.



20%

year-over-year growth.[1]
How ARS Technology scaled using OpenText as their foundation.



35%

of partner revenue compounds in year three[1]

Your 90-day roadmap to repeatable growth

Days 1 to 30: Define your standard

Start by deciding what your core Microsoft 365 security offering looks like and commit to making it your default recommendation for every customer. From there, build a standard bundle that includes Microsoft 365, endpoint security, backup, and email security, so you have a clear, repeatable offer that's easy to position and deliver. Resist the urge to tailor every proposal, as standardization is what makes your practice easier to sell, deliver, support, and scale. It's far easier to achieve when your products are delivered through a single platform.

Days 31 to 60: Create your sales process

Once your offer is defined, make sure your team knows how to position it by giving your sales and account managers clear messaging, customer talk tracks, and renewal playbooks that explain why layered security matters. Your partner or vendor can help bring this to life with the expertise, collateral, tools, and programs that help your team turn this strategy into a repeatable, customer-facing motion.

Days 61 to 90: Build it into your business

The final step is to make your process repeatable by building your bundle into every proposal, onboarding plan, renewal, and customer review so it becomes the default way your business operates. Measure conversion rates, recurring revenue, gross margin, and customer adoption so you can identify what's working and where to improve. The more consistent your process becomes, the easier it is to scale without increasing complexity.

Where this takes your business

The goal is to keep things simple by building one standard bundle and selling it to every Microsoft 365 customer, making it your default recommendation instead of a custom proposal. When your offer is standardized, your pricing reflects the value you deliver, and every renewal becomes an opportunity to deepen the relationship. Managed services revenue doesn't only grow, but builds over time.



Microsoft Solutions Partner

Ready to grow your Microsoft practice more profitably?

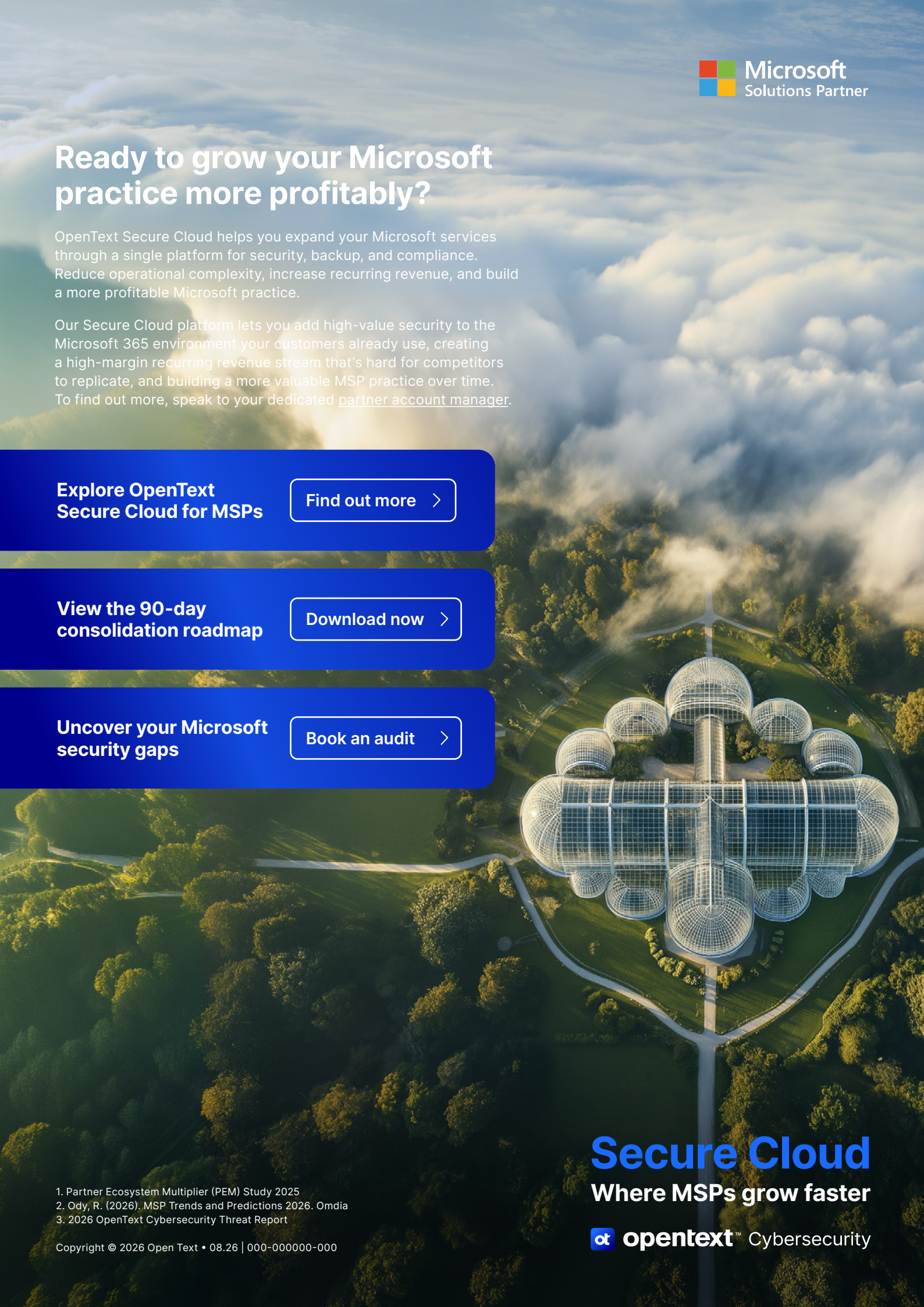
OpenText Secure Cloud helps you expand your Microsoft services through a single platform for security, backup, and compliance. Reduce operational complexity, increase recurring revenue, and build a more profitable Microsoft practice.

Our Secure Cloud platform lets you add high-value security to the Microsoft 365 environment your customers already use, creating a high-margin recurring revenue stream that's hard for competitors to replicate, and building a more valuable MSP practice over time. To find out more, speak to your dedicated partner account manager.

Explore OpenText Secure Cloud for MSPs — Find out more >

View the 90-day consolidation roadmap — Download now >

Uncover your Microsoft security gaps — Book an audit >



Secure Cloud

Where MSPs grow faster

opentext™ Cybersecurity

1. Partner Ecosystem Multiplier (PEM) Study 2025
2. Ody, R. (2026). MSP Trends and Predictions 2026. Omdia
3. 2026 OpenText Cybersecurity Threat Report

Copyright © 2026 Open Text • 08.26 | 000-000000-000