

Acronis

WHITE PAPER

The Microsoft 365 Maturity Model for MSPs



Setting the baseline, closing the gaps, tailoring services

Microsoft 365 continues to pose a major challenge to managed service providers (MSPs). Service providers constantly have to scramble to support the overwhelmingly popular platform, with revenue, profits and customer retention hanging the balance. But a new model for managing Microsoft 365 is emerging.

Since its introduction as Office 365 in 2011, the platform now known as Microsoft 365 has exploded in popularity, counting 400 million paid business seats in 2024. But as use of the platform has grown among companies of all sizes, MSPs have struggled to deliver it to clients in a way that is sustainable, profitable, secure and efficient.

This white paper explores the challenges MSPs face in delivering security services for Microsoft 365, including tool sprawl, difficulties with hiring experts, inadequate data backup in Microsoft 365 and problems forecasting pricing and profits. It then lays out a maturity model for MSPs that enables them to overcome those challenges and offer comprehensive Microsoft 365 protection without financial or operational barriers.

The challenges with offering — and managing — Microsoft 365 services

There are a few primary reasons why Microsoft 365 presents such a challenge for MSPs. Perhaps the most difficult is one that has long plagued the industry: staffing.

Most MSPs have to manage Microsoft 365 instances client by client and tenant by tenant, which often means assigning a technician to one or a few clients. As a result, service providers have to hire more and more experts as their client base grows. That's a big problem in an era when technical expertise is hard to find.

MSPs have a few issues when trying to recruit technicians. A quick online search reveals one of them: service provider technician has a reputation for being a demanding job. Since technical experts are still in

demand, they can generally find good jobs just about anywhere they look. And increasingly, they're bypassing MSPs because the demanding nature of working for an MSP can make a corporate job seem like better value for the salary available.

For smaller MSPs, then, recruiting can be a major issue. And MSPs that have difficulty recruiting or retaining employees have difficulty offering Microsoft 365 services to clients. The platform requires too much constant interaction from MSP employees for a small staff to possibly manage it effectively.

Technicians who move in and out of MSPs might also have adopted different third-party tools for managing Microsoft 365, depending on their expertise or preferences, leaving MSPs with a jumble of applications they might not be able to manage as technical experts turn over in their organization.

Microsoft 365 can't provide defense in depth

If Microsoft 365 just offered complete data security and backup, MSPs could set it and forget it, and move on to other tasks. They might be able to take on more clients and drive revenue as well. Unfortunately, Microsoft 365's shared responsibility model leaves a lot of holes in its data protection.

Microsoft takes care of keeping the Microsoft 365 platform up and running, and it does provide some basic security functions, such as limited email security. But Microsoft itself relies on third parties to provide many of those functions, which are thinner than what clients

generally need. Microsoft 365's built-in email security, for instance, cannot provide the additional layers of security MSPs need to adequately protect clients against increasingly frequent and more severe cyberattacks.

Defense in depth is now an accepted philosophy among cybersecurity experts. It's critical to have more than one layer of data protection in any given system, but Microsoft 365 can't provide layers since it's a single solution.

Consequently, running any Microsoft technology, which almost every company does, is not without risk.

Microsoft doesn't take responsibility for backing up customers' data

Microsoft is one of the most attacked entities in the world, with its customers facing a staggering 600 million cyberattacks every day. And the pace isn't slowing. From mid-2023 through mid-2024, Microsoft observed a 275% increase in ransomware attacks aimed at its customers.

But perhaps the biggest hole in Microsoft 365 data protection is one the company readily acknowledges. The company's own service agreement states that even the most sophisticated version of Microsoft 365 doesn't provide complete data protection:

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

Here is where the shared responsibility model is most glaring. Microsoft isn't responsible for customers' data. In fact, the company recommends that they back up their data with a third-party app or service. Data that's not fully backed up and quickly recoverable is not secure. And even if an attacker doesn't steal it, critical information could still disappear with Microsoft 365 as its sole protector.

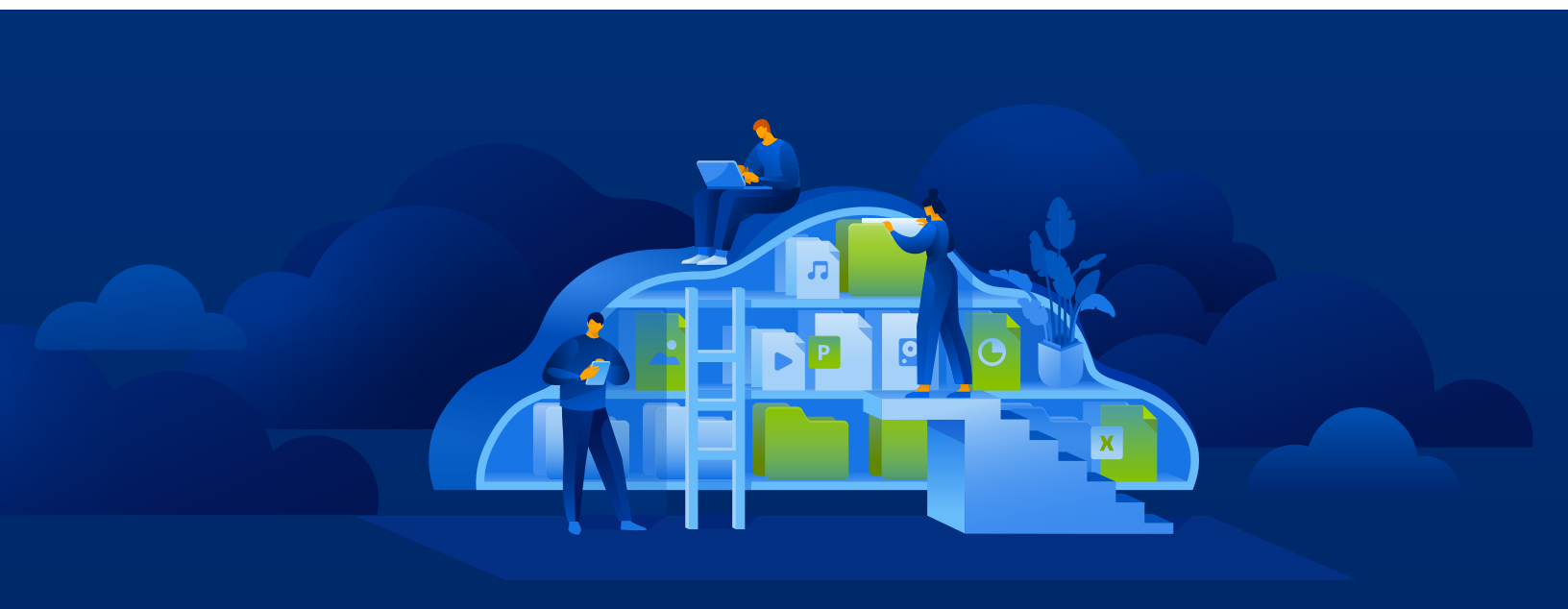
Tool sprawl creates chaos and broken integrations

MSPs turn to third-party tools to provide data security and backup for Microsoft 365 clients. That practice can quickly lead to tool sprawl, which introduces a new raft of challenges. Managing Microsoft 365 client by client is difficult, but trying to wrangle multiple other tools at the same time is basically impossible.

Technicians often come and go, leaving behind their preferred tools for bolstering Microsoft 365 security. Integrating those tools can be prohibitively time consuming and expensive. What's more, MSPs have to match a technician with expertise in a particular tool, which can quickly become costly and difficult.

Plus, most third-party tools don't talk to each other. That often requires using an API to link applications. The problem here is that two APIs tying applications together don't provide a stable integration that's easy to manage. An MSP still needs to commit resources for building, maintaining, securing and troubleshooting makeshift integrations.

The effort and expense service providers put into integration can become worthless in an instant, and



repairing a connection can be next to impossible without the right expertise in place. When MSPs run Microsoft 365 on weak connections and a laborious tenant-by-tenant setup, which many do, the setup is precarious, risky and unprofitable.

Management issues can make financial forecasting impossible

Estimating the amount of time, number of staff and overall effort required to service Microsoft 365 clients is almost impossible and fraught with financial risk. If a service manager, solution architect or systems engineer underestimates the resources required to offer Microsoft 365, the MSP loses money and negates the revenue boost of selling multiple security services.

But if service managers overestimate necessary resources, they risk building in costs that are too high and charging clients too much for cybersecurity services. If that happens, the MSP will have a hard time selling services and could price itself right out of the cybersecurity business.

As a result, MSPs are often hesitant to build Microsoft 365 services into managed service agreements (MSAs). The lack of predictability of cost makes supporting the platform too risky, but the reality is that most MSP clients use Microsoft 365 and want their MSPs to manage it.

When something does go wrong with Microsoft 365, clients expect an MSP to fix it. In an effort to be a reliable partner, the MSP will address the issue on a break-fix basis with one-time billing. And often, in the absence of an MSA, the MSP will cover the cost of the fix.

Even when the MSP does charge, every fix cuts into their profit. All of that gets expensive quickly for the service provider, and it's not a particularly positive situation for the client, either. Clients want the reassurance of having a platform as critical as Microsoft 365 covered in an MSA.

MSPs need to adapt to the new era of Microsoft 365

Microsoft 365 is far from new, but management tools for it haven't delivered the functionality MSPs need to offer the platform to clients without complications and complexity.

Increasingly, clients need to comply with ever-stricter regulations around security and data protection, meaning they require reliable Microsoft 365 services. They also need to defend themselves from the rapid growth in both the number and severity of cyberattacks, and many MSPs are scrambling because they don't have a solution that enables them to meet those needs.

When remote monitoring and management (RMM) came on the scene more than two decades ago, it reshaped the way MSPs did business by enabling them to manage endpoints proactively, predictably and therefore, more profitably as part of a subscription service.

Unfortunately, Microsoft 365 delivered similar, cloud-based capabilities and now manages many of the servers MSPs used to manage, including Exchange and SharePoint. However, the need to manage, secure and protect didn't disappear. MSPs had to deliver services for users, apps and data in the cloud. But MSPs didn't have tools similar to RMM to help them do the job with automation and a single point of access across their client base.

Service providers need to manage multiple Microsoft 365 tenants with a single point of control, and they need a solution that will fill the gaps in Microsoft 365 security and data protection.

Microsoft 365 is far from new, but management tools for it haven't delivered the functionality MSPs need to offer the platform to clients without complications and complexity.



The Acronis Cyber Protect Cloud Maturity Model for Microsoft 365

Moving from risky, incomplete Microsoft 365 coverage to confidently offering the platform to clients, is possible. To complete the journey, MSPs need to develop a step-by-step model that puts critical elements of Microsoft 365 protections in place. Acronis Managed 365 makes it possible by delivering every element of a maturity model in a single, natively integrated solution that's easy to implement and maintain.

Set a security baseline

Service providers can begin to put a maturity model in place with a first step, setting a security baseline. The baseline is the minimum setup an MSP must have in place in order to offer Microsoft 365 protection to clients without the challenges that most MSPs face when protecting the platform. It includes:

Security posture management

This is a critical element that brings multiple tenants into one place and a centralized point of command and makes Microsoft 365 management possible. With security posture management, MSPs can manage multiple clients from a single console without switching between accounts. They can also perform user onboarding and offboarding for multiple clients at once in a single interface.

As such, they can simplify complex tasks and enable less experienced technicians to handle responsibilities previously managed by senior staff. With simpler tasks being accomplished more rapidly by fewer people in a

unified interface, MSPs can avoid many of the challenges of finding qualified technicians. Service providers can get more done with fewer technicians and significantly cut time spent on managing clients' environments.

With hiring and resource allocation under control, MSPs can simplify MSAs by defining and packaging Microsoft 365 security management services. More control over hiring and less resource-intensive client management enables MSPs to reduce the risk of creating MSAs that include Microsoft 365 services. They can more easily forecast costs, revenues and profits, and build out MSAs with Microsoft 365 security and data protection services without incurring the financial risk they previously faced.

Of course, they need to be able to protect client environments. A unified cybersecurity solution gives them functionality Microsoft 365 doesn't have. It enables them to enhance risk detection by detecting previously unseen vulnerabilities when onboarding a client. They can also ensure always-on protection and minimize exposure windows with continuous monitoring of baseline deviations and automatic risk remediation.

All of those capabilities empower MSPs to provide stronger defenses than those built into Microsoft 365 as well as offer clients defense in depth. And wrapped around security capabilities are management features that enable MSPs to overcome the most challenging aspects of delivering Microsoft 365 security.



Backup and recovery

Most MSPs already provide backup and recovery. However, many struggle to manage multiple applications when providing services. They need to be able to consolidate tools and the reduce cost of their operations. Ultimately, they need a solution with natively integrated capabilities that include backup and recovery, email security and security posture management, among other functions.

Even so, backup and recovery remains an essential service for MSPs to offer. This capability enables MSPs to fill a major gap Microsoft itself makes no real effort to close. Data backup is only as valuable as an MSP's ability to recover it quickly and with minimal interruption to business. This element of data protection falls squarely into the category of customers' responsibility in Microsoft's shared responsibility model. MSPs have to provide it for clients.

Aside from delivering the obvious value of business continuity, backup and recovery capabilities are also critical for meeting regulatory requirements. Major regulations such as GDPR, HIPAA, FINRA and SOX include provisions for storage, protection and recovery of data.

The baseline provides MSPs a bare minimum for Microsoft 365 management. Once they have it in place and are providing services efficiently and profitably, they can move on and broaden their services.

Email security

Email remains a major vector for attacks of all kinds, particularly ransomware and malware threats. IBM notes that 70% of cyberattacks begin at an endpoint, and email is a major point of entry into endpoints. In Microsoft's shared responsibility model, the onus is on customers, not Microsoft, to protect endpoints.

Microsoft 365 does offer some email security, and the free Microsoft Defender application can deliver value to MSPs. But it's not enough. Microsoft isn't obligated to protect users' inboxes. MSPs need a solution that will protect email, preferably with proactive monitoring that can stop cyberattacks before they do any damage. As is the case with other elements of functionality, service providers also need to be able to manage email security for multiple tenants in a single console.

Close security gaps

The baseline provides MSPs a bare minimum for Microsoft 365 management. Once they have it in place and are providing services efficiently and profitably, they can move on and broaden their services. On the other hand, if they start expanding services while also stacking up more and more tools, they'll struggle to craft new offerings in a way that ensures sustainable efficiency and profitable growth.

So, the baseline is essential. Once it's in place, services MSPs could expand to provide include:

Security posture monitoring and remediation

This capability goes a step beyond security posture management and enables MSPs to automate both monitoring and remediation of events in clients' environments. The single-view access to multiple tenants remains, but service providers can upgrade from it to a system that enables them to find and fix problems without having a technician intervene.

Security posture monitoring and remediation enables MSPs to spend even less time managing Microsoft 365 for clients and allows them to reduce recruitment and hiring of technicians. The functionality also enables them to take on more clients and boost revenue without sacrificing profitability.

Security awareness training

People are consistently the weakest link in cybersecurity. According to the 2024 Verizon Data

Service providers can both proactively stave off risks for clients in Microsoft 365 and easily manage and deliver all cybersecurity, data protection and endpoint management services in a single solution with a single point of control.



Breach Investigations Report, almost 70% of data breaches involve an end-user mistake. The fewer mistakes users make at client sites, the fewer incidents MSPs will have to remediate.

MSPs can help themselves and drive revenue by offering security awareness training, which has become a requirement for compliance with many government regulations worldwide. With centralized control of client environments, delivering and managing training is both simple and profitable. Security awareness training is increasingly a requirement for compliance and cyber insurance, a selling point MSPs can use when pitching training to clients.

But delivering security awareness training effectively can be tricky. In an era in which users are overwhelmed with information and often lack patience, training has to be sharp, compelling and rapidly informative. So, MSPs need to choose a training partner that offers engaging, gamified lessons to make sure people actually absorb content and adjust their behaviors accordingly.

XDR integration

Extended detection and response (XDR) takes endpoint detection and response (EDR) to a new level. With XDR, MSPs can protect endpoints in Microsoft 365 with visibility across the most vulnerable attack surfaces, including email and identity. Service providers can cut the time required for threat analysis and response to just minutes with help from AI. They can conduct deeper investigations, respond faster and mitigate risks at scale.

With XDR, MSPs can automate responses to offer instantaneous remediation, enabling them to scale security operations and reduce costs. Tied into a natively integrated cybersecurity solution, service providers can both proactively stave off risks for clients in Microsoft 365 and easily manage and deliver all cybersecurity, data protection and endpoint management services in a single solution with a single point of control.

Tailor solutions to clients' needs

With functionality gaps closed and automation in place, MSPs can fine-tune their Microsoft 365 offerings.

Email archiving

Email archiving designed for MSPs enables them to deliver powerful search capabilities and rapid, self-service access to clients. Providing email archiving can help clients simplify adherence to regulations and regulatory requirements.

Security for collaboration applications

MSPs can also improve their offerings by delivering security for collaboration applications in Microsoft 365. Companies are rapidly migrating to SharePoint, Teams, OneDrive and other Microsoft 365 cloud collaboration apps, making them increasingly attractive targets for cyberattackers.

Microsoft 365 security for collaboration apps exists but does not provide comprehensive protection. With the right tools in place, MSPs can go beyond native Microsoft security by setting up alerts to notify them when malicious content is detected and prevent threats from spreading to end users by dynamically scanning every file and URL.

Native integration of cybersecurity capabilities is critical

While every element of the MSP security model is important, and particularly essential at the baseline level, the real value of cybersecurity maturity for MSPs lies in being able to deliver and manage all of the capabilities of the model in a single solution with centralized management.

With Acronis Ultimate 365, service providers can focus on the opportunities of delivering Microsoft 365 security and protection to clients without being burdened by legacy complications and complexities. The Acronis solution offers MSPs the consolidated, comprehensive

and natively integrated functionality they need to protect clients in a Microsoft 365 environment and redistribute resources. It effectively delivers RMM for Microsoft 365 and much more.

Acronis Ultimate 365 enables MSPs to efficiently deliver the most complete 7-in-1 protection for Microsoft 365, integrating backup, XDR, email security, collaboration app security, email archiving, security posture management and security awareness training into a single, intuitive, multitenant platform. MSPs pay only for the services they use and deliver clients maximum value for their money.

Acronis Ultimate 365 delivers:



Complete Microsoft 365 protection in a single integrated platform

Protect it ALL — Confidently protect all aspects of your clients' Microsoft 365 seats with natively integrated data protection, cybersecurity, posture management and security awareness training.



Fastest time to profit

Remove all barriers to product selection, contract negotiation, staff training and client onboarding. Just sell and enable services with the flick of a switch and start making money.



Most efficient management

Manage all customers and services in a single platform, with less time and expertise required.

MSPs that are not poised to confidently and profitably offer Microsoft 365 protection will inevitably fall behind those that are. With Acronis Ultimate 365, protecting the popular Microsoft 365 platform is no longer a problem. It's an opportunity.