



THE MSP PLAYBOOK TO

WORKING SMARTER
NOT HARDER



HORNETSECURITY



AMY BABINCHAK

Amy Babinchak is a distinguished IT professional, business owner, and thought leader with over two decades of experience in the technology industry. She owns several IT businesses, including Harbor Computer Services, and was ranked #40 among the top 501 MSPs in the U.S. before selling her MSP business in 2023.

Amy currently runs Third Tier, which offers advanced IT support services to vendors and consultants, focusing on Microsoft technologies.

Amy's technical prowess is widely acknowledged in the industry. For 18 years, she has been honored as a Microsoft Most Valuable Professional (MVP), a testament to her deep knowledge and contributions to the Microsoft ecosystem. Her advanced skills in network design, management, and implementation have earned her recognition as one of the top 100 IT professionals by MSP Mentor. In addition to her MVP status, Amy holds several Microsoft certifications, including Identity and Access Administrator.



PAUL SCHNACKENBURG

Paul started in IT when DOS and 286 processors were the cutting edge. He runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. He also works as an IT teacher at a Microsoft IT Academy.

Paul is a well-respected technology author and active in the community, writing in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies. He holds MCSE, MCSA and MCT certifications.

FOREWORD BY ERICK SIMPSON

The IT services industry is in constant flux, with Managed Service Providers (MSPs) evolving from behind-the-scenes support teams to trusted, strategic partners driving growth for their clients—and for themselves. This transformation is now rooted in addressing today's high-stakes cybersecurity challenges, meeting complex compliance demands, and staying ahead of the curve in a rapidly digitizing world.

As someone who has built an MSP from scratch, successfully sold it and then dedicated my career to coaching hundreds of MSPs around the globe, I've had a front-row seat to the incredible evolution of our industry. Each MSP's journey is unique, yet the common threads are the ability to adapt, think strategically, and balance the complexities of technology, client and vendor relationships, and operational efficiency.

This eBook is more than a guide—it's a lifeline for MSPs looking to do more than survive in today's landscape. It's about thriving and delivers actionable insights that align perfectly with the lessons I've learned throughout my career. Amy Babinchak and Paul Shackenburg have poured their experience and expertise into this work, offering a roadmap that MSPs of all sizes can follow.

The discussion on client onboarding, for instance, immediately stood out to me. A seamless onboarding process sets the stage for a strong, enduring partnership, and when done well, it can be the difference between a satisfied client and a lifelong advocate. The emphasis on providing proactive cybersecurity measures with a streamlined set of solutions aligns with my belief that we must control vendor and platform sprawl. This approach is essential for scaling our services to meet changing client needs while maximizing service efficiency and profits.

In my work helping MSPs grow, transform, and sometimes prepare for mergers or acquisitions, I've seen how critical it is to embrace efficiency and differentiation. This eBook zeroes in on both. From practical advice on leveraging automation to thoughtful strategies for staying ahead of cybersecurity threats, these are not just theoretical ideas—they're real-world solutions that can immediately impact an MSP's success.

What strikes me most about this eBook is its clarity and applicability. It's not just about identifying problems—it's about offering solutions you can put into practice right away. For any MSP looking to refine operations, strengthen client relationships, or position themselves as indispensable partners in today's digital era, this is the guide you've been waiting for.

To my fellow MSP leaders, whether you're just starting out or are seasoned veterans, this eBook offers insights that will challenge, inspire, and empower you and your teams. I'm confident that as you read, you'll discover solutions to some of your biggest challenges and new opportunities to elevate your business and ultimately enhance the value you bring to your clients.

Here's to your continued growth and success.



Erick Simpson

CEO and Chief Strategist
MSP Mastered® | Channel Mastered
<https://linkedin.com/in/ericksimpson>

Erick Simpson is an MSP expert, influencer, thought leader, and a trusted advisor to thousands of MSPs across North America. As the creator of the MSP Mastered® Methodology, he's helped countless IT Solution Providers transform their businesses to achieve consistent, profitable growth.



TABLE OF CONTENTS

CHAPTER 1	Introduction to Improving MSP Efficiency	4
CHAPTER 2	Onboarding	7
CHAPTER 3	Monitoring and Maintenance	14
CHAPTER 4	Customization	21
CHAPTER 5	Cybersecurity	26
CHAPTER 6	Vendor Management	33
CHAPTER 7	Conclusion	38



HORNETSECURITY



CHAPTER 1

INTRODUCTION TO IMPROVING MSP EFFICIENCY

This eBook aims to provide MSPs with practical strategies to operate more efficiently across several business areas and remain competitive in our rapidly evolving industry. By reading this eBook, you'll gain insights into how the most efficient MSPs operate, improve your profitability, and stay ahead of demand.

MSPs face unprecedented challenges and opportunities today. We'll explore how successful MSPs have leveraged automation tools to streamline operations and reduce costs while maintaining the all-important client relationship. This eBook will guide you through the essential strategies to thrive in this dynamic environment.

UNDERSTANDING HOW WE GOT HERE

The business model we call Managed Services was created when infrastructure was held on premises and owned by the client. Servers were ubiquitous, computers were stationary objects on desks tethered to ethernet cables, and little to no work was done on the weekend by the office staff. The Managed Services Provider (MSP) aspired to become the outsourced IT department for the business and brought cost savings by splitting their time across a small number of clients. The MSP staff were highly technical in infrastructure configuration, deployment, and troubleshooting skills. Most operations done by the MSP were performed manually and in person. The tools used were minimal troubleshooting aids like TechNet, Wireshark, and cable testers. A lot of pizza was eaten, and sugary, caffeinated drinks were consumed during server upgrades. Marathon troubleshooting sessions with Microsoft on the other end of the phone were the norm, and participating in user group meetings was a regular occurrence.

Then, the cloud came along.

The cloud required a change in skillset. Instead of focusing on server installation and connectivity, the MSP now had to understand how to manage applications from afar. Demand for services and a wider variety of services pushed MSPs to hire more staff and spread them across more clients to maintain profitability, as some revenue sources shifted from highly profitable infrastructure projects to low-margin software subscriptions with ongoing accounting overhead.

Then, the cybercriminal came along.

The cloud improved the likelihood that cybercriminals could access corporate data, so they set up more elaborate toolsets for themselves, inventing the plagues MSPs fight today, such as ransomware and phishing. There had always been an undercurrent of hacking but beginning with the invention of ransomware in 2013, business disruption ramped up fast.



 AUTOMATE.
 STANDARDIZE.
 GOVERN.



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)

Then, the cyber insurance industry and compliance regulations came along.

When ransoms began being paid, cybercrime exploded, and an alphabet soup of industry-specific cyber compliance requirements emerged. MSPs found themselves on the front lines of defense without the skill set or pricing model to support their clients' needs and had to pivot quickly to keep up with these new demands. Most invested heavily in more and more software tools to help them cover their skill gaps and automate repetitive tasks. Today, MSPs typically spend 20% or more of their revenue on software toolsets. It's become a crisis driven by inefficiency.

OPERATING AS AN EFFICIENT MSP

The change in the industry in which the MSP operates happened quickly. Still, the business model has been slow to adapt, and many MSPs are struggling to maintain profitability in an industry once known for high profits and a source of good-paying jobs. The good news is that businesses realize that they need MSPs, and MSPs know that they must modernize to remain successful and profitable.

This eBook explores key areas of MSP operations, highlighting where efficiencies can be improved and suggesting methods to achieve them. There is a heavy emphasis on Microsoft 365 and cybersecurity as we look at MSPs based on their practices in those product areas. We don't get into specific technical solutions or address financial issues but illustrate the big picture of how an efficient MSP operates. The result is that you'll understand how the industry can continue to create good jobs, provide a needed service, and get a handle on technical issues that aren't going away, like cybersecurity and compliance. The MSP plays a vital role in the success of all businesses in every economy worldwide. When an MSP is successful, everyone wins.

Are you ready to transform your MSP business and achieve new levels of efficiency? Let's dive in and discover the secrets to success, starting with the first job an MSP encounters with a new customer: Onboarding.





HORNETSECURITY



CHAPTER 2

ONBOARDING

Onboarding is often seen as an expense and a drain on labor resources. However, this chapter aims to transform your perspective by highlighting the benefits of a well-executed onboarding process and providing tips to enhance efficiency.

TWO VIEWS OF ONBOARDING

Understanding how a client views the work of an MSP can be challenging. Clients, who may not be very technical, focus on the experience of doing business with them, while MSPs tend to be outcome-focused. This difference in perspectives makes the onboarding process a crucial opportunity to impress and delight new clients.

What will impress the client? What will delight the client?

IMPRESS	DELIGHT
Professionalism	Personalization
Efficiency	Responsiveness
Expertise	Friendliness
Reliability	Attention to detail

Figure 1 Impressing and delighting clients

What are the outcomes that the MSP is focused on?

ONBOARDING OUTCOMES	
Joining endpoints to management solution	Migrating to Microsoft 365 solutions
Secure the endpoints	Minimize downtime
Deploy applications	Deploy MSP toolset
Configure compliance requirements	Finish quickly

Figure 2 Outcomes MSPs are focused on



Effortless onboarding, governance, and compliance for all M365 tenants

365 

MULTI-TENANT MANAGER FOR MSPs

LEARN MORE

ONBOARDING FROM THE CLIENT'S VIEW

As their MSP, it's increasingly the soft skills that your client is measuring you on. Initially, they will probably believe they can go anywhere and hire good technical skills. But it was your sales process that made them choose you. Your elevator pitch, your website, and the communication of your unique value proposition sold them on you over the other MSPs they interviewed. If you mess up that "good feeling" during onboarding, the client relationship can be forever tainted. You need to impress them from day one of onboarding.

Putting the two charts above into action, here's what you and your MSP staff should focus on.

1. PROFESSIONALISM:



Clear Communication: Maintain clear and consistent communication with the client throughout the onboarding process. Provide plain language explanations of each step and set clear expectations. Good communication helps clients remain calm and patient, as it addresses potential business problems.



Documentation: Provide plain language documentation for all processes and procedures. This helps the client understand what is being done and ensures they have a reference for what they see happening around them.



Appearance: Ensure that all interactions, whether in person or virtual, are conducted in a professional manner. This includes dressing appropriately and maintaining a professional and friendly demeanor.

2. EFFICIENCY:



Streamlined Processes: Clients may not understand the technical details, but they can recognize inefficiency. Implement strategies to make onboarding a repeatable process and apply learnings from each new client to improve the experience for the next one.



Automation: Automate onboarding to Microsoft Intune to simplify configuration, compliance, security configuration, and application deployment to Windows and other platform endpoints.



Quick Resolution: Address any issues or concerns promptly and efficiently to minimize downtime and ensure a smooth onboarding experience. Don't forget to communicate the process along the way and check in with the client to see how they are reacting to the resolution process.

3. EXPERTISE:



Knowledge Sharing: Prepare the client for the onboarding process by holding a short meeting to explain the steps involved. Afterward, share your expertise with the client by providing training sessions and resources that help them understand and utilize the services being provided.



Problem Solving: Demonstrate your expertise by solving any technical issues during the onboarding process. Don't hold them for later. The client will likely view any anomaly left as a failure to complete the onboarding process.



Customization: Tailor the onboarding process to meet the client's specific needs and requirements, showcasing your ability to provide personalized solutions. Simple things like adding their logo, company name, and background picture to your reports and platforms demonstrate that you are providing a solution just for them.

4. RELIABILITY:



Consistent Performance: New clients may have had negative experiences with previous MSPs. Ensure all tasks and processes are completed accurately and on time to build trust and confidence in your services.



Follow-Up: Follow up with the client after onboarding to address any lingering issues and ensure their satisfaction. If they think you missed something, solve it immediately.



Dependable Support: Provide reliable support throughout the onboarding process and beyond, ensuring that the client feels supported and valued.

If your MSP does each of these things, client delight will follow. By focusing on professionalism, efficiency, expertise, and reliability, you can create a delightful onboarding experience for your clients. When you follow up to get the client's impression of their onboarding experience, you should hear their words of delight, like "friendly," "professional," "expert," and "knowledgeable." Then, you'll know you did a great job cementing the client relationship by providing an exceptional onboarding experience.

It's often the little things – I remember onboarding a client, who still had a server onsite, and the business owner was amazed that we took the time to print out small labels for every cable connected to the server, as well as the networking cables. He said no one else had ever done that, and I explained that the little bit of extra time spent now, could save a lot of time in a crisis in the future. Labelling everything, and documenting everything is part of a good onboarding process.

ONBOARDING FROM THE MSP VIEW

While we understand what the client perceives as a successful onboarding experience, it's important to recognize that, from the MSP perspective, much of the work happens behind the scenes to ensure success.

In **Figure 2**, you might wonder why 'finishing quickly' is on the list. Finishing quickly keeps the client happy by ensuring that the migration to your services doesn't drag on and disrupt their business. From the MSP perspective, finishing quickly means only dedicating the necessary staff hours to the project, optimizing your resources and efficiency.

EFFICIENCY IN ONBOARDING

Step one in increasing your efficiency in onboarding new clients is to design a process for information gathering. For example, your MSP must gather the existing licensing, admin passwords, and MFA transition details and consolidate documentation into your system. Experience says that much of this information won't be available from the client or the previous MSP, so you'll need a proven method for gathering that information quickly.

Efficiency in onboarding is achieved through repeatability and automation. These two concepts enable your MSP to remain profitable while impressing clients with your professionalism and demeanor. With a Microsoft partner account that includes an Action Pack subscription or higher plans, you gain access to at least one demo tenant. Demo tenants are excellent for staging your standard settings.

One limitation of using only a demo tenant to stage your settings is that you don't experience what it's like to live with those settings. Therefore, consider using your MSP production tenant for settings as the "canary" ring. It's a good idea for you to experience the security level of your most secure tenant and uphold that as the gold standard. This concept is affectionately known in the industry as "eating your own dog food." Then, test the settings on a group of change-tolerant clients for your next test ring before making the broad rollout. Using this process, you'll make fewer mistakes and allow your marketing staff to prepare messaging about the new settings and your helpdesk staff to modify any of their procedures as needed.

COMPLETING OUR TASKS

To achieve efficiency in onboarding, you must accomplish the following four tasks:



Figure 3 Onboarding tasks

Using Hornetsecurity's **365 Multi-Tenant Manager for MSPs** your tenants can be onboarded into a "single pane of glass" portal easily. It allows you to select all your clients from the Microsoft Partner Portal or a selection of them, as seen in **Figure 4** below.

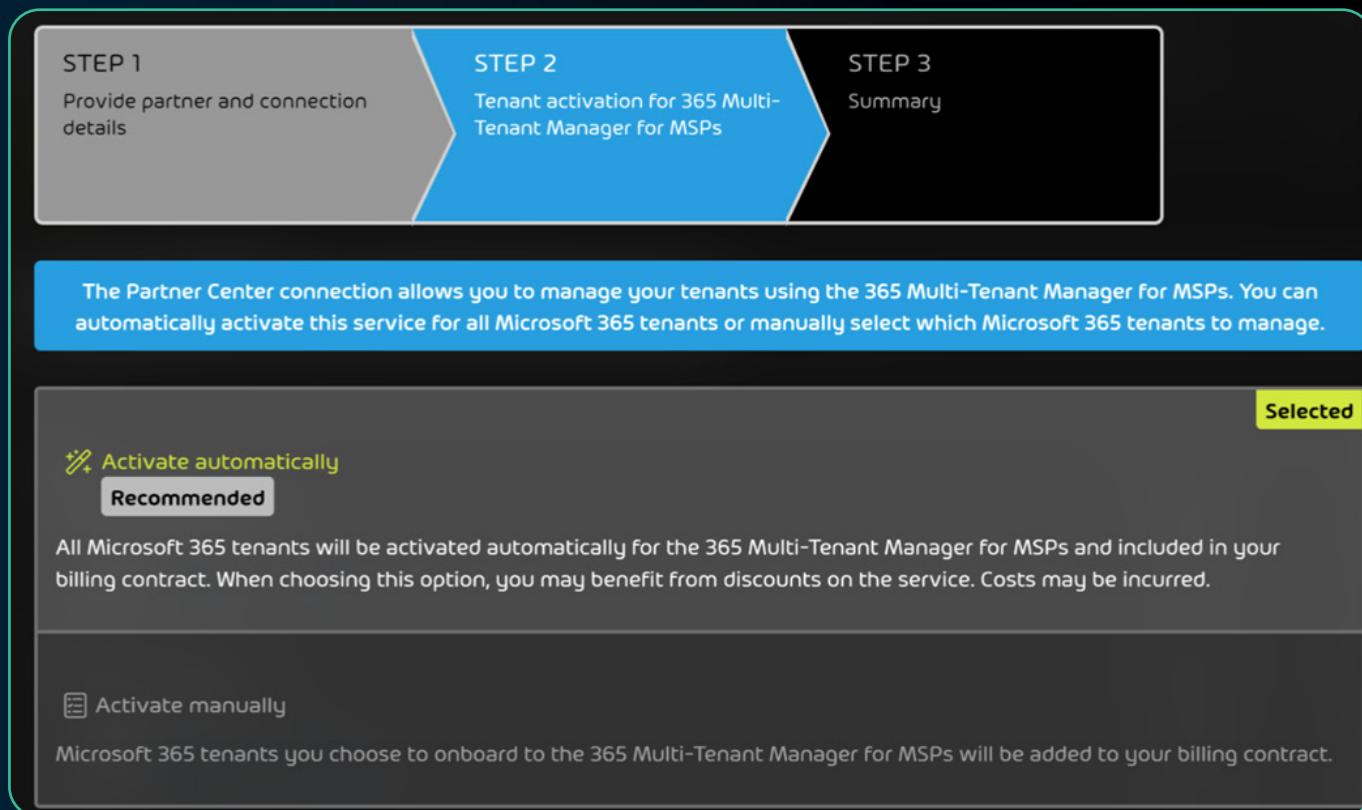


Figure 4 Use the wizard to quickly bring your tenants into your management portal.

Once your tenants are gathered, Microsoft includes several tools to facilitate device onboarding, each appropriate for different client scenarios.

- **Windows Autopilot** is ideal for automating device enrollment and configuration. It offers a streamlined Microsoft Entra join during the Windows Out-of-Box Experience (OOBE) and enables zero-touch deployment of new devices.
- **Bulk Enrollment** is suitable for existing devices or scenarios where Autopilot isn't applicable.
- **Microsoft Device Management (MDM) Enrollment with Intune** allows devices to be automatically enrolled in MDM during the Microsoft Entra join process, enabling management as soon as they join your organization.
- **Self-Service Enrollment** is good for BYOD scenarios. Users can enroll their own devices through the Windows Settings or OOBE.
- **PowerShell and Scheduled Tasks** can be used for existing Entra AD-joined devices that need to be enrolled in Intune. A PowerShell script with appropriate parameters can trigger the deviceenroller.exe, or a scheduled task running under system context can execute the enrollment script.

After onboarding devices using one of the above methods, they will be ready to configure with Microsoft Intune. Intune is your tool for pushing out device configuration and compliance settings. Microsoft provides security baselines and templates to assist you in creating your standards.

One key to efficiency is having a well-documented standard with checklists and Standard Operating Procedures (SOPs) so that the process is repeatable by all of your staff each time a new client is onboarded. There is no automated tool for this included in the Microsoft 365 suite. Instead, you are expected to purchase an industry tool or use Microsoft OneNote, for example.

The next step toward onboarding efficiency is standardizing portal configuration and security controls. Both happen at onboarding, and you need to maintain the standards over time, too. Microsoft provides tools to assist with the initial configuration, such as security baselines and the Microsoft Desired State Configuration (DSC) tool. However, each has its limitations. If you choose to use the security baselines, you'll have to test and adapt the changes to those as Microsoft releases them. In addition, the provided baselines tend to be very strict, and many users may find it challenging to perform their job function with the full implementation. You'll need to test them with each client. Once you establish the standard, you can create a "golden image" using the DSC tool. This tool allows you to push out that configuration to a tenant you need to onboard with identical settings.

In practice, most MSPs find these tools difficult to use. Better options may be available in third-party solutions like Hornetsecurity's **365 Multi-Tenant Manager for MSPs**. This solution lets you save a custom golden image and use your own set of settings to push out to a new onboarding client.

SUMMARY

In conclusion, achieving efficiency in onboarding is crucial for maintaining profitability and impressing clients with your professionalism and demeanor. By leveraging tools like Microsoft Intune for device configuration and compliance settings and utilizing security baselines and templates provided by Microsoft, MSPs can create a standardized and repeatable onboarding process. However, it is essential to have well-documented standards, checklists, and SOPs) to ensure consistency across all staff members.

Standardizing portal configuration and security controls during onboarding and maintaining these standards over time is vital. While Microsoft provides tools like security baselines and the Desired State Configuration tool, MSPs may find third-party solutions like Hornetsecurity's **365 Multi-Tenant Manager for MSPs** more user-friendly and effective for creating and deploying custom "golden images" and even, as we'll see in later chapters, maintaining and updating the security posture of their supported networks.

By focusing on automation, standardization, and thorough documentation, MSPs can streamline the onboarding process, minimize downtime, and ensure a smooth transition for new clients. This approach enhances efficiency and builds trust and confidence in the services provided, ultimately leading to a successful and delightful onboarding experience for clients.



HORNETSECURITY



CHAPTER 3

MONITORING AND MAINTENANCE

The bread and butter of the MSP has long been monitoring and maintenance. Maintenance helps with proactive work, while automated monitoring identifies and raises alerts when changes and threats are detected. With the rise of cybersecurity and compliance requirements, these tasks have never been more critical. Nor have they ever taken up more brain cycles than they do today.

Efficiency in monitoring and maintenance can be tricky. It's easy to believe that everything should be automated, but the reality is that human brains and expertise are still needed. You must also consider what happens when monitoring detects a serious issue. Your MSP needs to find the sweet spot of profitability by marrying the need for efficiency with human implementation of response. In some ways, this job is more challenging and complex today than ever, creating a lot of stress for MSP owners and their staff. Having procedures and plans in place is how to stay efficient and manage the workload effectively.

PROACTIVE MAINTENANCE

Proactive maintenance is essential for preventing issues before they become critical. Traditional Remote Monitoring and Maintenance (RMM) software is heavily laden with technical debt. Its focus is primarily on managing software updates and looking for hardware-level faults. While this is important, it's far less important today. Operating system updates are now safer, and users have become more sophisticated. Updates can be scheduled to install natively in the operating system and applications.

Hardware-level faults are fewer, and the industry has moved away from swappable components and those that require significant cooling. This study from Backblaze, which covered five years and several thousand SSD drives, showed the failure rate to be less than 1%.

Backblaze SSD Lifetime Annualized Failure Rates								
Reporting period: 10/1/2018 to 06/30/2023 inclusive for active drive models as of 06/30/2023								
MFG	Model	Size (GB)	Drive Count	Drive Days	Drive Failures	AFR	Confidence Interval	
Crucial	CT250MX500SSD1	250	598	205,743	9	1.60%	0.9%	3.3%
Dell	DELLBOSS VD	500	411	304,937	0	0.00%	0.0%	0.4%
Micron	MTFDDAV240TCB	250	88	83,259	9	3.95%	1.8%	7.5%
Seagate	SSDSCKKB240GZR	250	1	133	1	274.44%	0.0%	1012.4%
Seagate	ZA250CM10003	250	1,114	924,856	14	0.55%	0.3%	0.9%
Seagate	ZA500CM10003	500	3	1,125	0	0.00%	0.0%	119.7%
Seagate	ZA2000CM10002	2,000	3	5,538	1	6.59%	0.2%	36.7%
Seagate	ZA250CM10002	250	547	667,680	17	0.93%	0.5%	1.5%
Seagate	ZA500CM10002	500	18	29,739	0	0.00%	0.0%	4.5%
Seagate	ZA500GM10001	500	2	682	0	0.00%	0.0%	197.4%
Seagate	ZA250NM1002	250	80	15,523	0	0.00%	0.0%	8.7%
Seagate	SSD	250	106	151,465	3	0.72%	0.1%	2.1%
WDC	WD Blue SA510 2.5	250	65	3,716	4	39.29%	10.7%	100.6%
WDC	WDS250G2B0A	250	108	38,914	2	1.88%	0.6%	8.2%
Totals			3,144	2,433,310	60	0.90%		



Figure 5 <https://www.backblaze.com/blog/how-reliable-are-ssds/>

The growing trend toward laptops has also helped. While the 3-to-4-year hardware refresh cycle was a goal for a while, today, many MSPs find that 4-, 5-, and even 6-year-old machines are still running well.

What does this mean for maintenance? It means you should automate as much as possible and monitor for exceptions to the successful deployment. Maintenance activities should be reduced as the reliability of hardware has increased.

AUTOMATED MONITORING

While the time that maintenance requires has declined, the time spent on monitoring has increased, even with the assistance of automation. While alerts from issues like full hard drives have decreased due to cloud storage, alerts from phishing, identity, and application activities have skyrocketed. Automated monitoring plays a crucial role in identifying potential threats as it covers business continuity and cybersecurity issues. MSPs need a robust and intelligent monitoring solution simply to keep up with the onslaught of information discovered, from logs to settings changes to indicators of malware activity. The monitoring program is the backbone of any threat detection plan.

The automated monitoring program must be smart enough to understand the severity level of a single change or several changes taken together. The combination of Microsoft's built-in toolset, like Intune for device monitoring, Sentinel for alert management, and Defender XDR for incident tracking, act together to provide an intelligent monitoring solution that can take automated actions while mapping the activity and sending alert messages. Third-party suites, like Hornetsecurity's **365 Multi-Tenant Manager for MSPs** and business protection plans, are using several of their products along with Artificial Intelligence (AI) to help MSPs gain insight and automated protection from the monitoring program. Whichever product is chosen, it should be a complete suite of tools that work together to build not just a monitoring solution but one that can also act on the MSP's behalf when specific conditions are met.



Manage and monitor all
M365 tenants from one portal



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)

INCIDENT RESPONSE AND DISASTER RECOVERY

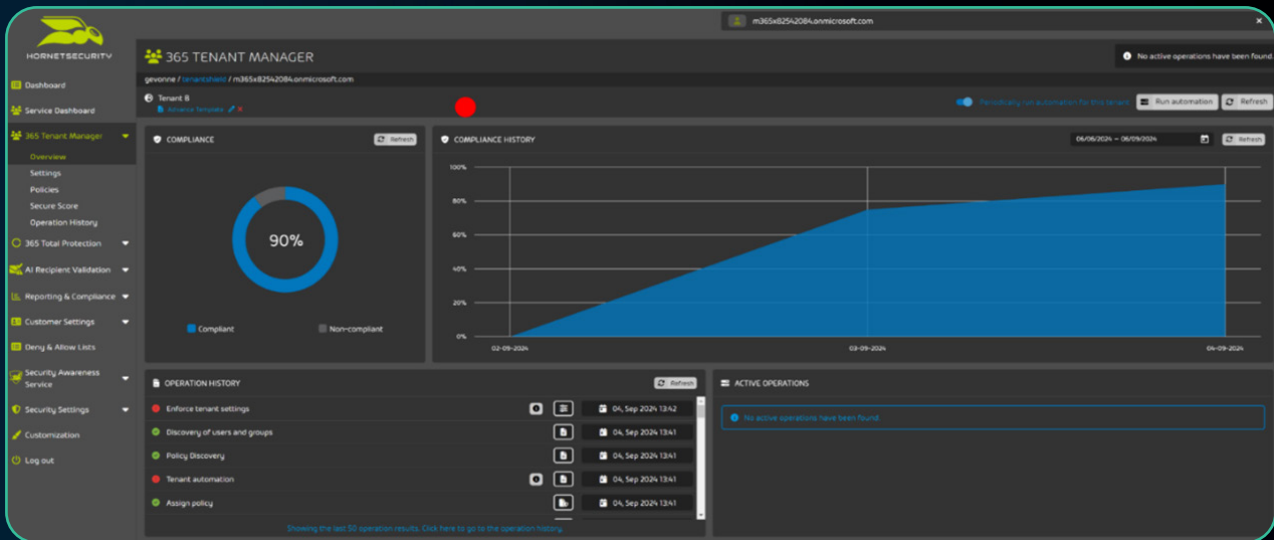
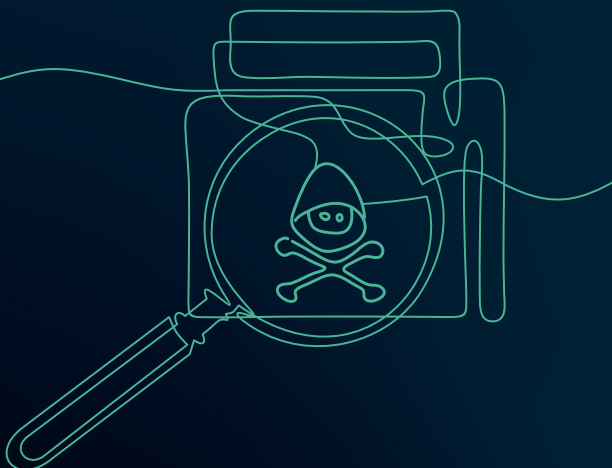


Figure 6 Tenant Overview in Multi-Tenant Manager

The complexity of incident response and disaster recovery has never been higher. With the rise in ransom demands by cybercriminals, insurance companies and regulatory agencies have become more involved in the recovery process. This means that today, a technical component, compliance, and insurance requirements must all be built into incident response and disaster recovery plans. While many cyber insurance plans use general terms such as “soon” or “promptly,” others have specific timeframes such as “within 72 hours”. Most MSP technicians want to jump into recovery mode immediately to get their clients’ businesses running again as quickly as possible. Still, cyber insurance will often have requirements that limit the immediate response to containment only, with the first step of the process being to contact them so their experts can assist with the recovery. In addition, compliance regulations may have reporting requirements. As if that isn’t enough, many businesses don’t want to invest as significantly in prevention and recovery planning as they should. Without a doubt, cybersecurity threats have made the business of the MSP far more difficult and complex.



One small SMB client of mine had a cyber security breach, and moved quickly to re-image end user laptops to “get back up and running quickly”, against our recommendation of taking our time to establish how they got in and exactly what was compromised. A few days later, the attackers were back, again deploying ransomware. It wasn’t until this happened a third time that the client let us bring in Digital Forensics Incident Response (DFIR) experts and their investigation unearthed a UEFI root kit implant which provided the attackers with a handy back door, even after laptops were re-imaged. The only solution was to purchase new laptops for everyone.

DISASTER RECOVERY

Even while incident response is happening, many have unfortunately taken their eye off the ball when it comes to the baseline: the “if everything else fails” backup. It’s like they forgot about business recovery as soon as the data was stored in the cloud! But backup has never been a built-in feature. It always had to be bolted on by a third party. Most cloud vendors will tout their backup feature, but their backup is not for the client, nor the MSP, it’s for them. Should they have a failure, they can restore the service and your data to you. But if you want the backup experience that a disaster recovery plan requires, you need a third party to provide it.

Hornetsecurity offers a modern **365 Total backup solution** that includes data stored in Microsoft 365, a comprehensive monitoring component, and endpoint backup:

- » **Multi-tenancy**
Manage and monitor all Microsoft 365 organizations and Windows endpoint backups through a central, multi-tenant online management console.
- » **User-friendly backup dashboard**
Centrally monitor backup and restore activities, backup health status, and recent restore history. Set notifications for successful, failed, or warning backup states, email alerts, or a daily summary digest.
- » **Automated Microsoft 365 backups**
M365 backups take place automatically multiple times per day. For endpoints, backups can be set to take place every 1 to 24 hours.
- » **Backup of on-premises and roaming endpoints**
Back up any endpoint, whether at the office or anywhere around the world, without requiring a VPN.
- » **Endpoint backup & policies**
Policy-driven file-level backup for Windows desktops and laptops. Configure settings for large groups of Windows endpoints by setting up policies to define backup directories, cloud storage, frequency and retention.
- » **Back up data anywhere, anytime**
Back up specific users, groups, MS Planner, SharePoint document libraries, and endpoints at any time.
- » **Four-eye approval process**
An additional layer of security that mitigates the risks of losing data due to actions of rogue and novice administrators, demanding that sensitivity actions such as deletion of data, changes to company settings, and more, require at least one approval from a selected approving administrator, separate to the initiating administrator.

This type of all-inclusive backup solution for disaster recovery is needed in today’s target-rich business environment. The likelihood of needing to restore data has increased in recent years, right in step with cybercrime.

INCIDENT RESPONSE

As much as MSPs would like to return to the days when restoring from backup was an incident response, they can't. The complexity has increased so much that MSPs need a defined incident response process. Here are six steps that make up incident response today. Notice that Recovery is step #5 in this top-down list.

- 1. Containment:** The first step is to contain the incident to prevent further damage. This may involve isolating affected systems, disabling compromised accounts, and stopping malicious processes. Your monitoring application should have alerted you to the threat while your chosen cybersecurity solution got started on disrupting the attack chain.
- 2. Notification:** Next, you must notify any regulatory body that needs to be informed. For smaller firms, that is probably the cyber insurance company. For regulated and public entities, it will be the legal department. They will need to be notified about the incident and will probably get their experts involved in the recovery process.
- 3. Investigation:** This may be the part where the experts come in to conduct a thorough investigation to determine the cause and extent of the breach. This involves analyzing logs, identifying compromised systems, and gathering evidence. The MSP may find themselves in an advisory role, providing information to the recovery team and will likely need to be in a communications role too. As the trusted advisor, the MSP knows the personalities of the business management and the function of the business. This puts them in a key position for bridging any communication gaps and setting expectations.
- 4. Eradication:** Your MSP may then be called in to remove the cause of the incident, such as deleting malware, closing vulnerabilities, and resetting passwords.
- 5. Recovery:** If the network has sustained damage or some area cannot be guaranteed safe and secure, then the MSP will need to restore affected systems and data from backups and ensure that all systems are fully operational.
- 6. Post-Incident Review:** Finally, your MSP and any other crime players involved in the investigation create a report and conduct a post-incident review to learn from the event and improve the incident response plan for future incidents.

There will probably be many lessons learned by the business and your MSP that will forever improve the security of the business network. The client is facing something they don't understand at a technical level, which is a business interruption, and they'll look to you not only for the technical recovery described above but also for reassurance and an explanation of the steps taken in each phase. This is a time of high stress for them and you. Good communication goes a long way in overcoming mismatched expectations, which are often at the heart of any discontent that may arise.

When you execute the disaster recovery plan well, your relationship with the client should become stronger than ever.

BALANCING EFFICIENCY AND HUMAN EXPERTISE

All of this activity is time-consuming, but luckily, machine learning and AI have come to our rescue. Provided that a modern solution set is subscribed to that includes automation and AI to help take some of the skill and time load from the MSP's helpdesk staff; the MSP should be able to handle a disaster recovery scenario alongside their regular deployment, monitoring, and alerting activities. Finding the right balance between efficiency and human expertise is key to successful monitoring and maintenance.

Many MSPs have trended toward hiring lower-skilled employees. Meanwhile, developers have focused on reducing the workload of less skilled staff. Since the tools that MSPs use for day-to-day operations are designed to minimize low-skilled work, they need to hire higher-skilled staff and more highly skilled personnel proficient in managing business continuity and disaster recovery. This staff should understand business motivation, communications, cybersecurity, and disaster recovery. Lower-skilled staff are still needed but will be more tools-based and customer service-focused.

Most importantly, the low-skilled staff are the ones that the client speaks to most often. They are the phone answerers, the triage team, and level-one technical assistance. Pay attention to your touch-points, as much of an MSP's customer service rating relies on how well they make the client feel in moments of stress.

SUMMARY

In this chapter, we explored the critical aspects of MSP efficiency in monitoring and maintenance activities. We dove into the importance of proactive maintenance, the role of automated monitoring, the importance of incident response procedure and disaster recovery planning and the need to balance efficiency with human expertise. By implementing effective procedures and plans, MSPs can enhance their performance, reduce stress, and achieve greater profitability.



Manage and monitor all
M365 tenants from one portal



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)



HORNETSECURITY



CHAPTER 4

CUSTOMIZATION

Customization is a tricky subject. While MSPs need to standardize, they must recognize that every client is unique and avoid the temptation to deploy cookie-cutter solutions that any competitor could replicate. MSPs need customization to help define themselves in the market.

Customization is complicated in its motivation, but the goal is to customize efficiently and where the impact matters. In this chapter, we draw a line between customization and custom deployment and consider when and why to perform each.

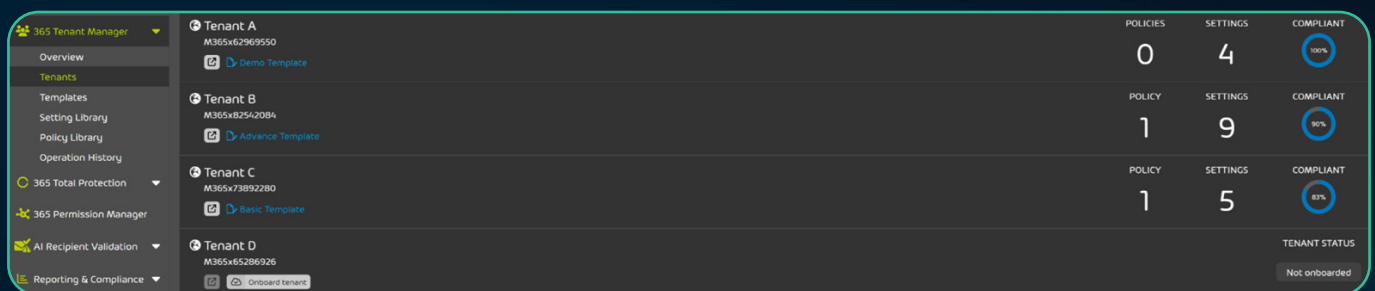
WHAT IS CUSTOMIZATION?

This might seem like a ridiculous question but it's a very important one. What is a custom deployment, and what is customization? It's important to differentiate between them so that you don't lose your goal of efficient operation.

A SOLUTION TO DEPLOY A CUSTOM CONFIGURATION

Using Hornetsecurity's **365 Multi-Tenant Manager for MSPs**, you can swiftly create a custom configuration based on your SOPs. This tool allows you to deploy an entire tenant's configuration in just a few moments, ensuring your design is immediately sent to all the tenants you support. Every MSP should have a custom deployment that reflects their standards while considering the recommended baselines.

Below is an example of what this might look like. Each client is assigned a template that represents your standard configuration for clients like themselves.



Tenant	Policy	Settings	Compliant
Tenant A M365x62969550 Demo Template	0	4	100%
Tenant B M365x82542084 Advance Template	1	9	90%
Tenant C M365x73892280 Basic Template	1	5	80%
Tenant D M365x65286926 Onboard tenant			Not onboarded

Figure 7 Hornetsecurity Multi-Tenant Manager

Using templates, you can maintain your custom solution by grouping clients into the appropriate template. When you make changes to the template, the clients with that template are automatically updated. This method is used to deploy a custom configuration efficiently.



Customize tenant configuration to meet each customer's unique M365 needs

365 

MULTI-TENANT MANAGER FOR MSPs

LEARN MORE

DEPLOYING CUSTOMIZATION EFFICIENTLY

But you should also perform customization. Certain areas of every Microsoft 365 tenant allow customization, which helps the client know that they are operating in their own network, within compliance and regulatory rules, and working safely. This is no different from when you installed a Microsoft Server and applied your settings to it. It was your custom deployment of that server and the physical presence of the box that let the client know that they owned it. Today, physical presence is replaced by customization.

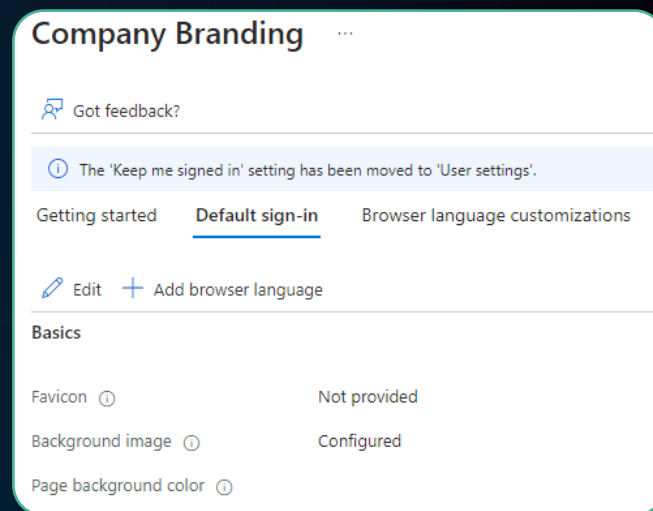


Figure 8 Customizing with a corporate-approved sign-on background image

You may not have that physical server anymore, but with a Microsoft 365 deployment, customization can include things like the corporate logo, business name, your MSP's support name and contact information, and a background image on the sign-in screen. These things help the business users understand when they are operating in their corporate network. For your MSP, it also differentiates you from others who don't take the time to make these customizations.

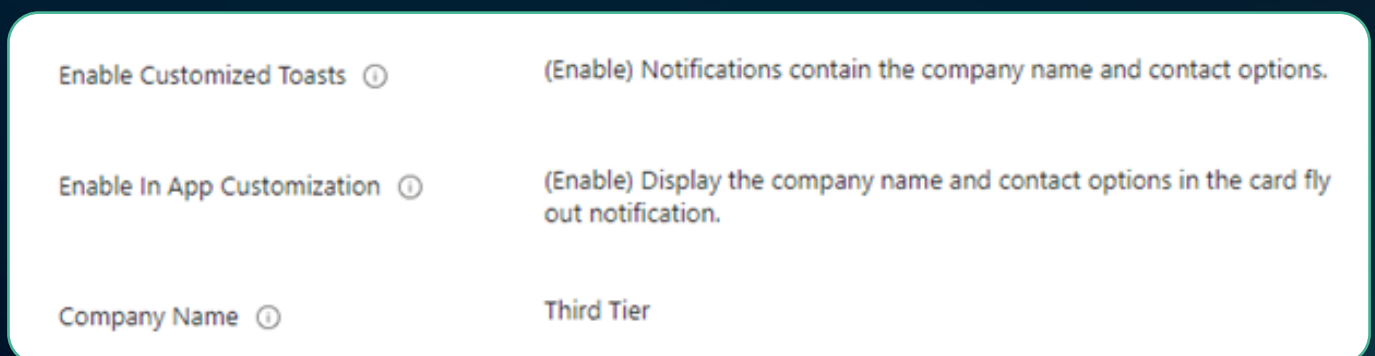


Figure 9 Customizing toast pop-ups with company name and contact information

Customization can also include some standardization that will be appropriate for a group of client tenants. Perhaps you have several clients who accept credit card payments and store this data. In this case, they will all need your PCI compliance policy.

Hornetsecurity's **365 Multi-Tenant Manager for MSPs** lets you apply that to the appropriate tenant as needed. As shown in **Figure 9** above, where you create a template for each type of business, you would do the same for the compliance and regulations your clients need and apply your settings template.

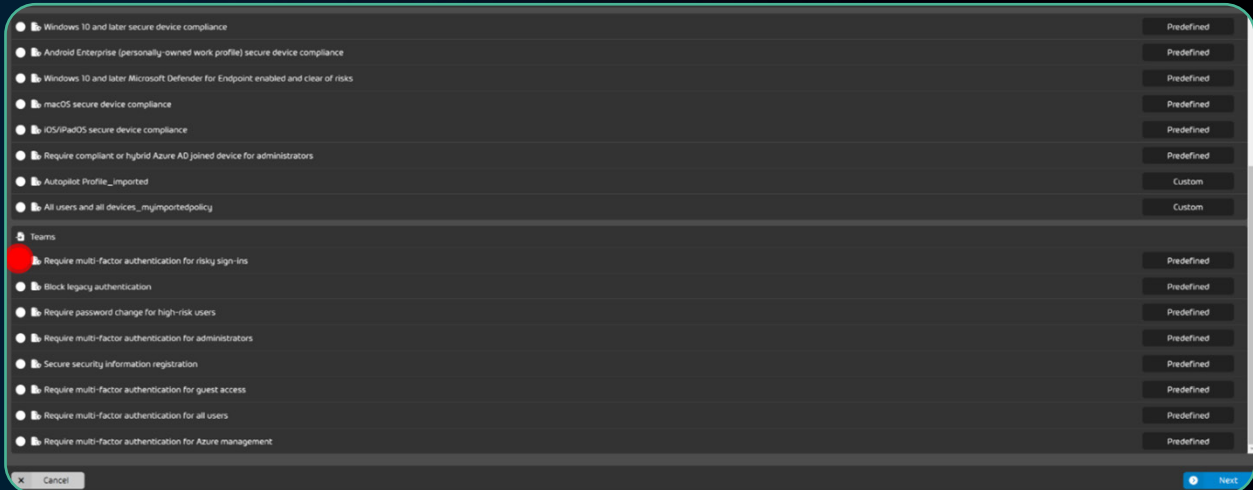


Figure 10 Multi-Tenant Manager settings templates

TIME MANAGEMENT

Time management is the key to MSP efficiency. To remain efficient, you need to:

- » Configure the initial deployment with domain name and DNS entries
- » Deploy your customized tenant configurations
- » Deploy compliance and regulatory configurations to the right tenants
- » Configure specific business customizations and user experiences

The time spent on each task is important. An efficient MSP should spend 10% or less of their time on tenant deployment and 90% on customization, including regulatory and compliance requirements. Why break it down this way? Because the custom deployment is for the MSP, while the customization is for the client. An MSP should always aim to spend the majority of their time working for the client.



**Customize tenant configuration
to meet each customer's
unique M365 needs**



**MULTI-TENANT
MANAGER FOR MSPs**

[**LEARN MORE**](#)



Remember, your client's reality is often very different from yours. They don't understand the technological details as you do; one classic example of this has hit my business a few times. I'll spend too much time identifying the most cost-effective solution to a business need while knowing that a more complete solution would be better in the long run, although it's more expensive. When checking in with the client, his answer was blunt: "I didn't ask you to save me money: "I asked for the best solution." Always check your assumptions before proceeding.

CHANGE MANAGEMENT

The final thing that you must master in your customization task is change management. The tools should help you track the change history, but it will be your SOPs that document why the change occurred. Nearly every change you make should apply to an existing group of clients with a template in common. Just be certain you are not applying fewer settings to accommodate one client assigned to the template. A good rule to operate within is never to create a policy based on the exception. If an exception is required for a single client, they should be in their own template. However, an efficient MSP will rarely do this. Instead, it will work toward bringing all clients to a higher standard.

SUMMARY

In conclusion, mastering custom deployment, customization, and change management is crucial for MSPs to differentiate themselves in the market and provide value to their clients. By efficiently deploying custom configurations and maintaining standardized templates, MSPs can ensure that their clients' unique needs are met while maintaining operational efficiency. Effective time management, with a focus on customization over deployment, allows MSPs to spend the majority of their time on client-focused tasks, ultimately leading to higher client satisfaction and a stronger value proposition when you go to market.



HORNETSECURITY



CHAPTER 5

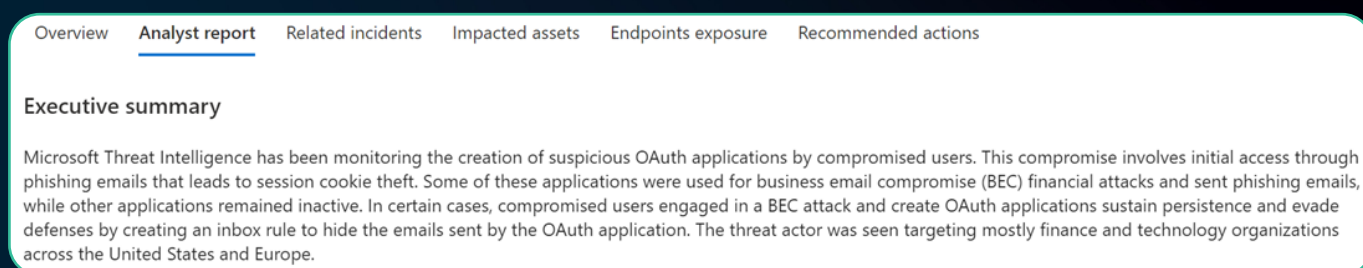
CYBERSECURITY

There is no greater topic today for MSPs and their clients than cybersecurity. Cybersecurity is worthy of an entire eBook of its own. There are numerous settings and ongoing maintenance required to stay ahead of cybercriminals and protect clients. In this chapter, we look less at the specific settings and more toward maintaining your efficiency and therefore profitability in the face of the rapidly changing cybersecurity landscape.

When considering how to protect the networks your MSP is responsible for, you must use the entire toolbox.

UNDERSTANDING VULNERABILITIES

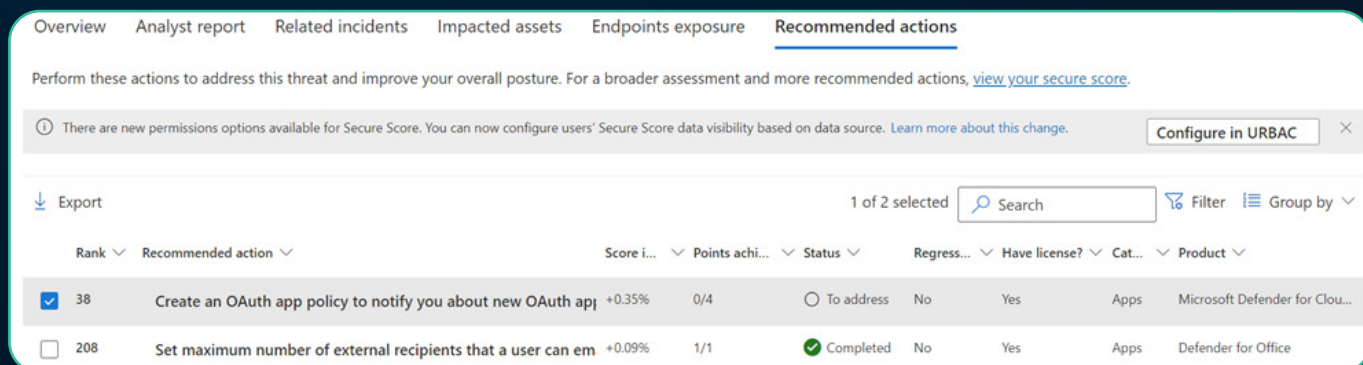
Microsoft provides Analyst Reports in the Threat Analytics area of Defender, offering a wealth of information produced by their threat analysts on how specific threats work. These reports are detailed yet easy to read, starting with an Executive summary and expanding on how the threat operates.



The screenshot shows the 'Analyst report' tab selected. The 'Executive summary' section contains the following text: 'Microsoft Threat Intelligence has been monitoring the creation of suspicious OAuth applications by compromised users. This compromise involves initial access through phishing emails that leads to session cookie theft. Some of these applications were used for business email compromise (BEC) financial attacks and sent phishing emails, while other applications remained inactive. In certain cases, compromised users engaged in a BEC attack and create OAuth applications sustain persistence and evade defenses by creating an inbox rule to hide the emails sent by the OAuth application. The threat actor was seen targeting mostly finance and technology organizations across the United States and Europe.'

Figure 11 Executive summary at the beginning of the detailed threat report


Across the tabs, you will find additional information about how this affects your specific tenant and the actions you can take to protect your network. Clicking on each uncompleted task will take you to the instructions for deploying the protection.



The screenshot shows the 'Recommended actions' tab. It displays a table of actions to be taken to address the threat. The table has columns for Rank, Recommended action, Score i..., Points achi..., Status, Regress..., Have license?, Cat..., and Product. Two actions are listed: 'Create an OAuth app policy to notify you about new OAuth app' (Rank 38, Status 'To address') and 'Set maximum number of external recipients that a user can em' (Rank 208, Status 'Completed').

Rank	Recommended action	Score i...	Points achi...	Status	Regress...	Have license?	Cat...	Product
38	Create an OAuth app policy to notify you about new OAuth app	+0.35%	0/4	To address	No	Yes	Apps	Microsoft Defender for Clou...
208	Set maximum number of external recipients that a user can em	+0.09%	1/1	Completed	No	Yes	Apps	Defender for Office

Figure 12 A checklist of actions you should take to protect your network from this cybercriminal



Make all your tenants secure, compliant, uniform

365  **MULTI-TENANT MANAGER FOR MSPs**

LEARN MORE

The Microsoft Defender portal also lists vulnerabilities not linked to specific threats – and there are a lot of them. Many are theoretically possible but not actively exploited. In the security recommendations list in **Figure 13**, red bugs indicate active exploits, while grey bugs indicate potential vulnerabilities. These active exploits may not have targeted your clients’ networks yet, but they are being used against others.







<input type="checkbox"/> Disable 'Enumerate administrator accounts on elevation'	Windows	1	
<input type="checkbox"/> Enable 'Require additional authentication at startup'	Windows	1	
<input type="checkbox"/> Disable 'Autoplay' for all drives	Windows	1	
<input type="checkbox"/> Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands'	Windows	1	
<input type="checkbox"/> Set LAN Manager authentication level to 'Send NTLMv2 response only. Refuse LM & NTLM'	Windows	1	
<input type="checkbox"/> Disable 'Allow Basic authentication' for WinRM Client	Windows	1	

Figure 13 Security recommendations by active exploit

By using these two tools, the efficient MSP can target their cybersecurity maintenance activities to vulnerabilities that are most likely to pose a threat to their clients.

When looking at the number of cyber vulnerabilities out there and the number of cybercriminals discovering new ways to enter networks, cybersecurity might seem like one of those vast problems that people shrug at and sigh out, “Well, you can’t boil the ocean.” This means that you’ll never get in front of cybersecurity. But by using the two tools described above, you can boil water for a cup of tea and sit down to the task of securing your clients’ networks.

BASELINES

Another tool available to help your MSP with cybersecurity efficiency is baselines. Microsoft provides security baselines for Windows, Edge, Windows 365, Defender for Endpoints, and Microsoft 365 apps.



Security Baselines	↑↓	Version
 Security Baseline for Windows 10 and later		Version 23H2
 Microsoft Defender for Endpoint Security Baseline		Version 24H1
 Security Baseline for Microsoft Edge		Version 117
 Windows 365 Security Baseline		Version 24H1
 Microsoft 365 Apps for Enterprise Security Baseline		Version 2306

Figure 14 Security baselines

You can use these baselines, but they are very strict and may be challenging for many businesses. Instead, the suggestion is to evaluate the setting in the baseline and create your own. Once you've done that, you'll have a standard that you can deploy across multiple tenants.

To do that though, you'll need a third-party tool like **Hornetsecurity's 365 Multi-Tenant Manager for MSPs** to assign your standards across the networks you're responsible for. The templating feature is very useful here.

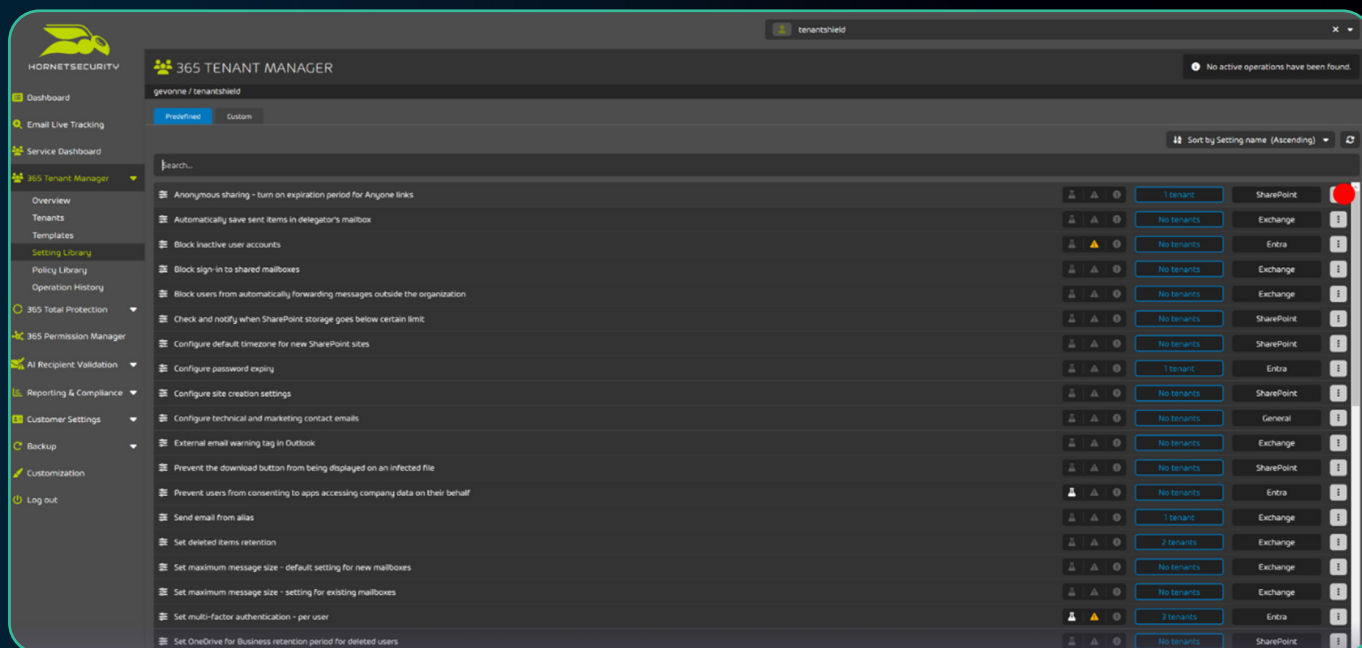


Figure 15 Hornetsecurity's Multi-Tenant Manager settings library

EMAIL SECURITY

Surprisingly, there's no baseline for email security. With the dramatic rise of business email compromise (BEC) as a vector for network infiltration you'd think that there might be. Instead, Microsoft has addressed this problem with preset email security policy templates within Defender for Business itself.

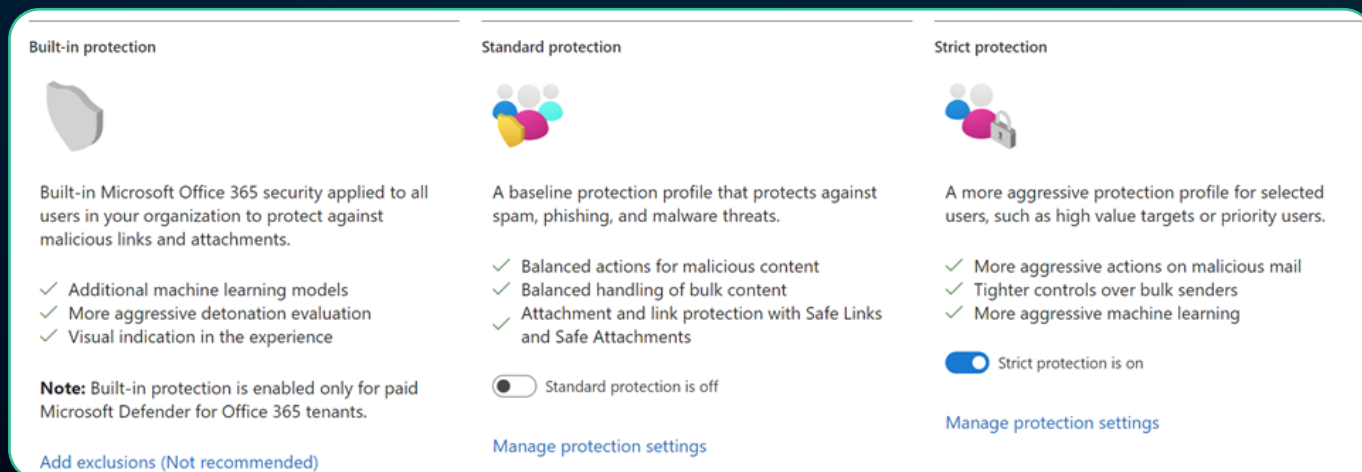


Figure 16 Email preset security policies

There's arguably no more important cybersecurity measure than a complete email solution. Cybercriminals are using phishing, spear phishing, QR code phishing, and other means of social engineering to take the first step into a network. Businesses today need to manage email with extreme caution. The ability to impersonate users, draft quality and compelling email content, and make fraudulent URLs appear legitimate has reached a pinnacle. The only way to combat it is with a complete email security program and some tolerance for false positives. Using the templates provided by Microsoft in combination with **Hornetsecurity's 365 Total Protection** is the way to accomplish this.

INTUNE AND CONDITIONAL ACCESS POLICIES

Intune, as discussed earlier in this eBook, is an excellent configuration tool. It pushes out your configurations and applications to devices in your network, providing fine-grained control over connected devices, which itself is a cybersecurity measure. With the addition of Entra Conditional Access rules, you can limit network use to devices that are joined to it! Can you imagine a world where cybercriminals decide to join a domain using the laptop they are working from? You can require that to happen using a Conditional Access (CA) policy, which says as soon as they achieve admin control, they either have to join or be blocked. Are they really going to join the domain? Another effective policy limits access to supported platforms. For example, if you don't use Linux, Mac, or even older Windows OS versions in your network, block them. You want to make it as difficult as possible for the cybercriminals to do their work.

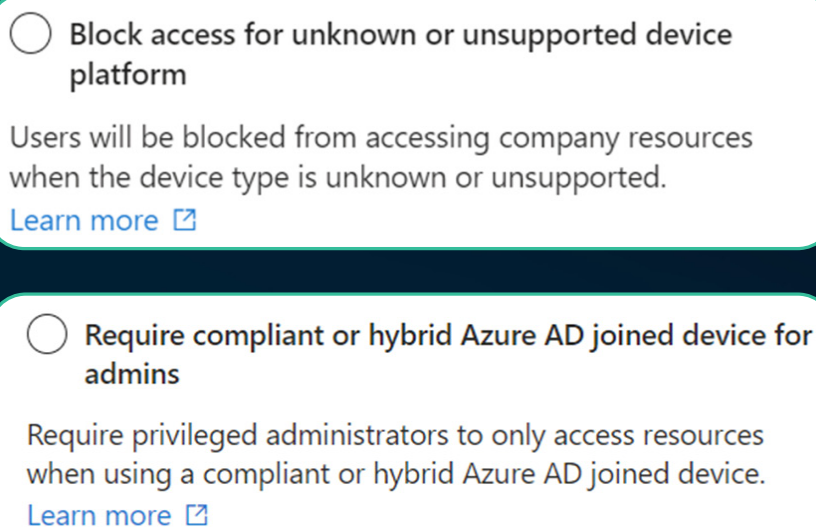


- 
- ☐ **Block access for unknown or unsupported device platform**
Users will be blocked from accessing company resources when the device type is unknown or unsupported.
[Learn more](#) 
 - ☐ **Require compliant or hybrid Azure AD joined device for admins**
Require privileged administrators to only access resources when using a compliant or hybrid Azure AD joined device.
[Learn more](#) 

Figure 17 Microsoft Entra conditional access rules

Advanced license packages of Microsoft 365 also include features like Risky User, Risky sign-in and Risky Device measurements that you can also add to your policies to allow only known safe users and devices to access the network.

Managing CA policies across all clients' tenants is vital, but doing it manually is time-consuming. Once again, Hornetsecurity's **365 Multi-Tenant Manager for MSPs** assists by handling the customization and deployment of CA policies at scale.

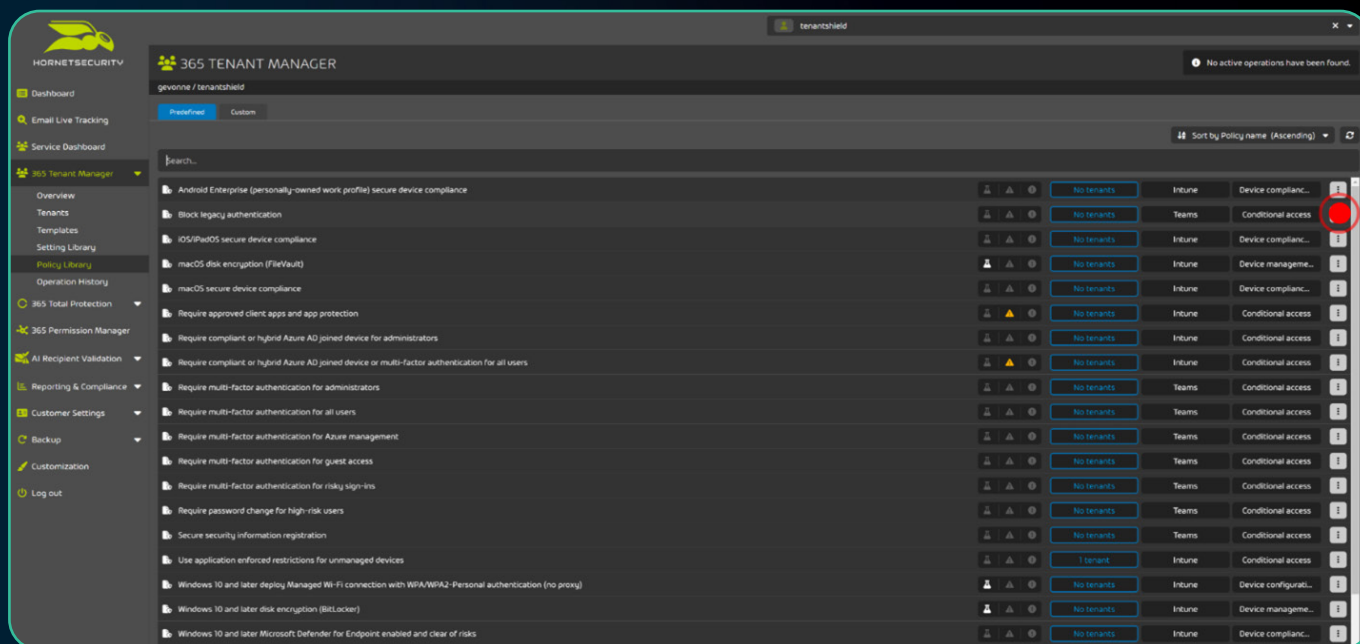


Figure 18 Conditional Access Policy library in Hornetsecurity Multi-Tenant Manager

AUTOPILOT, LIGHTHOUSE AND BACKUP

In addition to the tools that let you discover and set security configurations, you should also think of Autopilot, Lighthouse and a backup solution as part of your cybersecurity strategy. Autopilot allows you to positively identify devices that belong to your domain and gives you control over them from the out-of-box moment onward. Lighthouse allows you to manage some settings across clients if you're not using a third-party solution for that function. Backup provides business continuity if all else fails.

As discussed earlier, it's that business continuity piece that seems to have fallen from the offering of many MSPs. An easy-to-read dashboard that displays the backup status for all your tenants is an efficient way to watch the status of backups.

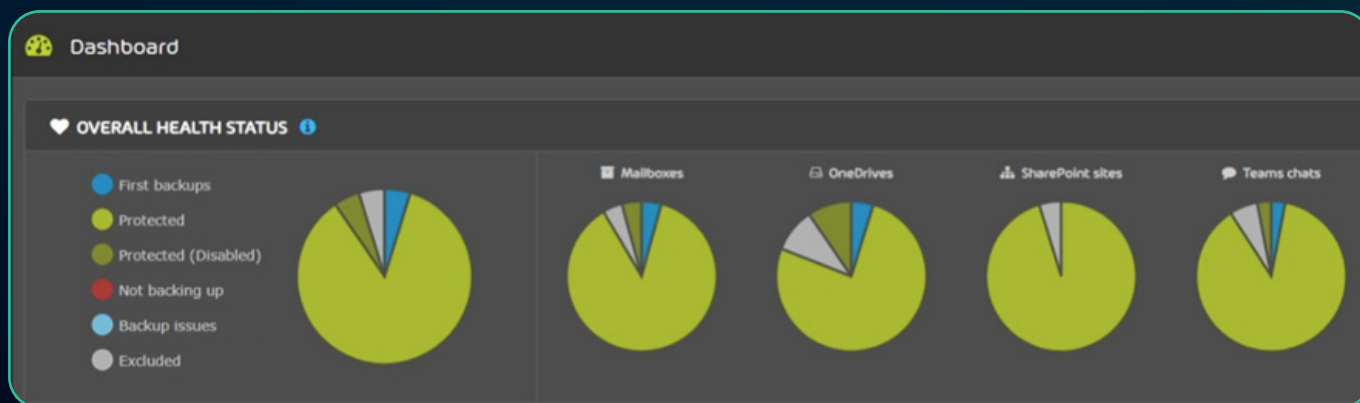
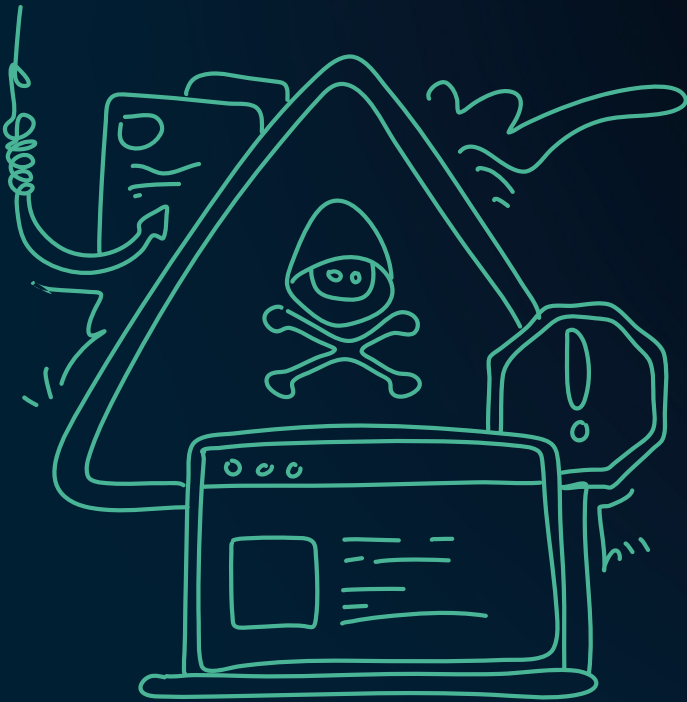


Figure 19 Backup status dashboard from Hornetsecurity Total Backup

To complete the business continuity process, your MSP should perform test restores at least quarterly to determine whether the backup is recoverable. A backup does not matter unless it can be successfully restored. It's a crazy thing, but there are a couple of truisms in IT. Printers and backups always fail. Taking your eyes off either of them is a bad idea.



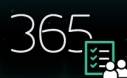
The key to managing cyber security for your clients is visibility. With a tuned system (such as Microsoft Sentinel, which I use with all my clients), I know within a few minutes if someone created a new Conditional Access policy, or added a new MFA method to their account, or was the victim of a MFA fatigue attack (so many prompts that the end user eventually just allows the prompt to make it stop). This near real-time visibility has allowed me to contain smaller incidents before they've progressed to larger breaches.

SUMMARY

To conclude this chapter on cybersecurity, it is essential to recognize that the landscape of cyber threats is constantly evolving. Small business-focused IT professionals must remain vigilant and proactive in their approach to cybersecurity. By leveraging the tools and strategies discussed in this chapter, IT professionals can effectively protect their clients' networks and data while remaining efficient and profitable. Remember, cybersecurity is not a one-time effort but an ongoing process that requires continuous learning and adaptation. Stay informed, stay prepared, and stay secure.



Make all your tenants secure,
compliant, uniform



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)



HORNETSECURITY



CHAPTER 6

VENDOR MANAGEMENT

There are several ways to decide how to manage vendors in your MSP. Should you seek many best-of-breed vendors or select a single vendor? The decision, on the face of it, seems easy; just choose between a single vendor or multiple vendors. But it's not that simple. Remembering that efficiency is your goal, there are many factors to consider. You must balance efficiency with providing a great solution to your clients. When presented with a complex decision, using a decision-making process like a decision table or SWOT is a good option. In this chapter, we explore both.

DECISION TABLE APPROACH

Many years ago, before cybersecurity became so complex and defense needs so comprehensive, I was on the side of best-of-breed. In those days, making that choice meant I had two vendors to manage. But I changed that opinion as the cybersecurity landscape altered due to the number of vendors that would have to be involved in a best-of-breed solution set today and the relatively minor differences between solutions as vendors in this space have matured.


FACTOR	SINGLE VENDOR APPROACH	BEST-OF-BREED APPROACH
Management Complexity	Simplified	Complex
Cost	Savings?	Higher Costs
Integration	Seamless	Challenging
Innovation	Limited?	High
Vendor Lock-in	High	Low?

Figure 20 Decision table


Making that decision was not simple because it meant compromise. The factors to be considered were management complexity, cost, integration, innovation, and, increasingly, vendor lock-in.

With the best-of-breed approach, complexity is always higher. You'll have multiple management portals to view and multiple vendors to pay, raising your MSP's overhead. Integration is, at best, challenging and usually not possible, and increasingly, you find yourself locked into long or difficult contracts. As an MSP, it's never easy to make a vendor change, but recently, vendors have made it even more difficult with onerous contractual language and terms.

In addition to these important considerations, you also have to wonder about the space between the products you've chosen from different vendors and where those boundaries are. You may often not know exactly where one vendor has chosen to stop their influence and another has started. You may unintentionally leave a gap when you use too many vendors.



Minimize resources for maximum profit

365 

MULTI-TENANT MANAGER FOR MSPs

LEARN MORE

SWOT APPROACH

A SWOT is a simple analysis of strengths, weaknesses, opportunities, and threats. It is a useful tool for many decision-making tasks. Using a SWOT can help you visualize the two approaches to cybersecurity vendor management.

SINGLE VENDOR SWOT

- **Strengths:** Simplified management, reduced complexity, consistent user experience, potential cost savings.
- **Weaknesses:** One size fits all, vendor lock-in, limited innovation.
- **Opportunities:** Streamlined operations, easier support.
- **Threats:** Dependency on a single vendor, potential gaps in security.

BEST-OF-BREED SWOT

- **Strengths:** Specialized expertise, flexibility, reduced vendor lock-in.
- **Weaknesses:** Complex management, higher costs, integration challenges.
- **Opportunities:** Access to cutting-edge technologies, tailored solutions.
- **Threats:** Increased complexity, unknown gaps between vendors.

A review of the literature on MSP vendor use showed that as many as 70 vendors were in play for the largest of MSPs and about 7 for the average MSP. However, it also showed a trend toward consolidation of vendors. Part of that is probably a result of the general trend toward consolidation in the vendor market in general, but some of it is a trend toward operational efficiency after recognizing that as an MSP, you simply can't manage many vendors nor train your staff on so many solutions. The ever-growing complexity of cybersecurity means you need to consolidate your efforts and make a choice.

While you'll never get down to a single vendor, it may make sense to adopt two as your standard, with Microsoft being one of them. Microsoft has increasingly invested in security and integrated its security products into the Microsoft 365 suites. It makes sense to use them. However, their enterprise approach means that much of it is designed for security teams with segmented specializations. The typical MSP is small and staffed with security generalists who must be familiar with the entire breadth of cybersecurity. This is not Microsoft's strong suit. A second vendor is warranted to fill those gaps. Remember, though, that it is important to pick an integrated **security suite of tools** to minimize the challenges of deploying and managing separate tools.

MULTI-TENANT MANAGEMENT WITH MULTIPLE VENDORS

A vendor like Hornetsecurity can help fill the spaces that Microsoft has left. For example, Microsoft doesn't offer a comprehensive backup solution for Microsoft 365. Increasingly, there are fewer gaps for vendors to fill, but one that will always remain is multi-tenant management.

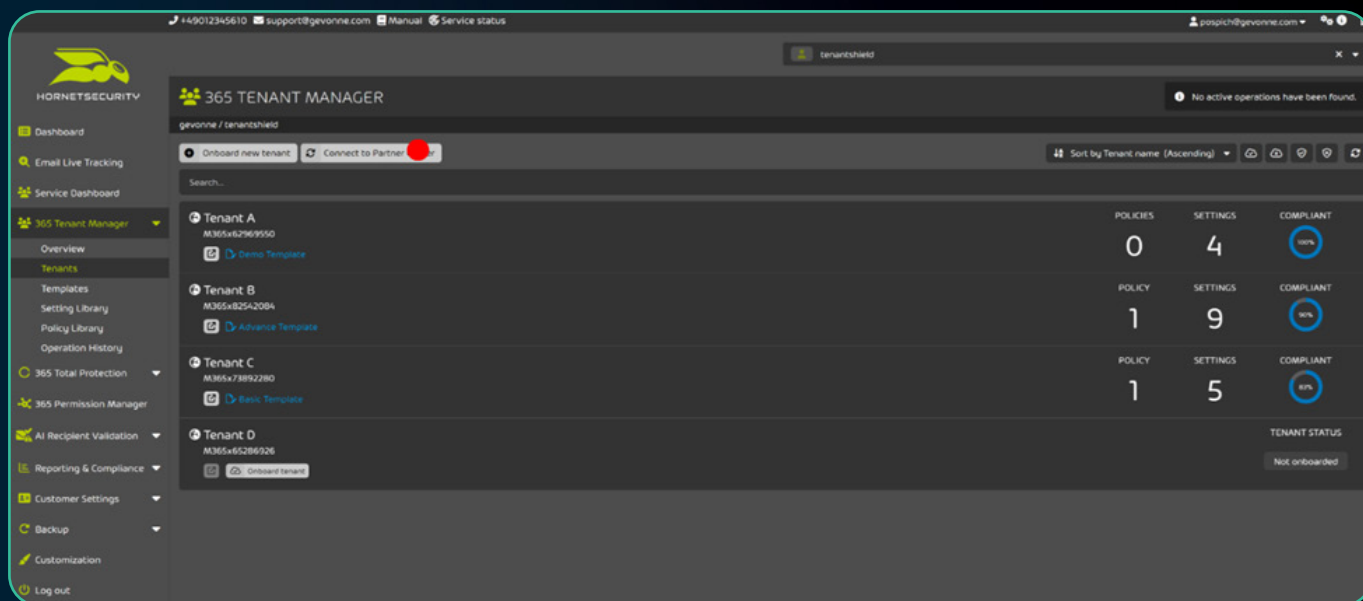


Figure 21 Onboarding tenants into Hornetsecurity Multi-Tenant Manager

While Microsoft has recently begun to add multi-tenant management to some of its products, like Defender XDR, it has placed limitations that seem arbitrary until you consider its perspective. Remembering that Microsoft builds solutions for the enterprise, they place a 50-tenant limitation on the Defender multi-tenant portal. This might make sense if you are an enterprise with multiple tenants. Many do have them for different lines of business or as a result of acquisitions. However, for the MSP, 50 tenants are not very many.



Some of our clients also have multiple tenants that they acquired through acquisition. In my 7-person MSP, we cared for 80 clients, which is already over the 50-tenant limit that Defenders' multi-tenant solution offers. So, while we prefer to use Defender XDR as a security solution, we need a different management system, because Microsoft's recommendation that we prioritize some clients over others is unacceptable. With an eye to efficiency and to bringing equal levels of service to the managed tenants, we need to engage another solution like Hornetsecurity's **365 Multi-Tenant Manager for MSPs**.

ADDITIONAL CONSIDERATIONS

Simplifying vendor management frees up your MSP to focus on delivering higher-level services, such as virtual Chief Information Officer (vCIO) or Chief Information Security Officer (CISO) engagements. This shift allows your MSP to provide strategic guidance, align cybersecurity initiatives with business goals, and obtain a competitive advantage. Clients value visible services more highly, and tangible outcomes like an improved security posture, regulatory compliance, and reduced risk lead to greater client satisfaction and loyalty. As an MSP, moving up the ladder of cybersecurity professionalism means higher profits, increased revenue streams, and more valued engagements with clients. By focusing on strategic services, your MSP can achieve sustainable business growth and capitalize on industry trends that demand higher-level services.

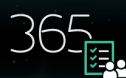
SUMMARY

In conclusion, managing vendors in an MSP environment requires a careful balance between efficiency and providing high-quality solutions to clients. The decision between a single vendor and a best-of-breed approach is not straightforward and involves considering factors such as management complexity, cost, integration, innovation, and vendor lock-in. While a single - vendor approach offers simplified management and potential cost savings, it may lead to vendor lock-in and limited innovation. On the other hand, a best-of-breed approach provides specialized expertise and flexibility but comes with higher management complexity and costs. Ultimately, the choice depends on the specific needs and goals of the MSP, and a thoughtful decision-making process, such as using a decision table or SWOT analysis, can help in making the best choice. By efficiently managing vendor relationships, MSPs can focus on delivering higher-level services and achieving sustainable business growth.

These frequently overlooked elements hold significant value for both the client and the MSP, highlighting the advantages of efficiently managing your vendor relationships.



Minimize resources for
maximum profit



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)



HORNETSECURITY



CHAPTER 7

CONCLUSION

This eBook covered five significant factors that drive an efficient MSP operation: Onboarding, Monitoring and Maintenance, Customization, Managing Cybersecurity, and Vendor Management. We examined these major areas of MSP operations, pointed out where efficiencies can be gained, and suggested ways to obtain them.

Here's what we learned.

EFFICIENT ONBOARDING

To achieve efficiency in onboarding, we must accomplish the following four tasks:



Figure 22 Efficient onboarding

Utilizing included and third-party tools to minimize the time required to complete these tasks is critical, but it has to be balanced with client service expectations and provide a great experience for the customer. Striking that balance will pay dividends long into the client relationship. In this section, we broke down the differences in the client's and MSP's viewpoints. Know that those differences don't just exist in this phase of the client relationship but through every aspect.

MONITORING AND MAINTENANCE

We explored aspects of MSP efficiency in monitoring and maintenance activities. We dove into the importance of proactive maintenance, the role of automated monitoring, the criticalness of incident response procedure and disaster recovery planning, and the need to balance efficiency with human expertise. There's a real need to automate in this area but we can't lose sight of the client relationship as we do.

Here again, we have an opportunity to automate and delight the client at the same time. So much of the work that an MSP does on a routine basis is invisible to the client. The MSP's helpdesk staff is their front door and a key component of how the client will view their services. Being friendly and efficient is key.

By implementing effective procedures and plans, MSPs can enhance their performance, reduce stress, and achieve greater profitability.

CUSTOMIZATION

Mastering customization and change management is crucial for MSPs to differentiate themselves in the market and provide value to their clients. By efficiently deploying custom configurations and maintaining standardized templates, MSPs can ensure that their clients' unique needs are met while maintaining operational efficiency. Effective time management, with a focus on customization over deployment, allows MSPs to spend the majority of their time on client-focused tasks, ultimately leading to higher client satisfaction and a stronger market presence. In addition, mastering efficiency in this area could allow the MSP to begin to specialize in particular verticals or regulatory requirements, thereby further increasing efficiency and profitability.

MANAGING CYBERSECURITY

It is essential to recognize that the landscape of cyber threats is constantly evolving. Small business-focused MSPs must remain vigilant and proactive in their approach to cybersecurity. By leveraging the tools and strategies discussed in this chapter, the MSP can effectively protect its clients' networks and data while remaining efficient and profitable.

Remember, cybersecurity is not a one-time effort but an ongoing process that requires continuous learning and adaptation. In this way, managing cybersecurity is not so different from monitoring and maintenance when it comes to efficiency and will be a feeder into new standards. It does require that the MSP have some higher-skilled staff to stay informed, stay prepared, and stay secure.

VENDOR MANAGEMENT

In the quickly changing business landscape that MSPs have found themselves subject to, many have experienced vendor sprawl as they added vendors to try to keep up with the rate of change. Reevaluating those decisions with an eye toward efficiency is an important task, and two methods, a SWOT and a decision table, are suggested to help with that analysis.

Simplifying vendor management frees the MSP to focus on delivering higher-level services, such as v CIO or CISO engagements. This shift allows MSPs to provide strategic guidance, align cybersecurity initiatives with business goals, and offer a competitive advantage. Clients value visible services more highly, and tangible outcomes like an improved security posture, compliance with regulations, and reduced risk lead to greater client satisfaction and loyalty. Moving up the ladder of cybersecurity professionalism means higher profits, increased revenue streams, and more valued client engagements. By focusing on strategic services, MSPs can achieve sustainable business growth and capitalize on industry trends that demand these more profitable, higher-level services.



 AUTOMATE.
 STANDARDIZE.
 GOVERN.

 365  MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)



LAST WORDS

If an MSP business owner and technical staff can learn to master the five areas that we explored, success will follow. The MSP plays a vital role in the success of all businesses in every economy around the world. Few businesses are large enough to employ their own IT department with the breadth of skill set the MSP can bring. The enormity of the market that an efficient MSP can serve makes the opportunity nearly limitless. When an MSP is successful, everyone wins, and efficiency will bring that success.



365 MULTI-TENANT MANAGER FOR MSPs

 AUTOMATE  STANDARDIZE  GOVERN

Managing M365 tenants is a resource-hogging task, with service providers spending several hours trying to juggle multiple admin portals to configure their customers. Configuring M365 tenants is a highly detailed and complex task, and simply knowing how to configure them isn't enough – service providers must also maintain tight security and keep risks at bay. Multiply all this across diverse tenant needs for different customers, and the problem very quickly grows into a mountain that can be overwhelming.

MANAGING MICROSOFT 365 TENANTS MADE AS EASY AS IT GETS

What is affected?

How does 365 Multi-Tenant Manager for MSPs help you?

What improves?



All Microsoft
365 tenants



Automate

Automatic discovery
of M365 tenants
leveraging Microsoft
Partner Center
connection.



Standardize

Out-of-the-box
templates, settings,
and policies with the
flexibility to fully
customize your own
configurations.



Govern

Detailed dashboarding
for comprehensive
analysis and call to
action for all
managed tenants.



Effortless
management,
governance, and
compliance for all
M365 tenants.



365 MULTI-TENANT MANAGER FOR MSPs

365 MULTI-TENANT MANAGER FOR MSPS FEATURES

Automatic discovery of M365 tenants leveraging Microsoft Partner Center connection, to facilitate the provisioning and streamlining of services.

Elimination of managing multiple Microsoft portals. With 365 Multi-Tenant Manager for MSPs, **a tenant can be managed from one consolidated solution through a single pane of glass.**

Simplification and standardization of otherwise complex workflows and inter-portal dependencies in Microsoft Azure/M365 administration.

User-friendly wizards that guide service providers from tenant onboarding to tenant configuration, customization, and monitoring of automated tasks.

Out-of-the-box settings, policies and templates that every organization can quickly adopt.

Built-in toolbox support for creation of custom settings and policies, and importing of tenant policies, ensuring that MSPs can meet each customer's unique needs within their M365 tenant.

Automatic remediation and enforcement when non-compliance is detected.

Extensive dashboards for monitoring and reporting purposes.

Detailed dashboarding functionality for **comprehensive analysis and call to action** for all managed tenants and their compliance states.



-  AUTOMATE.
-  STANDARDIZE.
-  GOVERN.



MULTI-TENANT
MANAGER FOR MSPs

[LEARN MORE](#)