Ontinue

Microsoft Security

eBOOK

How to Get More out of Microsoft 365 Defender

Modern security challenges demand a properly configured, consolidated toolset

Contributors:

Dean Ellerby,
Microsoft MVP in Security

Charlie Gough,
Microsoft MVP in Security

With cyberattacks increasing in sophistication and complexity, organizations are under constant and growing pressure to defend against threats. Coupling this with a global shortage of cybersecurity professionals means businesses are often on the back foot: Two steps behind the adversary and one step away from becoming the next high–profile organization to be compromised.

As the global workforce continues embracing flexibility given that hybrid work is here to stay, organizations are also facing the need to rethink cybersecurity defense, with the tenets of zero trust at its core. Yet, with budgets being stretched, cybersecurity leaders must ensure their investment in toolsets still allow them to achieve the goal of simplifying their operations. At the same time, CISOs need real-time visibility, collaboration across their environment, and the ability to respond to threats at speed.

Eliminating tool sprawl with a comprehensive solution

Given the sprawl of cybersecurity tools in market, the most common approach in buying and managing security tech stacks has been to buy the best tool in each area and attempt to integrate them. While there's an argument to be made for purpose-built, best-of-breed tools, if they're not deployed and configured as an integrated whole — or can't be integrated effectively — they can result in a less-than-effective security program.

When security tools can't communicate with other tools deployed within an environment, it can create what we call **vulnerability in depth**. The tools in place may each be outstanding on their own, but when they're ineffectively integrated with the broader security toolset, the result can expose attack surfaces that attackers find and exploit.

Identity and endpoint security are two key pillars that SecOps teams must prioritize in modern security. However, as tool sprawl reaches a critical mass, there is a third pillar emerging, and that is the interoperability of your security tools.

Without a fully integrated security toolset where each tool seamlessly communicates with the others, organizations can inadvertently create risk when adopting best-of-breed products. More and more, organizations are recognizing this difficulty, and single-vendor security platforms are increasing in popularity as a result. Comprehensive security platforms have integration and interoperability built in, and therefore don't have the same potential to create gaps as multi-vendor point solutions.

For this reason, Microsoft Security has become an increasingly popular choice of many organizations. At the same time, Microsoft's dedication to investing in its security portfolio to the tune of about $4 billion per year has led to its products outperforming competitors in third-party evaluations like MITRE ATT&CK, and analyst assessments like Gartner's Magic Quadrant.

The benefits of consolidating on Microsoft 365 E5 and Microsoft 365 Defender

A significant challenge for any organization is visibility. If you don't have built-in visibility across all the sources and toolsets within your security stack, it's difficult, or even impossible, to unify. The Microsoft Security portfolio of products is integrated natively, so cross-product communication is seamless, creating a comprehensive security platform that's even more secure.

With the Microsoft Security portfolio covering identity, endpoints, and interoperability at its core, as well as a market-leading cloud access security broker (CASB), threat and vulnerability management (TVM), and more, Microsoft 365 Defender covers all bases.

When evaluating any technology solution, it's important to understand both the cost-effectiveness and scalability. With a Microsoft 365 Enterprise E5 license, the sheer breadth of capability across the toolsets is impressive. E5 gives organizations access to advanced collaboration, calling and reporting, as well as next-level security capabilities.

While Microsoft 365 Enterprise E5 comes at an additional premium to Microsoft 365 Enterprise E3, it's the sensible choice for organizations that would otherwise buy these capabilities from multiple competing vendors. The math alone makes it a compelling investment. But multiple toolsets also present a supply chain risk, through attacks such as those involved in Solar Winds and others over the years involving malicious codes creating backdoors. There's a wider breadth of vulnerability to keep patched across the estate. But that's one less thing to worry about with consolidating on the Microsoft Security product portfolio. Every vendor poses some level of risk, so the more vendors in your security stack, the more you're increasing your risk.

No vendor can be 100% risk-free; the key is having the visibility and ability to quickly operationalize remediation, so you can quickly act on any insights or attacks. Microsoft is not only the largest investor in the cybersecurity space, but their solutions have earned recognition from analyst firms, as well.

When it comes to scalability, the fact that Microsoft 365 takes advantage of the Microsoft cloud ensures scalability is built in. Purchase Microsoft 365 Enterprise E5 for 300 users or 300,000 users, and the experience, capabilities and approach are the same.

While Microsoft 365 Enterprise E5 comes at an additional premium to Microsoft 365 Enterprise E3, it's the sensible choice for organizations that would otherwise buy these capabilities from multiple competing vendors. The math alone makes it a compelling investment.

But while the Microsoft Security portfolio of natively integrated products offers its customers a distinct advantage and avoids the vulnerability-in-depth dangers of multiple point solutions, proper deployment and configuration remain key to deriving the greatest value from your investment.

Configuration is key to making the most of Microsoft 365 Defender

The endpoint is often considered the initial attack surface. From trojans to ransomware, malicious software aims to infiltrate, damage or hijack systems. Microsoft Defender for Endpoint is the answer to such threats. By constantly monitoring endpoints, Defender for Endpoint can detect and isolate ransomware attempts, interrupt data exfiltration, and block attackers in real-time, at machine speed.

Defender for Endpoint is only part of the equation, however. Microsoft 365 Defender is a unified defense portfolio of products that provides protection across endpoints, identities, email and applications.

For example, phishing remains one of the most prevalent cybersecurity threats in today's threat landscape. Microsoft Defender for Office is at the forefront of this battle, offering an advanced email filtering system that actively scans for phishing, eliminating many of these threats before they reach an employee's inbox. On the rare occasions that malicious emails evade the initial screenings, Microsoft Defender for Office can automatically purge these threats as soon as they're detected.

Microsoft 365 Defender is a unified defense portfolio of products that provides protection across endpoints, identities, email and applications.

It isn't just about the tooling, however.

Protection from Microsoft 365 Defender is only as good as its implementation. But what does 'the right security configuration' look like?

This depends entirely on the environment being protected and the use cases in play. In particular, policies are worth paying attention to. Policies need to be developed correctly and as part of a holistic comprehensive plan to avoid conflicts, so be mindful of the approach you're taking. At a fundamental level, pay attention to your naming convention, and update the names of policies after you put them into use: it's all too common for organizations to get to a point that they have dozens of policies labelled "test."

If we look at Attack Surface Reduction (ASR) for example, there is a broad range of categories to configure for Defender for Endpoint and Defender for Servers. Each of these contain multiple crucial items that have an impact across the environment, including:

- application control
- controlled folder access
- network protection
- exploit protection

Organizations need to be sure the right configuration is in place across the entire estate — and test as you go. You can configure ASR rules in audit mode prior to enabling them; this allows you to test the rules and have a record of what will happen when you fully enable them. As Microsoft releases new features and configurations, those configurations may change. As with any other platform, organizations need to monitor and maintain Defender tools to ensure optimal protection.

Common misconceptions about the Microsoft Security product portfolio

While Microsoft 365 Enterprise E5 includes a broad array of security tools, they are rarely implemented to their fullest. Underutilization is rampant and typically caused by a lack of in-house expertise and limited awareness of the extensive capabilities, offering major opportunities for companies using the Microsoft Security product portfolio to consolidate their security portfolio, reduce complexities and increase visibility.

MFA is a powerful tool — if it's implemented effectively

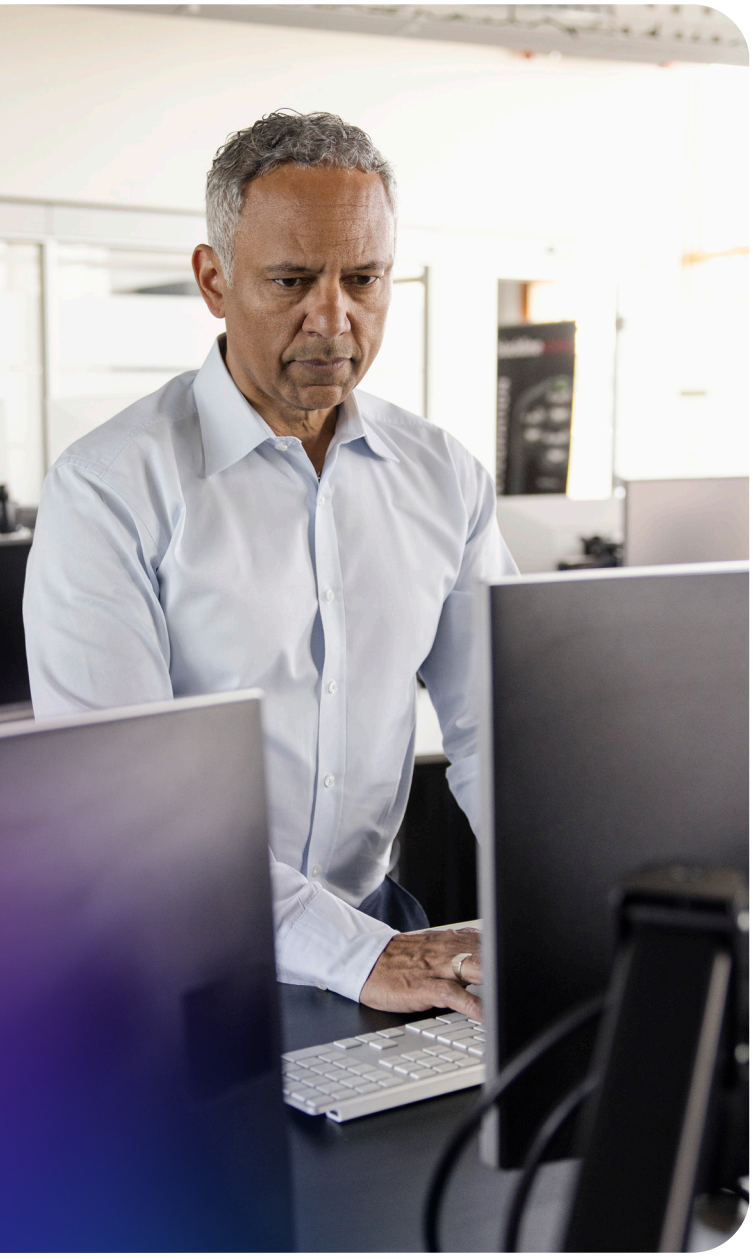
With good reason, multi-factor authentication is considered a best practice in identity and access control. And while many have enabled MFA for their users, some organizations focus on legacy "per-user" MFA. This approach prompts for authentication on a regular basis, which risks authentication fatigue, leading to workarounds and shortcuts and, ultimately, greater risk.

Microsoft Entra ID allows organizations to control app and data access through fine-grained Conditional Access policies. By leveraging Conditional Access, organizations can require users to require additional authentication steps only when accessing apps from a non-compliant device, such as from a personal phone or laptop. For example, if a user logs

in through an outside device, Conditional Access could require they go through multi-factor authentication and re-authenticate every hour, whereas if they logged in with a registered and compliant device, these steps wouldn't be required. When configured correctly, this reduces both the friction users face and the risk — without sacrificing identity security.

Microsoft 365 Defender: More than just endpoint security

A common misconception is that Defender for Endpoint is just an antivirus (AV) or an endpoint detection and response (EDR). But Microsoft 365 Defender offers far more than that protection — it also includes threat and vulnerability management, AV, and attack surface reduction, among others.



For endpoints, we often see organizations seeking feature parity between Microsoft Defender for Endpoint and its alternative third-party XDRs. This is especially true when considering a migration to the Microsoft platform.

But Defender for Endpoint should be looked at as a small (but key) part of Microsoft 365 Defender, which includes a whole suite of protections and controls. Where a traditional EDR must do all protection at the endpoint itself, Microsoft 365 Defender can protect across the whole ecosystem — endpoint, identity, cloud apps, and more, creating a true defense-in-depth posture. While Defender for Endpoint is the EDR, it seamlessly leverages the rest of the Microsoft 365 Defender platform to become a robust XDR comparable or superior to best-in-breed products.

Pay attention to the Microsoft Secure Score

Many organizations make the mistake of overlooking their Secure Score or not checking it regularly. Microsoft Secure Score is an enterprise-wide view into your organization's security posture across your entire digital estate. Even more than that, Microsoft Secure Score provides opportunities to improve your security posture, through actionable insights and recommendations.

Within the Secure Score page, you'll find a tab with recommended improvement actions that are most impactful to the score, listed in order of greatest impact. Check your Secure Score and the recommended improvements often. And when evaluating MDR providers, ask how often they make proactive hardening recommendations that will help you improve.

Don't let perfect be the enemy of the good

Sometimes, fully deploying a particular feature across your entire organization is difficult or impossible. As a result, many organizations put off adopting those features. In some scenarios, you'll still recognize significant benefits by deploying these features across the segments of your organizations where deployment is possible.

For example, we see many organizations who hesitate to adopt application control, because with certain groups (finance or security, for example) it's difficult or impossible to roll out because of features like Excel Macros and add-ins that can bring resistance and complexity. But other groups — such as HR, sales, operational staff, front-line workers — could benefit significantly from the protection of this feature. Critically evaluate areas where partial rollouts yield greater benefits than not adopting at all.

Microsoft 365 Defender Optimization Checklist

Based on Ontinue's experience in onboarding organizations who are also Microsoft 365 Defender customers, we offer the following recommendations in optimizing your implementation.

- [x] **Maintain the exclusions**
  Don't just copy exclusions from your old AV and leave the exclusions in place. If you exclude something, document the reason, in case you or anyone on your team need to review it.

- [x] **Don't leave ASR rules in audit mode**
  Leaving ASR rules in audit mode for longer than a few weeks doesn't actually protect you. They don't block malicious activities, they're just auditing. Know when to use audit mode and when not to — and for how long.

- [x] **Check your role-based access controls (RBAC)**
  If you don't check your role-based access controls from time to time, you could be granting access to the most privileged machines in your environment without knowing it. This is especially true if you just keep to the standard settings. Having good RBAC policies in place within Defender allows you to control who has access to what. And it's simply good governance. You could have someone with security admin rights, but you may not want them to have full control of domain controllers and the like.

- [x] **Allocate time for maintenance**
  Keep up to date with the configurations within the Microsoft Security product portfolio. Once you set them, they require maintenance. Don't think of Defender as just another AV tool. Sure, back in the day you'd install across the estate and only touch it when a new version came out to update the definitions — in those days, you wouldn't need to actively review policies, or exclusions. But with today's continually evolving threat landscape, Microsoft is constantly adding features and you need to keep your tools updated.

- [x] **Review alerts/incidents**
  Your tools may generate many alerts each day, and it's easy to fall behind in reviewing, investigating, and responding to them or closing them. Consider alerts in context of other alerts — that's easy because in Microsoft 365 Defender alerts from multiple Defender products are all rolled up together within incidents.

- [x] **Get the most out of your license**
  Don't neglect the full value of the Microsoft Security portfolio of products. The products and features included in a Microsoft 365 Enterprise E5 license are broad and deep. Far too often, organizations underutilize what they're paying for. The reality is that there is a tool for just about every security use case within the E5 license, so take the time to understand what you're paying for and form a plan to make the most of it.

Partnering with an MDR service provider who understands your environment

Managing day-to-day SecOps is challenging, even under perfect conditions. Even with a big budget, a full team, and all the right tools properly configured and deployed, organizations are still playing catch-up with adversaries whose tools and tactics evolve continually.

But far too often, security teams are operating under far less than ideal conditions. Budget constraints, the cybersecurity talent gap, and the alert fatigue caused by tool sprawl leave most security teams scrambling to keep up with alerts. Few have the time to proactively harden their posture and improve their security.

The trend in recent years has been to outsource day-to-day security operations to a managed security services provider (MSSP) or managed detection and response (MDR) provider. The reasons for this are obvious. These vendors have deeper benches, greater security knowledge, and can significantly help overburdened teams.

But it's critical that organizations evaluate potential MDR providers on a deep level to ensure that the provider can tailor their services to each organization and deliver truly localized service at scale. Without this capability, an MDR service can simply become yet another portal the team needs to manage, rather than a true security partner.

About the Contributors

Dean Ellerby, Senior Cloud Security Architect, Ontinue
Dean Ellerby is a Senior Cloud Security Architect with Ontinue Consulting, a dual Microsoft MVP, Microsoft Certified Trainer, and experienced creator on YouTube and Pluralsight Author. Having created hundreds of in-depth training videos on his YouTube channel and recognized by Microsoft for his work within the community, Dean is considered a thought leader in Security and Endpoint Management.

Charlie Gough, Senior Cloud Security Architect, Ontinue
Charlie Gough is a Senior Cloud Security Architect with Ontinue Consulting, a Microsoft MVP and a Microsoft Certified Trainer. Charlie is responsible for designing and implementing cloud security solutions for clients' systems and data, customized to meet specific security requirements. He advises clients on security best practices for securing cloud environments, including identifying potential vulnerabilities, implementing security controls, and ensuring regulatory compliance. Charlie is a thought leader in the areas of security, identity, and access management.

How to Evaluate an MDR Service Provider

To understand how much an MDR service provider can truly tailor their services to your organization, you should evaluate a potential vendor based on their ability to:

Localize the MDR service to your organization
One size does not fit all. Make sure the MDR provider you partner with explains how they learn about your environment, your workflows (including processes like escalation matrices and rules of engagement), and your risks. Ask how they can specifically tailor their service to your organization.

Meet you where you are
Collaborating is critical to security success. Your MDR provider should look, feel and act like an extension of your security team. Make sure you understand how your MDR provider will communicate with you, and vice versa. Ideally, they should use the same real-time collaboration tools you do, so communication is fast.

Know your tools
You've made an investment in the Microsoft Security portfolio, so your MDR provider must be an expert in deploying, configuring and managing those tools. The right MDR provider will help you get the most out of them, providing real-time visibility and the ability to act on that information fast.

Use AI and automation to enable experts
Understand how your MDR provider uses AI and automation, what use cases these tools are applied to, how data is managed, and exactly what benefits they provide. Responsible use of AI and automation to maximize what human expertise can deliver is key.

Ontinue ION: AI-Powered MXDR for Microsoft 365 Defender customers

Ontinue ION is the AI-powered managed extended detection and response (MXDR) service designed and built specifically for Microsoft customers. Combining artificial intelligence with human expertise to better understand our customers' environments, workflows and risks, Ontinue tailors our service to each customer's needs and business objectives, allowing us to operationalize security operations more fully on their behalf. Delivering across the entire security lifecycle, Ontinue goes beyond detection and response, helping our customers proactively harden their environments and reduce risk by delivering best practice guidance for using and configuring their existing Microsoft tools.

As a proud member of Microsoft Intelligent Security Association (MISA), Ontinue is an important partner for many Microsoft customers. With our expertise and support, our customers are able to realize the true value of their investment, increasing the depth and success of their adoption of Microsoft Security solutions.

Tour Ontinue ION MXDR Platform

If you need to ensure your organization gets the most from your investment in Microsoft Security products, take our self-guided tour to see how the Ontinue ION platform can help.

TAKE THE TOUR | CONTACT US | REQUEST A DEMO

Ontinue

Ontinue, a leading provider of AI-powered managed extended detection and response (MXDR) service, combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.