eBOOK

4 Benefits of an MXDR Built for Microsoft Security

Today's CISOs and their teams are protecting highly distributed and dynamic organizations, and so they face multi-faceted cybersecurity challenges—from complex environments to myriad tools that generate overwhelming alert noise. This makes it difficult to understand where the greatest risk is and where coverage gaps exist in the security posture. Security teams seldom have a clear picture of where business-critical assets reside, what those assets are connected to, and who owns them.

The standard practice is to deploy numerous siloed and specialized tools, stitching them together to get visibility and control across these environments. However, this approach creates further operational challenges because these tools must be continuously configured, maintained, and tuned to yield actionable security insights. And the additional complexity of myriad tools can create its own vulnerabilities, as security teams can struggle to identify and seal the gaps between those tools.

Adding to the challenge, the insights generated by these tools are often buried in a deluge of alert noise. Without a large team of skilled security analysts to help find the needles in the haystack, many threats are missed, response and remediation is delayed, and potential damage and costs increase.

Forward-thinking companies are already using the Microsoft technology stack—from Azure to server and desktop operating systems to business and office productivity software and more—to support their business operations and digital transformation initiatives. Complementing this stack with Microsoft security offerings is a natural fit, since it delivers native integration and often cost benefits.

The Microsoft security stack can then serve as the multi-device, multi-cloud control plane that can be deployed across heterogenous distributed environments to consolidate your existing security technology stack.

Microsoft is committed to security and has demonstrated its leadership as a security vendor with its continued investments in this space and a strong partner ecosystem to provide managed detection and response (MDR) services.

> Microsoft is committed to security and has demonstrated its leadership as a security vendor with its continued investments in this space and a strong partner ecosystem to provide managed detection and response (MDR) services.

Take a Closer Look at the Microsoft Security Stack

The Microsoft security stack offers a comprehensive suite of solutions that are natively integrated with Microsoft solutions and deliver advanced security capabilities to protect modern enterprises, including:

- **Defender for Identity.** A cloud-based security solution that identifies, detects, and investigates advanced threats, compromised identities, and suspicious user activities leveraging signals from your on-premises Active Directory (AD) domain controllers and member servers.
- **Defender for Office 365.** A cloud-based email filtering service that helps protect your organization against advanced email threats. Defender for Office 365 builds on the core protection offered in Exchange Online Protection (EOP) and provides investigation, hunting, and remediation capabilities to help organizations identify, prioritize, investigate, and respond to threats.

- **Defender for Endpoint.** An enterprise endpoint detection and response (EDR) solution that uses built-in Windows capabilities and Microsoft cloud services, including endpoint behavioral sensors, cloud security analytics, and threat intelligence. It leverages deep integration with the entire Microsoft security stack.
- **Defender for Cloud Apps.** A cloud access security broker (CASB) solution that enables visibility, control, and deep insights across all your cloud services. Defender for Cloud Apps provides native integration with Azure Active Directory (Azure AD) Conditional Access, which minimizes end-user impact while ensuring the appropriate level of control based on risk-based conditions such as device state, user, cloud app, location, and network.
- **Azure AD Identity Protection.** A Microsoft security tool that allows organizations to automate detection and remediation of identity-based risks, investigate risks, and export risk detection data to Microsoft Sentinel and other security information and event management (SIEM) platforms.
- **Microsoft Sentinel.** A cloud-native SIEM and security orchestration, automation, and response (SOAR) solution that leverages artificial intelligence (AI), machine learning (ML), a comprehensive set of out-of-the box connectors, and advanced analytics to link massive amounts of threat intelligence and security data and deliver unparalleled threat protection and detection. All the tools in the Microsoft security stack work together to pull in enormous amounts of data, enabling analysis of user behavior in context. The stack then correlates this data in real time to see things such as when a user connects from an IP address they'd never used before and is doing suspicious things on the network.

Microsoft Sentinel is an innovative SIEM platform built for a multi-cloud world. It connects to and collects data from all Microsoft customer sources including users, applications, servers, and devices running on-premises or in any cloud.

Sentinel addresses the problem of too many alerts by using machine learning and other technologies to separate signal from noise. It uses these technologies to examine vast quantities of low-level data and connect the dots with behavioral analysis to see sophisticated "low and slow" threats. The result is that resource-constrained incident response teams receive alerts for only the most credible threats—that is, the ones that matter. However, all of this doesn't just happen automatically. The machine learning algorithms need to be tuned to the environment. If an organization starts shipping alerts from all their different sources without properly configuring and tuning Sentinel, the result will be the all-too-common alert overload, as well as cost spikes.

Sentinel works best when experts in a 24/7 SOC monitor and track credible threats. A managed extended detection and response (MXDR) service built on Sentinel can provide the expertise to guide incident response teams on how to effectively respond to a threat before it causes damage to your organization.

Ontinue ION for Nonstop SecOps

Ontinue is the only MXDR provider delivering NonStop SecOps by leveraging AI-driven automation, human expertise, and the Microsoft security platform. This combination allows ION to continuously assess and protect an organization's environment and improve its security posture.

As a modern MXDR service, ION can make security teams faster, more proactive and more efficient by integrating key capabilities that operationalize the Microsoft control plane:

AI-driven automation: Ontinue ION leverages AI-driven automation to accelerate numerous security operations tasks, including incident triage; Tier 1, 2, and 3 investigations; and resolution. This automation allows ION to close up to 70% of high severity threats automatically. The Ontinue Data Science team also continually measures every aspect of day-to-day security operations to identify new opportunities for automation and optimization. Customers experience smarter, faster decision-making and execution that reduces MTTD/MTTR. Combining these powerful capabilities with the AI- and ML-driven efficiencies of Sentinel significantly streamlines security operations and can save up to two days of security analyst time per week.

Real-time collaboration in Microsoft Teams: ION customers interact directly with their designated Ontinue SecOps teams through Microsoft Teams, not a vendor portal, so they can easily collaborate in real time over virtually any device. This native Teams integration provides all the utility of a standalone portal including real-time dashboards on threats, security score monitoring, preventive measures, and even ongoing Sentinel cost analysis, while also allowing additional team members, such as IT staff, to join collaboration conversations easily, without having to grant them access to yet another system.

Risk-based, localized protection: Ontinue ION builds a deep understanding of each customer's environment, business operations and teams to provide tailored protection — instead of the one-size-fits-all approach other vendors use. This effort includes using the results from ongoing detection and response efforts to determine where to focus preventive measures, including proactive threat hunting.

Specialized Microsoft Expertise: Ontinue ION is specifically built to leverage every component of the Microsoft security and collaboration ecosystem — such as Microsoft Defender, Microsoft Sentinel, and Microsoft Teams — while some vendors merely provide basic integrations with them. This hyper-focus on Microsoft allows Ontinue to help customers realize the full potential of all the capabilities in the Microsoft security stack.

Prevention: The ION service proactively prevents threats from occurring — moving far beyond basic detection and response services. Informed by your organization's existing processes and teams, ION helps your team prioritize where to focus, and maps into your existing processes, rather than forcing a one-size-fits-all approach. By reviewing the previous month's incidents to help you identify unresolved risk, ION creates a virtuous cycle of security in which detection and response informs prevention.

Ontinue ION Benefits

The advanced capabilities of Ontinue ION deliver Nonstop SecOps with 24/7 always-on protection, enabling you to maximize your current Microsoft security investments for greater efficiency.

1

Accelerate security program maturity

The efficacy and scalability of customers' security programs is improved by continually applying lessons learned to adapt and change for the future to increase efficacy.

2

Detect and respond fast—really fast

AI-driven automation and real-time collaboration eliminates noise, focuses efforts and helps respond to threats without negatively impacting business operations.

3

Operationalize Microsoft investments

ION is purpose-built to fully leverage every component of the Microsoft security and collaboration ecosystem, unlike other MXDR services

4

Apply a SecOps force multiplier

The ION Cyber Defense Center brings together security experts, PhD data scientists and software developers to execute, measure and optimize security operations.

CONTACT US

LEARN MORE

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue ION is the MXDR service of choice for Microsoft security customers that want to accelerate MTTR, proactively reduce risk, and reduce costs. Together, the Ontinue ION Platform and designated cyber defense experts build a deep understanding of your organization's risk posture that focuses prevention, detection and response efforts to reduce risk and mitigate threats.

AI-driven automation delivers fast, accurate investigation and response. Our one-of-a-kind Microsoft Teams interface provides real-time access to our 24/7 ION Cyber Defense Center to resolve every incident.

As the 2022 Microsoft Security MSSP of the year, Ontinue knows how to optimize your Microsoft investments, simplifying your technology stack and improving ROI.