

CASE STUDY

Reducing Costs, Simplifying Operations and Increasing Security—eSentire Embraces Microsoft 365 Defender

Overview

eSentire delivers MDR to organizations around the world, via a team that is itself distributed (and that became even more distributed by the COVID-19 pandemic). Safeguarding customers is the company's number one objective and is dependent upon eSentire's ability to secure itself and maintain 24x7 operations. To that end, eSentire's takes serious measures to secure the company against cyberthreats and has invested heavily in commercial solutions and proprietary technologies that meet the operational needs of the business as efficiently as possible without sacrificing enterprise security. In 2019, eSentire selected Microsoft's Defender suite of enterprise security tools to accomplish this objective. The following is a summary of the process that lead to this decision.

Business and Security Outcomes

- The team estimates they will realize 50% cost savings in security spend
- Security operations were simplified and eliminated the need for 10 third-party security tools
- Increased MITRE ATT&CK coverage with integrations eSentire has built for Microsoft 365 Defender
- eSentire was able to successfully integrate with eSentire's MDR platform, increasing detection and response capabilities

The Challenge

Security Leadership

- Ensuring selection of security partners align with overall IT strategy, business objectives and eSentire's brand

Security Practitioner

- Ensuring that the security partner effectively integrates with and (ideally) improves day-to-day workflows

To protect the business and its ability to deliver MDR, eSentire's Enterprise Security Team is responsible for ensuring the company's defenses can withstand attacks from even the most determined adversaries. Needless to say, prospective solutions must meet extraordinarily high requirements. Over the years, eSentire's enterprise security stack has become very deep as the company executed upon a full-spectrum, multi-layer cybersecurity strategy—including an "eSentire runs eSentire" operational paradigm. All evaluated security solutions must demonstrate an ability to work effectively under this operational paradigm.

Company Snapshot:

eSentire® is the world's largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Global Security Operations Center (GSOC) hunts, investigates and responds in real-time to cyberthreats before they become business-disrupting events. Founded in 2001.

“As a CISO, I don't want to have our security efforts impede business productivity. The fact that we've chosen a platform that provides a great end user experience for all of our employees and includes high-quality security tools really makes it a win-win.”

- Peter Romano, CISO

Selection of Microsoft 365 Defender

Security Leadership

- Microsoft 365 Defender is included under Microsoft enterprise licensing which meets multiple business needs in a remote work operating model

Security Practitioner

- Out of the box integration across four attack vectors, increasing MITRE ATT&CK coverage

Hardening defenses is an ever-evolving pursuit, and as part of this endeavor the Enterprise Security Team conducted a thorough review of the Microsoft Defender 365 platform. They understood that the range of solutions, their quality and their out-of-the-box integration would contribute to a defensive strategy capable of disrupting threats at every step of the attack chain:

- **Azure Identity and Access Management:** Defender ties threat discovery into a user's sign-in risk assessment, permitting dynamic adjustment of what a particular user—or compromised machine—can access. The team regarded this feature as a vital addition to the security stack, as it limits what an attacker can achieve should they manage to gain access.
- **Microsoft Cloud App Security:** With the shift to a cloud-first mentality to enable a global workforce and support remote working models, being able to secure dozens of services behind a single authentication and access platform is crucial. With Microsoft Cloud App Security and Azure AD SSO, eSentire gains insight into the tools that employees are using, and can manage and monitor their OAUTH permissions to prevent vectors of compromise.
- **Defender for Microsoft 365:** Phishing attacks in the remote work world continue to be a major threat. With Defender for Office 365, eSentire's employees are quickly and easily able to report suspected phishing attacks directly from their mail client, generating alerts within the Microsoft Security Center that can be actioned and tracked by eSentire's own Security Team. Additionally, Microsoft's native Phishing Attack Simulator dramatically simplifies executing quarterly phishing drills, reducing overhead and producing trackable statistics—as well as dynamically assigning training to users based off their results.
- **Defender for Endpoint:** Through unique telemetry, Defender for Endpoint provides remarkable visibility into activity on endpoints, as it's built on the industry's deepest insight into Windows threats and shared signals across devices—including Windows 10, Windows Server 2008R2-2019, MacOS, Linux, and even iOS and Android mobile devices—identities and information. Importantly, Microsoft Defender for Endpoint is firmly in the top tier of endpoint protection solutions—[Forrester recently awarded it the highest score possible](#) in the endpoint telemetry, security analytics, threat hunting, ATT&CK mapping and response capabilities criteria and [Microsoft Threat Protection leads in real-world detection in MITRE ATT&CK evaluation](#). Plus, for Windows 10 and Windows Server 2019 devices, it's agentless and cloud powered, so there's no additional deployment or infrastructure and no delays or update compatibility issues—meaning it's always up to date.

“

By leveraging the integrations eSentire has built for Microsoft 365 Defender, I'm able to reduce my overhead by offloading investigations to the GSOC, and increase my ability to map breaches to the MITRE ATT&CK framework.

Jason Westhaver,
Enterprise Security,
Technical Security Lead

”

10

Third-party security-related products eliminated under Microsoft consolidation

50%

Cost savings in security spend

Outcomes

Security Leadership

- Improved security coverage while reducing overall spend on tools

Security Practitioner

- Successful integration with eSentire's MDR platform, increasing detection and response capabilities

The team also recognized that introducing Microsoft's solutions would allow them to eliminate 10 existing third-party security products (and the associated vendor relationships), simplifying operational overhead without sacrificing the security posture. In fact, the team concluded that consolidating under Defender 365 would improve upon what was already a world-class position. In commercial terms, it was also a "no brainer"—a cost analysis showed that implementing the full Microsoft 365 defender platform will reduce costs by at least 50%.

Once the decision was made, the Enterprise Security team worked closely with the Product team to integrate Defender's capabilities into eSentire's MDR platform, which overcomes the data challenge of modern cybersecurity to enabling rapid, effective response to threats—whether protecting eSentire's clients or eSentire's own assets. This internal integration upheld the "eSentire runs eSentire" philosophy and at the same time provides the scaffolding for commercial products that utilize Microsoft Defender.

Ready to get started? We're here to help.

Reach out and schedule a meeting to learn more.

eSENTIRE®

eSentire, Inc., founded in 2001, is the category creator and world's largest **Managed Detection and Response (MDR)** company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, visit www.esentire.com and follow [@eSentire](https://twitter.com/eSentire).