eSENTIRE | AVANT | SIDEKICK IT

PARTNER CASE STUDY

How eSentire, AVANT, and Sidekick IT Collaborated on a Complete Security Solution to Help a Leading Media Company Consolidate and Save with eSentire 24/7 MDR

The Business

The joint Customer is a leading media and technology services company in intercollegiate athletics, providing ticket sales, licensed merchandise, and digital content to its end customers.

- Nation-wide presence in sports and technology mid-market organization with multiple corporate offices
- Looking for expert-level guidance to identify and address gaps in their security program and maximize their Microsoft investment
- Replace their incumbent MDR provider and reduce of number of security tools under management

Solutions and Results

eSentire, AVANT, and Sidekick ITpartnered to enable the Customer to streamline their security operations, consolidate their security tool stack, and maximize their Microsoft investment:

- **24/7 MDR for Microsoft Defender for Endpoint and Defender for Identity** to stop advanced threats and minimize the risk of business disruption across endpoints with a Mean Time to Contain of <15 minutes.
- **24/7 Multi-Signal MDR for Log** for 24/7 active log monitoring to deliver critical multi-signal visibility, ensure compliance, offer a system of record across their environment, and expert guidance from the eSentire Blue Team.
- **24/7 Dark Web Monitoring** to identify early indicators of compromise (IOCs), provide contextual awareness into known and unknown threats, and inform threat response actions.
- **Named Cyber Risk Advisor** who understands the business objectives to prioritize risk mitigation, drive return on cyber investment, and drive continuous improvement.

Business and Security Outcomes

- 24/7 threat detection, investigation, and response capabilities with eSentire's global SOC operations
- Achieve seamless integration with existing Microsoft security tools to consolidate their security tool stack and maximize their investment in Microsoft
- Improved visibility and reduced threat detection gaps across the organization
- Unlimited threat hunting, original threat research, and regular updates to runbooks, detection rules and machine learning models from eSentire's Threat Response Unit (TRU) to help the Customer stay ahead of the latest threats
- Trusted expert-level guidance to analyze their security measures and rapidly deploy eSentire MDR services
- Alignment of cybersecurity strategy, business objectives and risk through a dedicated eSentire Cyber Risk Advisor

The Challenge

As a leading media and technology company prioritizing cybersecurity, the Customer is no stranger to Managed Detection and Response (MDR). However, as they were ending a multi-year contract with a competitive MDR provider, the Customer opted not to renew with the incumbent and start the selection process for a new MDR provider.

They turned to their long-time partner Sidekick IT to lead the new vendor sourcing process. Sidekick IT, a leading-edge IT solutions provider, and Trusted Advisor (TA) with AVANT brought the project to the Technology Service Distributor's (TSD) cyber security team for expert support and advice in delivering a well-researched and technically sound short list of MDR vendors for the Customer to include in their planned request for information (RFI).

Why the Customer Chose eSentire

Collaboration. AVANT engaged the Customer's IT and Security Directors to fill out their Interactive Quick Assessment (iQA) questionnaire to determine their technical and security requirements. Using the results of the iQA, AVANT worked closely with Sidekick IT and the Customer to create an exhaustive RFI and defined a shortlist of AVANT's preferred MDR partners that were the best fit to respond to the RFI. As AVANT and Sidekick IT collaborated to build the short list of providers, it became clear that the Customer had three main priorities:

1. **Consolidate and Get More Value from Their MDR Provider:** the Customer wanted to move away from multiple vendors to a single vendor to streamline their security operations and reduce complexity.
2. **Integrate with Microsoft E5 Licensing:** They were looking to integrate their existing E5 licensing with the new MDR solution and were interested in replacing other software solutions to go all-in with Microsoft Defender.
3. **Improve Security Posture:** the Customer wanted to protect key risk points such as the user, the asset, the email gateway, and perimeter security edge.

eSentire was at the top of the shortlist not only because AVANT believed we could deliver the security outcomes the Customer was looking for, but because we also demonstrated how eSentire MDR for Microsoft would protect their key risk points. In addition, eSentire was able to highlight the breadth of the eSentire Insight Portal, which impressed their decision makers.

AVANT and Sidekick IT played a critical role in consistently engaging and building upon their trusted relationship with their shared customer, which resulted in the selection of eSentire as the chosen MDR vendor.

"I think demonstrating value was a big differentiator for us, we didn't send them off on their own to figure things out." According to Phil Battaglia, VP of North American Sales at eSentire, "we actually took the time to walk them through our platform, how it works, and why we built it the way we did, implementing their feedback along the way."

Martin Rich, Partner at Sidekick IT stated, "through consistent engagement with both our team and our colleagues at AVANT, the eSentire team communicated a clear Microsoft strategy that helped maximize the value of the Customer's Microsoft E5 investment and eliminate unnecessary point solutions." As a result of this consolidation, the Customer was able to cut their MDR costs by ~60%.

Ready to get started?