



Three Ways We Can Amplify Your Defense Against Evolving Cyberthreats



Digital estates continue to grow. There are more devices, businesses are migrating to the cloud in droves, and the workforce is more distributed than ever. At the same time, ransomware attacks are evolving quickly, and between human resource and budget constraints, businesses often struggle to secure their digital estates.

As a technology partner with years of expertise in helping businesses remain secure, we recommend replacing traditional point solutions with a consolidated Security Operations (SecOps) one. As part of that, we advise our customers to deploy Microsoft Sentinel, Microsoft's integrated approach to security incident and event management (SIEM). Here's how it helps you improve your response time against evolving threats.

Protect Everything

With Microsoft Sentinel, it's simple to protect your entire digital estate. A codeless connector platform within the content hub means you can onboard any data source with no code, and includes 228 connectors so you can work with systems like Cisco, AWS, SAP, Fortinet, CrowdStrike, and more. The content hub also includes dashboards, detection rules, playbooks and hunting queries all packaged as solutions so you can easily accelerate threat defense and take full advantage of your existing security stack.

Investigate Intelligently with AI

Intelligence is built into Microsoft Sentinel, taking the burden off your security teams. Instead, easily hunt for threats across all data types at cloud speed and take advantage of AI with machine learning, which automatically correlates alerts into prioritized incidents and uncovers patterns of attack. Additionally, industry-leading threat intelligence provides insight into bad actors.

79% reduction of false positives by correlating alerts into prioritized incidents

80% reduction in labor associated with advanced investigations

Microsoft Sentinel + Microsoft XDR

Microsoft Sentinel works hand-in-hand with Microsoft XDR products to deliver comprehensive threat protection across your entire multicloud, multiplatform digital estate. As experts in cybersecurity, we can help you implement both

Source: A commissioned study conducted by Forrester Consulting, "The Total Economic Impact™ of Microsoft Azure Sentinel," November 2020. Results are for a composite organization.

Respond more quickly

With Microsoft Sentinel, built-in security, orchestration, automation, and response (SOAR) allows defenders to automate any recurring or predictable enrichment, response, or remediation tasks for faster response and to free SecOps time for other activities. Similarly, built-in case management supports extra fast response to issues through collaboration and routine actions are automated with 200 off-the-shelf customizable playbooks. Plus, you can use your own machine learning inside Sentinel for added flexibility and speed.

88% reduction in mean time to respond (MTTR) response time with automation and case management

60% reduction in the risk of material breach

Transform your SOC today for comprehensive threat protection tomorrow!

As security experts, we choose Microsoft Sentinel because we've seen firsthand how putting a modern SIEM solution in place transforms the SOC in businesses just like yours. Whether you need an assessment, are ready to deploy, or need customization or managed services, we're ready to help you optimize threat detection, investigation, and response.

Contact us to learn more about how we can help put you on the path to a consolidated SOC today!