AKINSIT

Microsoft Defender XDR Accelerator

We empower your security team to detect and respond to cyberthreats with expanded visibility, incident-level investigation tools, and built-in automation

Engagement Overview

We develop a robust XDR strategy tailored to your business for detecting and responding to threats.

We provide a comprehensive set of documentation for how the solution was designed, built and how to operate .

Our Microsoft Security experts work with your team to optimize policy and threat hunting and reduce attack surface and vulnerability exposure.

Why Microsoft Defender for XDR?

Microsoft Defender XDR (Extended Detection and Response) is an advanced security solution that provides a unified defense against sophisticated cyber threats. It extends detection and response capabilities across endpoints, identities, email, and applications, offering an integrated approach to prevent, detect, investigate, and respond to advanced attacks. By integrating various security components, Microsoft Defender XDR simplifies the security operations center (SOC) workflow, enabling a more efficient response to incidents. Organizations can experience a significant return on investment, as one study found a 242% ROI over three years with Microsoft Defender XDR.

Automated responses and self-healing capabilities reduce the manual workload on security teams, allowing them to focus on other critical tasks. Microsoft Defender XDR augments individual service components, providing a comprehensive view of threats and their impact on the organization. Artificial intelligence (AI) driven technology helps stop advanced attacks like ransomware early in the attack chain, limiting the attacker's progress. Security professionals can proactively search for cyber threats, enhancing the overall security posture. This solution empowers organizations to manage their security with greater efficiency and effectiveness.

Our Approach to Microsoft Defender XDR

Our service ensures a tailored Microsoft Defender XDR deployment, from planning and design to pilot implementation and policy optimization. We collaborate with your team to configure a robust cyber defense system, focusing on reducing vulnerabilities and enhancing security operations. Our goal is to empower your organization with a strong, efficient cybersecurity posture.

Determine your business and technical requirements and select the appropriate architecture	Deployment and configuration s based on Microsoft and industry best practices	Based on feedback we optimize the solution by fine tuning alerts and policies

What to expect

During this engagement, we'll partner with you to help you get your Microsoft Defender XDR solution properly designed, deployed and configured according to your requirements.

Planning and Design We work with your team to define technical requirements to build out the Microsoft Defender XDR solution tailored to your specific needs and environment. During this phase we develop a design for the XDR components: Defender for Identity, Defender for Office 365, Defender for Endpoint, Defender for Cloud Apps and Entra ID Conditional Access and Identity Protection.

Deployment of Pilot We manage the deployment of the Microsoft Defender XDR solution from end-to-end and with your permission can even perform the implementation for you. This includes deploying each component, and configuring each component according to Microsoft and industry best practices.

Exposure Management During the pilot we work with your team to configure attack surface mapping, attack paths, Secure Score and other components to proactively manage your attack surface and vulnerability exposure.

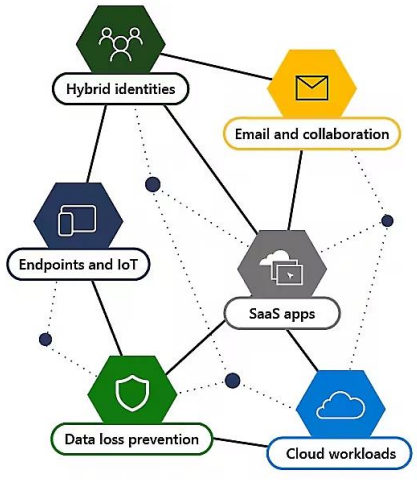
Policy Optimization During the pilot we work with your team to investigate and fine tune alerts and incidents by adjusting threat hunting queries and settings/policies across Microsoft Defender XDR.

About Microsoft Defender XDR

Microsoft Defender XDR is an advanced enterprise defense suite that provides integrated protection against sophisticated cyber threats. It coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications. Utilizing AI, it offers security teams powerful analytics and automated responses to secure digital environments. Defender XDR's cross-product layer augments individual services, delivering incident-level visibility and self-healing capabilities for mailboxes, endpoints, and user identities.

Extended

Get true visibility with incidents that span endpoints, identities, email, collaboration tools, data loss insights, and cloud.



Detection

Detect cyberthreats faster with Microsoft cyberthreat data informed by 78 trillion diverse daily signals for insights into a broad set of cyberthreat vectors.

Response

Streamline response with automatic cyberattack disruption, a unified investigation experience, and advanced AI.

AKINSIT

Schedule your implementation today!
https://www.akinsit.com/contact