Microsoft Security Roadmap

Microsoft: A Major Cyber Security Player

Organisations who are looking to keep pace with the challenges posed to security, data visibility, compliance, and incident response should look no further than Microsoft Security's best-in-class, integrated suite of solutions.

Security incidents and potential data breaches are unavoidable.

"You may not be able to avoid every potential incident, but what you can control is how you prevent them, and then how you respond when they do occur."

Rob McMillan
Research Director – Gartner

How Do You Keep Pace?

Cross-platform detection and response (XDR)

Use-case library – covering industry and compliance-specific initiatives

Scalable machine learning and automation

Data breach protection – a strategic data-centric approach to security

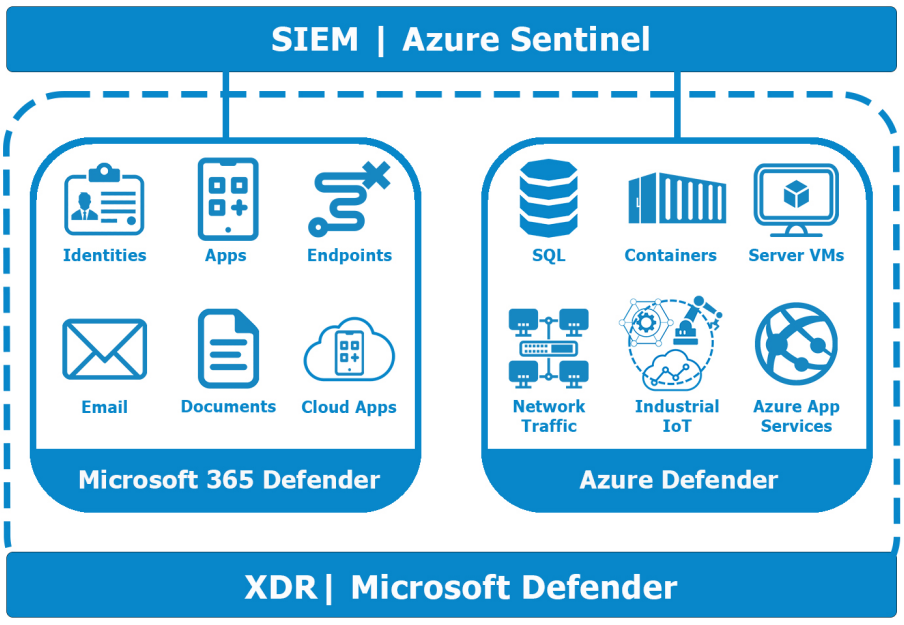
Incident response and threat hunting

Integration with existing tooling and processes

The Microsoft Security Roadmap

Consisting of Azure Sentinel and Defender, Microsoft and Satisnet ensure your organisation not only *keep pace* but excel in the requirements for *modern-day security*.

Microsoft Azure Sentinel: A cloud-based Security Information and Event Management (SIEM) tool that correlates log's and data from Microsoft and non-Microsoft platforms, providing a 'single pane of glass' for cyber security.



Microsoft 365 Defender: XDR capabilities for end user environments (email, documents, identity, apps, and endpoints) powered by four detection platforms – Defender for: Endpoint, Office 365, Identity, and MCAS
Azure Defender: XDR capabilities for infrastructure and cloud platforms (virtual machines, databases, containers, and IoT)

satisnet
streamlining security management

Microsoft

Microsoft XDR

In terms of platforms, correlations, threat intelligence, and machine learning, the Microsoft XDR coverage is far more advanced than any other offering.

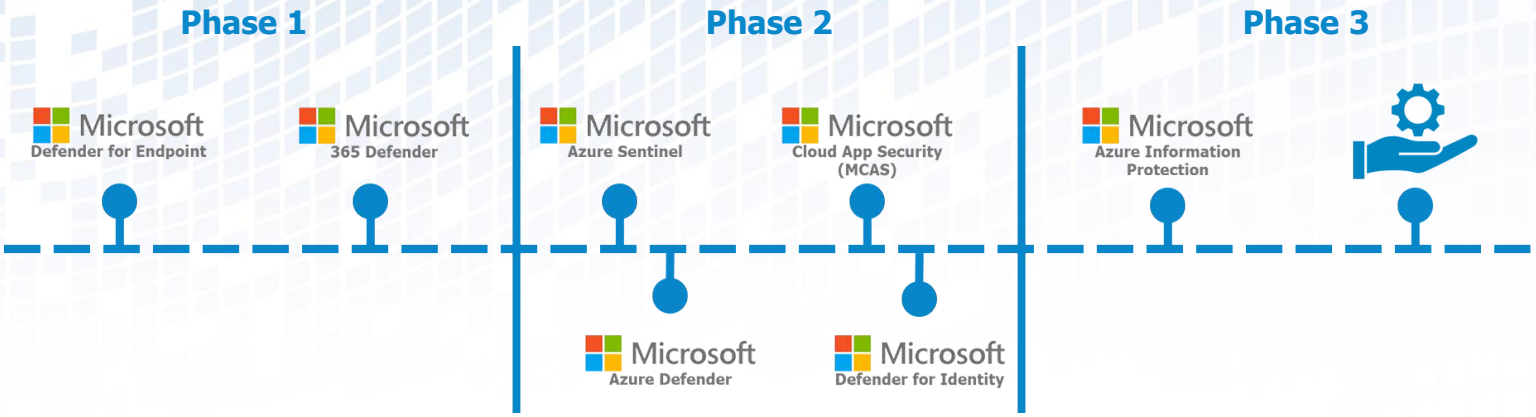
Email and Directory Services are still the largest attack surface used by hackers. As the developers of Office 365 and Active Directory (AD), Microsoft are a step ahead of the game when it comes to security, with inbuilt security metrics integrated throughout.

Your Microsoft Security Journey

Aiding your understanding of best practices around the powerfully rich, ever-evolving, and complex security features now available in the Microsoft suite, Satisnet provide end-to-end assistance with your journey.
Tailoring these capabilities to your environment and guiding their maturity over time, the Microsoft Security Roadmap optimises your security function.

The Roadmap Journey

To begin the XDR journey, organisations can start by using single elements of the XDR stack – ideally starting in areas most critical or where to achieve the earliest return. From there, more XDR components can be added to expand on the detections, cross-correlations, and inbuilt machine learning.



Microsoft Defender for Endpoint
- Protection (AV replacement), post-breach detection, automation investigation, and response

Microsoft 365 Defender
- Malicious email threats and links (URLs)
- Initial AIP-based DLP tagging and rules across endpoints and Office 365

Azure Sentinel
- Initial use-cases and incident response

Azure Defender
- Server and cloud estate monitoring

MCAS
- Cloud app monitoring

Defender for Identity
AD, DNS, and User and Entity Behavior Analytics (UEBA) monitoring

Azure Sentinel Maturity
- XDR and UEBA
- Third-party detections and logs
- Advanced threat hunting and automation

DLP
- Using AIP organisation-wide

The Roadmap Goal

The goal is to achieve a unified data protection platform utilising Azure Information Protection (AIP) – a Data Loss Prevention (DLP) platform that works across all XDR supported platforms covering the on-premise and cloud estates of an organisation.

www.satisnet.co.uk
+44 (0) 1582 369330

satisnet
streamlining security management