zensar

Unleashing Microsoft's Cloud-native SIEM/SOAR with Defender XDR:

Safeguarding Enterprise Infrastructure in the Digital Age

White paper

An RPG Company

Today, we delve into the capabilities of Microsoft's cloud-native modern SIEM/SOAR, featuring Microsoft Defender XDR and Security Copilot. This robust combination bolsters organizational security, safeguarding infrastructure, endpoints, data, network, and cloud edge services against security breaches, unauthorized access, and cyberattacks.

Our comprehensive white paper explores Microsoft's Zero Trust strategy model and its suite of services tailored for digital workplace infrastructures. We highlight how the advanced features of Microsoft Defender XDR, including extended detection and response (XDR), along with the power of AI-driven Security Copilot, enable proactive defense against unpredictable multivector cyberattacks and advanced persistent threats (APTs). We advocate for a holistic security approach that aligns with an organization's security objectives.

Introduction

In today's rapidly evolving digital landscape, hybrid workplaces have empowered organizations to operate with greater efficiency and productivity. However, despite growth in digital technologies, safeguarding enterprise infrastructure, endpoints, networks, clouds, and data against potential security threats and compliance remains challenging for enterprises worldwide.

Against this backdrop, Microsoft's security solution emerges as a powerful framework, offering a strategic model that helps organizations manage, defend, remediate, and respond to cyber threats. Supported by robust telemetry, Microsoft's security solution empowers enterprises to overcome regulatory compliance and traditional security challenges. This paper explores the advanced capabilities and services of SIEM/SOAR and Microsoft XDR's suite solution that can help address security challenges effectively.

Navigating enterprise security: Leveraging Microsoft's Zero Trust solution

With multi-layer unauthorized access, including ransomware, malware, and phishing attacks becoming increasingly common, organizations face significant risks to their operations and reputation. Adopting industry-standard practices is crucial to respond to such multivector threats and detect and mitigate them quickly. However, meeting these security regulatory standards and warding off potential attacks can be complex, tedious, and time-consuming. Microsoft offers a ready-to-deploy Zero Trust security solution, incorporating services like SIEM with Defender to efficiently and effectively manage these challenges.

Common attack order
(identity, email and apps, endpoints, hybrid cloud workloads):

- Phishing via enterprise emails or attachments
- Installing malicious software on enterprise assets
- Using root enterprise identity services accounts and cloud resources for unauthorized access

Common enterprise security operation challenges:

- MTTA (mean time to acknowledge) responsiveness
- MTTR (mean time to remediate) effectiveness

Key capabilities

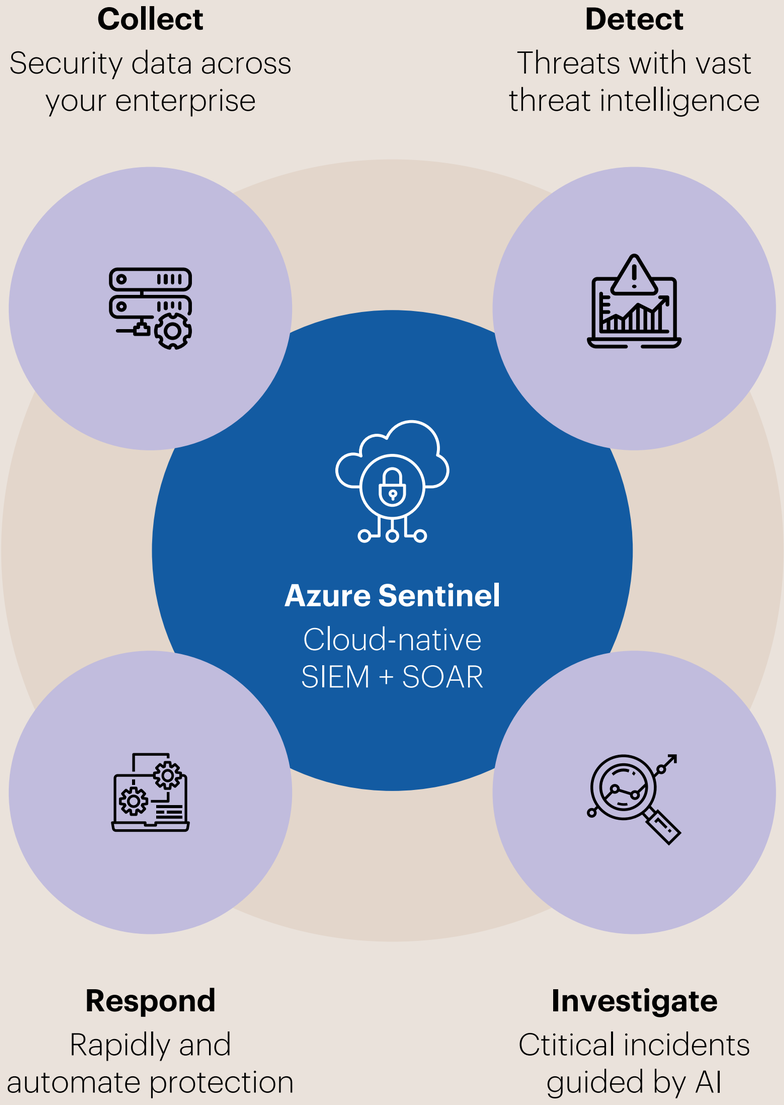
Capability	Services in use
Automated investigation and response (AIR)	Microsoft Defender XDR
Advanced hunting	Microsoft Defender XDR
Custom file indicators	Microsoft Defender XDR
Cloud discovery	Microsoft Defender for cloud apps
Custom network indicators	Microsoft Defender XDR
Endpoint detection and response (EDR) block	Microsoft Defender XDR
Device response capabilities	Microsoft Defender XDR
Live response	Microsoft Defender XDR
Secure cloud applications	Microsoft Defender for cloud
Improve your security posture	Microsoft Defender for cloud
Protect cloud workloads	Microsoft Defender for cloud
User and entity behavioral analytics (UEBA)	Microsoft Sentinel

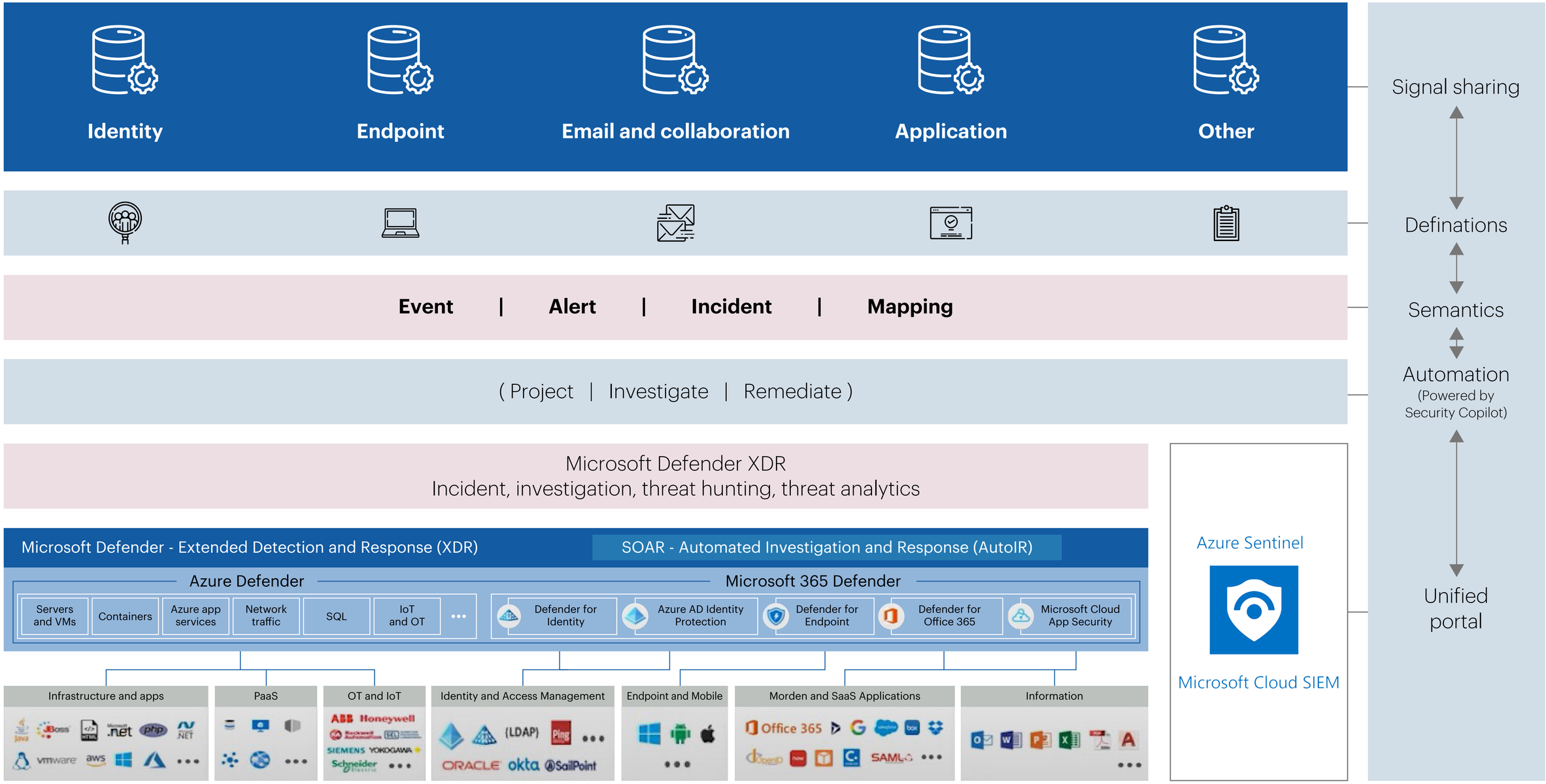
Capability	Services in use
Fusion	Microsoft Sentinel
Threat intelligence	Microsoft Sentinel
Automation	Microsoft Sentinel
Anomaly rules	Microsoft Sentinel
Scheduled queries	Microsoft Sentinel
Near-real-time (NRT) rules	Microsoft Sentinel
Hunting	Microsoft Sentinel
Microsoft Defender XDR connector	Microsoft Defender XDR and Microsoft Sentinel
Data connectors	Microsoft Sentinel
Content hub solution - zero trust (TIC 3.0)	Microsoft Sentinel
Security orchestration, automation, and response (SOAR)	Microsoft Sentinel

Revolutionizing enterprise security through XDR with Security Copilot

There is no question that Microsoft XDR has emerged as a game changer for enterprise security and vulnerability management. XDR plays a vital role by protecting enterprises against disparate modern threats and meeting industry-specific compliance and regulations such as GDPR, PCI, and DSS.

By prioritizing XDR along with Microsoft Sentinel, organizations can accelerate the ability to automatically respond to and remediate modern cybersecurity threat incidents, wherein Microsoft Defender XDR collects, correlates, and analyzes signal, threat, and alert data across all organization services. Microsoft Sentinel captures security information, event management security orchestration, and automation response to security incidents. AI-based tools and services such as Microsoft Security Copilot help organizations respond to attacks faster and more effectively. Security Copilot effectively summarizes incidents, analyzes threat and script codes, and takes appropriate actions and responses.




Identity
Endpoint
Email and collaboration
Application
Other
Event | Alert | Incident | Mapping
(Project | Investigate | Remediate)
Microsoft Defender XDR
Incident, investigation, threat hunting, threat analytics
Microsoft Defender - Extended Detection and Response (XDR)
SOAR - Automated Investigation and Response (AutoIR)
Azure Defender
Servers and VMs
Containers
Azure app services
Network traffic
SQL
IoT and OT
Microsoft 365 Defender
Defender for Identity
Azure AD Identity Protection
Defender for Endpoint
Defender for Office 365
Microsoft Cloud App Security
Infrastructure and apps
PaaS
OT and IoT
Identity and Access Management
Endpoint and Mobile
Morden and SaaS Applications
Information
Azure Sentinel
Microsoft Cloud SIEM
Signal sharing
Definations
Semantics
Automation
(Powered by Security Copilot)
Unified portal

Elevating security with strategic XDR partnerships

Organizations that prioritize multiple XDR solutions by partnering with established providers can significantly strengthen their security posture, minimize cost and effort, and effectively respond to security threats. Microsoft XDR solution stands out as a cornerstone in enterprise cybersecurity strategy and security, offering the ability to stay ahead of threats and protect critical assets.

As a leading IT services organization, Zensar has developed a mature and robust Microsoft XDR framework to offer support and essential platforms required to facilitate seamless integrations tailored to each enterprise's industry-specific standards. Microsoft XDR services continuously evolve, focusing on minimizing and avoiding business disruption. Zensar empowers organizations to harness all these technologies to ensure comprehensive protection. Organizations can maintain a competitive edge and attain enduring success in the digital era by meticulously strategizing, implementing, and prioritizing XDR solutions.

zensar

An RPG Company

We conceptualize, build, and manage digital products through experience design, data engineering, and advanced analytics for over 145 leading companies. Our solutions leverage industry-leading platforms to help our clients be competitive, agile, and disruptive while moving with velocity through change and opportunity.

With headquarters in Pune, India, our 10,500+ associates work across 30+ locations, including Milpitas, Seattle, Princeton, Cape Town, London, Singapore, and Mexico City.

For more information please contact: **velocity@zensar.com | www.zensar.com**