LOGICALIS
Architects of Change

Microsoft
Solutions Partner

Security Guide

Frontier IT Security: The Digital Perimeter Reimagined

How Logicalis and Microsoft Security protect the hybrid enterprise with a unified security fabric

Today’s organizations face an expanding digital attack surface that spans users, devices, apps, and infrastructure across cloud and on-premises environments.

In the modern world, the traditional security perimeter is dissolving, which means individual point solutions and specialized security tools are no longer enough. To stay protected, the hybrid enterprise needs a next-generation security fabric that simplifies protection and stays ahead of the cyber threat landscape.

Microsoft’s evolving stack, including Entra ID, Defender XDR, Sentinel, and Security Copilot, has been built for this new era. Together, they deliver an AI-driven, unified approach that rewrites the rules for securing the digital enterprise.

With Logicalis’ proven expertise and Microsoft's next-generation solutions, organizations of any size can create an integrated security fabric that protects collaboration, applications, endpoints, and critical infrastructure.

The New Digital Perimeter

Modern organizations are contending with a fractured security landscape, shifting network boundaries, and a continually evolving digital perimeter. To protecting sensitive data, users, and operations, security teams must look beyond traditional point solutions, which offer specialized functionality in specific areas but can leave gaping holes in others.

This is more important than ever as we move into an era dominated by AI, agents, and cloud-native software. Modern strategies must expand to cover these evolving domains, without creating gaps or overly complicating security workflows.

The Digital Perimeter is Evolving

Networks

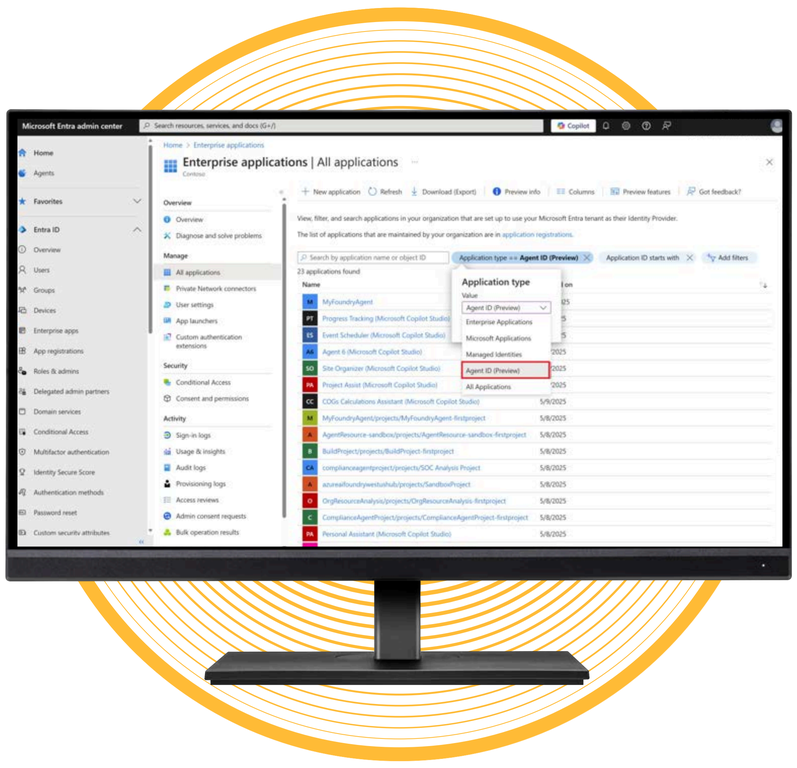
Endpoints

Identity

Next-Generation Identity and Governance with Microsoft Entra ID

Microsoft Entra is a family of identity and network access products that lets organizations implement a Zero Trust security strategy and create a trust fabric that verifies identities, validates access conditions, checks permissions, encrypts connection channels, and monitors for compromise.

Recently, Entra has expanded with new features, integrations, and capabilities:

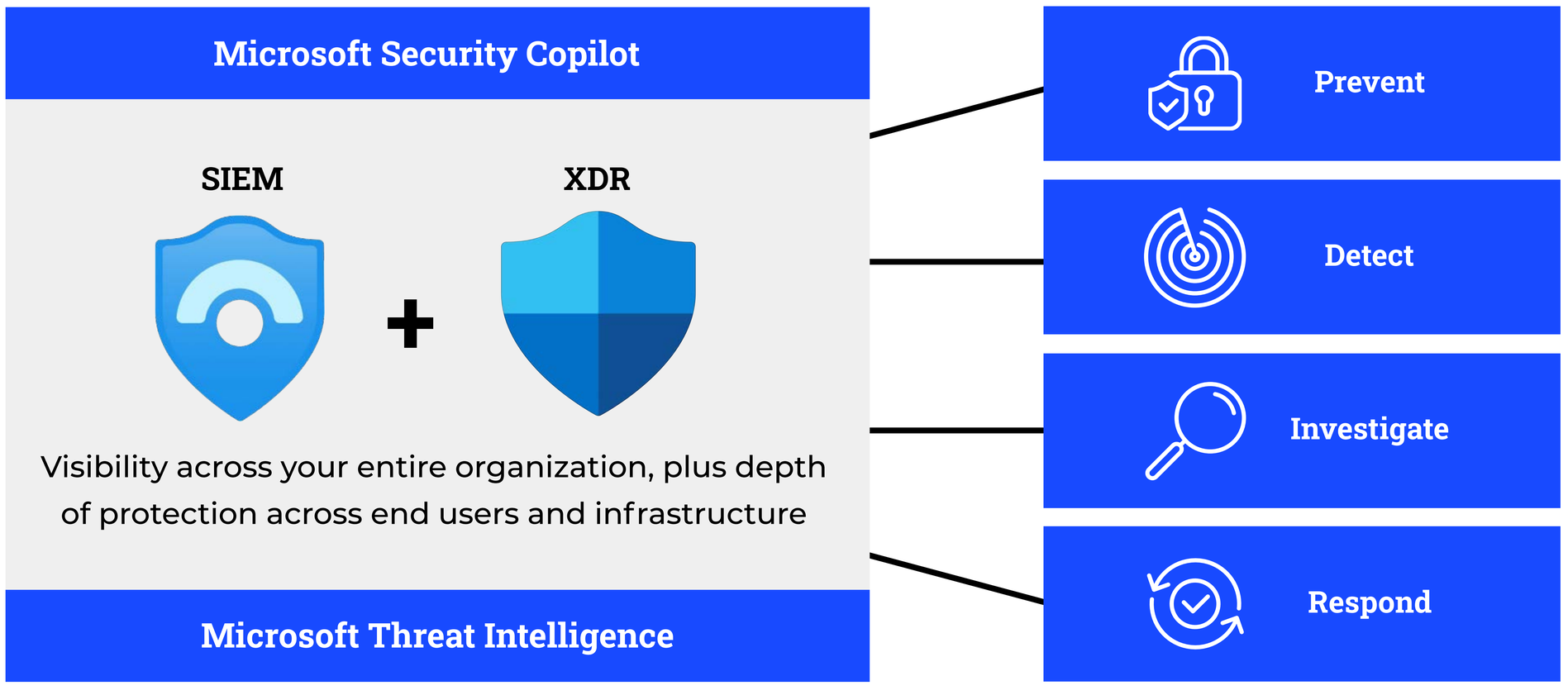


- **Lifecycle workflow enhancements** offer increased control and consistency in managing identities throughout their lifecycle
- **Separation of Duties (SoD) policies** allow enforcement of incompatible role combinations
- **Expanded access reviews** now include dynamic Microsoft 365 groups and richer decision insights
- **Advanced Microsoft Graph endpoints and SCIM enhancements** simplify automation
- **Conditional access** can now evaluate combined identity, device posture, and network trust
- **Microsoft Entra Agent ID** extends identity protections to enterprise AI agents

Microsoft Entra's evolution means every user, workload, and agent is governed, monitored, and protected by default.

Defender XDR and Microsoft Sentinel: Unified AI-Driven Detection and Response

Microsoft Defender XDR and Microsoft Sentinel now operate as a single, cloud-native XDR-SIEM platform. It gives security teams one place to see, investigate, and respond to threats by unifying advanced hunting, analytics, and automation. The integrated solution helps organizations break down tool silos, reduce mean time to detect and respond, and standardize operations on a modern, AI-driven SOC foundation.



Recent updates to the platform have significantly modernized its capabilities and security value:

- **Sentinel now lives within the Defender portal** and centralizes incident management, hunting, automation, and threat intelligence.
- **The newly released Microsoft Sentinel Data Lake** enables cost-effective, scalable storage and analytics, breaking down silos for richer insights.
- **The ADX operator in Defender** enables security analysts to hunt across Azure Data Explorer tables.
- **Defender Threat Intelligence** has now been converged directly into both Defender XDR and Sentinel.
- **All alerts, incidents, and hunting data** are bi-directionally synced
- **Sentinel supports multi-tenancy and AI agents** that autonomously correlate, escalate, and remediate threats
- **Defender for Office 365 and Teams add auto-remediation** for malicious messages and mail-bombing detection

Security Copilot as the Ultimate Force Multiplier

Microsoft Security Copilot brings generative AI directly into the security operations workflow, acting as a conversational assistant for the full Microsoft security stack. Security Copilot can interpret natural language questions, reason over real-time security data, and generate recommended actions.

With proper adoption, it can help to close close skills gaps, speed up investigations, and inform security decisions:

- **Security Copilot summarizes and correlates incidents,** provides step-by-step remediation advice, and autonomously handles high-volume investigations.
- **Teams can query their environment using plain language** to extract insights from Sentinel, Defender, Intune, and more
- **Copilot agents analyze access and recommend real-time policy adjustments** to maintain least-privilege access and respond to emerging threats
- **Agents can automatically generate** investigation summaries, posture management reports, and policy recommendations
- **Custom Copilot-driven agents or pre-built agents** can be used for key tasks, such as continuous policy analysis and data loss prevention

Security Copilot, a relatively new addition to the Microsoft Security portfolio, has already helped reduce incident resolution time and alert fatigue within three months of adoption.

Microsoft Security Copilot

Security Operations		Data Security	Identity & Access	Endpoint Management
Microsoft Defender	Microsoft Sentinal	Microsoft Purview	Microsoft Entra	Microsoft Intune
• Vibe Hunting • Phishing Triage	• Threat Detections • Threat Intelligence Briefing	• Data Security Triage • Data Security Posture	• Conditional Access • Access Review • Application Lifecycle	• Vulnerability • Device Lifecycle • Policy Compliance

Logicalis' Layered Identity and Security Approach Across the Microsoft Cloud

Logicalis overlays Microsoft's innovations with managed extended detection and response (MXDR) services and a digital fabric platform that amplifies security outcomes.

Microsoft-Verified MXDR Services: Security specialists provide 24/7/365 monitoring, proactive threat hunting, and incident response for Defender, Sentinel, and Entra for unified protection and regulatory compliance

Digital Fabric Platform: Our proprietary Digital Fabric Platform offers real-time, actionable insights across cloud, identity, data, and endpoints for enhanced control and resilience

Blueprint Approach: Solutions are tailored to customer needs, starting with risk assessments and architectural design, followed by deployment and ongoing managed services

Zero Trust and Compliance: We incorporate zero-trust pillars to ensure every user and workload operates under continuous assessment and adaptive controls

Over the years, we have helped organizations modernize with the Microsoft Security portfolio, our own technology solutions, and a proven framework for transformation.

Reimagining Your Digital Perimeter with Logicalis and Microsoft

Microsoft's security ecosystem is designed to integrate into a single fabric that protects collaboration, apps, endpoints, and infrastructure.

Entra governs users, machines, and agents with continuous validation and automated least-privilege access. Defender XDR and Sentinel provide comprehensive signal correlation and machine-speed response to threats across endpoints, identities, clouds, and apps. Security Copilot accelerates detection and response and enables automated security at scale. All of these technologies work together to create a unified shield that adapts and evolves with the organization.

With a partner like Logicalis, Microsoft's next-gen security portfolio protects collaboration, applications, endpoints, and core infrastructure with agility, intelligence, and resilience.

By architecting a unified security fabric, organizations can safeguard their digital future and stay focused on what matters most: their business.

Schedule a free executive briefing

- Global Azure Expert MSP, recognizing the highest standard of Azure managed services and complex cloud environments
- Five Microsoft Solution Partner designations across Security, Infrastructure (Azure), Data & AI, Digital & App Innovation, and Modern Work
- Multiple Microsoft Security Advanced Specializations, including Cloud Security, Identity & Access Management, Information Protection & Governance, Threat Protection
- Verified Microsoft Managed XDR (MXDR) provider and member of the Microsoft Intelligent Security Association (MISA)
- Global Security Operations Centers with more than 15 years of SOC experience
- 300+ dedicated Microsoft security professionals and hundreds of Microsoft-certified engineers across Azure, Security, and Modern Work