

Microsoft Defender XDR for Cloud

Comprehensive Cloud Security Posture Management
and Workload Protection

Overview

Microsoft Defender XDR (formerly Microsoft 365 Defender) is a unified Extended Detection and Response (XDR) suite that natively coordinates detection, prevention, and response across your entire digital estate. Celebal Technologies specializes in transforming siloed security point-solutions into a cohesive, AI-augmented defence engine. By integrating Endpoints, Identities, Email, and Cloud Apps, we empower your SOC to stop multi-stage attacks at machine speed.

Engagement Highlights

Comprehensive Zero Trust Assessment: End-to-end evaluation of your current security posture across all M365 domains.

Cross-Platform Endpoint Onboarding: Unified management for Windows, macOS, Linux, Android, and iOS devices.

Advanced Email & Collaboration Defence: Hardening Office 365 against BEC (Business Email Compromise), QR-code phishing, and malicious Teams links.

Hybrid Identity Protection: Deploying Defender for Identity sensors to bridge the gap between on-premises AD and cloud identities.

Shadow IT & Data Governance: Discovering unmanaged SaaS apps and enforcing session-level controls via Defender for Cloud Apps.

What We Assess

- ❖ Gap Analysis: Map existing tools against M365 to eliminate redundancies.
- ❖ Signal Readiness: Audit log quality across AD, mail, and SaaS connectors.
- ❖ Consolidation: Define the migration path from legacy vendors to Microsoft.
- ❖ Workflow Review: Identify SOC bottlenecks to improve MTTR via automation.

Key Features

- ❖ Auto-Containment: Stop ransomware instantly by isolating compromised users and devices.
- ❖ Identity Defense: Prevent lateral movement and credential-based attacks.
- ❖ SOC Automation: Reduce analyst workload by auto-remediating 90% of alerts.
- ❖ Proactive Hunting: Query 30 days of raw telemetry using KQL.

AI-Powered Security



NLP Investigation

Query security data with plain-English prompts.



Script Intelligence

Automated analysis of obfuscated code and CLI commands.



Guided Recovery

Tailored, step-by-step incident response playbooks.



Auto-Reporting

Weekly summaries of threat landscape and security posture.

Business Impact

1. 80% Reduction in Incident Response Effort: Shifting your team from "firefighting" to proactive security operations.
2. Up to 60% Lower TCO: Realizing significant cost savings through vendor consolidation and license optimization.
3. Zero Trust Operationalization: Enforcing risk-based Conditional Access at the moment of authentication.
4. Minimized Dwell Time: Machine-speed containment reduces the "blast radius" of successful intrusions.

Implementation Roadmap

1 Architecture & Design: Defining RBAC, alert tuning, and data retention policies (aligned to 2026 compliance standards).

2 Core Onboarding: Systematic rollout of Endpoint sensors, MDI sensors, and MDO threat policies.

3 Advanced Hardening: Enabling Attack Surface Reduction (ASR) rules, EDR in Block Mode, and Tamper Protection.

4 Operational Excellence: Configuring SOAR playbooks, custom detections, and Microsoft Security Copilot integration.

5 Maturity Handover: Delivering custom runbooks, training for Tier 1-3 analysts, and a 12-month evolution roadmap

Estimated Range

USD 12,000
(Fixed / Estimated).

Variables: Final cost is determined by the number of protected seats (identities/mailboxes), total endpoints, and the depth of automation required..

Why Celebal

- Unified SOC Pioneers: We are experts at merging Sentinel (SIEM) and Defender (XDR) into a single operational portal.
- Security Data Engineering: We don't just "turn on" features; we optimize your data lake to ensure cost-efficient, high-performance logging.
- AI-First Delivery: Celebal integrates Security Copilot as a standard part of our deployment, ensuring your team is future-proofed for 2026 and beyond.
- Microsoft DNA: Deep strategic alignment with the Microsoft product team to leverage early-access features and best-practice frameworks.