CLOUDGUARD

ADVISORY

Microsoft Defender XDR Accelerate

Microsoft Defender XDR Accelerate delivers a production-ready security foundation across the M365 ecosphere

Service overview

Microsoft Defender XDR delivers integrated protection across devices, identities, email, and applications within Microsoft 365 by unifying extended detection and response (XDR), threat intelligence, and built-in vulnerability management into a single security platform.

The Microsoft Defender XDR Accelerate engagement establishes Microsoft-recommended security baselines across Endpoint, Identity, Email, and Cloud Apps, forming a unified Defender XDR foundation. This enables organisations to move beyond fragmented, reactive security models and adopt a modern, integrated defence aligned to Microsoft's recommended security architecture.

Core Defender XDR capabilities—including endpoint protection, email and collaboration security, identity threat detection, and cloud application governance are implemented in a consistent and repeatable way. This delivers immediate improvements in threat visibility, risk reduction, and incident readiness across the Microsoft 365 environment.

The result is a production-ready Microsoft Defender XDR deployment with clear baseline controls and correlated threat signals, providing a strong operational foundation that security teams can confidently run, optimise, and extend as security maturity grows.

- **Readiness** – Setting the right security foundations.
- **Responsiveness** – faster adoption, and risk reduction.
- **Resilience** – Sustained security maturity

Service value

Defender XDR Accelerate delivers measurable security and business value:

- Accelerates time-to-value from Microsoft Defender XDR by rapidly deploying proven, Microsoft-recommended security baselines
- Reduces organisational risk through integrated protection across endpoints, identities, email and applications
- Improves threat visibility and investigation by correlating signals across the Defender XDR suite
- Strengthens incident readiness with live, operational detection and response capabilities
- Enables security teams with guidance and knowledge transfer to confidently operate and extend Defender post-engagement
- Establishes a scalable security foundation that supports future maturity, optimisation, and managed security services

Why this matters now

Cyber threats are growing more advanced, yet many organizations underuse their Microsoft 365 Defender tools. Without a solid baseline, security teams struggle with limited visibility and slow responses. Defender 365 Accelerate helps close this gap by maximising existing investments, reducing risks, and enhancing threat management.

CLOUDGUARD

Microsoft Defender XDR Accelerate Scope

Defender XDR Accelerate aligns to the following capability areas:

Endpoint protection
Deployment of Defender for Endpoint with best-practice security baselines, EDR enablement, and policy configuration across in-scope devices.

Email and collaboration security
Implementation of Defender for Office protections, including safe links, safe attachments, and anti-phishing controls across Exchange, Teams, SharePoint, and OneDrive.

Identity protection
Configuration of Defender for Identity to detect suspicious activity and threats targeting user identities across Active Directory.

Cloud application governance
Enablement of Defender for Cloud Apps to provide visibility into application usage and control risky or unsanctioned applications.

Engagement conclusion
The engagement concludes with validation activities, documentation, and structured close-out to ensure a stable, production-ready Defender XDR deployment.

Our approach

Delivered through a collaborative, structured engagement:

Focused alignment – We begin by confirming business objectives, security priorities, licensing readiness, and key stakeholders to ensure the engagement targets real risk and operational outcomes.

Baseline deployment – Core Microsoft Defender XDR capabilities are deployed using Microsoft-recommended configurations, prioritising controls that deliver immediate protection and visibility.

Controlled enablement – Where appropriate, policies are introduced in audit or monitored states to allow validation and tuning before full enforcement.

Operational readiness – Guidance, documentation, and knowledge transfer ensure internal teams can confidently operate, maintain, and extend Defender following deployment.

Why CloudGuard

CloudGuard delivers enterprise-grade cybersecurity for growing businesses. Combining automation-led technology with UK-based experts, we provide 24/7 protection, without the complexity or cost of traditional platforms. Our fully managed approach simplifies detection, protection and improvement, so you can focus on growing with confidence.

Get in touch