CLOUDGUARD

ADVISORY

Microsoft Defender XDR Assess

Microsoft Defender XDR Assess delivers a best practised mapped, and prioritised roadmap to security posture improvement.

Service overview

Microsoft Defender XDR delivers integrated security across identities, devices, email, applications, and cloud services within Microsoft 365. When correctly configured and actively monitored, it provides powerful detection, investigation, and protection capabilities across the modern attack surface.

The Microsoft Defender XDR Assess is a structured, outcome-focused engagement, designed to provide clear visibility into an organisation's current Defender XDR security posture. It evaluates existing Defender XDR configurations, identifies misconfigurations and gaps, and highlights unused or underutilised capabilities across the Defender XDR suite.

The assessment focuses on identifying security risk through analysis of alerts, vulnerabilities, Secure Score posture, high-risk assets, and key configuration areas such as email protection and identity security. All analysis is performed using native Microsoft tools with read-only access, ensuring the assessment is non-intrusive and safe.

The result is a tenant-specific view of current risk, combined with practical, prioritised recommendations that enable security teams to take informed action—providing clarity on where to focus effort to reduce risk and improve security maturity.

- **Readiness** – Know your true Security position.
- **Responsiveness** – Identify & act quickly on the risks that matter most.
- **Resilience** – Reduce future exposure through stronger, sustainable controls.

Service value

Microsoft Defender XDR Assess delivers immediate insight and measurable value:

- Provides a clear, tenant-specific view of security posture across identities, devices, apps, and data via Secure Score
- Reduces organisational risk by identifying the highest-impact vulnerabilities and security gaps
- Improves threat visibility by uncovering unresolved alerts and detection gaps
- Supports informed remediation decisions through prioritised, risk-based recommendations
- Validates email and phishing protection against current best-practice configurations
- Maximises return on the Defender XDR investment by highlighting unused or underutilised capabilities already licensed

Why this matters now

Many organisations use Microsoft's security products but often don't know how effective they are. Misconfigurations and unresolved issues increase breach risk, while unused features go to waste.

Microsoft Defender XDR Assess quickly reveals security status, helps prioritise improvements, and supports informed decisions without disrupting operations.

CLOUDGUARD

Microsoft Defender XDR Assess Scope

The Microsoft Defender XDR Assess service aligns to the following assessment areas:

Alert and threat discovery
Review of active alerts, unresolved items, and threat analytics to identify detection gaps and response risks.

Vulnerability assessment
Analysis of device vulnerabilities, highlighting those presenting the highest security and business impact.

Secure Score posture review
Identification of priority Secure Score actions across Identity, Device, Apps, and Data to improve overall posture.

Assets and at-risk device review
Identification of high-risk devices and applications contributing disproportionately to organisational risk.

Email and phishing protection review
Assessment of email security and anti-phishing policies against current best-practice configurations.

Defender XDR capability review
Evaluation of configured Defender XDR solutions and identification of unused or under-utilised capabilities that could further improve security posture.

Engagement conclusion
The engagement concludes with a formal handover, including an executive summary, prioritised findings, and a clear roadmap for remediation.

Our approach

Delivered through a focused, non-intrusive assessment engagement:

Targeted discovery – We analyse existing Microsoft Defender XDR configurations using read-only access, ensuring no changes are made to your environment.

Risk-based analysis – Findings are prioritised based on likelihood, impact, and relevance to real organisational risk rather than generic checklists.

Microsoft-aligned insights – Secure Score actions and Defender XDR findings are mapped to Microsoft-recommended best practices.

Actionable outcomes – Results are documented in a clear, prioritised report, supported by an executive summary to guide immediate and longer-term improvement.

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