

Premium Security Optimization Service for Microsoft 365

Secure. Govern. Protect

Make Your Microsoft License Go Further

This document outlines premium security service areas including advanced identity protection, data governance, AI security, advanced email and app protections, endpoint detection and response, and compliance. This service is scoped to Microsoft 365 E3 and E5 and/or Entra ID P2, Azure Information Protection P2, Purview add-on, Defender for Office 365 Plan 2, Defender for Endpoint Plan 2, Purview Communication Compliance and Defender Suite add-on licence capabilities.

All scoped deliverables in the Gold Security Optimization Service are included.

1. Scope of Services

Advanced Identity Protection

- Configure Privileged Identity Management (PIM) via Microsoft Entra ID P2 to enforce just-in-time and time-bound privileged role activation for administrative accounts.
- Configure access reviews to periodically validate and recertify privileged role assignments and guest access.
- Enable Microsoft Entra ID Protection risk policies (requires Entra ID P2): configure risk-based Conditional Access to automatically block or require MFA step-up on high-risk sign-ins, and enforce secure password reset upon detection of leaked credentials identified through Microsoft's dark web and breach database scanning pipeline.
- Configure FIDO2 security key and Temporary Access Pass (TAP) authentication methods for passwordless and break-glass access scenarios.
- Harden guest and external user access controls including cross-tenant access policies and B2B Conditional Access enforcement.
- Deploy Microsoft Defender for Identity to monitor on-premises Active Directory for lateral movement, pass-the-hash, pass-the-ticket, and other identity-based attacks. Requires hybrid environment with on-premises AD.

Data Protection & Governance

- Configure Microsoft Purview sensitivity labels and publish label policies across Microsoft 365 apps, SharePoint, OneDrive, and Exchange.
- Configure auto-labelling policies (requires E5 or Azure Information Protection P2) to automatically classify and protect documents and emails containing sensitive information types without user intervention.
- Deploy Microsoft Purview Data Loss Prevention (DLP) policies across Exchange, SharePoint, OneDrive, and Teams chat (Teams chat DLP requires E5 or Purview add-on).
- Configure Endpoint DLP to prevent sensitive data exfiltration via clipboard, USB removable media, print, and cloud upload on managed Windows devices (requires E5 or Purview add-on).
- Configure retention policies and retention labels to enforce records management obligations and data lifecycle requirements.

Securing AI (Microsoft Copilot)

- Apply Conditional Access policies scoped to Microsoft Copilot to restrict access to compliant and managed devices only.
- Configure DLP policies within Microsoft Purview to prevent sensitive labelled content from being processed or surfaced in Copilot prompts and responses.
- Enable Microsoft Purview audit logging for Copilot interactions to record prompt and response activity for compliance and investigation purposes (full Copilot interaction audit requires E5 or Purview Communication Compliance).
- Configure retention policies for Microsoft 365 Copilot interaction data.
- Enable Copilot usage telemetry reporting via the Microsoft 365 admin centre to monitor adoption and identify oversharing risks.

Advanced Email & Apps Protection

- Upgrade to Microsoft Defender for Office 365 Plan 2 capabilities: configure Automated Investigation and Response (AIR) to automatically investigate and remediate email threats without analyst intervention.

- Enable Threat Explorer for real-time investigation of malicious email, URLs, and files across Exchange Online, SharePoint, OneDrive, and Teams.
- Configure Threat Trackers to monitor active attack campaigns targeting the organisation.
- Enable real-time detonation sandboxing for zero-day malware detection across email attachments and URLs via Safe Attachments. Defender for Office 365 Plan 1 provides attachment sandbox scanning; Plan 2 extends this with post-delivery detonation, automated response, and Threat Explorer visibility.
- Configure advanced anti-phishing tuning including custom impersonation protection thresholds, mailbox intelligence, and first-contact safety tips.
- Extend DMARC configuration with DMARC policy enforcement (p=quarantine or p=reject) and configure aggregate and forensic reporting.
- Apply Teams restrictions including anonymous meeting join policies and external domain allow/block lists.

Endpoint Detection & Response (EDR)

- Upgrade endpoint protection to Microsoft Defender for Endpoint Plan 2 for full EDR capability including endpoint detection and response, automated investigation, and advanced threat hunting. Note: tenants using Defender for Business (included in Business Premium) require all-user licensing for Defender for Endpoint Plan 2 to access Plan 2 features.
- Configure Microsoft Defender for Endpoint threat and vulnerability management to continuously assess software vulnerabilities and misconfigurations, prioritised by exploitability and asset criticality.
- Enable threat analytics dashboards and threat intelligence reports to surface active threats relevant to the organisation's environment.
- Configure live response and advanced hunting queries (Kusto Query Language) for proactive threat investigation across endpoints.
- Enable six-month device data retention for extended incident investigation and forensic analysis.

Cloud App Security (CASB)

- Deploy Microsoft Defender for Cloud Apps to discover shadow IT and unsanctioned cloud application usage across the organisation (requires E5 or Defender Suite add-on).
- Configure app governance policies and session controls via Conditional Access App Control to restrict risky in-session activities in sanctioned SaaS applications.
- Configure anomaly detection policies to identify unusual user behaviour patterns within cloud applications, including mass download, impossible travel, and suspicious inbox manipulation rules.

Audit & Compliance

- Configure Microsoft Purview Audit (Premium) to extend audit log retention to one year for high-value user and administrator events (requires E5 or Purview add-on).
- Configure custom audit log retention policies for specific workloads requiring extended retention beyond the default 90-day standard audit period.
- Review and configure Microsoft Compliance Manager assessments to track configuration alignment against applicable regulatory frameworks.

2. Deliverables

- Privileged Identity Management (PIM) and access review configuration for administrative roles
- Entra ID P2 risk-based Conditional Access policies including leaked credential response
- FIDO2 and Temporary Access Pass authentication method configuration
- Microsoft Defender for Identity deployment (hybrid AD environments)
- Guest and external access hardening including cross-tenant access policies
- Sensitivity label policies and auto-labelling configuration across Microsoft 365 workloads
- DLP policies across Exchange, SharePoint, OneDrive, Teams chat, and endpoints
- Retention policies and records management configuration
- AI governance configuration for Microsoft Copilot including DLP, audit logging, and retention
- Defender for Office 365 Plan 2 configuration: AIR, Threat Explorer, and Threat Tracker
- Advanced anti-phishing tuning and DMARC enforcement configuration

- Defender for Endpoint Plan 2 EDR and threat hunting configuration
 - Vulnerability management configuration with exploitability-based prioritisation
 - Defender for Cloud Apps deployment and shadow IT discovery configuration
 - Audit (Premium) configuration and extended log retention policies
 - Compliance Manager assessment review and documentation
 - Customised documentation and updated security posture report
-

3. Expected Outcomes

- Stronger protections for privileged identities through just-in-time access, access reviews, and risk-based Conditional Access
 - Proactive detection of compromised credentials through automated leaked credential monitoring and risk remediation
 - Enhanced data governance with automated classification, labelling, and DLP enforcement across all Microsoft 365 workloads
 - Minimised data leakage risk across email, cloud apps, Teams chat, and managed endpoints
 - Secure and auditable usage of Microsoft Copilot with DLP enforcement, retention, and interaction audit trails
 - Higher phishing and spoofing resistance through advanced anti-phishing policies, DMARC enforcement, and automated email threat remediation
 - Improved endpoint threat detection and response capability with full EDR, automated investigation, and threat hunting
 - Improved visibility into cloud application usage and insider risk through CASB controls and anomaly detection
 - Extended audit trail and forensic investigation capability through Audit (Premium) and six-month endpoint data retention
 - Higher security compliance alignment with Centre for Internet Security (CIS), NIST CSF 2.0, PCI-DSS, and ISO/IEC 27001 Microsoft best practices
-

Note: Specific feature availability within this service is subject to the customer's active Microsoft 365 licence tier. Features marked as requiring E5, and/or Entra ID P2, Azure Information Protection P2, Purview add-on, Defender for Office 365 Plan 2, Defender for Endpoint Plan 2, Purview Communication Compliance and Defender Suite add-on licence will only be configured where the applicable licence is in place. Knovation Solutions will confirm licence eligibility during the Assessment & Roadmap phase.