

Gold Security Optimization Service for Microsoft 365

Secure. Govern. Protect

Make Your Microsoft License Go Further

This document outlines key gold security service areas including identity protection, email and app security, endpoint enrolment, and endpoint protection. This service is scoped to Microsoft 365 Business Standard, Business Premium, F1, F3 and M365 E3 licence capabilities where applicable.

1. Scope of Services

Assessment & Roadmap

- Establish cybersecurity frameworks, identity strategy, admin account strategy, device management approach, licensing, and notification contacts.
- Review Microsoft Secure Score and document baseline security posture across identity, email, endpoint, and data.

Identity Protection

- Implement least privilege access, break-glass emergency access accounts, and Named Location policies.
- Configure Multi-Factor Authentication (MFA) policies and Conditional Access policies using Microsoft Entra ID P1.
- Enable Self-Service Password Reset (SSPR) and configure password protection policies to block known weak and banned passwords.
- Configure Microsoft Entra ID sign-in risk and user risk policies available at Entra ID P1 tier, including block policies for legacy authentication protocols.

Email & Apps Protection

- Configure SPF, DKIM, and DMARC records to authenticate outbound mail and prevent domain spoofing.
- Enable Microsoft Defender for Office 365 Plan 1 protections: Safe Links (time-of-click URL filtering), Safe Attachments (real-time sandbox scanning of email attachments), and anti-impersonation and anti-phishing policies.
- Configure anti-malware, anti-spam, and outbound spam policies across Exchange Online.
- Configure audit logs, alert policies, and Defender for Office 365 threat policies.
- Apply Teams and external access policies to restrict guest and anonymous access to collaboration services.

Endpoint Enrolment

- Define mobility management strategy using Microsoft Intune Plan 1 for Mobile Device Management (MDM) and Mobile Application Management (MAM).
- Configure enrollment restrictions, device compliance policies, and app protection policies for Windows, iOS, Android, and macOS.
- Onboard devices using Windows Autopilot for zero-touch deployment and configure device onboarding profiles.

Endpoint Protection

- Configure Microsoft Defender for Business, including next-generation antivirus, behavioural-based protection, and cloud-delivered protection.
- Configure firewall rules, network protection, and web content filtering policies.
- Deploy Attack Surface Reduction (ASR) rules to reduce exploit vectors across Office applications, scripting engines, and email.
- Enable disk encryption via BitLocker for Windows devices, enforced through Intune compliance policies.
- Configure automated investigation and remediation to contain and resolve detected threats without manual intervention.
- Enable vulnerability management via Defender for Business to identify and track software vulnerabilities and misconfigurations on enrolled devices.

2. Deliverables

- Baseline security configuration across the Microsoft 365 environment
 - Secure Score review and documented security posture report
 - Implementation of identity protection, MFA, and Conditional Access policies
 - SPF, DKIM, and DMARC configuration for all active sending domains
 - Defender for Office 365 Plan 1 configuration: Safe Links, Safe Attachments, and anti-phishing policies
 - Email and application security hardening including anti-malware, anti-spam, and alert policies
 - Teams and external access policy configuration
 - Endpoint enrollment setup including Intune compliance policies and device onboarding
 - Endpoint protection configuration including Defender for Business, ASR rules, BitLocker encryption, and automated remediation
 - Vulnerability management configuration for enrolled devices
 - Ongoing monitoring, auditing, and alerting setup
 - Customised documentation and security posture reports
-

3. Expected Outcomes

- Reduced risk through strong identity and access controls with MFA and Conditional Access enforced across all users and devices
 - Improved resilience against phishing, malware, and email-based threats through Defender for Office 365 Plan 1 protections
 - Full device lifecycle security from zero-touch enrollment through active endpoint protection and automated remediation
 - Reduced attack surface through ASR rules, network protection, and legacy authentication blocking
 - Improved visibility into security incidents through centralised monitoring, audit logging, and alerting
 - 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 and will only be configured where the applicable licence is in place. Knovation Solutions will confirm licence eligibility during the Assessment & Roadmap phase.