
KNOVATION
SOLUTIONS
Microsoft Security
Optimization Service

Microsoft Security Gold Optimization Security Service

KNOVATION SOLUTIONS

Secure. Govern. Protect

Make Your Microsoft License Go Further

This service is scoped to Microsoft 365 Business Standard, Business Premium, F1,F3 and M365 E3 licence capabilities where applicable

Scope of Services

KNOVATION SOLUTIONS

Assessment & Roadmap

Establish
- cybersecurity frameworks
- identity strategy
- admin account strategy
- device management approach
- licensing
- notification contacts

Review
- Microsoft Secure Score
- Document baseline security posture across
  - identity
  - Email
  - Endpoint
  - 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.

Scope of Services continued

KNOVATION SOLUTIONS

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.

Endpoint Protection continued

- **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.

Deliverables

KNOVATION SOLUTIONS

Deliverables 1

- **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

Deliverables 2

- **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

Expected Outcomes

KNOVATION SOLUTIONS

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
Lifecycle Security	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
Security Compliance	Higher security compliance alignment with Center 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.

Microsoft Security Premium Optimization Service

KNOVATION SOLUTIONS

Secure. Govern. Protect

Make Your Microsoft License Go Further

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 Microsoft Managed Gold Security Service are included.

Scope of Services

KNOVATION SOLUTIONS

Advanced Identity Protection

Configure Privileged Identity Management (PIM)to enforce just-in-time and time-bound privileged role activation. accounts.
Configure access reviews to 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
Deploy Microsoft Defender for Identity to monitor on-premises Active 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
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.

Scope of Services continued

KNOVATION SOLUTIONS

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
Configure advanced anti-phishing tuning including custom impersonation protection thresholds, mailbox intelligence, and first-contact safety tips.
Extend DMARC configuration with DMARC policy enforcement and configure aggregate and forensic reporting.
Apply Teams restrictions including anonymous meeting join policies and external domain allow/block lists.

Endpoint Detection & Response (EDR)n

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.
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.

Scope of Services continued

KNOVATION SOLUTIONS

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

Deliverables

KNOVATION SOLUTIONS

Deliverables 1

- **Privileged** Identity Management (PIM) and access review configuration
- **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 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

Deliverables 2

- **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
- reports

Expected Outcomes

KNOVATION SOLUTIONS

Privledged Identities	Stronger protections for privileged identities through just-in-time access, access reviews, and risk-based Conditional Access
Proactive Detection	Proactive detection of compromised credentials through automated leaked credential monitoring and risk remediation
Data Governance	Enhanced data governance with automated classification, labelling, and DLP enforcement across all Microsoft 365 workloads
Data Leakage	Minimised data leakage risk across email, cloud apps, Teams chat, and managed endpoints
Secure AI	Secure and auditable usage of Microsoft Copilot with DLP enforcement, retention, and interaction audit trails

Expected Outcomes continued

KNOVATION SOLUTIONS

Spoofing Resistance	Higher phishing and spoofing resistance through advanced anti-phishing policies, DMARC enforcement, and automated email threat remediation
Full EDR	Improved endpoint threat detection and response capability with full EDR, automated investigation, and threat hunting
Visibility	Improved visibility into cloud application usage and insider risk through CASB controls and anomaly detection
Audit Capability	Extended audit trail and forensic investigation capability through Audit (Premium) and six-month endpoint data retention
Improved Compliance	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.

KNOVATION
SOLUTIONS