

Email Security Posture Assessment

ASSESSMENT

Delivered by Knovation Solutions

What it is: An email security audit that scans existing mailboxes for threats already sitting undetected, drawing on historical data going back up to 365 days. Uses artificial intelligence to understand sender intent, detecting social engineering attacks that have bypassed native filtering. Agentless assessment. No software to install.

When you use it: Where email filtering is in place but nobody has checked what has already made it through. Native and third-party filtering report on what they stop. This reports on what reached the inbox anyway, going back up to a year.

Capabilities

Historical Threat Discovery

- Scans mailbox history going back up to 365 days for threats that have already reached the inbox
- Surfaces attacks that passed through native and existing email filtering undetected
- No impact on mail flow or email performance during the scan

Account Takeover Detection & Response

- Monitors internal email patterns and login behaviour for anomalies
- Detects compromised accounts through behavioural analysis, not signature matching
- Automatically removes malicious messages sent from a compromised account

Impersonation & Social Engineering Detection

- Uses artificial intelligence to assess sender intent rather than relying on known signatures
- Detects business email compromise, conversation hijacking, and extortion attempts
- Identifies spear phishing crafted to bypass native Microsoft 365 filtering

Domain Fraud Visibility

- Assesses DMARC authentication status against the organisation's domain
- Identifies exposure to brand impersonation and domain spoofing
- Flags gaps in existing authentication configuration

Targeted User Exposure

- Breaks down detected threats by employee, threat type, and time period
- Identifies which users are most frequently targeted by attackers
- Informs where security awareness training should be prioritised

Compliance Visibility

- Delivers audit-ready evidence of email threat exposure without manual assembly
- Supports retention, e-discovery, and regulatory reporting requirements
- Structured reporting suitable for governance and board-level review

Automated Remediation

- Identified threats can be actioned directly from the findings report
- Issues are surfaced continuously during the scan, not discovered after the fact
- Findings feed directly into a prioritised remediation roadmap

Prerequisites for POC

Required

- Active Microsoft 365 tenant with Exchange Online in use
- One user account with Global Administrator privileges (required for historical mailbox access)

Optional (Extends Assessment)

- Extended mailbox retention or archiving enabled, to lengthen the historical scan window
- Multiple verified domains connected, for consolidated domain fraud reporting

Typical POC Timeline

- **Day 1:** Tenant access provisioning, administrator consent granted
- **Day 1-2:** Automated scan across up to 365 days of mailbox history
- **Day 3:** Findings review, threat report, and domain authentication posture review

Outcomes

You will have:

- Complete history of threats already sitting undetected in employee mailboxes
- Identification of business email compromise, conversation hijacking, and extortion attempts
- Breakdown of most targeted employees by attack type and time period
- Domain fraud and authentication posture assessment
- Account takeover risk exposure across the tenant
- Prioritised remediation roadmap
- Email security governance baseline for compliance reporting

Next step: Findings inform your email security strategy and feed into broader endpoint and network architecture decisions.

Closing

*We appreciate the opportunity to support your organisation in strengthening its email security posture.
Please contact us at info@knovation.co.za with any questions regarding this assessment.*