

Cloud Security Posture Assessment

ASSESSMENT

Delivered by Knovation Solutions

What it is: A cloud application security audit for Microsoft 365, Google Workspace, and 40+ other SaaS platforms. Discovers identity threats, data exposure vectors, misconfiguration risks, and insider-threat patterns across cloud environments. Agentless assessment. No software to install.

When you use it: Where the tenant has grown over time and how it is configured has never been independently reviewed. Cloud platforms are restrictive by default in some respects and permissive by default in others. This establishes which is which in your environment, and who has been given access along the way.

Capabilities

Shadow IT Discovery

- Discovers all cloud applications and OAuth-connected integrations across the organisation
- Identifies unauthorised SaaS tools and AI applications in use
- Detects which applications carry risk and enforces application use policies

Identity Threat Detection and Response (ITDR)

- Monitors user and account behaviour across SaaS platforms
- Detects compromised accounts, MFA bypass, impossible travel, and suspicious activity
- Automatically revokes access or enforces controls in real time

Misconfigurations

- Identifies default settings, overly permissive sharing, and configuration drift
- Detects easy entry points that attackers exploit without sophisticated hacking
- Auto-fix available for common misconfiguration violations

SaaS Posture Management

- Continuously monitors cloud application configurations against security best practices
- Detects risky settings, over-permissive sharing, and configuration drift
- Automatically remediates identified issues

Data Exposure Detection

- Inventories shared files and folders across cloud platforms
- Identifies files shared externally and oversharing scenarios
- Auto-fix available for risky external access and oversharing rules

Compliance Visibility

- Pre-configured policy mappings to CIS Controls, NIST CSF, and SOC 2
- Delivers audit-ready evidence without manual assembly
- Built-in reporting for compliance frameworks

Automated Remediation

- Bulk remediation across all environments
- Issues are fixed continuously, not discovered weeks later during periodic audits

Prerequisites for POC

Required

- Microsoft 365 Business Basic subscription licence (or higher) for the tenant being assessed
- One user account with these roles:
 - Global Reader
 - Privileged Role Administrator
 - Exchange Administrator
 - Application-specific administrator roles (for example, Teams Administrator and SharePoint Administrator)
- Alternatively, a single Global Administrator account can be used
- Google Workspace admin account (for external sharing inventory)

Typical POC Timeline

- **Day 1:** Role assignment, platform access provisioning
- **Day 2-3:** Tenant integration followed by automated discovery and assessment across tenant
- **Day 4:** Findings review, misconfiguration audit and data exposure report

Outcomes

You will have:

- Complete inventory of cloud applications and SaaS tools in active use
- Identification of unauthorised applications and AI tools creating data exposure
- Compromised account detection: impossible travel, MFA bypass attempts, suspicious activity
- Data exposure assessment across cloud platforms (files, external sharing, oversharing)
- Configuration drift audit: settings and policies deviating from security best practices
- Compliance evidence ready for CIS Controls, NIST CSF, and SOC 2 reporting
- Prioritised remediation roadmap with auto-fix recommendations
- Cloud governance baseline for ongoing compliance tracking

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

Closing

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