



The cloud makes work easier – and breaches easier too.

Our Cloud Security Services help you secure your cloud platforms by identifying misconfigurations, improving access controls, and applying best-practice policies tailored to your environment and risk profile.

What Are Cloud Security Services?

Your data, email, apps, and user identities are now hosted in the cloud – but are they configured securely? Cloud platforms offer powerful security controls, but they require tuning, monitoring, and proper implementation.

We assess and secure environments like:

- **Microsoft 365** (including Exchange Online, SharePoint, Teams, and Azure AD)
- **Google Workspace** (Gmail, Drive, Docs, Admin Console)
- **Amazon Web Services (AWS)**
- **Microsoft Azure**
- **Hybrid or multi-cloud setups**

What We Do

Cloud Security Assessment

- Review current cloud configurations against best practice (CIS Benchmarks, Microsoft Secure Score, AWS Well-Architected, etc.)
- Assess risks across identity, access, logging, encryption, data loss prevention, and admin control
- Identify misconfigurations, legacy accounts, and over-permissioned users
- Score your environment's risk posture

Recommendations & Remediation Plan

- Prioritised action plan tailored to your risk tolerance and business operations
- Quick wins and long-term improvement areas
- Optional implementation support

Policy & Governance Uplift

- Secure configuration baselines for cloud platforms
- Cloud usage and access control policies
- Support for compliance frameworks: Essential Eight, ISO 27001, NIST, ISM





Common Cloud Security Issues We Fix

- Shared admin accounts with no MFA
- Excessive user permissions or "shadow IT"
- Insecure mail forwarding or inbox rules
- Lack of data loss prevention (DLP) or audit logging
- Weak device controls for BYOD/laptops
- Unmonitored third-party app integrations

Who This Is For

- **SMBs** that have migrated to Microsoft 365 or Google Workspace but haven't reviewed security
- **Councils or NFPs** looking to align their cloud security with ISM or Essential Eight
- **Organisations** pursuing ISO 27001 or privacy compliance (e.g., OAIC, GDPR, HIPAA)
- **Teams** concerned about ransomware, account takeovers, or phishing

What Our Clients Say

"We assumed Microsoft 365 was secure by default — until vCISO.One showed us where we were exposed. Their review helped us tighten controls and meet insurance requirements."

— General Manager, Mid-Sized Construction Firm

Outcomes You Can Expect

- ✓ Improved Microsoft Secure Score or AWS Well-Architected rating
- ✓ Reduced risk of account compromise and phishing
- ✓ Aligned cloud setup with compliance frameworks
- ✓ Greater visibility and control across users, apps, and devices
- ✓ Confidence that your data is protected — wherever it's stored

Optional Add-Ons

- Cloud backup configuration and validation
- Email phishing protection (DMARC, SPF, DKIM setup)
- SSO and identity federation reviews
- Ongoing monitoring via MSS or vCISO support
- Policy development for cloud governance

Don't Leave Cloud Security to Chance

Let's secure your cloud environment before someone else finds the gaps.

[Schedule a Cloud Security Review](#)