M365 SECURITY ASSESSMENT

Overexposure by Default

M365 Security Gaps Are Now Business Problems

How your Microsoft 365 tenant shapes operational impact:

Microsoft 365 is where your users live, your data flows, and attackers hunt. With over a million businesses on the platform, threat actors have turned M365 misconfigurations into a primary path to ransomware, wire fraud, and data breaches. Microsoft secures the platform. You own the configuration.

Your tenant configuration sits in the middle.
When MFA is inconsistent, mail rules are unmonitored, and sharing is wide open, leadership sees an environment that is hard to defend and even harder to explain after an incident.

eSurelTy's M365 Security Assessment connects your Microsoft 365 configuration to real-world attack patterns and control expectations, so you can prove security posture, not just hope nothing breaks.

Default–Collaborative. Over-Exposed. Exploited Accordingly

Carriers and underwriters increasingly expect Microsoft 365 to demonstrate:

- Strong MFA and conditional access across all users
- Tight control of admin roles and privileged groups
- Email controls that materially reduce BEC and phishing risk
- Logging, retention, and alerting that support forensics
- Sensible external sharing patterns and DLP coverage

If your answers are vague—or your evidence is thin—insurers assume more risk than your IT team does. That gap is where pricing pressure, exclusions, and claim challenges start.

eSurelTy's M365 Security Assessment is built to close that gap.

Default–Collaborative. Over-Exposed. Exploited Accordingly.

Microsoft 365 is built to make sharing effortless. Without deliberate hardening, the very features that power collaboration become evidence of weak security control:

- Weak authentication posture – Users without enforced MFA or conditional access; legacy auth still enabled.
- Unrestricted data sharing – Files and sites shared externally with no expiration, encryption, or governance.
- Over-privileged admin and service accounts – Global admins, app owners, and service principals with excessive rights and no monitoring.
- Inconsistent logging and auditing – Gaps in mailbox, SharePoint, and Teams logging that break incident reconstruction.
- Email spoofing and phishing exposure – Incomplete SPF, DKIM, and DMARC, plus lax mail-flow rules that enable business email compromise.

For organizations subject to HIPAA, PCI, GDPR, or state privacy laws, these weaknesses are not just IT issues. They become drivers of audit findings, regulatory scrutiny, and customer distrust.

Contact Us

info@eSurelTy.com

www.eSurelTy.com

What Your Tenant Reveals About Security Maturity

Modern security, audit, and compliance reviews increasingly expect Microsoft 365 to demonstrate:

- Strong MFA and conditional access for all users.
- Tight control of admin roles and privileged groups.
- Email controls that meaningfully cut BEC and phishing risk.
- Logging, retention, and alerting that enable real forensics.
- Sensible external sharing with effective DLP.

If your answers or evidence are vague, reviewers assume your controls are weaker than IT thinks—and that's where findings and escalations start. eSureITy's M365 Security Assessment closes that gap.

Deliverables That Strengthen Security And Governance

You don't need another checklist. You need artifacts that hold up with leadership, auditors, and the board.

Microsoft 365 Security Risk Report

- Clear risk summary mapped to Secure Score and CIS benchmarks
- Prioritized findings by severity and business/regulatory impact
- Evidence packs ready for risk committees, audits, and regulators

Remediation & Compliance Roadmap

- Concrete configuration changes for identity, email, and collaboration
- Recommendations aligned to NIST, ISO, and modern review expectations
- Milestones that show measurable progress

Ongoing Risk Posture Support (Optional)

- Periodic reassessments to track Secure Score and control improvement
- Drift reviews before major changes, platform updates, or audits

From "We Think We're Secure" To "We Can Prove It"

After an eSureITy Microsoft 365 Security Assessment, you get:

- Verified configuration against recognized baselines
- Higher Secure Score and better regulatory alignment
- A defensible audit trail for governance and audits
- Lower risk of credential compromise, BEC, and M365-based breaches

It's not just email hardening; it's protecting your brand, data, and ability to stay operational under pressure.

Risk-Based M365 Security Assessment Built For Assurance Outcomes

Authentication & access

- MFA coverage by user and role
- Conditional Access, break-glass accounts, session controls
- Password policies, legacy protocols, external access

Identity & roles

- User/group structures, high-risk and stale accounts
- Admin roles, delegated permissions, directory sync risks
- Service principals, app registrations, privilege creep

Email & content security

- Mail flow rules affecting spoofing and BEC
- Anti-phishing, anti-malware, safe links/attachments
- DLP for PHI/PII, payments, regulated data

Apps & integrations

- Third-party app permissions and OAuth consent
- Legacy protocols and insecure access paths

Data protection & collaboration

- Encryption and retention for OneDrive, SharePoint, Teams
- External sharing, anonymous links, guest access

Mobile & endpoints

- Intune configuration, device compliance, Conditional Access tie-in

Logging & monitoring

- Unified audit log configuration and retention
- Alerts tied to identity, email, and data-movement events

Why eSureITy

- Risk alignment first – Built around what decision makers actually ask, measure, and challenge.
- Certified expertise – CISSP, CEH, CISA, and M365 Security Administrator practitioners who speak both tech and high-stakes review language.
- Standards-based method – Uses Secure Score, CIS, and NIST 800-53 to produce evidence that holds up to scrutiny.
- Clear for execs and engineers – Board-ready narratives plus technical depth that keep IT, security, risk, and compliance aligned.

Protect your Microsoft 365 environment—and meet the control expectations many cyber insurance carriers now treat as prerequisites for coverage. Schedule an eSureITy M365 Security Assessment review and see exactly how your tenant configuration stands up against modern threats and security benchmarks.

Contact Us
info@eSureITy.com
www.eSureITy.com