QUISITIVE

Cloud Security Checklist

Addressing the Top 5 Critical Gaps in Your Azure and Microsoft 365 Environments

We've conducted thousands of Microsoft 365 and Azure security assessments—and the same issues keep showing up.

Use this checklist to identify and address the top five vulnerabilities putting your cloud environment at risk.

1. Block Legacy Authentication

- ☐ Legacy authentication protocols are disabled *(e.g., POP, IMAP, SMTP)*
- ☐ Conditional Access rules block legacy auth attempts
- ☐ Modern authentication is enforced across all services

99% of password spray attacks involve legacy authorization

Microsoft

2. Enforce Multi-Factor Authentication (MFA)

- ☐ Admin and high-privilege accounts have MFA enforced
- ☐ Authenticator apps or phishing-resistant methods are used *(e.g., FIDO2)*
- ☐ Legacy MFA exclusions have been reviewed and removed

MFA can block **99.2%** of account attacks

Microsoft

3. Implement Strong Conditional Access Policies

- ☐ Policies are scoped to all users and apps
- ☐ Legacy auth is blocked through Conditional Access
- ☐ Policies include location, device compliance, and sign-in risk conditions
- ☐ Break-glass accounts are excluded but monitored
- ☐ Regular review and testing of policies is in place

Conditional Access is the foundation of a Zero Trust model

Microsoft

4. Enable Vulnerability Scanning & Auditing

- ☐ Microsoft Defender for Cloud is enabled and configured
- ☐ VM, container, and app layer vulnerability scanning is active
- ☐ Secure Score is monitored and acted upon
- ☐ Alerts and incidents are triaged regularly
- ☐ Export of audit logs and security data is enabled for SIEM

75% of cloud security failures will result from poor management of configurations and identities

Gartner

5. Use Privileged Identity Management (PIM)

- ☐ PIM is enabled for all privileged roles *(Owner, Global Admin, etc.)*
- ☐ MFA is required to activate privileged roles
- ☐ Role assignments are time-limited and require justification
- ☐ Activation notifications and approval workflows are enabled
- ☐ Access reviews are scheduled and enforced

PIM helps enforce least privilege and just-in-time access.

Next Step: Get a Pro Assessment

Want help securing your Microsoft 365 or Azure environment? Our experts can identify your risks and build a prioritized action plan.

Book a Cloud Security Assessment

No time to tackle these tasks?

We can help! Learn more about [Quisitive Security Services]

Microsoft MSSP

Member of Microsoft Intelligent Security Association

Microsoft Security