Kaseya 365
User

8 must-have controls for Microsoft 365 & Google Workspace

A SaaS security checklist

Microsoft 365 and Google Workspace are indispensable tools for modern organizations due to their convenience, flexibility and scalability. However, these SaaS platforms are also prime targets for phishing, ransomware and identity-based attacks because of the large volumes of business-critical information they store. To stay resilient, IT and security teams must go beyond native platform settings and implement layered controls that prevent compromise, accelerate threat detection and ensure rapid data recovery when it matters most.

This checklist presents eight vital controls every MSP and IT leader should implement now to reinforce SaaS defenses and protect both business and client environments.

1 Enforce MFA for everyone

MFA is one of the most effective defenses against identity compromise and account takeover attacks.

- ☐ **Implement:** Require MFA for all users. Make phishing-resistant authentication methods, such as hardware security keys (FIDO2), mandatory for admins to further strengthen protection.
- ☐ **Check:** Regularly audit and verify that all admin and break-glass (emergency access) accounts have strong MFA enforcement.
- ☐ **Monitor:** Look for MFA-disabled events or sudden spikes in failed MFA attempts.

2 Block legacy authentication

Legacy authentication methods, such as Internet Message Access Protocol (IMAP) and Post Office Protocol 3 (POP3), are among the most exploited entry points for business email compromise (BEC) and credential-based attacks.

- [ ] **Implement:** Disable basic authentication across all Microsoft 365 and Google Workspace services and restrict IMAP/POP access to OAuth-based connections only.
- [ ] **Check:** Attempt to log in to Microsoft 365 and Google Workspace services using basic authentication to verify that it is denied.
- [ ] **Monitor:** Watch for repeated or high-volume legacy authentication attempts.

3 Use Conditional Access/Context-Aware Access

Conditional Access in Microsoft 365 or Context-Aware Access in Google Workspace blocks risky login attempts and enforces step-up authentication to reduce unauthorized access, while creating a seamless user experience.

- [ ] **Implement:** Define access policies based on business context and risk level. Apply device, location and risk-based access rules.
- [ ] **Check:** Regularly assess policies by performing test logins from unmanaged devices or unapproved locations.
- [ ] **Monitor:** Check for risky sign-in events and conditional access policy changes.

4 Adopt least privilege and just-in-time security practices

By adopting least privilege and just-in-time (JIT) security practices, businesses can significantly reduce the attack surface and limit the damage if admin credentials are compromised.

- [ ] **Implement:** Minimize the number of permanent administrative accounts and replace always-on administrative access rights with JIT or Privileged Identity Management (PIM) elevated privilege.
- [ ] **Check:** Regularly review the number of standing administrative accounts across Microsoft Entra ID (Azure AD) and Google Workspace Admin Console.
- [ ] **Monitor:** Watch out for new role assignments, privilege escalations and elevation requests.

5 Govern app consent and OAuth access

Malicious OAuth applications have become a significant data exfiltration vector, allowing attackers to gain persistent access to corporate data without detection.

- [ ] **Implement:** Require administrator approval for all high-risk permissions and restrict the use of unverified apps.
- [ ] **Check:** Regularly review OAuth consent logs and app permissions to confirm that all high-risk scopes are routed through an administrative approval process.
- [ ] **Monitor:** Watch for new OAuth grants and set up alerts for apps requesting excessive permissions.

6 Enable anti-phishing and email authentication (DMARC/DKIM/SPF)

Implementing a layered approach that combines advanced anti-phishing controls with domain-based email authentication, such as Domain-based Message Authentication, Reporting & Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF), helps prevent BEC, impersonation and inbound spoofing.

- [ ] **Implement:** Enable advanced phishing protection features, such as email filtering, link scanning and impersonation detection.
- [ ] **Implement:** Enforce DMARC to authenticate emails and take appropriate actions, such as delivering, quarantining or rejecting messages that fail SPF or DKIM checks.
- [ ] **Check:** Perform controlled phishing simulations and domain spoofing tests to verify that all protections are working properly.
- [ ] **Monitor:** Track phishing detections and DMARC authentication failures to support faster responses to emerging security threats.

7 Use SaaS backup and perform quarterly restore tests

Microsoft 365 and Google Workspace SLAs only guarantee service availability, not data recovery. They do not protect against data loss due to accidental or malicious deletion, misconfiguration or ransomware.

- [ ] **Implement:** Use a reliable SaaS backup solution that covers mailboxes, calendars, contacts and file repositories such as OneDrive, SharePoint and Google Drive.
- [ ] **Check:** Conduct quarterly restore exercises to verify data integrity and ensure your recovery plan works as expected.
- [ ] **Monitor:** Closely monitor incomplete backups and failed restore validations to ensure issues are identified and fixed promptly.

8 Clean up user and guest accounts

Regularly removing unused identities and open guest access reduces your attack surface and strengthens overall identity hygiene.

- [ ] **Implement:** Automate the discovery and removal of inactive user accounts.
- [ ] **Implement:** Enforce guest account expiration dates.
- [ ] **Check:** Generate monthly reports identifying stale, inactive and guest accounts across your SaaS environment.
- [ ] **Monitor:** Watch out for a sudden increase in inactive user counts, expired guest accounts that remain active or unusual logins from old accounts.

Strengthen Microsoft 365 and Google Workspace security with Kaseya 365 User

Achieving all eight controls doesn't have to be complex or time-consuming. Kaseya 365 User unifies prevention, response and recovery across Microsoft 365 and Google Workspace — from GenAI-powered email security and automated SaaS threat detection and response to effortless backup and recovery. Explore how Kaseya 365 User can help your team save time, close security gaps and scale protection with confidence.

Learn more

Kaseya®