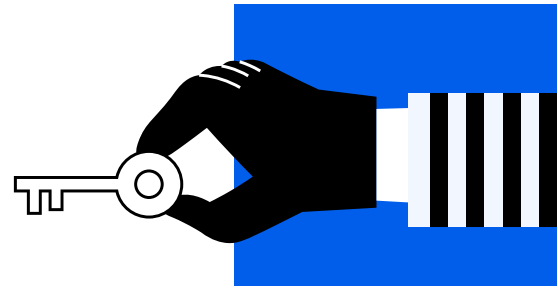


Quick Guide To Cybersecurity For Google Admins



Enterprises face escalating cyber threats targeting proprietary data, intellectual property, and financial information in Google Workspace. This guide outlines 10 essential security measures with clear priorities to help you build a layered defense against sophisticated attacks.

START HERE: Identity & Access (measures 1-2), then layer in Data Protection (3-4), and expand from there.

Common Threats Targeting Enterprises



- **Misconfiguration & Data Breaches:** Attackers exploiting overly permissive file-sharing settings
- **Targeted Phishing & Ransomware:** AI-enhanced campaigns against executives leading to account takeovers
- **Insider Risks:** Accidental exposure or malicious misuse by current or departing employees
- **Advanced Persistent Threats (APTs):** Sophisticated infiltration of privileged administrator accounts
- **Shadow IT Risk:** Unvetted third-party apps gaining excessive access to corporate data

10 Essential Security Measures



PRIORITY 1: Identity & Access Foundation

1. Identity & Access Foundation

- Use advanced firewalls and intrusion detection systems.
- Regularly patch applications and endpoints.
- Enforce strong password policies and mandatory multi-factor authentication.

2. Access Control and Least Privilege

- Apply Role-Based Access Control (RBAC) so users only have access aligned to their role.
- Audit and restrict privileged accounts regularly.
- Automate onboarding and offboarding to close access gaps quickly.

PRIORITY 2: Protect Your Data

3. Data Protection and File Sharing Governance

- Encrypt sensitive data in transit and at rest.
- Audit Drive file-sharing activity regularly.
- Identify externally owned files and sensitive document sharing across your domain.

4. Third-Party App Governance

- Review connected third-party apps in Google Workspace.
- Block high-risk or unused applications.
- Apply granular rules to balance productivity with security.



10 Essential Security Measures

PRIORITY 3: Monitor and Respond

5. Threat Prevention and Real-Time Monitoring

- Deploy enterprise-grade anti-malware and endpoint protection.
- Continuously monitor account activity for suspicious logins or bulk downloads.
- Automate policy enforcement to reduce response times.

6. Workforce Awareness

- Run regular phishing simulations and employee security training.
- Define clear security and device use policies for remote and hybrid teams.

7. Mobile and Remote Work Security

- Secure every endpoint with MDM controls such as remote wipe, encryption, and strong authentication.
- Maintain visibility over browser activity across distributed teams.

PRIORITY 4: Prepare for the Worst

8. Incident Response and Business Continuity

- Create and maintain an enterprise incident response plan.
- Test response procedures regularly with tabletop exercises.
- Implement secure, automated data backups for all critical assets.

9. Compliance and Auditing

- Align with GDPR and other enterprise compliance standards through continuous auditing.
- Monitor activity across Drive, Gmail, Meet, and more to surface potential exposure risks.

10. Ongoing Policy Updates and Education

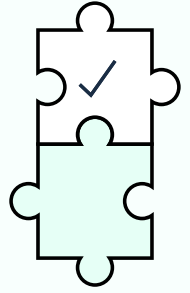
- Review and update policies regularly to reflect evolving threats.
- Communicate policy changes clearly across all teams.

0100100110
1100010010
100110010



10 Essential Security Measures

30-Day Quick Start Checklist



Week 1: Audit multi-factor authentication adoption and privileged account access

Week 2: Conduct a Drive file-sharing audit and remove public or external links

Week 3: Review third-party app connections and block risky integrations

Week 4: Test your incident response plan with a tabletop exercise

How GAT Labs Helps Enterprises Build Cyber Resilience

Google Workspace provides a strong foundation for security, but at enterprise scale, native tools leave critical blind spots. Large organizations need deeper visibility, centralized control, and automated enforcement across thousands of users.

That's where GAT Labs comes in.

Our suite of tools helps enterprise Google Admins go beyond visibility and take direct, large-scale action:

- **GAT+:** Comprehensive auditing across Drive, Gmail, Meet, and more. Identify data exposure, track permissions, and automate reporting for compliance.
- **GAT Flow:** Automate onboarding, offboarding, and access management to keep identity security tight at every stage of the user lifecycle.
- **GAT Shield:** Monitor browser activity, detect unusual behavior, and block risky downloads in real time.

Together, GAT Labs gives enterprises what Google Workspace alone cannot: complete visibility, automated enforcement, and the ability to act instantly across your entire domain, before small misconfigurations become major breaches.