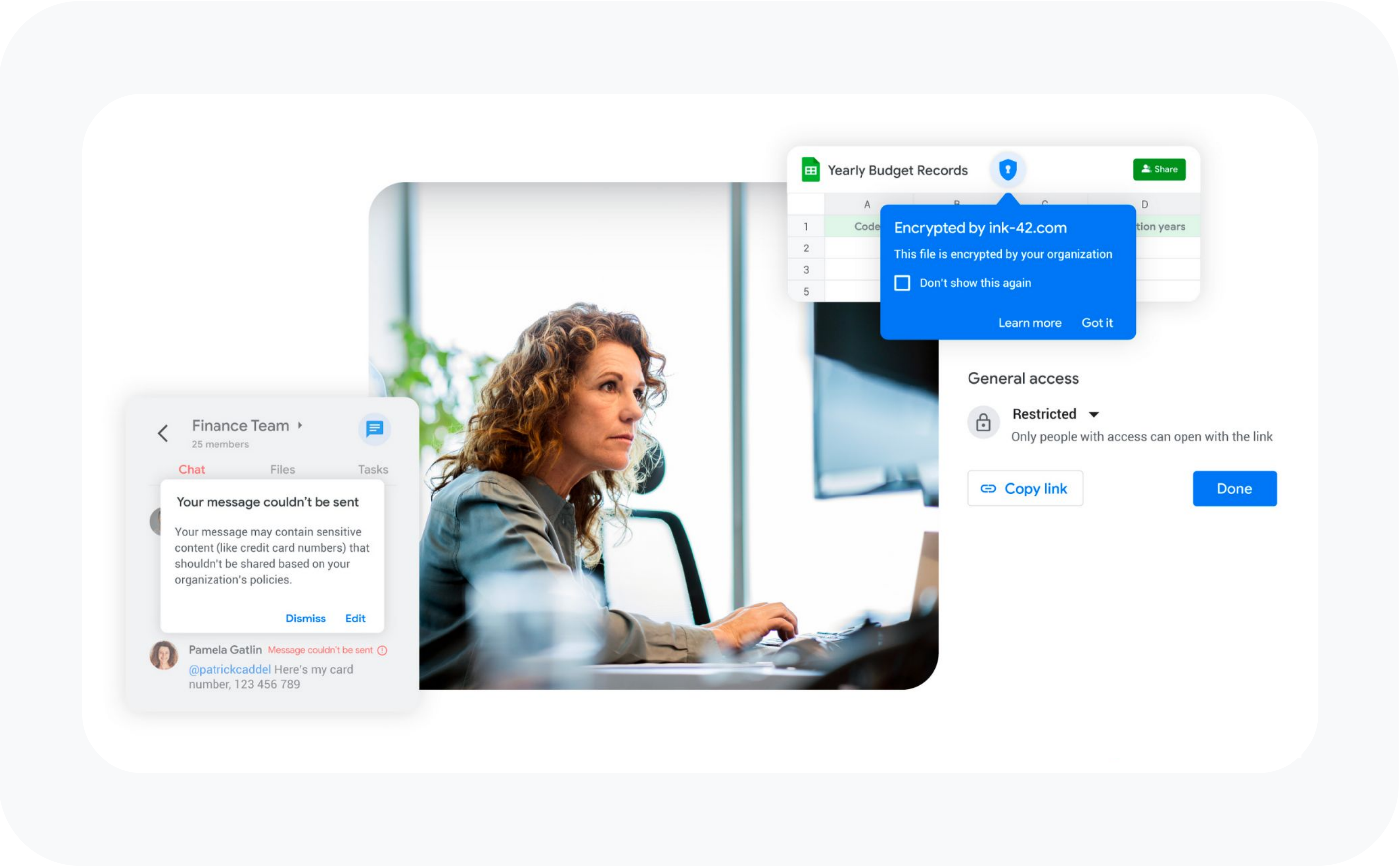
Google Workspace

Zero trust best practices guide for U.S. public sector agencies

Disclaimer: This guidebook applies to Google Cloud and Google Workspace products described at cloud.google.com and workspace.google.com. The content contained in this guidebook is current as of March 2024 and represents the status quo as of the time it was written. References to forthcoming features are annotated as such and do not constitute a commitment to a specific release schedule. Google's security policies and systems may change going forward, as we continually improve protection for our customers. The availability of the product features and capabilities described in this paper are subject to license availability of various Google Workspace editions and Google Cloud product offerings.



Your message couldn't be sent

Your message may contain sensitive content (like credit card numbers) that shouldn't be shared based on your organization's policies.

Pamela Gatlin Message couldn't be sent

@patrickcaddel Here's my card number, 123 456 789

Encrypted by ink-42.com

This file is encrypted by your organization

□ Don't show this again

General access

Restricted

Only people with access can open with the link

✨ 90 ✌🏾 29

Introduction

As a cloud-first and cloud-native solution, Google Workspace is a pioneer in zero trust. Google enforces critical access controls based on information about a device and its state and the associated user and their context. This approach considers both internal and external networks to be inherently untrusted, and we dynamically evaluate user access throughout their journey.

This guide is designed to provide a set of best practices to leverage Google Workspace security and compliance controls to align Google Workspace deployments with the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0. This guide is not exhaustive. It's a starting point to highlight key features and configurations within Google Workspace that align with CISA's zero-trust principles.

About the Zero Trust Security Model

Client-side encryption in Gmail was built with openness and interoperability in mind. The underlying technology being used is S/MIME, an open standard for sending encrypted messages over email. S/MIME is already supported in most enterprise email clients, so users are able to communicate securely, outside of their domain, regardless of what provider the recipient is using to read their mail. S/MIME uses asymmetric encryption, the public key and the email of each user are included in the user's S/MIME certificate. Similar to the Transport Layer Security (TLS) protocol used for HTTPS, each certificate is digitally signed by a chain of certificate authorities up to a broadly trusted root certificate authority. The certificate acts as a virtual business card, enabling anyone getting it to encrypt emails for that user. The user's private keys are kept secure under customer control, and are

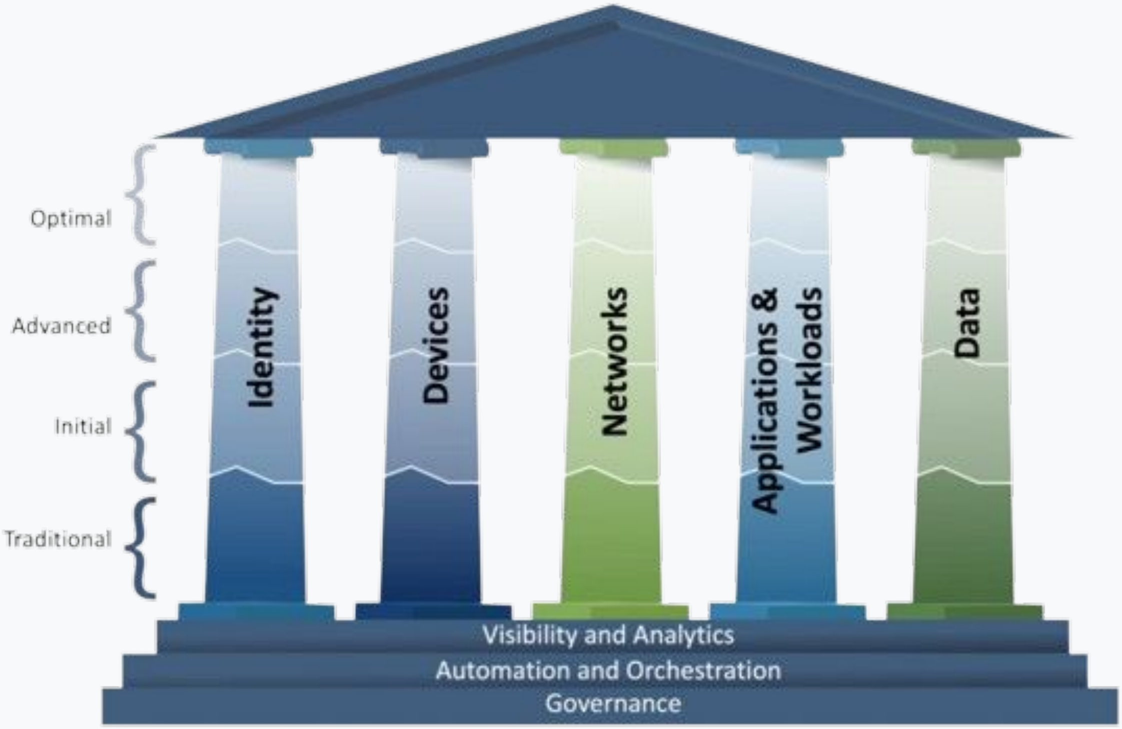
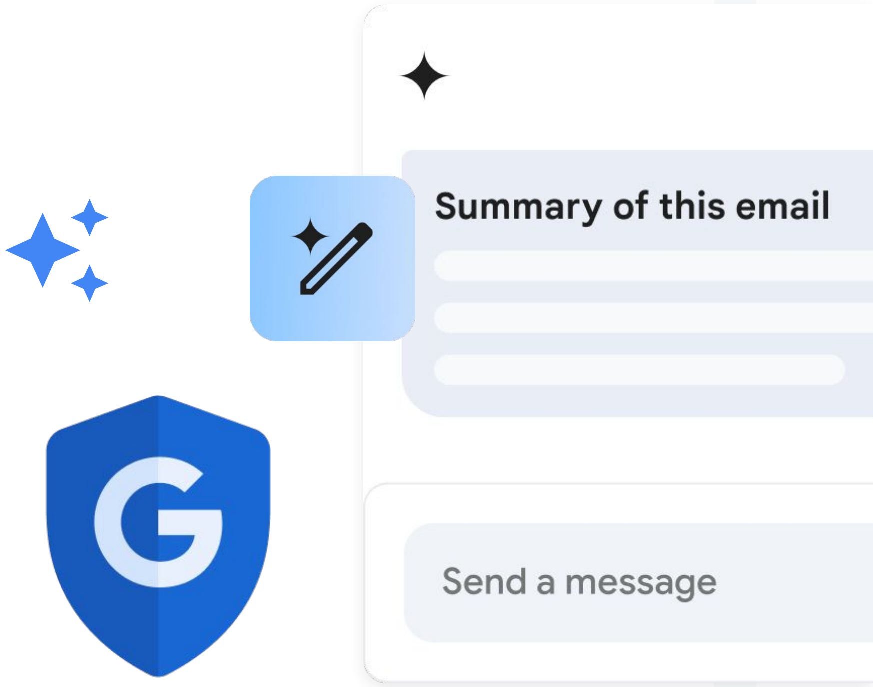


Figure 3: Zero Trust Maturity Evolution; page 9

Zero-trust maturity varies from agency to agency. The model outlines a path to mature from traditional security postures to an optimal state. Across the pillars, high degrees of interoperability and automation characterize the advanced and optimal states.

Google Workspace best practices



Identity ✉

CISA guidance

Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities. Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

ZTMM Identity, section 5.1, page 13

Identity management in Google Workspace

As a Google Workspace administrator, you can configure many tools to meet the security and system-integration requirements of your organization. You can set up authentication features, such as 2-Step Verification and single sign-on, and email security, such as TLS to encrypt email for privacy.

TIP

Monitor sign-in activity, including 2-Step Verification enrollment and suspicious behavior, with User log events. You can also access pre-configured security reports and analyze data using the Reports API.

Identity best practices and considerations

- If you use a third-party identity provider, such as Microsoft Azure Active Directory or Okta, to authenticate users, you can set up SAML-based single sign-on.
- With a catalog of over 200 pre-integrated SAML apps, configure your users' cloud apps to use SAML 2.0. Then, they can use their Google Workspace credentials and sign in once for all cloud apps.
- Google’s Secure LDAP service provides a simple and secure way to connect your LDAP-based applications and services to Cloud Identity or Google Workspace.
- You can make 2-Step Verification optional or required for your users. We recommend enforcing 2-Step Verification for your administrator account and users who work with your most important business information. Google Workspace supports several methods of 2-Step Verification, including hardware and software-based security keys.

Devices

CISA guidance

Devices may be agency-owned or bring-your-own-device (BYOD) property of employees, partners, or visitors. Agencies should secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and associated vulnerabilities as they become known.

ZTMM, Devices, section 5.2, page 16

Device management in Google Workspace

Use Google endpoint management to help protect corporate data on users' personal devices and your organization's company-owned devices. Users get secure access to Google Workspace services, and you can set policies to keep devices and data safe. You can require screen locks and strong passwords and wipe devices to erase confidential data. Control Android and iOS devices as well as block access to specific Windows, ChromeOS, Linux, and MacOS sessions.

TIP

Consider browser management to enhance security with Chrome Browser Cloud Management. Across devices, you can configure extension access workflows, managed browser reporting, and centrally control Chrome Browser security policy.

Beyond Corp Enterprise brings threat and data protection to the Chrome browser, centrally managed from the Google Workspace admin console. BCE also provides tooling to extend device access policies beyond Workspace, to protect other SaaS apps, private web apps, and cloud resources.

Device management best practices and considerations

- For granular asset and policy requirements, configure advanced management controls to take advantage of features, such as device inventory and approvals, security policies, and strong password enforcement.
- Using Context-Aware Access, you can create security policies for apps based on attributes, such as user identity, location, device security status, and IP address.
- Leverage Beyond Corp Alliance partners to make granular access decisions based upon device security posture.
- Define custom rules or use our templates to automate device management tasks and get security alerts. For example, you can automatically block devices that report suspicious activity.

Networks

CISA guidance

ZTAs enable a shift away from traditional perimeter-focused approaches to security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity, and enhance enterprise-wide network visibility. ZTAs permit security controls to be implemented closer to the applications, data, and other resources and augment traditional network-based protections and improve defense-in-depth. Each application can be treated uniquely by the network for its demands on access, priority, reachability, connections to dependency services, and connection pathways. These network application demands can be captured as an application profile, and repeated profiles can then be treated as a traffic class.

ZTMM Networks, section 5.3, page 20

Google’s global network

Google’s approach to network security includes multiple layers of controls that protect Google’s network from external attacks. It starts with industry-standard firewalls and access control lists (ACLs) to enforce network segregation and route all traffic through custom Google Front End (GFE) servers to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally. This “default deny” configuration prevents GFE servers from accessing unintended resources. Finally, logs are routinely examined to reveal any exploitation of programming errors and to make sure access to networked devices is restricted to authorized personnel. The bottom line? Only authorized services and protocols that meet our security requirements are allowed to traverse our network. Anything else is automatically dropped.

Encryption is an important part of our approach to network security. Data stored “at rest” is encrypted on disks and backup media. We also encrypt all data in transit while it’s traveling over the internet and across the Google network between data centers. Learn more in How Google Workspace uses encryption to protect your data.

Network best practices and considerations

- When using Google services, your organization’s data is protected by one of the world's safest and most invested-in networks.

🔔 **TIP**

As part of Google's long-term commitment to security and transparency in the delivery of our services, you can use Access Transparency to review logs of actions taken by Google staff when accessing user content, including:

- Actions by the Support team that you may have requested by phone
- Basic engineering investigations into your support requests
- Other investigations made for valid business purposes, such as recovering from an outage

Learn more about Access Transparency.

Applications and Workloads

CISA guidance

Agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats. Per OMB M-22-09, agencies should begin to explore opportunities to make their applications available over public networks to authorized users. Best practices for DevSecOps and CI/CD processes, including the use of immutable workloads, should also be adopted to the extent possible. Agencies should explore options to shift their operations away from a focus on accreditation boundaries and updating ATOs to supporting applications as if they are externally facing and provide commensurate security.

ZTMM, Applications and Workloads, section 5.4, page 23

Google's approach to application and workload security

As a cloud-based business application solution provider, our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy)
- SOC 2 and SOC 3 reports

Google also participates in sector and country-specific frameworks, such as FedRAMP (U.S. government) and the Secure Cloud Business Applications (SCuBA) Project from CISA.

Application and workload best practices and considerations

- Review compliance offerings to see the list of U.S.-based regulations and frameworks with which Google Workspace supports compliance.
- Configure third-party and internal app access to your organization's Google Workspace data to protect your users and sensitive data. Learn more.

TIP

It's important to make sure applications authorized to access your Google Workspace data are trusted. To make this easier, Google Workspace has a verification process to help provide confidence and consistency regarding security and privacy. For details, go to What is a verified third-party app?.

Data

CISA guidance

Agency data should be protected on devices, in applications, and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data; protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise.

ZTMM, Data, section 5.5, page 26

Google's approach to data security

Least-privilege access is at the heart of how Google Workspace protects customer data. Our highly interoperable tooling enables you to programmatically and automatically identify, classify, and label sensitive information. As a Google Workspace administrator, you can govern how your organization's data is accessed. Data preservation, retention, and deletion can be configured based on attributes, such as Google Drive item classification. You can then review detailed log event data in the security investigation tool or through the Reports API. For more complex analysis, you can use BigQuery and Chronicle.

Data best practices and considerations

- (Beta) Leverage Google's strength in AI to automatically and continuously inventory and classify data in Google Drive to help ensure data is appropriately identified and protected from exfiltration.
- Create fine-grain internal and external sharing boundaries with Drive trust rules.
- Govern the external sharing of sensitive information with data loss prevention (DLP) rules.
- Configure context-based access control policies leveraging Context Aware Access.

TIP

You can monitor data access, mutations, and permission changes with Drive log events and track your users' attempts to share sensitive data with Rule log events. For more robust analysis, such as monitoring for irregular behavior and data exfiltration, consider collecting Google Workspace logs by setting up a Chronicle export.

❤️ 12 ✌️ 24