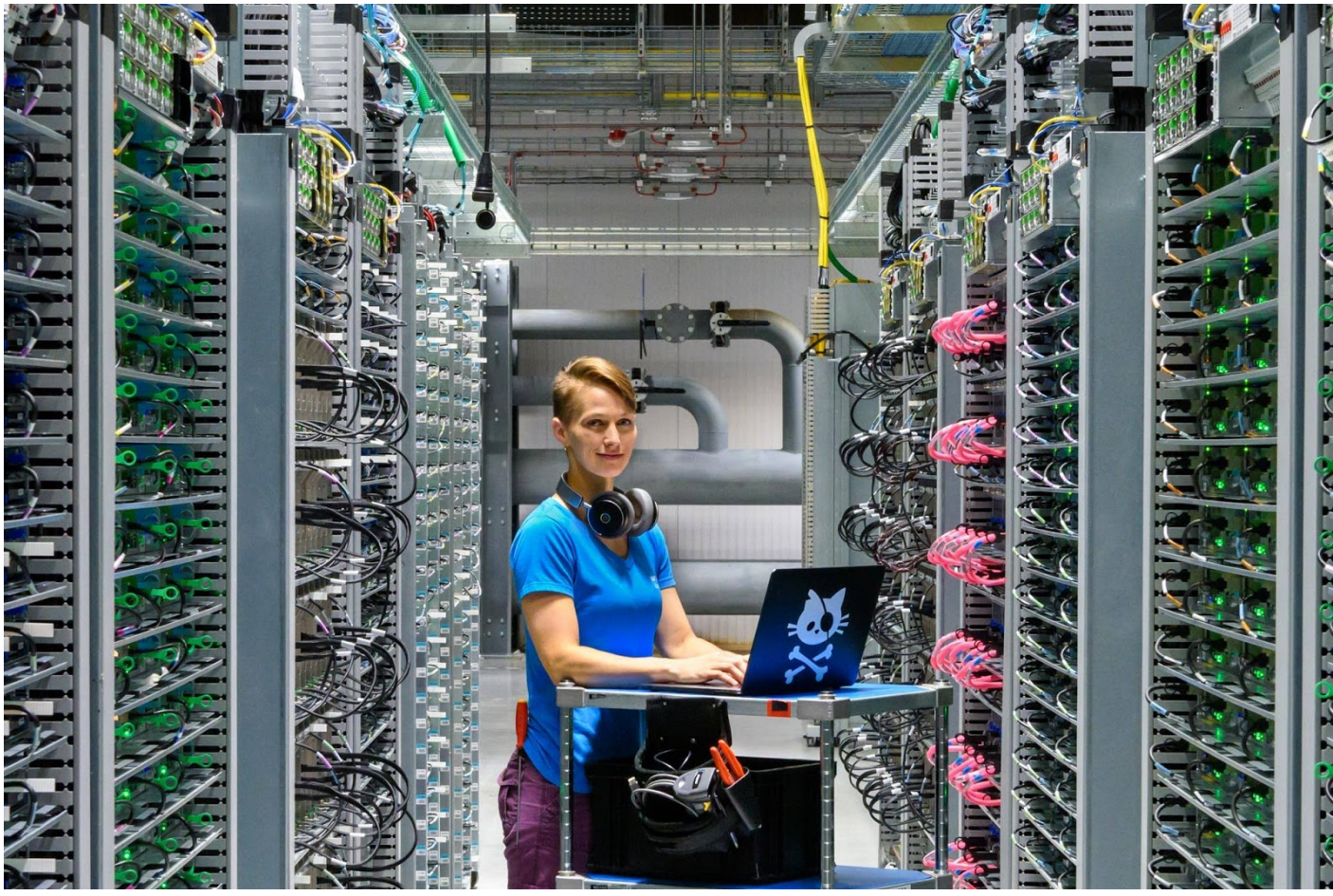
Google Cloud Whitepaper
October 2020

Google Workspace security whitepaper



Google Cloud

Table of contents

Introduction

Cloud computing has changed the way that companies today do business. Organizations primarily look to the public cloud to manage their infrastructure, operations, and delivery of services, realizing that providers can invest more in people and processes to deliver secure and compliant infrastructure.

As a cloud pioneer, Google fully understands the security implications of the cloud model. That's why we designed our cloud services to deliver better security than many traditional on-premises solutions. We make security a priority to protect our own operations. Our customers run on that same Google infrastructure, so your organization directly benefits from these protections.

Security and data protection drive our organizational structure, training priorities and hiring processes. These principles shape our data center operations and technology. They're central to our everyday operations and disaster planning, including how we address threats. They're prioritized in the way we handle customer data. And they're the cornerstone of our account controls, our compliance audits and the certifications we offer our customers. Our commitments to your business and your data are captured in our Google Cloud Trust Principles and affirm how we protect the privacy of customers whenever they use Google Workspace and Google Cloud Platform.

This whitepaper outlines Google's approach to security and compliance for Google Workspace, our cloud-based productivity suite. Used by more than five million organizations worldwide, from large banks and retailers with hundreds of thousands of people to fast-growing startups, Google Workspace and Google Workspace for Education include the collaboration and productivity tools found here. Google Workspace and Google Workspace for Education are designed to help teams work together securely in new, more efficient ways, no matter where members are located or what device they use. For instance, Gmail scans over 300 billion attachments for malware every week and prevents more than 99.9% of spam, phishing, and malware from reaching users.[1] We're committed to protecting against security threats of all kinds, innovating new security tools for users and admins, and providing our customers with a secure cloud service.

Note: We are bringing Google Workspace to our nonprofit customers in the coming months. G Suite for Nonprofits will continue to be available to eligible organizations through the Google for Nonprofits program. Unless indicated otherwise, the context of this document includes Google Workspace and Google Workspace for Education.

Disclaimer

The content contained herein is correct as of October 2020, and represents the status quo as of the time it was written. Google Cloud's security policies and systems may change going forward, as we continually improve protection for our customers.

[1] As of April 2020.

Google's security and privacy focused culture

Google has created a vibrant and inclusive security and privacy focused culture for all employees. The influence of this culture is apparent during the hiring process, employee onboarding, as part of ongoing training and in company-wide events to raise awareness.

Employee background checks

Before someone joins our staff, Google verifies their education and previous employment, and performs internal and external reference checks. Where local labor law or statutory regulations permit, Google may also conduct identity, criminal, and credit checks and confirm immigration status, depending on the position.

Security training for all employees

All Google employees undergo security training as part of the orientation process, and throughout their Google careers. During orientation, new employees also agree to our Code of Conduct, which highlights our commitment to keeping customer information safe and secure.

Depending on their role, employees participate in additional training on specific aspects of security. For example, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.

Secure Environment

Google's zero-trust approach enforces critical access controls based on information about a device, its state, its associated user, and their context. This approach considers both internal and external networks to be inherently untrusted, which creates our concept of borderless compliance where we dynamically assert and enforce levels of access at the application layer. This enables Google's security and compliance teams to be as secure and effective during an emergency as they would be at any other time.

As COVID-19 has not only changed the way we work, but where we work from, creating the need for new solutions that nonetheless continue to meet industry compliance requirements. By leveraging zero trust you can offer your employees and extended workforce a secure and scalable solution for telework that is not dependent on VPN or location requirements.

Internal security and privacy events

Security and privacy is an ever-evolving area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. It's with this in mind that Google hosts regular internal conferences, open to all employees, to raise awareness and drive innovation in security and data privacy, and hosts regular "Tech Talks" that often focus on security and privacy topics. A prime example is "Privacy Week," during which Google hosts events across our global offices to raise awareness of all facets of privacy, from software development and data handling, to policy enforcement.

Our dedicated security team

Google employs a dedicated team of full-time security and privacy professionals as part of our software engineering and operations division. This team includes some of the world's foremost experts in information, application and network security. Tasked with maintaining our defense systems, developing security review processes, building security infrastructure and implementing the company's security policies, the team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Within Google, members of the information security team provide a range of critical services. They review security plans for all networks, systems and services; provide project-specific consulting services to Google's product and engineering teams; monitor for suspicious activity on Google's networks; address information security threats; perform routine security evaluations and audits; and engage outside experts to conduct regular security assessments. On top of that, Google specifically built a full-time team, known as Project Zero, that aims to prevent targeted attacks by reporting bugs to software vendors and filing them in an external database.

It doesn't end there. The security team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. In addition, the security team publishes security research papers, which are made publicly available, as well as organizes and participates in open-source projects and academic conferences.

Our privacy teams

Google's Privacy teams are an integral part of Google product launches. Privacy has built a set of automated monitoring tools to help ensure that services that process your personal information operate as designed and in accordance with our data protection commitments. Design documentation and code audits are also reviewed to ensure that privacy requirements are followed.

Cross-functional teams help release products that reflect strong privacy standards, including: transparent collection of user data, and providing users and administrators with meaningful privacy configuration options, while continuing to be good stewards of any information stored on our platform. After products launch, Google's compliance and privacy programs oversee automated processes that

audit data traffic to verify appropriate data usage. Google also conducts research providing thought leadership on privacy best practices for our emerging technologies.

Internal audit and compliance specialists

Data protection regulations place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed. We have dedicated teams of engineers and compliance experts who support our customers in navigating their regulatory compliance and risk management obligations. Our approach includes collaborating with customers to understand and address their specific regulatory needs. As new auditing standards are created, the team determines what controls, processes and systems are needed to meet them, while facilitating and supporting independent audits and assessments by third parties. Under certain circumstances we also allow customers to conduct audits to validate Google's security and compliance controls.

Collaboration with the security research community

Google has long enjoyed a close relationship with the security research community, and we greatly value their help identifying vulnerabilities in Google Workspace and other Google products. Our Vulnerability Reward Program was developed to honor all the external contributions that help us keep our users safe. The Program encourages researchers to report design and implementation issues that affect the confidentiality or integrity of user data or puts customer data at risk. Rewards can reach tens of thousands of dollars.

Due to our collaboration with the research community, in 2019 we paid out over $6.5 million in rewards, doubling what we've ever paid in a single year. We publicly thanked these individuals and listed them as contributors to our products and services.

Operational security

Security at Google isn't an afterthought or subject of occasional initiatives, it is an integral part of our operations.

Vulnerability management

Google's vulnerability management process actively scans for security threats using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration efforts, quality assurance processes, software security reviews, and external audits. Once a vulnerability requiring remediation has been identified, the vulnerability team logs it, prioritizes it according to severity, and assigns it to an owner. The team tracks each issue and follows up frequently until they can verify that it has been remediated.

Google also maintains relationships and communicates frequently with members of the security research community to track reported issues in Google services and open-source tools. More information about reporting security issues can be found at Google Application Security.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. Google takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware.

Malware sites or email attachments install malicious software on users' machines to steal private information, perform identity theft, or attack other computers. When people visit these sites, software that takes over their computer is downloaded without their knowledge. Google's malware strategy begins with infection prevention by using manual and automated scanners to scour Google's search index for websites that may be vehicles for malware or phishing. In addition, one of our key protections is our attachment malware scanner that processes more than 300 billion attachments each week to block harmful content. 63% percent of the malicious documents we block differ from day to day. To stay ahead of this constantly evolving threat, we recently added a new generation of document scanners that rely on deep learning to improve our detection capabilities.

More than four billion devices are protected by Google's Safe Browsing technology every day. Every day Safe Browsing discovers thousands of new unsafe sites, many of which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on Google Search and in web browsers.

In addition to our Safe Browsing solution, Google operates VirusTotal, an online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners. Its mission is to help in improving the antivirus and security industry and make the Internet a safer place through the development of free tools and services.

Google makes use of multiple antivirus engines in Gmail, Drive, servers and workstations to help identify malware that may be missed by antivirus signatures.

Monitoring

Google's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. Internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections, at many points across our global network, using a combination of open-source and commercial tools for traffic capture and parsing.

We supplement this network analysis even further through a proprietary correlation system built on Google technology, and by examining system logs to identify unusual behavior, like attempted access of customer data. Google security engineers place standing search alerts on public data repositories to look for security incidents that might affect the company's infrastructure, and actively review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis helps determine potential unknown threats and escalates them to Google security staff, a process that is supplemented by automated analysis of system logs.

Incident management

Incident response is a key aspect of Google's overall security and privacy program. We have a rigorous process for managing data incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data.

Google's incident response program is managed by teams of expert incident responders across many specialized functions to ensure each response is well-tailored to the challenges presented by each incident.

Subject-matter experts from these teams are engaged in a variety of ways. For example, incident commanders assess the nature of the incident and coordinate incident response, which includes completing the triage assessment of the incident, adjusting its severity if required, and activating the required incident response team with appropriate operational/technical leads who review the facts and identify key areas that require investigation. As part of the resolution process, the digital forensics team detects ongoing attacks and performs forensic investigations. Product engineers work to limit the impact on customers and provide solutions to fix the affected product(s). The legal team works with members of the appropriate security and privacy team to implement Google's strategy on evidence collection, engages with law enforcement and government regulators, and advises on legal issues and requirements. Support personnel manage notifications to customers and respond to customer inquiries and requests for additional information and assistance.

Following the successful remediation and resolution of a data incident, the incident response team evaluates the lessons learned from the incident. When the incident raises critical issues, the incident commander may initiate a post-mortem analysis. During this process, the incident response team reviews the cause(s) of the incident and Google's response and identifies key areas for improvement. In some cases, this may require discussions with different product, engineering, and operations teams and product enhancement work. If follow-up work is required, the incident response team develops an action plan to complete that work and assigns project managers to spearhead the long-term effort. The incident is closed after the remediation efforts conclude.

Technology with security at its core

As an innovator in hardware, software, network and system management technologies, Google used the principle “defense in depth” to create an IT infrastructure that is more secure and easier to manage than more traditional technologies. We custom-designed our servers, proprietary operating system and geographically distributed data centers to ensure that Google Workspace runs on a technology platform that is conceived, designed and built to operate securely.

State-of-the-art data centers

Google’s focus on security and protecting data is among our primary design criteria. Our data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, in addition to data center floors that feature laser beam intrusion detection.

Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders, with access logs, activity records, and camera footage available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training.

The closer you get to the data center floor, the tighter these security measures become. In fact, less than one percent of Google employees will ever set foot in one of our data centers. Those that do have specific roles have been pre-approved and access the floor in the only way possible: through a security corridor that implements multi-factor access control using security badges and biometrics.

Powering our data centers

To keep things running 24/7 and ensure uninterrupted services, Google’s data centers feature redundant power systems and environmental controls. Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. In case of an incident, every critical component has a primary power source and an equally powerful alternate. Our diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Fire detection and suppression equipment—including heat, fire, and smoke detectors—triggers audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks, helping to prevent hardware damage.

Environmental impact

Google cares deeply about minimizing the environmental impact of our data centers, to the point that we design and build our own facilities using the latest “green” technology. We install smart temperature controls, utilize “free-cooling” techniques like using outside air or reused water for cooling, and redesign how power is distributed to reduce unnecessary energy loss. We constantly gauge how we’re doing by calculating the performance of each facility using comprehensive efficiency measurements.

We’re proud to be the first major Internet services company to gain external certification of our high environmental, workplace safety, and energy management standards throughout our data centers. Specifically, we achieved voluntary ISO 14001, OHSAS 18001 and ISO 50001 certifications, which are all built around a very simple concept: Say what you’re going to do, then do what you say—and then keep improving.

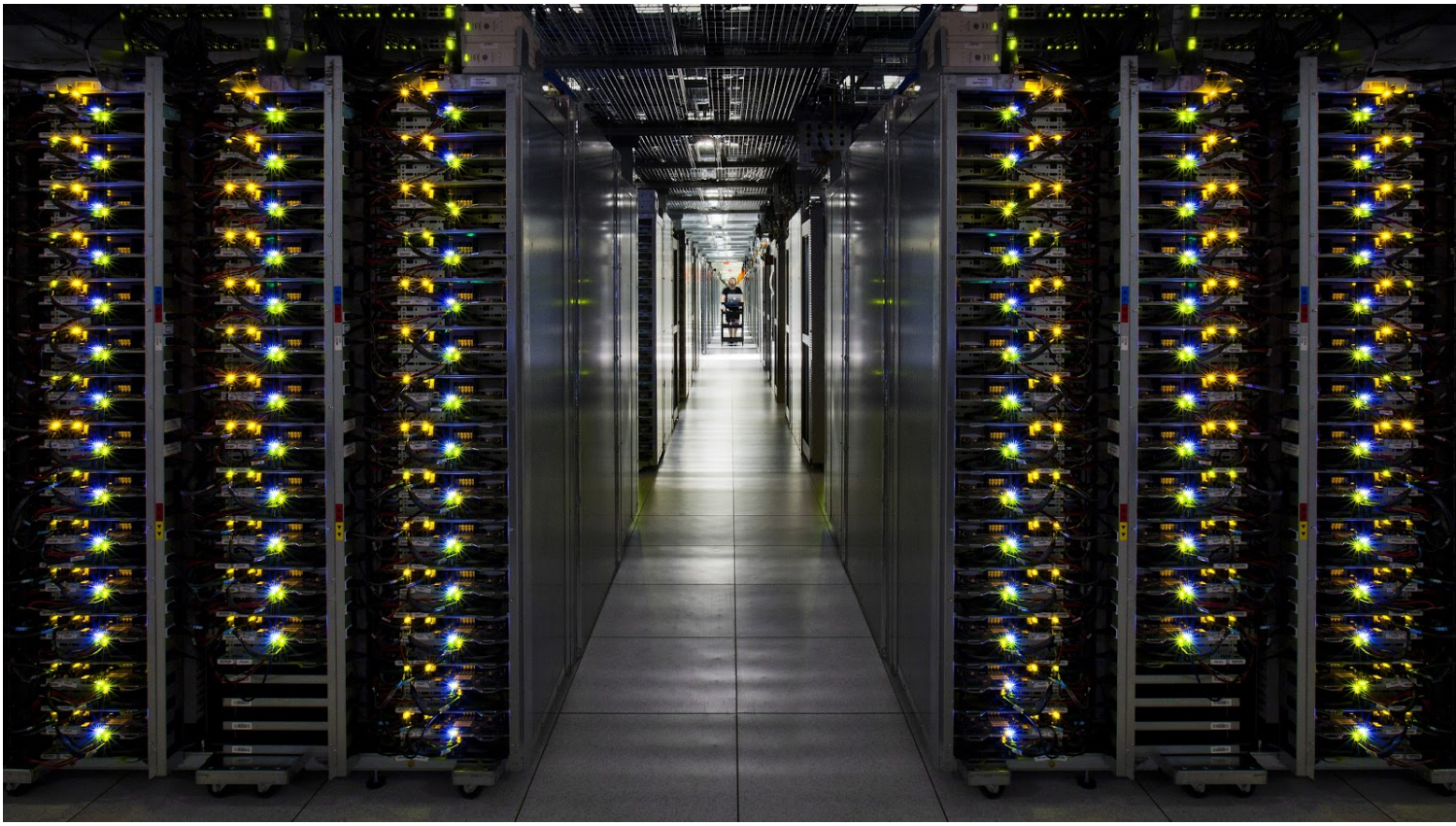
Custom server hardware and software

Google’s data centers house energy-efficient custom, purpose-built servers and network equipment that we design and manufacture ourselves. Our production servers also run a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. In other words, Google’s servers and their OS are designed for the sole purpose of providing Google services, which means that, unlike much commercially available hardware, Google servers don’t include unnecessary components such as video cards, chipsets, or peripheral connectors, that can introduce vulnerabilities. Google server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. These automated, self-healing mechanisms enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential network compromises before they become critical issues.

Hardware tracking and disposal

Google uses barcodes and asset tags to meticulously track the location and status of all equipment within our data centers from acquisition and installation, to retirement and destruction. We have also implemented metal detectors and video surveillance to help make sure no equipment leaves the data center floor without authorization. During its lifecycle in the data center, if a component fails to pass a performance test at any point, it is removed from inventory and retired.

Each data center adheres to a strict disposal policy and any variances are immediately addressed. When a hard drive is retired, authorized individuals verify that the disk is erased, writing zeros to the drive and performing a multiple-step verification process to ensure it contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. This physical destruction is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility.



A global network with unique security benefits

Google's IP data network consists of our own fiber, public fiber, and undersea cables, enabling us to deliver highly available and low latency services across the globe.

With other cloud services and on-premises solutions, customer data must make several journeys between devices, known as "hops," across the public Internet. The number of hops depends on the distance between the customer's ISP and the solution's data center, and each additional hop introduces a new opportunity for data to be attacked or intercepted. Because it's linked to most ISPs in the world, Google's global network can limit the number of hops across the public Internet, improving the security of data in transit.

Defense in depth describes the multiple layers of defense that protect Google's network from external attacks. It starts with industry-standard firewalls and access control lists (ACLs) to enforce network segregation, and all traffic being routed 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, a "default deny" configuration that prevents GFE servers from accessing unintended resources. Finally, logs are routinely examined to reveal any exploitation of programming errors, and 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.

Encrypting data in transit and at rest

Encryption is an important piece of the Google Workspace security strategy, helping to protect your emails, chats, video meetings, files, and other data. First, we encrypt certain data as described below while it is stored "at rest"—stored on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. Second, we encrypt all customer data while it is "in transit"—traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data. We'll take a detailed look at how we encrypt data stored at rest and data in transit below.

Google has led the industry in using Transport Layer Security (TLS) for email routing, which allows Google and non-Google servers to communicate in an encrypted manner. When you send email from Google to a non-Google server that supports TLS, the traffic will be encrypted, preventing passive eavesdropping. We believe increased adoption of TLS is so important for the industry that we report TLS progress in our Email Encryption Transparency Report. We also improved email security in transit by developing and supporting the MTA-STS standard allowing receiving domains to require transport confidentiality and integrity protection for emails. Google Workspace customers also have the extra ability to only permit email to be transmitted to specific domains and email addresses if those domains and addresses are covered by TLS. This can be managed through the TLS compliance setting.

For further information on encryption, please see our Google Workspace Encryption whitepaper.

Low latency and highly available solution

Google designs all the components of our platform to be highly redundant, from our server design and how we store data, to network and Internet connectivity, and even the software services themselves. This "redundancy of everything" includes error handling by design and creates a solution that is not dependent on a single server, data center, or network connection.

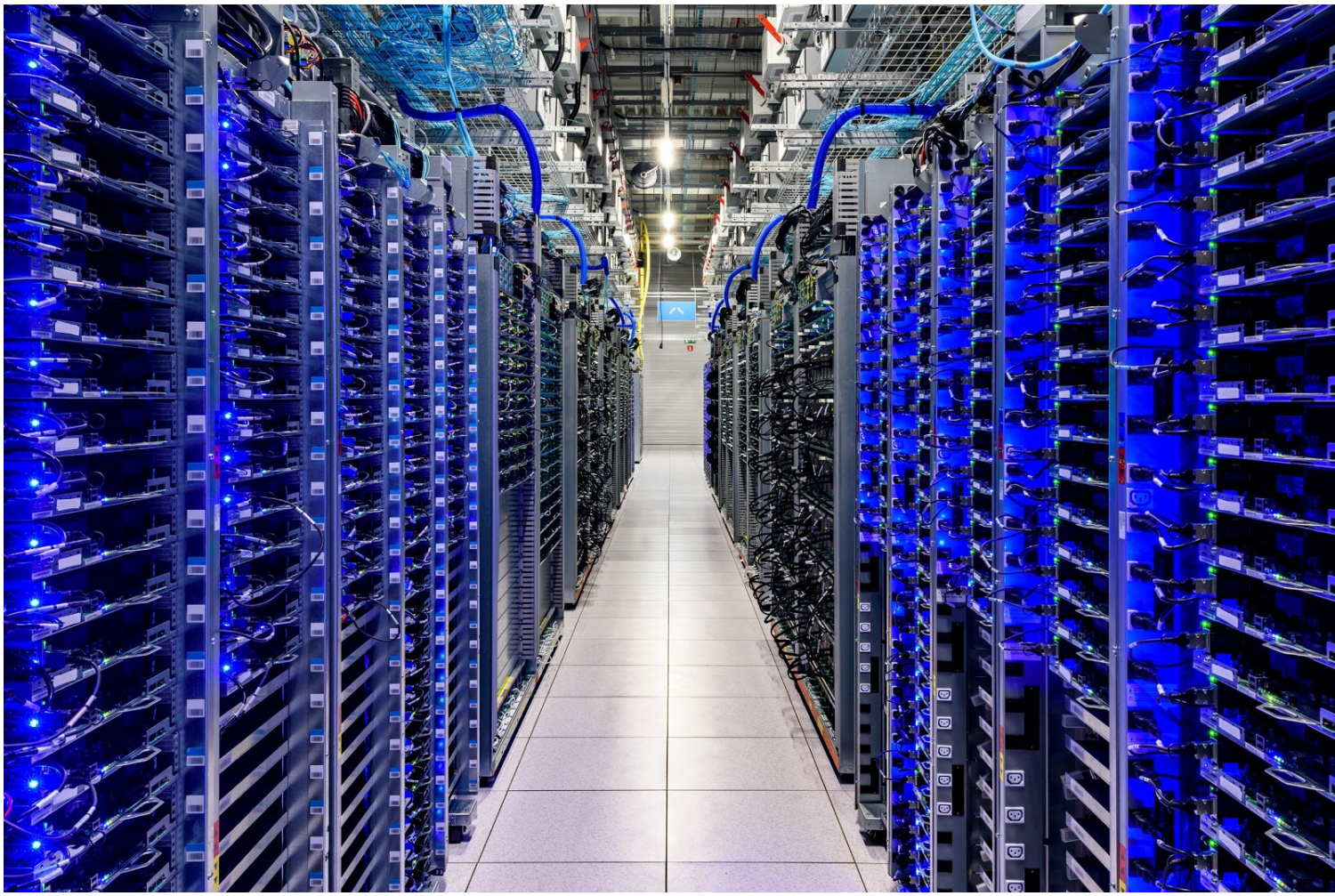
Google's data centers are geographically distributed to minimize the effects of regional disruptions such as natural disasters and local outages. In the event of hardware, software, or network failure, data is automatically shifted from one facility to another so that, in most cases, Google Workspace customers can continue working without interruption. This also means customers with global workforces can collaborate on documents, video conferencing and more without additional configuration or expense, sharing a highly performant and low latency experience as they work together on a single global network.

Google's highly redundant infrastructure also helps protect our customers from data loss. For Google Workspace, our recovery point objective (RPO) target is zero, and our recovery time objective (RTO) design target is also zero. We aim to achieve these targets through live or synchronous replication: actions you take in Google Workspace products are simultaneously replicated in two data centers at once, so that if one data center fails, we transfer your data over to the other one that's also been reflecting your actions.

To do this efficiently and securely, customer data is divided into digital pieces with random file names. Neither the content nor the file names of these pieces are stored in readily human-readable format, and stored customer data cannot be traced to a particular customer or application just by inspecting it in storage. Each piece is then replicated in near-real time over multiple disks, multiple servers, and multiple data centers to avoid a single point of failure. To further prepare for the worst, we conduct disaster recovery drills that assume individual data centers—including our corporate headquarters—won't be available for 30 days.

Service availability

Some of Google's services may not be available in some jurisdictions currently or temporarily. Google's Transparency Report shows recent and ongoing disruptions of traffic to Google products. Our code allows us to observe worldwide traffic patterns over time, enabling us to detect significant changes. We also look into our graphs when we receive inquiries from journalists, activists, or other people on the ground. We provide this data to help the public analyze and understand the availability of online information.



Supporting compliance requirements

Google is committed to providing secure products and services that meet your compliance and reporting needs. We share extensive information on best practices and provide easy access to our compliance documentation. Google Cloud's industry-leading security, third-party audits and certifications, documentation, and legal commitments help support your compliance. Our products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations of compliance, or audit reports against standards around the world. As a part of the independent verification process, third-party auditors examine our end-to-end security practices, including data centers, infrastructure, and operations, at a regular cadence. We've also created resource documents and mappings against frameworks and laws where formal certifications or attestations may not be required or applied. Our Compliance resource center contains details on our compliance documentation and resources.

We're constantly working to expand our compliance coverage. Google evaluates the available guidance from leading standards and regulatory bodies and adjusts our security and privacy programs as the compliance landscape changes. We carefully curate programs by region and industry to ensure customers are able to leverage our compliance resources to make informed decisions for their business.

When you consider Google Workspace, our compliance offerings can help to confirm whether the product suite meets your security and compliance needs.

Regulatory compliance

Our customers operate across regulated industries, including finance, government, healthcare and education. Google Cloud provides products and services in a way that enables our customers to be compliant with numerous industry-specific requirements. More information is available here.

Independent third-party certifications and attestations

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 (US government), BSI C5 (Germany), MTCS (Singapore), and many others. We also provide resource documents and mappings for certain frameworks where formal certifications or attestations may not be required or applied.

For a complete listing of our compliance offerings, please visit the Compliance resource center.

Data usage

Our philosophy

Google Workspace customers own their customer data, not Google. Customer data that Google Workspace organizations put into our systems is theirs, and we do not scan it for advertisements. We offer our customers a detailed Data Processing Amendment that describes our commitment to protecting customer data. Furthermore, if customers delete their data, we commit to deleting it from our systems within 180 days. Finally, we provide tools that make it easy for customer administrators to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by Google.

No advertising in Google Workspace

There is no advertising in the Google Workspace Core Services, and we have no plans to change this in the future. Google does not collect, scan or use data in Google Workspace Core Services for advertising purposes. Customer administrators can restrict access to Non-Core Services from the Google Workspace Admin console. Google indexes customer data to provide beneficial services, such as spam filtering, virus detection, spellcheck and the ability to search for emails and files within an individual account.

Data access and restrictions

Administrative access

We've designed our systems to limit the number of employees that have access to customer data and to actively monitor the activities of those employees. Google employees are only granted a limited set of default permissions to access company resources. Access to internal support tools is controlled via access control lists (ACLs). Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees. Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for Google Workspace products. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events.

Furthermore, as part of Google's long-term commitment to transparency and user trust, we provide Access Transparency.[2] This is a feature that enables customers to review logs of actions taken by Google staff when accessing your specific customer data. For services integrated with Access Transparency, Google uses a tool to validate that the business justification presented for access is valid, and log the justification to Access Transparency Logs.

For further information, please refer to the Trusting you data with Google Workspace whitepaper.

For customer administrators

Customers can control access to data and services on Google Workspace to help ensure that data is protected in accordance with the organization's desired configuration. Role-based access controls enable customers to appoint users as administrators, granting the user the ability to access and perform certain tasks in the Google Workspace Admin console. You can make a user a super administrator who can perform all tasks in the Admin console. Or you can assign a role that limits which tasks the administrator can perform, for example, by allowing them only to create groups, manage service settings, or reset a user's password.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests and it is Google's policy to direct the government to request such data directly from the customer. However, like other technology and communications companies, Google may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also

[2] Access Transparency is only available with Google Workspace Enterprise and Google Workspace for Education Plus.

meeting our legal obligations. Respect for the privacy and security of data you store with Google remains our priority as we comply with these legal requests.

Detailed information about data requests and Google's response to them is available in our Transparency Report. Further information is also available in the Trusting you data with Google Workspace whitepaper.

Third-party suppliers

Google directly conducts virtually all data processing activities to provide our services. However, Google may engage some third-party suppliers to provide services related to Google Workspace, including customer and technical support. Prior to onboarding third-party suppliers, Google conducts an assessment of the security and privacy practices of third-party suppliers to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

Empowering users and administrators to improve security and compliance

Google builds security into its structure, technology, operations and approach to customer data. Our robust security infrastructure and systems become the default for each and every Google Workspace customer. Beyond these levels, users are actively empowered to enhance and customize their individual security settings to meet their business needs through dashboards and account security wizards.

Google Workspace also offers administrators full control to configure infrastructure, applications, and system integrations in a single dashboard via our Admin Console—regardless of the size of the organization—simplifying administration and configuration. Consider the deployment of DKIM (a phishing prevention feature) in an on-premise email system. Traditionally, administrators would need to patch and configure every server separately, with any misconfiguration causing a service outage. Using our Admin Console, however, DKIM can be configured in minutes across thousands, or hundreds of thousands, of accounts with peace of mind and no outage or maintenance window required.

That's just one example. Administrators have many powerful tools at their disposal, including authentication features like 2-step verification and single sign-on, and email security policies like secure transport (TLS) enforcement, which can be configured to meet the security and system integration requirements of any organization.

Access and Authentication

2-step verification and security keys

Customers can strengthen account security by using 2-step verification and security keys.[3] These can help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts.[4] With the Advanced Protection Program for enterprise, we can enforce a curated set of strong account security policies for enrolled users. These include requiring security keys, blocking access to untrusted apps, and enhanced scanning for email threats.

Single sign-on (SAML 2.0)

Google Workspace offers customers a single sign-on (SSO) service that lets users access multiple services using the same sign-in page and authentication credentials. It is based on SAML 2.0, an XML standard that allows secure web domains to exchange user authentication and authorization data. For additional security, SSO accepts public keys and certificates generated with either the RSA or DSA algorithm. Customer organizations can use the SSO service to integrate single sign-on for Google Workspace into their LDAP or other SSO system.

OAuth 2.0 and OpenID Connect

Google Workspace supports OAuth 2.0 and OpenID Connect, an open protocol for authentication and authorization that allows customers to configure one single sign-on service (SSO) for multiple cloud solutions. Users can log on to third-party applications through Google Workspace—and vice versa—without re-entering their credentials or sharing sensitive password information.

Information Rights Management (IRM)

Most organizations also have internal policies which dictate the **handling of sensitive data**. To help Google Workspace administrators maintain control over sensitive data, we offer **information rights management** in Google Drive. Administrators and users can use the access permissions in Google Drive to protect sensitive content by preventing the re-sharing, downloading, printing or copying of the file or changing of the permissions.

Restricted email delivery

By default, users with Gmail accounts at your domain can send mail to and receive mail from any email address. In some cases, administrators may want to restrict the email addresses users can exchange mail with. For example, a school might want to allow its students to exchange mail with the faculty and other students, but not with people outside the school.

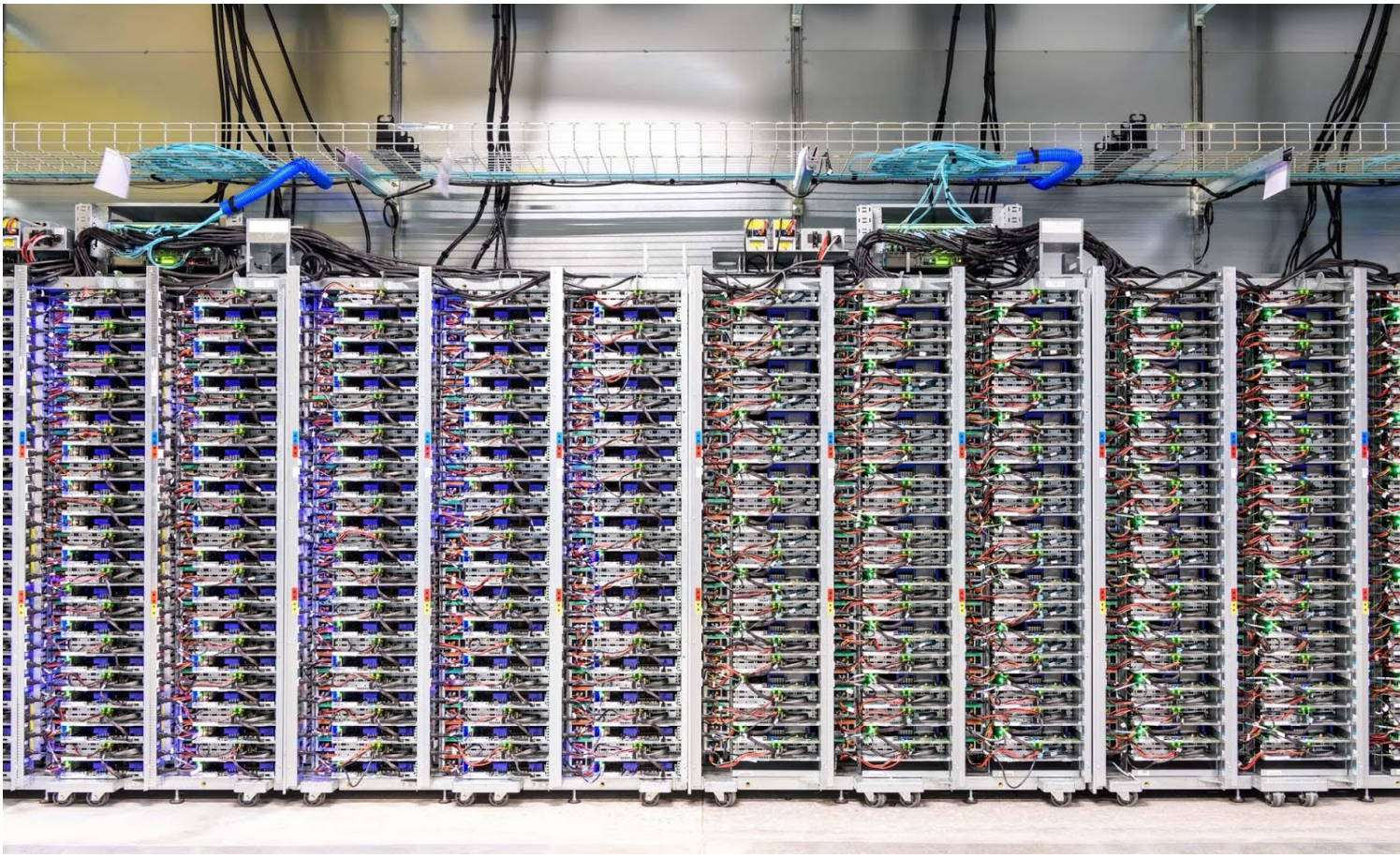
Using the restrict delivery setting allows administrators to specify the addresses and domains where users can send or receive email messages. When administrators add a restrict delivery setting, users

[3] Further information about deploying 2-step verification can be found on our support page.
[4] See security best practices guidance on our security checklists page.

can only communicate with authorized parties. Users who attempt to send mail to a domain not listed will see a message that specifies the policy prohibiting mail to that address, and confirms that the mail is unsent. Likewise, users receive only authenticated messages from listed domains. Messages sent from unlisted domains—or messages from listed domains that can't be verified using DKIM or SPF records—are returned to the sender with a message about the policy.

App access based on user context

To facilitate easier user access, while at the same time protecting the security of data, Google has developed context-aware access.[5] This provides granular controls for Google Workspace apps, based on a user's identity and context of the request (such as device security status or IP address). Based on the BeyondCorp security model developed by Google, users can access web applications and infrastructure resources from virtually any device, anywhere, without utilising remote-access VPN gateways while administrators can establish controls over the device. You can also still set access policies, such as 2-Step Verification, for all members of an organizational unit or group.



[5] Integrated with Cloud Identity. Using context-aware access capabilities to protect access to Google Workspace apps requires a Cloud Identity Premium or Google Workspace Enterprise license.

Asset Protection

Email spam, phishing and malware protection

Gmail protects your incoming mail against spam, phishing attempts, and malware. Our existing machine learning models are highly effective at doing this, and in conjunction with our other protections, they help block more than 99.9% of threats from reaching Gmail inboxes. One of our key protections is our malware scanner that processes more than 300 billion attachments each week to block harmful content.[6] 63% percent of the malicious documents we block differ from day to day.[7] In addition, Gmail can scan or run attachments in a virtual environment called Security Sandbox. Attachments identified as threats can be placed in users' Spam folders or quarantined.

We're continuing to improve spam detection accuracy with early phishing detection, a dedicated machine learning model that selectively delays messages (less than 0.05 percent of messages on average) to perform rigorous phishing analysis and further protect user data from compromise.

Our detection models integrate with Google Safe Browsing machine learning technologies for finding and flagging phishy and suspicious URLs. These new models combine a variety of techniques, such as reputation and similarity analysis on URLs, allowing us to generate new URL click-time warnings for phishing and malware links. As we find new patterns, our models get better with time, and adapt more quickly than manual systems ever could.

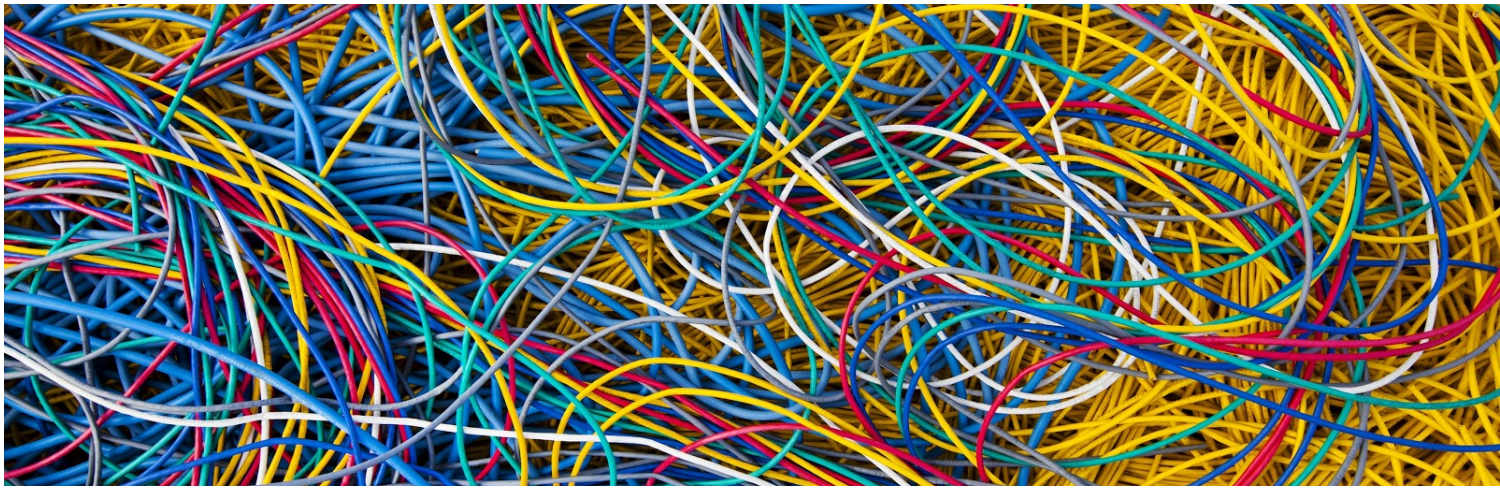
Email spoofing prevention

Spammers can sometimes forge the "From" address on an email message so that it appears to come from a reputable organization's domain. To help prevent this email spoofing, Google participates in the DMARC program, which lets domain owners tell email providers how to handle unauthenticated messages from their domain. Google Workspace customers can implement DMARC by creating a DMARC record within their admin settings and implementing an SPF record and DKIM keys on all outbound mail streams.

Warnings for employees to prevent data loss

When employees are empowered to make the right decisions to protect data, it can improve an enterprise's security posture. To help with this, Gmail displays unintended external reply warnings to users to help prevent data loss. If you try to respond to someone outside of your company domain, you'll receive a quick warning to make sure you intended to send that email. And because Gmail has contextual intelligence, it knows if the recipient is an existing contact or someone you interact with regularly, to avoid displaying warnings unnecessarily.

[6] As of February 2020.
[7] As of February 2020.



Hosted S/MIME to provide enhanced security

With Google's hosted S/MIME solution, once an incoming encrypted email with S/MIME is received, it is stored using Google's encryption. This means that all normal processing of the email can happen, including extensive protections for spam, phishing and malware, as well as admin services (such as vault retention, auditing and email routing rules) and high-value end user features such as mail categorization, advanced search and Smart Reply. For the vast majority of emails, this is the safest solution, giving the benefit of strong authentication and encryption in transit without losing the safety and features of Google's processing.

Gmail confidential mode

Gmail users can help protect sensitive information from unauthorized access using Gmail confidential mode. Recipients of messages in confidential mode don't have the option to forward, copy, print, or download messages, including attachments. Users can set a message expiration date, revoke message access at any time, and require an SMS verification code to access messages.

Data Loss Prevention (DLP) for Gmail and Drive

Data loss prevention (DLP)[8] adds another layer of protection designed to prevent sensitive or private information such as payment card numbers, national identification numbers, or protected health information, from leaking outside of an organization. DLP enables customers to audit how sensitive data is flowing in their enterprise or turn on warning or blocking actions, to prevent users from **sending confidential data**. To enable this, DLP provides predefined content detectors, including detection of global and regional identifiers, medical information and credentials. Customers can also define their own custom detectors to meet their enterprise needs. For attachments and image-based documents, DLP uses Google's optical character recognition to increase detection coverage and quality. Learn more here about Gmail DLP. DLP can also be used to prevent users from sharing sensitive content in Google Drive or shared drive with people outside of your organization. In addition, customers can automate IRM controls and classification of Drive files advanced DLP rules.

[8] Available to Google Workspace Enterprise and paid editions of Google Workspace for Education customers only.

Configuring Google Workspace security settings

Security and alert management

With multiple security and privacy controls in place, organizations **need a centralized location where they can prevent, detect, and remediate threats**. The Google Workspace security center[9] provides advanced security information and analytics, and added visibility and control into security issues affecting your domain.[10] It brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users.
As an administrator, you can use the security dashboard to see an overview of different security center reports. The security health page provides visibility into your Admin console settings to help you better understand and manage security risks. Furthermore, you can use the security investigation tool to identify, triage, and take action on security and privacy issues in your domain. Administrators can automate actions in the investigation tool by creating activity rules to detect and remediate such issues more quickly and efficiently. For example, you can set up a rule to send email notifications to certain administrators if Drive documents are shared outside the company.

The alert center for Google Workspace provides all Google Workspace customers with alerts and actionable security insights about activity in your domain to help protect your organization from the latest security threats, including phishing, malware, suspicious account, and suspicious device activity. You can also use the alert center API to export alerts into your existing ticketing or SIEM platforms.

Trusted domains for drive sharing

Administrators can control how users in their organization share Google Drive files and folders. For example, whether users can share files with people outside of their organization or whether sharing is restricted to only trusted domains.[11] Optional alerts can be established to remind users to check that files aren't confidential before they are shared outside of the organization.

Video meetings safety

Google Meet takes advantage of the same secure-by-design infrastructure, built-in protection, and global network that Google uses to secure your information and safeguard your privacy. Our array of default-on anti-abuse measures that include anti-hijacking measures for both web meetings and telephony dial-ins, keep your meetings safe.

---

[9] Included with Google Workspace Enterprise edition and Google Workspace for Education Standard and Google Workspace for Education Plus.
[10] You must be an administrator with a Google Workspace Enterprise, Google Workspace for Education Standard, Google Workspace for Education Plus, Drive Enterprise, or Cloud Identity Premium Edition license to access the security center. With Drive Enterprise or Cloud Identity Premium Edition, you receive a subset of security center reports on the security dashboard.
[11] Certain features, such as restricting sharing to only whitelisted domains, are only available with Google Workspace Enterprise, Google Workspace for Education Plus , Drive Enterprise, Business, and Nonprofits edition.

For users on Chrome, Firefox, Safari and new Edge we don't require or ask for any plugins or software to be installed, Meet works entirely in the browser. This limits the attack surface for Meet and the need to push out frequent security patches on end-user machines. On mobile, we recommend that you install the Google Meet app from Apple App Store or the Google Play Store.

We support multiple 2 Step Verification (2SV) options for Meet that are both secure and convenient - hardware and phone-based security keys, as well as Google prompt. Meet users can enroll their account in Google's Advanced Protection Program (APP). APP provides our strongest protections available against phishing and account hijacking and is specifically designed for the highest-risk accounts, and we've yet to see people successfully phished if they participate in APP, even if they are repeatedly targeted. For more information, check out this page.

Endpoint management

The protection of information on **mobile and desktop devices** can be a key concern for customers. Google Workspace customers can use **endpoint management**[12] to help protect corporate data on users' personal devices and on an organization's company-owned devices. By enrolling the devices for management, users get secure access to Google Workspace services and organizations can set policies to keep devices and data safe through device encryption and screen lock or password enforcement. Furthermore, if a device is lost or stolen, corporate accounts can be remotely wiped from mobile devices and users can be remotely signed out from desktop devices. IT admins can also **manage and configure Windows 10 devices** through the Admin console, and users can use existing Google Workspace account credentials to login to Windows 10 devices and access apps and services with single sign-on (SSO). Reports enable customers to monitor policy compliance and get information about users and devices. You can obtain further information on endpoint management here.

Reporting analytics

Google Workspace audit logs

Enterprises storing data in the Cloud seek **visibility into data access** and account activity. Google Workspace audit logs help security teams maintain audit trails in Google Workspace and view detailed information about Admin activity, data access, and system events. Google Workspace admins can use the Admin Console to access these logs and can customize and export logs as required.

Security reports

Google Workspace administrators have access to security reports that provide vital information on their organization's exposure to data compromise. They can quickly discover which particular users pose security risks by not taking advantage of 2-step verification, installing external apps, or sharing documents indiscriminately. Administrators can also choose to receive alerts when suspicious login activity occurs, indicating a possible security threat.

[12] Included as standard with Google Workspace.

Insights using BigQuery

Google Workspace admins can export audit logs and other information to BigQuery. With BigQuery, Google's enterprise data warehouse for large-scale data analytics, customers can analyze Google Workspace logs using sophisticated, high-performing custom queries, and leverage third-party tools for deeper analysis.

Data Recovery

Restore a recently deleted user

An administrator can restore a deleted user account for up to twenty days after the date of deletion. After twenty days, the Admin console permanently deletes the user account, and it can't be restored, even if you contact Google technical support. Please note that only customer administrators can delete accounts.

Restore a user's Drive or Gmail data

An administrator can restore a user's Drive or Gmail data for up to 25 days after the data is removed from the user's trash, subject to any retention policies set in Vault. After 25 days, the data cannot be restored, even if you contact technical support. Google will delete all customer-deleted data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

Retention and eDiscovery

An administrator can turn on Google Vault to retain, hold, search, and export data in support of your organization's retention and eDiscovery needs. Vault supports such data as Gmail messages, files in Google Drive, and recordings in Google Meet, among others.

Data Residency

As an administrator, you can choose to store your covered data in a specific geographic location (the United States or Europe) by using a data region policy. Data region policies cover the primary data-at-rest (including backups) for these Google Workspace Core Services. Covered data includes Drive file content, Google Chat messages and attachments, Gmail mail subjects and messages, as well as other Core Services data.

Conclusion

The protection of your data is a primary design consideration for all of Google's infrastructure, products and personnel operations. We believe that Google can offer a level of protection that very few public cloud providers or private enterprise IT teams can match.

Google designed Google Workspace to meet stringent privacy and security standards based on industry best practices. Google has strong contractual commitments regarding data ownership, data use, security, transparency, and accountability. These commitments ensure you maintain control over your data and how it is processed, including the assurance that your data is not used for advertising or any purpose other than to deliver Google Cloud services. In addition, we give you the tools you need to help meet your compliance and reporting requirements.

Furthermore, because protecting data is core to Google Workspace, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees you to focus on your business and innovation. Google's operations and collaboration with the security research community also enable us to address vulnerabilities quickly or prevent them entirely.

For these reasons and more, over six million organizations across the globe trust Google with their most valuable asset: their information. Google will continue to invest in Google Workspace to allow you to benefit from our services in a secure and transparent manner.