Google Workspace Whitepaper
January 2023

Trusting your data with Google Workspace

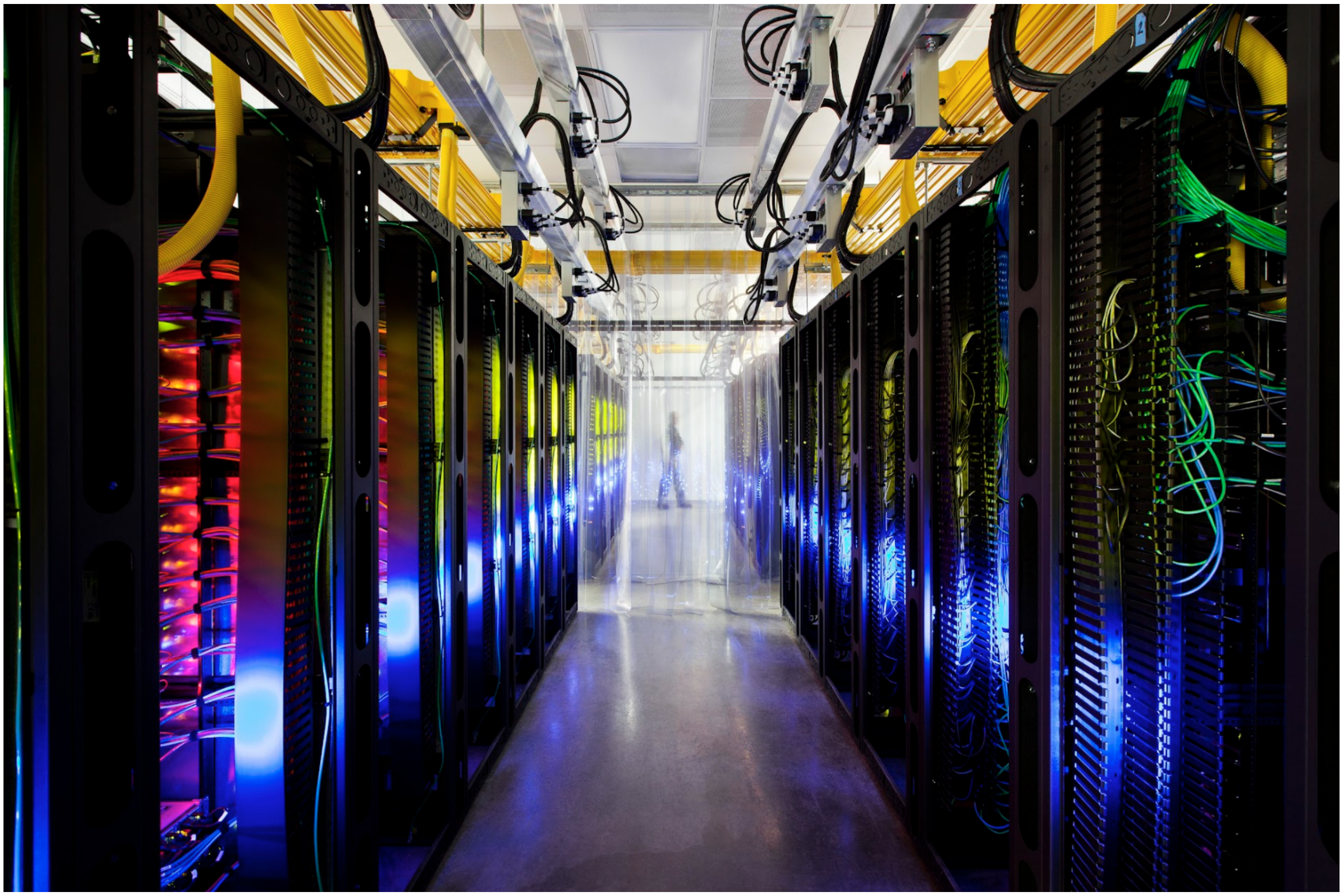

Table of Contents

Disclaimer

This whitepaper applies to Google Workspace products described as “Core Services” at Google Workspace Services Summary. The content contained herein is correct as of January 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

1. Introduction

At Google Cloud, we've set a high bar for what it means to host, serve, and protect our customers' data. Security and data protection are at the core values of how we design and build our products. We start from the fundamental premise that Google Cloud customers own their data and control how it is used. The customer data stored and managed on Google Workspace is processed per your instructions in accordance with the Data Processing Amendment (DPA) and for no other purpose. Not for advertising, not for anything else. Our Google Cloud Trust Principles summarize our commitment to protecting the privacy of data stored by customers in Google Workspace.

This whitepaper details how we provide customers with transparency and control over their data in Google Workspace. Google Workspace offers built-in data protection at scale, by default, designed to protect your business from intrusions, theft, and attacks. In addition to continuous security monitoring for external threats, we explain the robust controls and auditing in place to protect against insider access to customer data. These include providing customers with near real-time logs of Google administrator access data, via Access Transparency logs.. If you'd like to learn more about how we define customer data, please refer to our Google Workspace Terms.

Google Workspace products regularly undergo independent, third-party audits and certifications to verify that our data protection practices match our controls and commitments. An overview of our key compliance reports and certifications, as well as how we support our customers with their compliance journey is also provided in this paper. Lastly, Google participates in such declarations as the EU Cloud Code of Conduct to further evidence to our customers our commitments to accountability, compliance support, and robust data protection principles.

While this whitepaper provides information on the tools and resources offered by Google Cloud, please note that, as a provider of cloud services, we are not in a position to provide our customers with legal advice - this is something only legal counsel can provide.

2. Managing your data on Google Workspace

This section describes the data lifecycle in Google Workspace through the lens of security and privacy.

2.1 Data Protection

Using Google Workspace services involves transferring data between your computer (typically via your browser) or mobile device, Google's servers, and, sometimes, other users. Google enables encryption in transit by default between your device and our data centers, and uses Transport Layer Security (TLS) protocol to encrypt requests before transmission outside Google. This helps prevent third parties from **exploiting vulnerabilities** in internet connections to access sensitive data.

Google Workspace also applies encryption by default when content is stored at rest – stored on a disk (including solid-state drives) or backup media. We use an Advanced Encryption Standard (AES) cipher with a unique 128-bit or stronger key for each chunk of Google Workspace data stored on a local disk.

Each chunk key is then encrypted by another 128-bit or stronger key that is managed by a Google-wide key management service (KMS). Google Workspace data is also encrypted when stored on backup media, each of which is protected with a 256-bit secret key that itself is encrypted via KMS. For further information on encryption, please see our Google Workspace Encryption whitepaper.

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 the administrator's tasks, for example, by allowing them only to create groups, manage service settings, or reset a user's password. You can also review our data protection implementation guide for Workspace and Workspace for Education for additional resources.

Customers can strengthen account security by using 2-step verification and security keys. These can help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts. 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.

To facilitate easier user access, while at the same time protecting the security of data, Google has developed BeyondCorp Enterprise. 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 utilizing remote-access VPN gateways while administrators can establish controls over the device.

Protecting information on **mobile and desktop devices** can be a key concern for customers. Google Workspace customers can use endpoint management 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. Reports enable customers to monitor policy compliance and get information about users and devices. We discuss endpoint management further in our managing devices for your organization documentation.

2.2 Data Deletion

Customers may also seek control over the **deletion of data**. The safe deletion of data is important to protect against the risk of accidental data loss. At the same time, when customers instruct deletion of data, it is equally important that this data be deleted completely from servers after a period of time.

When you delete data in Google Workspace, we immediately start the process of removing it from the product and our systems unless it is subject to a Google Vault retention policy per the customer's instructions. Immediately, we aim to remove it from view. We then begin a process designed to safely and completely delete the data from our storage systems. Each Google storage system from which data gets deleted has its own detailed process for safe and complete deletion. This might involve repeated passes through the system to confirm all data has been deleted. Our services also use encrypted backup storage as another layer of protection to help recover from potential disasters. Data can remain on these systems for up to six months.

2.3 Data export and download

Customers may want to export and download their data securely from our services. We provide **portability and migration** capabilities and our specific data portability commitments are included in our data processing agreement.

The data export tool available in your Google Workspace Admin console enables you to export all supported data for each active user in your organization. We also provide the ability for your users to directly download their data on an individual level.

2.4 Data governance

Enterprises operating in certain countries or regulated industries, such as Healthcare and Financial Services, may be **required to meet certain compliance obligations**, e.g., HIPAA, PCI DSS, and GDPR. By using security settings in Google Workspace and leveraging the compliance certifications Google Workspace has achieved, customers can manage their compliance. Section 4.2 of this paper provides an overview of the compliance support we offer customers.

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 permissions. 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. Optional alerts can be established to remind users to check that files aren't confidential before they are shared outside of the organization.

Many organizations are required to **preserve data** for certain periods of time and to delete sensitive data after a time period. Google Vault, the retention solution for Google Workspace customers, can be used to set retention rules that control how long specific types of data are retained. When retention coverage ends, Vault immediately begins to remove affected data. Customers can create as many custom rules as their organization needs. Learn more about how Vault manages retention.

Data loss prevention (DLP) 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 and turn on warning or blocking actions to prevent users from either **accidentally or maliciously sending confidential data**. To enable this, DLP provides over 100 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 needs. For attachments and image-based documents, DLP uses Google's leading 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.

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 users can use the Admin Console to access these logs and can customize and export logs as required.

Customers may wish to allow their users **access to third-party apps** or may even wish to develop their own custom apps. Google Workspace has a robust developer ecosystem, with thousands of apps available via Google Workspace Marketplace and directly to customers, and a rich API framework enabling users to develop custom apps. However, not all third-party apps will conform to every customer's security policy. With app access control, enterprises can see which third-party apps users have approved to access their Google Workspace data and can reduce this risk by limiting access to trusted apps. We also help enterprises manage risk with app verification, which ensures that apps accessing Gmail data meet security and privacy standards.

2.5 Data residency

Google's globally distributed data centers reduce latency for multinational organizations and protect their data with geo-redundancy. Some organizations, however, have requirements around where their data is stored, and we're committed to meeting their needs.

Data regions for Google Workspace provide control over the geographical location for storage of email messages, documents, and other Google Workspace content. Customers can choose between the United States, Europe, or global storage. Additionally, data regions offer the flexibility to choose one data region for some of your users, or different data regions for specific departments or teams. Additional information is available on the data regions support page.

2.6 Incident detection & response

With multiple security and privacy controls in place, organizations **need a centralized location where they can prevent, detect, and respond to threats**.The Google Workspace security center provides advanced security information and analytics, and added visibility and control into security issues affecting your domain. 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.

In addition, 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.

Google has a rigorous internal 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. You can learn more about how Google detects and manages our own incidents in our Data incident response process whitepaper.

2.7 Interoperability and Portability

Google's belief in an open cloud stems from our deep commitment to open source. We believe that open source is the future of public cloud: It's the foundation of IT infrastructure worldwide and has been a part of Google's foundation since day one. This is reflected in our contributions to projects like Kubernetes, TensorFlow, Go, and many more. We believe customers should use us because they love us, not because they are locked in.

We are committed to an open cloud that enables our customers to set up the optimal solution, spanning on-premise and multiple clouds, without being locked into a single provider. We offer tools that operate across systems and vendors and allow you to monitor your system from a single place.

Google Cloud built Google Workspace with its commitment to open source technology and interoperability top-of-mind. We know that our customers use Google Workspace for critical communication and collaboration that keeps businesses running and have built the services within Google Workspace to ensure that data is not only secure, but also readily portable in the event that they need to change providers or take data offline.

We have published the Google Cloud Transparency Declaration which demonstrates Google Cloud's adherence to the SWIPO (Switching Cloud Providers and Porting Data) Data Portability Codes of Conduct for IaaS and SaaS services. These voluntary Data Portability Codes govern the relationship between Cloud customers and Cloud Service Providers (CSPs) to ensure customers are able to effectively migrate their data from one cloud provider to another. Customers can confidently carry out their work on Google Workspace, knowing that it offers robust data sovereignty capabilities and that we continue to invest in the development of additional capabilities.

3. Safeguarding access to your data

At Google, protecting the sensitive data that customers and enterprises trust us with is a top priority. Our zero trust-based architecture and least privilege principles include:

- The industry's strongest authentication protocols
- Is highly resistant to data exfiltration, and,

- Deploys 24/7 advanced monitoring and analytics to restrict the misuse of credentials, detect abnormal employee activity, and automatically respond to new or evolving threats.

3.1 Data access controls

Google Cloud believes that customers should have a robust level of control over data stored in the cloud.We've developed product capabilities that enhance your control over your data and provide expanded visibility into when and how your data is accessed. Google has **three types of controls** in place to ensure that each of these access pathways function as intended:

1. **Direct customer access**: All authentication sessions to Google Workspace are encrypted and users can only access the services enabled by their Domain Administrator.
    - **Zero trust access model**: Google Workspace customers can also use Context-Aware Access to create granular access control policies to apps based on attributes such as user, location, device security status, and 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 utilizing remote-access VPN gateways while administrators can establish controls over the device. Access decisions are not based solely on static credentials or whether they originate from a corporate intranet. The complete context of a request (user identity, location, device ownership and configuration, and fine-grained access policies) is evaluated to determine its validity and guard against phishing attempts and credential-stealing malware.
2. **Internal Google access by authorized individuals**: As part of Google's long-term commitment to security and transparency, you can use Access Transparency to review logs of actions for covered service data taken by Google staff - when accessing certain customer data as permitted by law. Google implements strict access controls to ensure the person accessing the data is authorized to do so and validates that a business justification for access is provided. The justification is made visible to the customer through Access Transparency Logs.
3. **Google Workspace Service Access**: When internal Google Workspace services access your data, Google uses technologies like Binary Authorization to validate the provenance and integrity of the software.

Client-side Encryption

Google Workspace's unique approach to client-side encryption provides our customers with authoritative privacy control over their data through encryption keys they can hold on-site, within a nation's borders, or within any other boundary they define. Google never has access to the keys or key holders, which means the data is indecipherable to us, and we have no technical ability to access it. We deliver this level of encryption without needing legacy desktop clients while maintaining the same high-quality experience for your users such as online co-authoring.

Organizations can choose to use Client-side encryption pervasively across all their users, or create rules that apply to specific users, organizational units, or shared drives. Client-side encryption is now generally available for Google Drive, Docs, Sheets, and Slides.

3.2 Data access transparency

Google Cloud is explicit in its commitment to customers: **you own your data**, and we will never use it for any purpose other than those necessary to fulfill our contractual obligations. We also know that in addition to commitments, customers want additional transparency and control from their cloud service provider.

As part of Google's long-term commitment to transparency and user trust, we provide Access Transparency, a feature that enables customers to review logs of actions taken by Google staff when accessing your specific customer data.

Access Transparency log entries include the following types of details: the affected resource and action; the time of the action; the reasons for the action (for example, the case number associated with a customer support request); and data about who is acting on the data (such as the Google staff member's location).

Access Transparency logs are generated when people at Google access data in an Access Transparency supported service (for example, if a Support engineer accesses your data to fix a Calendar problem). Google Workspace customers can monitor the logs through the Google Workspace Admin console.

Learn more about Access Transparency for Google Workspace on this support page.

3.3 Google employee access authorization

Google employees undergo background checks, are required to execute a confidentiality agreement, and comply with Google's code of conduct. In addition, 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 Cloud 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**.

For further information on employee onboarding and security and privacy training, please refer to our security whitepaper.

3.4 Organizational safeguards

3.4.1 Transparency

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud. We understand that a big part of being transparent is providing information on when requests are made for access to your data.

In our Transparency Reports, we share our data about how the policies and actions of governments and corporations affect privacy, security, and access to information.

We also offer Access Transparency for Google Workspace that logs and surfaces the customer administrative access to customer data by Google Cloud as permitted by law. We also undergo third-party audits to publicly verify our privacy and security compliance obligations.

3.4.2 Use of subprocessors

Google companies directly conduct the majority of data processing activities required to provide Google Cloud services. However, we do engage with some carefully selected third-party vendors to perform limited activities in connection with Google Cloud services.

We recognize the importance of transparency about the third parties we engage with who may process your data. We share information about our vendors on our Google Workspace and Cloud Identity Subprocessor page to provide our customers with visibility. This includes who they are, where they are located, the specific services they support, and the limited processing of customer data they are authorized to perform.

Google expects our Subprocessors to meet the same high standards that we do. Before onboarding Subprocessors, Google assesses their security and privacy practices. We do this to ensure that Subprocessors provide a level of security and privacy appropriate to their data access and the scope of the activities they are engaged to perform.

Once Google has assessed the risks, the Subprocessor is required to enter into appropriate security, confidentiality, and privacy contract terms. In particular, Google requires our Subprocessors to only access and use your data to the extent required to perform the obligations subcontracted to them and to do so in accordance with our contract with you. Google will remain fully liable for all obligations subcontracted to our Subprocessors.

To enable you to retain oversight of our Subprocessors, we will notify you when we engage a new Subprocessor so that you know in advance before any new Subprocessor starts processing your data.

3.4.3 Government requests for data

Our Transparency Report discloses, where permitted by the applicable laws, the number of requests made by law enforcement agencies and government bodies for Enterprise Cloud customer information. The historical numbers disclosed in our report for Enterprise Cloud Requests for customer information show that the number of Enterprise Cloud-related requests is extremely low compared to our Enterprise Cloud customer base.

We also work hard to help give our customers a clear and detailed understanding of our process for responding to government requests for Cloud customer data in the rare cases where they do happen.

Customers and end users can also review the number of requests Google LLC has received under U.S. National Security authorities for all Google services (including Google Cloud) in our Transparency Report.

4. Security and compliance standards

4.1 Independent verification of our control framework

Moving to the cloud means protecting sensitive workloads while achieving and maintaining compliance with complex regulatory requirements, frameworks, and guidelines. Failure to comply with regulations in any part of this network can lead to cascading compliance issues throughout the ecosystem.

Google Cloud's industry-leading security, third-party audits, and certifications help support your compliance. 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 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- ISO 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy - Data Processor)
- SOC 2 and SOC 3 reports
- NIST 800-53
- CSA Star
- GxP

Google also participates in sector and country-specific frameworks, such as FedRAMP (US government), BSI C5 (Germany), MTCS (Singapore), HIPAA (US government), iRAP (Australia), MeitY (India) and many others. We also provide resource documents and mappings to frameworks and laws where formal certifications or attestations may not be required or applied.

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

Furthermore, for years, Google Cloud's industry-leading controls, contractual commitments, and accountability tools have helped organizations across Europe meet stringent data protection regulatory requirements. This commitment to supporting the compliance efforts of European companies has earned us the trust of businesses like retailers, manufacturers and financial services providers.

As part of our continued efforts to uphold that trust, Google Cloud was one of the first cloud providers to support and adopt the EU GDPR Cloud Code of Conduct (CoC). The CoC is a mechanism for cloud providers to demonstrate how they offer sufficient guarantees to implement appropriate technical and organizational measures as data processors under the GDPR.

4.2 Compliance support for customers

Regulations such as GDPR place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and security incidents will be managed. Google Cloud has dedicated teams of engineers and compliance experts who support our customers in meeting their regulatory compliance and risk management obligations. Our approach includes **collaborating with customers** to understand and address their specific regulatory needs. Together with our reports and certifications, we assist our customers in documenting an **integrated controls and governance framework**.

For customers in certain regions or customers operating in certain regulated verticals, we allow customers to conduct **audits** to validate Google's security and compliance controls.

5. Conclusion

Protecting customer data is a primary design consideration for Google Cloud's infrastructure, applications, and personnel operations. Google's security practices are verified by independent third-parties, providing assurance to customers regarding our security controls and practices. Google offers strong contractual commitments to ensure our customers maintain control over their data and its processing, including the commitment that we only process your customer data according to your instructions.

Google Cloud is designed 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 Cloud, 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, 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.