G Suite Security and Trust

Protecting your data is our top priority

Google Cloud

Table of contents

Leading with a security-first mindset

Google started in the cloud and runs on the cloud, so it's no surprise that we fully understand the security implications of powering your business in the cloud. Because Google and our enterprise services run on the same infrastructure, your organization will benefit from the protections we've built and use every day. Our robust global infrastructure, along with over 700 security professionals and our drive to innovate, enables Google to stay ahead of the curve and offer a highly secure, reliable, and compliant environment.

Trusted by the world's leading organizations.

Whirlpool CORPORATION

asics

hp

Shaw FLOORS

pwc

salesforce

Secure by design

Cutting-edge cloud security

Top-notch data center security

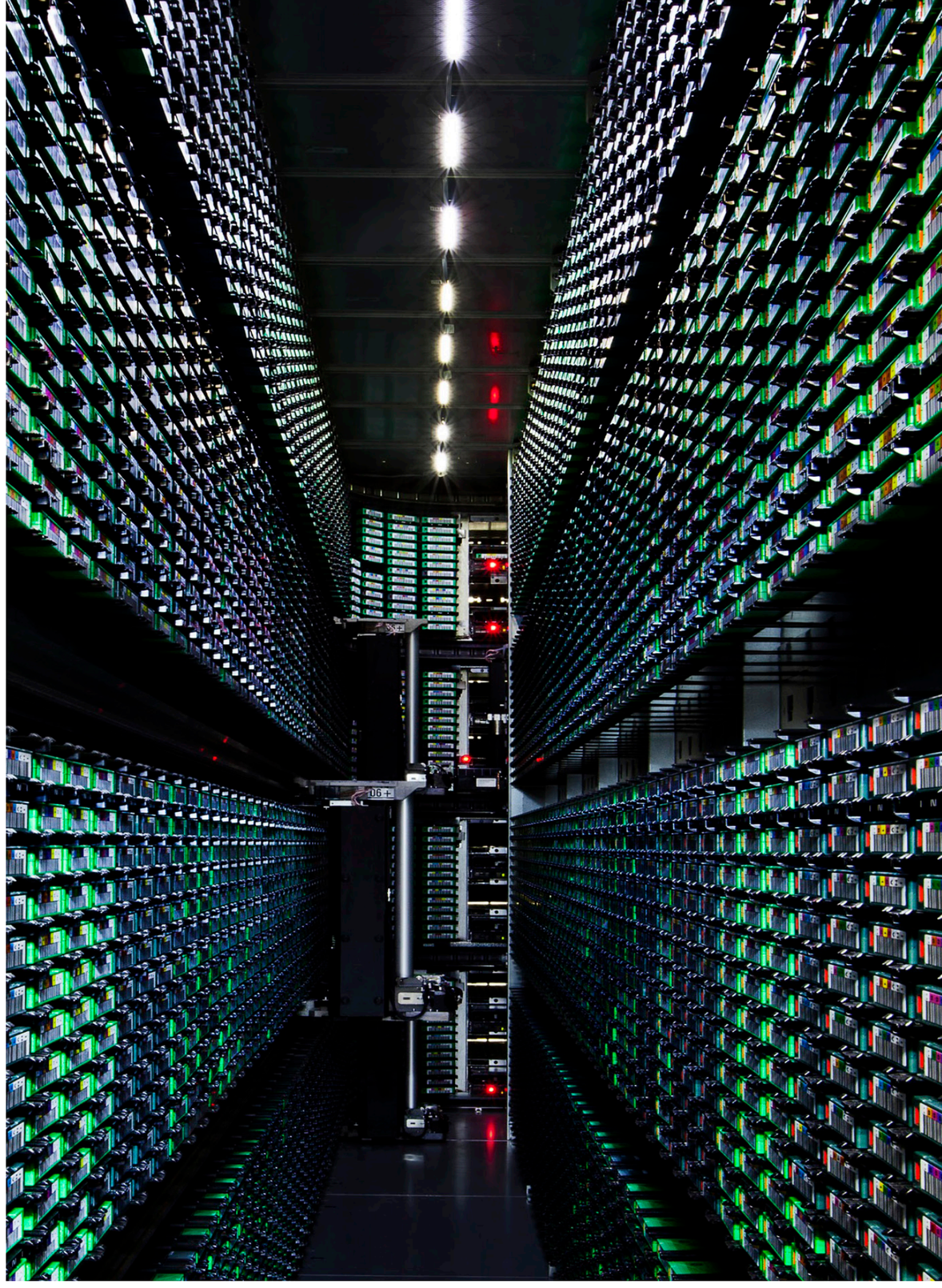
Security and data protection are central to the design of Google's data centers. Our physical security model includes safeguards like custom electronic access cards, perimeter fencing, and metal detectors. We also use cutting-edge tools like biometrics and laser-based intrusion detection to make physical breaches a "Mission: Impossible" scenario for would-be attackers. See inside a Google data center.

Hardware designed for performance

Google runs its data centers using custom designed hardware with a hardened operating system and file system. Each of these systems is optimized for security and performance. Since Google controls the hardware stack, we can quickly respond to any threats or weaknesses that may emerge.

A resilient, highly reliable network

Google's application and network architecture is designed for maximum reliability and uptime. Because data is distributed across Google's servers and data centers, your data will still be accessible if a machine fails—or even if an entire data center goes down. Google owns and operates data centers around the world to keep the services you use running 24 hours a day, every day of the year. Our integrated approach to infrastructure security works in concert across multiple layers: hardware infrastructure, service deployment, user identity, storage, Internet communication, and operations security. Learn more in Google Cloud's Infrastructure Security Design Whitepaper.



Data Encryption at Every Step

Google's private, global, software-defined network provides more flexibility, control, and security than any other cloud service provider. Our network connects multiple data centers using our own fiber, public fiber, and undersea cables. This allows us to deliver identical, highly available, low-latency services to G Suite customers across the globe, and limits exposure of customer data to the public Internet, where it may be subject to intercept. G Suite customers' data is encrypted when it's on a disk, stored on backup media, moving over the Internet, or traveling between data centers. Encryption is an important piece of the G Suite security strategy, helping to protect your emails, chats, Google Drive files, and other data.

Get additional details on how data is protected at rest, in transit, and on backup media, as well as information on encryption key management, in the G Suite Encryption Whitepaper.

Contributing to the community

Google's research and outreach activities protect the wider community of Internet users—beyond just those who choose our solutions. Our full-time team known as Project Zero aims to discover high-impact vulnerabilities in widely used products from Google and other vendors. We commit to doing our work transparently and to directly reporting bugs to software vendors—without involving third parties.

Promoting a culture of security

At Google, all employees are required to think "security first." Google employs more than 700 full-time security and privacy professionals, including some of the world's leading experts in information, application, and network security. To ensure Google stays protected, we incorporate security into our entire software development process. This can include having security professionals analyze proposed architectures and perform code reviews to uncover security vulnerabilities and better understand the different attack models for a new product or feature. When situations do arise, our dedicated G Suite Incident Management Team is committed to ensuring incidents are addressed with minimal disruption to our customers through rapid response, analysis, and remediation.

Staying ahead of the security curve

Security has always been a top priority for Google. Here are a few ways we've set the bar higher.

- **Perfect forward secrecy**
  Google is the first major cloud provider to enable perfect forward secrecy, which encrypts content as it moves between our servers and those of other companies. With perfect forward secrecy, private keys for a connection are ephemeral, which in turn prevents retroactive decryption of HTTPS sessions by an adversary or even the server operator. Many industry peers have followed suit or committed to adoption in the future.

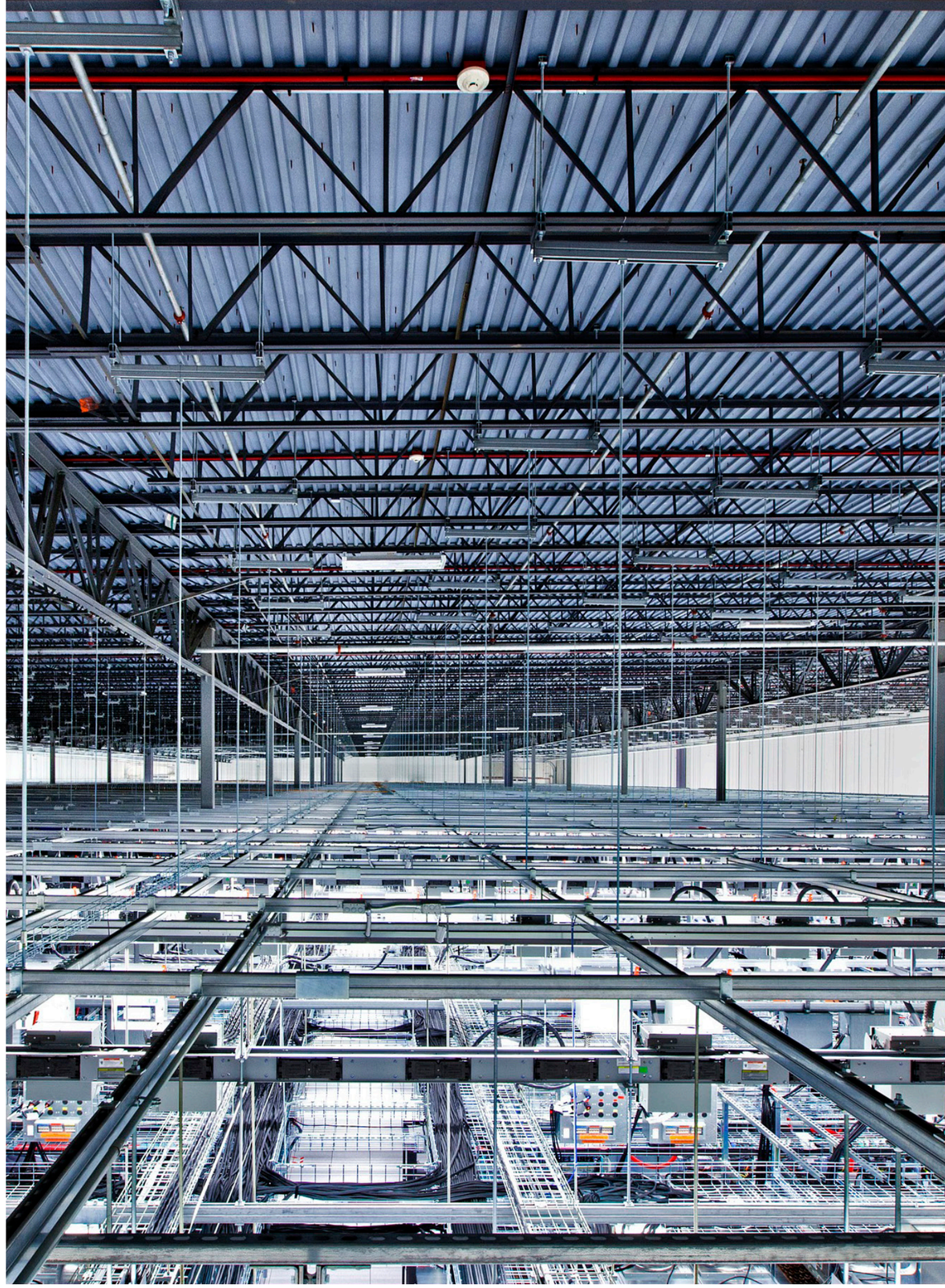
- **100% email encryption**
  Every single email message you send or receive is encrypted while moving between Google's data centers. This ensures that your messages are safe not only when they move between your devices and Gmail's servers, but also as they move internally within Google. We were also the first to let users know when their email was sent insecurely across providers with the introduction of our TLS indicator.

- **Strengthening Encryption**
  To protect against cryptanalytic advances, in 2013 Google doubled its RSA encryption key length to 2,048 bits and started changing them every few weeks, raising the bar for the rest of the industry.

Product security innovation

Data protection you can trust and tailor

G Suite offers administrators enterprise control over system configuration and application settings—all in a dashboard that you can use to streamline authentication, asset protection, and operational control. You can choose the G Suite edition that best meets your organization's security needs.



Access and authentication

- **Strong authentication**
  2-step verification greatly reduces the risk of unauthorized access by asking users for additional proof of identity when signing in. Our security key enforcement offers another layer of security for user accounts by requiring a physical key. The key sends an encrypted signature and works only with the sites that it's supposed to, helping to guard against phishing. G Suite administrators can easily deploy, monitor, and manage the security keys at scale from within the administrator console—without installing additional software.
- **Suspicious login monitoring**
  We use our robust machine learning capabilities to help detect suspicious logins. When we discover a suspicious login, we notify administrators so they can work to ensure the accounts are secured.
- **Centralized cloud access management**
  With support for single sign-on (SSO), G Suite enables unified access to other enterprise cloud applications. Our identity and access management (Cloud IAM) service lets administrators manage all user credentials and cloud-application access in one place.
- **Enhanced email security**
  G Suite allows administrators to set customized rules requiring email messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME). These rules can be configured to enforce S/MIME when specific content is detected in email messages.

Asset protection

Data loss prevention

G Suite administrators can set up a data loss prevention (DLP) policy to protect sensitive information within Gmail and Drive. We provide a library of predefined content detectors to make setup easy. Once the DLP policy is in place, for example, Gmail can automatically check all outgoing email for sensitive information and automatically take action to prevent data leakage: either quarantine the email for review, tell users to modify the information, or block the email from being sent and notify the sender. With easy-to-configure rules and optical character recognition (OCR) of content stored in images, DLP for Drive makes it easy for administrators to audit files containing sensitive content and configure rules that warn and prevent users from sharing confidential information externally. Learn more in our DLP Whitepaper.

Asset Protection

- **Spam detection**
  Machine learning has helped Gmail achieve 99.9% accuracy in spam detection and block sneaky spam and phishing messages—the kind that could actually pass for wanted email. Less than 0.1% of email in the average Gmail inbox is spam, and incorrect filtering of mail to the spam folder is even less likely (less than 0.05%).
- **Malware detection**
  To help prevent malware, Google automatically scans every attachment for viruses across multiple engines prior to a user downloading it. Gmail even checks for viruses in attachments queued for dispatch. This helps to protect everyone who uses Gmail and prevents the spread of viruses. Attachments in certain formats, such as .ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .EXE, .HTA, .INS, .ISP, .JAR, .JS, .JSE, .LIB, .LNK, .MDE, .MSC, .MSI, .MSP, .MST, .NSH, .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF, and .WSH are automatically blocked—even when they're included as part of a compressed file.
- **Phishing prevention**
  G Suite uses machine learning extensively to protect users against phishing attacks. Our learning models perform similarity analysis between previously classified phishing sites and new, unrecognized URLs. As we find new patterns, we adapt more quickly than manual systems ever could. G Suite also allows administrators to enforce the use of security keys, making it impossible to use credentials compromised in phishing attacks.
- **Brand phishing defense**
  To help prevent abuse of your brand in phishing attacks, G Suite follows the DMARC standard, which empowers domain owners to decide how Gmail and other participating email providers handle unauthenticated emails coming from your domain. By defining a policy, you can help protect users and your organization's reputation.

Operational control

- **Integrated device management**
  G Suite's fully integrated mobile device management (MDM) offers continuous system monitoring and alerts you to suspicious device activity. Administrators can enforce mobile policies, encrypt data on devices, lock lost or stolen mobile devices, and remotely wipe devices.

- **Third-party application access controls**
  As part of our authentication controls, administrators get visibility and control into third-party applications leveraging OAuth for authentication and corporate data access. OAuth access can be disabled at a granular level, and vetted third-party apps can be whitelisted.

- **Information rights management**
  To help administrators maintain control over sensitive data, we offer information rights management (IRM) in Drive. Administrators and users can disable downloading, printing, and copying of files from the advanced sharing menu, as well as set expiration dates on file access.

Operational control

- **Security center**

  The security center for G Suite provides a single, comprehensive view into the security posture of your G Suite deployment. It brings together security analytics, best practice recommendations, and integrated remediation that empower you to protect your organization's data, devices, and users.

- **Data regions**

  Many organizations leverage the power of our distributed data centers to maximize critical benefits, such as minimal latency and robust geo-redundancy. However, for organizations with stringent control requirements, data regions for G Suite lets you choose where certain covered data should be stored at rest—globally distributed, US, or Europe.

- **Alert center**

  The alert center for G Suite is a new way for admins to view essential notifications, alerts, and actions across G Suite. Insights around these potential alerts can help administrators assess their organization's exposure to security issues. Integrated remediation with the security center offers a streamlined way to resolve these issues.

Compliance, eDiscovery, and analytics

Equipped for the toughest standards

Google designed G Suite to meet stringent privacy and security standards based on industry best practices. In addition to strong contractual commitments regarding data ownership, data use, security, transparency, and accountability, we give you the tools you need to help meet your compliance and reporting requirements.

Certification audits and assesments

Google customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis.

- **ISO 27001**
  ISO 27001 is one of the most widely recognized and accepted independent security standards. Google has earned ISO 27001 certification for the systems, technology, processes, and data centers that run G Suite. View our ISO 27001 certificate.
- **ISO 27017**
  ISO 27017 is an international standard of practice for information security controls based on ISO/IEC 27002 specifically for cloud services. Our compliance with the international standard was certified by Ernst & Young CertifyPoint, an ISO certification body accredited by the Dutch Accreditation Council (a member of the International Accreditation Forum, or IAF). View our ISO 27017 certificate.
- **ISO 27018**
  G Suite's compliance with ISO/IEC 27018:2014 affirms our commitment to international privacy and data protection standards. ISO 27018 guidelines include not using your data for advertising, ensuring that your data in G Suite services remains yours, providing you with tools to delete and export your data, protecting your information from third-party requests, and being transparent about where your data is stored. View our ISO 27018 certificate.

Certification audits and assessments

- **SOC 2 and SOC 3**
  The American Institute of Certified Public Accountants (AICPA) SOC (Service Organization Controls) 2 and SOC 3 audit framework relies on its Trust Principles and Criteria for security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports. Download our SOC 3 report.

- **FedRAMP**
  G Suite products are compliant with the requirements of the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is the cloud security standard of the U.S. government. G Suite is authorized for use by federal agencies for data it has classified at a “Moderate” impact level, which may include PII and Controlled Unclassified Information. G Suite has been assessed as adequate for use with “OFFICIAL” (including “OFFICIAL SENSITIVE”) information in accordance with the UK Security Principles. For details on product and services compliance, visit the FedRAMP Google Services page.

- **PCI DSS**
  G Suite customers who need to maintain Payment Card Industry Data Security Standard (PCI DSS) compliance can set up a data loss prevention (DLP) policy that prevents emails containing payment card information from being sent from G Suite. For Drive, Vault can be configured to run audits and make sure no cardholder data is stored.

Certification audits and assessments

- **FISC Compliance**
  FISC (Center for Financial Industry Information Systems) is a public interest incorporated foundation tasked with conducting research related to technology, utilization, control, and threat/defense related to financial information systems in Japan. One of the key documents created by the organization is the “FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions,” which describes controls related to facilities, operations, and technical infrastructure. Google has developed a guide to help customers understand how Google’s control environment aligns with the FISC guidelines. Most of the controls outlined in our guide are part of our third-party audited compliance programs, including ISO 27001, ISO 27017, and ISO 27108 certifications. View our response to the FISC controls. For further information, please contact sales.

- **Esquema Nacional de Seguridad (ENS) - Spain**
  The Esquema Nacional de Seguridad (ENS) accreditation scheme for Spain has been developed by La Entidad Nacional de Acreditación (ENAC) in close collaboration with the Ministry of Finance and Public Administration and the National Cryptologic Centre (CCN). The ENS was established as part of Royal Decree 3/2010 (amended by Decree 951/2015) and serves to establish principles and requirements for the adequate protection of information for Spanish public sector entities. Google Cloud (GCP and G Suite) has met the requirements to comply with ENS at the ‘High’ level.

Regulatory compliance

- **HIPAA**
  G Suite supports customers' compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA), which governs the safeguarding, use, and disclosure of protected health information (PHI). Customers who are subject to HIPAA and wish to use G Suite for PHI processing or storage can sign a Business Associate Amendment with Google. View more details about HIPAA compliance with G Suite.

- **EU Model Contract Clauses**
  G Suite meets data protection recommendations from the Article 29 Working Party and maintains adherence to EU Model Contract Clauses with our Data Processing Amendment, Subprocessor Disclosure, and EU Model Contract Clauses. Google also maintains compliance with Privacy Shield and allows for Data Portability, wherein administrators can export data in standard formats without any additional charge.

Regulatory compliance

- **General Data Protection Regulation**
  At G Suite, we champion initiatives that prioritize and improve the security and privacy of user data. We've made updates to our Data Processing Amendment to ensure that G Suite customers can confidently use our services now that the General Data Protection Regulation (GDPR) is in effect. We've also implemented stringent policies, processes, and controls through our Data Processing Amendment and Model Contract Clauses. In those agreements we commit to comply with the obligations applicable to us under the GDPR with respect to the processing we do on behalf of our customers, and we have worked closely with European Data Protection Authorities to meet their expectations. Learn more
- **U.S. FERPA**
  Millions of students rely on G Suite for Education. G Suite for Education services comply with the Family Educational Rights and Privacy Act (FERPA). Our commitment to this compliance is included in our agreements.
- **COPPA**
  Protecting children online is important to us. We contractually require G Suite for Education schools to obtain the parental consent that the Children's Online Privacy Protection Act of 1998 (COPPA) requires, and our services can be used in compliance with COPPA.
- **South Africa's POPI Act**
  Google provides product capabilities and contractual commitments to facilitate customer compliance with South Africa's Protection of Personal Information (POPI) Act. Customers who are subject to POPI can define how their data is stored, processed, and protected by signing a Data Processing Amendment.

eDiscovery and archiving

- **Data retention and eDiscovery**
  Google Vault lets you retain, archive, search, and export your organization's email for your eDiscovery and compliance needs. Vault is entirely web-based, so there's no need to install or maintain extra software. With Vault, you can search your Gmail, Drive, and Groups data, set custom retention policies, place user accounts (and related data) on litigation hold, export point-in-time Drive files, and manage related searches.

- **Export evidence**
  Google Vault allows you to export specific emails, on-the-record chats, and files to standard formats for additional processing and review—all in a manner that supports legal standards while respecting chain-of-custody guidelines.

- **Content compliance**
  G Suite's monitoring tools allow administrators to scan email messages for alphanumeric patterns and objectionable content. Administrators can create rules to either reject matching emails before they reach their intended recipients or deliver them with modifications.

Reporting analytics

- **Easy monitoring**
  Easy interactive reports help you assess your organization's exposure to security issues at a domain and user level. Extensibility with a collection of application programming interfaces (APIs) enable you to build custom security tools for your own environment. With insight into how users are sharing data, which third-party apps are installed, and whether appropriate security measures such as 2-step verification are in place, you can improve your security posture.

- **Audit tracking**
  G Suite allows administrators to track user actions and set up custom alerts within G Suite. This tracking spans across the Admin Console, Gmail, Drive, Calendar, Groups, mobile, and third-party application authorization. For example, if a marked file is downloaded or if a file containing the word "Confidential" is shared outside the organization, administrators can be notified.

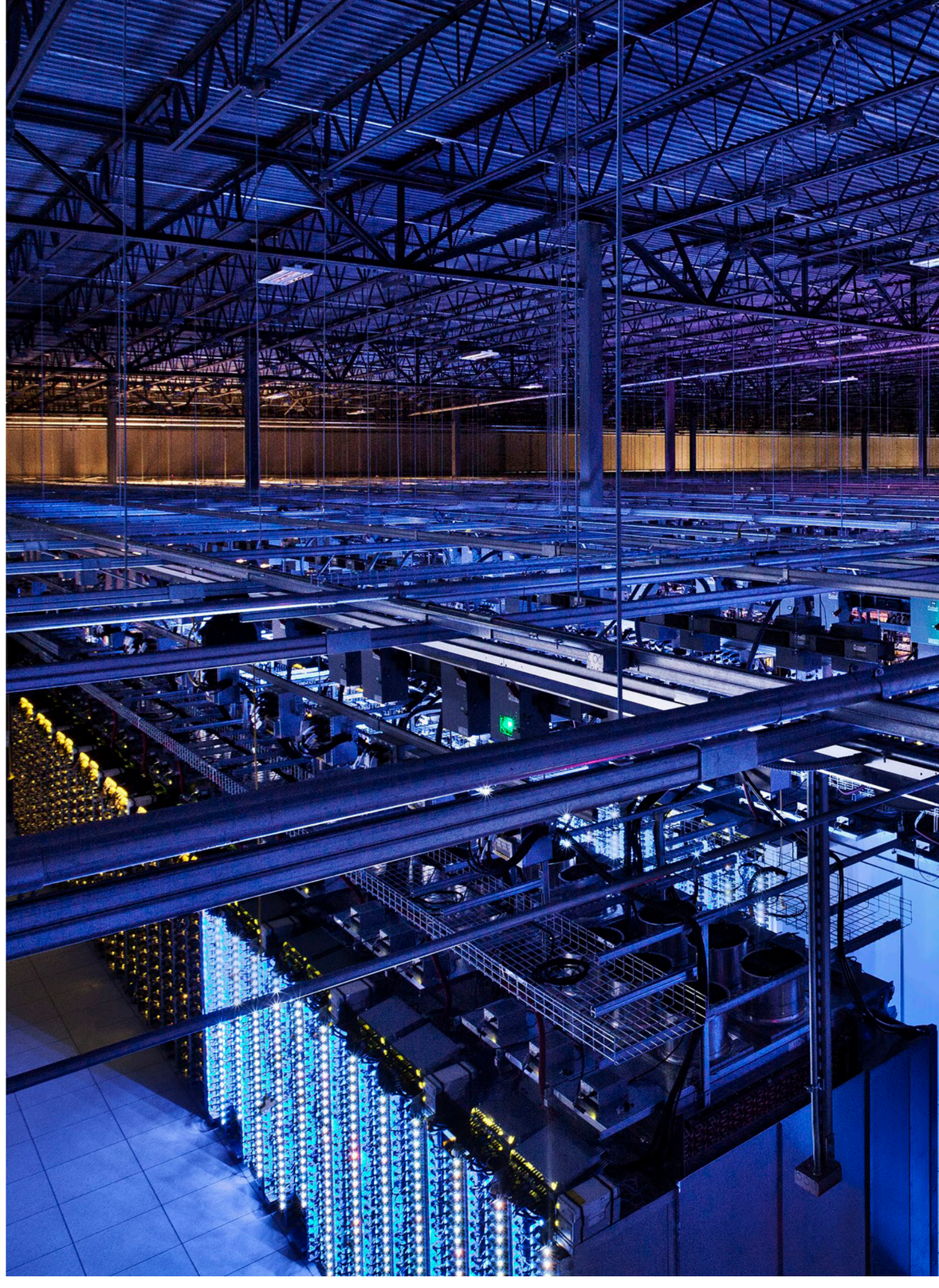
- **Insights using BigQuery**
  With BigQuery, Google's enterprise data warehouse for large-scale data analytics, you can analyze Gmail logs using sophisticated, high-performing custom queries, and leverage third-party tools for deeper analysis.

Transparency

Trust is essential to our partnership

Transparency is part of Google's DNA. We work hard to earn and maintain trust with our customers through transparency. The customer — not Google — owns their data. Google does not sell your data to third parties; there is no advertising in G Suite; and, we never collect or use data from G Suite services for any advertising purposes."

Google offers customers a detailed Data Processing Amendment that describes our commitment to protecting your data. For example, under the Data Processing Amendment, Google will process your data for any purpose specified in your agreement. Further, we commit to deleting all data from our systems within 180 days of your deleting it in our services. Finally, we provide tools to make it easy for you to take your data with you if you choose to stop using our services altogether, without penalty or additional cost imposed by Google.



Trust is essential to our partnership

- **No ads, ever**
  Google does not collect, scan, or use your data in G Suite services for advertising purposes, and we do not display ads in G Suite. We use your data to provide G Suite services, and for system support, such as spam filtering, virus detection, spell-checking, capacity planning, traffic routing, and the ability to search for emails and files within an individual account.

- **You own your data**
  The data that companies, schools, and government agencies put into G Suite services does not belong to Google. Whether it's corporate intellectual property, personal information, or a homework assignment, Google does not own that data, and Google does not sell that data to third parties.

- **Your apps are always accessible**
  G Suite offers a 99.9% service level agreement. Furthermore, G Suite has no scheduled downtime or maintenance windows. Unlike most providers, we plan for our applications to always be available, even when we're upgrading our services or maintaining our systems.

- **You stay in control and in the know**
  We're committed to providing you with information about our systems and processes—whether that's a real-time performance overview, the results of a data handling audit, or the location of our data centers. It's your data; we ensure you have control over it. You can delete your data or export it at any time. We regularly publish Transparency Reports detailing how governments and other parties can affect your security and privacy online. We think you deserve to know, and we have a long track record of keeping you informed and standing up for your rights.

Google Cloud