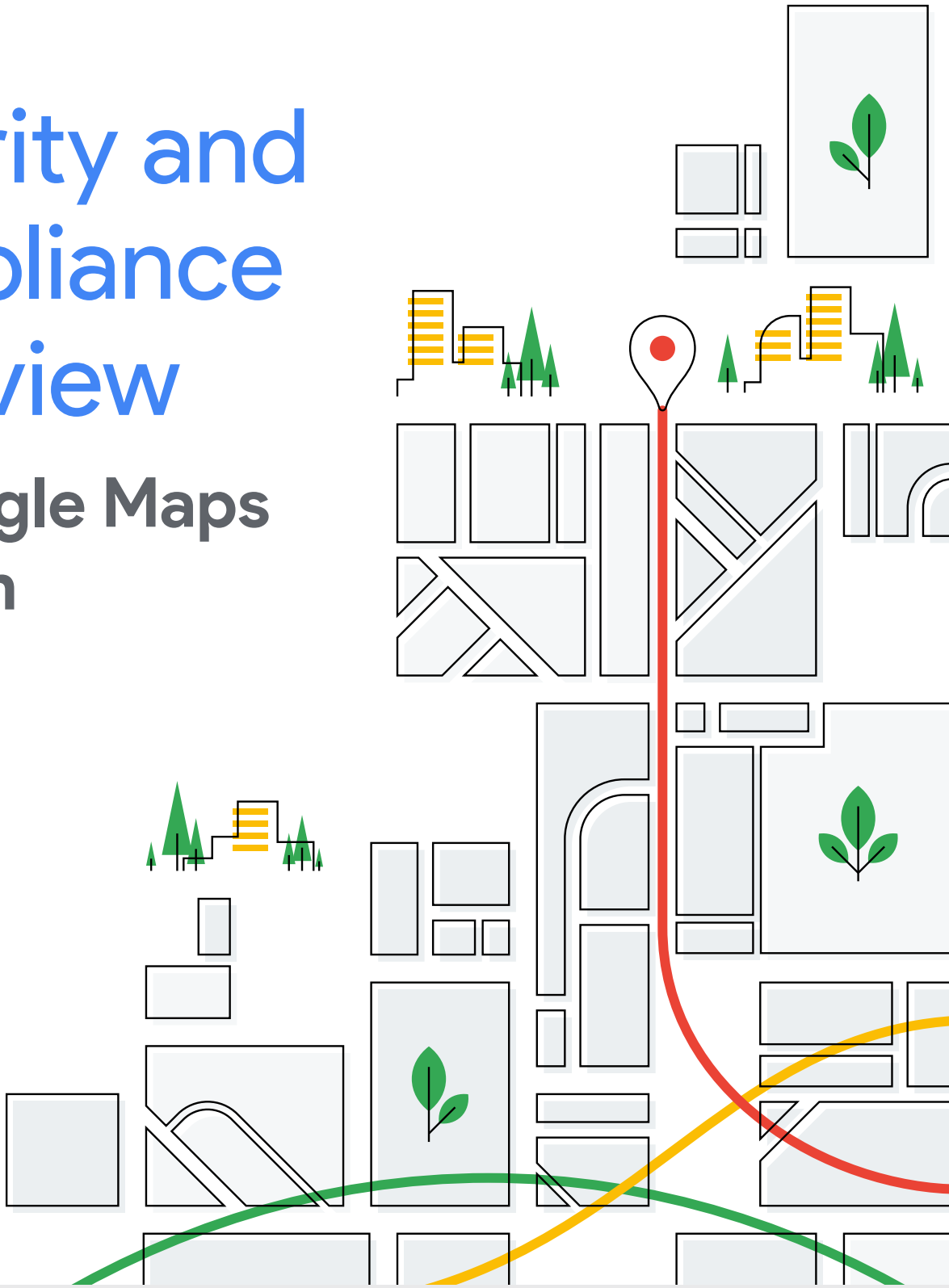
Security and Compliance Overview

for Google Maps Platform



Google Maps Platform

Contents

continues next page

Contents

Security and Compliance Overview

for Google Maps Platform

This content was last updated in April 2024, 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.

Introduction

Google Maps Platform provides APIs and SDKs for customers and partners to develop web and mobile applications using Google's geospatial technology. Google Maps Platform offers over 50+ APIs and SDK for customers across multiple industries. As a customer in industry, you must often meet security, data usage, and regulatory requirements when building your solutions. This includes ensuring your third-party technology meets those same requirements.

This document provides a high-level summary of the people, process, and technology controls offered by Google Maps Platform, along with describing the benefits of using the platform. First, it's important to understand the two primary technology pillars beneath Google Maps Platform:

- **Google-provided technologies, data centers, and infrastructure.** Google Maps Platform operates entirely on Google-provided data centers and infrastructure. From this basis it applies internal and 3rd-party audits to the security controls it inherits from Google to validate that Google Maps Platform correctly implements the security, operational, and technical controls described in this paper.
- **Google Maps Platform technology.** In addition to the inherited controls, Google Maps Platform provides additional security, privacy, data, and operational controls for Google's product suites.

This document summarizes Google Maps Platform's security processes and controls, grouped as follows:

- Focus on security and privacy at all levels of Google's organization
- Technical infrastructure and hardware security
- Operational security
- Key security controls
- Client-side security, both web and mobile
- Current certifications and audits in Google Maps Platform
- Supported legal frameworks, globally

Potential customers can reach out to their Google sales representative for additional information.

Google's security and privacy-focused organization

Security drives the organizational structure, culture, training priorities, and hiring processes across Google. It shapes the design of Google data centers and the technology they provide. Security underpins Google's everyday operations, including disaster planning and threat management. Google prioritizes security in how it handles data, account controls, compliance audits, and industry certifications. Google designs its services to deliver better security than many on-premise alternatives that rely on multiple vendors and multiple platforms where security is often an unconnected process. You benefit from Google's integrated security programs and controls when you leverage Google Maps Platform products for your business. Google Maps Platform makes security a priority in its operations—operations that serve over a billion users across the world.

Together, Google and Google Maps Platform provide multiple layers of security throughout the company and organization:

- Google dedicated security team
- Google Maps Platform product security team
- Active involvement with the global security research community
- Google Maps Platform privacy team
- Google employee security and privacy training
- Internal audit and compliance specialists

Dedicated security teams at Google

Google provides dedicated security teams across the company and within product areas.

The **Google-wide security teams** support multiple product areas at Google, including Google Maps Platform. The security team includes some of the world's foremost experts in information security, application security, cryptography, and network security. Their activities include the following:

- **Develops, reviews, and implements security processes.** This includes reviewing security plans for Google networks and providing project-specific consulting to product and engineering teams across Google. For example, cryptography specialists review product launches that implement cryptography as part of the offering.
- **Actively manages security threats.** Using both commercial and custom tools, the team monitors ongoing threats and suspicious activity on Google networks.
- **Performs routine audits and evaluations**, which can involve engaging outside experts to conduct security assessments.
- **Publishes security articles to the wider community.** Google maintains a security blog and a YouTube Series highlighting several of the specific Security Teams and their accomplishments.

The Google Maps Platform security team collaborates with the Google-wide security team, working more closely with product development and SRE to oversee security implementation. Specifically, this team manages the following:

- Google Maps Platform's Disaster Resilience Testing (DiRT), which tests the business continuity and failover of Google Maps Platform products, runs on Google's highly available infrastructure.
- Third party penetration testing. Google Maps Platform products are penetration tested on at least an annual basis to enhance Google's security posture and provide you with independent security assurance.

Collaboration with the security research community

Google has long enjoyed a close relationship with the security research community, and Google greatly values their help with identifying potential vulnerabilities in Google Maps Platform and other Google products.

- **Online community collaboration via Project Zero.** Project Zero is a team of security researchers dedicated to researching zero-day vulnerabilities. Some examples of this research are the discovery of the Spectre exploit, the Meltdown exploit, the POODLE SSL 3.0 exploit, and cipher suite weaknesses.
- **Academic research** - Google's security engineers and researchers actively participate and publish in the academic security community and the privacy research community. Security related publications can be found on Google's Google Research site. Google's security teams have published an in-depth account of their practices and experience in the Building Secure and Reliable Systems book.
- **Vulnerability Rewards Program** - Google Maps Platform participates in the Vulnerability Reward Program which offers rewards in the tens of thousands of dollars for each confirmed vulnerability. The program encourages researchers to report design and implementation issues that might put customer data at risk. In 2022, Google awarded researchers over $11.9 million in prize money. For more information about this program, including the rewards Google gave, see Bug Hunters Key Stats. Additional information on reporting security issues, see How Google handles security vulnerabilities.
- **Open source security research** - Google's engineers also organize and participate in open source projects and academic conferences. To improve open-source code, the Vulnerability Reward Program also provides subsidies to open-source projects.
- **Cryptography** - Google's world-class cryptographers worked to protect TLS connections against quantum computer attacks and developed the combined elliptic-curve and post-quantum (CECPQ2) algorithm. Google cryptographers developed Tink, which is an open source library of cryptographic APIs. Google also uses Tink in its internal products and services.

Google Maps Platform's dedicated privacy team

The dedicated privacy team operates separately from product development and security organizations. It supports internal privacy initiatives to improve all parts of privacy: critical processes, internal tools, infrastructure, and product development. The privacy team performs the following:

- Ensures that product launches incorporate strong privacy standards around data collection. It participates in every Google product launch through both design documentation and code reviews.
- After product launch, the privacy team oversees automated processes that continually verify appropriate data collection and use.
- Conducts research on privacy best practices.

Google employee security and privacy training

Security and privacy are an ever-changing area, and Google recognizes that dedicated employee engagement is a key means of raising awareness. All Google employees undergo security and privacy training as part of the orientation process, and they receive ongoing, mandatory security and privacy training throughout their Google careers.

- **During orientation:** New employees agree to Google's Code of Conduct, which highlights Google's commitment to keeping customer information safe and secure.
- **Specialized training by job role.** Certain job roles require training on specific aspects of security. For instance, the information security team instructs new engineers on secure coding practices, product design, and automated vulnerability testing tools. Engineers attend regular security briefings and receive security newsletters that cover new threats, attack patterns, mitigation techniques, and more.
- **Ongoing events.** Google hosts regular internal conferences open to all employees to raise awareness and drive innovation in security and data privacy. Google hosts events across global offices to raise awareness of security and privacy in software development, data handling, and policy enforcement.

Internal audit and compliance specialists

Google Maps Platform has a dedicated internal audit team that reviews Google products' compliance with security laws and regulations around the world. As new auditing standards are created and existing standards are updated, the internal audit team determines what controls, processes, and systems are needed to help meet those standards. This team supports independent audits and assessments by third parties. For more information, see Security Certifications & Audits section later in this document.

Platform built with security at its core

Google designs its servers, proprietary operating systems, and geographically distributed data centers using the principle of defense in depth. Google Maps Platform runs on a technical infrastructure designed and built to operate securely. We've created an IT infrastructure that is more secure and easier to manage than more traditional on-premises or hosted solutions.

State-of-the-art data centers

Google's focus on security and protection of data is among Google's primary design criteria. The physical security in Google data centers is a layered security model. Physical security includes safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. In addition, to detect and track intruders, Google uses security measures such as laser beam intrusion detection and 24/7 monitoring by high-resolution interior and exterior cameras. Access logs, activity records, and camera footage are available in case an incident occurs. Experienced security guards, who have undergone rigorous background checks and training, routinely patrol Google's data centers. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible through a security corridor that implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Google employees will ever set foot in one of Google's data centers.

Google operates data centers globally and to maximize the speed and reliability of its services. Its infrastructure is generally set up to serve traffic from the data center that is the closest to where the traffic originates. Therefore the precise location of Google Maps Platform data may vary depending on where such traffic originates, and this data may be handled by servers located in the EEA and UK or transferred to third countries. Google customers' offerings where Google Maps Platform products are implemented are generally available globally and often attract a global audience. The technical infrastructure that supports these products is deployed globally to reduce latency and ensure redundancy of systems. Google Maps Platform uses a subset of Google Global Data Center Network listed below for reference:

North & South America

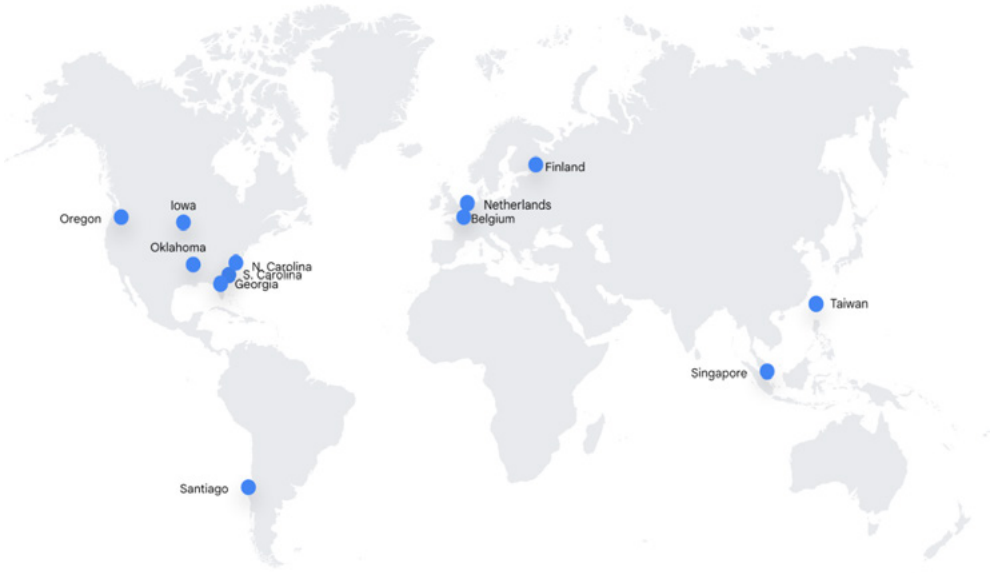
- The United States
- Chile

Europe

- Belgium
- Finland
- The Netherlands

Asia

- Taiwan
- Singapore



Powering Google data centers

To keep things running 24/7 and provide uninterrupted services, Google data centers have redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature for servers and other hardware, which reduces the risk of service outages while minimizing environmental impact. Fire detection and suppression equipment helps prevent hardware damage. Heat detectors, fire detectors, and smoke detectors trigger audible and visible alarms at security operations consoles and at remote monitoring desks.

Google is the first major internet services company to get external certification of its high environmental, workplace safety, and energy management standards throughout Google data centers. For example, to demonstrate Google's commitment to energy management practices, Google obtained voluntary ISO 50001 certifications for its data centers in Europe.

Custom server hardware and software

Google data centers have purpose-built servers and network equipment, some of which Google designs. While Google's servers are customized to maximize performance, cooling, and power efficiency, they are also designed to help protect against physical intrusion attacks. Unlike most commercially available hardware, Google's servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, all of which can introduce vulnerabilities. Google vets component vendors and chooses components with care, working with vendors to audit and validate the security properties that are provided by the components. Google designs custom chips, such as Titan, that help us securely identify and authenticate legitimate Google devices at the hardware level, including the code that these devices use to boot up.

Server resources are dynamically allocated. This gives us flexibility for growth and lets us adapt quickly and efficiently to customer demand by adding or reallocating resources. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary-level modifications. Google's automated, self-healing mechanisms are designed to enable us to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromises on the network.

Secure service deployment

Google services are the application binaries that Google developers write and run on Google's infrastructure. To handle the required scale of the workload, thousands of machines might be running binaries of the same service. A cluster orchestration service, called Borg, controls the services that are running directly on the infrastructure.

The infrastructure does not assume any trust between the services that are running on the infrastructure. This trust model is referred to as a zero-trust security model. A zero-trust security model means that no devices or users are trusted by default, whether they are inside or outside of the network.

Because the infrastructure is designed to be multi-tenant, data from Google's customers (consumers, businesses, and even Google's own data) is distributed across shared infrastructure. This infrastructure is composed of tens of thousands of homogeneous machines. The infrastructure does not segregate customer data onto a single machine or set of machines

Hardware tracking and disposal

Google meticulously tracks the location and status of all equipment within its data centers using barcodes and asset tags. Google deploys metal detectors and video surveillance to help make sure that no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its lifecycle, it's removed from inventory and retired.

Google storage devices, including hard drives, solid-state drives, and non-volatile dual in-line memory modules (DIMM), use technologies like full disk encryption (FDE) and drive locking to protect data at rest. When a storage device is retired, authorized individuals verify that the disk is erased by writing zeros to the drive. They also perform a multiple-step verification process to ensure the drive contains no data. If a drive cannot be erased for any reason, it's physically destroyed. Physical destruction is done by using a shredder that breaks the drive into small pieces, which are then recycled at a secure facility. Each data center adheres to a strict disposal policy and any variances are immediately addressed.

Security benefits of Google's global network

In other geospatial cloud and on-premises solutions, data travels between devices across the public internet in paths known as *hops*. The number of hops depends on the optimal route between the customer's ISP and the data center. Each additional hop introduces a new opportunity for data to be attacked or intercepted. Because Google's global network is linked to most ISPs in the world, Google's network limits hops across the public internet, and therefore helps limit access to that data by bad actors.

Google's network uses multiple layers of defense—defense in depth—to help protect the network against external attacks. Only authorized services and protocols that meet Google's security requirements are allowed to traverse it; anything else is automatically dropped. To enforce network segregation, Google uses firewalls and access control lists. All traffic is routed through Google Front End (GFE) servers to help detect and stop malicious requests and distributed denial-of-service (DDoS) attacks. Logs are routinely examined to reveal any exploitation of programming errors. Access to networked devices is restricted to only authorized employees.

Google's global infrastructure allows us to run Project Shield, which provides free, unlimited protection to websites that are vulnerable to DDoS attacks that are used to censor information. Project Shield is available for news websites, human rights websites, and election-monitoring websites.

Low latency and highly available solutions

Google's IP data network consists of its own fiber, of publicly available fiber, and of undersea cables. This network allows us to deliver highly available and low-latency services across the globe.

Google designs the components of its platform to be highly redundant. This redundancy applies to Google's server design, to how Google stores data, to network and internet connectivity, and to the software services themselves. This "redundancy of everything" includes exception handling and creates a solution that is not dependent on a single server, data center, or network connection.

Google data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption.

Google's highly redundant infrastructure also helps you protect your business from data loss. Google's systems are designed to minimize downtime or maintenance windows for when we need to service or upgrade our platform.

Operational security

Security is integral to Google's operations, not an afterthought. This section describes Google's vulnerability management programs, malware prevention program, security monitoring, and incident management programs.

Vulnerability management

Google's internal vulnerability management process actively scans for security threats across all technology stacks. This process uses a combination of commercial, open source, and purpose-built in-house tools, and includes the following:

- Quality assurance processes
- Software security reviews
- Intensive automated and manual penetration efforts, including extensive Red Team exercises
- Recurring external penetration testing for Google Maps Platform products
- Recurring external audits

The vulnerability management organization and its partners are responsible for tracking and following up on vulnerabilities. Because security improves only after issues are fully addressed, automation pipelines continuously reassess the state of a vulnerability, verify patches, and flag incorrect or partial resolution.

Security monitoring

Google's security monitoring program is focused on information that's gathered from internal network traffic, from employee actions on systems, and from outside knowledge of vulnerabilities. A core Google principle is to aggregate and store all security telemetry data in one location for unified security analysis.

At many points across Google's global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. Google uses a combination of open source and commercial tools to capture and parse traffic so that Google can perform this analysis. A proprietary correlation system built on top of Google's technology also supports this analysis. Google supplements network analysis by examining system logs to identify unusual behavior, such as attempts to access customer data.

The Threat Analysis Group at Google monitors threat actors and the evolution of their tactics and techniques. Google security engineers review inbound security reports and monitor public mailing lists, blog posts, and wikis. Automated network analysis and automated analysis of system logs helps determine when an unknown threat might exist. If the automated processes detect an issue, it's escalated to Google's security staff.

Intrusion detection

Google uses sophisticated data processing pipelines to integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Google's investigation and incident-response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. Google conducts Red Team exercises in addition to external penetration testing to measure and improve the effectiveness of Google's detection and response mechanisms.

Incident management

Google has a rigorous incident management process for security events that might affect the confidentiality, integrity, or availability of systems or data. Google's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61). Google provides training for key staff members in forensics and in handling evidence in preparation for an event, including the use of third-party and proprietary tools.

Google tests incident response plans for key areas. These tests consider various scenarios, including insider threats and software vulnerabilities. To help ensure the swift resolution of security incidents, the Google security team is available 24/7 to all employees.

Software development practices

Google uses source control protections and two-party reviews to proactively limit the introduction of vulnerabilities. Google also provides libraries that prevent developers from introducing certain classes of security bugs. For example, Google has libraries and frameworks designed to eliminate XSS vulnerabilities in SDKs. Google also has automated tools for detecting security bugs, such as fuzzers, static analysis tools, and web security scanners.

Source code protections

Google's source code is stored in repositories with built-in source integrity and governance, which makes it possible to audit both current and past versions of the service. The infrastructure requires that a service's binaries be built from specific source code after it is reviewed, checked in, and tested. Binary Authorization for Borg (BAB) is an internal enforcement check that occurs when a service is deployed. BAB does the following:

- Ensures that the production software and configuration deployed at Google is reviewed and authorized, particularly when that code can access user data
- Ensures code and configuration deployments meet certain minimum standards
- Limits the ability of an insider or adversary to make malicious modifications to source code and also provides a forensic trail from a service back to its source

Reducing Insider Risk

Google limits and actively monitors the activities of employees who have been granted administrative access to the infrastructure. Google continually works to eliminate the need for privileged access for particular tasks by using automation that can accomplish the same tasks in a safe and controlled way. For example, Google requires two-party approvals for some actions, and Google uses limited APIs that allow debugging without exposing sensitive information.

Google employee access to end-user information is logged through low-level infrastructure hooks. Google's security team monitors access patterns and investigates unusual events.

Disaster Recovery Testing - DiRT

Google Maps Platform runs annual, company-wide, multi-day Disaster Recovery Testing events (DiRT) to ensure that Google Maps Platform's services and internal business operations continue to run during a disaster. DiRT was developed to find vulnerabilities in critical systems by intentionally causing failures, and to fix those vulnerabilities before failures happen in an uncontrolled manner. DiRT tests Google's technical robustness by breaking live systems and tests Google's operational resilience by explicitly preventing critical personnel, area experts, and leaders from participating. All generally available services are required to have ongoing, active DiRT testing and validation of their resilience and availability.

To prepare for a DiRT exercise, Google employs a consistent set of rules around prioritization, communication protocols, impact expectations, and test design requirements, including pre-reviewed and approved rollback plans. DiRT exercises and scenarios not only force technical failures in the service itself, but also can include designed failures in process, availability of key personnel, supporting systems, communications, and physical access. DiRT validates that the processes in place actually work in practice. It also ensures that teams are pre-trained and have experience they can draw upon during actual outages, disruptions, and disasters man-made or natural.

Key security controls

This section describes the main security controls that Google Maps Platform implements to protect its platform.

Encryption

Encryption adds a layer of defense for protecting data. Encryption ensures that if an attacker gets access to data, the attacker cannot read the data without also having access to the encryption keys. Even if an attacker gets access to data (for example, by accessing the wire connection between data centers or by stealing a storage device), they won't be able to understand or decrypt it.

Encryption provides an important mechanism in how Google helps protect the privacy of data. It allows systems to manipulate data—for example, for backup—and engineers to support Google's infrastructure, without providing access to content for those systems or employees.

Encryption at rest

Encryption "at rest" in this section means encryption used to protect data that is stored on a disk (including solid-state drives) or backup media. Data is encrypted at the storage level, generally using AES256 (Advanced Encryption Standard). Data is often encrypted at multiple levels in Google's production storage stack in data centers, including at the hardware level, without requiring any action by Google customers. Using multiple layers of encryption adds redundant data protection and allows Google to choose the optimal approach based on application requirements. Google uses common cryptographic libraries which incorporate Google's FIPS 140-2 validated module to implement encryption consistently across products. Consistent use of common libraries means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code.

Protecting data in transit

Data can be vulnerable to unauthorized access as it travels across the internet. Google Maps Platform supports strong encryption in transit between customer devices and networks, and Google's Google Front End (GFE) servers. Google recommends that customers/developers use Google's strongest supported cipher suite (TLS 1.3) when creating applications as a best practice. Some customers have use cases that require older cipher suites for compatibility reasons, so Google Maps Platform supports these weaker standards, but does not recommend using them whenever possible. Google Cloud also offers you additional transport encryption options, including Cloud VPN for establishing virtual private networks using IPsec for Google Maps Platform products.

Protecting data in transit between Google data centers

Application Layer Transport Security (ALTS) ensures that the integrity of Google traffic is protected and encrypted as needed. After a handshake protocol between the client and the server is complete and the client and the server negotiate the necessary shared cryptographic secrets for encrypting and authenticating network traffic, ALTS secures RPC (Remote Procedure Call) traffic by forcing integrity, using the negotiated shared secrets. Google supports multiple protocols for integrity guarantees, such as AES-GMAC (Advanced Encryption Standard), with 128-bit keys. Whenever traffic leaves a physical boundary controlled by or on behalf of Google, for example in transit over WAN (Wide Area Network) between data centers, all protocols are upgraded automatically to provide encryption and integrity guarantees.

Google Maps Platform Service Availability

Some Google Maps Platform services might not be available across all geographies. Some service disruptions are temporary (due to an unanticipated event, such as a network outage), but other service limitations are permanent due to government-imposed restrictions. Google's comprehensive Transparency Report and status dashboard show recent and ongoing disruptions of traffic to Google Maps Platform services. Google provides this data to help you analyze and understand Google's uptime information.

Client-side security

Security is a shared responsibility between a Cloud Service Provider and the customer/partner implementing Google Maps Platform products. This section details the customer/partner responsibilities that should be considered when architecting a Google Maps Platform solution.

JavaScript APIs

Secure Sites

Maps JavaScript API publishes a set of recommendations that allow a customer to fine tune their site Content Security Policy (CSP) to avoid vulnerabilities like cross-site scripting, clickjacking, and data injection attacks. The JavaScript API supports two forms of CSP: strict CSP using nonces and allowlist CSP.

Secure JavaScript

The JavaScript is regularly scanned for known security anti-patterns, and problems are quickly remediated. The JavaScript API is released on a weekly cadence or on demand, should any problems arise.

Mobile Application Security (MAS)

Mobile Application Security (MAS) is an open, agile, crowd-sourced effort, made of the contributions of dozens of authors and reviewers from all over the world. The OWASP Mobile Application Security (MAS) flagship project provides a security standard for mobile apps (OWASP MASVS) and a comprehensive testing guide (OWASP MASTG) that covers the processes, techniques, and tools used during a mobile app security test, as well as an exhaustive set of test cases that enables testers to deliver consistent and complete results.

- OWASP Mobile Application Security Verification Standard (MASVS) provides a baseline for complete and consistent security tests for both iOS and Android.
- OWASP Mobile Application Security Testing Guide (MASTG) is a comprehensive manual covering the processes, techniques, and tools used during mobile application security analysis, as well as an exhaustive set of test cases for verifying the requirements listed in the MASVS.
- The OWASP Mobile Application Security Checklist contains links to the MASTG test cases for each MASVS control.
    - Security Assessments / Pentests: Ensure you're at least covering the standard attack surface and start exploring.
    - Standard Compliance: Includes MASVS and MASTG versions and commit IDs.
    - Learn and practice your mobile security skills.
    - Bug Bounties: Go step by step covering the mobile attack surface.

Consider leveraging the OWASP MAS to enhance your iOS and Android application security, testing, and authentication capabilities.

Android

When developing Android applications, another resource to consider are the Android community application best practices. The Security guidelines contain best-practices guidance on enforcing secure communications, defining the correct permissions, safe data storage, service dependencies and more.

iOS

When developing iOS applications, consider Apple's Introduction to Secure Coding Guide, which contains best practices for the iOS Platform.

Data collection, usage, and retention

Google Maps Platform is committed to transparency regarding data collection, data usage, and data retention. Google Maps Platform's data collection, usage, and retention are subject to the Google Maps Platform Terms of Service, which includes the Google Privacy Policy.

Data collection

Data is collected through use of Google Maps Platform Products. As a customer, you are in control of what information you transmit to Google Maps Platform through APIs and SDKs. All Google Maps Platform requests are logged, which include response status codes from the product.

Google Maps Platform logged data

Google Maps Platform logs data across the product suite. Logs contain multiple entries which typically include:

- **Account identifier** which can be an API key, Client ID, or Cloud project number. This is required for operations, support, and billing.
- **IP address** of the requesting server, service, or device. For APIs, note that the IP address sent to Google Maps Platform will be dependent on how the API invocation is implemented in your application/solution. For SDKs, the IP address of the invoking device is logged.
- **Request URL**, which contains the API and parameters being passed to the API. For example, the Geocoding API requires two parameters (address and API key). Geocoding also has a number of optional parameters. The request URL would contain all parameters passed to the service.
- **Date and time** of the request.
- **Web applications** have **request headers** logged which typically include data such as type of web browser and operating system.
- **Mobile Applications using an SDK** have the Google Play version, library, and application name logged.

Google Maps Platform log access

Access to logs is highly **restricted** and **authorized** only to specific team members who have a **legitimate** business need. Each **access** request to the log files is documented for **auditing** purposes, which is verified through Google's ISO 27001 and SOC 2 third-party audits.

Data usage

Data collected by Google Maps Platform is used for the following purposes:

- Improving Google products and services
- Providing customer technical support
- Operational monitoring and alerting
- Maintaining platform security
- Platform capacity planning

Please note that Google Maps Platform never sells user operation data to third parties as documented in Google's Privacy Policy.

Data retention and anonymization

Data collected in Google Maps Platform logs may be retained for various lengths of time based on business needs, subject to Google's data anonymization and redaction policies. IP addresses are automatically anonymized as soon as practicable (part of the IP address is deleted). Anonymized, aggregate usage statistics derived from logs may be retained indefinitely.

Security, industry, high availability, and environmental certifications & audits

ISO 27001:2022

The International Organization for Standardization (ISO) is an independent, non-governmental international organization with an international membership of 163 national standards bodies. The ISO/IEC 27000 family of standards helps organizations keep their information assets secure.

ISO/IEC 27001 outlines and provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks.

Google Maps Platform and Google's Common Infrastructure are certified as ISO/IEC 27001 compliant. The 27001 standard does not mandate specific information security controls, but the framework and checklist of controls it lays out allow Google to ensure a comprehensive and continually improving model for security management.

You can download and review the Google Maps Platform ISO 27001 certification from the Google Compliance Reports Manager.

SOC 2 Type II

The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). The purpose of this report is to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy. SOC 2 Type II reports are issued semi-annually around June and December.

You can download and review the Google Maps Platform SOC 2 Type II Audit Report from the Google Compliance Reports Manager.

Cloud Security Alliance (CSA)

The Cloud Security Alliance (1, 2) is a nonprofit organization whose mission is to "promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

The CSA's Security, Trust, and Assurance Registry Program (CSA STAR) is designed to help you assess and select a cloud service provider through a three-step program of self-assessment, third-party audit, and continuous monitoring.

Google Maps Platform has achieved the third-party assessment-based certification (CSA STAR Level 1: Attestation)

Google is also a CSA sponsor and a member of CSA's International Standardization Council (ISC), and a founding member of the CSA GDPR Center of Excellence.

ISO 22301:2019

The International Organization for Standardization (ISO) is an independent, non-governmental international organization with an international membership of 163 national standards bodies.

ISO 22301:2019 is an international standard for business continuity management that is designed to help organizations implement, maintain and improve a management system to prevent, prepare for, respond to, and recover from disruptions when they arise.

The data centers which support Google Maps Platform products are certified as ISO 22301:2019 and BS EN ISO 22301:2019 compliant after undergoing an audit by an independent third-party auditor. Compliance with these standards for Google's data centers demonstrates that locations hosting Google products and services meet the requirements as defined by ISO 22301:2019 and BS EN ISO 22301:2019.

ISO 50001:2018

The International Organization for Standardization (ISO) is an independent, non-governmental international organization with an international membership of 163 national standards bodies.

ISO 50001:2018 is an international standard for energy management that is designed to help organizations implement, maintain, and improve a management system to integrate energy management into their overall efforts to improve quality and environmental management.

The Google EMEA data centers used by Google Maps Platform are certified as ISO 50001:2018 compliant after undergoing an audit by an independent third party auditor. ISO 50001:2018 compliance for Google's data centers demonstrates that in-scope locations hosting Google products and services meet the requirements as defined by ISO 50001:2018.

Supported legal frameworks

Following are global contractual commitments.

European contractual commitments

This section describes European contractual commitments.

EU General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is privacy legislation that replaced the 95/46/EC Directive on Data Protection of 24 October 1995 on May 25, 2018. GDPR lays out specific requirements for businesses and organizations that are established in Europe or who serve users in Europe. Google Maps Platform champions initiatives that prioritize and improve the security and privacy of customer personal data, and want you, as a Google Maps Platform customer, to feel confident using Google's services in light of GDPR requirements. If you partner with Google Maps Platform, it will support your GDPR compliance efforts by:

1. Committing in Google's contracts to comply with the GDPR in relation to Google's processing of personal data in all Google Maps Platform services
2. Giving you the documentation and resources to assist you in your privacy assessment of Google's services
3. Continuing to evolve Google's capabilities as the regulatory landscape changes

EU, EEA, Swiss, and UK adequacy decisions

As documented in the Google privacy policy, the European Commission has determined that certain countries outside of the European Economic Area (EEA) adequately protect personal information, which means that data can be transferred from the European Union (EU) and Norway, Liechtenstein, and Iceland to those countries. The UK and Switzerland have adopted similar adequacy mechanisms.

EU Standard Contractual Clauses

The European Commission has published new EU SCCs to help safeguard European data together with the SCCs. Google has incorporated the SCCs into its Google Maps Platform contracts to protect data and meet the requirements of European privacy legislation. Like the previous SCCs, these clauses can be used to facilitate lawful transfers of data.

UK Data Protection Act

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). "UK GDPR" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

Swiss Federal Act on Data Protection (FDPA)

The Swiss Data Protection Act, known formally as the Federal Act on Data Protection (FADP), is a data protection regulation that aims to protect persons' privacy and fundamental rights when their data is processed.

Non-European contractual commitments

This section describes non-European contractual commitments.

Lei Geral de Proteção de Dados (LGPD)

Brazil's Lei Geral de Proteção de Dados (LGPD) is a data privacy law that governs the processing of personal data by businesses and organizations who are established in Brazil, or who serve users in Brazil, among other cases. The LGPD is now effective, and offers the following protections:

- Regulates how businesses and organizations can collect, use, and handle personal data
- Supplements or replaces existing federal sectoral privacy laws to increase accountability
- Authorizes fines on businesses and organizations that fail to meet its requirements
- Allows for the creation of a Data Protection Authority
- Imposes rules on the transfer of personal data collected within Brazil

Google offers products and solutions that you can use as part of a LGPD compliance strategy:

- Security and privacy features that help you to comply with LGPD and better protect and govern personal data
- Services and infrastructure built to ensure the security of data processing and employing appropriate privacy practices
- Continuous evolution of Google's products and capabilities as the regulatory landscape changes

Google Maps Platform customers need to evaluate their processing of personal data and determine if the LGPD's requirements are applicable to them. Google recommends that you consult with a legal expert to obtain guidance on LGPD specific requirements applicable to your organization, as this site does not constitute legal advice.

US State contractual commitments

Connecticut's Act Concerning Data Privacy and Online Monitoring

The Connecticut's Act Concerning Data Privacy and Online Monitoring, Pub. Act No. 22015 went into effect on January 1, 2023. Refer to the Google Controller-Controller Data Protection Terms for more information.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) (1, 2) is a data privacy law that provides California consumers with a number of privacy protections, including right to access, delete, and opt-out of the "sale" of their personal information. Starting January 1, 2020, businesses that collect California residents' personal information and meet certain thresholds (for example, revenue, volume of data processing) will need to comply with these obligations. The California Privacy Rights Act (CPRA) is a data privacy law that amends and expands upon the CCPA. The law takes effect on January 1, 2023. Google is very committed to helping its customers meet their obligations under these data regulations by offering convenient tools and building robust privacy and security protections into Google's services and contracts. You can find more information about your responsibilities as a business under the CCPA on the California Office of the Attorney General's website. Refer to the Google Controller-Controller Data Protection Terms for more information.

Colorado Privacy Act (CPA)

The Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq. went into effect on January 1, 2023. The act creates personal data privacy rights and applies to legal entities that conduct business or produce commercial products or services that are intentionally targeted to Colorado residents and that either:

- Control or process personal data of at least 100,000 consumers per calendar year
- Derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers

Refer to the Google Controller-Controller Data Protection Terms for more information.

Utah Consumer Privacy Act (UCPA)

The Utah Consumer Privacy Act, Utah Code Ann. § 13-61-101 et seq. went into effect on January 1, 2023. The UCPA applies to the sale of personal data and targeted advertising, and defines what does and does not include a sale: "the exchange of personal data for monetary consideration by a controller to a third party."

Refer to the Google Controller-Controller Data Protection Terms for more information.

Virginia Consumer Data Protection Act (VCDPA)

The Virginia Consumer Data Protection Act ("VCDPA") went into effect on January 1, 2023. This law provides Virginia residents certain rights for personal data collected by businesses under conditions outlined in the law.

Please refer to the Google Controller-Controller Data Protection Terms for more information.

Summary

Security is a primary design criteria for all of Google's infrastructure, products, and operations. Google's scale of operations and its collaboration with the security research community enable us to address vulnerabilities quickly, and often to prevent them entirely. Google runs its own services, such as Search, YouTube, and Gmail, on the same infrastructure that it makes available to its customers, who benefit directly from Google's security controls and practices.

Google believes that it can offer a level of protection that few public cloud providers or private enterprise IT teams can match. Because protecting data is core to Google's business, we can make extensive investments in security, resources, and expertise at a scale that others cannot. Google's investment frees you to focus on your business and innovation. We will continue to invest in our platform to let you benefit from Google services in a secure and transparent manner.