



Cybersecurity
Action Team

Google Infrastructure Security Design Overview

March 2022

Table of contents

Introduction	3
Secure low-level infrastructure	4
Security of physical premises	4
Hardware design and provenance	4
Secure boot stack and machine identity	4
Secure service deployment	5
Service identity, integrity, and isolation	6
Inter-service access management	6
Encryption of inter-service communication	7
Access management of end-user data in Google Workspace	7
Secure data storage	9
Encryption at rest	9
Deletion of data	10
Secure internet communication	10
Google Front End service	10
DoS protection	11
User authentication	11
Operational security	12
Safe software development	12
Source code protections	12
Keeping employee devices and credentials safe	13
Reducing insider risk	13
Threat monitoring	13
Intrusion detection	14
What's next	14

This content was last updated in March 2022, 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

This document provides an overview of how security is designed into Google's technical infrastructure. It is intended for security executives, security architects, and auditors.

This document describes the following:

- Google's global technical infrastructure, which is designed to provide security through the entire information processing lifecycle at Google. This infrastructure helps provide the following:
 - Secure deployment of services
 - Secure storage of data with end-user privacy safeguards
 - Secure communication between services
 - Secure and private communication with customers over the internet
 - Safe operation by Google engineers
- How we use this infrastructure to build internet services, including consumer services such as Google Search, Gmail, and Google Photos, and enterprise services such as Google Workspace and Google Cloud.
- Our investment in securing our infrastructure and operations. We have many engineers who are dedicated to security and privacy across Google, including many who are recognized industry authorities.
- The security products and services that are the result of innovations that we implemented internally to meet our security needs. For example, [BeyondCorp](#) is the direct result of our internal implementation of the [zero-trust security model](#).
- How the security of the infrastructure is designed in progressive layers. These layers include the following:
 - [Low-level infrastructure](#)
 - [Service deployment](#)
 - [Data storage](#)
 - [Internet communication](#)
 - [Operations](#)

The remaining sections of this document describe the security layers.

Secure low-level infrastructure

This section describes how we secure the physical premises of our data centers, the hardware in our data centers, and the software stack running on the hardware.

Security of physical premises

We design and build our own data centers, which incorporate multiple layers of physical security. Access to these data centers is tightly controlled. We use multiple physical security layers to protect our data center floors. We use biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems. For more information, see [Data center security](#).

We also host some servers in third-party data centers. In these data centers, we ensure that there are Google-controlled physical security measures on top of the security layers that are provided by the data center operator. For example, we operate biometric identification systems, cameras, and metal detectors that are independent from the security layers that the data center operator provides.

Hardware design and provenance

A Google data center consists of thousands of servers connected to a local network. We design the server boards and the networking equipment. We vet the component vendors that we work with and choose components with care. We work with vendors to audit and validate the security properties that are provided by the components. We also design custom chips, including a hardware security chip (called [Titan](#)), that we deploy on servers, devices, and peripherals. These chips let us identify and authenticate legitimate Google devices at the hardware level and serve as hardware roots of trust.

Note: Variants of the Titan hardware chip are also used in [Pixel devices](#) and the [Titan Security Key](#).

Secure boot stack and machine identity

Google servers use various technologies to ensure that they boot the correct software stack. We use cryptographic signatures for low-level components like the baseboard management controller (BMC), BIOS, bootloader, kernel, and base operating system image. These signatures can be validated during each boot or update cycle. The first integrity check for Google servers uses a hardware root of trust. The components are Google-controlled, built, and hardened with integrity attestation. With each new generation of hardware, we strive to continually improve security.

For example, depending on the generation of server design, the boot chain's root of trust is in one of the following:

- The Titan hardware chip
- A lockable firmware chip
- A microcontroller running our own security code

Each server in the data center has its own unique identity. This identity can be tied to the hardware root of trust and the software with which the machine boots. This identity is used to authenticate API calls to and from low-level management services on the machine. This identity is also used for mutual server authentication and transport encryption. We developed the [Application Layer Transport Security \(ALTS\)](#) system for securing remote procedure call (RPC) communications within our infrastructure. These machine identities can be centrally revoked to respond to a security incident. In addition, their certificates and keys are routinely rotated, and old ones revoked.

We developed automated systems to do the following:

- Ensure that servers run up-to-date versions of their software stacks (including security patches).
- Detect and diagnose hardware and software problems.
- Ensure the integrity of the machines and peripherals with verified boot and implicit attestation.
- Ensure that only machines running the intended software and firmware can access credentials that allow them to communicate on the production network.
- Remove or re-allocate machines from service when they're no longer needed.

Secure service deployment

Google services are the application binaries that our developers write and run on our infrastructure. Examples of Google services are Gmail servers, Spanner databases, Cloud Storage servers, YouTube video transcoders, and Compute Engine VMs running customer applications. 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 our customers (consumers, businesses, and even our 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, except in specific circumstances, such as when you are using Google Cloud to provision VMs on [sole-tenant nodes for Compute Engine](#).

Google Cloud and Google Workspace support regulatory requirements around data residency. For more information about data residency and Google Cloud, see [Implement data residency and sovereignty requirements](#). For more information about data residency and Google Workspace, see [Data regions: Choose a geographic location for your data](#).

Service identity, integrity, and isolation

To enable inter-service communication, applications use cryptographic authentication and authorization. Authentication and authorization provide strong access control at an abstraction level and granularity that administrators and services can understand.

Services do not rely on internal network segmentation or firewalling as the primary security mechanism. Ingress and egress filtering at various points in our network helps prevent IP spoofing. This approach also helps us to maximize our network's performance and availability. For Google Cloud, you can add additional security mechanisms such as [VPC Service Controls](#) and [Cloud Interconnect](#).

Each service that runs on the infrastructure has an associated service account identity. A service is provided with cryptographic credentials that it can use to prove its identity to other services when making or receiving RPCs. These identities are used in security policies. The security policies ensure that clients are communicating with the intended server, and that servers are limiting the methods and data that particular clients can access.

We use various isolation and sandboxing techniques to help protect a service from other services running on the same machine. These techniques include Linux user separation, language-based (such as the [Sandboxed API](#)) and kernel-based sandboxes, application kernel for containers (such as [gVisor](#)), and hardware virtualization. In general, we use more layers of isolation for riskier workloads. Riskier workloads include user-supplied items that require additional processing. For example, riskier workloads include running complex file converters on user-supplied data or running user-supplied code for products like App Engine or Compute Engine.

For extra security, sensitive services, such as the cluster orchestration service and some key management services, run exclusively on dedicated machines.

In Google Cloud, to provide stronger cryptographic isolation for your workloads and to protect data in use, we support [Confidential Computing](#) services for Compute Engine VMs and Google Kubernetes Engine (GKE) nodes.

Inter-service access management

The owner of a service can use access-management features provided by the infrastructure to specify exactly which other services can communicate with the service. For example, a service can restrict incoming RPCs solely to an allowed list of other services. That service can be configured with the allowed list of the service identities, and the infrastructure automatically enforces this access restriction. Enforcement includes audit logging, justifications, and unilateral access restriction (for engineer requests, for example).

Google engineers who need access to services are also issued individual identities. Services can be configured to allow or deny their access based on their identities. All of these identities (machine, service, and employee) are in a global namespace that the infrastructure maintains.

To manage these identities, the infrastructure provides a workflow system that includes approval chains, logging, and notification. For example, the security policy can enforce multi-party authorization. This system uses the two-person rule to ensure that an engineer acting alone cannot perform sensitive operations without first getting approval from another, authorized engineer. This system allows secure access-management processes to scale to thousands of services running on the infrastructure.

The infrastructure also provides services with the canonical service for user, group, and membership management so that they can implement custom, fine-grained access control where necessary.

End-user identities are managed separately, as described in [Access management of end-user data in Google Workspace](#).

Encryption of inter-service communication

The infrastructure provides confidentiality and integrity for RPC data on the network. To extend these security benefits to other application layer protocols such as HTTP, we encapsulate the data inside our infrastructure RPC mechanisms (which are variants of [gRPC](#)). Encapsulation provides application-layer isolation and removes any dependency on the security of the network path. Encrypted inter-service communication can remain secure even if the network is tapped or a network device is compromised.

To help protect against sophisticated adversaries who might be trying to tap our network links, the infrastructure automatically and efficiently (with help of hardware offload) encrypts infrastructure RPC traffic.

Access management of end-user data in Google Workspace

A typical Google Workspace service is written to do something for an end user. For example, an end user can store their email on Gmail. The end user's interaction with an application like Gmail might span other services within the infrastructure. For example, Gmail might call a People API to access the end user's address book.

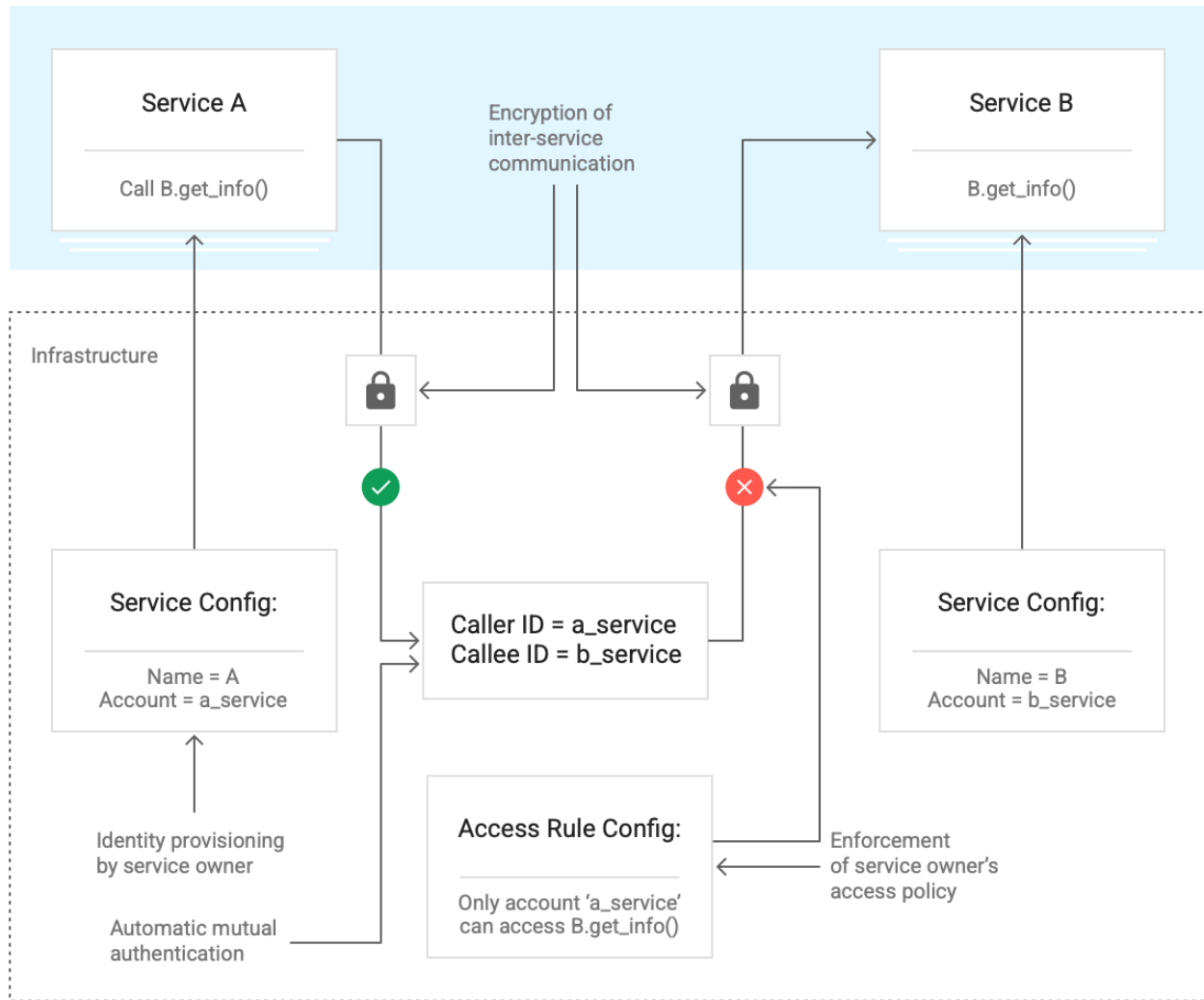
The [Encryption of inter-service communication](#) section describes how a service (such as Google Contacts) can be configured to only allow RPC requests from another service (such as Gmail). However, this level of access control is still a broad set of permissions because Gmail is able to request the contacts of any user at any time.

When Gmail makes an RPC request to Google Contacts on behalf of an end user, the infrastructure lets Gmail present an end-user permission ticket in the RPC request. This ticket proves that Gmail is making the RPC request on behalf of that particular end user. The ticket enables Google Contacts to implement a safeguard so that it only returns data for the end user named in the ticket.

The infrastructure provides a central user identity service that issues these end-user permission tickets. The identity service verifies the end-user login and then issues a user credential, such as a cookie or OAuth token, to the user's device. Every subsequent request from the device to our infrastructure must present that end-user credential.

When a service receives an end-user credential, the service passes the credential to the identity service for verification. If the end-user credential is verified, the identity service returns a short-lived end-user permission ticket that can be used for RPCs related to the user's request. In our example, the service that gets the end-user permission ticket is Gmail, which passes the ticket to Google Contacts. From that point on, for any cascading calls, the calling service can send the end-user permission ticket to the callee as a part of the RPC.

The following diagram shows how Service A and Service B communicate. The infrastructure provides service identity, automatic mutual authentication, encrypted inter-service communication, and enforcement of the access policies that are defined by the service owner. Each service has a service configuration, which the service owner creates. For encrypted inter-service communication, automatic mutual authentication uses caller and callee identities. Communication is only possible when an access rule configuration permits it.



For information about access management in Google Cloud, see [IAM overview](#).

Secure data storage

This section describes how we implement security for data that is stored on the infrastructure.

Encryption at rest

Google's infrastructure provides various storage services and distributed file systems (for example, Spanner and [Colossus](#)), and a central key management service. Applications at Google access physical storage by using storage infrastructure. We use several layers of encryption to protect data at rest. By default, the storage infrastructure encrypts all user data before the user data is written to physical storage.

The infrastructure performs encryption at the application or storage infrastructure layer. Encryption lets the infrastructure isolate itself from potential threats at the lower levels of storage, such as malicious disk firmware. Where applicable, we also enable hardware encryption support in our hard drives and SSDs, and we meticulously track each drive through its lifecycle. Before a decommissioned, encrypted storage device can physically leave our custody, the device is cleaned by using a multi-step process that includes two independent verifications. Devices that do not pass this cleaning process are physically destroyed (that is, shredded) on-premises.

In addition to the encryption done by the infrastructure, Google Cloud and Google Workspace provide key management services. For Google Cloud, [Cloud KMS](#) is a cloud service that lets customers manage cryptographic keys. For Google Workspace, you can use client-side encryption. For more information, see [Client-side encryption and strengthened collaboration in Google Workspace](#).

Deletion of data

Deletion of data typically starts with marking specific data as scheduled for deletion rather than actually deleting the data. This approach lets us recover from unintentional deletions, whether they are customer-initiated, are due to a bug, or are the result of an internal process error. After data is marked as scheduled for deletion, it is deleted in accordance with service-specific policies.

When an end user deletes their account, the infrastructure notifies the services that are handling the end-user data that the account has been deleted. The services can then schedule the data that is associated with the deleted end-user account for deletion. This feature enables an end user to control their own data.

For more information, see [Data deletion on Google Cloud](#).

Secure internet communication

This section describes how we secure communication between the internet and the services that run on Google infrastructure.

As discussed in [Hardware design and provenance](#), the infrastructure consists of many physical machines that are interconnected over the LAN and WAN. The security of inter-service communication is not dependent on the security of the network. However, we isolate our infrastructure from the internet into a private IP address space. We only expose a subset of the machines directly to external internet traffic so that we can implement additional protections such as defenses against denial of service (DoS) attacks.

Google Front End service

When a service must make itself available on the internet, it can register itself with an infrastructure service called the Google Front End (GFE). GFE ensures that all TLS connections are terminated with correct certificates and by following best practices such as supporting perfect forward secrecy. GFE also applies protections against DoS attacks. GFE then forwards requests for the service by using the RPC security protocol discussed in [Access management of end-user data in Google Workspace](#).

In effect, any internal service that must publish itself externally uses the GFE as a smart reverse-proxy frontend. The GFE provides public IP address hosting of its public DNS name, DoS protection, and TLS termination. GFEs run on the infrastructure like any other service and can scale to match incoming request volumes.

Customer VMs on Google Cloud do not register with GFE. Instead, they register with the Cloud Front End, which is a special configuration of GFE that uses the Compute Engine networking stack. Cloud Front End lets customer VMs access a Google service directly using their public or private IP address. (Private IP addresses are only available when [Private Google Access](#) is enabled.)

DoS protection

The scale of our infrastructure enables it to absorb many DoS attacks. To further reduce the risk of DoS impact on services, we have multi-tier, multi-layer DoS protections.

When our fiber-optic backbone delivers an external connection to one of our data centers, the connection passes through several layers of hardware and software load balancers. These load balancers report information about incoming traffic to a central DoS service running on the infrastructure. When the central DoS service detects a DoS attack, the service can configure the load balancers to drop or throttle traffic associated with the attack.

The GFE instances also report information about the requests that they are receiving to the central DoS service, including application-layer information that the load balancers don't have access to. The central DoS service can then configure the GFE instances to drop or throttle attack traffic.

User authentication

After DoS protection, the next layer of defense for secure communication comes from the central identity service. End users interact with this service through the Google login page. The service asks for a username and password, and it can also challenge users for additional information based on risk factors. Example risk factors include whether the users have logged in from the same device or from a similar location in the past. After authenticating the user, the identity service issues credentials such as cookies and OAuth tokens that can be used for subsequent calls.

When users sign in, they can use second factors such as OTPs or phishing-resistant security keys such as the [Titan Security Key](#). The Titan Security Key is a physical token that supports the [FIDO Universal 2nd Factor \(U2F\)](#). We helped develop the U2F open standard with the FIDO Alliance. Most web platforms and browsers have adopted this open authentication standard.

Operational security

This section describes how we develop infrastructure software, protect our employees' machines and credentials, and defend against threats to the infrastructure from both insiders and external actors.

Safe software development

Besides the [source control protections and two-party review process](#) described earlier, we use libraries that prevent developers from introducing certain classes of security bugs. For example, we have libraries and frameworks that help eliminate XSS vulnerabilities in web apps. We also use automated tools such as fuzzers, static analysis tools, and web security scanners to automatically detect security bugs.

As a final check, we use manual security reviews that range from quick triages for less risky features to in-depth design and implementation reviews for the most risky features. The team that conducts these reviews includes experts across web security, cryptography, and operating system security. The reviews can lead to the development of new security library features and new fuzzers that we can use for future products.

In addition, we run a [Vulnerability Rewards Program](#) that rewards anyone who discovers and informs us of bugs in our infrastructure or applications. For more information about this program, including the rewards that we've given, see [Bug hunters key stats](#).

We also invest in finding zero-day exploits and other security issues in the open source software that we use. We run [Project Zero](#), which is a team of Google researchers who are dedicated to researching zero-day vulnerabilities, including [Spectre and Meltdown](#). In addition, we are the largest submitter of CVEs and security bug fixes for the Linux KVM hypervisor.

Source code protections

Our source code is stored in repositories with built-in source integrity and governance, where both current and past versions of the service can be audited. 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 happens when a service is deployed. BAB does the following:

- Ensures that the production software and configuration that is deployed at Google is reviewed and authorized, particularly when that code can access user data.
- Ensures that 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.

Keeping employee devices and credentials safe

We implement safeguards to help protect our employees' devices and credentials from compromise. To help protect our employees against sophisticated phishing attempts, we have replaced OTP second-factor authentication with the mandatory use of U2F-compatible security keys.

We monitor the client devices that our employees use to operate our infrastructure. We ensure that the operating system images for these devices are up to date with security patches and we control the applications that employees can install on their devices. We also have systems that scan user-installed applications, downloads, browser extensions, and web browser content to determine whether they are suitable for corporate devices.

Being connected to the corporate LAN is not our primary mechanism for granting access privileges. Instead, we use zero-trust security to help protect employee access to our resources. Access-management controls at the application level expose internal applications to employees only when employees use a managed device and are connecting from expected networks and geographic locations. A client device is trusted based on a certificate that's issued to the individual machine, and based on assertions about its configuration (such as up-to-date software). For more information, see [BeyondCorp](#).

Reducing insider risk

We limit and actively monitor the activities of employees who have been granted administrative access to the infrastructure. We continually work 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, we require two-party approvals for some actions and we use limited APIs that allow debugging without exposing sensitive information.

Google employee access to end-user information can be logged through low-level infrastructure hooks. Our security team monitors access patterns and investigates unusual events.

Threat monitoring

The [Threat Analysis Group](#) at Google monitors threat actors and the evolution of their tactics and techniques. The goals of this group are to help improve the safety and security of Google products and share this intelligence for the benefit of the online community.

For Google Cloud, you can use [Google Cloud Threat Intelligence for Chronicle](#) and [VirusTotal](#) to monitor and respond to many types of malware. Google Cloud Threat Intelligence for Chronicle is a team of threat researchers who develop threat intelligence for use with [Chronicle](#). VirusTotal is a malware database and visualization solution that you can use to better understand how malware operates within your enterprise.

For more information about our threat monitoring activities, see the [Threat Horizons report](#).

Intrusion detection

We use 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. [Our investigation and incident-response teams](#) triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year. We conduct [Red Team](#) exercises to measure and improve the effectiveness of our detection and response mechanisms.

What's next

- To learn more about how we protect our infrastructure, read [Building secure and reliable systems \(O'Reilly book\)](#).
- Read more about [data center security](#).
- Learn more about how we protect against [DDoS attacks](#).
- Read about our zero-trust solution, [BeyondCorp](#).