# Google Infrastructure Security Design Overview

June 2024

# Table of contents

*This content was last updated in June 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

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.
- 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.

Inside the data center, we implement additional controls to ensure that physical access to servers is protected and monitored. For more information, see How Google protects the physical-to-logical space in a data center.

We also host some servers in third-party data centers. In these data centers, we align with the same regulatory standards as we do in our own data centers. We ensure that there are Google-controlled physical security measures and Google-controlled connectivity 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.

Unless specifically stated, the security controls in this document apply to both Google owned data centers and third-party data centers.

## Hardware design and provenance

Google data centers consist 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 intended software stack. At each step in the boot process, Google implements industry-leading controls to help enforce the boot state that we expect and to help keep customer data safe.

We strive to continually improve our servers with each successive hardware generation, and to bring these improvements to the rest of the industry through engagement in standards processes with Trusted Computing Group and DMTF.

Each server in the data center has its own unique identity. This identity can be tied to the hardware roots of trust and the software that 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 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 repair machines if they don't pass the integrity check or when they're no longer needed.

For more information about how we secure our boot stack and machine integrity, see How Google enforces boot integrity on production machines and Remote attestation of disaggregated machines.

# 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-based virtualization. In general, we use more layers of isolation for riskier workloads. Riskier workloads include workloads that process unsanitized input from the internet. For example, riskier workloads include running complex file converters on untrusted input or running arbitrary code as a service for products like 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 virtual machine (VM) instances and Google Kubernetes Engine (GKE) nodes.

## Inter-service access management

The owner of a service can manage access by creating a list of other services that can communicate with the service. This access management feature is provided by Google infrastructure. For example, a service can restrict incoming RPCs solely to an allowed list of other services. The owner can also configure the service with an allowed list of service identities, which the infrastructure enforces automatically. 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-workload communication

The infrastructure provides confidentiality and integrity for RPC data on the network. All Google Cloud virtual networking traffic is encrypted. Communication between Google Cloud infrastructure workloads is encrypted, with exemptions that are granted only for high-performance workloads where traffic doesn't cross the multiple layers of physical security at the edge of a Google data center. Communication between Google Cloud infrastructure services has cryptographic integrity protection.

The infrastructure automatically and efficiently (with help of hardware offload) provides end-to-end encryption for the infrastructure RPC traffic that goes over the network between data centers.

## 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.

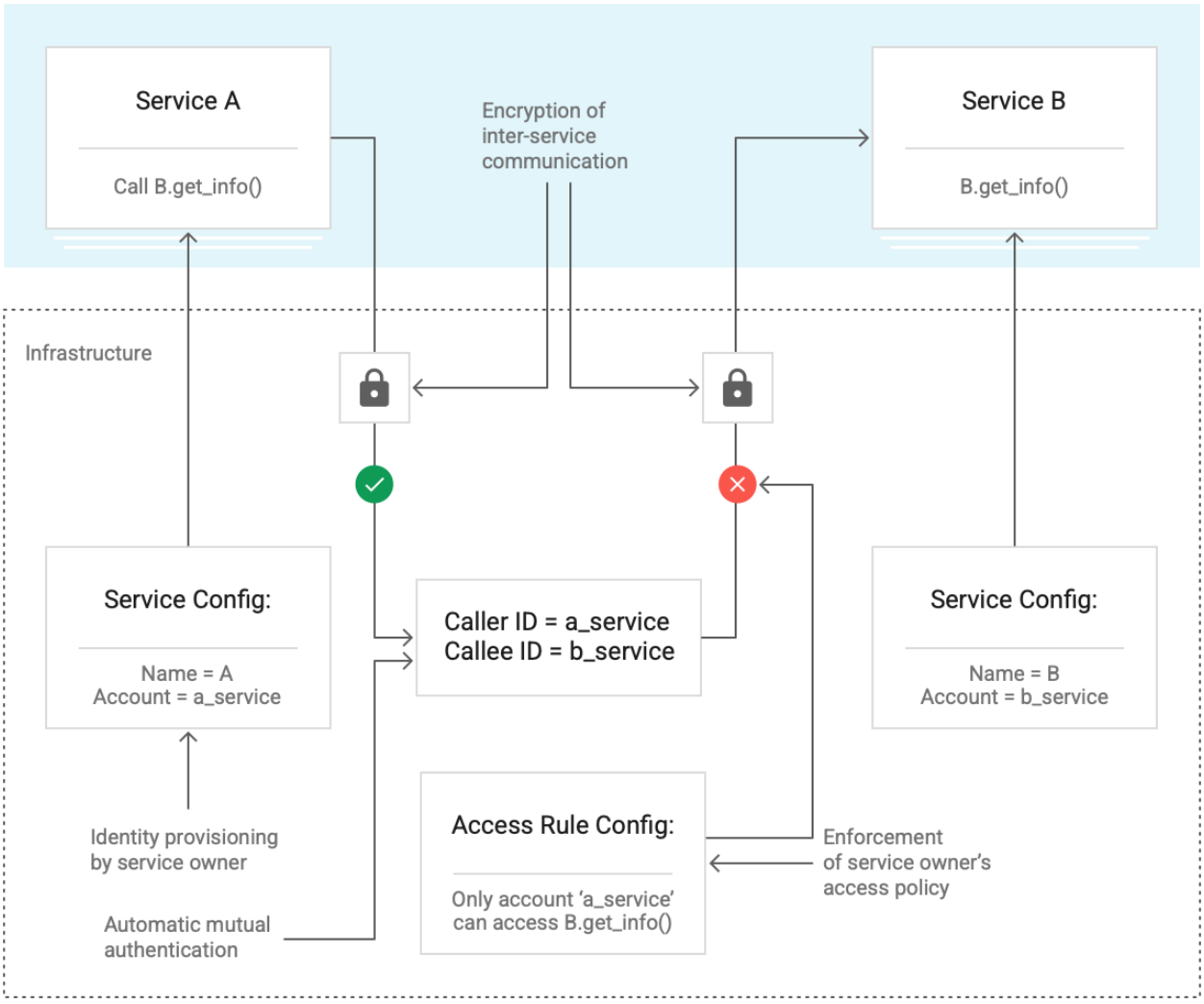
The Encryption of inter-service communication section describes how a service (such as Google Contacts) can be configured to only allow RPC requests from another service (such as Gmail). However, this level of access control is still a broad set of permissions because Gmail is able to request the contacts 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 context 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 context 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 context ticket that can be used for RPCs related to the user's request. In our example, the service that gets the end-user context 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 context 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.




## Access management of end-user data in Google Cloud

Similar to Access management of end-user data in Google Workspace, the infrastructure provides a central user identity service that authenticates service accounts and issues end-user context tickets after a service account is authenticated. Access management between Google Cloud services is typically done with service agents rather than using end-user context tickets.

Google Cloud uses Identity and Access Management (IAM) and context-aware products such as Identity Aware Proxy to let you manage access to the resources in your Google Cloud organization. Requests to Google Cloud services go through IAM to verify permissions.

The access management process is as follows:

1. A request comes in through the Google Front End service or the Cloud Front End service for customer VMs.

2. The request is routed to the central user identity service that completes the authentication check and issues the end-user context tickets.
3. The request is also routed to check for items such as the following:
    - IAM access permissions, including policy and group membership
    - Access transparency using Access Transparency
    - Cloud Audit Logs
    - Quotas
    - Billing
    - Attribute calculator
    - VPC Service Controls security perimeters
4. After all of these checks pass, the Google Cloud backend services are called.

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. The keys for this encryption are managed and owned by Google. 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 with Google-owned and Google-managed keys, Google Cloud and Google Workspace provide key management services for keys that you can own and manage. For Google Cloud, Cloud KMS is a cloud service that lets you create your own cryptographic keys, including hardware-based FIPS 140-3 L3 certified keys. These keys are specific to you, not to the Google Cloud service, and you can manage the keys according to your policies and procedures. 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 cryptographic material or data typically starts with marking specific keys or data as scheduled for deletion. The process for marking data for deletion takes into account the service-specific policies and the customer's specific policies.

By scheduling the data for deletion or disabling the keys first, we can recover from unintentional deletions, whether the deletions are customer-initiated, are due to a bug, or are the result of an internal process error.

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. For more information about how to use Cloud KMS to disable your own keys, see Destroy and restore key versions.

# 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.

When customer VMs in Google Cloud VPC networks access Google APIs and services that are hosted directly on Borg, the customer VMs communicate with specific GFEs that are called *Cloud Front Ends*. To minimize latency, Cloud Front Ends are located within the same cloud region as the customer VM. Network routing between customer VMs and Cloud Front Ends doesn't require that the customer VMs have external IP addresses.

When Private Google Access is enabled, customer VMs with only internal IP addresses can communicate with the external IP addresses for Google APIs and services using Cloud Front Ends. All network routing between customer VMs, Google APIs, and services depend on next hops within Google's production network, even for customer VMs that have external IP addresses.

## 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

*Insider risk* is the potential of a current or former employee, contractor, or other business partner who has or had authorized access to our network, system, or data to misuse that access to undermine the confidentiality, integrity, or availability of our information or information systems.

To help reduce 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. We expose limited APIs that allow debugging without exposing sensitive data, and we require two-party approvals for certain sensitive actions performed by human operators.

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. For more information, see Privileged Access Management in Google Cloud.

We use Binary authorization for Borg to help protect our supply chain from insider risk. In addition, our investment in BeyondProd helps to protect user data in Google infrastructure and to establish trust in our services.

In Google Cloud, you can monitor access to your data using Access Transparency. Access Transparency logs let you verify that Google personnel are accessing your content only for valid business reasons, such as fixing an outage or attending to your support requests. Access Approval ensures that Cloud Customer Care and engineering require your explicit approval when they need to access your data. The approval is cryptographically verified to ensure the integrity of the access approval.

For more information about production service protections, see How Google protects its production services.

## 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.