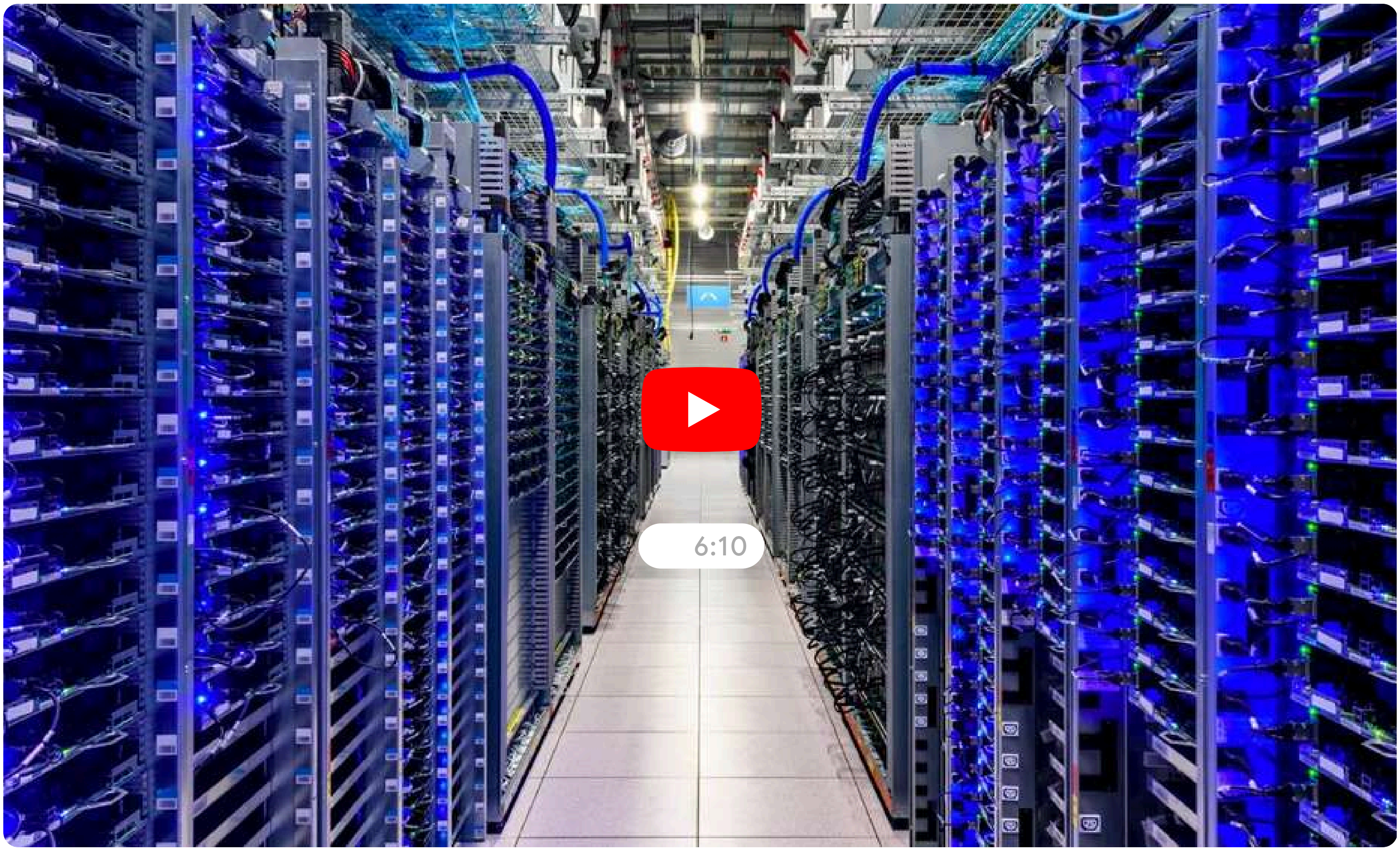
One percent of Googlers get to visit a data center, but I did

Jun 30, 2020 · 4 min read

Share

Stephanie Wong
Developer Advocate, Google Cloud



Listen to article 6 minutes

For years I've wondered what it's like behind the protected walls of a Google data center, and I'm not alone. In my job at Google, I spend my days working with developers. Our data centers are crucial to the work that they do, but most have never actually set foot inside a data center. And until recently, neither had I. I went on a mission to find answers to common questions like: Why are visits so tightly restricted? How secure is a Google data center? How do we meet regulatory requirements? Here's what I found out.

To keep our customers' data safe, we need to make sure the physical structure of the data center is absolutely secure. Each data center is protected with six layers of physical security designed to thwart unauthorized access. Watch the video above to follow my journey through these layers to the core of a data center, and read on to learn even more.

"Least privilege" is the rule to live by

There are two rules strictly enforced at all Google data centers. The "least privilege" protocol is the idea that someone should have only the bare minimum privileges necessary to perform their job. If your least privilege is to enter Layer 2, you won't have luck moving to Layer 3. Each person's access permissions are checked at badge readers that exist at every access point in a data center facility. Authorization measures happen everywhere using this protocol.

Another rule exists that prevents a vehicle or individual closely following another to gain entry into a restricted area without a badge swipe. If the system detects a door open for too long, it immediately alerts security personnel. Any gate or door must close before the next vehicle or person can badge in and gain access.

Two security checks: badge first, then circle lock

You've probably seen dual-authentication when you try to sign into an account and a one-time password is sent to your phone. We take a similar approach at the data centers to verify a person's identity and access. At some layers in the data center, you're required to swipe your badge, then enter a circle lock, or tubular doorway. You walk into a special "half portal" that checks your badge and scans your eyes to gain access to the next layer of the data center. It prevents tailgating because only one person is allowed in the circle lock at a time.

Shipments are received through a secure loading dock

The facility loading docks are a special section of Layer 3, used to receive and send shipments of materials, such as new hardware. Truck deliveries must be approved for access to Layer 3 to enter the dock. For further security, the loading dock room is physically isolated from the rest of the data center, and guard presence is required when a shipment is received or sent.

All hard drives are meticulously tracked

Hard drive tracking is important to the security of your data because hard drives contain encrypted sensitive information. Google meticulously tracks the location and status of every hard drive within our data centers —from acquisition to destruction—using barcodes and asset tags. These asset tags are scanned throughout a hard drive's lifecycle in a data center from the time it's installed to the time it's removed from circulation. Tracking hard drives closely ensures they don't go missing or end up in the wrong hands.

We also make sure hard drives are properly functioning by doing frequent performance tests. If a component fails to pass a performance test, it's deemed no longer usable. To prevent any sensitive information from living on that disk, we remove it from inventory to be erased and destroyed in Layer 6, Disk Erase. There, the disk erase formatter uses a multi-step process that wipes the disk data and replaces each bit of data with zeros. If the drive can't be erased for any reason, it's stored securely until it can be physically destroyed.

Layered security extends into the tech itself

Our layered security approach isn't just a physical safeguard for entering our data centers. It's also how we protect the hardware and software that live in our data centers. At the deepest layer, most of our server boards and networking equipment are custom-designed by Google. For example, we design chips, such as the Titan hardware security chip, to securely identify and authenticate legitimate Google hardware.

At the storage layer, data is encrypted while it travels in and out of Google's network and when it's stored at the data center. This means whether data is traveling over the internet outside of Google's facilities, or stored on our servers, it's protected. Google Cloud customers can even supply their own encryption keys and manage them in a third-party key management system deployed outside Google's infrastructure. This defense-in-depth approach helps to expand our ability to mitigate potential vulnerabilities at every point.

To learn more about our global data centers, visit our Data and Security page. We will also be sharing more about our security best practices during the upcoming Google Cloud Next '20: OnAir event.

POSTED IN:

Data Centers and Infrastructure   Safety & Security   Google Cloud