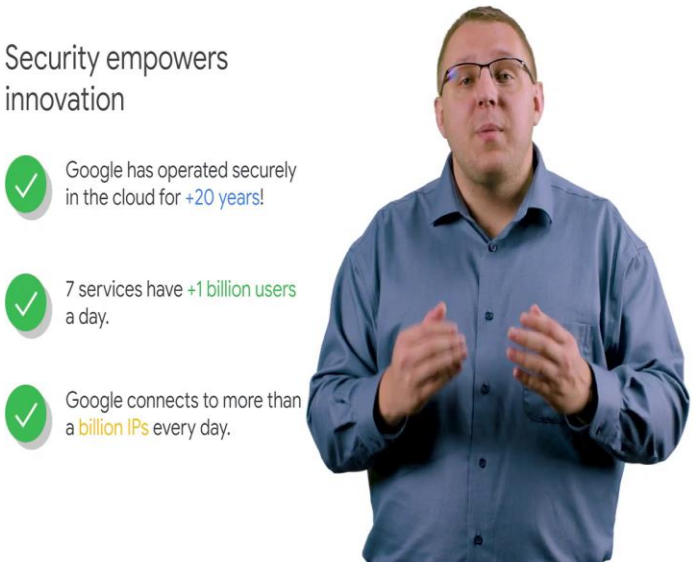
Google Cloud Computing Foundation Course
Seth Vargo
Google Cloud

Lecture-44
Introduction to Security in the Cloud

(Refer Slide Time: 00:04)

Let us start with the first topic an introduction to security in the cloud. At Google we believe that security empowers innovation. If you put security first everything else will follow.

(Refer Slide Time: 00:13)



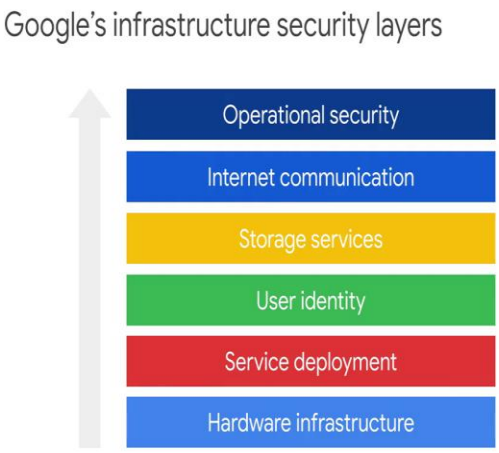
Google has been operating securely in the cloud for nearly 20 years. We have 7 services each with over 1 billion users every day. This means that Google and Google cloud connect to more than a billion IP addresses every day. Designing for security is pervasive throughout our entire infrastructure and security is always paramount. Countless organizations have lost data due to a security incident a single breach could cost millions in fines and lost business. But more importantly a serious data breach can permanently damage an organization's reputation with the loss of customer trust.

As a result security is increasingly top of mind for organizational leadership like CEOs and CSO's. Unfortunately many organizations do not have access to the resources they need to implement state-of-the-art security controls and techniques. Google invests heavily in its technical infrastructure and has dedicated engineers tasked with providing a secure and robust platform.

(Refer Slide Time: 01:25)

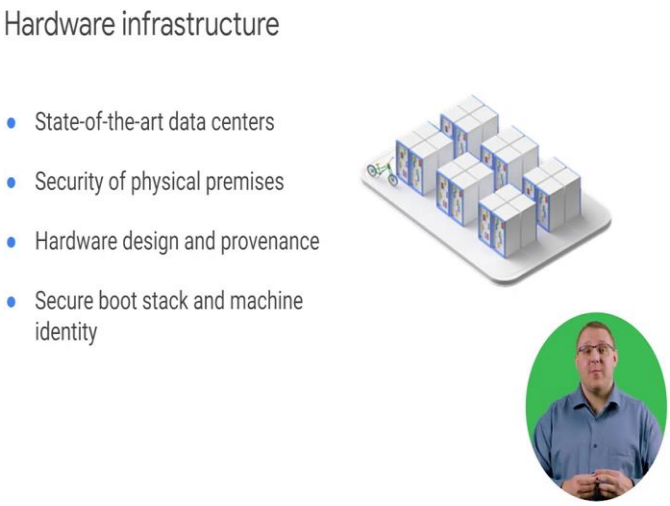
By choosing GCP you can leverage that same infrastructure to help secure your services and your data through the entire information processing lifecycle including the deployment of services, the storage of data, communication between services and operation by administrators.

(Refer Slide Time: 00:04)



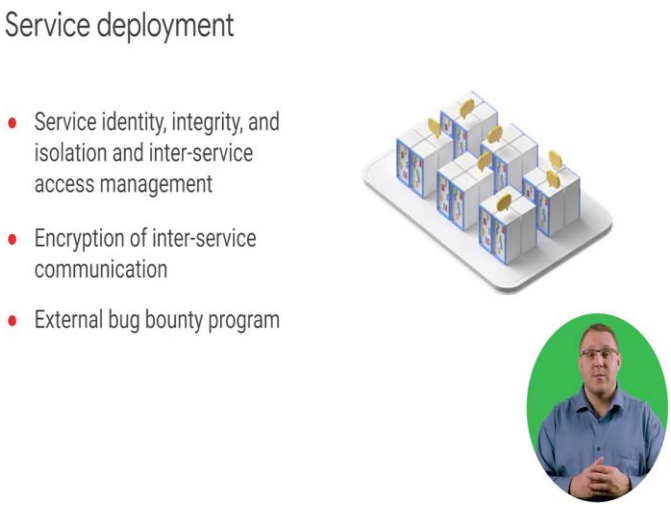
Security cannot be an afterthought it must be fundamental in all designs that is why at Google we build security through progressive layers that deliver true defense-in-depth meaning. Our cloud infrastructure does not rely on one single technology to make it secure.

(Refer Slide Time: 02:04)



Let us start by talking about securing low level infrastructure. We design and build our own data centers that incorporate multiple layers of security protections. As just one example access to these data centers is limited to a very small fraction of Google employees. We design our own servers networking equipment and hardware security chips in those data centers. Our servers use cryptographic signatures to make sure they are booting the correct software at the correct version in the correct data center.

(Refer Slide Time: 02:42)



Now let us talk about a different layer of the stack service deployments. Specifically let us talk about Google service deployments which provide the fabric for Google cloud. When services communicate with one another they do so via a remote procedure call or RPC. If you are not familiar with RPC that is okay it is just a way to facilitate communication between two services like REST over HTTP or XML over SOAP.

Google's infrastructure provides cryptographic privacy and integrity for all RPC calls for service to service communication. In addition to our own security practices Google also has an external bug bounty program in which third-party security researchers and developers can gain monetary rewards for finding vulnerabilities in Google's software components.