SECURITY AT SCALE WITH CLOUD COMPUTING:

A Minute in the Life of Google

Ancoris

Google Cloud

00101 GOOGLE CLOUD OVERVIEW 00011010011101010 0001101 1110 0101 0101101 0011 1001 00011010 1110 0101 01101010011 1001 01101 11010101 0101101 01101001 001101 11010101 101101 101001 00110 101 10 001 101 001

No one in today's highly connected world is exempt from security threats like phishing, ransomware, or denial-of-service (DoS) attacks. Certainly not Google.

Google operates seven services with more than ***one billion active users*** each (including Google Search, YouTube, Maps, and Gmail). We see every type of attack, bad software, and bad actors—multiple times a day—and we're proud of what our people, processes, and technology do to stop them.

Google has published ***more than 160 academic research papers*** on computer security, privacy, and abuse prevention and has privately warned other software companies of weaknesses discovered in their systems. Within Google, we enforce a zero-trust security model, which monitors every device on the internal network.

PARTNER WITH ANCORIS TO MODERNIZE YOUR INFRASTRUCTURE

Improve your speed to innovation with faster deployment, scale, and greater security, all while freeing up engineering resources from infrastructure management. Cloud computing leverages all these benefits, but planning a migration or identifying the right solution can get complicated, fast.

Talk to us to help you migrate your onsite computing to stronger security with Google Cloud.

101101 101001
00110 101
10 001
101
001

CONSIDER WHAT GOOGLE DOES
EVERY MINUTE OF THE DAY

00101 EVERY MINUTE 00011010011101010 10

10 MILLION	***spam messages are prevented*** from reaching Gmail customers.
694,000	***indexed Web pages are scanned*** for harmful software.
7,000	***deceitful URLs, executables, and browser extensions*** that may carry viruses, unwanted content, or phishing attempts are spotted and stopped.
6,000	***instances of unwanted software*** and nearly ***1,000 instances of suspected malware are reported*** to Chrome users.
2	***phishing sites and 1 malware site are found*** and labeled.

00101 EVERY DAY 00011010011101010 10

6 BILLION	***mobile apps downloaded to Android phones are scanned*** to protect from infection.
2 BILLION	***mobile phones, laptops, tablets, and other devices are protected*** with Google's Safe Browsing technology.
400 MILLION+	***Android devices are checked*** for health.
2,000+	times a day we ***notify Webmasters about suspect content*** that's been inserted into their sites, and we annually ***notify 22,000 Internet service providers of harmful content***.

001101 11010101
101101 101001
00110 101
10 001
101
001

11001 WHY THIS MATTERS 11010011101010

Defending the world's largest network against persistent and constantly evolving cyber threats has driven Google to architect, automate, and develop advanced tools to help keep us ahead. Understanding how we've built and evolved our defenses in response can help you make smart architectural decisions of your own as you move forward.

BUILDING A SECURE FOUNDATION

Most organizations invest in infrastructure security because a shaky foundation imperils the apps and data that run on top. At Google, we run our own supply chains, purposely creating our proprietary motherboards, chips, and networking equipment from diverse sources. No third party can learn the whole of our architecture. A special microchip in each new Google server identifies and protects the equipment too.

In our network communications, protocols we've developed change multiple times per second, over fiber we control directly. Connections into Google Cloud are also encrypted to keep out intruders.

Google's network has a built-in level of internal capacity multiple times that of any traffic load we anticipate. If there is a denial-of-service attack, we have time to isolate and shut down a malicious agent.

We put tremendous effort into minimizing software vulnerabilities. Core to this is our patch and security configuration management. When organizations don't realize they are vulnerable, or forget to apply a software patch, it leaves them exposed to ransomware and other malicious software.

Our software runs in Google's containers, which enable system-wide management. Configuration changes and patches can be deployed everywhere, quickly, with no required downtime. That keeps our exposure to software vulnerabilities low.

Our open-source version of these containers, Kubernetes, is a popular choice for developing and deploying cloud software. If you are building your own cloud software, Kubernetes is a top choice.

Infrastructure security often gets challenging as organizations deal with the growth and scale of data, compute, and connectivity. They must trust their hardware, software, and communications. For some, the resources and investment required for this can be prohibitive. Using a cloud provider with a shared responsibility model can ensure you get a highly secure foundation that enables you to invest in other areas of security, IT, or your business.

PROTECTING DATA WHEREVER IT IS

Encryption and other data protection measures can prevent unauthorized disclosures of sensitive and regulated information. It's critical to know where sensitive data is, but that can be difficult in older heterogeneous systems. Kubernetes can help here too.

At Google, we encrypt our customers' data in different ways, depending on what the data is doing: whether it is stored, in a database, or in transit between the user and Google. It all happens by default, with no user action required.

Data is encrypted at the hardware layer inside our data center. That way it can only be decrypted in our cloud on another verified Google machine. When stored, data is broken up into different chunks and sent to different servers. Depending on the size of a data set, it may consist of hundreds, or even millions, of encrypted chunks. This guards against hackers and is good for disaster recovery and business continuity, insuring against natural disasters, unplanned downtimes, and equipment failures.

When you call up a document in Google Drive, for example, the document is recalled from all of its storage points, decrypted, and reassembled in the blink of an eye.

Increasingly, online storage and collaboration are important parts of office communication—and another attractive hacker target. Files in Google Drive undergo a malware scan prior to any download or sharing. Drive stores files in non-executable formats, which prevents ransomware from propagating within Drive.

As everyone's data increases, the ability to find and protect data is a must. Organizations must either develop a plan to deliver and scale their capabilities or leverage the cloud for storage, analytics, and integrated data protection functionality.

SPOTLIGHT

5 SECURITY MEASURES EVERY COMPANY SHOULD TAKE TODAY

You're probably not going to build your own Google-scale network tomorrow—but you also don't need to. Here are a few of the security measures you can (and should) take right now.

01**01**001 **Encrypt data at rest.** Wherever your data is stored, ensure that encryption measures are in place.

01**02**100 **Adopt a zero-trust lens.** Google's BeyondCorp approach to enterprise security assumes that no network should be trusted. This replaces the old "perimeter" security model—increasingly difficult to manage in a world of global, mobile, continuous access—with individual- and device-level security. Adopting a zero-trust lens can help organizations manage identity, access, and network security in a way that better accounts for modern realities.

00**03**011 **Containerize software development.** Containers enable system-wide management so you can change configurations or patch vulnerabilities everywhere, fast. Open-source container management tools like Kubernetes allow for containerization on any infrastructure: on-prem, cloud, or hybrid.

10**04**101 **Equip your workforce to be the first line of defense.** It doesn't have to be a sophisticated training program: even simple measures, such as an internal email to raise awareness about phishing attacks, can help.

11**05**001 **Vet your technology providers.** We've detailed our security approach here, and you can read more about our security infrastructure here. Whether it's a cloud SaaS provider for CRM or an on-prem ERP system, be sure you know how your technology providers are addressing key security concerns, from data protection to IAM to phishing and DDoS prevention.

MANAGING USERS AND DEVICES

It doesn't take a rogue employee to compromise data or a network. A stolen password, an infected thumb drive, or spyware embedded in a mobile app can mean damage.

Traditionally, companies have employed endpoint protection technologies and authentication mechanisms, like firewalls, or else actively limited access to the network. Over time, this creates an expensive and hard-to-maintain system.

At Google, we undertook a massive project to rethink how to provide employees with secure remote access to applications: the result is BeyondCorp, our network security model.

Instead of assuming a person or a machine is either inside or outside the whole corporate network, BeyondCorp uses lots of computation to allow access to individual services as needed, based on trusted identities and devices.

To avoid the usual trade-off between security and user convenience, Google developed small form-factor authentication Security Keys that connect to a user's computer or phone. Touching a key confirms identity. It preserves privacy and secures against attackers, making it ideal for broad deployment.

We also make extensive use of Chrome OS, our device operating system, and Chromebooks, our network-connected laptops. System software is verified each time the device boots, so we know the OS hasn't been compromised. Apps are sandboxed to limit any malicious code from impacting the rest of the machine. The OS is frequently and automatically updated with new features and security patches while people do their work.

AUDIT AND REGULATORY COMPLIANCE

Audits show you're in line with internal policy and external regulations, but they can take a lot of time. Another benefit of running a containerized cloud is the speed with which you can execute security audits, quickly accessing secure and sensitive data logs.

One large financial customer had a compliance requirement to monitor overall asset liquidity. It took six days to complete on their traditional computer system. With Google Cloud, the time was reduced to about six minutes, and the cost fell below one dollar.

Running a global network, we adopt the most stringent policies set by any nation where we operate, and we can apply them everywhere. We have the encryption standards of South Korea, regarded as the world's most stringent, and the privacy mandates of U.S. medical records, also considered the toughest. We monitor and meet regulatory changes, and we can efficiently keep customers up to date on changing requirements. It's one reason we have the highest certifications for security and privacy compliance.

PUTTING IT ALL TOGETHER: STOPPING PHISHING

According to the 2017 Verizon Data Breach Investigations Report, 90% of incidents and breaches that involved social actions by external actors included phishing. For all the technology, many security problems come down to exploiting people, not machines. Everyone is overwhelmed with email, and it just takes one person to hurriedly click on a rogue message to have a phishing incident.

Our first defense is to prevent phishing emails from reaching people. Incoming emails to Gmail get a real-time scan: any virus detected in an attachment is blocked. Gmail restricts the use of file types that carry a high potential for security risks, even inside a compressed file, to defeat malware. Google has never, and will never, scan the data of our Cloud customers for commercial purposes, such as ads or profiling.

Normally, when someone clicks on a malicious link in an email, two things may happen. They may be directed to a hacker-controlled site looking to capture their username, password, or other sensitive information. On our network, the hacker would still be unable to impersonate the user, because they would not have the user's physical Security Key that they need to prove their identity when they log on.

Sometimes a malicious site may try to install malware on their device. That is why our Safe Browsing technology blocks these sites. Chromebooks, if they do somehow get infected, can quickly and easily be restored to a known good state.

These multiple layers of security drastically reduce threats to our users and infrastructure. Adopting some or all of these elements can make your organization much more resilient too.

SPOTLIGHT

CLOUD ADOPTION ACCELERATES AS CONFIDENCE IN CLOUD SECURITY GROWS

According to a survey of more than 500 global IT leaders conducted by MIT Sloan Management Review on behalf of Google Cloud, cloud adoption continues to accelerate, with security being one of the primary drivers of adoption. According to the survey:

01**01**001

Confidence in cloud security is driving adoption.

Respondents cited "increased confidence in cloud security" as a primary driver of cloud adoption, second only to an increased need for agility/speed to market.*

01**02**100

Direct experience drives confidence in cloud security.

A majority of respondents (67%) cited direct experience with cloud vs. on-prem security as a primary reason for increased confidence in cloud security, followed by detailed audits or examinations of their own cloud and on-premise systems (51%).**

00**03**011

Data security and auditability top the list of cloud security priorities.

A majority of respondents (71%) deem protecting data from compromise or unauthorized access as "very important." Other top priorities include auditability for compliance/regulatory/auditing purposes (52%) and protecting applications or websites from compromise or downtime (59%).

**Respondents were asked to identify the top two reasons for increased cloud adoption. "Increased need for agility/speed to market" ranked among the top two for 45% of respondents, and "increased confidence in cloud security" for 44%. Other top reasons included cost savings (34%), positive experience working with a cloud provider (30%), and launching new/experimental apps that are well suited to the cloud (25%).*

***Respondents were asked to identify the top two reasons for increased confidence in cloud security. "Direct experience of security in the cloud vs. on-premise" ranked among the top two for 67% of respondents, and "detailed audits/examinations of my on-premise vs. cloud security" for 51%. Other drivers included media/analyst reports (34%) and conversations with peers (21%).*

001101 11010101
101101 101001
00110 101
10 001
101
001

LOOKING AHEAD

At present, we filter 99.9% of spam and malicious email. It's not perfect, and we know we have more to do. We act fast on anything that gets through. A recent and rare phishing case affected fewer than 0.1% of our users and was shut down in less than an hour. Later the same day, we took measures to make sure it couldn't happen again, system wide.

Unfortunately, hackers are moving from lone actors to something like professional entities. Sometimes these involve state-backed or affiliated groups. We do not expect security problems to end. Big, well-funded outfits learn to automate things; that raises the prospect of global attacks on more entities.

We are investing and working hard to prepare ourselves and continue to warn our customers and subscribers, even of suspected account compromises. Rapid information sharing about phishing and malware attempts will continue to be an important part of system defense.

At Google Cloud, we obsess about security so that our customers don't have to. We believe that security is a critical component in furthering the positive impact of technology-in the enterprise, in education, in government, and especially when we use technology in our personal lives.

Contact Ancoris for help with migrating your on-site computing to Google Cloud for greater security.

Call 0845 2626747 or email info@ancoris.com , alternatively visit https://www.ancoris.com