Google Cloud

Safer With Google

How Gmail and Google Cloud help protect 1.5B users from attackers

What are zero-day attacks?

Zero-day vulnerabilities are unknown software flaws. Until they're identified and fixed, they can be exploited by attackers. Google's Threat Analysis Group and Project Zero actively hunts for these types of attacks because they are particularly dangerous and have a high rate of success.

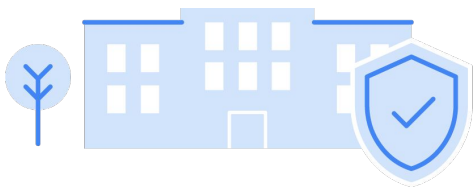
Why are on-premise systems more vulnerable?

On-premise systems offer a unique set of vulnerabilities because of different attack vectors at the operating system (OS) and application level, and because of delayed security patches.

On-premise systems can be difficult to keep up-to-date, and thus are easy for attackers to target. To make the situation more complex, attackers change their tactics all the time.

How do I keep my organization safe?

Protection against cyber threats requires a layered defense system, which can be implemented incrementally, if needed. We recommend using a cloud-native email solution with a focus on security, adopting security keys to provide an stronger authentication layer, and using secure endpoints (such as Chrome OS devices) that stop malware from running. The next few pages of this document outlines steps you can take to keep your organization safe.



Safer with Gmail

- Gmail is a **cloud-native** service and doesn't require any on-premise email server. Security updates are applied automatically without any user intervention required.
- Gmail helps keep users safe. We've yet to see anyone that participates in the Advanced Protection Program be successfully phished, even if they're repeatedly targeted.
- Gmail blocks **more than 99.9% of spam, phishing, and malicious emails** from reaching our users.
- Gmail blocks more than 100 million phishing emails every day and more than 300 billion attachments are scanned for malware every week.

> Gmail is much better than our previous malware filter. The first month after we migrated, we ran the two systems in parallel. Gmail removed 107,000 malicious emails that the old system didn't catch."
>
> State of Arizona Customer Story

Google Cloud

How Gmail and Google Cloud can help keep you safe

Google started in the cloud and runs on the cloud, so it's no surprise that we fully understand the security implications of powering your business in the cloud. Our robust global infrastructure, along with dedicated security professionals and continuous innovation, enables Google to stay ahead of the curve and offer a highly secure, reliable, and compliant environment.

1. Secure email systems

Why is this important: "The second most popular ransomware attack vector is email phishing. Using links, attachments, or both, an email phishing attack seeks to trick users into taking some sort of action. Phishing emails containing links may appear to come from a known contact asking a user to enter credentials for a bogus purpose." - Digital Defense

The Gmail Advantage: Gmail is a cloud-native email service. Advanced phishing and malware protection within Gmail are on by default. Controls also help you quarantine emails, defend against anomalous attachment types, and protect from inbound spoofing emails. Security Sandbox detects the presence of previously unknown malware (Zero-Day attacks) in attachments. VirusTotal (a Google Cloud product) can also be used to research malware.

2. Limit web attacks

Why is this important: "[A poisoned DNS cache] gives your web browser or other internet application a malicious IP address. Instead of going to where you want to go, you're sent to a fake site. That forged website can then upload ransomware to your PC or grab your user name, password, and account numbers." - ZDNet

The Chrome Browser Advantage: Chrome is one of the most secure browsers in the world with advanced technology like site isolation, sandboxing, and predictive phishing protection. Safebrowsing protects 4 billion devices from a range of deceptive sites and downloads. BeyondCorp Enterprise extends advanced malware protection, real-time phishing protection, and data leakage prevention to Chrome for enterprise users. Chrome automatically updates every six weeks, so your system is always running the latest security features and fixes.

3. Stop account takeovers

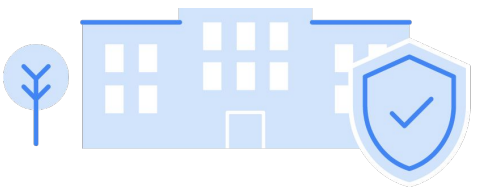
Why is this important: "Once malicious actors attain credentials, they can bypass endpoint protection and begin wreaking havoc on enterprise systems, including wiping or encrypting data backups." - Digital Defense

The Advanced Protection Program Advantage: Google's Advanced Protection Program has yet to see anyone who has participated in the program be successfully phished. Google employs many layers of machine-learning systems for **anomaly detection** to differentiate between safe and anomalous user activity across browsers, devices, application logins, and other usage events.

4. Choose resilient cloud services

Why is this important: "CISA has determined that this exploitation of Microsoft Exchange on-premises products poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. This determination is based on the current exploitation of these vulnerabilities in the wild, the likelihood of the vulnerabilities being exploited, the prevalence of the affected software in the federal enterprise, the high potential for a compromise of agency information systems, and the potential impact of a successful compromise." - dhs.gov

The Google Cloud Advantage: Google Cloud Platform and Google Workspace services aren't as vulnerable to malware like traditional on-prem solutions. Google Cloud's services are also automatically patched against the latest security threats.



Google Cloud

5. Adopt cloud-first devices

Why is this important: "Software vulnerabilities come in third among common ransomware delivery methods. Unpatched software not only opens the door to malware intrusions, but lays out a welcome mat as well. In some cases, when software is not properly updated or patched, attackers can access networks without having to harvest credentials." - Digital Defense

The Chrome OS And Device Advantage: Chromebooks are designed to protect against phishing and ransomware attacks with a low on-device footprint, read-only capabilities, a constantly updating Operating System (in the background), sandboxing, verified boot, safe browsing and Titan-C security chips.

6. Recover critical files

Why is this important: "Although data backups are part of the layered approach to protecting your business, many organizations are improperly backing up their data, and these backups must be protected and kept safe from ransomware attacks. Businesses that do not adhere to strict data backups procedures may find themselves in an awkward position if their files become encrypted during a ransomware attack."

- Infosecurity Magazine

The Google Drive Advantage: Drive keeps older versions of files from a pre-ransomware time, which can then be safely recovered.

7. Investigate attacks

Why is this important: "Most forms of malware use the network to either spread or send information back to their controllers, so network traffic contains signals of malware infection that you might otherwise miss; [...] tools analyze logs from various computers and appliances across your infrastructure looking for signs of problems, including malware infection. " - CSO

The Chronicle Advantage: Chronicle is a threat detection solution that identifies threats, including ransomware, at speed and scale. It includes a rules engine that operates at the speed of search, a rules language to express complex threat behavior, and a regular stream of new rules and indicators.

8. Remediate compromised systems

Why is this important: "It's an imperfect world, and there are products out there that contain vulnerabilities, known or as of yet undiscovered. Having a strategy in place to manage vulnerabilities throughout the entire lifecycle of a device can help the security team keep control of potential security worries." - ZDNet

The Security Center Advantage: Google Workspace Security Center and **GCP Security Command Center** are security and data risk platforms that can help organizations gather data, identify threats, and help remediate issues.

Did you know...

Gmail blocked more than 18 million malware and phishing emails, and 240 million spam messages, daily related to COVID-19.

To learn more, visit:

https://cloud.google.com/security
http://workspace.google.com/security