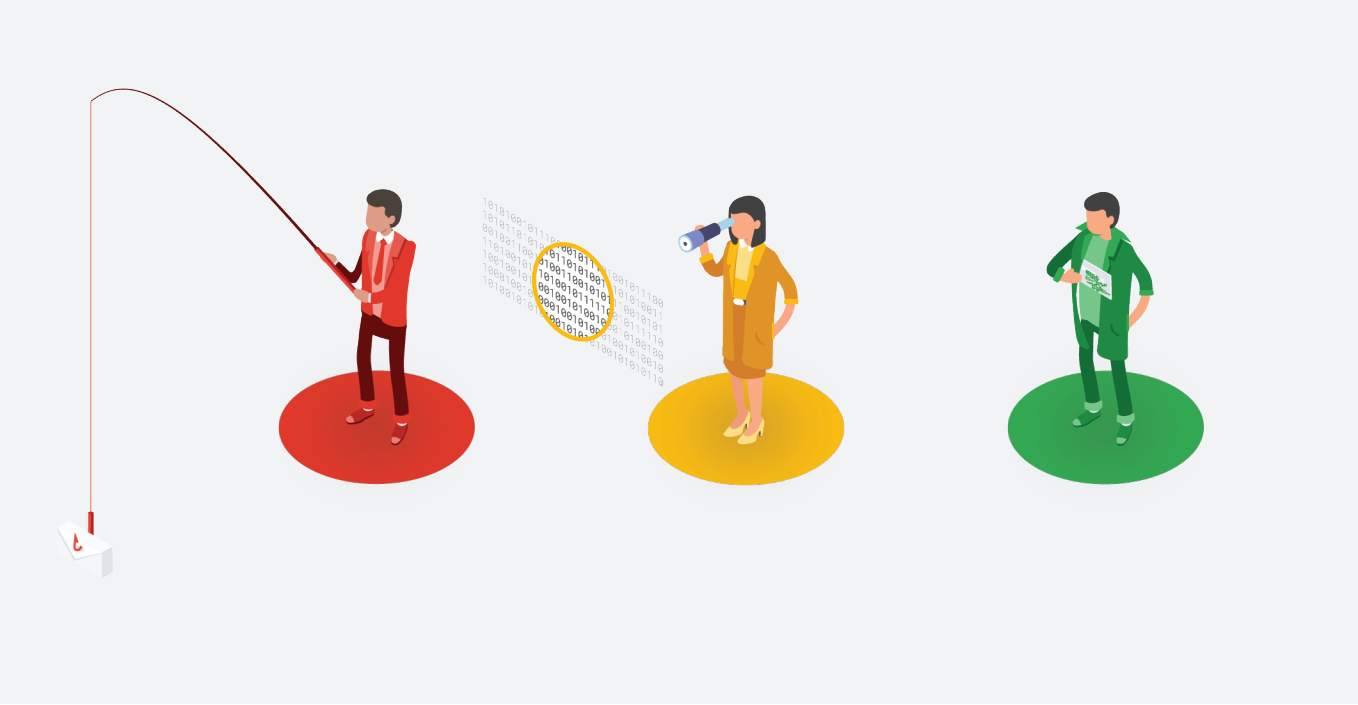
Cloud-Native Security for Endpoints

Chrome Enterprise's innovative approach to protecting data and simplifying IT management



chrome enterprise

chrome enterprise

Table of Contents

There Has to Be a Better Way

Endpoint security is a mess

Protecting endpoints is one of the greatest single challenges faced by cybersecurity and IT operations professionals. They find themselves facing intractable problems and continuously evolving attacks.

Traditional endpoints are complex. They typically:

1. Contain hundreds of pieces of software that bad actors can target, including old and unpatched versions and non-approved software packages
2. Are vulnerable when users visit malicious websites, download unknown apps, or prevent needed software updates from being applied
3. Store gigabytes of intellectual property, personally identifiable information (PII), and user credentials
4. Have poorly-enforced boundaries between processes, so a single compromised software module can give attackers access to the entire system and the corporate network

In this environment, cybersecurity teams expend tremendous effort attempting to monitor endpoints, identify vulnerabilities, and detect compromises. Operations teams are overwhelmed trying to enforce consistent images and to patch and update firmware, operating systems, utilities, drivers, browsers, and applications across hundreds of distributed devices. To make matters worse, increasingly users are working at home or on the road, so tools and processes designed for corporate networks are becoming less and less effective.

Time to rethink the model

Now you have an opportunity to escape from this quagmire and make game-changing improvements in endpoint security and administration.

First, IT organizations can capitalize on the inherent advantages of cloud-based architectures for security and operations. It is easier to monitor information assets when they are stored and shared in the cloud rather than on vulnerable endpoints. It is much easier to track and update software executing on a central cloud platform instead of on hundreds of remote devices.

Second, technology vendors are fundamentally rethinking “cloud-native” security and introducing remarkable new capabilities for strengthening endpoint security and simplifying endpoint management.

In this white paper we will examine how Google has re-engineered endpoint security by leveraging the inherent advantages of cloud computing and by creating innovative multi-layered defenses at five levels: device, firmware, operating system, browser, and application.

We will also explore examples of how:

1. Google’s innovative security features protect against specific threats such as malware, phishing, drive-by downloads, and APTs
2. Chrome Enterprise dramatically simplifies operational tasks such as updating software, coping with lost and stolen devices, and managing security policies for distributed devices
3. You can utilize Microsoft Active Directory and leading third party enterprise mobility management (EMM) tools to automate endpoint management

Leveraging the Inherent Advantages of Cloud Computing

Fewer assets on endpoints

One of the inherent advantages of cloud-based architectures is that most information assets are stored in the cloud and not on endpoints. You don't have to worry that customer lists, business plans, earnings reports, human resources data, or software programs are exposed when a laptop is lost or stolen. If a device is compromised, bad actors are much less likely to find customer credit card numbers, employee medical information, or passwords that give them access to company financial systems.

A reduced attack surface

With a cloud-based architecture, far fewer pieces of software are installed on endpoints. Distributed devices still need firmware and an operating system, but not the dozens of utilities, drivers, browsers, business applications, and personal apps that accumulate on traditional endpoints. Compared to traditional endpoints, there are not nearly as many vulnerabilities that attackers can target, and a fraction of the number of software components that need to be installed, managed, and protected.

Fast, frequent updates

With traditional endpoints, there is no end to the exhausting routine work of patching and updating software components on devices across the country or the world. Also, every time a vulnerability is announced or a new attack technique is uncovered, cybersecurity and operations staffs must race to patch or add controls on hundreds of endpoints. The longer the "window" stays open, the greater the chance that aggressive hackers will exploit the opportunity.

With cloud-based architectures, you can update software centrally, deploy and manage controls in one place, and dramatically reduce the work required to keep endpoints current.

The Device: Built-in Security and Consistency

A cloud-based architecture offers a remarkable number of opportunities for innovative security and management features. These start with Chrome devices such as laptops and tablets powered by Google's Chrome OS and Chrome browser. Chromebooks are available from a range of industry-leading technology companies such as Acer, ASUS, Dell, Google, HP, Lenovo, and Samsung.

The hardware security module

All recent Chromebooks include a hardware security module designed to meet Google's specifications. The module includes flash memory, ROM, RAM, and tamper-detection features on a dedicated chip, making it extremely difficult to tamper with information stored in the module. The hardware security module stores critical information and cryptographic keys so they are inaccessible to the operating system, and protects against certain types of side-channel information leakage attacks and physical fault injection techniques.

Encryption and separation of user data

All Chromebooks encrypt user data and settings by default. This encryption cannot be disabled by users (or anyone else).

In addition, each user's data and settings are encrypted with a unique key. To use that key, an attacker would almost always need both the user password and access to the security module. That makes it very hard for bad actors to read any user's data, and even if bad actors have possession of a Chromebook and one user's passcode they cannot decrypt and read the data from other users.

Separating user data has another benefit as well: it makes it safer to share devices with colleagues and family members, and to adopt leading-edge practices such as "Grab and Go" sharing for loaner devices and temporary workers.

Scenario: Preventing an insider breach

A Chromebook is shared by Xavier, Yao, and Zelda, three contractors who work on different days. Unfortunately, Xavier is an amateur hacker who wants to access a server that Zelda supports. He knows that valuable algorithms and proprietary software are stored there. Xavier signs onto the Chromebook and uses it for his own work — but he can't access Zelda's credentials, network connections, or any of her other data or settings. The data on that server is safe.

Consistency across endpoints

Chromebook manufacturers agree to meet or exceed specifications set by Google for quality, performance, and security. Google reviews and approves the hardware designs before the devices can be shipped with the Chrome brand. The manufacturers also agree to use consistent firmware and the same Chrome OS and Chrome browser that run on every other Chromebook. (Figure 1)

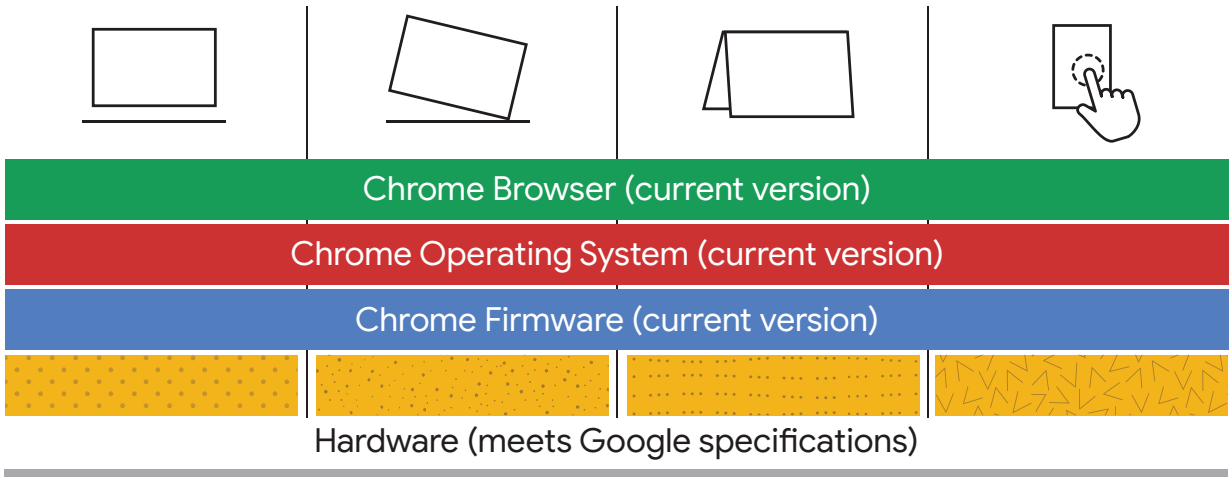


Figure 1: For a seamless user experience and simplified management, all Chromebooks run consistent versions of the firmware, Chrome operating system, and Chrome Browser.

This commonality is an important advantage for both users and administrators. Users enjoy a consistent experience and a higher comfort level across all Chromebooks. Security and operations teams can provide a standard operating environment. They don't have to manage multiple versions of firmware, operating systems, system utilities, and browsers, or worry that incompatible software releases will create vulnerabilities. When issues do occur, troubleshooting is much easier and faster.

Good decisions for security

Google works with its ecosystem partners to identify features and default settings that promote security for users who may not be savvy about cybersecurity — or about using computers at all. Above we mentioned that all user data is encrypted by default, and we will discuss more examples later in this document.

Firmware: A Chain of Verification

"Persistence" is a key element of most advanced targeted attacks. Sophisticated attacks typically depend on planting code or scripts on endpoints that allow the attackers to maintain a presence on the endpoint through a reboot or system failure.

Cloud-based architectures deny to attackers many of the techniques they use on traditional endpoints to gain persistence. For example, if there are no user installable drivers or scripts stored on the endpoints they cannot be used to retain malicious code through a reboot.

However, bad actors can still attempt to inject code into the writable firmware, operating system, and browser that are stored on the device.

To prevent this, Google uses a technique called "verified boot" to ensure that the firmware, operating system, and browser code executing after reboot are all software from Google, with no alterations.

Scenario: Block That Rootkit!

Bela, a cybercriminal, gains access to a Chromebook and obtains superuser privileges. She remounts the root partition read-write directly, then adds a rootkit in the form of a kernel module. However, on the next reboot, the signature of that part of the root partition doesn't match the expected signature. The boot process stops and the device reboots using the backup image of the firmware and OS. After the reboot Bela can no longer use the rootkit to control the device.

When a Chromebook boots up, read-only firmware uses a signature and a signed hash to verify that the writable firmware exactly matches the image approved by Google (i.e., it computes a hash for the firmware code and verifies that it matches the signed hash). The now-verified writable firmware then uses the same process to verify the kernel, which goes on to verify all of the blocks of code in the operating system and the Chrome browser. If any evidence of malware or other discrepancies are found, the boot process stops, and the device reboots with a backup version of the writable firmware and operating system. (Figure 2)

Verified boot not only protects against a dangerous class of attacks, it also enables operations staff to avoid the tedious work required to remediate compromised firmware and files.

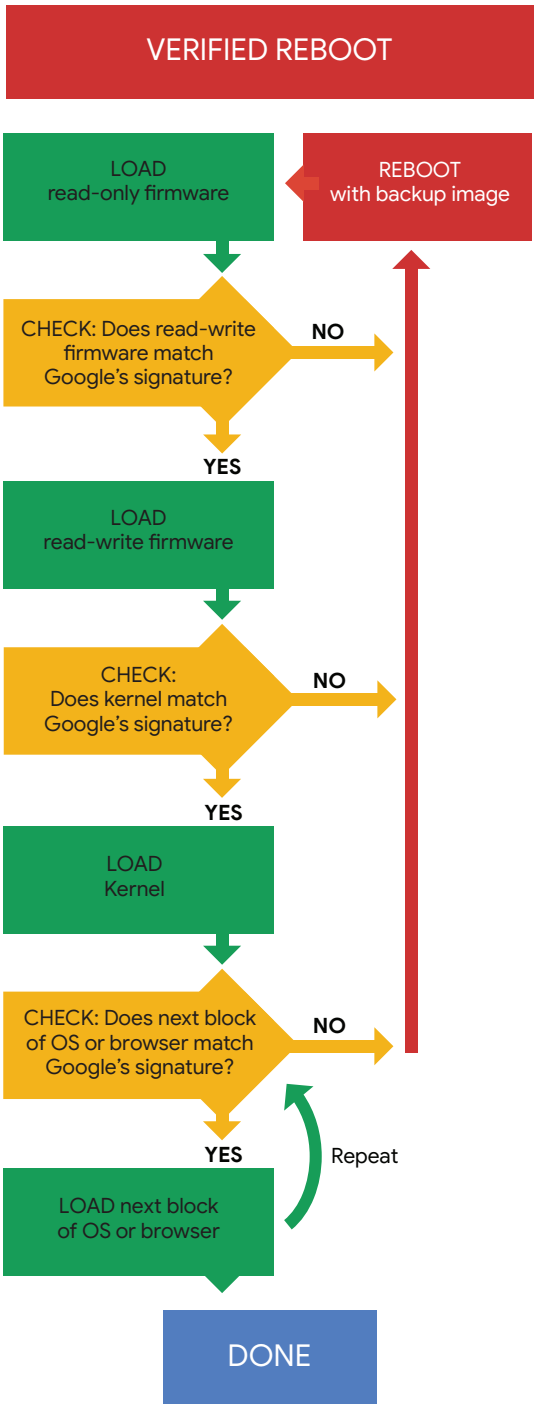


Figure 2: The verified boot process ensures that nobody has tampered with the firmware, operating system, or browser.

Operating System: Process Sandboxing and Seamless Updates

The Chrome operating system includes several security features that protect applications and eliminate the hassles usually involved in updating and patching operating systems.

Privilege separation and process sandboxing

Several classes of cyberattack use compromised websites or cloud-based applications to take control of software components on the endpoint.

In a cloud-native environment there are far fewer operating system components, utilities, drivers, and other pieces of software that can be compromised. But the architecture of Chrome OS does even more to prevent applications under the control of attackers from affecting other software.

For example, Chrome OS utilizes process sandboxing. This enforces strict boundaries between processes while they are executing, so applications can't communicate with each other except under strictly limited conditions. Each executing process is only able to use the privileges it actually needs. Much as security-oriented organizations restrict access to confidential information to people with a "need to know," Chrome OS limits the interaction between processes to those with a real "need to use."

Scenario: Rejecting Ransomware

Arjun is taking a few minutes off to find new digital wallpaper for his Chromebook screen. Unfortunately, the Fortnite fan website he lands on is a "watering hole" controlled by cybercriminals. When he clicks on a link to download a file, malicious code attempts to encrypt all data and files on the Chromebook. Fortunately, the actions of the code are contained within a single process sandbox. Arjun sees a prompt saying "You can't run this file," and the ransomware attack is halted before it can reach any user data.

Seamless updates of the operating system

Keeping operating systems current is a huge headache for most security and operations teams. Operating system updates on traditional endpoints are disruptive to end users. They can lock up endpoints for a few minutes, or over an hour. This creates a real cost in terms of lost productivity, and can lead to user frustration and unpleasant thoughts about the IT organization.

Even worse, often users decline to allow the updates, leaving their devices vulnerable to attack.

Google provides an innovative solution to this challenge. Each device stores two versions of the operating system, the current one and a previous version. While the system is running using the current operating system, an updated version can be downloaded and stored transparently behind the scenes, with no impact on the user. When the user reboots, the updated operating system is loaded in seconds. (Figure 3)

This arrangement also simplifies the verified boot process, which we described earlier. If the system finds during bootup that someone has tampered with the code of the running copy of the operating system, the previous, clean version is already on the device, ready to be used immediately.

Chromebooks eliminate the headaches involved in routine updates of operating system components. In fact, Google is able to update Chrome OS about every six weeks, far more often than other major operating systems. It also deploys security patches extremely quickly against newly discovered operating system vulnerabilities, to reduce the window of exposure.

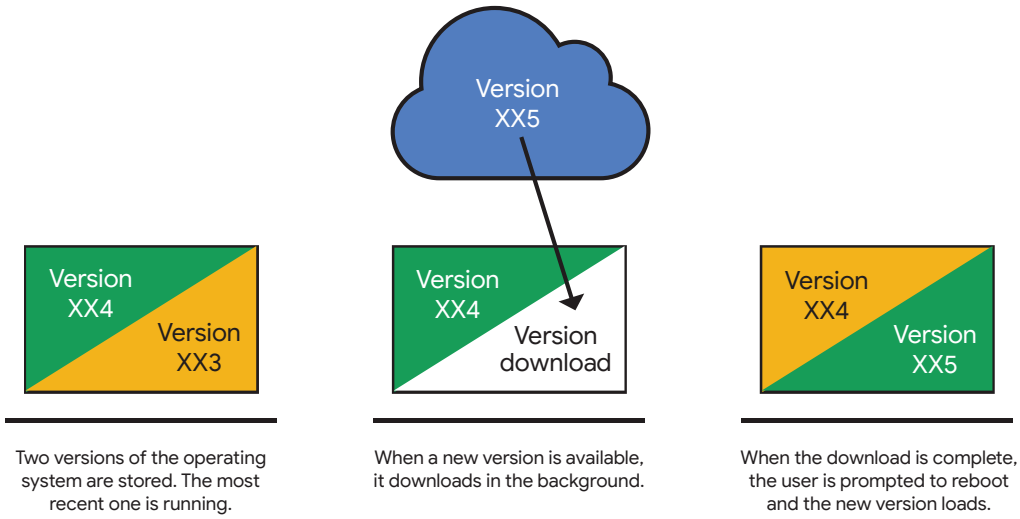


Figure 3: New versions of the operating system are downloaded in the background, without disrupting the user's work.

Browser: Site Isolation, Safe Browsing, and Two-Factor Authentication

On Chromebooks, all interactions with the web are through the Chrome browser. Users benefit from the innovative security features built into Google's industry-leading browser.

Tab sandboxing and site isolation

The concept of sandboxing we discussed in reference to the Chrome OS is also applied in the Chrome browser. Every open tab in the browser has its own sandbox, which greatly limits the chances that an attack in one tab can leak over and affect others.

The principle can be carried even further with site isolation. There are many situations where several websites are accessed within a single tab. For example, reading an HTML web page on one site might cause images to be downloaded from a second site, videos from a third site, and a script from a fourth. With site isolation, the processes from each of those sites are kept separate. (Figure 4) With the Chrome browser, administrators can choose to isolate all sites or selected sites.

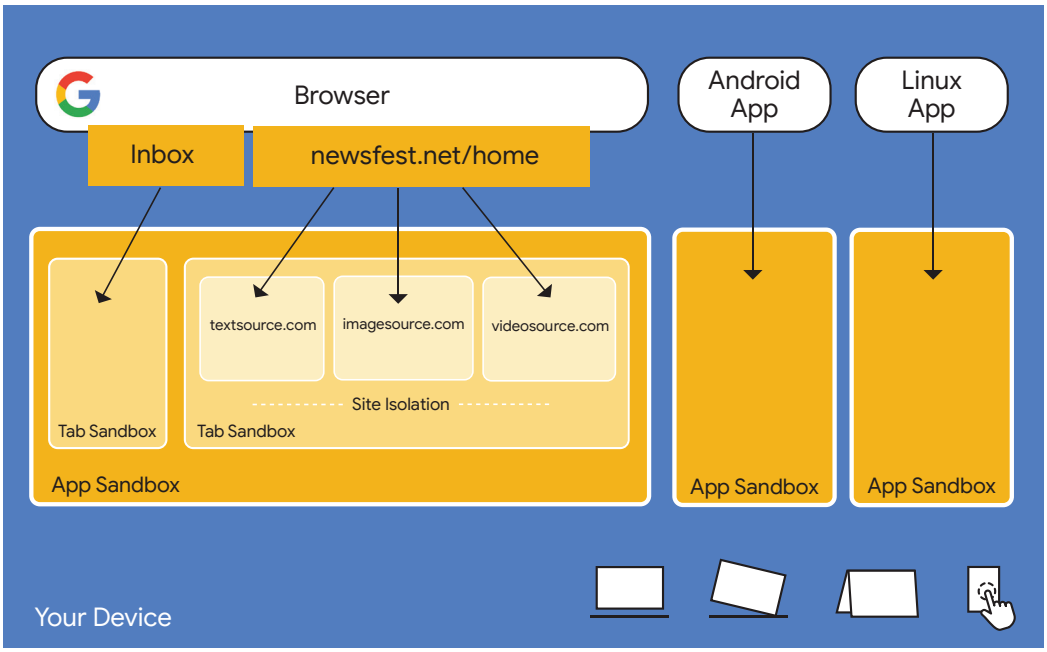


Figure 4: The Chrome OS and Chrome browser offer multiple levels of isolation — site, tab, and application.

These capabilities help protect against threats like universal cross-site scripting (UXSS) and speculative execution side-channel attacks (such as Spectre and Meltdown) where a malicious website tries to access processes or data in memory belonging to a different website.

Safe browsing

Many of the greatest dangers to enterprises today involve malware and phishing attacks launched from compromised websites.

Google's Safe Browsing feature presents users with warnings when they attempt to navigate to websites that contain malware or phishing content, or to download suspicious files. It is based on a Google service that discovers thousands of unsafe websites every day and protects 3 billion devices.

Safe Browsing messages are displayed not only from Chrome browser screens, but also in Google searches and Android apps to warn of dangerous sites, and in Gmail messages to warn of email links to malicious sites.

Scenario: Dodging a Phishing Attack

Emily is the chief financial officer at a small manufacturing company. She receives an email from the CEO to wire $20,000 to a new supplier in China, immediately, to lock in a supply of a component that is in very short supply. Emily knows that the CEO is travelling in China to line up vendors, so the email is plausible. But when she clicks on a link in the email to the new vendor's website, she receives a warning that the site is deceptive and is invited to click a "Back to Safety" link on the warning screen. Safe Browsing has helped Emily dodge a business email compromise (BEC) phishing attack.

Security keys and two-factor authentication

Two-factor authentication (also called two-factor verification) can protect systems and data even when user credentials have been compromised. To authenticate themselves, users are asked to provide something they know, typically a password, with something they have, often an authentication key or a code sent to their smartphone.

Google offers what may be the world's fastest, easiest way to implement effective two-factor authentication. Users only need to go to their Google accounts, select "2-Step Verification," and pick an option for their second authentication method. The options include being sent a code in text, tapping a prompt on their phone, or using a Titan Security Key that connects to Chromebooks through a USB port. For convenience, users can designate some devices as trusted, and sign into those devices without the second authentication method.

Applications: Malware Detection, Whitelisting and Blacklisting

Chromebooks can run a wide variety of applications, including Android apps, office productivity applications such as Gmail, Google Docs, Google Sheets, Google Slides, and Google Drawings, Chrome extensions, Linux-based apps, and PWAs (progressive web apps: applications that load quickly and offer functionality and responsiveness on a par with locally installed applications).

When enterprises give users access to Google-supplied applications via the Chrome Web Store and to Android apps through the Google Play Store, they benefit from a number of capabilities that strengthen security and simplify administration.

Server-side malware detection and remote uninstall

Google Play Protect is the most widely deployed mobile threat protection service in the world, securing two billion users daily. Experts on the security team for Android subject all Android apps to rigorous security testing before allowing them to appear in the Google Play Store. Apps and developers that violate Google policies are not accepted for the store.

In addition, Google Play Protect continuously scans and verifies apps in the Google Play Store. When malware is found in an app, not only is that app suspended immediately from the Google Play Store, it is also uninstalled from all systems where it had been downloaded.

App curation and whitelisting through the Google Play Store

Users all too often facilitate data breaches by downloading applications that contain vulnerabilities or are actually developed by bad actors.

For decades, IT administrators have tried to curb promiscuous downloading by exhorting users to install only approved applications, or by locking down endpoints

Scenario: Putting a Brake on Shadow IT

Carlos manages an international marketing team on four continents. He wants to implement a collaboration tool to improve communication and planning. When he finds online an article called The Top 20 Online Collaboration Tools it doesn't occur to him that many of them lack enterprise-grade security and management features. Luckily, before he spends too many hours playing with all 20, he checks his company's managed Google Play store. He finds that there are two approved team collaboration apps, Slack and Google Hangouts. Both have excellent functionality and security. As a bonus, they are supported by the company's IT organization, and using either of them will allow his team to collaborate with all of the other groups using the same apps.

so only approved applications could run on them. The former approach has been ineffective because the list of approved applications is inevitably too small to satisfy everyone's needs for business applications and their desires for personal applications and entertainment. The latter approach has failed because technology to lock down traditional endpoints has been difficult to implement and has usually met considerable resistance from users.

Web-based technologies give security and operations teams new opportunities to stem the flow of unauthorized applications without disappointing or annoying users.

Google Play Store offers users thousands of apps for business productivity, communication and collaboration, managing business processes, news, entertainment, and games, all tested by the Android security team to make sure they do not contain vulnerabilities or serious security flaws.

Administrators can create a managed Google Play store for their organization and curate a wide, but still generous, set of applications. They might, for example, offer employees of their company a large selection of productivity and collaboration applications, but limit the availability of games and social media apps. (Figure 5)

When it is appropriate, the managed Google Play Store makes it easy to go even further and implement a whitelist, so that everyone in the organization is required to use the same productivity and collaboration tools and allowed to pick from a modest selection of other apps.

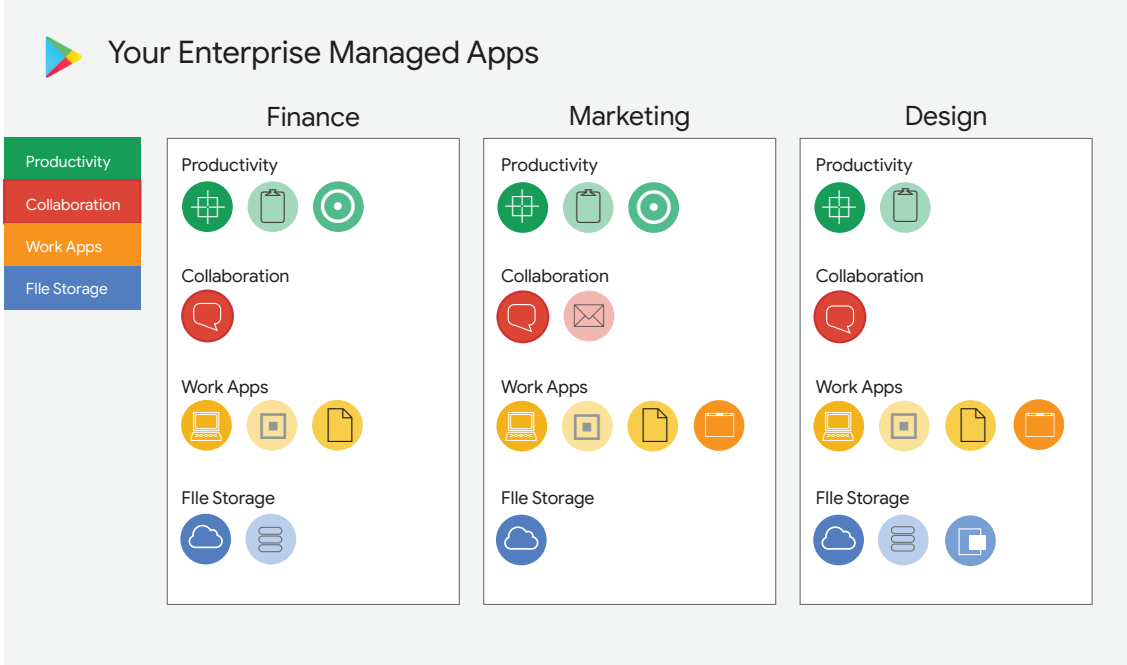


Figure 5: With a managed Google Play store, each group in the enterprise can access a curated list of authorized applications.

Centralized Administration with Chrome Enterprise

Chrome Enterprise enables security and operations teams to centrally manage policies on Chromebooks and other endpoints with the Chrome OS, as well as policies for Chrome browsers on Windows, Mac, and Linux systems. Chrome Enterprise Upgrade combines device management capabilities with 24/7 support from Google, and helps enterprises scale to environments with tens of thousands of users and devices.

Overview of selected Chrome Enterprise policies

Chrome Enterprise allows administrators to set and enforce on endpoints more than 300 security and configuration policies. Key security-related capabilities for managed Chrome devices include:

Provisioning and deprovisioning devices. Administrators can enroll devices, or allow users to enroll devices, so they can be managed and protected by the Chrome Enterprise policies defined for the user's organization. Administrators can deprovision devices to disable the policies and prevent the devices from accessing corporate resources.

Remotely disabling devices. If devices are lost or stolen, they can be disabled remotely.

Restricting sign-in. Administrators can allow people to sign into a device anonymously (guest browsing), or require a Google or G Suite account, or restrict access to one or a few named individuals.

Setting ephemeral mode (wiping user data on log-out). Administrators can set devices to ephemeral mode, so that when users log out their data and settings (including browser history, extensions and their data, and web data like cookies) are wiped. Ephemeral mode makes it safer to use devices for sharing, for kiosks, and for short-term users.

Restricting or requiring web apps and browser extensions. Administrators can block users from installing any Chrome web apps and browser extensions (small software programs that customize the browsing experience), or block them from installing specific apps and extensions, or allow them to install apps and extensions only from specified URLs. They can also force the installation of specified apps and extensions.

Blocking applications based on permissions. Many Chrome apps and browser extensions request permissions to use resources on the devices where they are installed. Administrators can block the installation of apps and extensions that use specified permissions. For example, they can prevent the installation of apps and extensions that request permission to capture screen, window, or tab content, read the contents of the clipboard, capture audio or video from the device's microphone or camera, obtain the user's geo location, query metadata about the device's network, or override the device's power management features. This capability allows the IT organization to reduce risk while giving users freedom to install "harmless" apps that do not threaten security.

Disabling bluetooth and geolocation. Bluetooth and location tracking can be disabled on devices.

Restricting the use of external storage devices. The use of external storage devices such as USB flash drives, external hard drives and optical storage devices, and memory cards, can be blocked entirely, or allowed only in read-only mode.

Managing remote access and single sign-on. Administrators can set parameters for remote access and SAML-based single sign-on (SSO), so that users can access the network and web applications with the right balance between security and convenience.

Tracking devices and users. For each device, reports are available showing data such as the operating system and firmware levels, statistics on CPU and RAM usage, storage devices attached, usage metrics, diagnostic data, which users have logged on recently, and when those users were active.

Delegated administration and flexible management

With Chrome Enterprise, administration tasks can be delegated to share work and give the right individuals responsibility for managing groups and departments. Roles can be created to give administrators different permissions to read or write settings for managed devices, users, and applications.

Chrome Enterprise offers flexibility in how policies are created and applied. Administrators can create policies for users and user groups, in which case each user sees the same policies applied on all of his or her devices. Alternately, administrators can create policies for devices, and those policies will be enforced for each device, no matter who is using it.

Scenario: No, You Can't Listen to This Meeting

Your CEO and CFO are going overseas to negotiate a critical deal. It could cost your company a lot of money if their strategy sessions could be overheard by the other party or the host country's intelligence service. Fortunately, you can temporarily disable bluetooth and block the Chrome web applications and browser extensions that could access the microphone and camera on their Chromebooks (you might have to ask them to reboot to allow the changes to take effect).

Leveraging Your Management Infrastructure

Chrome Enterprise provides its own console for administrators, but is also designed to fit into your existing management infrastructure.

Integration with Active Directory and Google Cloud Identity

The Chrome Enterprise admin console is integrated with Microsoft Active Directory and Google Cloud Identity. For example, you can enroll Chrome devices in Active Directory. You can also push Chrome policies to users and devices based on user groups defined in Active Directory.

Working with leading EMM solutions

Enterprise Mobility Management (EMM) products help enterprises enroll, manage, and support laptops, tablets, smartphones, and other mobile devices. If your enterprise has invested in EMM solutions such as Cisco Meraki, Citrix XenMobile, IBM MaaS360, ManageEngine Mobile Device Manager Plus, and VMWare Airwatch, you can continue to use those products to manage Chromebooks alongside other endpoints.

Summary: Game-Changing Security and Operational Control

Cloud computing gives enterprises an opportunity to rethink the traditional endpoint model. A cloud-native approach can greatly strengthen endpoint security and dramatically simplify endpoint management.

Chrome devices leverage the inherent advantages of cloud computing, including fewer assets on endpoints, a smaller attack surface, and simple, fast updates. In addition, a cloud-native mindset paves the way for innovative security and management capabilities. These include security features built into the hardware and firmware, effective use of sandboxing and user-level encryption, fast, seamless updating of operating systems, safe browsing, simple two-factor authentication, application whitelisting, and simple management of security and operational policies scaling to tens of thousands of users and devices.

The result is a computing environment that is:

1. Secure by design
2. Far easier to administer than traditional endpoints
3. Ready to be integrated into your existing infrastructure

Learn more about
Chrome Enterprise security
(at https://cloud.google.com/chrome-enterprise/security/)