Protecting the Extended Workforce with BeyondCorp Enterprise

Google Cloud

White paper
May 2021

Table of Contents

Google Cloud

Google Cloud

Protecting the extended workforce

BeyondCorp protected profiles

As companies grow, the requirements and scope of supporting their workforce usually increases as well. Many times, in addition to hiring new employees, organizations may get supplemental help from contractors, vendors, or even temporary workers - an extended workforce - and these organizations also need to support this base of workers. This can prove challenging when the extended workforce is geographically distributed or located outside of the company's network perimeter, but still requires access to corporate resources. Furthermore, an additional layer of complexity is added when this group of workers uses personal devices or devices not managed by the enterprise.

BeyondCorp Enterprise recently introduced a new feature, **protected profiles**, which provides secure access to corporate resources from unmanaged devices via Chrome - all without the need for a VPN or a local agent. This paper will go over the key benefits and use cases of protected profiles, in addition to providing an overview of the admin and end-user experience.

Solution overview

2B

Users supported by Chrome

Chrome is one of the most popular browsers in the world, leveraged by over 2 billion users. In addition to providing cutting edge security and productivity features, Chrome allows enterprises to manage and customize the browser to fit their unique needs.

Chrome Browser Cloud Management gives IT administrators powerful and flexible management capabilities both in the cloud and on premises, at no additional cost.

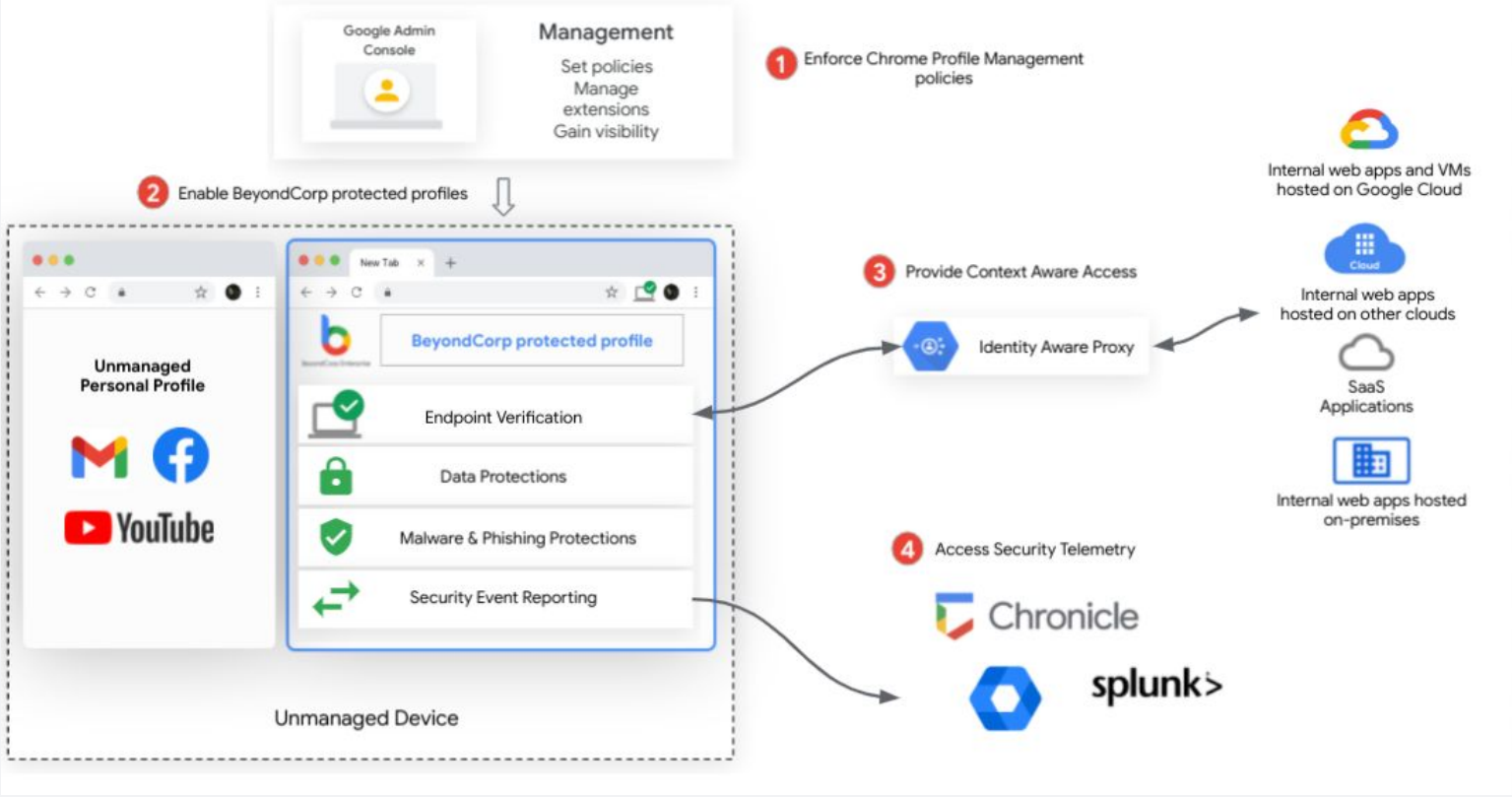
Administrators can choose to manage Chrome at the device level and at the user level:

- Device-level management is best for corporate-owned devices and allows admins to set up Chrome features for users, install Chrome apps and extensions, and easily manage policies.

- User-level (profile) management is best for unmanaged devices when admins are not able to install agents on the devices. Through profile management, admins can set hundreds of policies to enforce security standards set by individual organizations, and require installation of extensions.

Protected profiles leverage Chrome's user-level management capabilities to not only provide zero trust access to applications and resources, but also enable BeyondCorp Enterprise threat and data protection functionality on unmanaged devices.

Below is a high-level overview of the protected profiles feature:

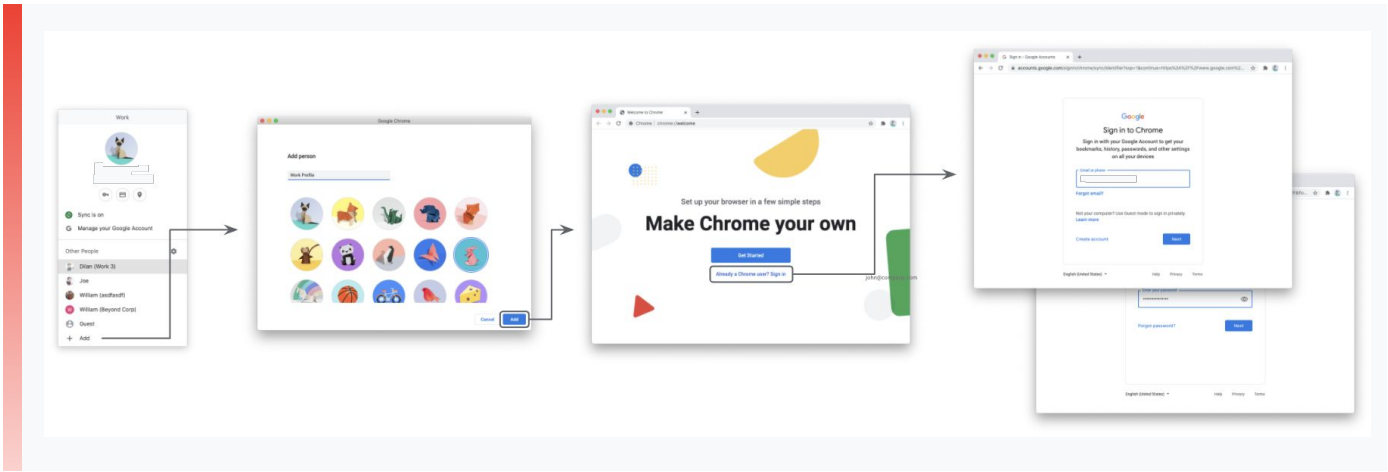


End-user experience

Protected profiles can be accessed by end-users from any Chrome Browser, whether the user is on a managed or unmanaged device.

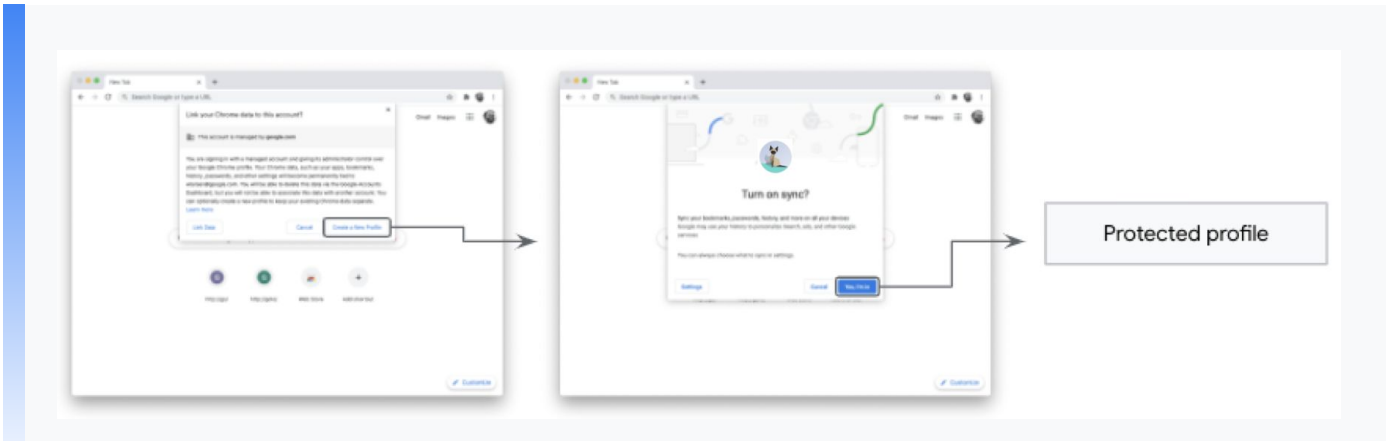
Signing in to a protected profile

Users will be able to access protected profiles from any Chrome Browser when they sign in to a new profile using their managed Google identity. Users can either click on the user icon (top right side of Chrome Browser) or sign in to a newly installed Chrome Browser.



Depending on the Google account and the access policies set by administrators, a user may be prompted for additional information at sign-on, such as two-factor authentication. Users will follow the instructions on their screen to complete signing into their Google account and authenticating their identity.

Once sign in is complete, users will be shown an end-user disclosure that informs them that they are about to sign in to a Managed Chrome Profile and that their administrator will be able to enforce policies within this profile. In addition, users will have to agree to turn on Chrome Sync for Chrome to be able to fetch and enforce enterprise policies.



After this step, users can resume their work and access SaaS applications and internal web applications as they normally would.

Admin experience

Manage user profiles on Chrome Browser

Whether your workforce shares devices or has a bring your own device (BYOD) policy whereby devices are not corporately owned or managed, organizations can still provide access, threat, and data protections with profile-level management.

As a Chrome Enterprise admin, you can enforce policies from your admin console that apply when users sign into the Chrome Browser from any Chrome OS, Windows, Mac, or Linux computer - not just from corporate-managed devices. In order to do so, your users must have managed accounts in your Google Admin console, such as with Google Workspace, Chrome Enterprise licenses, or Cloud Identity.

Managing user profiles on Chrome Browser allows you to leverage hundreds of Chrome policies including:

- Enforce Safe Browsing and prevent users from turning it off
- Allow, block, or force install extensions
- Enable Chrome Password Manager
- Enable BeyondCorp Enterprise threat and data protections

Learn more about setting Chrome policies for users here.

Admins can leverage the Chrome Browser Enterprise Security Configuration Guide for recommendations and critical items to consider when enabling or disabling Chrome Browser security policies for their organizations.

Enable context-aware access

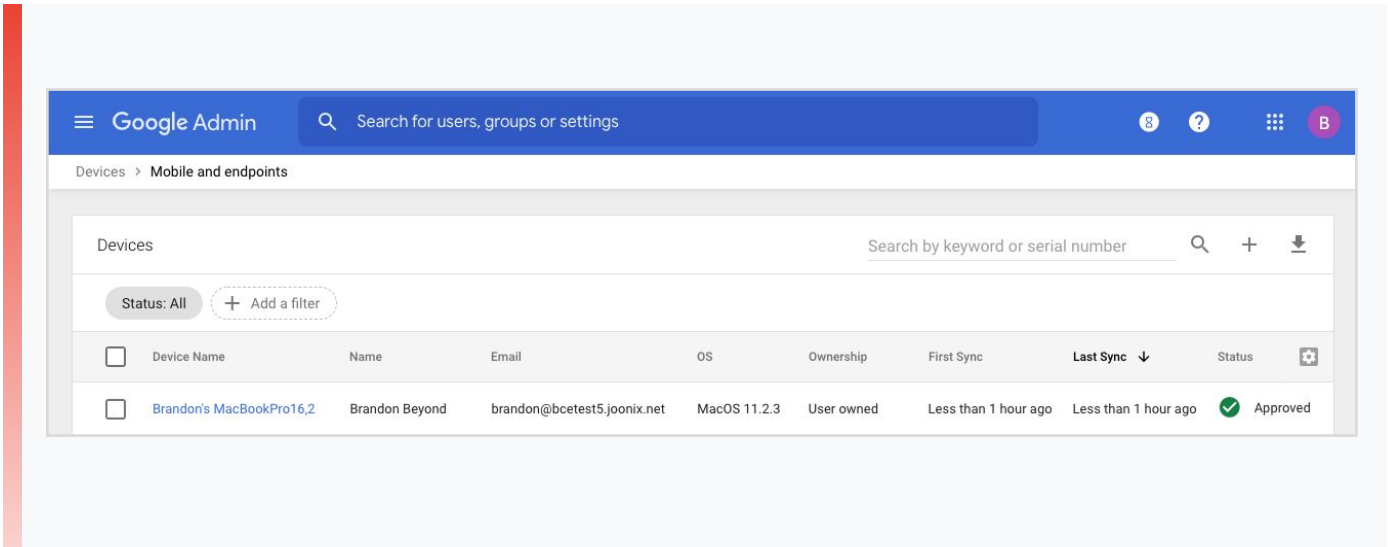
As an administrator, you can use Endpoint Verification to get details about devices running Chrome OS or Chrome Browser that access your organization's data. For example, you can get information about the OS, device, and user for personal devices and devices owned by your organization.

With this information, you can set up context-aware access policies to control device access to data and applications based on the device's location, security status, or other attributes. For example, you can require device approval, then create a context-aware access policy that blocks data access if the device status is pending approval or blocked.

There are multiple ways in which you can deploy Endpoint Verification to your environment, including:

1. Deploying the Endpoint Verification extension with Google Admin Console
2. Deploying the Endpoint Verification native helper with third-party tools
3. Self-installing the Endpoint Verification extension and native helper

Using the same Chrome Browser user profile management capability described above, administrators can configure to have the Endpoint Verification force-installed for all protected profiles logged in with corporate credentials.



Deploy threat and data protection

In addition to enforcing hundreds of Chrome policies, managing user profiles on Chrome now gives admins the ability to enforce BeyondCorp Enterprise threat and data protections at the profile level. As an admin, you can use the Google Admin console to ensure checks for sensitive data or help protect your Chrome users from content that may contain malware. You can also enable certain files to be sent for analysis (or prevent certain types of files from being analyzed). You can then choose to allow or block uploads and downloads for those scanned and unscanned files.

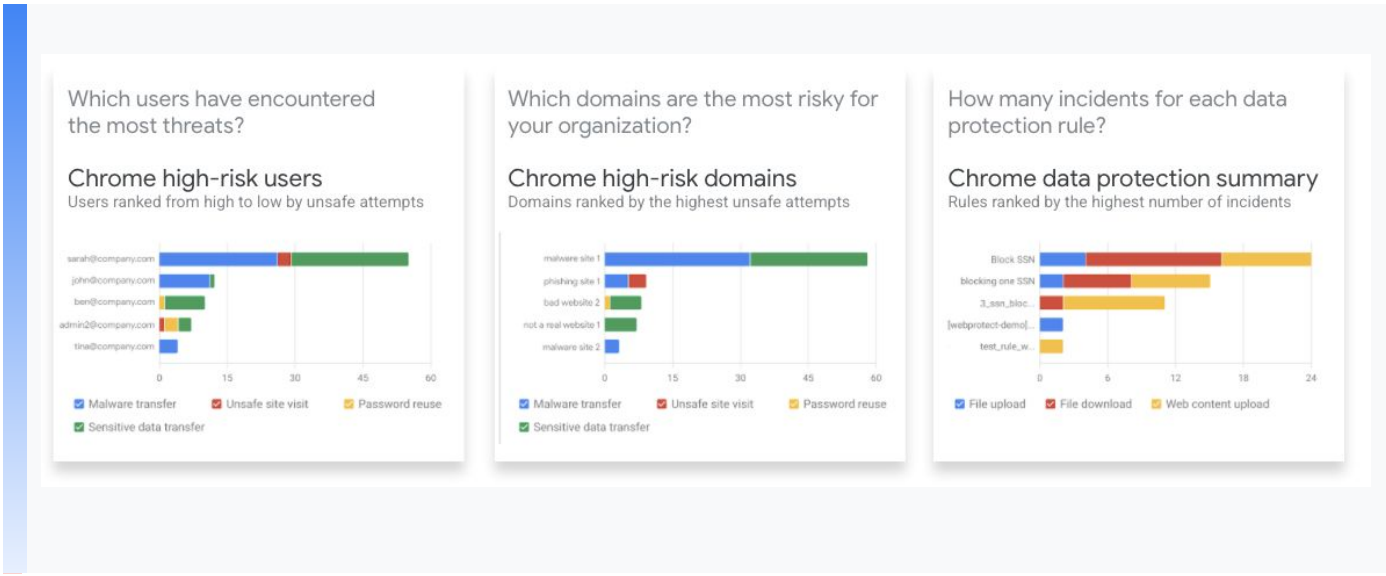
To enable protections against data loss and malware in Chrome, you need to enable Chrome Enterprise connectors so content gathered in Chrome is uploaded to Google Cloud for analysis. The Chrome Enterprise connectors must be enabled for data loss prevention (DLP) rules to integrate with Chrome.

After you enable Chrome Enterprise Connectors, you can create DLP rules. These rules are specific to Chrome and warn of or block the sharing of sensitive data. The rules trigger alerts and messages in the Chrome Browser, letting users know that file uploads or downloads are blocked, or warning that sensitive data might be shared.

For more detail about these rules, learn more here.

View security reports

The Security events reporting capability of BeyondCorp Enterprise allows administrators to view security telemetry from managed user profiles in Chrome. These events can be viewed directly in the security center for Google Workspace, a tool that brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users.



Available reports to view include:

- Chrome high risk users report which provides an overview of users who have encountered the highest number of unsafe Chrome-related events. Users are ranked by the number of unsafe attempts from all threat categories.
- Chrome data protection summary report which provides an overview of the number of Chrome-related incidents for the top data protection rules.
- Chrome threat protection summary report which provides an overview of various Chrome-related threat categories and related activities.
- Chrome high risk domains report which provides an overview of the domains that are most risky for the organization, ranked by the number of unsafe attempts.

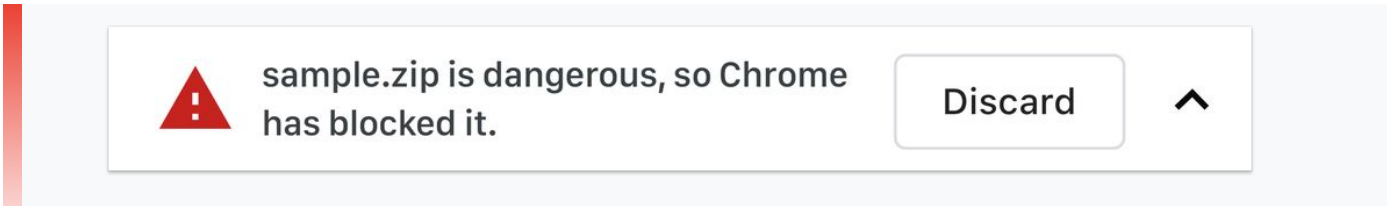
Use cases and scenarios

Protected profiles are ideal for different types of user groups within your extended workforce. For instance, frontline workers who share devices may need access to different applications depending on their role, but separate devices for each employee may be cost-prohibitive or unnecessary. Additionally, the remote workforce might need access to corporate resources from their personal devices. And of course, contractors often need to access corporate data from devices that are managed by their own organization, not their client's company.

In each of these cases, protected profiles allow an organizations' administrators to apply different security policies and access controls based on who has logged into the Chrome profile. Whether devices are shared, personally owned, or managed by another enterprise, protected profiles provide protection from malicious websites, phishing, and data loss, and allow end users to access corporate resources securely from any Chrome Browser by simply creating a profile.

Malware protection

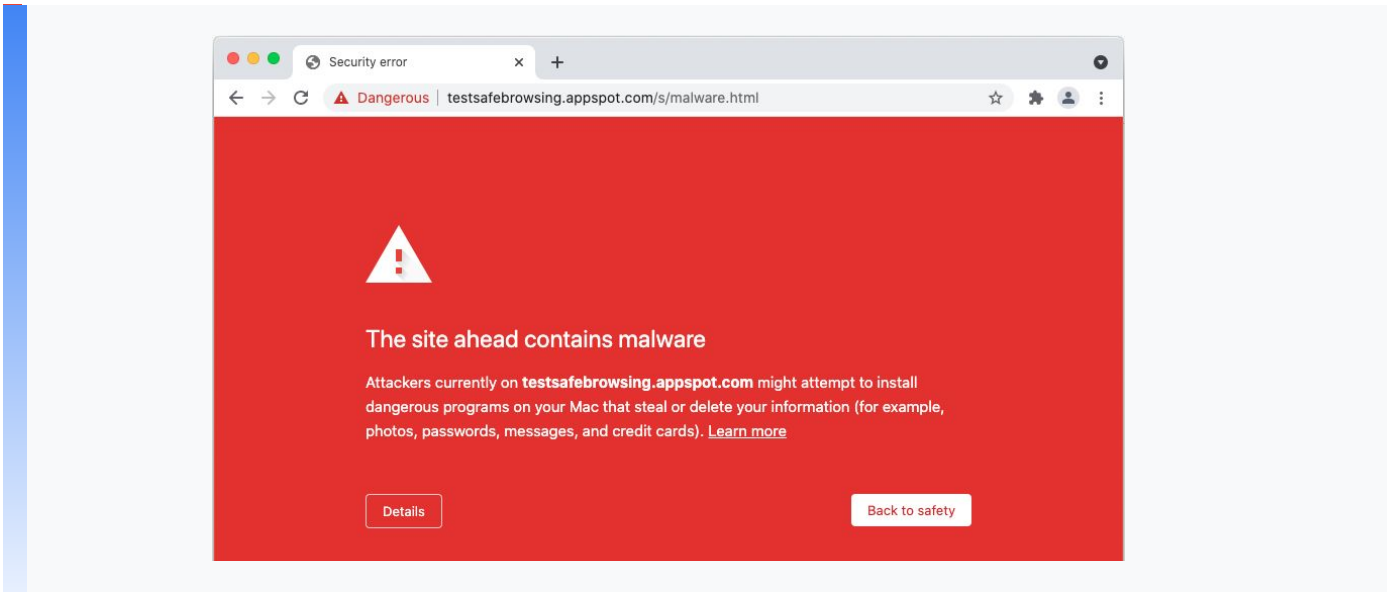
Once profiles are activated, administrators can control and monitor the use of corporate data. File uploads or downloads from inside protected profiles are scanned by Google Safe Browsing and its full suite of malware detection technology before they are allowed to be opened. If Safe Browsing determines that a file is malicious, Chrome will warn the user. Administrators can choose to allow users to bypass such warnings or prevent users from opening such files.



Real time phishing protection

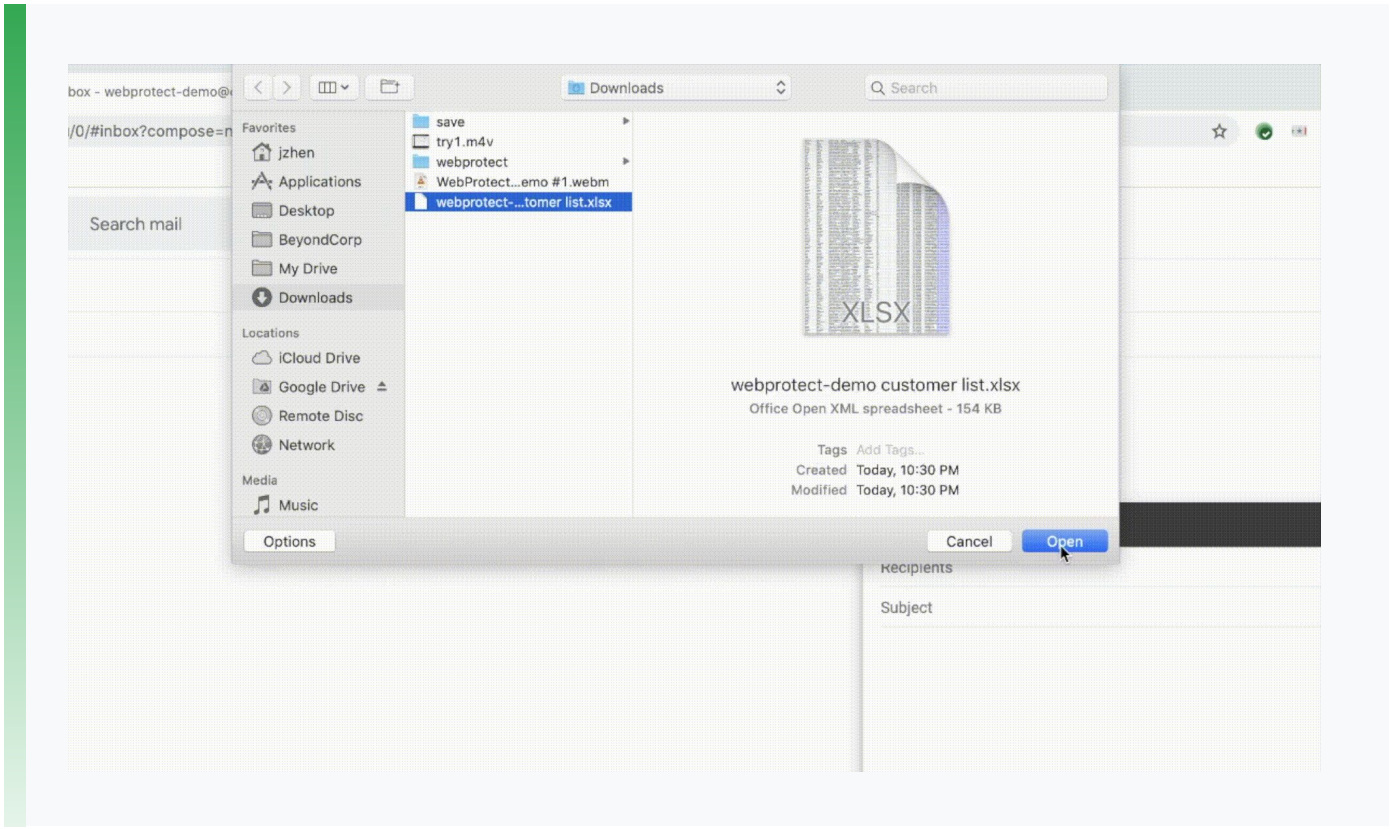
Real time checks inspect the URLs of pages visited from within protected profiles against the Safe Browsing database in real time.

When a user visits a website, Chrome checks it against a list of thousands of popular websites that are known to be safe. If the website is not on the safe list, Chrome checks the URL with Google Safe Browsing (after dropping any username or password embedded in the URL) to find out if users are visiting a dangerous site. If the site is determined to be suspicious by Safe Browsing, users are shown a warning. Administrators have the choice to allow users to bypass such warnings or prevent users from bypassing them.



Protect against data loss

BeyondCorp Enterprise allows enterprises to enforce a company's customized rules for the types of data that can be uploaded, downloaded or copied and pasted across sites. Any file that a user uploads or downloads or any content that is pasted across sites from within a protected profile is checked for compliance against customized DLP Rules configured by an administrator. If it is determined that the content violates a DLP rule, end users are shown warnings or prevented from completing the action based on the severity of the violation.



Leveraging protected profiles, admins can easily create granular policies and deploy them for specific user groups or activities, without disrupting operations.

The simplicity of this solution and our agentless approach with Chrome is ideal for all end users, but particularly seamless for the extended workforce, as they can securely and productively work and access resources as they normally would from a managed device.

Next steps

With BeyondCorp Enterprise, organizations can protect data and users against threats, and provide information to inform access decisions directly from the browser.

To learn more or to speak with a representative, please visit the BeyondCorp Enterprise product page.

g.co/cloud/bce

Google Cloud

Google Cloud