chrome enterprise

Implementing **zero trust security** with Chrome Enterprise and BeyondCorp Enterprise

Introduction

Network firewalls have provided perimeter security to organizations for decades. However, as news stories of data breaches prove, malicious actors can breach even the most robust firewall, wreaking havoc on an organization's operations and reputation.

Recently, securing firewalls has become even more challenging as organizations and their employees adopt mobile devices and cloud-enabled technologies.

Google's BeyondCorp Enterprise zero trust solution shifts access control from the network to individual users, enabling secure and safe access to enterprise resources based on contextual device and user credentials. It doesn't matter if the user is physically located in a company building or working from a home office; if their device and credentials cannot be authenticated, the user cannot access privileged network resources.

BeyondCorp Enterprise empowers IT professionals to enforce fine-grained access to enterprise applications and resources and enables users to work from any network without the need to connect to the privileged network via a traditional VPN.

Chrome Browser is the primary and most secure conduit for users to access sensitive corporate resources. Chrome's browser-based threat and data protection capabilities in BeyondCorp Enterprise provide real-time data loss prevention, malware scanning, and URL checks — all with visibility through the Google Admin Console.

Use cases

Chrome Enterprise and BeyondCorp Enterprise provide zero trust protection by combining Google's best-in-class security technologies, including context-aware zero trust access; data protection; and malware, phishing, and ransomware prevention.

BeyondCorp Enterprise's zero trust capabilities provide enterprise-grade protection across a wide range of use cases, including:

- Onboard a new employee or vendor and provide them secure access to corporate apps without the need for a VPN or local agent
- Ensure that a spreadsheet with sensitive data is only shared when policies you set are met, such as via corporate email and from devices that have enterprise-grade protections against phishing or ransomware
- Identify all employees who reuse their corporate passwords on non-corporate websites and automatically ask them to reset their passwords
- Protect privileged resources from malicious attacks with two-step verification
- Provide a partner access to privileged network resources based on authentication and contextual information based on what is known about the partner and their devices.
- Prevent leakage of sensitive data such as Protected Health Information (PHI) using data leak prevention capabilities in Chrome OS and Chrome Browser
- Prohibit malware transfers and lateral movements via sanctioned applications
- Block users from visiting phishing URLs embedded in emails or application content

These capabilities provide authenticated users with an end-to-end secure environment for accessing privileged resources with minimal performance impact.

Chrome Browser's role in BeyondCorp Enterprise

Chrome Browser extends zero trust security to the web. Technologies like Safe Browsing, Site Isolation, and sandboxing make Chrome a secure browser for all enterprises. Chrome's fast and automatic updates help ensure users are on the most secure version. But with BeyondCorp Enterprise, Chrome provides you with additional enterprise-grade defenses against external threats from malicious actors, mistakes from careless users, and internal threats around sensitive data and exfiltration leaks.

Because users spend so much of their workday getting things done in their web browser, Chrome should be seen as an integral part of an organization's zero trust security model (figure 1).

With Chrome's browser-based threat detection and data protection capabilities as part of your zero trust strategy, you can:

Create an inventory of devices running Chrome Browser and Chrome OS that access your organization's data. Device inventory Endpoint Verification provides valuable information that you can use to maintain security. When paired with context-aware access offerings, Endpoint Verification helps enforce fine-grained access control.

Protect company data in real time by preventing users from being phished. Combining Google's latest intelligence on malicious sites with enterprise real-time URL scanning through Safe Browsing, you can ensure users aren't attempting to visit known malicious sites (figure 2).

Stop suspicious files in real time before they exploit your network. Chrome provides real-time file scanning and analysis right within Google Cloud (figure 3).

You can configure whether the user can access the file ahead of analysis or wait until the file has been fully vetted. Chrome also supports three-stage malware detection through reputation-based detection, static analysis, and advanced cloud sandboxing.

Prevent both accidental and intentional exfiltration of company data. Data leak prevention leverages preconfigured and customized rules to block actions or notify the user when uploads across websites go against corporate policy. This is particularly valuable for organizations that interact with customer information that's protected under regulatory compliance measures (figure 4).

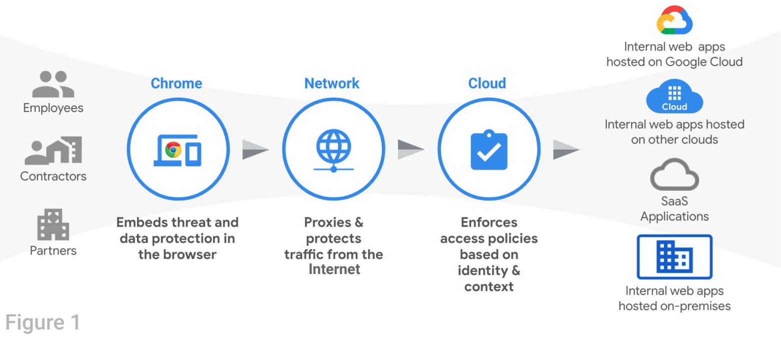
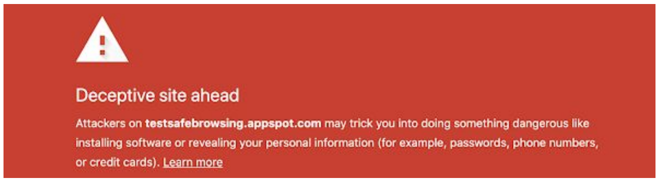

Employees
Contractors
Partners
Chrome
Embeds threat and data protection in the browser
Network
Proxies & protects traffic from the Internet
Cloud
Enforces access policies based on identity & context
Internal web apps hosted on Google Cloud
Cloud
Internal web apps hosted on other clouds
SaaS Applications
Internal web apps hosted on-premises

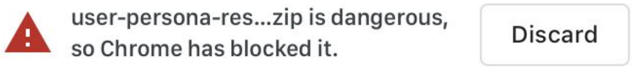
Figure 1



Deceptive site ahead

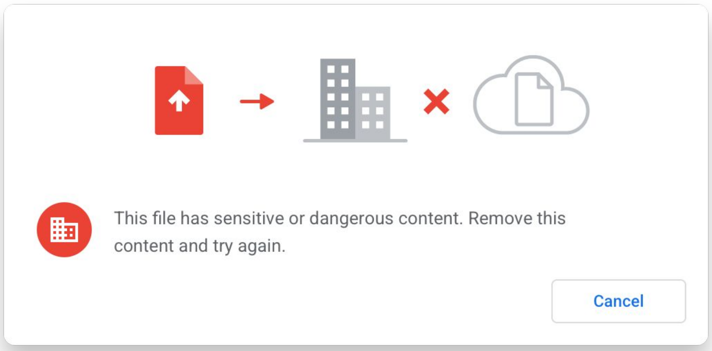
Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

Figure 2



user-persona-res...zip is dangerous, so Chrome has blocked it.

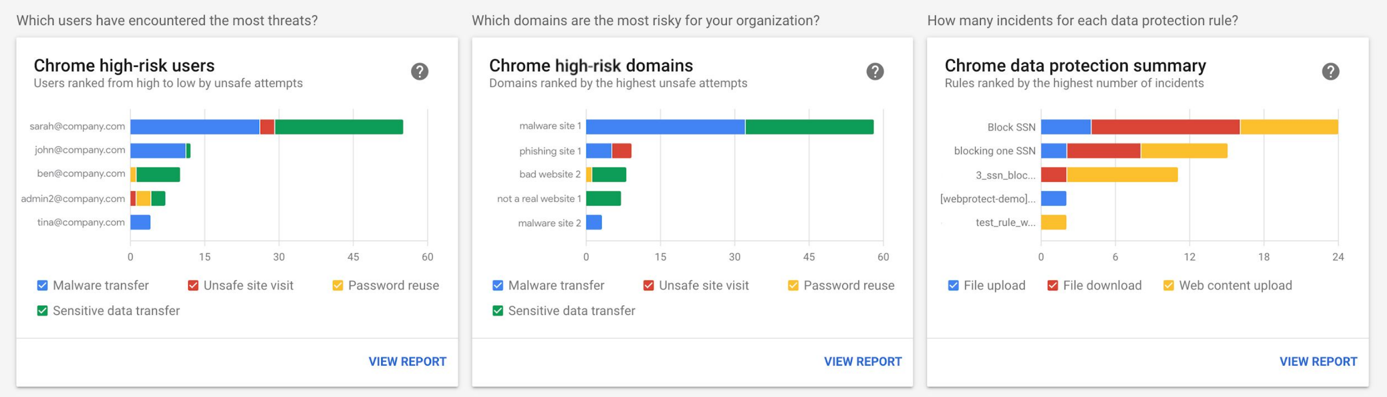
Figure 3



This file has sensitive or dangerous content. Remove this content and try again.

Figure 4

Generate alerts, logs, and reports of unsafe activity. IT teams can support their security and compliance initiatives by getting additional insights into security events around suspicious downloads, URLs, password re-use, and potential data leaks. They can also identify high-risk behaviors and users based on this information.


Which users have encountered the most threats?

Chrome high-risk users

Users ranked from high to low by unsafe attempts

Which domains are the most risky for your organization?

Chrome high-risk domains

Domains ranked by the highest unsafe attempts

How many incidents for each data protection rule?

Chrome data protection summary

Rules ranked by the highest number of incidents

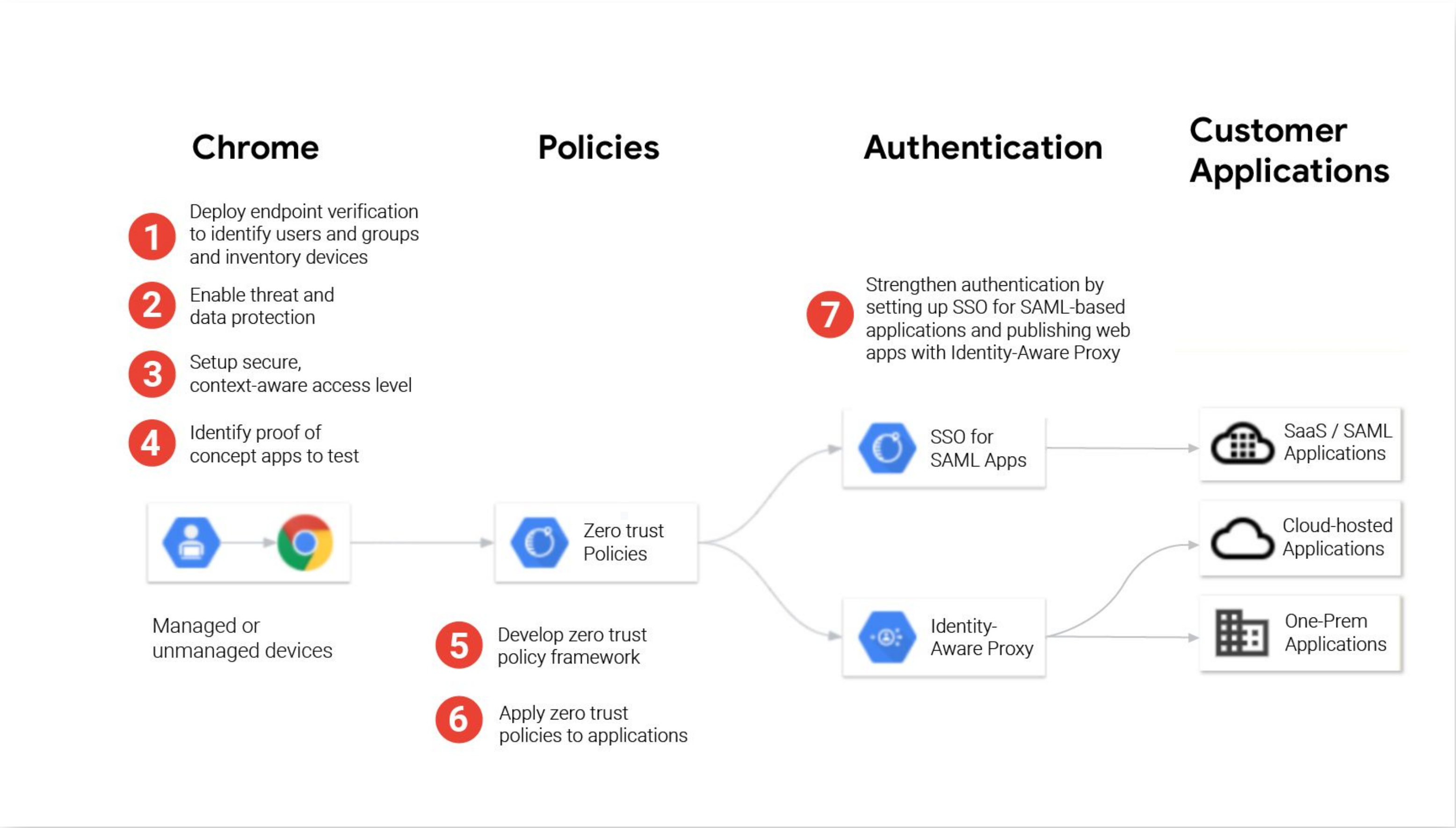
Enhancing Zero Trust Security with Chrome OS

In addition to taking advantage of advanced threat and data protections in Chrome Browser, you can also further extend your security with Chrome OS. A secure-by-design operating system, Chrome OS is a critical enabler to zero trust security models.

When combined with Chrome Browser and BeyondCorp Enterprise, Chrome OS offers organizations the ability to mitigate risks from the hardware level, to internal and external apps, all the way through to the open web.

Migrating to BeyondCorp Enterprise

Migrating every network user and every application to the BeyondCorp Enterprise zero trust framework is a continuous journey. By taking a phased migration approach, you reduce risks to business continuity and increase the opportunity to move large groups of network users to BeyondCorp Enterprise with no effect on their productivity.



Chrome

Policies

Authentication

Customer Applications

1 Deploy endpoint verification to identify users and groups and inventory devices

2 Enable threat and data protection

3 Setup secure, context-aware access level

4 Identify proof of concept apps to test

5 Develop zero trust policy framework

6 Apply zero trust policies to applications

7 Strengthen authentication by setting up SSO for SAML-based applications and publishing web apps with Identity-Aware Proxy

Managed or unmanaged devices

Zero trust Policies

SSO for SAML Apps

Identity-Aware Proxy

SaaS / SAML Applications

Cloud-hosted Applications

One-Prem Applications

Conclusion

Chrome Enterprise and BeyondCorp Enterprise support organizations working towards a zero trust security framework. Traditional, perimeter-based security models are no longer effective in today's world, especially with the increase of remote work. Organizations with a distributed workforce need the ability to grant access to business-critical applications and services, yet may struggle to do this in a simple and secure manner.

With BeyondCorp Enterprise, users benefit from additional threat and data protection services available in Chrome, giving organizations an added layer of security by protecting against phishing, malware, and data loss, and gaining visibility into unsafe activity.

To learn more about BeyondCorp Enterprise, visit g.co/cloud/bce.

Resources

To deepen your understanding of Chrome Browser, Chrome OS, Chrome Enterprise, and BeyondCorp Enterprise, consider the following resources:

Chrome Browser

- Chrome Browser downloads for your enterprise
- Learn more about Chrome Browser Enterprise Support
- Read the latest Chrome Browser Enterprise Release Notes
- Stay up to date on the latest Chrome Browser release updates via the Chrome Releases blog
- Explore Google's official Safety & Security blog
- Visit the Chrome Browser Enterprise Help Center and Chrome Browser Help Forum
- Explore Chrome Browser Cloud Management options
- Read the Google Chrome Privacy Notice
- Read the Google Chrome Privacy Whitepaper

Chrome OS

- Learn more about Google's cloud-first operating system
- Visit the Chromium Blog

Chrome Enterprise

- Discover more about how Google Chrome Enterprise unlocks the business capabilities of Chrome OS, Chrome Browser, and Chrome devices
- Visit the Chrome Enterprise blog

BeyondCorp Enterprise

- Read more about BeyondCorp Enterprise
- Visit the BeyondCorp Enterprise blog