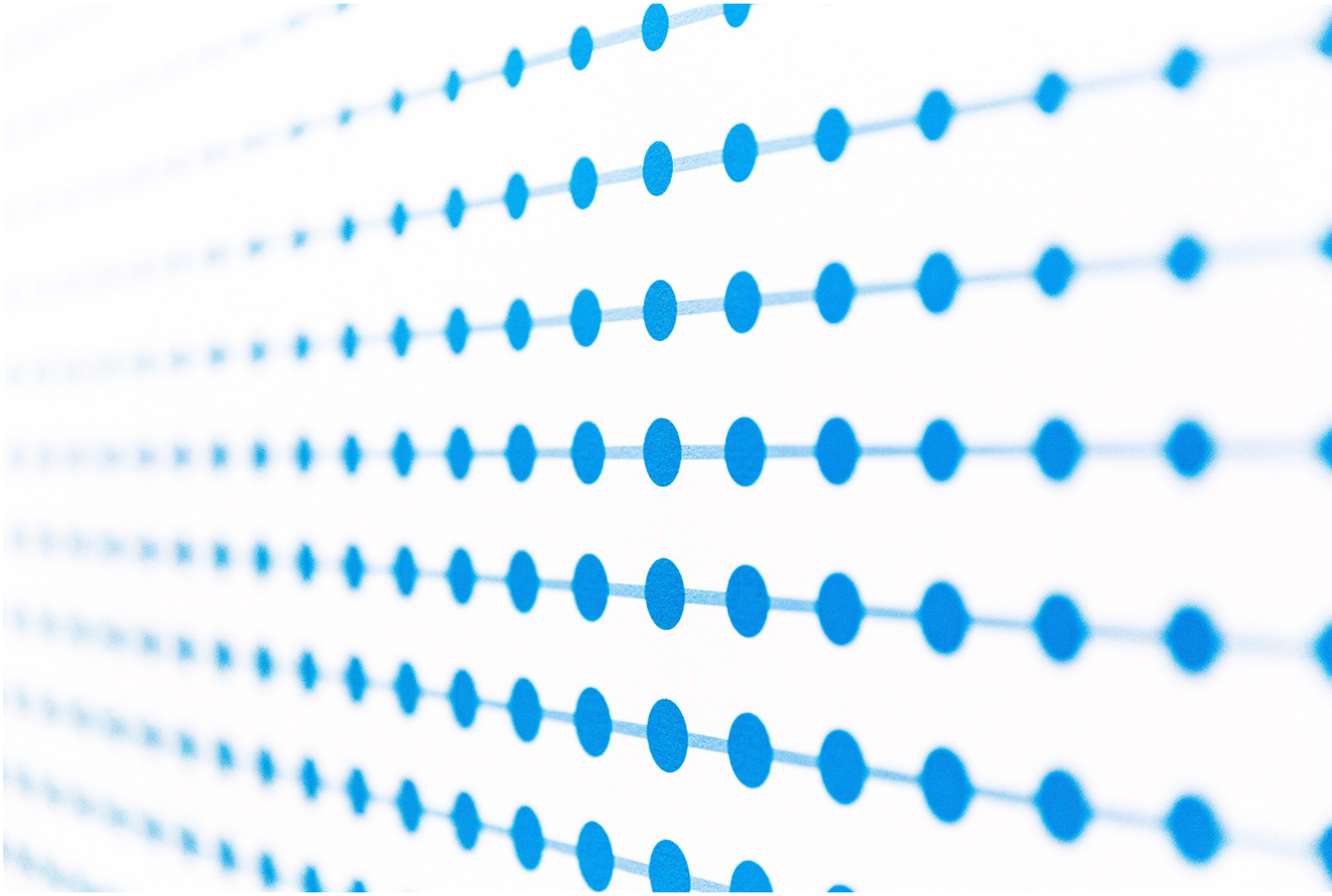
Google Cloud Whitepaper
February 2021

Secure access to SaaS applications with BeyondCorp Enterprise



Google Cloud

Table of contents

Table of contents **1**
Disclaimer 1
Introduction **2**
Use cases **3**
Govern zero trust access to sanctioned SaaS applications 3
Protect access to SaaS applications with two-step verification 4
Prevent leakage of sensitive data from SaaS applications 5
Prevent cross-site information theft by untrustworthy websites 6
Detect and prevent SaaS application password leakage and reuse 7
Prevent visits to phishing URLs embedded in emails or application content 8
Prevent malware transfers and lateral movements via sanctioned applications 9
Capture and monitor unsafe or login activities for forensic investigations 10
Conclusion **11**
Get started **11**

Disclaimer

This whitepaper applies to Google Cloud Platform products described at cloud.google.com. The content contained herein is correct as of February 2021 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

As a result of the COVID-19 pandemic, 74% of companies plan to permanently shift to more remote work. Keeping users safe and ensuring they have appropriate access to data in a time when remote work has become the new normal is becoming more important than ever for enterprise IT leaders. With employees at the average enterprise using upwards of 400 SaaS applications - or possibly as many as 1,800 shadow IT SaaS applications, IT and security administrators are faced with a growing landscape to protect. In fact, in a recent study, 84% of IT leaders said data loss prevention is more challenging when employees work from home.

By combining our best security technologies into a zero trust offering, Google can help enable an organization's workforce to access SaaS applications simply, safely, and securely, from virtually any device, over any network, without fear of threats such as malware, phishing, or data loss.

BeyondCorp Enterprise, Google's zero trust product offering, provides simple and secure access to applications and cloud resources and offers integrated threat and data protection, including critical security capabilities which allow users to:

- Govern access to SAML-based applications based factors such as device and user trust
- Prevent intentional or accidental data leakage when accessing applications and data
- Prevent untrustworthy websites from stealing corporate information
- Prevent credential leakage to phishing sites or unsanctioned applications
- Prevent malware transfer via SaaS applications
- Block lateral movement across the network by containing security to the application

These capabilities are fully integrated with the Chrome Browser and do not require additional agents or SSL-breaking proxies.

Use cases

Enterprise IT leaders are looking for solutions that can protect their employees and extended workforce accessing SaaS applications, whether they are sanctioned or unsanctioned. Below we have outlined some of the critical SaaS application use cases supported by BeyondCorp Enterprise.

Govern zero trust access to sanctioned SaaS applications

A foundational principle of Google's own zero trust implementation, BeyondCorp, is access to services is granted based on what we know about the user and the device. This means that the level of trust assigned to a single user and/or a single device is dynamically inferred from various attributes including user identity, user group, hardware, software, policies, integrity, location, and other similar criteria.

Google's context-aware access capabilities give you granular control over access to your SaaS applications, including Google Workspace, and other popular SaaS apps such as Salesforce or Box. Employees and the extended workforce, including contractors and vendors, can access SAML-enabled applications if attributes such as user identity, location, device security status, and IP address meet the rules and standards set according to the access policies created.

For example, you can use context-aware access policies when you want to do things such as:

- Allow access to apps only from company-issued devices.
- Allow access to Drive only if a user storage device is encrypted.
- Restrict access to apps from outside the corporate network.

You can also combine multiple criteria into one policy. For example, you could create an access policy that requires devices to be company-owned, encrypted, and meet a minimum OS version, in order to access certain applications.

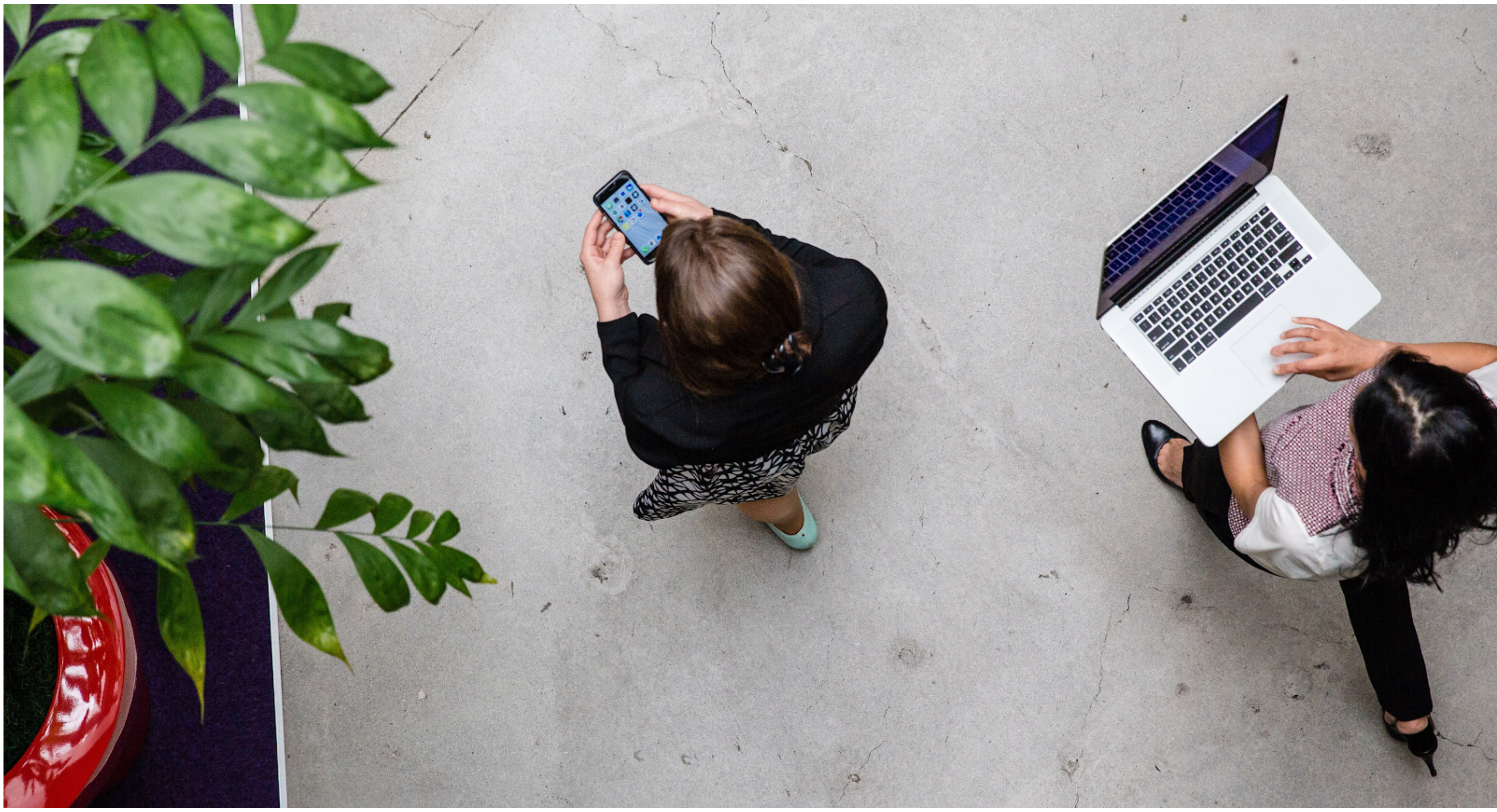
Protect access to SaaS applications with two-step verification

All SaaS applications can be protected with 2-Step Verification (2SV), which puts an extra barrier between your organization and cybercriminals who try to steal usernames and passwords to access sensitive data. Turning on 2-Step Verification is the single most important action you can take to protect your business. Administrators can enable 2SV as a requirement for their workforce to access certain SaaS apps.

Google's 2SV capability supports multiple verification methods, including:

- Security keys - The most secure form of 2SV is a hardware security key (we recommend keys from full service enterprise hardware providers such as Yubico) or your phone's built-in security key. Security Keys are a great way to protect against phishing threats.
- Google prompt - Users can set up their Android or Apple mobile devices to receive a sign-in prompt, and then tap a notification on their phone to confirm their identity.
- Verification code generators - Users generate one-time verification codes on a hardware token or through an app such as Google Authenticator on their mobile device. The user then enters the code to sign in to their computer and other devices.
- Text message or phone call - Google sends a 2-Step Verification code to mobile devices via text message or voice call.
- Backup codes - If a user doesn't have their mobile device or works in an area where they can't carry mobile devices, they can generate backup verification codes in advance.

In addition to enabling 2SV for access to SaaS applications, administrators can also set up context-aware access levels that require a specific level of authentication strength before allowing access to certain applications. For example, in order to access certain financial applications, administrators can set up a context-aware policy to require the user be authenticated with a hardware security key before access is granted.



Prevent leakage of sensitive data from SaaS applications

Protecting sensitive personal information, such as Protected Health Information (PHI) or Personally Identifiable Information (PII), is extremely critical, not only for our customers, but also for their end users. For example, laws such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) provide requirements for the processing of personal data.

Whether your data live on-premises or in the cloud, by embedding Cloud Data Loss Prevention (DLP) capabilities directly within the Chrome Browser, BeyondCorp Enterprise can provide better control of sensitive personal information as it transfers across endpoint devices and applications. The DLP integration gives users control over which data can be shared, including sensitive data which may be uploaded or downloaded, or content that is copied, pasted, dragged or dropped. Administrators can also set policies to block actions using sensitive information, such as Social Security numbers or credit card numbers.

Google's BeyondCorp Enterprise data protection capabilities include:

- Protection at file upload, download and content paste
- Real-time alerts per protection rule
- Audit, warning, and blocking actions
- Support for different file formats, including documents, image file types, compress/archived files, and custom types
- Hundreds of built-in sensitive data detectors, as well as custom regex and lists
- Implementation of conditions such as URL filters and full content inspection

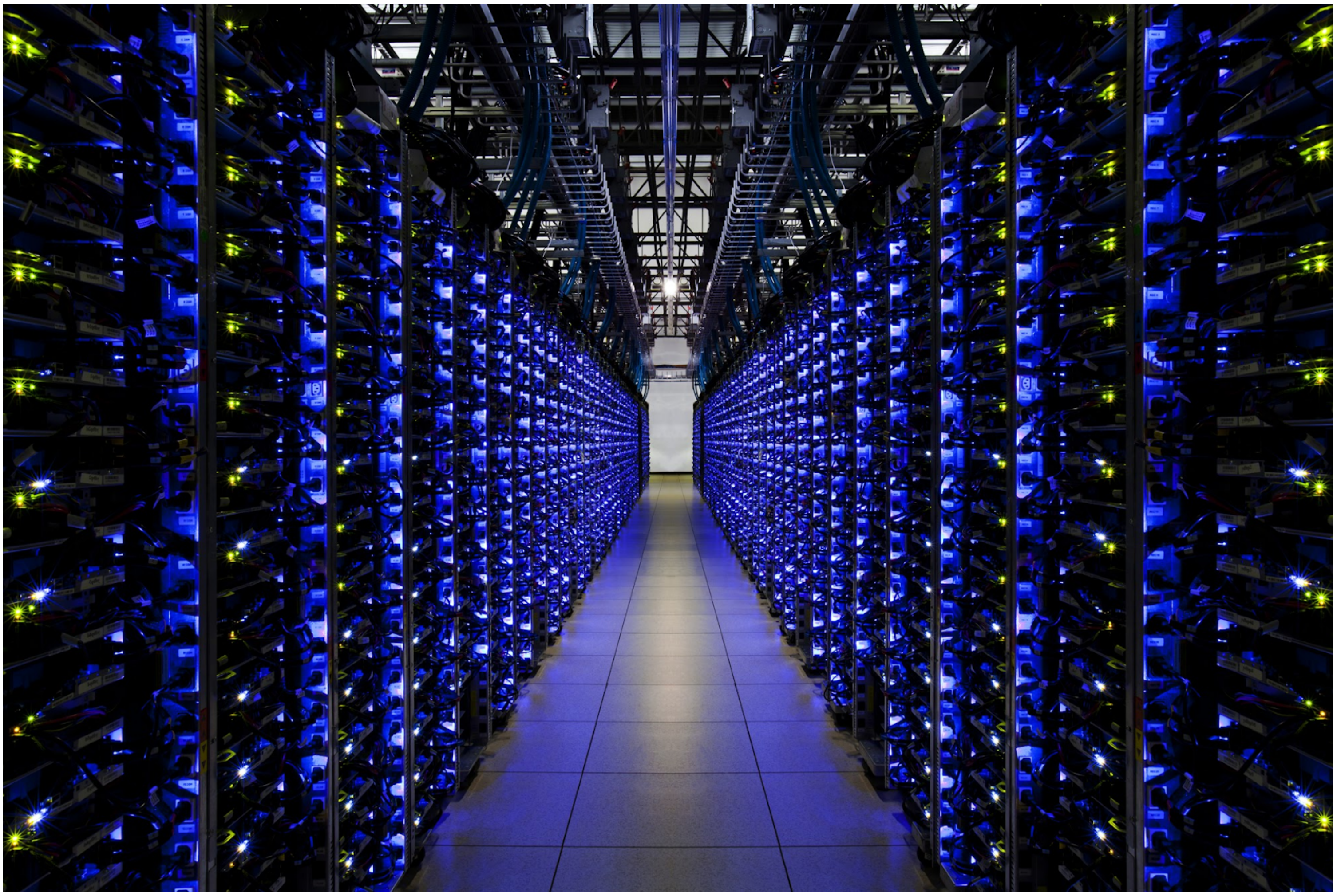
Prevent cross-site information theft by untrustworthy websites

Our modern, agentless approach leverages the Chrome browser and its many security features. For instance, Chrome's site isolation, a security feature on-by-default and available to all Chrome users, is designed to thwart untrustworthy websites from accessing or stealing information from websites and SaaS applications accessed through the browser by separating pages from different websites. In combination with same-origin policy, which protects sites from one another, this feature offers a multi-layered defense to make such attacks less likely to succeed.

Site isolation ensures that pages from different websites are always put into different processes, each running in a sandbox that limits what the process is allowed to do. It also makes it possible to block the transfer of certain types of sensitive data from other sites. As a result, a malicious website will find it much more difficult to steal data from other sites, even if it can break some of the rules in its own process.

This protection is made possible by the following behavior in the Chrome browser:

- Cross-site documents are always put into a different process, whether the navigation is in the current tab, a new tab, or an iframe (i.e., one web page embedded inside another).
- Cross-site data (specifically HTML, XML, JSON, and PDF files) is not delivered to a web page's process unless the server says it should be allowed (using cross-origin resource sharing (CORS)).
- Security checks in the browser process can detect and terminate a misbehaving renderer process.



Detect and prevent SaaS application password leakage and reuse

Use of stolen credentials is one of the first tactics employed during many attacks. As a security administrator, you need to ensure that employees and contractors are not using previously leaked credentials and are not accidentally entering their corporate SaaS passwords into dangerous websites that aren't authorized by your organization.

When users sign in to specific pages, Chrome can perform two specific actions. First, Chrome checks the entered username and password, in a privacy-preserving manner, against Google's database of leaked credentials. Users are warned if their entered credentials have been publicly leaked.

Second, Chrome generates a password fingerprint or hash, and shortens it to 37 bits, which is enough to identify the password if it's reused on dangerous or disallowed websites. Chrome then encrypts the partial hash using the OS-level username, if available. When users use the saved passwords on phishing websites or websites outside of the authorized list, Chrome displays a warning to users and prompts them to change their password. In addition, you can prompt users to change their password if they enter it on a website that you don't allow.

By stopping these two attack vectors, BeyondCorp Enterprise can protect your organization from compromised accounts and ensure your users are accessing sensitive information inside a secure environment.

Prevent visits to phishing URLs embedded in emails or application content

Phishing is the number one action taken during the first step of malicious attacks, and it's also the top social engineering tactic. According to the 2020 Verizon Data Breach Investigations Report, phishing, social attacks, and use of stolen credentials are used in 67% or more of breaches. Therefore, it is paramount that IT administrators ensure users are not visiting unsafe URLs that are embedded in emails or shared within SaaS applications.

Google's Safe Browsing technology protects billions of devices worldwide from unsafe URL visits, making it one of the largest threat intelligence databases. It also continuously crawls the Internet and websites to analyze and identify new phishing or malicious sites, and updates the database in real-time when unsafe sites are identified.

BeyondCorp Enterprise leverages this threat intelligence database and lists of unsafe web resources to provide real-time safety checks to determine whether the URL is a malicious or phishing URL, and whether the site contains deceptive content or malware.

Prevent malware transfers and lateral movements via sanctioned applications

The use of malware or ransomware is usually the number one action taken in the second step of malicious attacks (the first step is usually phishing or use of stolen credentials). Malware is also used in 17% of successful breaches, according to the 2020 Verizon Data Breach Investigations Report.

It is imperative for IT and security administrators to ensure any SaaS protection solutions can inspect, detect and block malware and ransomware in all files uploaded or downloaded. This will minimize the opportunity for users to get infected or spread malware accidentally.

BeyondCorp Enterprise employs a multi-stage malware prevention architecture and includes:

1. Reputation check - checks the safety of the website where the files are downloaded using URL reputation and signature matching
2. Static analysis - checks the signature as well as the file content against multiple signature databases and libraries of binary string static analysis rules
3. Cloud sandboxing - uses advanced technologies to detonate files in cloud sandboxes to observe malicious or suspicious behaviors such as file encryption activities

These malware protection capabilities support Windows executables, documents (e.g. PDFs, Office .docs), and archive files, and work on all major desktop operating systems, including Windows, Mac, Linux and ChromeOS.

Capture and monitor unsafe or login activities for forensic investigations

Visibility of unsafe user activities is one of the most critical aspects of security programs. You can't control what you can't see.

As such, BeyondCorp Enterprise provides detailed audit logs for security administrators to monitor, review, and analyze user activities and behaviors. These audit logs include:

- Context-aware access audit logs, which keep track of all denied user access requests to applications so administrators can troubleshoot and determine the root cause.
- Threat and data protection audit logs, which provide detailed audit trails of all unsafe activities such as malware transfer, unsafe site visits, sensitive data transfer, password reuse or changes, and content not scanned.
- Data protection rules audit logs, which track users' attempts to share, download, upload or paste sensitive data.
- Login audit logs, which track user login events such as successful and failed logins, leaked passwords, and suspicious logins.
- Devices audit logs, which report activities on computers and mobile devices that are used to access your organization's data, including device security posture information and password policy violations.

In addition, security administrators can leverage the security center investigation tool to report, aggregate, filter and sort collected security events. Administrators can use pre-built reports or create their own. The pre-built reports include:

- Chrome threat protection summary - Provides a high level overview of all the threat categories as well as various counts. The goal is to provide analysts and executives a quick glance of the overall threat landscape.
- Chrome data protection summary - Provides a high level overview of the DLP incidents and the number of incidents for the top five data protection rules, staggered by triggered action.
- High risk users - Provides an overview of users who have encountered the highest number of unsafe Chrome-related events.
- High risk domains - Provides an overview of the domains that are most risky for the organization, ranked by the number of unsafe attempts.

Finally, as many organizations use a centralized security information and event management (SIEM) solution for a consolidated view of incidents, Google provides different ways to export security events for additional analysis:

- Exports API that allows admins to retrieve a list of activities for a specific customer's account for the above audit logs.
- BigQuery export that allows admins to export specific audit logs to Google Cloud BigQuery tables on a daily basis.

Conclusion

Google's BeyondCorp Enterprise solution provides enterprises with zero trust security, combining Google's best security technologies, including context-aware access, data protection, website isolation, and malware, phishing and ransomware prevention, to provide your employees and extended workforce with an end-to-end secure environment for accessing SaaS applications.

Get started

The complete solution reflected in the use cases we've outlined requires BeyondCorp Enterprise, Google Workspace Enterprise Standard or Plus (or Cloud Identity Premium), and Chrome (browser and/or Chrome OS).

To learn more about using BeyondCorp Enterprise to manage access to SaaS applications on Google Cloud, hosted in other clouds, or on-premises, as well as how to define and enforce access policies based on user, device, and other contextual factors, please visit the product documentation.

To get started today, take these steps or contact us to speak with someone from our team.