Technical Validation

Google BeyondCorp Enterprise

Providing Simple and Secure Access to Applications and Cloud Resources with a Zero Trust Approach

By Jack Poller, Senior Analyst; and Tony Palmer, Senior Validation Analyst

August 2021

This ESG Technical Validation was commissioned by Google and is distributed under license from ESG.

Contents

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Executive Summary

In this Technical Validation, ESG evaluated the ability of BeyondCorp Enterprise (BCE)—a zero trust solution built on Google's global network—to provide customers with simple and secure access to applications and cloud resources with integrated threat and data protection.

BeyondCorp Enterprise provides continuous and real-time end-to-end protection, authenticating users and validating access to resources for every transaction. Leveraging Google's global network and Chrome browser, BCE provides access protection, threat and data protection, and application protection.

ESG validated that configuring BeyondCorp Enterprise to provide secure access to on-premises, SaaS, and cloud applications was quick and easy. We could create granular user, group, and company access policies with conditions based on many different parameters such as locations, addresses, device state and configuration, and more. And we could apply these policies to both managed employee devices and unmanaged extended workforce devices.

BeyondCorp Enterprise leverages Google Cloud's built-in, customizable DLP facilities to identify and protect sensitive data. End-users can accomplish their jobs, accessing and viewing sensitive data, and BCE can block downloading to prevent the exfiltration of sensitive data. BCE also leverages Google's global network and threat prevention features built into the Chrome browser to stop phishing attacks, malicious websites, and downloads.

ESG validated that BeyondCorp Enterprise was simple and easy to use. Configuration of BCE is integrated into the Google Cloud admin console, and configuration changes were propagated throughout the environment in a matter of seconds. Likewise, end-users can securely access private web and SaaS applications without having to install VPNs or agents.

If your organization is looking for an agentless platform to enhance security and provide quick and simple, secure access to cloud and on premises applications, it would be smart move to take a serious look at Google BeyondCorp Enterprise.

Background

According to ESG research, 59% of organizations say that cybersecurity in general (i.e., knowledge, skills, management, operations, etc.) has become more difficult than it was two years ago. The primary factors responsible for the added difficulty include an expansion in the number of remote workers (cited by 41%), the expanding threat landscape (38%), the growth in the number of cloud applications (32%), and an increase in the number of mobile devices (31%).[1]

Zero trust approaches are arguably more relevant than ever as a strategy to address this difficulty. Whether implementing least-privilege tenets for user access or securing the connections to and between the disparate aspects of today's hybrid multi-cloud deployments, zero trust can provide a framework to secure even the most complex environments. The sudden shift to work-from-home models has only highlighted the importance of a zero trust approach.

While the majority (51%) of organizations view zero trust through the lens of cybersecurity modernization, reducing incidents, preventing breaches, and enabling secure remote access are the top priorities for implementing zero trust strategies (see Figure 1).[2]

[1] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2021.
[2] Ibid.

Figure 1. Most Important Business Drivers of Zero Trust Strategies

Source: Enterprise Strategy Group

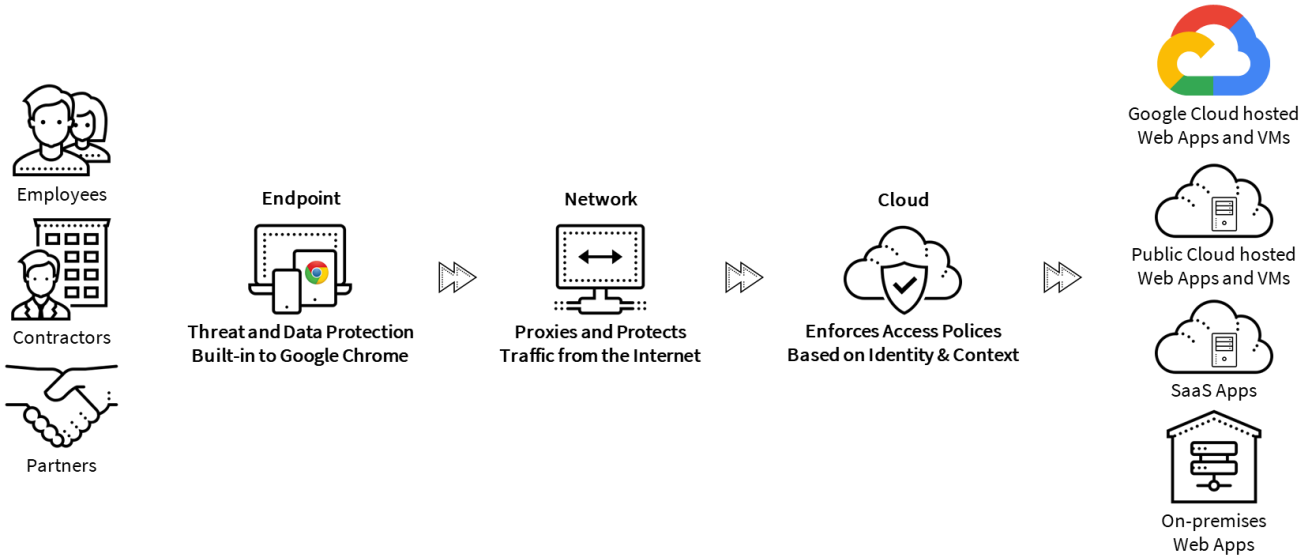
Google BeyondCorp Enterprise

Google has a long history with zero trust, stemming from its decade of work with BeyondCorp, Google's own implementation of a zero trust strategy, which shifted access controls from the network perimeter to individual users and devices and provided VPN-less secure access for the entire global Google workforce of more than 100,000 employees.

BeyondCorp Enterprise—a new solution from Google—builds on the knowledge, experience, and heritage Google has amassed to enable organizations to implement their own zero trust strategy. Leveraging Google's global network, BeyondCorp Enterprise (BCE) enables simple and secure access to applications and cloud resources and offers integrated threat and data protection.

BCE is a scalable zero trust platform based on a secure, agentless architecture (see Figure 2). The platform uses Google Chrome to provide secure, agentless endpoint access. Google's global network, with more than 140 edge locations in over 200 countries and territories and capable of absorbing the largest DDoS attacks, proxies and protects traffic from the internet. Google designed its cloud infrastructure with security and scale in mind, including verifiable platform security and a planet-scale identity management service. The cloud infrastructure enforces access policies based on identity and context.

Figure 2. Google BeyondCorp Enterprise



Source: Enterprise Strategy Group

BeyondCorp Enterprise provides continuous and real-time end-to-end protection, including:

- Access protection—with continuous authorization of every interaction between user and resource, phishing-resistant strong authentication (security keys), and pre- and post-login risk assessments.
- Threat and data protection—preventing malicious or unintentional data exfiltration loss, preventing malicious downloads, and warning users before visiting potentially unsafe URLs.
- Application protection—using application-based segmentation, built-in public SSL certificate management, global load balancing, and DDoS protection.

BCE can be deployed as a no-impact overlay to existing security architectures and can be rolled out in phases by targeting specific sets of users and applications, reducing legacy access and network controls as deployment increases.

ESG Technical Validation

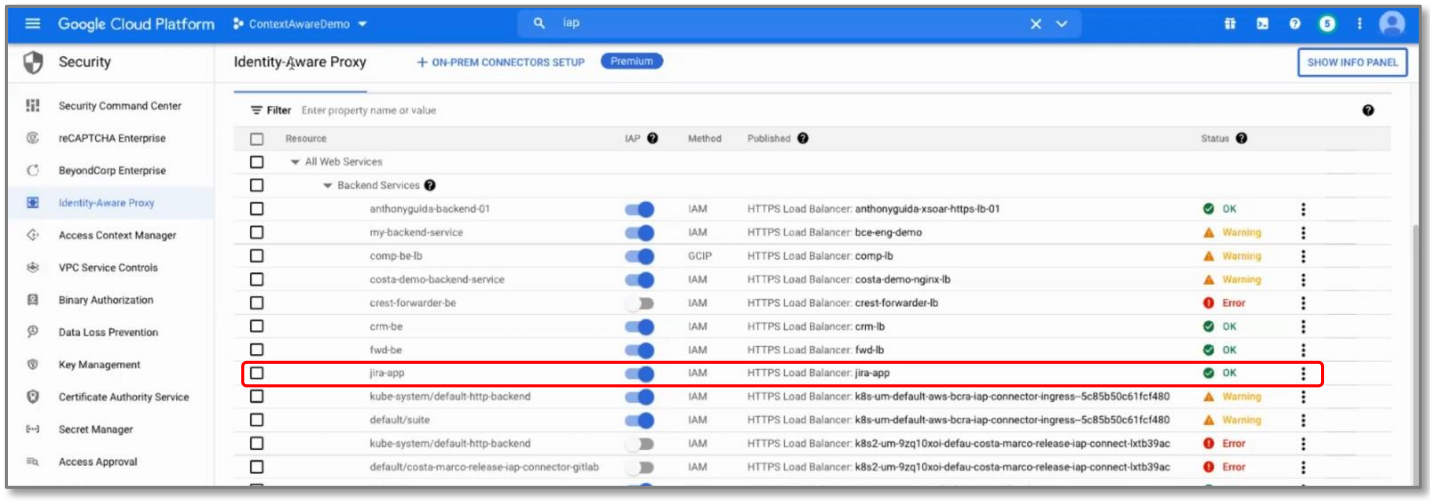
ESG validated the capabilities of BeyondCorp Enterprise through a series of demonstration sessions. The validation was designed to demonstrate how the BeyondCorp zero trust solution simplifies secure, policy-based access to resources for both end-users and administrators with integral threat and data protection.

Secure Access

Google designed BeyondCorp Enterprise to provide secure access to resources, including cloud applications hosted on GCP, AWS, and Azure; on-premises applications; SaaS applications; and VMs accessed via TCP/IP, SSH, and RDP. Administrators configure BCE through the GCP administrator console, creating and applying access and data policies.

Our validation began by logging in to the GCP administrator console in a demo environment. In the console, we selected ***Security,*** then ***Identity-Aware Proxy***, to get to the IAP console, as shown in Figure 3. The console presented a hierarchically organized filterable list of applications configured to use IAP. The list provided a simple on/off switch for IAP, the access method, published application, and status.

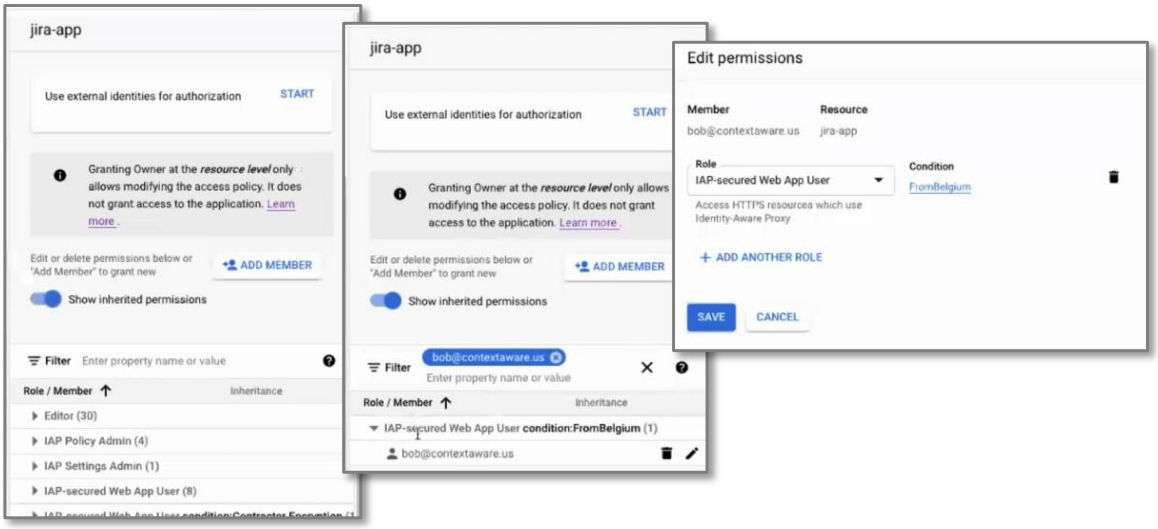
Figure 3. Identity-Aware Proxy Administrator Console



Source: Enterprise Strategy Group

We used the three-dot menu on the right-hand side of the interface to select and review the IAP configuration for the Jira application and the console displayed a filterable list of roles and members configured to use Jira. We searched for the demo user ***bob@contextaware.us*** and then clicked on the pencil icon to view Bob's permissions. We could see that Bob was authorized to use the Jira app with the condition ***FromBelgium***, as shown in Figure 4.

Figure 4. Editing Access Policies



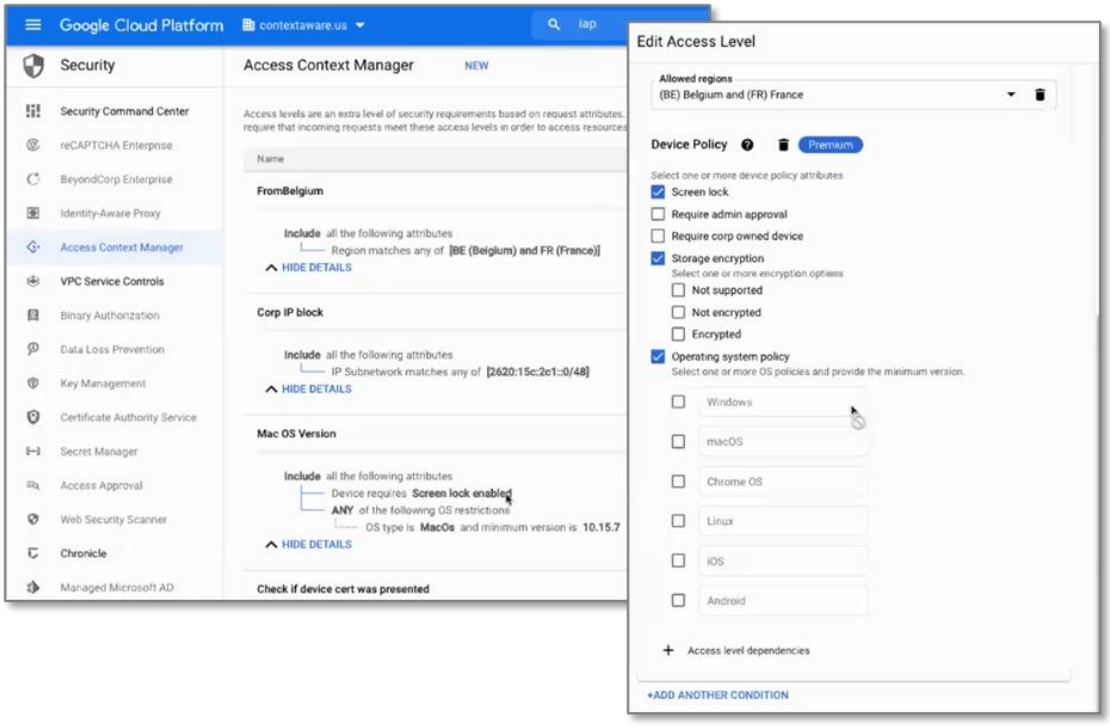
Source: Enterprise Strategy Group

Next, we reviewed the context policy FromBelgium. Clicking on the context policy name brought up the Access Context Manager, as shown in Figure 5, and we could see that the condition included the attribute ***Region matches any of [BE (Belgium) and FR (France)]***. We also observed additional context rules such as ***Corp IP block***, which required matching an IP address, and ***Mac OS Version***, which required that the endpoint had screen lock enabled and was using MacOS with a minimum version of 10.15.7.

We verified that when Bob met the criteria, he seamlessly was able to access Jira, and when we changed the policy such that Bob no longer met the criteria, his access to Jira was blocked.

We used the three-dot menu to edit the FromBelgium policy and observed additional device policy options such as admin approval requirement, corporate-owned devices, storage encryption, and other operating systems and versions. We observed that BCE provides granular policy options, enabling admins to customize policies based on their organization's needs and preferences. These policy changes were propagated throughout the environment in a matter of seconds, ensuring that admins can update their security to match rapidly changing requirements.

Figure 5. Access Context Policies



Source: Enterprise Strategy Group

Why This Matters

Digital transformation (DX) is continuing to accelerate—72% of organizations are currently implementing DX initiatives—and most organizations are now using on-premises, SaaS, and cloud applications. Likewise, the vast majority (93%) of organizations expect to maintain a hybrid on-premises and remote workforce for the foreseeable future.[3]

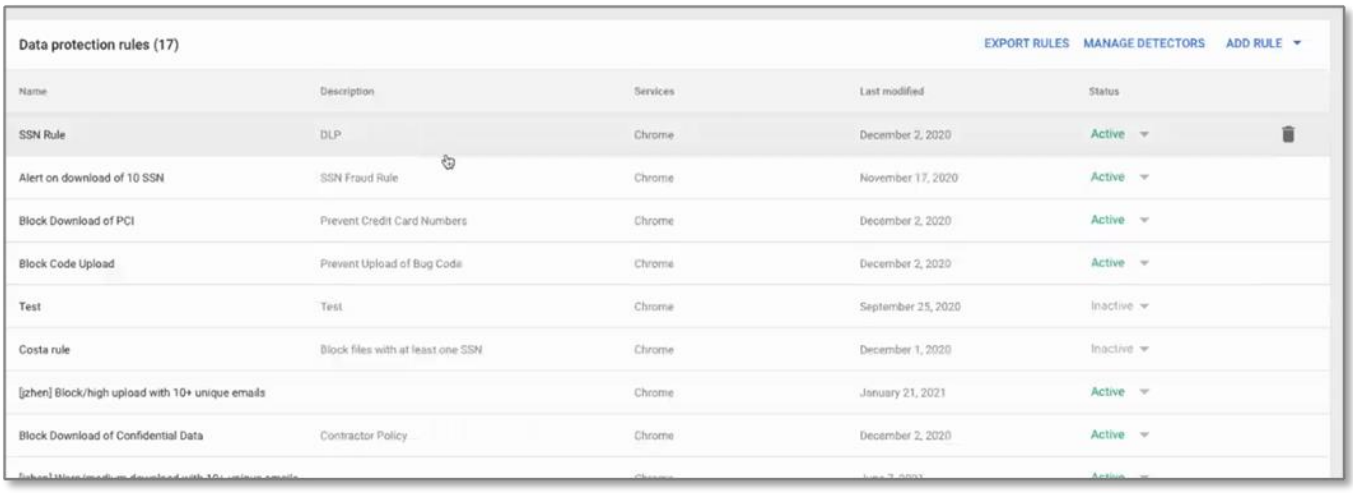
ESG validated that Google BeyondCorp Enterprise can provide secure access to on-premises, SaaS, and cloud applications. We found configuring identity-aware proxy access policies to be quick and easy. We could create granular policies specific to users, groups, and the entire organization. We could also create granular access conditions, ensuring access from specific locations with specific device parameters, including local security configurations such as device lock screens, local storage encryption, and minimum operating system versions. Using Google BeyondCorp Enterprise, we could support a remote workforce using employee-owned devices. Using the Identity-aware proxy, BCE validated every transaction between the user and the application, continuously ensuring secure access to corporate applications.

[3] Source: ESG Master Survey Results: *2021 Technology Spending Intentions Survey*, December 2020.

Enhanced Security

BeyondCorp Enterprise leverages existing Google Cloud data loss prevention (DLP) and threat protection capabilities to enhance security. We navigated the GCP console menu to select data protection rules to review the configured DLP policies, as shown in Figure 6.

Figure 6. Data Protection Policies



Source: Enterprise Strategy Group

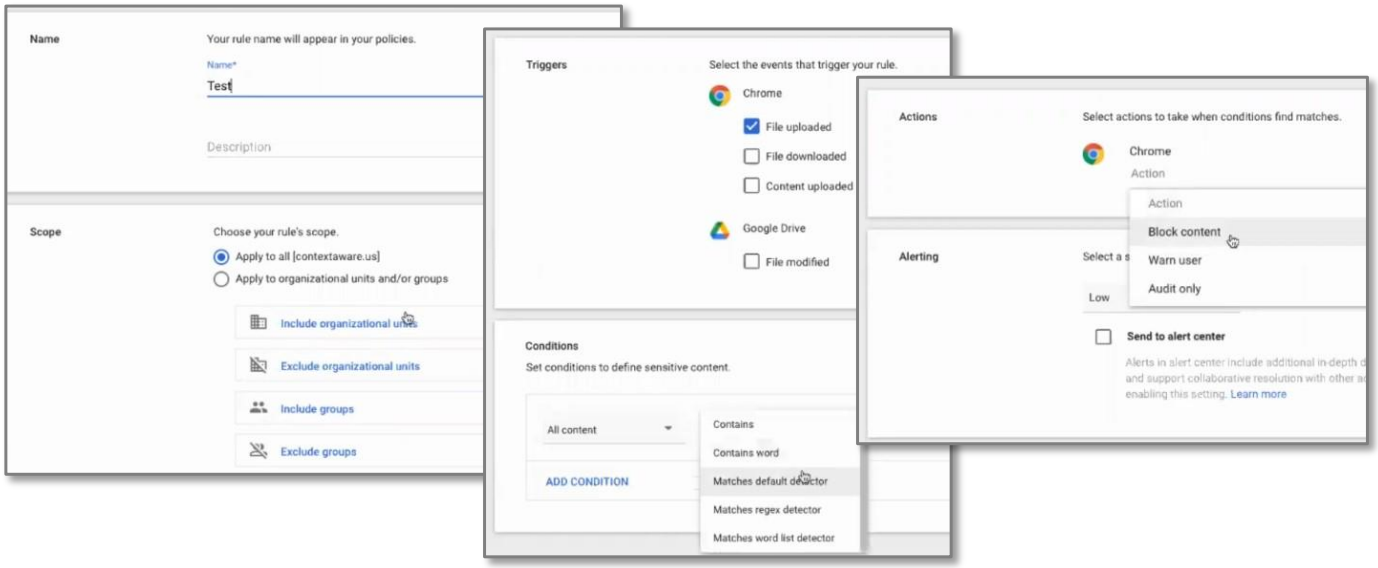
As with the access policies, DLP policies are easily customizable. We selected ***ADD RULE*** to create our own DLP policy. As shown in Figure 7, the rule creation wizard guided us through specifying the rule name and scope, rule triggers, conditions, actions, and alerting mechanisms. GCP's data protection engine provided us with granular scoping, and we could apply the rule to the entire organization or limit the rule to specific users and groups.

We could trigger DLP checking on file upload, file download, content upload, or Google Drive file modification. Thus, GCP enabled us to ensure that we could prevent inadvertent or malicious data infiltration and exfiltration.

Next, we specified the conditions that define sensitive data. We could leverage Google's built-in data detectors, including detectors for country- or region-specific sensitive data types such as US Social Security numbers, as well as globally applicable data types such as names, telephone numbers, email addresses, and credit card numbers. We could also create our own detectors.

Next, we specified the action to take when a detector finds sensitive data. We could block the content, warn the user, or create an audit log entry. We could also create an alert when a detector finds sensitive data.

Figure 7. Creating DLP Policies



Source: Enterprise Strategy Group

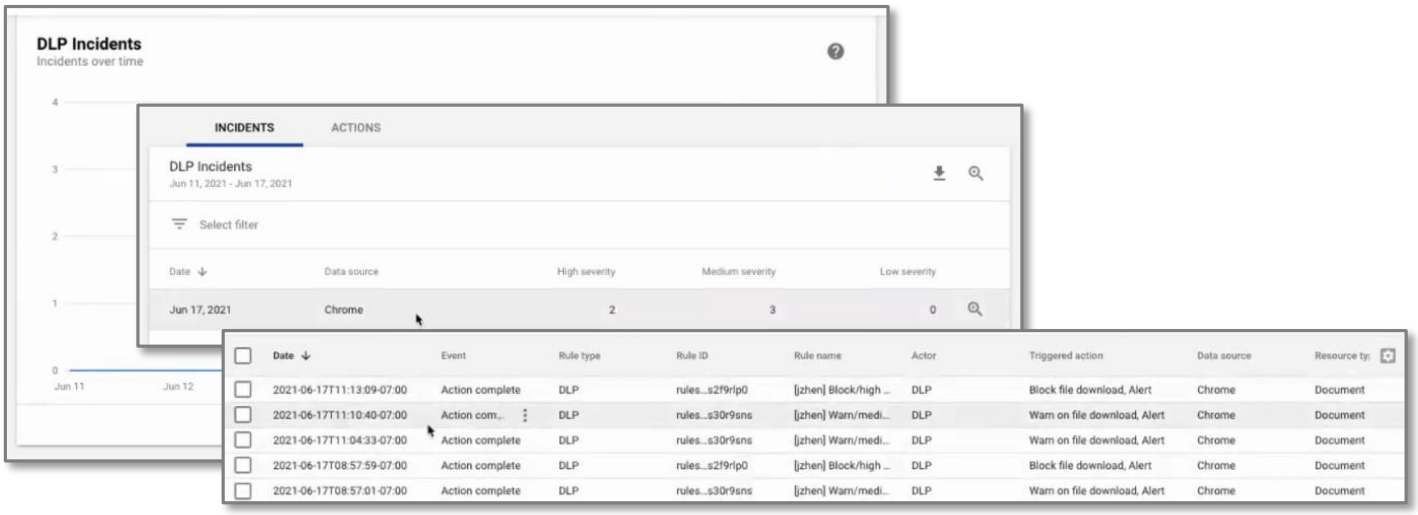
Next, we switched to the end-user view and had Bob open the Dropbox application and view a file in the cloud storage. Although this file contained sensitive data, we could use Dropbox's built-in file viewer to view the contents of the file. However, when we clicked on download, the DLP detector triggered and blocked the download, as seen by the end-user and shown in Figure 8.

Figure 8. Data Access Policy Enforcement

Source: Enterprise Strategy Group

Next, we switched to the GCP Security Dashboard for admins to view DLP incidents, as shown in Figure 9. The admin dashboard provided a graph and list of incidents over time, and we could click to drill down for more information.

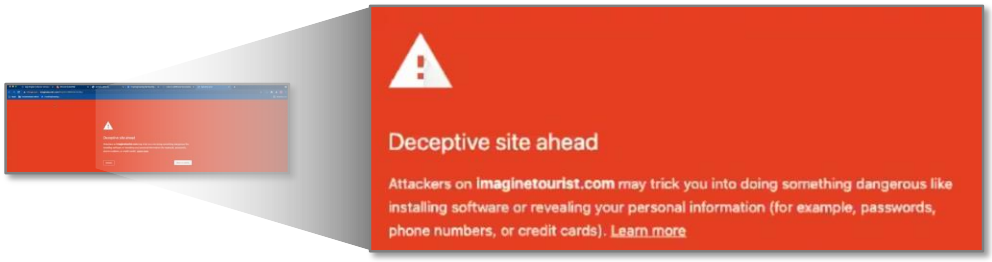
Figure 9. Data Access Policy Incidents



Source: Enterprise Strategy Group

We then went back to Bob and clicked on a link in the Dropbox file. While it appeared that the link was directing us to an internal website, the link redirected us to an external website. Google's Safe Browsing feature detected that the destination URL was a malicious site and provided an obvious warning to the end-user, as shown in Figure 10. BCE leverages Google Safe Browsing and Google threat protection capabilities to protect users from phishing, malicious downloads, and other common threats and attacks.

Figure 10. Threat Protection



Source: Enterprise Strategy Group

Why This Matters

While the aphorism that "you can't protect what you don't know" is still true, with ever-increasing volumes of data, it's almost impossible to identify every piece of sensitive data created and stored by the organization. So how can an organization identify and protect its sensitive data?

ESG validated that BCE leverages GCP's built-in DLP facilities to define the characteristics of sensitive data, such as social security numbers, credit card numbers, and more. Users can view sensitive data while BCE blocks downloading, protecting the organization from data exfiltration. We also validated that BCE uses Google's threat prevention features to stop phishing attacks, malicious websites, and downloads.

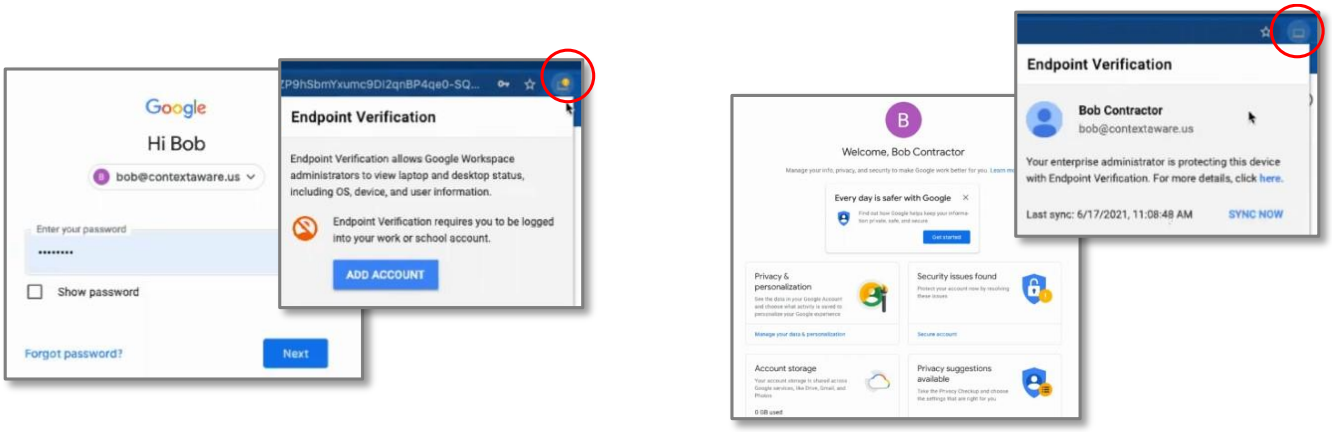
Simplicity and Ease of Use

Google BeyondCorp Enterprise is an agentless solution and leverages Google's Chrome browser to provide end-users with secure access to private web and SaaS applications. BCE and Chrome ensure continuous authorization of every interaction between user and resource, and this protection works for both employees using managed devices and the extended workforce using unmanaged devices. A simple Chrome extension enables the end-user to verify the endpoint and BCE device security status and provides device information to BCE. ESG started by logging in to a new Chrome browser session.

As shown in Figure 11, before logging in, the BCE verification plugin icon in the Chrome browser bar was highlighted with a yellow warning exclamation point. We clicked on the plug-in icon, which displayed a popup that noted the system was not providing endpoint verification.

Next, we logged in as bob@contextaware.us, and the plugin icon changed to remove the warning. Again, we clicked on the icon, and the plugin displayed the message, "Your enterprise administrator is protecting this device with Endpoint Verification," with a link to information about protected profiles. Chrome uses protected profiles to deploy policies and protections to users, ensuring unmanaged devices receive the same access, threat, and data protection as managed devices. Profiles also enable users to keep their bookmarks, history, passwords, and other settings separate from other users.

Figure 11. Chrome-based Access

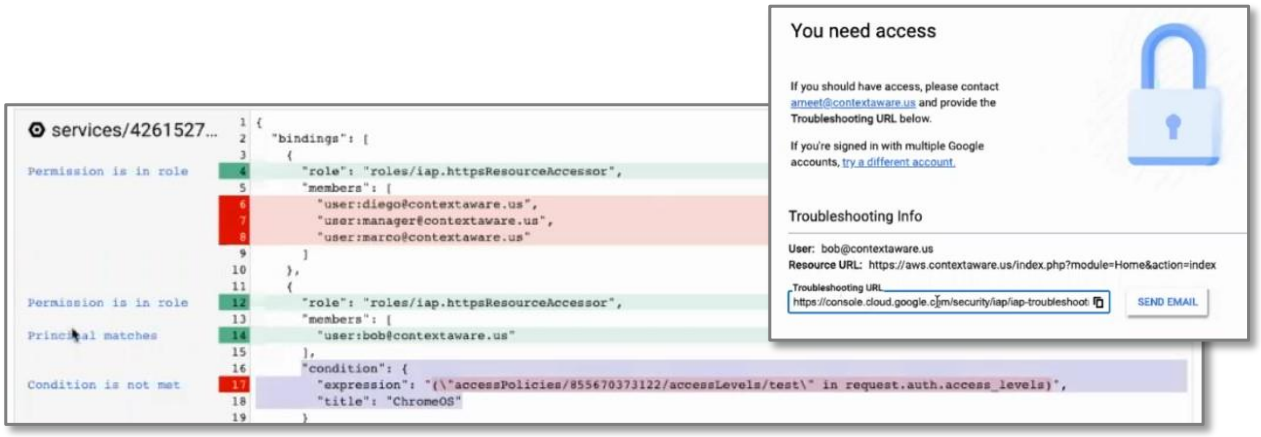


Source: Enterprise Strategy Group

Next, we navigated to Jira. As shown in Figure 12, BCE applied the previously configured access policy (user located in Belgium or France, matching a specific corporate IP address block, and using MacOS 10.15.7 or later) and denied access to the user. BCE provided instructions on how to troubleshoot the denial, including an option to send a link to the administrator to help the admin investigate the issue.

Logging in to GCP as an administrator, we clicked on the troubleshooting link and observed that the access was denied because the user didn't meet the condition that the user's OS was ChromeOS.

Figure 12. Access Denials

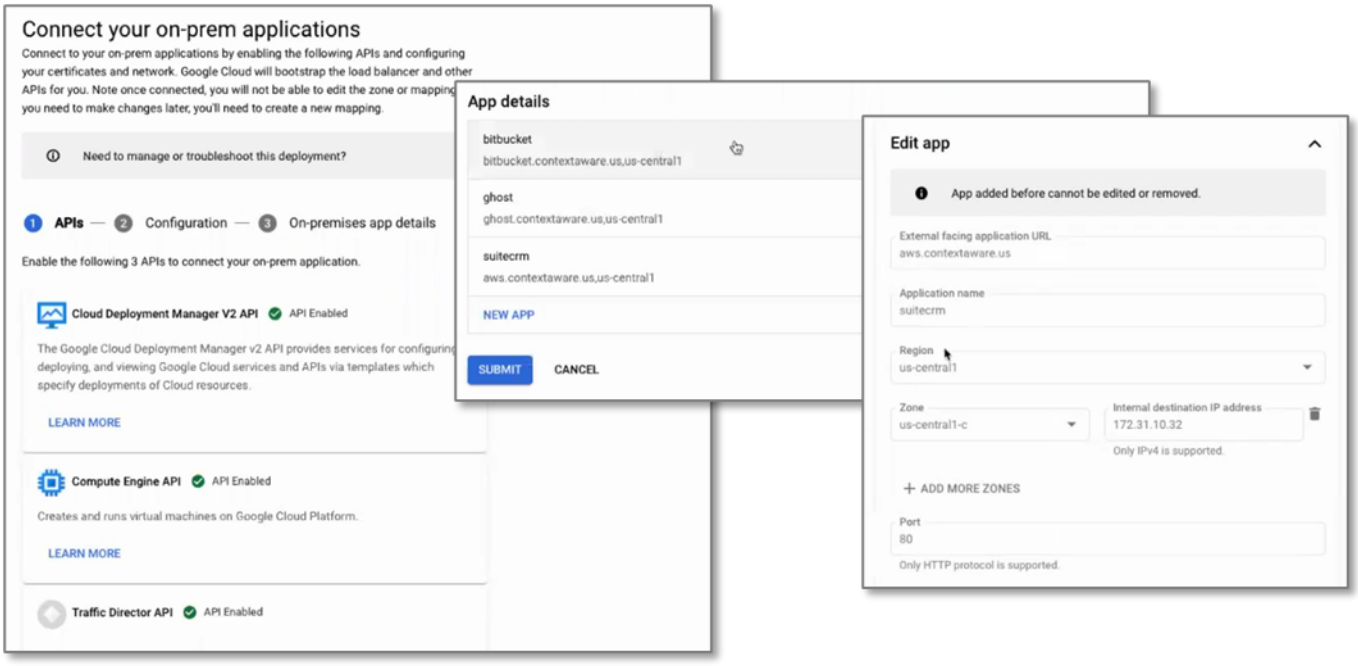


Source: Enterprise Strategy Group

Configuring BCE to Provide Secure Access to Applications

From the GCP admin console, we selected Identity-Aware Proxy to configure BCE to secure access to an application. As shown in Figure 13, we first ensured that three APIs (Cloud Deployment Manager, Compute Engine, and Traffic Director) were enabled. We clicked on ***NEW APP***, and provided the app region, zone, IP address, and port, and we then enabled IAP. In addition to externally hosted apps, BCE can protect any GCP-hosted app—all that is required is to have a load balancer in front of the app and then enable IAP.

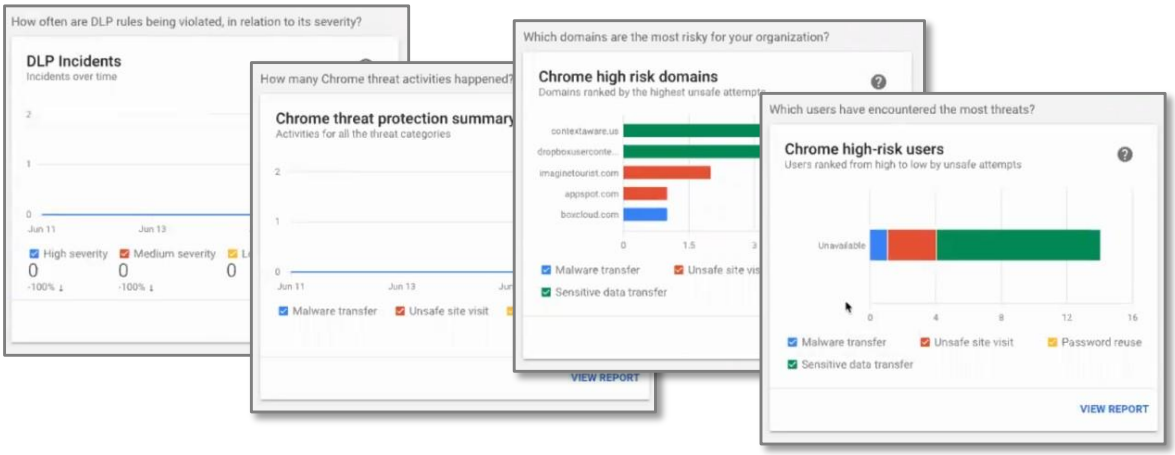
Figure 13. Configuring BCE to Provide Secure Access to Applications



Source: Enterprise Strategy Group

As a last step, we switched to the GCP Security Dashboard. As shown in Figure 14, the dashboard includes several charts related to BCE, including DLP incidents and Chrome threat protection. The live charts show graphs of events over time. Clicking on ***VIEW REPORT*** brings up more details, and admins can pivot data to get a better understanding of the current status and effectiveness of BCE in providing secure access to applications.

Figure 14. Security Dashboard



Source: Enterprise Strategy Group

Why This Matters

According to ESG research, three-quarters of organizations (75%) believe IT complexity has increased in the past two years. This complexity presents challenges to end-users, IT administrators, and security teams who must secure the plethora of devices and applications.[4]

ESG validated that Google BeyondCorp Enterprise provided easy-to-use secure agentless access to applications. To take advantage of integrated threat and data protection, Google recommends customers use the Chrome browser for the best experience of BCE. The Endpoint Verification extension is not required for access but is necessary for leveraging device information in policies.

ESG also validated that it was simple to configure BCE to provide secure access. All configuration is performed in the GCP console. Adding secure access controls to an application required a few clicks and the application's IP address and port. This simplicity reduces the administrative workload, freeing admins and architects to work on deploying zero trust throughout the organization.

The Bigger Truth

Though there is still not universal agreement as to exactly what zero trust means and how it should be implemented, zero trust has evolved to include a large number of cybersecurity disciplines. Regardless, nearly half (45%) of organizations rate their zero trust initiatives as very successful and claim benefits such as reduced security incidents (43%), better SOC efficiency (43%), fewer data breaches (41%), and higher user productivity (36%) and satisfaction (34%).[5]

Google BeyondCorp Enterprise can help organizations attain the benefits of zero trust strategies. Leveraging Google's threat protection, BCE can prevent phishing attacks and access to malicious websites, reducing security incidents. Google's DLP features can help organizations automatically identify and prevent the downloading of sensitive information, resulting in fewer data breaches. Furthermore, admins can incorporate signals from enterprise mobility management (EMM) and mobile device management (MDM) services into their access policies. Google has partnered with a number of technology

[4] Source: ESG Master Survey Results: *2021 Technology Spending Intentions Survey*, December 2020.
[5] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2021.

vendors as part of the BeyondCorp Alliance to provide an open and extensible ecosystem, ensuring organizations can leverage and integrate partner information to create stronger policies and enhance security.

For organizations that need to support more complex use cases, the BeyondCorp Enterprise product team is building more functionality to support legacy apps, and the roadmap has been designed to give organizations flexibility and options across their environment.

BCE's agentless approach using the Chrome browser simplifies the end-user experience. For the most part, zero trust access becomes invisible to the end-user, doing away with the need to install and run cumbersome VPN or other agent-based access solutions, leading to improved productivity and satisfaction. Likewise, BCE simplifies administrative workload by integrating configuration into the GCP console, improving IT and SOC efficiency.

Zero trust can be a significant undertaking, crossing multiple security disciplines spanning the technology stack, including the network, data, identity, endpoints, and operations and analytics. It follows then that the vast majority of organizations are using or interested in zero trust platforms. Of course, any organization should evaluate the needs of its environment before deciding on a zero trust platform. But if you want to accelerate your zero trust journey by using an agentless platform that can simply and quickly provide secure access to cloud and on-premises applications, ESG recommends that you consider the advantages of Google BeyondCorp Enterprise.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188