

Security & Identity

# Zero trust is a must: Supporting our customers with new BeyondCorp Enterprise features

August 20, 2021



**Jian Zhen**  
Group Product Manager

### Try Google Cloud

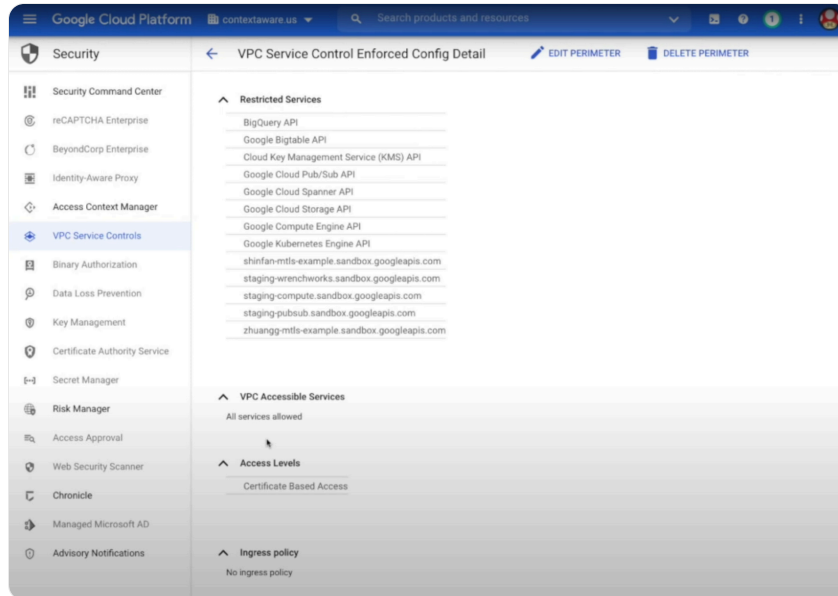
Start building on Google Cloud with \$300 in free credits and 20+ always free products.

Free trial

Since [launching](#) BeyondCorp Enterprise in January, our team has been busy working with customers to understand how they are using the product and what we can do to better support their needs as they continue on their zero trust journey. We believe zero trust is an effective way to enhance overall security and provide a better user experience and [BeyondCorp Enterprise](#) can help make this possible. Today, we're excited to announce three new BeyondCorp Enterprise features designed to help our customers provide their users simple and secure access to key applications.

## Certificate-based access via VPC-SC

First, [certificate-based access](#) for GCP APIs via [VPC Service Controls](#) (VPC-SC) is now generally available. Using bearer credentials to authenticate access to Cloud Console and Google Cloud APIs is nothing new, but if these credentials are accidentally exposed, they will invariably be found and used by attackers for illegitimate access. Using certificate-based access protects against credential theft or accidental exposure by only granting access when credentials plus a verified device certificate are presented. We now offer native support for client certificates for eight types of VPC-SC resources: GCE, GKE, PubSub, Spanner, Cloud KMS, GCS, BigQuery, and Logging, with more to follow. To begin leveraging certificate-based access for these APIs, visit our documentation [page](#) and get started.



## On-prem connector

Next, we are giving customers a choice for how they connect to on-premises resources with our On-prem connector, which is also now generally available. Customers can secure HTTP or HTTPS based on-premises applications (outside of Google Cloud) with Identity-Aware Proxy (IAP) by deploying a connector. When a request is made for an on-premises app, IAP authenticates and authorizes the user request and then routes the request to the connector. To deploy the connector for your on-premises applications, see our step-by-step guidance on the Identity-Aware Proxy documentation [page](#).

## Easy to configure custom access policies

Finally, we're excited to announce the availability of even more zero trust access conditions in [Access Context Manager](#), the zero trust policy engine behind BeyondCorp Enterprise. The ability to leverage new attributes gives administrators even more ways to build fine-grained access control policies to safeguard their applications and Google Cloud resources. Three new sets of attributes are now in public preview and customers can begin using these today:

- [Time and date](#)  
When evaluating zero trust access, it is often necessary to restrict user access to resources to particular days and time (e.g. shift workers or temporary employees). The time and date restriction is a feature for enterprise customers to enable access controls based on specific times, dates, and/or ranges.
- [Credential strength](#)  
Configuring two-step verification is an important action to prevent security breaches. By leveraging credential strength as another condition in access control policies, enterprises can enforce access controls based on the usage of hardware security keys or other forms of multi-factor authentication. BeyondCorp Enterprise now supports push notifications, SMS codes, 2SV software and hardware keys, one-time passwords, or a general use of any form of MFA.
- [Chrome Browser](#)  
To ensure that users are accessing resources from secure environments, administrators can set zero trust policies that ensure the user's browser environment has these threat and data protection capabilities turned on. The following are new access conditions that can be used in ACM's custom access levels: management state, minimum version, real-time URL checks enabled, file upload/download analysis enabled, bulk text (paste) analysis enabled, and security event reporting enabled.

## We're just getting started

We'll continue to make strides to help our customers. If you'd like to take a deeper look at BeyondCorp Enterprise, check out the [BeyondCorp Enterprise Technical Validation](#) report, recently released by the Enterprise Strategy Group. This report provides an assessment of the solution, stating: "ESG validated

that configuring BeyondCorp Enterprise to provide secure access to on-premises, SaaS, and cloud applications was quick and easy.”

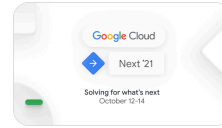
To learn more about these new features and the other exciting work we’re doing in the zero trust space, be sure to [register](#) for [Google Cloud Next '21](#). We have a great lineup of security sessions planned for you!

Google Cloud Next

## Registration is open for Google Cloud Next: October 12–14

Register now for Google Cloud Next on October 12–14, 2021

By Alison Wagonfeld • 1-minute read



Posted in [Security & Identity—Google Cloud](#)

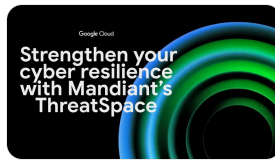
### Related articles



Security & Identity

**Cloud CISO Perspectives: 2025 in review: Cloud security basics and evolving AI**

By Nick Godfrey • 5-minute read



Security & Identity

**How Mandiant can help test and strengthen your cyber resilience**

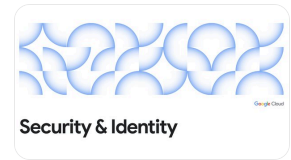
By Ilan Lanz • 3-minute read



Security & Identity

**Cloud CISO Perspectives: Our 2026 Cybersecurity Forecast report**

By Francis deSouza • 14-minute read



Security & Identity

**Expanding the Vision: Welcoming Palo Alto Networks to Google Unified Security Recommended**

By Chris Corde • 3-minute read

Follow us



[Google Cloud](#) [Google Cloud Products](#) [Privacy](#) [Terms](#)

[? Help](#)

[English](#) ▾