Google Cloud

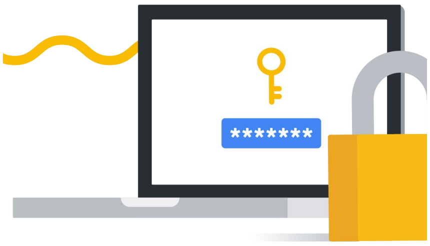
Zero Trust with BeyondCorp

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

BeyondCorp is Google's implementation of the zero trust security model that builds upon eight years of building zero trust networks at Google, combined with ideas and best practices from the community. By shifting access controls from the network perimeter to individual users and devices, BeyondCorp allows employees, contractors, and other users to work more securely from virtually any location without the need for a traditional VPN.

Secure Google.

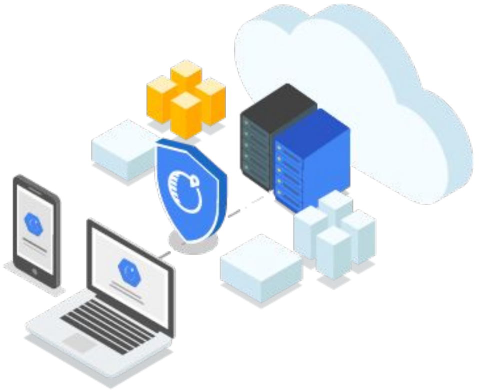
BeyondCorp began as an internal Google initiative to enable every employee to work from untrusted networks without the use of a VPN. BeyondCorp is used by most Googlers every day, to provide user- and device-based authentication and authorization for Google's core applications.



BeyondCorp for everyone

BeyondCorp can now be enabled at virtually any organization with Google Cloud's context-aware access solution, powered by Cloud Identity, Cloud Identity-Aware Proxy, Cloud IAM, and VPC Service Controls. Enterprise administrators can enforce granular access controls to web apps, VMs, APIs, and G Suite apps based on attributes like user identity, device security status, IP address, and more

Google Cloud



Context Aware Access

context-aware access allows enterprises to enforce granular access controls to web apps, VMs, GCP APIs, and G Suite apps based on a user's identity and context of the request without the need for a traditional VPN. It enables the ability to provide a simpler access for your users, enforce granular controls, and use a single platform for both your cloud and on-premises applications and infrastructure resources.

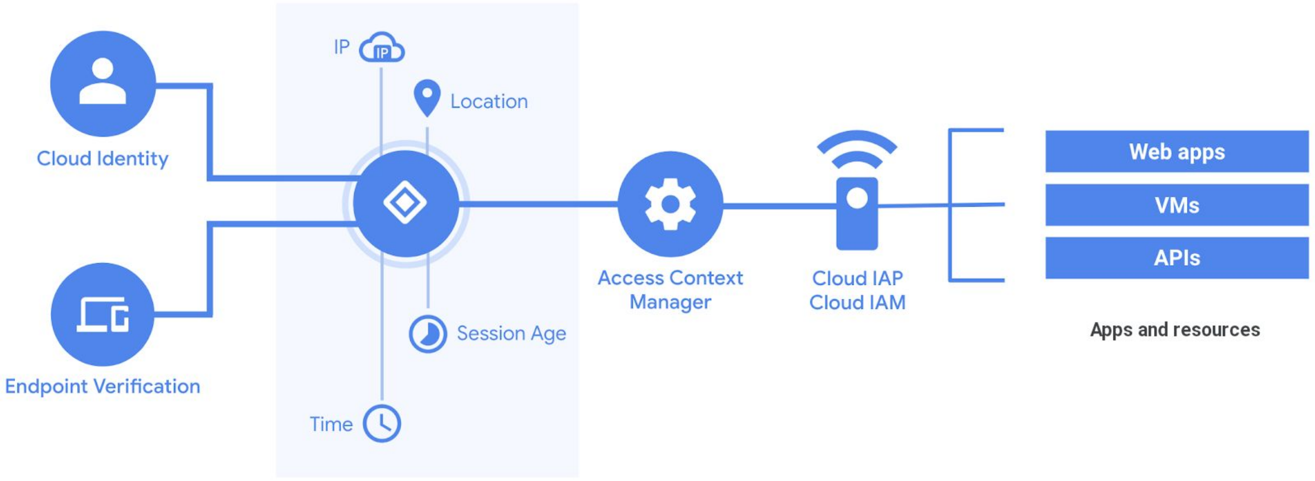
Cloud Identity-Aware Proxy

Cloud Identity-Aware Proxy (Cloud IAP) controls access to your cloud applications and VMs running on Google Cloud Platform (GCP). Cloud IAP works by verifying user identity and context of the request to determine if a user should be allowed to access an application or a VM. Cloud IAP is a building block toward BeyondCorp, an enterprise security model that enables every employee to work from untrusted networks without the use of a VPN.

Cloud Identity

A unified identity, access, app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency, protect company data, and transition to a digital workspace.

Cloud IAM lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage cloud resources centrally. For established enterprises with complex organizational structures, hundreds of workgroups, and potentially many more projects, Cloud IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes.



Virtual Private Cloud (VPC) Service Controls

VPC Service Controls allow users to define a security perimeter around Google Cloud Platform resources such as Cloud Storage buckets, Bigtable instances, and BigQuery datasets to constrain data within a VPC and help mitigate data exfiltration risks. With VPC Service Controls, enterprises can keep their sensitive data private as they take advantage of the fully managed storage and data processing capabilities of Google Cloud Platform.

Using VPC Service Controls and Private Google Access, enterprises can configure private communication between cloud resources from VPC networks that span cloud and on-premises hybrid deployments to keep sensitive data private. With a secure boundary in place, you can take advantage of fully managed Google Cloud Platform technologies like Cloud Storage, Bigtable, and BigQuery.

Zero Trust Security

Leverage the BeyondCorp security model to achieve a tighter, more granular control over who is accessing your apps and infrastructure, on-premises or in the cloud.

Unified Access Management

Control access to your apps, infrastructure, and APIs based on a user's identity and the context of the request.

Simplified User Access

Open up user access to applications and infrastructure from virtually any device, anywhere, without requiring a VPN.

> "The BeyondCorp vision is without question the future of enterprise IT. BeyondCorp is an enterprise security model that builds upon 6 years of building zero trust networks at Google, combined with best-of-breed ideas and practices from the community.
>
> Steve Pugh
> Ionic Security CISO and former White House Military Office CISO

Learn more about BeyondCorp at https://cloud.google.com/beyondcorp/