Google Cloud

BeyondCorp Remote Access

Enable Secure Remote Access With A Modern Zero Trust Architecture

BeyondCorp Remote Access is a software as a service (SaaS) solution that enables responsive and easy-to-use access to internal web apps for employees and the extended workforce from virtually any device, anywhere using a web browser without a traditional VPN.

Business Challenge

Employees, now more than ever, require flexibility on when, where, and how they work. Providing remote access traditionally relied on legacy technologies such as VPNs which don't provide a good end-user experience or the flexibility that users require. Employers today need a solution that enables their employees to securely and efficiently work from the office, home, or anywhere.

Employee Satisfaction	Technical Enablement	COVID-19 Effect
80% of employees want to work from home at least some of the time	54% of HR leaders indicated that poor technology is the biggest barrier to effective remote working	8x increase in forecasted number of employees working from home multiple days per week post COVID-19

Solution Overview

BeyondCorp Remote Access (BCRA) was originally developed for internal Google use over 10 years ago to build a new Zero Trust Architecture (ZTA) that enables and enforces least privilege from the ground up. Google then took the lessons learned from deploying this technology internally to build BCRA that customers can now take advantage of today. BCRA is a Zero Trust Architecture that focuses on the user, device, and application versus the legacy network-based castle and moat approach which fails to deliver the needed security and user experience in an ever increasing mobile world.

BeyondCorp was created with 3 key principles:

- Connecting from a particular network must not determine which services you can access
- Access to services is granted based on what we know about you and your device
- All access to services must be authenticated, authorized, and encrypted

Using BCRA, organizations are able to provide secure access to SaaS applications, cloud applications (Google Cloud or other public cloud providers), or even on-premise web applications. BCRA enables organizations to quickly deploy remote access to existing applications, lower total cost of ownership, while maintaining strict control over data, device, application, and data access.

BeyondCorp Remote Access Solution

BeyondCorp Remote Access provides a flexible and dynamic solution that allows employees, contractors, and partners to access web applications regardless of where they are hosted easily and securely by leveraging Google's hyperscale Global Frontend to securely proxy the traffic and protect the web applications from the internet. *Figure 1* depicts how the user and application access works.

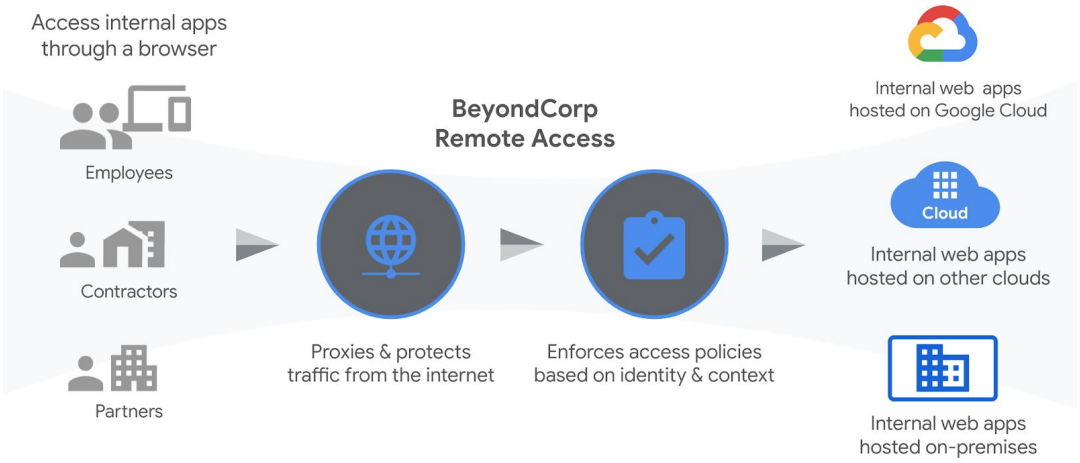

Figure 1. User and Application Access Workflow

There are four key components in a BeyondCorp Remote Access solution:

User and Devices

The first component is to identify users and their behavior (e.g. access patterns) and their device (e.g. employer owned, patched, etc). This telemetry information can help reduce lateral movement and insider threat risks.

Global Frontend

The Global Frontend provides built-in load balancing and acts as a security hardened reverse proxy keeping web apps highly available and secure.

Rules Engine

Both coarse and fine-grained rules can be created that dictate the who, where, and from what device can be granted access to specific resources ensuring that least privilege can be applied.

Enforcement Point

The enforcement point leverages network and user controls to validate and enable what resources a user/device has access to based on the results of the rules engine and enforcing only authorized access.

Figure 2 shows a high-level diagram on how each of these components fit together to provide a least-privileged secure remote access solution for users.

Sample Deployment of BeyondCorp Remote Access

The Google Front End (GFE) acts as the Global Frontend and provides DDoS mitigation, global load balancing, and TLS termination. The rules engine allows for global rules such as preventing low privileged devices (e.g. personal devices) from accessing high privileged information (e.g. PII/PHI data) that can be applied to all services and help reduce the risk with compromised credentials. Service-specific rules can also be created that for instance only allow a certain group of users (e.g. employees) to access a specific application (e.g. organization chart) or restrict the times when applications are available (e.g. only during business hours).

BeyondCorp Remote Access is able to be deployed on top of existing network infrastructure, identity management, and security controls. BCRA is then able to be rolled out on a per user group, per device, per application basis which allows organizations to initially focus on securing user access to mission critical applications first without impacting legacy infrastructure and other applications.

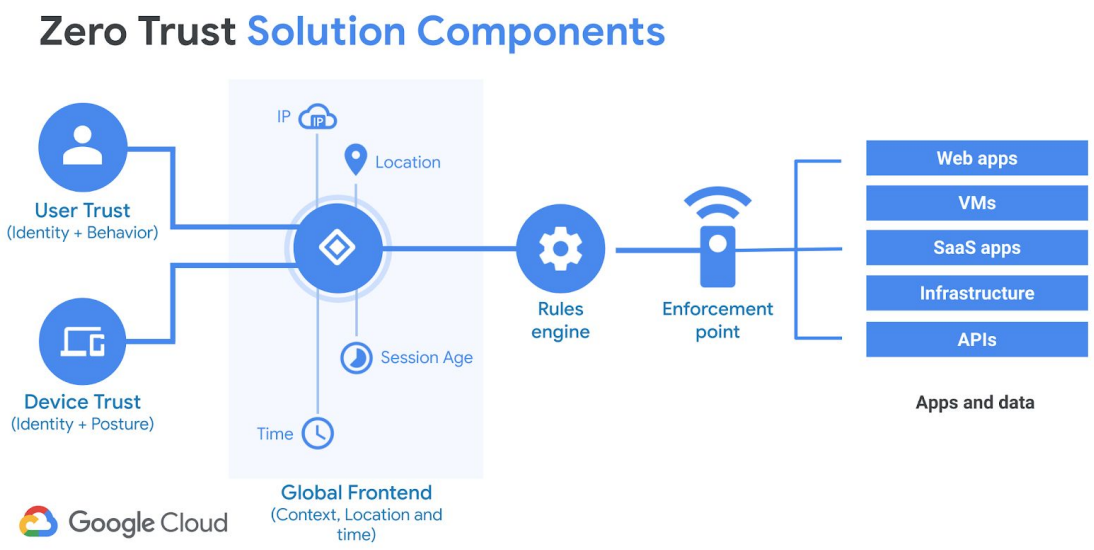

Figure 2. Zero Trust Solution Components

The BeyondCorp deployment model ensures that organizations are able to add additional security controls and empower users without doing an entire modernization effort all at once or requiring significant downtime to mission critical applications.

Deploy	Target	Reduce
No-impact overlay to your existing security architecture	Specific sets of users (highly privileged) and applications (high value) and expand as desired	Legacy access, network, and identity controls as deployment increases

Google Cloud Professional Services Offerings

Google Cloud's Professional Services Organization (PSO) is able to work directly with customers to help plan a deployment of BeyondCorp Remote Access, a software as a service (SaaS) solution enabling easy-to-use access to internal web apps for your employees and external workforce from virtually any device, anywhere, using a web browser.

Key activities

- **Deployment Planning**
  - Review and evaluate the current architecture and security configurations of your GCP environment to determine additional requirements for BeyondCorp Remote Access implementation.
- **Technical Design Creation**
  - Capture findings and develop a technical design document outlining how to implement your new remote access solution.

Deliverables

- **Technical Design** - Reference architecture and high-level design documents depicting the BeyondCorp Remote Access solution recommended by Google Professional Services
- **Hands-on Advisory Services -** Jumpstart for the customer's engineering team to accelerate the deployment journey

Engagement Details

- Prerequisites: A clear business use case for secure remote access for employees or contractors
- The timeframe for the engagement is dependent upon project scope and is agreed upon in the project charter or statement of work (SOW)
- The typical team consists of cloud consultants and subject matter experts (SMEs) with technical expertise based on solution components
- Work is performed offsite.
- Depending on the PSO and number of users, an initial BCRA deployment costs $250k-$750k

Let's connect to discuss how Google Cloud BeyondCorp can help your organization!

For more information visit https://cloud.google.com/solutions/government