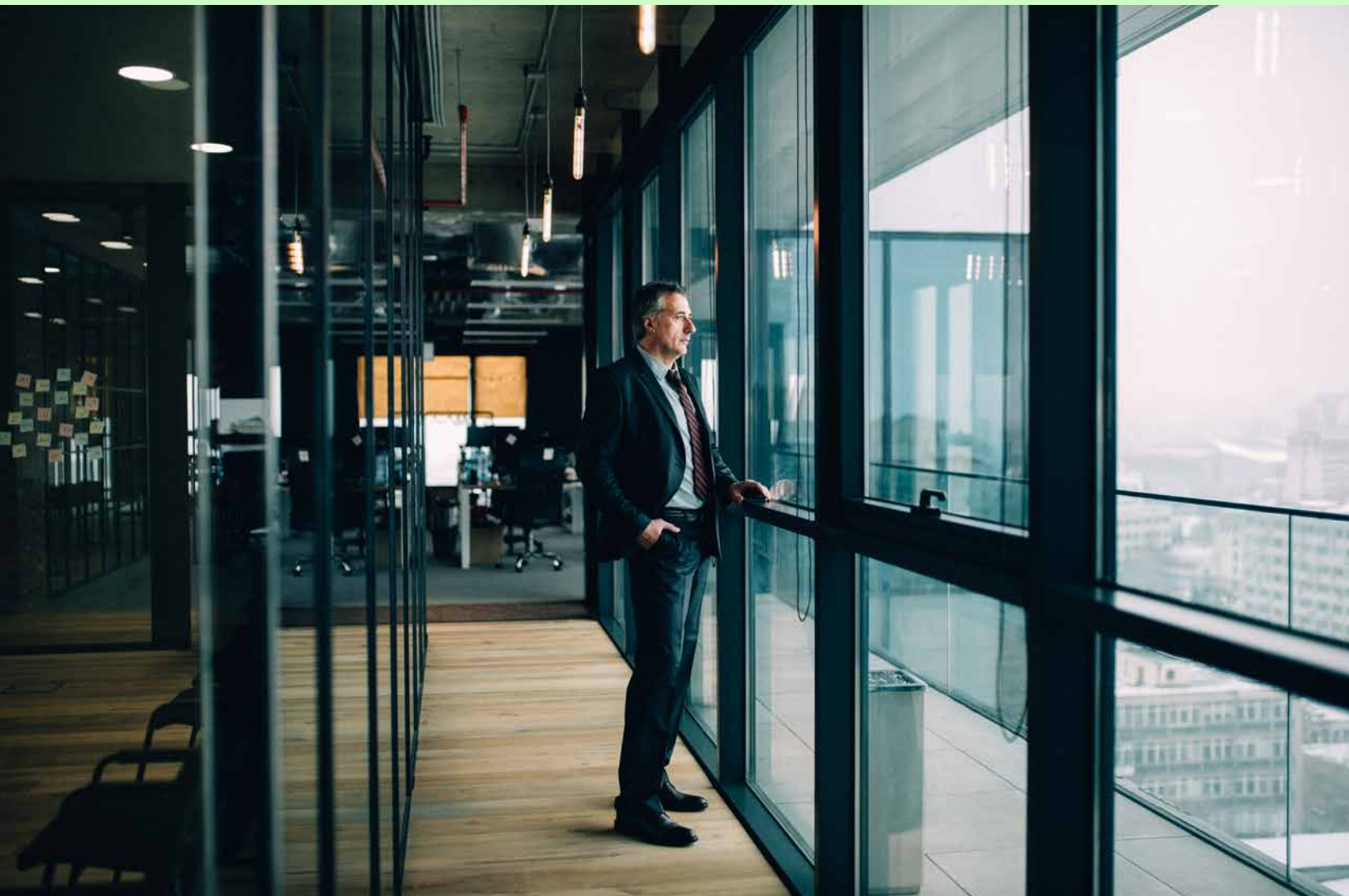
Solution Brief

Deliver workspace security and zero trust with Citrix and Google Cloud



About this solution brief

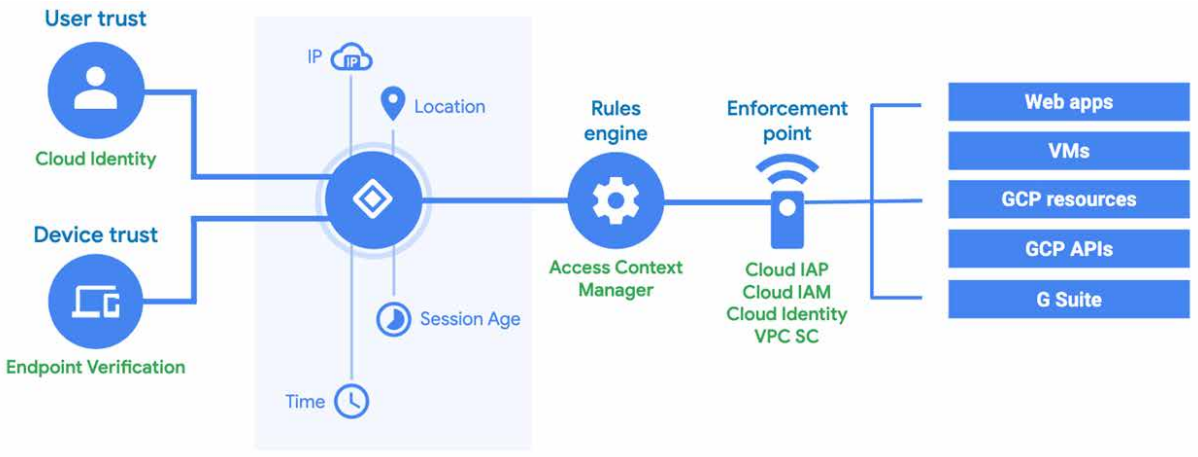
Citrix and Google have been thought leaders, pioneers, and innovators in the secure remote access space for decades, enabling people to do their best work on terms they can influence. When you combine some of this alliances newest, most forward-thinking offerings, the **opportunities to make a difference** for individual workers, the teams that support them, and the businesses they serve emerge brightly! This brief explores how the combination of Citrix Workspace and Google BeyondCorp provides unified, secure, and intelligent zero trust access to SaaS and web apps, plus Citrix Virtual Apps and Desktops.

Solution Overview

For over a decade, Google has been championing a unique, zero trust based approach to enterprise security. With the publishing of "BeyondCorp - A New Approach to Enterprise Security", this approach got a name, and was shared with the world. In 2020, this approach, plus the enabling Google technologies and services, went to market as BeyondCorp Remote Access. The BeyondCorp solution brings together a number of discreet Google services and features to provide secure remote access to web apps **without deploying a traditional remote access VPN**. These services/ features include the following Google components:

- Cloud Identity / G Suite identity
- Cloud IAP (Identity Aware Proxy)
- Cloud IAM (Identity and Access Management)
- Access Context Manager (access policy definition)
- Cloud External HTTP(S) Load Balancing
- Chrome and Chrome Enterprise
- Endpoint Verification (Chrome extension, device inventory collection)

The BeyondCorp solution works by publishing an application or resource to the Internet via a DNS name/URL that's under your control and configuring/ enabling IAP for the application. Users then access the application/resource via a web browser such as Google Chrome, which provides the best user experience and enterprise grade security. The Endpoint Verification extension can be deployed to collect device state information, which can then be incorporated into sophisticated and flexible access policies, enabling fine grained policy definition and enforcement. Google Cloud HTTP(S) Load Balancer calls into IAP to drive authentication, authorization, and context-aware access policy evaluation to make a decision whether the request should be allowed or not.



Since well before pervasive corporate Internet access was a thing, Citrix has been breaking down the obstacles between users and applications and enabling work to get done. Citrix's application virtualization technology (brought to market in the earlier years under such iconic names as Citrix WinView, Citrix WinFrame, and Citrix MetaFrame) has formed the foundation of many companies' remote access solution for almost 30 years. While Citrix virtualization technology still fills this role for many companies today (now available as the Citrix Virtual Apps and Desktops Service), Citrix's solution stack has also evolved into an intelligent, comprehensive security solution delivering VPN less to all types of applications, and information, including intranet web apps and SaaS applications. It's called Citrix Workspace.

Citrix Workspace:

Is a secure, intelligent, and high-performance digital workspace platform that removes distractions, context switching, and complexity creating a better employee experience.

Provides users with a simple, organized, and curated work experience, one they access from anywhere without location or device dependencies.

Consolidates the apps, data, and services employees need to work into a secure feed that uses intelligence to organize, automate, and simplify tasks.

Helps unlock innovation, engage employees, and drive better business results, while giving IT more visibility and control for simplified management, security, and compliance.

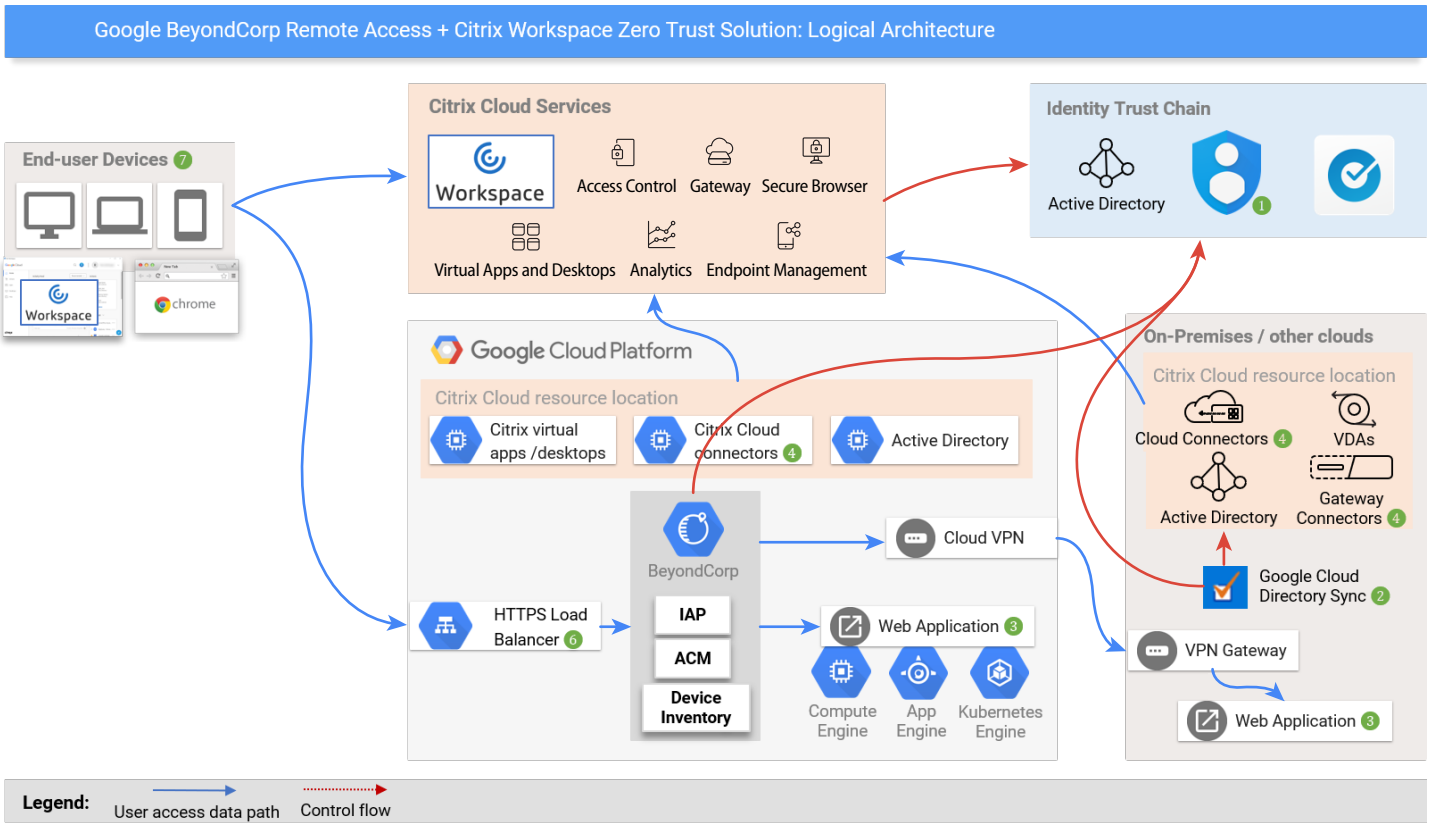
The Citrix Access Control Service, a component Citrix Workspace, delivers secure VPN-less access with single sign-on to on-premises web and SaaS apps, and uses contextual app controls to govern access. Administrators get powerful tools such as policy-based contextual security controls, app protection policies, remote browser isolation, and web-filtering capabilities to enforce corporate policies and protect information assets while enabling users to do their best work.

Web and SaaS applications are defined in the Citrix Workspace library, where they're authorized for specific subscribers (users/groups) and configured for single sign-on and policy enforcement. When users log in to Citrix Workspace, their authorized applications are presented in a rich, curated experience that is accessible through the Citrix Workspace app or web browser. When users launch authorized applications from the Workspace, they are automatically signed on based on their identity, and access is flexibly and dynamically granted to authorized applications. Further access and actions within these authorized applications are enforced based on granular security controls. Web and SaaS applications can be launched using a variety of methods, including a locally installed web browser, the Workspace app's embedded browser (on Mac and Windows devices), a company managed virtualized browser, or Citrix's purpose-built Secure Browser service.

The Citrix Workspace + Google BeyondCorp solution for zero trust access leverages the Citrix Workspace app and Google Chrome. Applications protected by Google Cloud IAP are added to the Citrix Workspace library, where hey are delivered to authorized users when they log in to Citrix Workspace. This provides a simple, unified, and consistent access experience for users inclusive of web, SaaS, virtualized applications/ desktops, and files.

Solution architecture

The diagram below represents the architecture of the Citrix Workspace + BeyondCorp solution for zero trust access:



The foundation of the solution is built upon cloud services from Citrix and Google, delivered from Citrix Cloud (Citrix's managed service delivery platform) and Google Cloud. Identity is federated between Citrix Workspace and Google Cloud Identity 1, and often leverages Google Cloud Directory Sync 2 (or other 3rd party products/services) to include Microsoft Active Directory in the identity trust chain.

Web 3, SaaS, and virtualized applications and desktops are aggregated and delivered by Citrix Workspace, providing a simplified, curated, single sign-on access experience. Virtualized apps and desktops run in Citrix Cloud 'resource locations', which are commonly deployed next to the apps/data being delivered. Citrix connectors 4 in each resource location securely proxy access to virtualized and web applications without exposing them directly to the Internet.

Google's BeyondCorp solution is implemented primarily through Identity Aware Proxy (IAP), which is leveraged to provide browser-based access to web applications. IAP protected apps are 'published' through Google Cloud HTTPS Load Balancers 6 and are accessed using publicly accessible DNS names. Web apps can live anywhere that can be fronted by an HTTPS Load Balancer, including private data centers, Google Cloud, or other public clouds. The BeyondCorp solution applies policy controls based upon contextual information available as the user accesses the application. When using Chrome Enterprise devices, the Endpoint Verification extension provides additional device-related signals which can be incorporated into policy decisions defined in Access Context Manager. It also facilitates applying additional policy controls and enables ongoing policy enforcement without additional authentication events.

The URL's for IAP protected web apps are published through Citrix Workspace via library objects, where authorized subscribers are defined as well as where SSO and Citrix enhanced security policies are defined. Users access Citrix Workspace from devices with the Citrix Workspace app or Google Chrome 7. For managed endpoint environments, Chrome Enterprise is used to deploy/configure Chrome browser, the Endpoint Verification extension, the Citrix Workspace app for Chrome OS, and other desired solution components.

End users access BeyondCorp protected web apps via Citrix Workspace/Chrome on various different types of devices, including BYO and managed devices. They're provided with context aware access to all applications, with corporate policy enforced by Citrix Workspace and/or Google's BeyondCorp solution.

Use cases

Joint customers can leverage Google's BeyondCorp solution and Citrix Workspace today to publish IAP-protected applications through Citrix Workspace. This provides customers with the following high-level benefits:

VPN-less access to corporate web and Citrix virtualized apps and desktops from any device

- Access Citrix Virtual Apps and Desktops, corporate web apps, and publicly accessible SaaS apps with SSO from one end-user portal.
- Security policies to protect information accessed using BYO and unmanaged devices.
- Curated access experience on a broader range of devices such as thin clients in addition to desktops and mobile devices.
- Broader range of application support like web apps, native apps, client/server apps and files.
- Amazing user experience with the low latency, and global scale of Google Cloud.

Consistent and contextual security policies for all apps

- Protect workspace users and data from malware, DLP, phishing and credential theft.
- Protect virtual apps and desktops access with Citrix Access Control.
- Protect web and SaaS apps access under different access scenarios and security models with Google BeyondCorp and Citrix Workspace contextual controls.
- DDOS attack prevention with planet scale Google Context-Aware Network.

Additional information

For more information on Google BeyondCorp solutions, see:

- About BeyondCorp: Google's implementation of the zero trust security model
- BeyondCorp Remote Access Solution page
- Context-Aware Access overview
- Identity-Aware Proxy overview
- Tutorial: Enable secure access to apps hosted on Google Cloud
- Tutorial: Secure access to apps hosted on-premises or other clouds

For more information on Citrix Workspace and zero trust access, see:

- Citrix Workspace product page
- Citrix Access Control product page
- Citrix Access Control Deployment Guide
- Secure Access to Internal Web Applications with Citrix Access Control: Proof of Concept Guide
- Secure Access to SaaS Applications with Citrix Access Control: Proof of Concept Guide

For more information regarding the Citrix Workspace and Google BeyondCorp solution and how it is evolving, please contact your Citrix or Google account manager.

citrix Google Cloud

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States