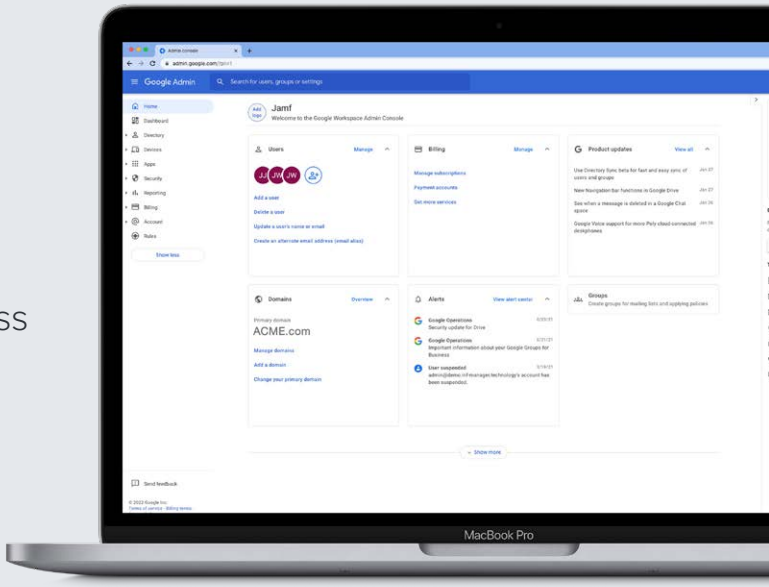
jamf | Google

Google BeyondCorp

Enterprise security through context-aware access



Use Jamf Pro and Google BeyondCorp to construct a compliance and security framework around end-user devices, blending Jamf's device management with Google's endpoint management software for a comprehensive, cloud-based, zero trust solution for your enterprise.

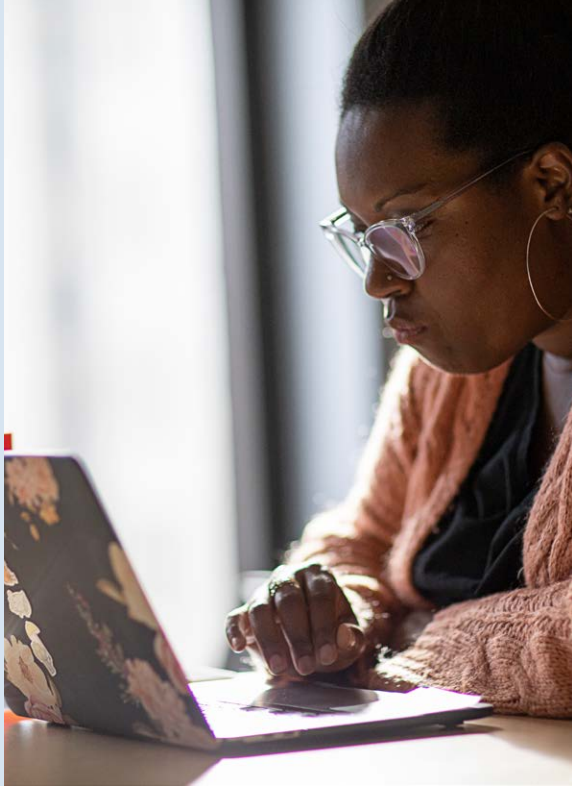
As the last few years have seen a significant increase in the prevalence of remote work, it has become more important than ever before to have security frameworks that provide protection beyond the walls of an office. Organizations that rely on Google's Zero Trust framework BeyondCorp can now integrate compliance information from Jamf Pro. This means that only trusted users on secure macOS devices can access Google protected resources, whether they reside in the Cloud or on-premises.

Jamf integrations brings together the best of Google enterprise architecture with the Apple hardware and operating systems employees love. Now you can leverage the industry-leading tool for Apple device management and simultaneously increase your Google security posture with Jamf's BeyondCorp Context Aware Access integration.

Google's growing role in the enterprise

While Microsoft 365 maintains a dominant presence in office productivity tools and other enterprise software solutions, Google is at work to capture an increasing share of this market sector. Business Insider reported that in 2019, over **5 million** businesses were paying customers of Google Workspace (known at the time as G Suite). As of March 2020, the number of individual active monthly users had reached **2 billion.**

BeyondCorp represents Google's reinvention of security architecture by establishing user- and device-based workflows for authentication and authorization, forgoing network segmentation to protect sensitive resources. In this Zero Trust model, access to resources must be mediated by security controls but are available regardless of what network a user is on. Access is granted based on contextual information about the user and device that can be enhanced using the data collected by Jamf Pro.



Understanding the BeyondCorp integration for Jamf Pro

BeyondCorp Enterprise

It is increasingly important for admins to create multi-tier security protocols that integrate entire IT stacks. Up to this point, many customers have managed their devices in Google's basic mobile device management (MDM) solution to attain elevated levels of security with BeyondCorp. This integration now allows customers to choose Jamf for their Apple device management needs while continuing to rely on Google's Zero Trust protection. The result is a combined compliance and security framework built around end-user devices rather than a network perimeter.

With BeyondCorp, admins can protect access to Google Workspace for Mac and other Cloud or on-premises resources using compliance polices that leverage Jamf telemetry, including such information as whether a device is managed or compliant. For example, an admin can require that all devices that access Google Drive must be running the latest version of macOS with FileVault enabled.

Jamf is leading the pack with Google integrations

This integration is simply one element of our ongoing and broad-based efforts to streamline and enhance connections between the Apple and Google ecosystems.

jamf

www.jamf.com

To learn more about bringing together the best of Apple and Google with Jamf, visit us **here.**