Jamf and Google – Managing and Securing Apple Together

As organizations embrace remote work and an increasingly mobile and distributed workforce, IT and **Security** leaders face several growing challenges:

- How to manage and secure a network of devices and users with sensitive data being accessed from a range of locations
- How to consolidate tooling, do more with less, while at the same time increasing management and security capabilities

While many new advanced technologies have been developed to meet these modern challenges, many organizations still struggle to keep both users and data safe despite tools and solutions available that simplify transitioning to remote/hybrid work environments.

This can often result in...

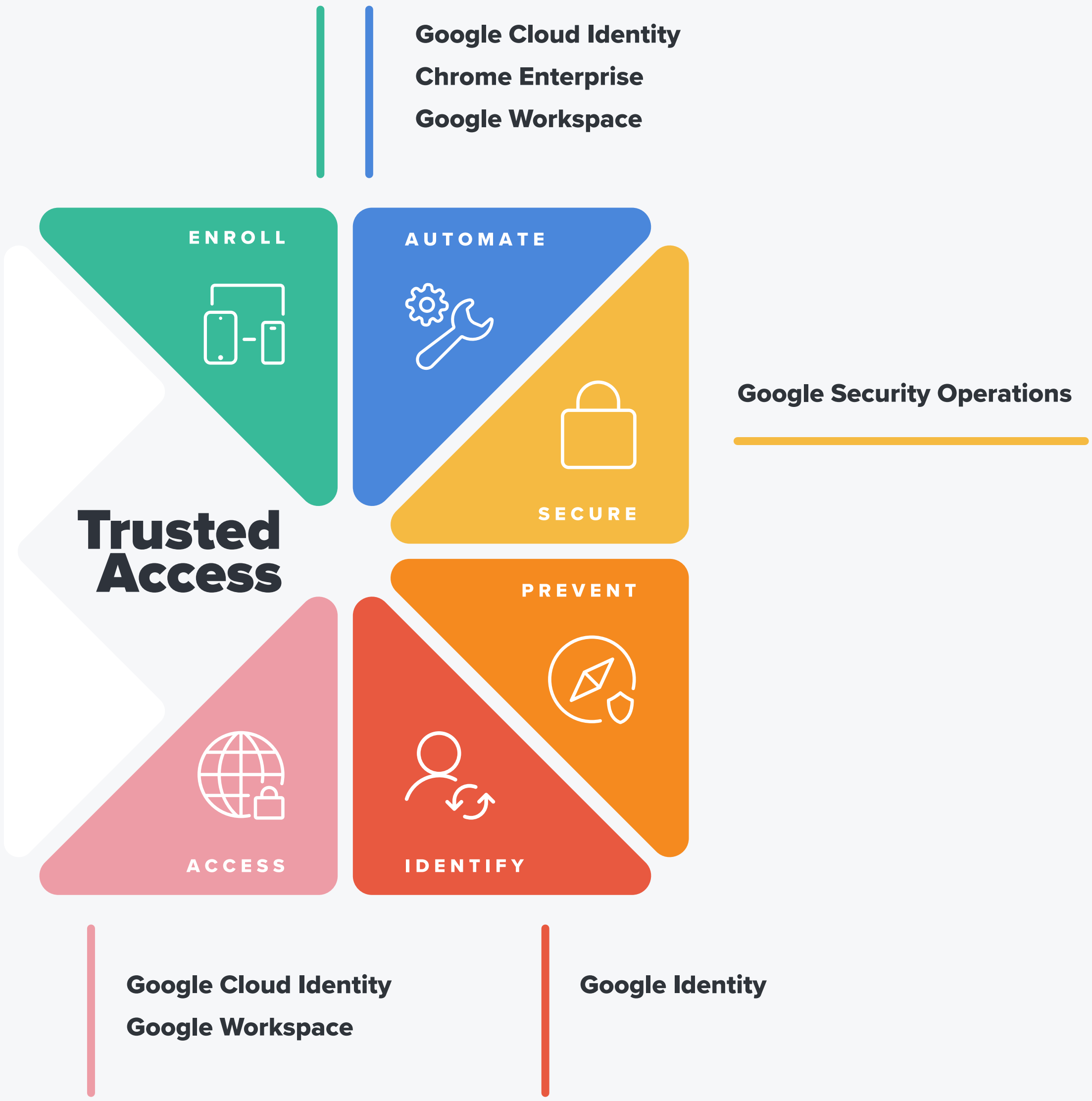
- Unnecessary complexity when configuring comprehensive security
- A poor user experience that also adds administrative overhead to management
- Security gaps that do not extend to all devices across the infrastructure
- A lack of consistent controls over sensitive company resources, including data
- Undermanaged and under-secured endpoints
- Management and endpoint security that doesn't maximize native OS features

Google and Jamf work together so that organizations of all sizes can connect, create, collaborate and work securely. Jamf brings together the best of Apple device management, user identity and endpoint protection with Google Workspace, Chrome Enterprise, Google Identity, and Google Security Operations, to deliver Trusted Access seamlessly.

Trusted Access enables organizations to ensure that only authorized users on enrolled and secured devices can connect to business applications and data. Trusted Access requires integration with a cloud identity provider (IdP), which is why Jamf and Google make perfect sense. All enrolled devices are secured by management and endpoint protection, with all traffic controlled by Zero Trust Network Access (ZTNA) for secure remote connectivity — designed to adapt to the modern threat landscape while correcting the failings of legacy VPNs. Google and Jamf have long been aligned on our approach to VPNs and their shortcomings, providing VPN alternative solutions that complement each other and can be layered.

Integrating Jamf and Google seamlessly achieves the Trusted Access paradigm, which is critical to the success of Apple at work, for organizations that rely on Google for a flexible, innovative and trusted work experience that allows employees to collaborate on work.

Check out the value that Jamf offers with Google to simplify Apple in your organization.



Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Google Product
Secure LDAP for Querying Users and Groups	Directory information about an organization's users (name, email, role, etc.). This information can be used to ensure the right apps and settings get to the right end users. By pulling this information in, the admin doesn't have to recreate it manually.	Integrating with Google Secure LDAP	Jamf Pro	Google Workspace, Google Cloud Identity
Google Chrome Enterprise Context-Aware Access	The integration allows mobile and Mac devices to share the Jamf-determined compliance state with BeyondCorp. Restrict access to applications protected by Context-Aware policies.	Google BeyondCorp Enterprise Integration	Jamf Pro	Google Workspace, Google Cloud Identity, Google Cloud
Enabling Chrome Enterprise Core and Premium	Chrome Enterprise has features and functionality that benefit organizations at scale. Jamf Pro and Jamf School can help enable the enterprise features within Google Chrome.	Enroll browsers with Jamf Pro (macOS)	Jamf Pro, Jamf School	
SSO for Cloud Identity	This allows for the Admin(s) at an organization to login to their Jamf Pro instance, Jamf macOS Security Cloud portal and Jamf Security cloud portal, with their Google credentials.	Configuring Single Sign-On with Google Workspace	Jamf Pro, Jamf Protect, Jamf Security Cloud	Google Workspace, Google Cloud Identity
Cloud based identity for Mac	This allows for the end users at an organization to login to their Mac using their Google credentials. This is the same experience available on Chromebook or on Windows with GCPW.	Integrating with Google Identity	Jamf Connect	Google Workspace, Google Cloud Identity
Jamf Protect Parsers for Google Security Operations	The Jamf Protect and Google Security Operations integration allows detailed event data, Alert and Unified Logging events captured by Jamf Protect be sent to Chronicle for logging and analysis.	Google Chronicle	Jamf Protect	
Jamf Pro Parsers for Google Security Operations	Inventory information from Jamf Pro can be parsed by Google Security Operations	Google Chronicle	Jamf Pro	Google Security Operations
Account Driven User Enrollment with Google Identity for iOS BYOD	Provide device management that respects user privacy on personal mobile devices. Users simply onboard via the settings app, leveraging their Google credentials to enroll into device management, to receive profiles and apps.	User Enrollment for BYOD	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity

jamf

www.jamf.com

To learn more about about the Google and Jamf partnership, check out our **Google integrations** page. To get started **request a trial.**