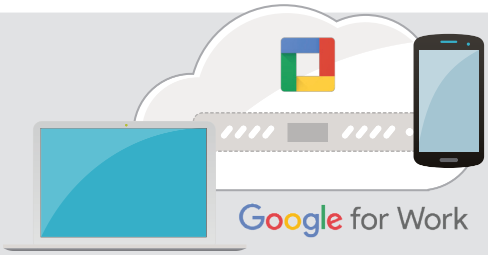
# Seven Reasons to Use Centrify with Google Cloud

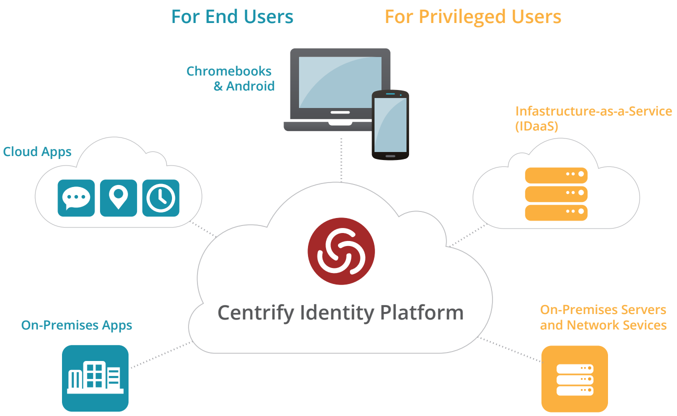


You've made the decision to go Google Cloud. Whether that's adopting G Suite for productivity and collaboration, deploying Android and Chromebooks to your mobile workforce or building and running workloads on Google's infrastructure with Compute Engine, you've decided to use the best of Google for your business. All these innovative cloud and mobile technologies and tools from Google can help your teams work faster and better together. But, the move to cloud and mobile also creates new security challenges as traditional perimeter security is no longer effective. Centrify enables companies to confidently adopt mobile, cloud apps and cloud infrastructure from Google, by adding a critical layer of security and management based on identity — of the device and user.

## 1 **Identity Platform** means you can embrace the cloud — for apps and infrastructure — with confidence.

The cloud is transforming the way business gets done. Employees and lines of business are adopting cloud apps, like G Suite, to improve productivity and drive business results. At the same time IT teams and developers are moving more workloads to cloud infrastructure, like Google Compute Engine. And these apps and resources can be accessed from any device, anywhere. As more of your apps, infrastructure and data move to the cloud, you can no longer rely on your perimeter security because work happens everywhere, not only within the four walls of your organization.

So how do you protect your critical data when your perimeter defense is no longer effective? Forward-thinking organizations are safeguarding their data by establishing a new perimeter, one based on identity.


For End Users
For Privileged Users
Chromebooks & Android
Infastructure-as-a-Service (IDaaS)
Cloud Apps
Centrify Identity Platform
On-Premises Apps
On-Premises Servers and Network Sevices

The Centrify Identity Platform is the first and only cloud-based identity platform that secures and manages both end-user and privileged user access. Rather than rely on multiple vendors and products, Centrify gives you a single, end-to-end solution that secures and manages access for end-users and privileged users across cloud and on-premises apps and infrastructure.

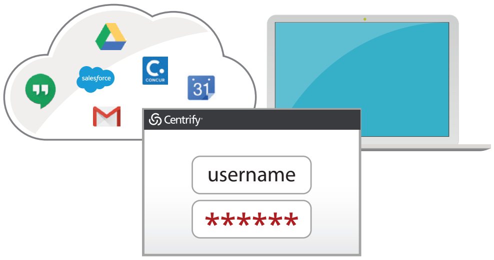
Your end users get secure single sign-on to apps, automated user provisioning to the apps they need, and integrated mobility management. Privileged users get secure access to critical IT infrastructure with share account password management and session monitoring.

## 2 **Single sign-on** means one source of identity and convenience for end users.

As more organizations adopt cloud apps like  G Suite, Salesforce, ServiceNow and others, single sign-on (SSO) using existing identity data becomes critical from both a security and user experience perspective. Centrify lets you control and simplify the sign-on experience by using industry standard SAML and without replicating sensitive user credentials to the cloud or a third-party.

Many organizations have already invested in a directory service, like Microsoft Active Directory or LDAP. Rather than create another user directory for each cloud app or service that your organization uses, Centrify lets you leverage a single source of identity to control access. This eliminates standalone identity silos, which can be an attack point for the bad guys.

SSO also improves the user experience. Instead of creating and remembering multiple usernames and passwords or re-using the same easy to remember (and hack) password, users have one

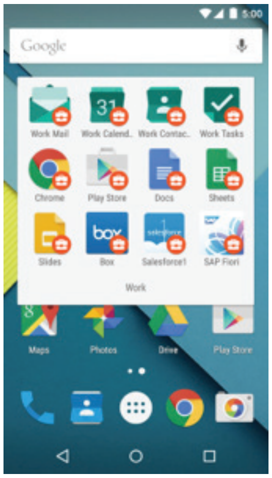


corporate credential, controlled by IT, to access G Suite, other cloud apps, on-premise apps and Chromebooks. SSO. It's a win-win for IT and for users. Users get a better sign-on experience from any device. IT gets fewer helpdesk calls for password issues and improves security by eliminating the need for re-used, weak or unmanaged passwords.

## 3 **Automated provisioning and de-provisioning** means easy come, and easy go.

It's easy to on-board users automatically into G Suite using Centrify. You can pre-assign roles with users and groups in your directory service (Active Directory, LDAP, or Cloud Directory) for provisioning. When users log into Google Cloud on their computer or phone for the first time, their account is available and accessible. If an employee changes job roles (for example, from engineering to sales), reassigning them to a different group in your directory service triggers a change to their software entitlements for G Suite.
If an employee leaves your organization, removing them from your directory service automatically disables access to their G Suite account. Easy come and easy go.

## 4 **Integrated Enterprise Mobility Management** (EMM) means you can confidently say yes to Android in the enterprise.



Mobility is the new business normal. It allows employees and companies to achieve greater productivity and efficiency. With integrated Enterprise Mobility Management (EMM) that includes Android for Work support, Centrify helps you confidently adopt and support Android devices in the workplace, regardless of who owns the device.

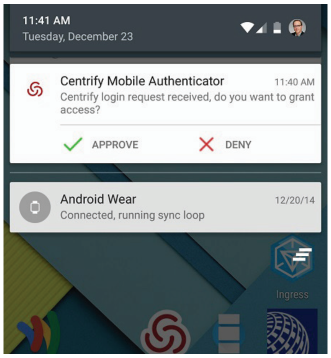
From a single integrated management console, you can manage devices, apps and access policies. Enroll Android devices and provision an encrypted, dedicated Work Profile that separates personal and work data. Work apps and data are protected and managed by IT. Personal apps and data stay private.

As a mulit-OS EMM, Centrify lets you manage all your Android and other devices from one dashboard. With Android for Work, you get consistent management on all Android devices that support the Work Profile or the Android for Work app (for Android 4+ devices). Configure Wi-FI and VPN settings. Set policies for passcodes, encryption, data leak prevention and more. Remotely lock and wipe devices.

In addition to managing devices, Centrify provides mobile application management. You can centrally distribute and manage apps so employees can be productive from day one. Push corporate email profiles to the managed Work Profile. Add internally built or third-party apps to the Google Play app store. Set policies such as blocking apps from unknown sources and sideloading of apps.

Because Centrify integrates EMM and identity, you get device-aware authentication that improves security. By leveraging device attributes, location, network, and user and device certificates, you can help ensure that your application data is protected from unauthorized access.

## 5 **MFA and policy** means you can implement adaptive access controls to apps and infrastructure.


11:41 AM
Tuesday, December 23

Centrify Mobile Authenticator 11:40 AM
Centrify login request received, do you want to grant access?

Android Wear 12/20/14
Connected, running sync loop

Most cloud and on-premises applications and infrastructure support access via username and password. But for some applications and resources, you may want to require stronger authentication. Centrify provides context-aware mulit-factor authentication (MFA) based on the identity of the device and of the user to secure your organization's data.

You may want to require stronger authentication for G Suite or Compute Engine servers in certain situations. For example, you could create a policy requiring additional authentication when a user logs in to their G Suite account or a Compute Engine virtual server from an unmanaged device, when they're outside the corporate IP address range, or when their IP address indicates they may be in a different country.

MFA can be a hassle for end users, but Centify makes MFA easy to use and minimally disruptive for end users. Instead of typing in a complicated code on their device, Centrify provides hassle-free MFA. The Centrify mobile authenticator, available on smartphones, tablets and smartwatches, allows users to easily provide a second factor of authentication via automated push notification or fingerprint. No code to remember and type in — just a simple tap.

Centrify Mobile Authenticator
Centrify login request received, do you want to grant access?

## 6 **Shared Account Password Management** means increased security for privileged account access

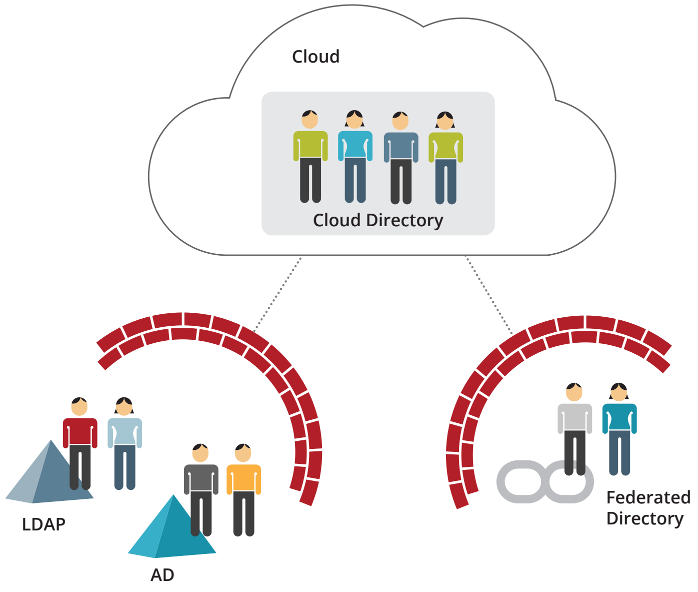
With security breaches in the headlines daily, companies need to protect against the leading cause of breaches – compromised credentials. Centrify helps reduce the risk of breach when sharing privileged accounts, which are increasingly the focus for bad actors. With Centrify, you can enforce centralized control over who can access privileged account credentials, audit all password check-in/check-out and record privileged sessions. And rather than grant access to all resources in your Google Compute Engine environment, Centrify lets you limit access to specific servers, resources or applications.

## 7 **Identity from Anywhere** means freedom to have it your way.

Centrify lets you store your identity data where you want it. You can federate identity from on-premises Active Directory or LDAP, without replicating your identity data into the cloud. While other Identity-as-a-Service (IDaaS) providers claim a single source of “truth” from Active Directory, they’re actually replicating your Active Directory into their Cloud.

Many organizations prefer to keep their directory data on-premises as a way to limit exposure of their sensitive identity data to potential cyberattacks. Rather than storing copies in multiple identity silos, they leverage a single source of identity controlled by IT. That’s why Centrify was built to proxy authentication information for on-premises directories, and never to replicate sensitive user credentials into the cloud. Centrify not only improves security, but also eliminates potential problems caused by directories becoming out-of-sync.

For organizations that don’t have or don’t want to maintain an on-premises directory service, Centrify provides a Cloud Directory. User identities are created and stored in the Centrify Cloud Directory, and the cloud is the single source of account federation.



Our Identity from Anywhere approach gives you choice in deployment options, combining the best of both worlds — on-premises and cloud. For example, you can store your regular full time employees’ identity in existing Active Directory, employees from a recent acquisition in a separate Active Directory forest, customers in LDAP, and contractors or partners in separate Centrify Cloud Directories.

## Conclusion

There you have it. Seven reasons to use Centrify with Google Cloud. But you don’t have to take our word for it. Give it a try for yourself. Start a free, full-featured 30-day trial of Centrify Identity Service for Google Cloud, Android for Work or Chromebooks for Work, or Centrify Privilege Service for shared password management and monitoring for Google Compute Engine today.

Centrify strengthens enterprise security by securing identities from cyberthreats. Centrify uniquely unifies identity for privileged and end users across cloud, mobile and data center. Centrify improves security, compliance, agility and productivity for over 5000 customers, including over half of the Fortune 50 and over 80 federal agencies. www.centrify.com.

| | |
|---|---|
| SANTA CLARA, CALIFORNIA | +1 (669) 444 5200 |
| EMEA | +44 (0) 1344 317950 |
| ASIA PACIFIC | +61 1300 795 789 |
| BRAZIL | +55 11 3958 4876 |
| LATIN AMERICA | +1 305 900 5354 |
| EMAIL | sales@centrify.com |
| WEB | www.centrify.com |