

Centrify Application Services

Stop Breaches that Target Apps

Cloud and mobile apps are quickly forcing their way into the enterprise, facilitating employee productivity, but exposing business-critical data. Cloud apps, and the mobile devices that can access app data, are often outside of IT control.

Managing Access is the Problem

Too many locks — too many keys

Managing and securing access to each individual cloud app and mobile device means managing unique accounts, passwords, and policies across hundreds — often thousands — of endpoints and apps. With so many disparate systems and devices, IT needs a single solution from which to provision users and manage access policy across all apps, from any device, regardless of location.

Password sprawl wastes time for IT and users

With growing application access, users are resorting to password sharing and reuse, exposing corporate data to attacks based on compromised credentials. Compounding this issue is an exponential increase in helpdesk calls and tickets for password resets — reducing IT productivity and user satisfaction.

User productivity leads to IT inefficiency

With dozens — or hundreds — of apps in use, controlling which users have access to specific apps becomes unmanageable. Staying on top of account provisioning is not only cumbersome, but leads to security holes and failed compliance audits if terminated employees have access to corporate apps and data after they leave.

Identity is the Solution

Integrated cloud app and mobile management

Centrify Application Services uniquely unifies cloud app and mobile management into an enterprise cloud service. Centrify leverages identity to secure and manage users' access to applications from any device, regardless of location.

By leveraging a single identity across cloud, mobile and onsite apps, users get a single username and password across all the apps they use for work, and IT can enforce consistent access policies based on user identity. IT gains real-time visibility and control of managed and unmanaged devices, ensuring apps and data are readily accessible to only secure and managed endpoints.

Application Services provides a single, simple cloud portal for app management. Users get one-click access all their apps from any device, and IT gets policy-based control, and automated provisioning and account management.



SINGLE SIGN-ON — PROTECT CLOUD AND MOBILE APPLICATIONS

- Secure app access with adaptive MFA based on device content
- Improve security by eliminating reused, improperly stored passwords
- Simplify app access with SSO for all users



ADAPTIVE MFA FOR APP ACCESS — BEHAVIOR BASED MFA FOR APPS

- Increase security by blocking high risk access attempts
- Simplify MFA through policy based on user behavior
- Enforce policy in real time



WORKFLOW & LIFECYCLE MANAGEMENT — REDUCE RISK & ATTACK SURFACE

- Improve security with automatic user provisioning and role based permissions within apps
- Manage app requests, approval and provisioning with automated workflows
- Prevent unauthorized access automatically



APP GATEWAY — ELIMINATE VPN RISK — THE LEADING BREACH VECTOR

- Stop breaches that establish network foothold via VPN connections
- Reduce attacks by providing only specific app access
- Eliminate security gaps with seamless access policy and MFA



MOBILITY MANAGEMENT — STOP BREACHES THAT TARGET MOBILE APPS

- Eliminate passwords from mobile apps
- Manage and secure both native and web apps on endpoints and mobile devices
- Incorporate device posture with application access policy to minimize risk of lost or stolen devices

Centrify Application Services: The Benefits of Integrated Identity Management

Centrify Application Services provides security, simplicity and control. IT gets one place to manage all accounts and devices. Users get single sign-on across cloud and mobile apps from any device.

Security

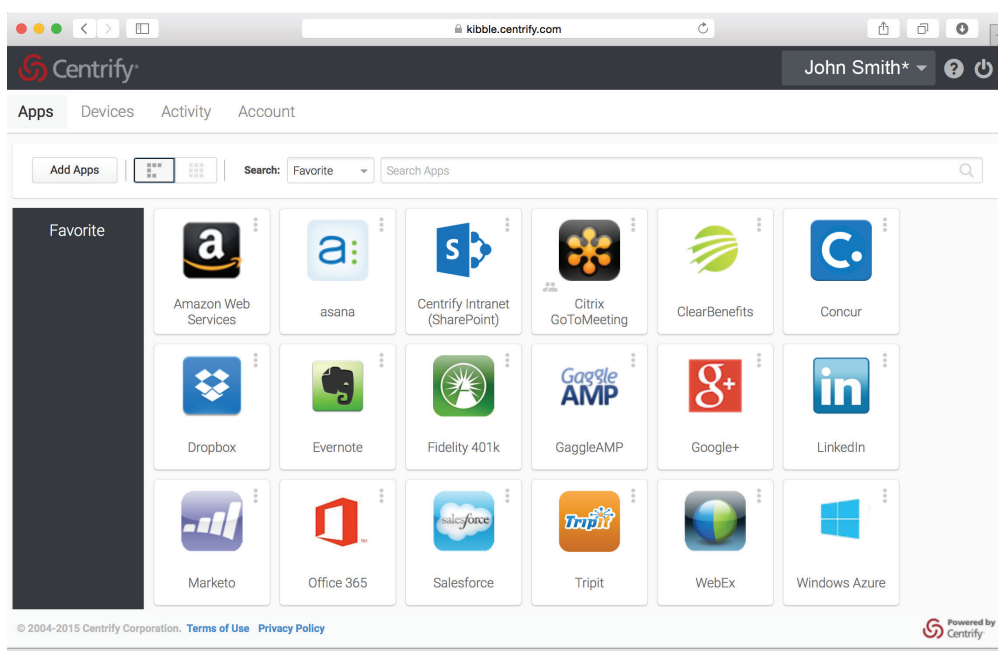
- Eliminate the security risk of simple, reused and/or improperly managed passwords
- Control cloud and mobile applications with identity-based policy across apps and devices
- Enable secure, remote access to on-premises apps — without the risks and hassles of VPNs
- Implement a secure BYOD policy with Centrify's integrated mobile device management. Secure the Centrify app on mobile devices by unlocking with NFC, PIN, passcode or fingerprint.

Simplicity

- Automate account provisioning/deprovisioning and licensing entitlements for business apps
- Eliminate separate policy silos. Integrate management of cloud, mobile and onsite apps
- Reduce helpdesk tickets for password resets, app requests, and device management, with user self service and automated workflows

Control

- Prove ROI and show compliance with granular app and device reporting
- Enforce user policy from a single authoritative source, applied across devices, apps, and locations
- Control access using Active Directory, LDAP, Google Directory, Cloud Directory, external users, or any combination



As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit www.centrify.com. The Breach Stops Here.

Centrify is a registered trademark, and The Breach Stops Here and Next Dimension Security are trademarks of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners.

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