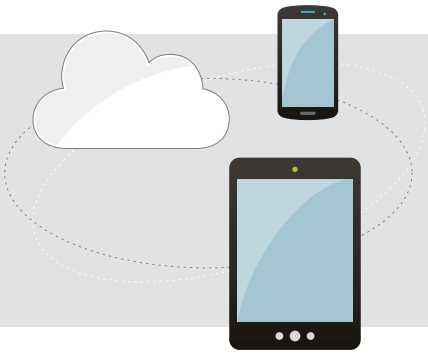
Centrify®

Five Simple Steps to Securing Your Corporate Identities



Identity Challenges in Today's Cloud and Mobile World

The days of on-site servers running local applications that could only be accessed via on-site PCs are over. An ever-increasing number of cloud apps are now available to consumers and businesspeople, and all it takes to adopt these new services is a browser and simple registration. In today's cloud and mobile world, there's no way IT can enforce a secure a perimeter around business data.

- **Business data is officially everywhere:** Onsite servers, hosted servers, cloud app backends, and mobile apps as well. On average, today's employees access their business data from 4 different devices, which are easily lost or stolen.
- **Cloud and mobile apps are established in the enterprise:** "Shadow IT" cloud apps, purchased and implemented by Line of Business (LOB) leaders in Sales and Marketing, are reducing IT visibility and control over user access to critical business data.
- **Users are stuck with countless usernames and passwords:** Each user accesses dozens of apps, and unique credentials for each are impossible to remember. Instead, employees reuse the same passwords across apps and services, exposing corporate data to attacks based on compromised credentials.

The Secure Perimeter is Dead

IT can no longer put a firewall between corporate data and the rest of the Internet, but there are new ways to enforce security policies. Identity-as-a-Service (IDaaS) solutions allow easy user access to apps, from any kind of device, while still securing and managing those apps. These new IDaaS solutions move away from the old perimeter-based security solutions, and instead apply security where it's needed—across cloud apps.

Five Key Steps to Secure Corporate Identity with IDaaS

1 Eliminate standalone identity silos and provide single sign-on

Each new business app, service, or management tool requires a new user directory for access management. Each of these directories is just another identity silo that's outside of IT control, is a target for attackers, and forces users to create and remember yet another password.

IDaaS solutions let IT leverage a single source of identity, like Active Directory, to tie authentication back to a single source of truth, and federate identity from there. When investigating IDaaS solutions, IT should ensure that identity federation extends across the apps and devices users need—and that corporate directory information isn't exposed to attacks or replicated across multiple sources.

With a single source of identity, and federation in place, IT can provide a single username and password to employees to use across all their apps and devices. Users get single sign-on (SSO), and IT eliminates the need for re-used, weak, or unmanaged passwords across cloud apps.

2 Create per-app access policies, based on role

IDaaS also allows IT to provide a cloud portal from which users can gain one-click (or one-tap) access to their apps and data. The best IDaaS solutions also enable IT to create secure access policy that protects app data. Policies that include user, role, network, device type, time of day, location, and more can be implemented to ensure only the appropriate users gain access.

3 Secure the devices used to access your business data

Implementing truly secure app access policy means securing the devices used to access those apps. In today's BYOD world, at minimum, a passcode must be in place, and the device used must be able to be located, locked, or wiped if it is lost or stolen.

Better IDaaS solutions allow much more granular control, including SSO for mobile apps, certificate-based policy for secure access to email, Wi-Fi, and VPN. The best solutions integrate device location and security posture into app access policy—so IT has total control of apps regardless of where, when, or how, they are accessed.

4 Implement Multi-Factor Authentication for critical apps

Most cloud and on-premises apps require only a username and password for access. While that's may be enough security, sometimes more stringent authentication is required. Some IDaaS solutions can implement Multi-Factor Authentication (MFA) to add an extra level of authentication, including secure SMS, phone call, email, or mobile device authenticator. Like all strong authentication solutions, it's always best to find a balance between stringent security and user adoptability—in the case of IDaaS, leveraging a mobile device as a second factor of authentication is often a good balance.

5 Automate provisioning and de-provisioning

With dozens, and sometimes hundreds, of apps to manage, adding new users on an app-by-app basis is just too time consuming for IT. Revoking access for terminated employees is equally cumbersome, and exposes companies to risk of stale accounts if not done properly.

Rather than manually handling these account changes, IDaaS can automate account setup (provisioning), and teardown (de-provisioning).

With automated account management, IDaaS solutions, new employees are automatically given access to the apps and devices they need, based on their role, and access is automatically revoked when their corporate account is deactivated.

Today's Security is Based on Identity

By placing user identity at the core of security policy, IT can minimize risk due to compromised credentials, and better track which users have access to corporate data. Rather than relying on a traditional perimeter-based security that only protects the apps and data on a specific network, leveraging Identity as the source of policy means that IT security can follow users across networks, apps, and devices.

Best of all, the five simple steps outlined above can all be addressed with the right IDaaS solution. Not all IDaaS is equal; these solutions are still relatively new, and different vendors have specific strengths and focus areas within the space.

The best solutions leverage Identity wherever policy is required, including on-premises, in the cloud, and on mobile devices, Macs, and more.

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