Centrify®

SOLUTION BRIEF

If You Manage Identity for App Access, You Must Manage Mobile

New App Landscape — everything is accessed via mobile

Business data is everywhere. Your employees use apps like Salesforce, Marketo, Box, Concur, Office 365, Google Apps for Business — all in the cloud. And more than ever, those apps are all accessed via mobile devices.

The intersection of apps and devices is the best point for IT to apply security policy. For it is only at this intersection that the full context of device type, security posture, and usage, as well as user identity and app access policy can be effectively used to protect application data.

So why is it that legacy mobile device management (MDM) and identity management (IAM) vendors continue to only address one or the other half of the problem? It's clear that the market is starting to shift.

Let's review each of these technology areas, and then examine how organizations can benefit when identity is cleanly integrated across these two solutions.

Mobility, Apps and Identity

MDM has moved to EMM

Over the last couple of years, MDM has become fully commoditized, with all MDM features being controlled by device manufacturers' APIs. Those APIs are available to anyone, so every legacy MDM vendor has nearly the exact same functionality.

The better MDM vendors have had to reinvent themselves, becoming broader enterprise mobility management (EMM) vendors. Their focus has shifted from pure device management to mobile application management (MAM) and mobile content management (MCM).

Managing the device has become a secondary priority. The key security strategy is to manage the content within the apps that are accessed by the device. App data is stored in a cloud backend; it is the interface between the device and the cloud data that must be secured and managed to ensure that corporate data is protected.

Features of EMM are becoming part of the mobile operating system

Just as the once-hot MDM market has become commoditized, some features of EMM are also becoming a commodity. EMM vendors have defined proprietary mechanisms to secure apps and data using technologies such as app wrapping and containerization. Now the OS vendors are including these capabilities by default.

For instance, both Android and iOS enable IT to manage applications and their data. Samsung takes this one step further with their KNOX container and KNOX EMM, co-developed with Centrify.

OS vendors understand that these once consumer-focused devices are being used more and more in a business context, and they want to capitalize on both markets. To do this, they need to provide the "hooks" that vendors can use to secure and manage app data.

EMM vendors are now leveraging identity

In reaction to commoditization, forward-thinking EMM vendors are now moving to the next value area, which is tying identity across mobile and cloud apps. They are looking to combine SSO and identity products alongside their mobile-focused offerings.

SSO vendors are realizing their lack of mobile identity capabilities

Along the same lines, SSO vendors are realizing the critical end-point is mobile, and they must secure and enable these devices or the identity story begins to crumble. Mobile-aware app access is critical to a healthy IAM ecosystem. Realizing this late in the game, many SSO vendors are scrambling to build partnerships with MDM vendors.

Integration Is the Answer

Some vendors that claim mobile and app integration just bundle together a legacy MDM or EMM product, and then add an IAM product alongside—then market them as a solution. But these kinds of market-ware solutions are not really integrated. Without common policy across apps and devices, based on a single identity, these types of products only provide administrators with a console to create siloed MDM and SSO rules.

Centrify believes in a truly integrated approach. End users should have a seamless experience across all devices. Administrators should be managing their users, their apps, and their devices all from one console — with a single set of credentials — upon which all policy can be enforced.

The key goal around integrating identity management and EMM is all about creating and enforcing an integrated, mobile-ready policy for app access and usage.

Centrify: Integrated SSO and EMM

Unlike point vendors of cloud single sign-on or EMM, Centrify provides a solution with one seamless management and policy platform. The Centrify Identity Service was architected from day one as a single platform with a cloud- and mobile-first mindset. When we describe policy, for instance, we have all aspects of that policy in one place—the identity, the app, and the device information. Any combination of these provides the permutations needed for fine- or course-grained policy management.

With Centrify Identity Service, IT can create device-aware policy for application access. Combining device security posture, location, time of day, user role, and more, IT can create rules that block, allow, or challenge for multi-factor authentication—on a per-app basis.

> **Example:** Employee A can access Salesforce from any device when she is inside HQ, between 8am and 5pm. But when she is outside of the physical office, or after hours, she will be prompted for additional authentication before she can access the app. This is a very simple policy, but one that cannot be done without the context of the device being used for access, combined with the user identity within the app.

When provisioning an application with Centrify Identity Service, the mobile application can also be provisioned on the mobile device.

Users get a seamless experience from desktop to mobile — with SSO capabilities across devices — wherever they access the app. Users can also add and launch their own apps, manage, locate, and lock their own devices, and generally take a more proactive role — freeing IT resources to focus on larger issues.

"Organizations manage the device and applications as a means toward protecting the data. Increasingly, organizations will focus more closely on protecting the data through technologies such as DRM and IAM."

Gartner

"Innovation around the EMM space in mobile application management, mobile data management, IAM and mobile security may alter the way organizations approach these challenges, as well as broaden the technologies in the EMM toolset."

Gartner

Another example of the integrated IAM+EMM policy is multi-factor authentication for application access. Identity Service takes advantage of the fact that users carry their mobile devices at all times, and uses those devices as a form of multi-factor authentication. The built-in Centrify Mobile Authenticator can be used to push a request transparently to the user's mobile device to confirm or deny an authentication request.

The lines between EMM and SSO are blurring to the point of being indistinct. Secure mobile access requires identity policy to protect app data, and secure application access has to consider mobile context for effective policy enforcement.

Analysts like Gartner underscore this shift. In the most recent Gartner Magic quadrant on EMM, Gartner said: "*Organizations manage the device and applications as a means toward protecting the data. Increasingly, organizations will focus more closely on protecting the data through technologies such as DRM and IAM.*"

Gartner goes on to highlight the pending integration of IAM and EMM: "*Innovation around the EMM space in mobile application management, mobile data management, IAM and mobile security may alter the way organizations approach these challenges, as well as broaden the technologies in the EMM toolset.*"

Centrify

Centrify delivers secure and unified identity management for end users and privileged users across cloud, mobile and data center environments. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, shared account password management, auditing for compliance and enterprise mobility management.

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