10 Best Practices for Managing and Securing Apple Devices in the Enterprise

Many IT organizations have built their management infrastructure through Microsoft tools, but are now seeing a significant influx of Apple computers and mobile devices being used for work. Rather than barring employees from using Apple devices, IT should look for ways to extend their existing management processes to the Apple platform. This protects corporate resources without compromising the user experience. Following are ten best practices allowing workers to use their preferred devices while maintaining strong corporate IT security policies.

1 Use Your Existing Toolset

You don't need a major investment in tools to manage configuration and implement security protocols for Apple computers and devices. There's a variety of methods to join your devices to Windows-based networks, so you can leverage Active Directory-based authentication. This minimizes disruption and allows IT to continue working with familiar tools.

2 Provide Self-service Management

Managing devices running on multiple platforms is complex and time-consuming for IT. Allow users to manage their own devices through self-service tools for app deployment and in case of a lost or stolen device, activate the remote lock and wipe function. This saves IT time, while empowering users to manage their devices.

3 Use Apple DEP

Apple's Device Enrollment Program (DEP) simplifies deployment of Mac laptops and mobile devices in a corporate environment. It automates device configuration with account settings, applications and access to corporate resources. Enroll all your corporate-owned Macs in DEP to accelerate deployment and development, sparing IT from having to access and set up each device individually.

4 Leverage Identity-based Policies

Provide each user with a single identity to access resources through multiple devices and implement role-based controls so employees access only the resources for which they are authorized.

5 Automate Resource Provisioning

IT can spend a lot of time setting up each user's account applications and devices and then have to turn them off when users change roles or leave. To avoid this time-consuming, errorprone process, automate the provisioning of resources such as applications and configuration of WiFi, VPN and home directories. Automation can significantly reduce IT helpdesk costs.

6 Limit Critical Data Exposure

To minimize exposure of critical data, make your business applications accessible only on Macs and mobile devices integrated into Active Directory. This way you ensure those Macs and devices are secured and managed in compliance with corporate protocols. Strong authentication and single sign-on further ensure the users trying to access those applications are authorized to do so.

7 Provide Remote Access

Managing Macs and mobile devices through Active Directory enables continuous enforcement of security policies, whether those devices are on premise or off. This approach, coupled with the issuance of a single identity for each user, makes it safer to provide employees access to corporate resources from outside the network.

8 Provide users with a single identity

Provide users with a single set of credentials for authenticating and then leverage those secured sessions to access corporate applications

and data. This simplifies the access management of applications and data and makes it easier for users to remember their credentials.

9 Centrally manage FileVault 2 encryption

FileVault 2 uses encryption to bar unauthorized access to data on Apple devices, should a device be lost or stolen. From a corporate standpoint, this is an extra layer of protection for data at rest. To take advantage of it, consider centralizing and remotely managing the encryption keys for each device, and using Active Directory credentials to unlock an encrypted disk when necessary.

10 Implement a single platform

Some companies shy away from using multiple platforms and devices to avoid setting up a separate infrastructure to manage them. But that's not necessary when you deploy a unified, integrated solution to manage PCs, Macs and mobile devices. This simplifies management, maximizes security and helps reduce operational costs.

Learn how Centrify can help you manage and secure Apple devices and users.
Visit www.centrify.com/apple.

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