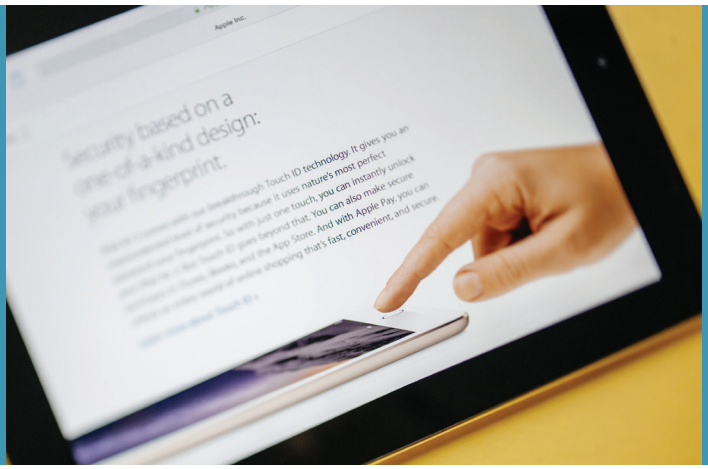

Maximizing Mac Security Through Modern Enterprise Management

With Apple's popularity steadily rising, Gartner predicts the number of businesses using Macs in some capacity could approach 100% in the next two years. One of the key factors leading many IT admins and users to switch from Windows-based PCs is the belief that Macs are less vulnerable to hacks, viruses and other malware. But while the Mac OS X operating system is built on a robust UNIX kernel, the technology's inherent immunity to threats is only one factor in securing it. IT professionals stress the importance of considering technology, people and process when deploying, managing and securing any computing platform, including the Mac. Following are three potential gaps in Mac security that can be addressed through applied best practices.

Not Taking Advantage of Secure Technology

The Mac OS X operating system includes state-of-the-art security technology. But if the Mac is not set up to correctly leverage it, or the user circumvents the built-in security features, it can become a risk for the organization. For example, Mac OS X includes FileVault 2 full disk encryption which, when used properly, makes it virtually impossible to gain access to the data stored on the disk without the correct credentials. But the Mac must be set up to use disk encryption and strong password policies must be enforced in order to prevent unauthorized access to the device.

Securing the connection between the user's Mac, the corporate network and applications is essential to prevent malicious eavesdropping. But setting up and maintaining secure networks and the associated certificate management can be a complicated process, especially for remote employees using their own devices. Ideally, your Mac management solution should automate the process of securing network connections and the management of certificate-based security.

Even with encryption and secure networking, concerns over lost devices or hackers gaining access to information stored on the device persist. Mac management software can alleviate these concerns by taking advantage of Apple's strong, hardware-based computer lock and wipe capabilities to allow both users and IT admins to lock a device remotely and, if necessary, wipe and render it unusable.

Don't Underestimate the People Factor

It's estimated that over 50% of employees reuse the same simple-to-remember password for both personal and business logins. Others write down passwords and leave them in insecure places. Employees may be your biggest liability when it comes to computer security.

In response, IT should strive to provide workers with one username and password for all business access. Once authenticated on the device, users should automatically receive seamless access to all appropriate corporate apps and resources. Mac management software should allow users both inside and outside the firewall to securely authenticate to the corporate network and instantly gain access to the apps, data and resources they need — with one set of credentials.

Lack of Process Managed Through Policies

Ensuring a well-defined set of processes and policies are enforced with all users on all devices goes a long way toward locking down computing platforms. To that end, as a matter of policy, lock screen passwords should be mandatory for all employees who use their own devices for business purposes. And password strength should also be enforced.

Rules based on user roles can easily be created to build access policies across different departments within an organization. For example, people in the sales organization should be allowed access to the sales order entry system, but not to company payroll information.

There should also be a well-defined process for workers who leave the company. Ideally, the IT department should be able to simply turn off a user account and with that, all access to applications (such as email), customer data and corporate resources should be automatically terminated as well.

© 2015 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The End Result: A Truly Secure Mac Platform

Applying customized rules for granular control over devices and groups of users should be simple and easily deployed. Software solutions are available to enable admins to push out and enforce policies on remote Macs and to block corporate network access when necessary.The end result: A truly secure Mac platform

Relying on the Mac's security reputation is not sufficient to ensure users and corporate assets are protected. And simply trusting users to create strong passwords, enable disk encryption and only access data via secure networks is also not a viable security strategy. Ultimately, only a solution that combines the management of technology, people and process will be effective in protecting corporate networks and resources.

Centrify Identity Service, Mac Edition addresses all three areas to maximize Mac security by:

1. Simplifying the configuration and the ongoing management and enforcement of the security technology built into Mac OS X.
2. Enabling single sign-on technology to both enforce strong password creation and eliminate the need for users to remember numerous complex passwords.
3. Providing over 300 out-of-the-box policies to enable granular control for IT to manage and monitor these systems and ensure proper use.

For more information on Centrify Identity Service, Mac Edition visit Centrify's web site at www.centrify.com/mac.

To find out how you can substantially improve the way Macs are being incorporated into your IT environment, check out this white paper on Best Practices for Adding Macs to Microsoft Networks.

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.

Centrify is a registered trademark, and Centrify Identity Service is a trademark 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