Centrify Enables Organisations to Stop Breaches That Start on Mac Endpoints

Submitted by: Origin Comms Ltd
Tuesday, 6 June 2017

New capabilities reduce risk by securing local administrator passwords and simplifying Mac application management with turnkey Munki integration

Centrify, the leader in securing hybrid enterprises through the power of identity services, has announced enhancements to the Centrify Identity Platform that deliver local administrator password management for Macs and comprehensive Mac application management and software distribution via turnkey integration with the Munki open source solution. These new capabilities enable Mac administrators to solve critical challenges by implementing best practices for controlling privileged access on Macs while at the same time simplifying management of Mac endpoints.

“Our latest security capabilities extend shared account password management (SAPM) from servers, network devices, Windows and Linux endpoints to Mac, while at the same time simplifying Mac application management with Munki support that enables users to install applications without knowing the admin password,” said Bill Mann, chief product officer at Centrify. “The Centrify Identity Platform secures Mac endpoints as well as Windows and Linux with our market leading Identity-as-a-Service (IDaaS) and privileged identity management (PIM) solutions that help stop breaches across endpoints, infrastructure and apps.”

Control Shared Passwords

It is common for organisations to maintain administrative accounts on their users’ Macs and use the same admin password across all Macs. This introduces risk, because inevitably the password is shared with an end user who needs to install applications on their Mac, or is known by admins who leave the company. These users and ex-employees now have full administrative privilege across every Mac. This leaves an organisation highly susceptible to breaches that start on Mac endpoints, and demands a solution that enables organisations to minimise and centrally control access to Mac administrative accounts, just like they do for Windows and Linux endpoints, servers and network devices.

The Centrify Identity Platform closes this gap in security with local administrator password management (LAPM) for Mac that enables administrators to generate a unique administrator password for each Mac. With Centrify, organisations are eliminating the sharing of a single Mac admin password across an entire organisation. The solution can be enabled for all Macs enrolled in the cloud-based management service, ensuring support for remote machines as well as those on the corporate network. Authorised admins can check out the admin password, and the rotation of the admin password is automated. Who accessed what and when is fully audited across Mac administrative access and all other endpoints and infrastructure and available through comprehensive reporting.

Eliminate Admin Access for Daily Use

End users cannot install software without local admin rights. However, local admin rights mean your end users—or anyone who compromises their accounts—are privileged users on their Mac. This increases your

attack surface and makes endpoints an effective target for malware and rogue applications. By seamlessly combining the Centrify Identity Platform with the open source Munki solution — the leading Mac app and patch management solution — your end users can install and manage applications without local admin rights.

Munki's open-source toolset provides a rich Apple App Store like end user experience, where the specific apps an organisation approves are available for seamless installation. Centrify simplifies the Munki setup, management, security and ongoing support to make it easier for organisations to deploy and operate their own enterprise Mac app store. Additionally, Centrify's cloud-based app repository extends Munki to remote Mac users regardless of their location or status on the corporate network.

Controlling access to shared administrative passwords for endpoints and eliminating the need for local admin rights to install software on Macs are established PIM best practices. A recent Forrester study found a direct correlation between the number of PIM best practices an organisation has implemented and the number of security incidents it encounters. The Centrify Identity Platform now makes it easy for organisations to extend best practices to Mac in order to stop breaches that start on endpoints.

For more information, go to http://www.centrify.com/mac.

About Centrify

Centrify redefines security from a legacy static perimeter-based approach to protecting millions of scattered connections in a boundaryless hybrid enterprise. As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure each user's access to apps and infrastructure through the power of identity services. This is Next Dimension Security in the Age of Access. Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organizations. To learn more visit www.centrify.com.
The Breach Stops Here.

Media contact:

Amanda Hassall, Consultant
T:+44 (0) 16 2882 2741
M: +44 (0) 78 5535 9889
E: amanda@origincomms.com

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Origin Comms Ltd

Copyright © 1999-2026 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com