Jamf Extends Collaboration with Microsoft Enterprise Mobility + Security with iOS Device Compliance

September 10, 2020

MINNEAPOLIS, Sept. 10, 2020 (GLOBE NEWSWIRE) -- The need to support a remote workforce has shifted security focus from what was previously within the perimeter of a corporate network to extend beyond these walls. Because of this, organizations are looking for a streamlined way to manage and secure all of their devices. Today Jamf, the standard in Apple Enterprise Management, announced it is extending its collaboration with Microsoft Enterprise Mobility + Security by launching iOS Device Compliance, available now in a closed preview.

Through this offering, organizations are empowered to choose Jamf for iOS management while also sharing important device information, like compliance status, with Microsoft Endpoint Manager. IT teams can utilize Jamf features for Apple ecosystem management, while leveraging Conditional Access powered by Azure Active Directory and Microsoft Endpoint Manager to ensure that only trusted users from compliant devices, using approved apps, are able to access company data.

“Trends like employee technology choice programs and the consumerization of IT continue to grow, and organizations need management tools that can adapt and shift to hybrid environments,” said Brad Anderson, corporate vice president at Microsoft. “With Microsoft and Jamf, IT teams can consolidate management of employee devices, while not losing the ability to provide key ecosystem-specific functionality.”

iOS Device Compliance is expected to be generally available for all Jamf customers later this year.

Organizations already enjoy the ability to leverage Conditional Access on macOS devices, by sharing inventory data from Jamf with Microsoft Endpoint Manager. Today’s announcement of an expanded collaboration adds iOS support. Now IT teams can prevent an authorized user from using any macOS or iOS device that does not comply with security policies, and leverage Jamf Self Service for remediation.

Jamf addresses this by requiring the user to register devices they want to use to access applications connected with Azure Active Directory, including Microsoft 365 Apps. First, compliance criteria is established and measured on the iOS device by Jamf. The device information collected by Jamf is then sent to Microsoft Endpoint Manager. Finally, Endpoint Manager checks the device’s compliance state and leverages Azure Active Directory to dynamically grant or deny access. If the device is not compliant, a notification is sent to the user, requiring remediation in Jamf Self Service.

“We know IT teams want the simplicity of managing and securing all their devices within a single pane, while still providing the intended Apple experience employees demand and deserve,” said Jason Wudi, chief technology officer, Jamf. “Jamf and Microsoft have a long history of collaborating to better empower the end user and IT, and today’s announcement of iOS Device Compliance shows we are committed to continuing to innovate to make the modern management experience better for enterprises growing their Apple fleet.”

In 2017, Jamf and Microsoft announced a collaboration to bring Conditional Access to macOS, which included the ability to share inventory data from Jamf Pro to Microsoft Intune, apply Conditional Access and offer remediation paths – ensuring that trusted users are accessing corporate data from trusted applications on trusted devices. Then in 2018, Jamf again expanded Microsoft technology integration to create a more seamless login experience for end users.

About Jamf
Jamf, the standard in Apple Enterprise Management, extends the legendary Apple experience people love to businesses, schools and government organizations through its software and the world’s largest online community of IT admins focused exclusively on Apple, Jamf Nation. To learn more, visit: www.jamf.com.

Media Contact:
Rachel Nauen
media@jamf.com