jamf

WHITE PAPER

Bringing Jamf and Microsoft together for the better

As the world of work has changed this year, so has the day-to-day reality of managing Apple devices in the enterprise. Supporting remote staff has never been more critical and many admins need the best purpose-built tools to help their organization succeed: Jamf for Apple and Microsoft for other devices.

Where many would think this needs to be a choice of one platform over the other, the conversation is no longer around picking the device type you want to standardize, nor having one ineffective platform to force management all in the same way. These devices, to their core, function differently. The solution is about arming yourself with the best options for each device, for yourself, and letting integrations and relationships like Microsoft and Jamf's lead the way.

This white paper covers:

- Why Mac is on the rise in the enterprise and how to accommodate
- How Jamf and Microsoft work together for ultimate ease, efficiency and flexibility

Mac is on the rise in the enterprise

Users are changing the technology narrative and demanding to use the hardware they are most comfortable with. Often, that's Mac.

The Power of Choice

As employee-choice programs in the workplace become the norm, more Mac are poised to hit your networks. How many? When given a choice between PC and Mac, 72%* choose Mac. Why do organizations and IT need to start taking Mac seriously in the enterprise? Because a happy, efficient employee is a productive one. The results are in from a global research study** focused on Mac in the enterprise. Here's what Mac users say...

97%
report increased productivity

95%
report increased creativity

94%
report greater self-sufficiency

91%
report increased collaboration

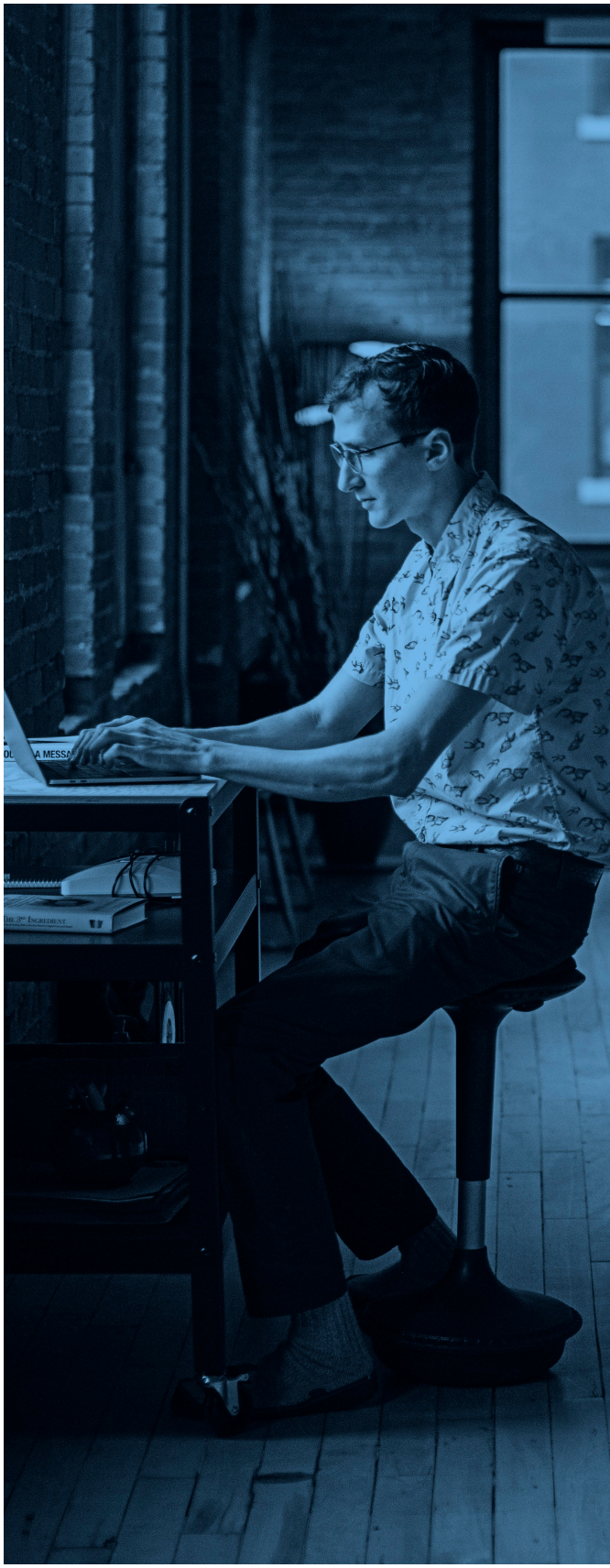
Mac is also perceived to be more effective in the workplace than any other device brand. Of those surveyed, 79% agree they could not do their job as effectively without being able to use a Mac. And 83% of respondents in the job roles of Information Technology and Human Resources feel using a Mac is critical to their job function.

Boosting Employee Retention with Mac

Employee-choice programs and offering Mac are also important factors for workers when they are choosing to stay or leave a company.

95% of survey respondents agree they are more likely to choose/stay at a company which offers them choice in work technology

And offering Mac doesn't prevent users from leveraging the Microsoft productivity software they love.



Jamf and Microsoft: Working Together

It's no secret that Jamf and Apple have a very close relationship, and this is all the more reason to help users with a secure and strategic integration with Microsoft.

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 before a continued partnership in 2020 with Device Compliance for iOS, which will be covered in more detail later in this white paper. In 2021, Jamf integrated the Mac-focused security, visibility, detection and remediation of Jamf Protect with the cloud-native SIEM and SOAR capabilities of Azure Sentinel to provide security organizations with extensive control and security insights across their Mac fleet.

As workflows and user processes have changed over the years and continue to adapt to a "new normal" in the enterprise, Jamf and Microsoft continue to close the gap to create a streamlined experience for end users and IT alike.

From an IT perspective

As an IT admin, it's important to create a reliable, secure fleet of devices that is easy to update, protect and maintain. End users want the same service, security, and manageability regardless of selecting Mac or Windows.

Whether coming from a world of Apple or a world of Windows, understanding the other side can sometimes open up opportunities for error. Many Mac IT admins are well aware of and used to Jamf Pro, but with new integrations and partnerships between Apple, Jamf and Microsoft, there are plenty who come from a world of Microsoft and managing Mac with Intune wondering when to combine the two.

As a Windows admin, what's important is security in a zero-trust environment. Microsoft Intune is not a part of this process to be the better management platform for Mac, it's there to provide Identity Protection coming from a Mac to any application.

To do this, as a Windows Admin, you need to understand how the Apple ecosystem works. How is it encrypted? How can running anti-malware be guaranteed? How do you detect malicious behavior and remediate breaches? How does one sign into it?

Jamf Pro and Microsoft Intune

Jamf Pro is the engine that manages the device and is sending reporting data back to Microsoft Intune. Microsoft Intune is then responsible for looking at that data and determining if the device is compliant or not.

Compliance is completely up to admins. Specific settings, complex passwords, encryption, or a state a of sleep after timed inactivity can all be required (or not). These compliance settings are the communication point between Microsoft Intune and Jamf Pro. Applying these policies, allows admins to know if the device is properly configured or needs action.

Where things differ is the action of associating this state of compliance or non-compliance to a user. Enter Conditional Access. A Microsoft Intune-only feature allowing others to integrate, but the control exists within Intune. With these policies, compliance, and security measures we see the communication between Intune and Jamf Pro forming, the relationship created, and a level of security takes form.

It's the beauty of this relationship. You can get the full spectrum of management capabilities through Jamf Pro while protecting identities and accesses to the services from your Mac with Microsoft Intune and Azure AD. Therefore, standardizing on one platform is unnecessary.

Microsoft Enterprise Mobility + Security and Device Compliance for iOS

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 the walls of the office. Because of this, organizations are looking for a streamlined way to manage and secure all of their devices. In order to best support organizations, Jamf, the standard in Apple Enterprise Management, announced it is extending its collaboration with Microsoft Enterprise Mobility + Security by launching Device Compliance for iOS.

“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.”

Organizations already enjoy the ability to leverage Conditional Access on macOS devices, by sharing inventory data from Jamf with Microsoft Endpoint Manager. With Device Compliance for iOS, IT teams can now also 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 are 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.

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.

Jamf Protect and Microsoft Azure Sentinel

As organizations' devices and network infrastructure become more complex, security teams are experiencing increased reliance on tools like security incident and event managers (SIEM) and security orchestration automated response (SOAR) to secure their environment. To bring real security and control to the Mac world, Jamf has integrated its endpoint security tool, Jamf Protect, into the data flow for Microsoft Azure Sentinel.

Jamf Protect is Mac-only endpoint protection and natively pushes all Mac-specific security data and alerts directly into Azure Sentinel with minimal configuration. All malicious or suspicious Mac activity, as well as malware notifications, integrate easily with preexisting workflows, which means little effort and time demanded from your security staff. With Jamf Protect's attack detection and log information, Azure Sentinel can extend its capabilities to identify and remediate broad attacks against all of the Mac devices in a customer's environment while maintaining better security for the organization as a whole.

By combining the capabilities of Microsoft and Jamf, customers will have complete visibility into security activity across their Mac estate from within their familiar single pane of glass, Azure Sentinel.

Conclusion

With integrations like this and the relationship between Jamf and Microsoft, there is no reason not to welcome Mac into your environment with open arms. Even as a Windows Admin, you can make Mac as secure, as manageable and as integrated as any of your Windows devices.

Request a trial of Jamf today and see for yourself. Or contact your preferred authorized reseller of Apple devices to get started.

Sources:
**https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/*
***https://www.jamf.com/resources/e-books/global-survey-mac-in-the-enterprise/*