



Jamf and Microsoft – Managing and Securing Apple in the Enterprise

*As organizations embrace modern work,
IT and Security teams are searching for
the best way to support Apple users.*

Organizations commonly face the same challenges when creating a strategy for Apple::

- How to manage and secure devices with sensitive data that are being access from everywhere
- How to consolidate tooling, do more with less, while at the same time increasing management and security capabilities
- How to support employee choice programs, mobile devices and BYO devices

While many advanced technologies have been developed to meet these modern challenges, organizations still struggle to keep both users and data safe.

This can often result in...

- Unnecessary complexity when configuring comprehensive security
- A poor user experience that also adds administrative overhead to management
- Security gaps that do not extend to all devices across the infrastructure
- A lack of consistent controls over sensitive company resources, including data



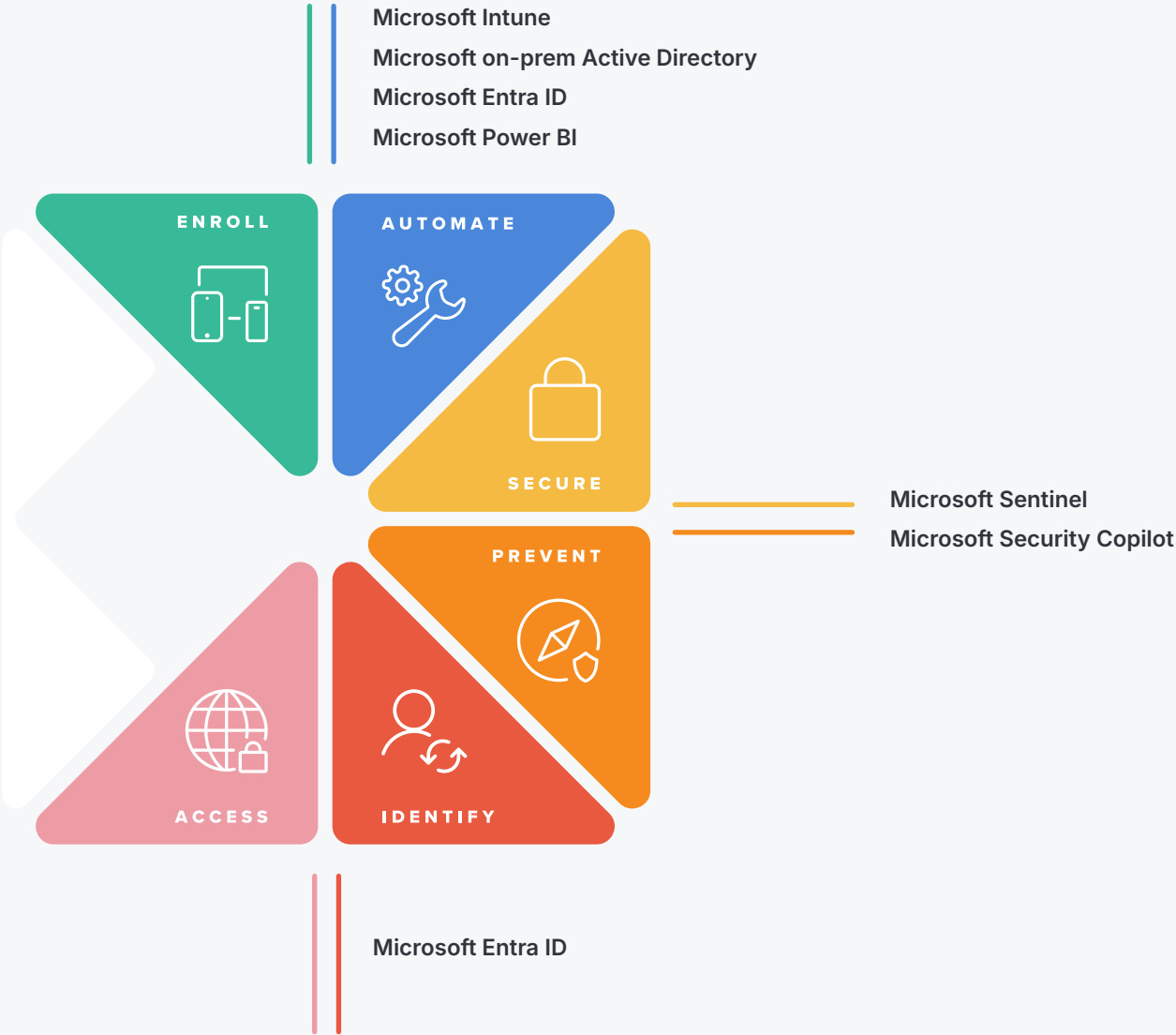
How Jamf + Microsoft effectively support Apple in organizations utilizing Microsoft platforms

Jamf is uniquely positioned to bring together the best of Apple device management, user identity and endpoint protection to deliver a Apple-first zero-trust outcome with Microsoft. This enables organizations to ensure that only authorized users on enrolled and secured devices can connect to business applications and data. To achieve this zero trust outcome, joint customers leverage an integration with a cloud identity provider (IdP), which is why Jamf and Microsoft make perfect sense. All enrolled devices are secured by management and endpoint protection, with all traffic

controlled by Zero Trust Network Access (ZTNA) for secure remote connectivity — designed to adapt to the modern threat landscape while correcting the failings of legacy VPNs.

Integrating Jamf and Microsoft is the key to success with Apple in organizations leveraging Microsoft platforms to drive their infrastructure.

Check out the integrations that Jamf offers with Microsoft to simplify Apple in your organization.



Device Management Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Microsoft Product	Customer feedback
LDAP for Querying Users and Groups	Directory information about organization's users (name, email, role, etc.) can be used to ensure the right apps and settings get to the right end users. The Admin doesn't have to recreate this information manually.	Integrating with LDAP Directory Services	Jamf Pro	On-prem Active Directory	
Cloud Identity Provider for Querying Users and Groups	Information about an organization's users (name, email, role, etc.) is found in Cloud IdP now which can be used to ensure the right apps and settings apply to the right users and devices. Connecting this info into Jamf Pro allows admins to not have to insert manually.	Microsoft Entra ID Integration	Jamf Pro	Microsoft Entra ID and Intune (Microsoft Endpoint Manager)	"Easy-to-follow documentation provided by both Jamf and Microsoft. Most straight forward integration I have ever been involved in." I Borota
Dashboard Analytics Reporting	Get everything you need for free to create and save unlimited interactive reports. Use the Jamf Pro Power BI app to bring a deeper level of data analytics to your Jamf deployment. Extend reporting capabilities of Jamf Pro and capture it within your Power BI architecture. Data available: Computer & Mobile Devices, Details, Applications, Extension Attributes and Groups	Power BI	Jamf Pro	Microsoft Power BI	Power BI with Jamf Pro "Power BI integrates seamlessly with Jamf Pro to provide detailed reports on all aspects of your Jamf Pro instance. Set up reports on macOS versions, Virus Definition versions, number of devices per building etc etc. Absolutely love this tool for providing data we can act on." C McBride



Identity and Access Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Microsoft Product	Customer feedback
Device Compliance for macOS, iOS and iPadOS	Organizations want to ensure that trusted users are on a compliant device before they allow them to access company materials. This integration allows for Jamf Pro to verify if a device is compliant, and sends that yes/no status to Microsoft. *This replaces Conditional Access starting in Jamf Pro 10.4	Device Compliance	Jamf Pro	Microsoft Entra ID and Intune	"An Integration to make sure access of office data is provided on to the devices which are compliant. Seamless integration between Jamf and Microsoft Entra ID helps us to achieve this security ask. A must to implement solution from an Security point of view." Samstar777
SSO for Cloud Identity	This allows for the Admin(s) at an organization to login to their Jamf Pro instance, Jamf macOS Security Cloud portal and Jamf Security cloud portal, with their Entra ID.	Configuring Single Sign-On with Active Directory Federation Services Microsoft Entra SSO integration with Jamf Pro	Jamf Pro	Microsoft Entra ID and Intune	Best IDP Integration "Microsoft Entra ID integrates with everything we have that supports an external IDP. The Cloud Identity Provider feature for SSO in Jamf Pro and the integration for Jamf Protect brings your corporate identities to your Jamf products and other third party services with ease." T Ellis
Cloud based identity for Mac	This allows for the end users at an organization to login to their Mac using their Entra ID.	Integrating with Microsoft Entra ID	Jamf Connect	Microsoft Entra ID and Intune	"Implementing was easy with the instructions given. SSO is a life changer." Tyler Verlato

Member of
**Microsoft
Intelligent
Security
Association**



