



# 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 accessed 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



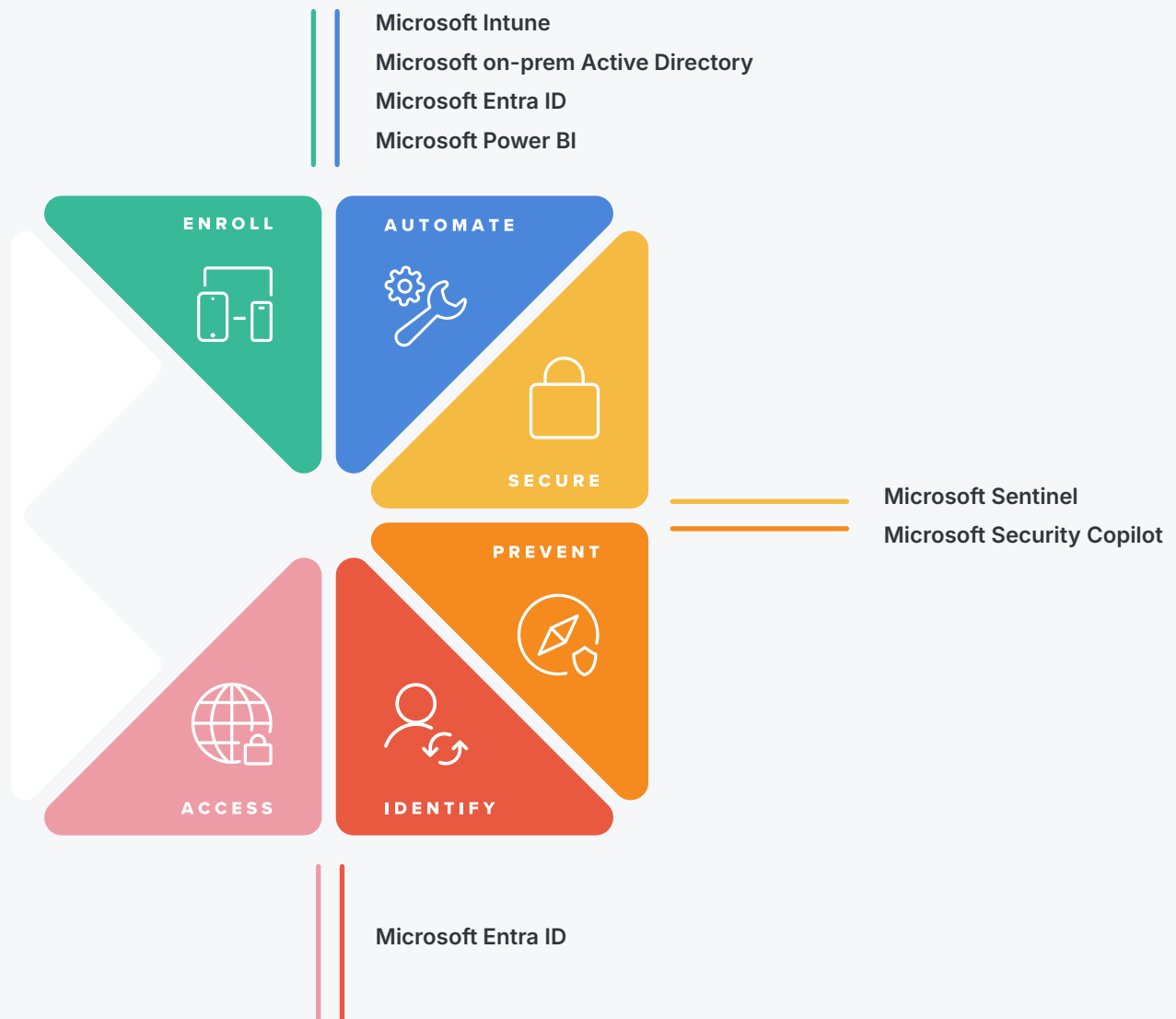
## How Jamf + Microsoft effectively support Apple in organizations utilizing Microsoft platforms

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.	<a href="#">Integrating with LDAP Directory Services</a>	<a href="#">Jamf Pro</a>	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.	<a href="#">Microsoft Entra ID Integration</a>	<a href="#">Jamf Pro</a>	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	<p>Get everything you need for free to create and save unlimited interactive reports.</p> <p>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.</p> <p>Data available: Computer &amp; Mobile Devices, Details, Applications, Extension Attributes and Groups</p>	<a href="#">Power BI</a>	<a href="#">Jamf Pro</a>	Microsoft Power BI	<p><b>Power BI with Jamf Pro</b></p> <p>"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."</p> <p>C McBride</p>



Identity and Access Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Microsoft Product	Customer feedback
Device Compliance for macOS, iOS and iPadOS	<p>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.</p> <p>*This replaces Conditional Access starting in Jamf Pro 10.4</p>	<p><a href="#">Device Compliance</a></p>	<p><a href="#">Jamf Pro</a></p>	<p>Microsoft Entra ID and Intune</p>	<p>"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."</p> <p>Samstar777</p>
SSO for Cloud Identity	<p>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.</p>	<p><a href="#">Configuring Single Sign-On with Active Directory Federation Services</a></p> <p><a href="#">Microsoft Entra SSO integration with Jamf Pro</a></p>	<p><a href="#">Jamf Pro</a></p>	<p>Microsoft Entra ID and Intune</p>	<p><b>Best IDP Integration</b></p> <p>"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."</p> <p>T Ellis</p>
Cloud based identity for Mac	<p>This allows for the end users at an organization to login to their Mac using their Entra ID.</p>	<p><a href="#">Integrating with Microsoft Entra ID</a></p>	<p><a href="#">Jamf Connect</a></p>	<p>Microsoft Entra ID and Intune</p>	<p>"Implementing was easy with the instructions given. SSO is a life changer."</p> <p>Tyler Verlato</p>

Member of  
**Microsoft  
Intelligent  
Security  
Association**



Endpoint Security Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Microsoft Product	Customer Quote
Jamf Protect for Microsoft Sentinel	The <b>Jamf Protect</b> for Microsoft Sentinel integration sends detailed event data from macOS devices into Microsoft Sentinel in a simple and easy workflow. This provides security teams with visibility into unique security events happening on Macs by leveraging Sentinel Workbooks and Analytic Rules containing <b>Alert</b> and <b>Unified Logs</b> captured by Jamf Protect.	<a href="#">Jamf Protect for Microsoft Sentinel</a>	<a href="#">Jamf Protect</a>	Microsoft Sentinel	<b>"Sentinel Security works with Jamf.</b> The application and tie in with Jamf Protect can increase workflows and in a nutshell can help you win over SecOps with increased productivity and a deep insight to your device fleet security posture. Highly recommended." <b>- Dominic Vasquez</b>
Endpoint Telemetry Data Forwarding	By default, Macs collect all sorts of data about their performance and applications. While this can be a lot of information, we have the ability to filter it down to what they care about by using Jamf Protect, and send it onto their security tools for further use.	<a href="#">Integrating Jamf Protect with Microsoft Sentinel</a>	<a href="#">Jamf Protect</a>	Microsoft Sentinel	"Another example of how well the integration with Jam and Azure works!"  User-MrCcSti BF
Network Threat Stream Event Forwarding	The Network Traffic Stream enables organizations to stream, record and review all network activity that is processed by the service's infrastructure via third-party log aggregators and analytics tools. Events are sent in real time in a Common Event Format (CEF)-encoded syslog over Transport Layer Security (TLS) to ensure that the data is securely transported.  The Threat Events Stream can send events in real time as Common Event Format (CEF)-encoded syslogs or JSON-encoded HTTP events. Both streams can be integrated into Microsoft Sentinel.	<a href="#">Network Traffic Stream</a>  <a href="#">Threat Event Stream</a>	<a href="#">Jamf Protect and Jamf Connect</a>	Microsoft Sentinel	"Great integration with Azure and Sentinel. The tie in with Jamf Protect is so helpful."  Catherine Breese
Plugin for Security Copilot	With this plugin, a Security Admin can quickly query Jamf Pro device information following a security event in natural language, receiving inventory information via the chat interface without having to go into the Jamf Pro console.	<a href="#">How to integrate in Copilot for Security, How to integrate Jamf Pro</a>	<a href="#">Jamf Pro</a>	Microsoft Security Copilot	