jamf

Jamf and Microsoft – **Managing** and **Securing** Apple in the Enterprise

Member of Microsoft Intelligent Security Association

Microsoft

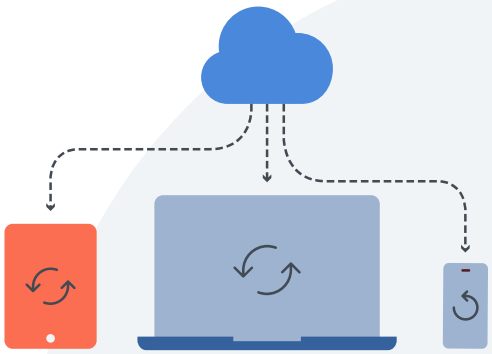
As organizations embrace remote work and an increasingly mobile and distributed workforce, **IT** and **Security leaders** face several growing challenges:

- How to manage and secure a network of devices and users with sensitive data being accessed from a range of locations
- How to consolidate tooling, do more with less, while at the same time increasing management and security capabilities

While many new advanced technologies have been developed to meet these modern challenges, many organizations still struggle to keep both users and data safe despite tools and solutions available that simplify transitioning to remote/hybrid work environments.

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



Additional security implications

Protecting an organization's most sensitive data and applications involves a complex set of variables today:

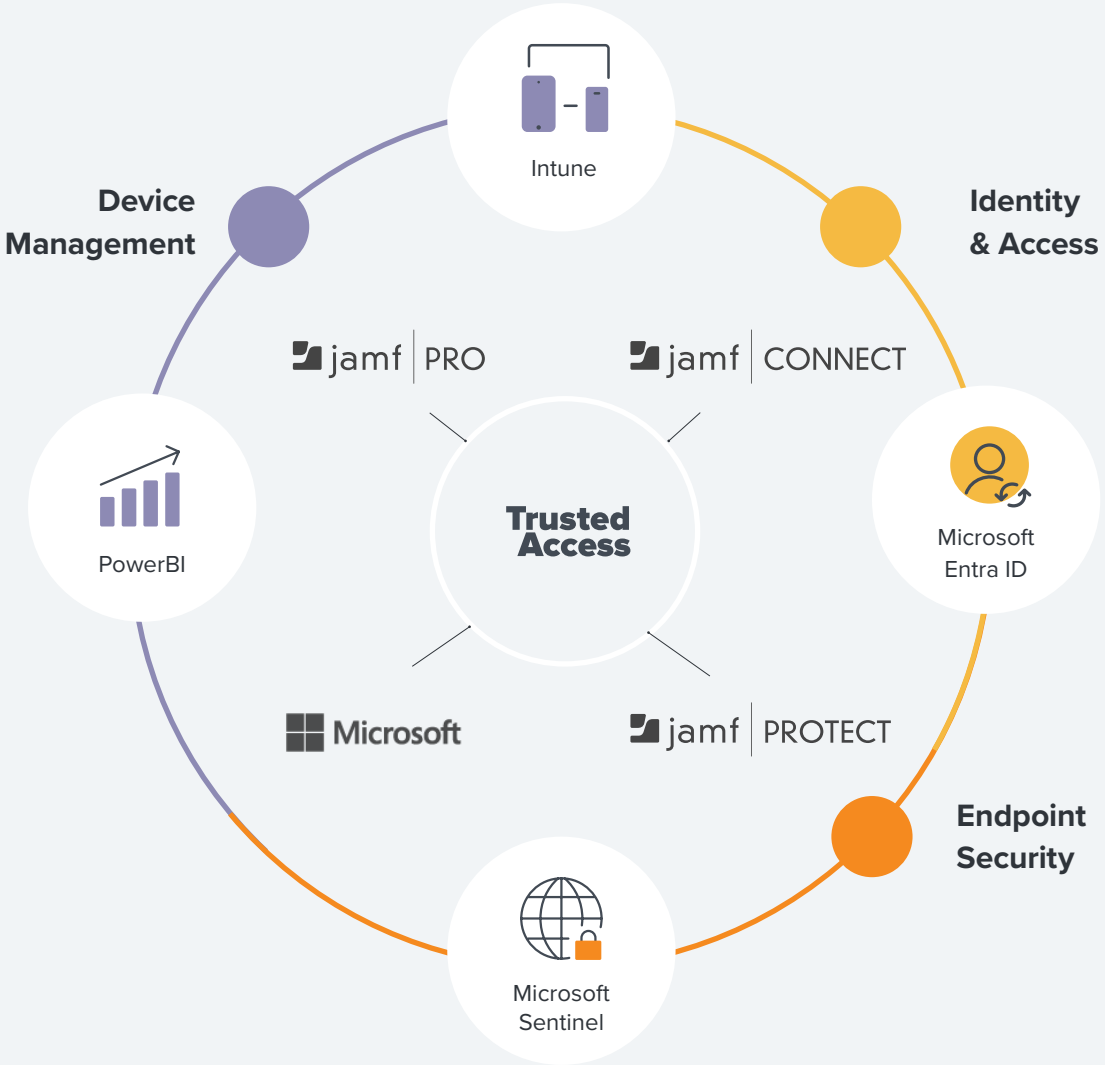
- Employee choice, mobile devices and BYOD introduce new requirements to manage and secure devices
- Modern platforms require modern solutions for verifying user identity and securely connecting to data
- New devices, use cases and regulatory compliance requirements introduce new risks

How Jamf + Microsoft solve these issues

Jamf is uniquely positioned to bring together the best of Apple device management, user identity and endpoint protection to deliver Trusted Access seamlessly with Microsoft. Trusted Access enables organizations to ensure that only authorized users on enrolled and secured devices can connect to business applications and data. Trusted Access requires 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 seamlessly achieves the Trusted Access paradigm, which is critical to the success of Apple at work, for organizations that rely on 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 Quote
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)	**Seamless Integration Between Jamf Pro and Microsoft Entra ID** "Easy-to-follow documentation provided by both Jamf and Microsoft. Most straight forward integration I have ever been involved in." I Borota
Device Inventory Reporting	Many IT admins enjoy a "single pane of glass" when managing Windows and Apple devices. This integration allows Jamf Pro to send a limited set of attributes to Intune for visibility in one place. NOTE: This integration is set to end by Microsoft in Sept 2024.	**Conditional Access**	**Jamf Pro**	Microsoft Intune (Microsoft Endpoint Manager)	"Intune, makes adding additional macOS registration for inventory purposes easy and clear to view and maintain. With the ability to setup quickly the additional compliance policy you can apply with a little knowledge of Intune is super helpful and helps keep the SecOps teams at bat, for a little while. Over all a good experience." Dominic Vasquez
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 PowerBi	**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 Quote
Device Compliance for macOS/ iOS	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 (Microsoft Endpoint Manager)	"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
Conditional Access for macOS	Organizations want to ensure that trusted users are on a compliant device before they allow them to access company materials (ex: OS updated, passcode enabled). This integration allows for a small number of inventory attributes to be forwarded from Jamf Pro to Microsoft Intune to get a yes/no status on whether that user can access that application. Depreciation Notice: Jamf supports a migration path to Device Compliance today that should be completed before Sept 1, 2024.	**Conditional Access**	**Jamf Pro**	Microsoft Entra ID and Intune (Microsoft Endpoint Manager)	**macOS in Windows environment** "As a Mac Integrator I am often involved in projects to insert macOS in Windows environments. The building blocks for this are the combination of Jamf Pro and Microsoft Entra ID. Conditional access and macOS compliance have never been so efficient." N Lecchi
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 Azure credentials.	**Configuring Single Sign-On with Active Directory Federation Services** **Microsoft Entra SSO integration with Jamf Pro**	**Jamf Pro**	Microsoft Entra ID and Intune (Microsoft Endpoint Manager)	**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 Azure credentials.	**Integrating with Microsoft Entra ID**	**Jamf Connect**	Microsoft Entra ID and Intune (Microsoft Endpoint Manager)	"Implementing was easy with the instructions given. SSO is a life changer." Tyler Verlato

Endpoint Security Integrations	Description	Product Documentation or Marketplace Listing	Jamf Product	Microsoft Product	Customer Quote
Jamf Protect for Microsoft Sentinel	The **Jamf Protect** 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 **Alert** and **Unified Logs** captured by Jamf Protect.	**Jamf Protect for Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	"**Sentinel Security works with Jamf.** 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." **- Dominic Vasquez**
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.	**Integrating Jamf Protect with Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	"Another example of how well the integration with Jam and Azure works!" User-MrCcStilBF
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.	**Network Traffic Stream** **Threat Event Stream**	**Jamf Protect** and **Jamf Connect**	Microsoft Sentinel	"Great integration with Azure and Sentinel. The tie in with Jamf Protect is so helpful." Catherine Breese
Plugin for Copilot for Security	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.	**How to integrate in Copilot for Security, How to integrate Jamf Pro**	**Jamf Pro, Jamf Protect**	Microsoft Copilot for Security	

jamf

www.jamf.com

To learn more about about the Microsoft and Jamf partnership, check out our Microsoft integrations page. To get started request a trial.