jamf

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

As organizations shift to 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

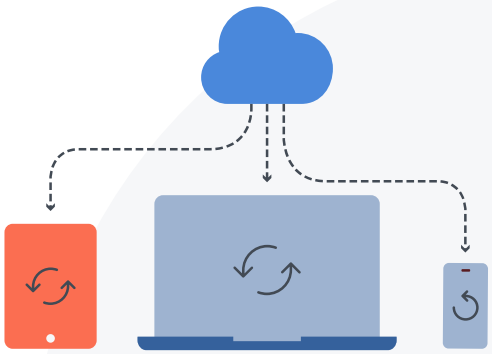
While many new advanced technologies have been developed to meet these modern challenges, many organizations still struggle to keep both users and data safe despite tools and solutions available that simplify transitioning to remote/hybrid work environments.

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

Member of
Microsoft
Intelligent
Security
Association

Microsoft



What additional challenges are there?

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

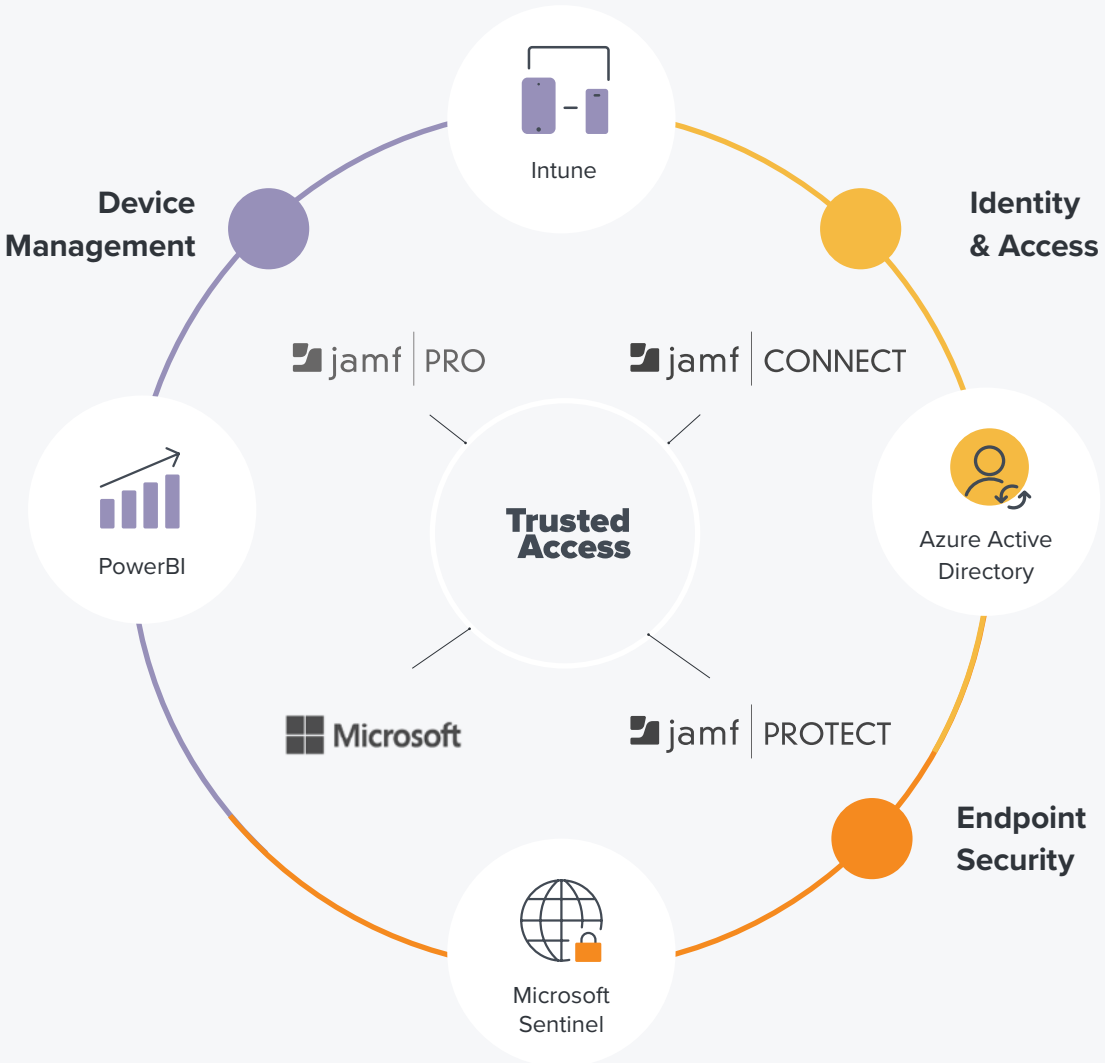
- Employee choice, mobile devices and BYOD introduce new requirements to manage and secure devices
- Modern platforms require modern solutions for verifying user identity and securely connecting to data
- New devices, use cases and regulatory compliance requirements introduce new risks

How Jamf + Microsoft solves 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.

Jamf is the perfect solution between what Apple provides and what organizations require. 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 an organization's users (name, email, role, etc.). This information can be used to ensure the right apps and settings get to the right end users. By pulling this information in, the Admin doesn't have to recreate this information manually.	**Integrating with LDAP Directory Services**	**Jamf Pro**	On Prem AD	
Cloud Identity Provider for Querying Users and Groups	Directory information about an organization's users (name, email, role, etc.). This information can be used to ensure the right apps and settings get to the right end users. By pulling this information in, the Admin doesn't have to recreate this information manually.	**Azure AD Integration**	**Jamf Pro**	Microsoft Azure AD and InTune (Microsoft Endpoint Manager)	**Seamless Integration Between Jamf Pro and Azure AD** "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	A lot of times you'll hear Admins say they'd love a "single pane of glass" when it comes to their fleets, especially if they're not all Windows or Apple. This allows for Jamf Pro to send a limited amount of macOS data to Intune for visibility on mixed fleet environments in one place.	**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	Go from data to insights in minutes with Power BI Desktop. 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 • Computer & Mobile Devices • Details • Applications • Extension Attributes • 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 (ex: OS updated, passcode enabled). This integration allows for Jamf Pro to verify if a device is compliant, and sends that yes/no status to Microsoft. *This is replacing Conditional Access in Jamf Pro 10.43	**Device Compliance**	**Jamf Pro**	Microsoft Azure AD 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 Azure ADD 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. *This is being deprecated and replaced by Device Compliance in Jamf Pro 10.43 (we will continue supporting this integration for one year after Microsoft deprecates the API)	**Conditional Access**	**Jamf Pro**	Microsoft Azure AD 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 Azure Active Directory. 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**	**Jamf Pro**	Microsoft Azure AD and InTune (Microsoft Endpoint Manager)	**Best IDP Integration** "Azure AD 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 Azure AD**	**Jamf Connect**	Microsoft Azure AD 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 solution creates detailed event data from macOS endpoints into a Microsoft Sentinel workspace in a simple and easy workflow. The solution provides you with full visibility into Apple Endpoint Security by leveraging Workbooks and Analytic Rules containing **Alert** and **Unified Logging** events captured by Jamf Protect and the **macOS built-in security events** that occurred across the protected organizational endpoints.	**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