



Jamf und Microsoft - Verwaltung und Absicherung von Apple im Unternehmen

Da Unternehmen auf moderne Arbeitsmethoden umsteigen, suchen IT- und Sicherheitsteams nach der besten Möglichkeit, die Nutzer:innen von Apple zu unterstützen.

Unternehmen stehen bei der Entwicklung einer Strategie für Apple häufig vor denselben Herausforderungen:

- Wie verwaltet und schützt man Geräte mit sensiblen Daten, auf die von überall her zugegriffen wird?
- Wie konsolidiert man Werkzeuge, um mit weniger mehr erreichen und gleichzeitig die Verwaltungs- und Sicherheitsfunktionen verbessern?
- Wie unterstützt man Mitarbeiterwahlprogramme, Mobilgeräte und BYO-Geräte?

Obwohl viele fortschrittliche Technologien entwickelt wurden, um diesen modernen Herausforderungen zu begegnen, haben Unternehmen immer noch Schwierigkeiten, die Sicherheit der Nutzer:innen und deren Daten zu gewährleisten.

Dies kann oft dazu führen, dass ...

- Das Konfigurieren einer umfassenden Sicherheit unnötig kompliziert ist
- die Benutzerfreundlichkeit leidet und der Verwaltungsaufwand steigt
- Sicherheitslücken entstehen, die sich nicht auf alle Geräte in der Infrastruktur erstrecken
- keine einheitlichen Kontrollen über sensible Unternehmensressourcen, einschließlich Daten, durchgeführt werden



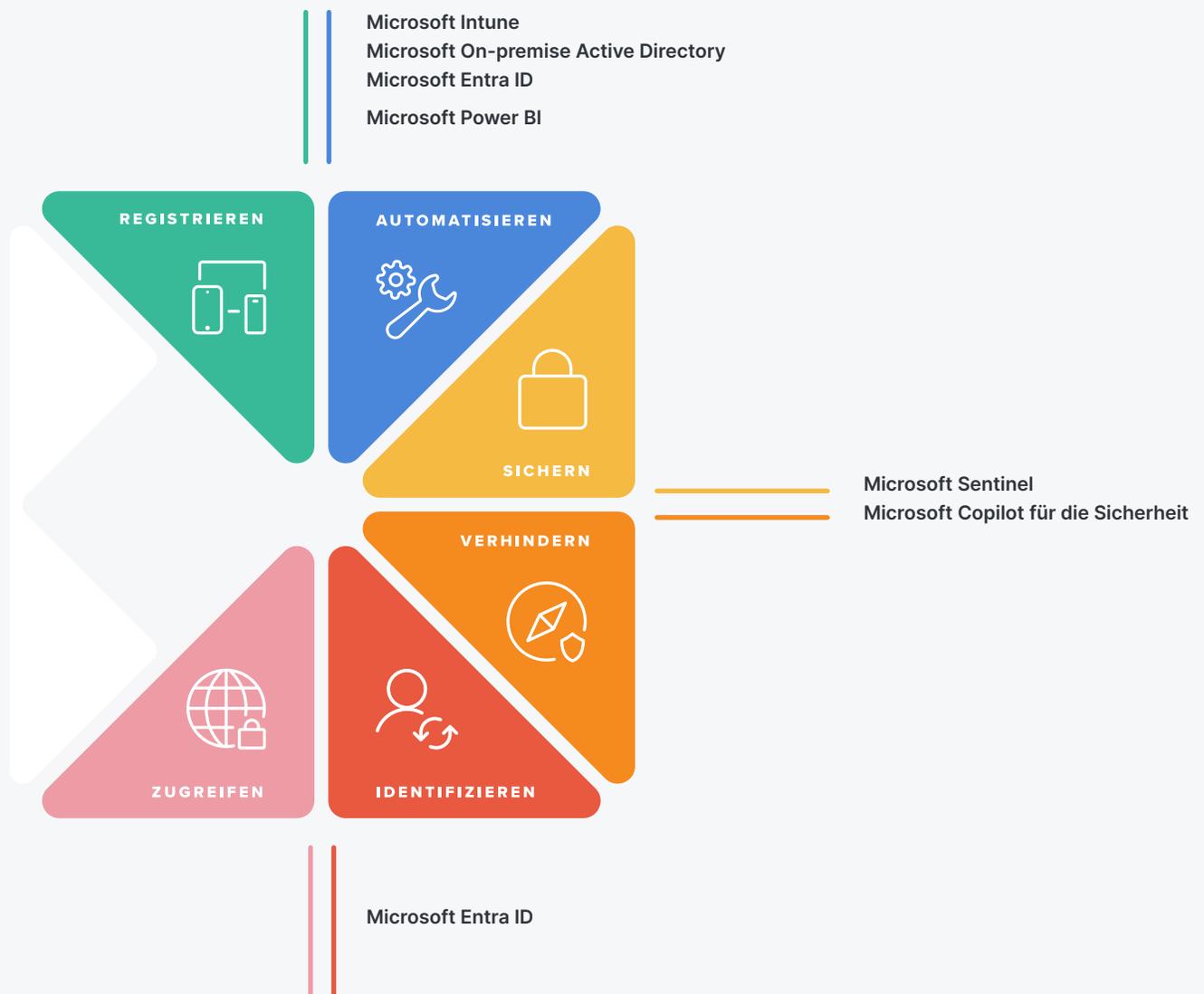
Wie Jamf + Microsoft Apple in Unternehmen, die Microsoft-Plattformen nutzen, effektiv unterstützen

Jamf hat sich so positioniert, um das Beste aus der Apple Geräteverwaltung, der Nutzeridentität und dem Endpoint-Schutz zu vereinen und so ein Apple-first Zero-Trust-Ergebnis mit Microsoft zu erzielen. Dadurch können Unternehmen sicherstellen, dass nur autorisierte Nutzer:innen mit registrierten und gesicherten Geräten auf Geschäftsapps und -daten zugreifen können. Um dieses Zero-Trust-Ergebnis zu erreichen, nutzen gemeinsame Kunden eine Integration mit einem Cloud Identity Anbieter (IdP), weshalb Jamf und Microsoft perfekt zusammenpassen. Der gesamte Datenverkehr wird durch Zero Trust Network Access

(ZTNA) kontrolliert, um eine sichere Remote-Konnektivität zu gewährleisten. Diese Lösung wurde entwickelt, um sich an die moderne Bedrohungslandschaft anzupassen und gleichzeitig die Schwächen älterer VPNs zu beheben.

Die Integration von Jamf und Microsoft ist der Schlüssel zum Erfolg mit Apple für Unternehmen, die Microsoft-Plattformen zur Steuerung ihrer Infrastruktur nutzen.

Schauen Sie sich die Integrationen an, die Jamf mit Microsoft anbietet, um Apple in Ihrem Unternehmen einfach zu verwalten.



Integrationen zur Geräteverwaltung	Beschreibung	Produktdokumentation oder Eintrag im Marketplace	Jamf Produkt	Microsoft Produkt	Kundenfeedback
LDAP für die Abfrage von Nutzer:innen und Gruppen	Verzeichnisinformationen über die Nutzer:innen der Organisation (Name, E-Mail, Rolle usw.) können verwendet werden, um sicherzustellen, dass die richtigen Apps und Einstellungen an die richtigen Endnutzer:innen gelangen. Admins müssen diese Informationen nicht manuell neu erstellen.	Integration mit LDAP-Verzeichnisdiensten	Jamf Pro	On-premise Active Directory	
Cloud Identity Anbieter für die Abfrage von Nutzer:innen und Gruppen	Informationen über die Nutzer:innen einer Organisation (Name, E-Mail, Rolle usw.) finden sich in Cloud IdP, die dazu verwendet werden können, um sicherzustellen, dass die richtigen Apps und Einstellungen für die richtigen Nutzer:innen und Geräte gelten. Die Konnektivität zu Jamf Pro erlaubt es den Admins, diese Informationen nicht manuell einfügen zu müssen.	Integration von Microsoft Entra ID	Jamf Pro	Microsoft Entra ID und Intune (Microsoft Endpoint Manager)	„Leichtverständliche Dokumentation, die sowohl von Jamf als auch von Microsoft bereitgestellt wird. Die einfachste Integration, an der ich je beteiligt war.“ I Borota
Dashboard Analytics Berichterstattung	Holen Sie sich kostenlos alles, was Sie brauchen, um unbegrenzt viele interaktive Berichte zu erstellen und zu speichern. Verwenden Sie die Power BI-Anwendung von Jamf Pro, um Ihre Jamf Bereitstellung auf eine tiefere Ebene der Datenanalyse zu bringen. Erweitern Sie die Berichtsfunktionen von Jamf Pro und erfassen Sie sie in Ihrer Power BI-Architektur. Daten verfügbar: Computer & Mobilgeräte, Details, Anwendungen, Erweiterungsattribute und Gruppe	Power BI	Jamf Pro	Microsoft Power BI	Power BI mit Jamf Pro „Power BI lässt sich nahtlos in Jamf Pro integrieren und liefert detaillierte Berichte über alle Aspekte Ihrer Jamf Pro Instanz. Man kann Berichte über verschiedene MacOS Versionen, Virendefinitionsversionen, Anzahl der Geräte pro Gebäude und vieles mehr erstellen. Wir sind begeistert von diesem Tool, weil es uns Daten liefert, mit denen wir arbeiten können.“ C McBride



Identitäts- und Zugangsintegration	Beschreibung	Produktdokumentation oder Eintrag im Marketplace	Jamf Produkt	Microsoft Produkt	Kundenfeedback
Geräte Compliance für iOS, iPadOS und macOS	<p>Unternehmen wollen sicherstellen, dass registrierte Nutzer:innen ein konformes Gerät verwenden, bevor sie ihnen den Zugriff auf Unternehmensressourcen gewähren. Durch diese Integration kann Jamf Pro überprüfen, ob ein Gerät kompatibel ist, und diesen Ja/Nein-Status an Microsoft senden.</p> <p>*Dies ersetzt den Conditional Access ab Jamf Pro 10.4</p>	<p>Geräte Compliance</p>	<p>Jamf Pro</p>	<p>Microsoft Entra ID und Intune</p>	<p>„Eine Integration, die sicherstellt, dass der Zugriff auf Bürodaten auf den Geräten erfolgt, die den Vorschriften entsprechen. Mithilfe der nahtlosen Integration zwischen Jamf und Microsoft Entra ID können wir diese Sicherheitsanforderung erfüllen. Ein Muss für die Umsetzung der Lösung unter dem Gesichtspunkt der Sicherheit.“</p> <p>Samstar777</p>
SSO für Cloud Identität	<p>Dies ermöglicht es den Admins einer Organisation, sich mit ihren Azure-Anmeldedaten bei ihrer Jamf Pro Instanz, dem Jamf macOS Security Cloud Portal und dem Jamf Security Cloud Portal anzumelden.</p>	<p>Konfigurieren von Single Sign-On mit Active Directory Federation Services</p> <p>Microsoft Entra SSO Integration mit Jamf Pro</p>	<p>Jamf Pro</p>	<p>Microsoft Entra ID und Intune</p>	<p>Beste IDP-Integration</p> <p>„Die Integration von Microsoft Entra ID funktioniert mit allem, was wir haben und was einen externen IDP unterstützt. Mit der Funktion des Cloud Identitätsanbieters für SSO in Jamf Pro und der Integration von Jamf Protect können Sie Ihre Unternehmensidentitäten problemlos mit Ihren Jamf Produkten und anderen Diensten von Drittanbietern verbinden.“</p> <p>T Ellis</p>
Cloudbasierte Identität für Mac	<p>Dies erlaubt es den Nutzer:innen in Ihrem Unternehmen, sich mit ihrer Entra ID bei ihrem Mac anzumelden.</p>	<p>Integration mit Microsoft Entra ID</p>	<p>Jamf Connect</p>	<p>Microsoft Entra ID und Intune</p>	<p>„Die Umsetzung war mit den gegebenen Anweisungen einfach. SSO verändert das Leben.“</p> <p>Tyler Verlato</p>

Member of
**Microsoft
Intelligent
Security
Association**



Integrationen für den Endpoint-Schutz	Beschreibung	Produktdokumentation oder Eintrag im Marketplace	Jamf Produkt	Microsoft Produkt	Kundenstimmen
Jamf Protect für Microsoft Sentinel	Die Integration von Jamf Protect für Microsoft Sentinel sendet detaillierte Ereignisdaten von macOS Geräten in einem einfachen und unkomplizierten Workflow an Microsoft Sentinel. Dies verschafft den Sicherheitsteams Sichtbarkeit für einzelne Sicherheitsereignisse auf Macs, indem sie Sentinel-Arbeitsmappen und analytische Regeln mit Warnmeldungen und Unified Logs nutzen, die von Jamf Protect erfasst wurden.	Jamf Protect für Microsoft Sentinel	Jamf Protect	Microsoft Sentinel	„ Sentinel Security arbeitet mit Jamf. Die App und die Verknüpfung mit Jamf Protect können die Arbeitsabläufe verbessern und, kurz gesagt, Ihnen helfen, SecOps durch erhöhte Produktivität und einen tiefen Einblick in die Sicherheitslage Ihrer Geräteflotte zu gewinnen. Äußerst empfehlenswert.“ - Dominic Vasquez
Weiterleitung von Endpoint-Telemetriedaten	Macs sammeln standardmäßig alle möglichen Daten über ihre Leistung und Programme. Das können zwar viele Informationen sein, aber wir können sie mit Jamf Protect auf das Wesentliche beschränken und sie zur weiteren Verwendung an ihre Sicherheitstools weiterleiten.	Integration von Jamf Protect mit Microsoft Sentinel	Jamf Protect	Microsoft Sentinel	„Ein weiteres Beispiel dafür, wie gut die Integration mit Jamf und Azure funktioniert!“ Benutzer-MrCcSti BF
Network Threat Stream Event Weiterleitung	Der Threat Events Stream ermöglicht Unternehmen das Streamen, Aufzeichnen und Überprüfen aller Netzwerkaktivitäten, die von der Infrastruktur des Dienstes über Protokollaggregatoren und Analysetools von Drittanbietern verarbeitet werden. Ereignisse werden in Echtzeit in einem Common Event Format (CEF)-kodierte Syslog über Transport Layer Security (TLS) gesendet, um sicherzustellen, dass die Daten sicher transportiert werden. Der Threat Events Stream kann Ereignisse in Echtzeit als Common Event Format (CEF)-kodierte Syslogs oder JSON-kodierte HTTP-Ereignisse senden. Beide Streams können in Microsoft Sentinel integriert werden.	Network Traffic Stream Threat Event Stream	Jamf Protect und Jamf Connect	Microsoft Sentinel	„Großartige Integration mit Azure und Sentinel. Die Verbindung mit Jamf Protect ist sehr hilfreich.“ Catherine Breese
Plug-in für Security Copilot	Mit diesem Plug-In können Jamf Pro Geräteinformationen von Sicherheitsadmins in natürlicher Sprache abgefragt und Bestandsinformationen über eine Chat-Funktion abgerufen werden, ohne dass eine Anmeldung in die Jamf Pro Konsole erforderlich ist.	Integration in Copilot für Sicherheit, Integration von Jamf Pro	Jamf Pro	Microsoft Copilot für die Sicherheit	

