

Den Microsoft Stack für Apple vervollständigen.

Jamf verbindet Apple Geräteverwaltung und Sicherheit mit Microsoft Sentinel, Entra und Intune. So erhalten IT- und Sicherheitsteams ***vollständige Transparenz*** *über jedes Apple Gerät – an jedem Ort.*

Microsoft Solutions Partner

Unternehmen, die Apple Geräte in Microsoft Umgebungen verwalten, kämpfen mit Sicherheitslücken. Entscheidungen zu Identität und Zugriff sind nur so belastbar wie die Gerätesignale, auf denen sie beruhen. Ohne tiefgehende, Apple-native Konformitätsdaten kann bedingter Zugriff die Zero-Trust-Prinzipien nicht flottenweit durchsetzen.

Sicherheitsteams, die Mac, iPhone und Windows Geräte verwalten, arbeiten oft mit einem unvollständigen Bild, da generische, plattformübergreifende Werkzeuge Apple-spezifische Telemetrie nur unzureichend erfassen. Tools, die vor allem für Windows Umgebungen entwickelt wurden, erfordern zudem manuelle Behelfslösungen und erreichen Apple Geräte erst mit Verzögerung.

Generische Verwaltung treibt die Kosten, ohne einen entsprechenden Gegenwert zu liefern. Und wenn Unternehmen ihren Apple Bestand ausbauen, unterbrechen uneinheitliche Authentifizierung und uneinheitliches Onboarding zusätzlich die Produktivität.

Jamf + Microsoft = eine Plattform für Apple

Gemeinsam bieten Microsoft und Jamf ihren Kunden einen einheitlichen, durchgängigen und integrierten Stack, der die gesamte Belegschaft unterstützt. IT-Teams erhalten einheitliche Transparenz, Sicherheitsteams lückenlose Abdeckung – und Endbenutzer nahtloses Onboarding sowie ein reibungsloses Arbeitserlebnis im Alltag, auf jedem Apple Gerät und an jedem Standort.

Gemeinsam besser. Von Grund auf.

Funktionsbereich	Kurze Vorteilsbeschreibung
Apple unternehmensweit bereitstellen und verwalten	Geräte kommen konfiguriert, konform und einsatzbereit an. Die vollautomatische Bereitstellung nutzt die Anmeldedaten aus Microsoft Entra ID und Apple School Manager.
Konformität in Echtzeit mit Entra ID	Apple-native Konformitätssignale fließen in den bedingten Zugriff von Microsoft Entra ein. Ist ein Gerät einem Risiko ausgesetzt, wird der Zugriff automatisch eingeschränkt.
Nahtlose Identität für alle Benutzer:innen	Benutzer:innen melden sich mit ihren Anmeldedaten aus Microsoft Entra ID an. Jamf automatisiert die Account-Bereitstellung und die FileVault-Verschlüsselung.
Umfassende Apple Transparenz in Microsoft Sentinel	Apple-native Telemetrie fließt direkt in Sentinel. Sicherheitsteams erhalten damit eine einheitliche Sicht auf Mac, Mobilgeräte und Windows.
Einheitlicher Sicherheitsbetrieb mit Security Copilot	Das Plug-in von Jamf zeigt den Kontext von Apple Geräten direkt im Workflow der Analyst:innen und beschleunigt so Untersuchung und Reaktion.

Ergebnisse für Kunden

- Konformitäts- und Transparenzlücken bei Apple im Microsoft Stack schließen
- IT-Abläufe vereinfachen – mit vollautomatischer Bereitstellung und automatisierter Durchsetzung
- Mitarbeitererlebnis verbessern – ohne Abstriche bei der Sicherheit





Integrationen zur Geräteverwaltung	Beschreibung	Produktdokumentation oder Marketplace-Eintrag	Jamf Produkt	Microsoft Produkt	Kundenfeedback
LDAP für die Abfrage von Benutzer:innen und Gruppen	Verzeichnisinformationen über die Benutzer:innen der Organisation (Name, E-Mail, Rolle usw.) können verwendet werden, um sicherzustellen, dass die richtigen Apps und Einstellungen die richtigen Endnutzer:innen erreichen. Administrator:innen müssen diese Informationen nicht manuell neu erstellen.	**Integration mit LDAP-Verzeichnisdiensten**	**Jamf Pro**	Lokal bereitgestelltes Active Directory	
Cloudbasierter Identitätsdienst zum Abfragen von Benutzern und Gruppen	Informationen zu den Benutzer:innen eines Unternehmens (Name, E-Mail, Rolle usw.) liegen inzwischen im cloudbasierten Identitätsdienst. So gelangen die richtigen Apps und Einstellungen zu den richtigen Benutzer:innen und Geräten. Werden diese Informationen mit Jamf Pro verbunden, entfällt die manuelle Eingabe für Administrator:innen.	**Microsoft Entra ID Integration**	**Jamf Pro**	Microsoft Entra ID und Intune (Microsoft Endpoint Manager)	„Die Dokumentation von Jamf und Microsoft ist leicht verständlich. Das war die unkomplizierteste Integration, an der ich je beteiligt war." I Borota
Dashboard-Analyse und Berichterstattung	Alles, was Sie zum Erstellen und Speichern unbegrenzt vieler interaktiver Berichte brauchen – kostenlos. Mit der Jamf Pro Power BI App vertiefen Sie die Datenanalyse für Ihre Jamf Bereitstellung. Sie erweitern damit die Berichtsfunktionen von Jamf Pro und binden sie in Ihre Power BI Architektur ein. Verfügbare Daten: Computer und Mobilgeräte, Details, Apps, Erweiterungsattribute und Gruppen	**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 zu allen Aspekten Ihrer Jamf Pro Instanz. Sie können Berichte zu macOS Versionen, Versionen von Virendefinitionen, Anzahl der Geräte pro Gebäude und vielem mehr einrichten. Ein großartiges Tool, das uns Daten liefert, mit denen wir arbeiten können." C McBride



Integrationen für Identität und Zugriff	Beschreibung	Produktdoku-mentation oder Marketplace-Eintrag	Jamf Produkt	Microsoft Produkt	Kundenfeedback
Gerätekonfor-mität für iOS, iPadOS und macOS	Organisationen möchten sicherstellen, dass vertrauenswürdige Benutzer ein konformes Gerät verwenden, bevor sie ihnen den Zugriff auf Unternehmensressourcen erlauben. Mit dieser Integration kann Jamf Pro die Konformität eines Geräts überprüfen und den Ja/Nein-Status an Microsoft übermitteln. *Ersetzt den bedingten Zugriff ab Jamf Pro 10.4	**Gerätekonfor-mität**	**Jamf Pro**	Microsoft Entra ID und Intune	„Eine Integration, die sicherstellt, dass nur konforme Geräte Zugriff auf Office-Daten erhalten. Die nahtlose Integration zwischen Jamf und Microsoft Entra ID hilft uns, diese Sicherheitsanforderung zu erfüllen. Aus Sicherheitsperspektive eine unverzichtbare Lösung.“ Samstar777
SSO für Cloud Identity	Damit können sich die Administrator:innen einer Organisation mit ihrer Entra ID bei ihrer Jamf Pro Instanz, dem Jamf macOS Security Cloud Portal und dem Jamf Security Cloud Portal anmelden.	**Konfigurieren von Single Sign-On mit Active Directory Federation Services** **Microsoft Entra SSO Integration mit Jamf Pro**	**Jamf Pro**	Microsoft Entra ID und Intune	**Beste IdP-Integration** „Microsoft Entra ID lässt sich mit allem verbinden, was bei uns einen externen Identitätsdienst unterstützt. Die Funktion ‚Cloudbasierter Identitätsdienst‘ für SSO in Jamf Pro und die Integration für Jamf Protect bringen Ihre Unternehmensidentitäten mühelos in Ihre Jamf Produkte und in andere Dienste von Drittanbietern.“ T Ellis
Cloud-basierte Identität für Mac	Endbenutzer:innen einer Organisation können sich mit ihrer Entra ID an ihrem Mac anmelden.	**Integration mit Microsoft Entra ID**	**Jamf Connect**	Microsoft Entra ID und Intune	„Die Einrichtung war dank der bereitgestellten Anleitung einfach. SSO verändert alles.“ Tyler Verlato

Member of
Microsoft
Intelligent
Security
Association

Microsoft



Integrationen für Endpunktsicherheit	Beschreibung	Produktdokumentation oder Marketplace-Eintrag	Jamf Produkt	Microsoft Produkt	Kundenstimmen
Jamf Protect für Microsoft Sentinel	Die Integration **Jamf Protect** für Microsoft Sentinel übermittelt detaillierte Ereignisdaten von macOS Geräten über einen einfachen Workflow an Microsoft Sentinel. Sicherheitsteams gewinnen so Transparenz über spezifische Sicherheitsereignisse auf Macs – mithilfe von Sentinel Workbooks und Analyseregeln, die von Jamf Protect erfasste **Warnhinweise** und **Unified Logs** enthalten.	**Jamf Protect für Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	„**Sentinel Security funktioniert mit Jamf.** Die Anwendung und die Anbindung an Jamf Protect verbessern die Workflows und helfen Ihnen, kurz gesagt, das SecOps-Team zu überzeugen – durch höhere Produktivität und tiefe Einblicke in den Sicherheitsstatus Ihrer Geräteflotte. Sehr empfehlenswert.“ **- Dominic Vasquez**
Weiterleitung von Endpunkt-Telemetriedaten	Macs erfassen standardmäßig zahlreiche Daten zu ihrer Leistung und zu ihren Apps. Das kann zwar eine große Menge an Informationen sein. Mit Jamf Protect filtern Sie diese jedoch auf das Wesentliche und leiten sie zur weiteren Verwendung an Ihre Sicherheitstools weiter.	**Integration von Jamf Protect mit Microsoft Sentinel**	**Jamf Protect**	Microsoft Sentinel	„Noch ein Beispiel dafür, wie gut die Integration von Jamf und Azure funktioniert!“ User-MrCcSti|BF
Weiterleitung von Ereignissen des Network Threat Stream	Mit dem Network Traffic Stream können Organisationen sämtliche Netzwerkaktivitäten, die von der Infrastruktur des Dienstes verarbeitet werden, über Log-Aggregatoren und Analysetools von Drittanbietern streamen, aufzeichnen und überprüfen. Ereignisse werden in Echtzeit als CEF-codiertes Syslog (Common Event Format) über Transport Layer Security (TLS) gesendet, um eine sichere Übertragung der Daten zu gewährleisten. Der Threat Events Stream kann Ereignisse in Echtzeit als CEF-codierte Syslogs (Common Event Format) oder als JSON-codierte HTTP-Ereignisse senden. Beide Streams lassen sich in Microsoft Sentinel integrieren.	**Network Traffic Stream** **Threat Event Stream**	**Jamf Protect** und **Jamf Connect**	Microsoft Sentinel	„Großartige Integration mit Azure und Sentinel. Die Anbindung an Jamf Protect ist wirklich hilfreich.“ Catherine Breese
Plug-In für Security Copilot	Mit diesem Plug-In können Sicherheitsadministrator:innen nach einem Sicherheitsereignis Geräteinformationen aus Jamf Pro schnell in natürlicher Sprache abfragen und Bestandsinformationen über die Chat-Oberfläche erhalten – ohne die Jamf Pro Konsole öffnen zu müssen.	**Integration in Security Copilot, Integration von Jamf Pro**	**Jamf Pro**	Microsoft Security Copilot	

jamf

www.jamf.com/de/

© 2002–2026 Jamf, LLC. Alle Rechte vorbehalten.

Mehr über die Partnerschaft von Microsoft und Jamf erfahren Sie auf unserer Seite zu den Microsoft Integrationen. Für den Einstieg können Sie eine Testversion anfordern.