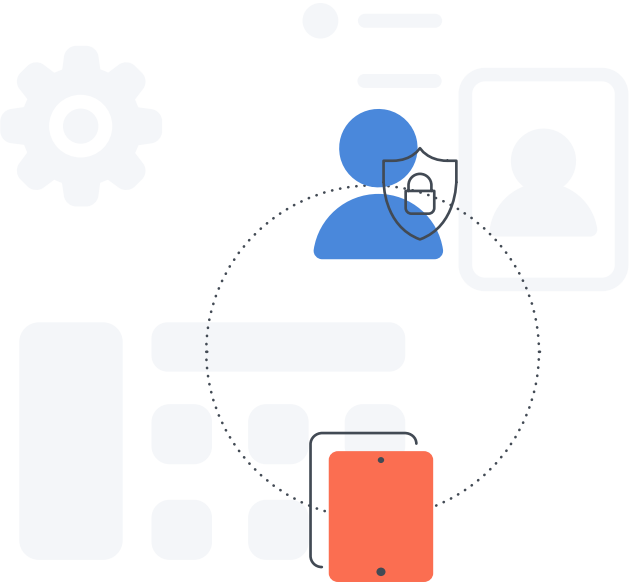
Schritte zur Erfüllung der Microsoft Enterprise Compliance

Geräte-Compliance für iOS und macOS erweitert die Partnerschaft zwischen Jamf und Microsoft und unterstützt die gesamte Apple Unternehmensflotte.

Arbeiten im Homeoffice, Fernunterricht und Telemedizin - die Sicherheit von Mobilgeräten ist jetzt wichtiger denn je. Ganz gleich, ob Ihr Unternehmen Patient*innen auf dem Flur versorgt oder Mitarbeiter*innen auf der ganzen Welt unterstützt, Geräte sind oft ein wichtiger Bestandteil Ihrer Produktivitätsstrategie. Immer weniger Unternehmen nutzen ausschließlich Windows und immer mehr bieten ihren Mitarbeiter*innen Wahlprogramme für ihre Arbeitsgeräte an. Daher ist es an der Zeit, Sicherheits-Workflows für Apple zu etablieren, die über den Sicherheits-Standard für Windows-Geräte hinausgeht.
Die Geräte-Compliance für iOS und iPadOS (allgemein als Device Compliance für iOS bezeichnet) sowie die Geräte-Compliance für macOS sind ein wichtiger Bereich der Partnerschaft von Jamf mit Microsoft.



Mehr erfahren:

Diese Microsoft-Integration folgt auf die proxyfreie Zugangskontrolle für Mac, die von Jamf und Microsoft Enterprise Mobility + Security ermöglicht wird.

Alle Details zu Mac Workflows von Microsoft und Jamf

Die Entwicklung der Partnerschaft zwischen Jamf und Microsoft

2017

Jamf und Microsoft haben eine einzigartige Partnerschaft angekündigt, um Conditional Access auf den Mac zu bringen. Die Partnerschaft zwischen Jamf und Microsoft Enterprise Mobility + Security (EMS) bietet eine automatisierte Compliance-Management-Lösung für Mac Geräte, die auf Apps zugreifen, die mit Entra ID-Authentifizierung eingerichtet wurden. Bei dieser Zusammenarbeit wird der Conditional Access genutzt, um sicherzustellen, dass nur vertrauenswürdige Benutzer*innen auf Unternehmensdaten zugreifen können.

2018

Jamf erweiterte seine Integration, um eine nahtlosere Anmeldeerfahrung für Endbenutzer*innen zu schaffen. Die Integration von Jamf und Microsoft Technologie bietet Endbenutzer*innen eine nahtlosere Login-Erfahrung. Mit Jamf Pro, Jamf Connect und Microsoft Enterprise Mobility + Security (EMS) können sich Benutzer*innen mit Microsoft Entra ID-Anmeldedaten bei einem neuen Mac anmelden, wodurch die Erstellung und Verwaltung eines lokalen Benutzernamens und Kennworts auf dem Mac eines Endbenutzers/einer Endbenutzerin entfällt.

2020

Jamf baute seine Partnerschaft mit Microsoft weiter aus und brachte als erster Anbieter Zugangskontrollsysteme für mobile Apple Geräte auf den Markt. Unternehmen genießen bereits die Möglichkeit, Conditional Access auf macOS Geräte zu nutzen, indem Bestandsdaten aus Jamf mit Microsoft Endpoint Manager geteilt werden. Die erweiterte Zusammenarbeit zwischen Jamf und Microsoft wird um iOS Unterstützung ergänzt. IT-Teams können jetzt verhindern, dass ein autorisierter Benutzer/eine autorisierte Benutzerin ein macOS oder iOS Gerät verwendet, das nicht mit den Sicherheitsrichtlinien konform ist, und können Jamf Self Service nutzen, um alle Apple Geräte zu schützen und zu unterstützen.

2021

Ein bedeutender Schritt in der Sicherheitspartnerschaft wurde durch die Integration von Microsoft Sentinel und Jamf Protect gemacht, um Apple spezifische Bedrohungsdaten in Echtzeit direkt in das bevorzugte SIEM-Tool für IT und Sicherheit in einer Microsoft-Umgebung zu übertragen.

2023

Jamf wird Mitglied der Microsoft Intelligence Security Association (MISA), einem Ökosystem von unabhängigen Softwareanbieter*innen und Anbieter*innen von verwalteten Sicherheitsdiensten, die sich in Microsoft Security integriert haben, um sich gegen die zunehmenden Cybersecurity-Bedrohungen zu schützen. Mit einer gemeinsamen Vision für Apple Sicherheit wurde Jamf als MISA-Mitglied für unsere Integrationen anerkannt, die eine effektive Geräteverwaltung, einen sicheren Zugang zu Unternehmensressourcen und Endpoint-Sicherheit für Apple am Arbeitsplatz unterstützen.

Wer iOS Geräte-Compliance benötigt

iOS Geräte-Compliance ist für alle gedacht. Unternehmen mit hybriden Umgebungen, Unternehmen mit unterschiedlichen Leiter*innen für IT- und Informationssicherheitsteams, jedes Unternehmen mit Apple und Microsoft Geräten wird von der Geräte-Compliance für iOS profitieren.
Unternehmen haben bereits die Möglichkeit, Conditional Access auf macOS Geräten zu nutzen, indem sie Inventardaten von Jamf mit Microsoft Intune teilen. IT-Teams können jetzt verhindern, dass ein autorisierter Benutzer/eine autorisierte Benutzerin jedes beliebige iOS Gerät verwendet, das nicht den Sicherheitsrichtlinien ihres Unternehmens entspricht, und können Jamf Self Service für die Problembehebung nutzen.

Wie es funktioniert

Compliance-Kriterien festlegen:
Mit Geräte-Compliance können Administrator*innen Compliance-Kriterien festlegen, um sicherzustellen, dass iOS und macOS Geräte Sicherheitsstandards erfüllen, bevor sie auf Unternehmensressourcen zugreifen.

Umfang der Compliance-Kriterien bestimmen:
Jamf Pro nutzt patentierte Smart Groups, um die Compliance-Kriterien einzugrenzen, prüft die Compliance des Geräts und gibt dann ein „konform / nicht konform”-Flag zurück an Microsoft Entra ID.

Compliance-Meldung:
Die von Jamf gesammelten Geräteinformationen werden dann an Entra ID gesendet. Da Entra ID die von Jamf Pro gescannten Informationen im Gerätedatensatz speichert und die Kennzeichnung liest, bevor der Zugriff auf Unternehmensressourcen wie OneDrive, Outlook usw. gewährt wird, sind die Vermögenswerte, Daten und Ressourcen des Unternehmens besser geschützt und sicherer.

Abhilfe schaffen:
Wird ein Gerät als „nicht konform“ gekennzeichnet, wird der Zugriff verweigert und es müssen Maßnahmen getroffen werden, bevor der Endbenutzer/die Endbenutzerin den Vorgang fortsetzen kann. Der Endbenutzer/die Endbenutzerin, dessen Zugriff verweigert wurde, wird an Jamf Self Service weitergeleitet, um mit dem Prozess zu beginnen, damit er wieder richtlinienkonform wird.

Was anfangs benötigt wird

- Jamf Pro integriert mit Microsoft Intune
- Smart Group mit Geräten, die auf Compliance überwacht werden sollen
- Jamf Pro Benutzerkonto mit Berechtigungen für Conditional Access
- Richtlinie für Conditional Access, die vorgibt, dass Geräte als konform gekennzeichnet werden müssen, um auf die Ressourcen des Unternehmens zugreifen zu können
- Microsoft Enterprise Mobility + Security (speziell Microsoft AAD Premium und Microsoft Intune)

Um die Geräte-Compliance überwachen zu können, benötigen die Geräte:

- Jamf Pro 10.29.0 oder höher, gehostet in Jamf Cloud
- Ein Jamf Pro Benutzerkonto mit Geräte-Compliance Rechten
- iOS 11 oder höher, oder iPadOS 13 oder höher und macOS 10.11 oder höher
- Microsoft Authenticator App (verfügbar im App Store) für iOS und iPadOS
- Jamf Self Service für iOS 10.10.3 oder neuer
- Neueste Version der App Microsoft Intune Company Portal für macOS

Auf die Plätze, fertig, Compliance

Unternehmen weltweit wird Zero-Trust-Geräte-Compliance immer wichtiger. Weil die Technologieerfahrung aufgrund der Telearbeit im Prinzip die gesamte Mitarbeitererfahrung ausmacht, kann die Bedeutung von Compliance und Sicherheit gar nicht überbetont werden.
iOSGeräte-Compliance mit Apple und Microsoft – den Standards in Unternehmen – sorgt für die Verbesserung der Sicherheit und Verwaltung Ihrer iOS Geräte, stellt die Geräte-Compliance sicher und unterstützt alle Apple Geräte in Ihrem Unternehmen.

Beginnen Sie noch heute

Aktuelle Kund*innen, die Jamf Cloud nutzen, sehen diese Integration in Jamf Pro als „iOS Geräte-Compliance“ im Menü „Globale Verwaltung“. Weitere Informationen über dieses neue Feature finden Sie in unserem **technischen Leitfaden.**
Falls Sie noch kein Jamf Kunde/keine Jamf Kundin sind, können Sie eine kostenlose Testversion anfordern, oder kontaktieren Sie Ihren bevorzugten Apple Partner.

Testversion anfordern