

Jamf und Google – Verwaltung und Schutz von Apple Geräten für Cloud-native Organisationen

*Bei Unternehmen, die eine große Auswahl an Geräten und eine flexible Arbeitsweise anbieten, besteht die Herausforderung für Führungskräfte im Bereich Technologie darin, **effiziente, sichere und skalierbare Abläufe** zu gewährleisten, ohne das Benutzererlebnis zu beeinträchtigen.*



Die Nutzung von Apple in einem Unternehmen sollte eine strategische Entscheidung sein, kein Kompromiss. Wenn Organisationen Apple Geräte für ihre Arbeitskräfte anbieten, benötigen sie Tools, die speziell für die Plattform entwickelt wurden. Es ist hilfreich, wenn Tools für die Produktivität wie Google Workspace plattformübergreifend eingesetzt werden können, aber wenn es um Verwaltung und Sicherheit geht, ist ein umfassendes Know-how über die Plattform entscheidend.

Werden Windows-orientierte oder plattformübergreifende Tools für den Support von Apple eingesetzt, entstehen häufig Reibungspunkte, unnötige Komplexität und Sicherheitslücken:

1. Aufgeblähte Endpunktagenten, die die Leistung beeinträchtigen.
2. Traditionelle VPNs vergrößern die Angriffsfläche und frustrieren die Benutzer.
3. Unzureichend verwaltete macOS- und iOS-Endpunkte mit schlechter Sichtbarkeit.

Plattformspezifische Tools gelten als bewährte Grundlage für den langfristigen Erfolg eines Geräteprogramms. Der Umstieg von herkömmlichen Management-Stacks auf speziell entwickelte Apple Lösungen stärkt die Benutzer und macht die Investitionen Ihres Unternehmens in das Google-Ökosystem sichtbar.

Jamf bietet die einzige Apple first-Lösung, die umfassend in Google Workspace, Chrome Enterprise, Google Cloud Identity und Google Security Operations integriert ist. Das Ergebnis? Ein optimiertes Zero-Trust-Ökosystem, das für interne IT- und Sicherheitsteams in Cloud-orientierten Organisationen entwickelt wurde.

Google und Jamf arbeiten zusammen, damit Unternehmen jeder Größe sich verbinden, kreativ sein, zusammenarbeiten und sicher arbeiten können.

Gemeinsam bieten Jamf und Google eine hohe Produktivität und eine gute Zusammenarbeit für Apple Benutzer, wobei alles durch ein identitätsgesteuertes Zero-Trust-Ergebnis für Apple im Unternehmen geschützt ist.

Dadurch können Unternehmen sicherstellen, dass nur autorisierte Benutzer mit registrierten und gesicherten Geräten auf Geschäftsapps und -daten zugreifen können. Diese Geräte werden durch eine robuste Verwaltung, Netzwerkkontrollen und Endpunktsicherheit geschützt. Der gesamte Datenverkehr wird über Zero-Trust-Netzwerkzugriff (ZTNA) für einen sicheren, skalierbaren Zugang aus der Ferne geregelt.

Jamf und Google haben seit langem die gemeinsame Vision, klassische VPNs durch moderne, mehrschichtige Sicherheitslösungen zu ersetzen. Gemeinsam bieten wir ein

nahtloses, Apple first Zero-Trust-Erlebnis, das auf die Bedürfnisse der heutigen Unternehmen mit einer hybriden Arbeitsweise zugeschnitten ist.

Mit Google Workspace, das eine sichere Zusammenarbeit und Produktivität ermöglicht, und Chrome, das ein sicheres, richtliniengesteuertes Browsing auf Macs und mobilen Geräten bietet, können die Unternehmen ihre Apple Benutzer mit erstklassiger Verwaltung und Sicherheit unterstützen.

Durch die Kombination von Jamf mit den Cloud-basierten Produktivitäts-Tools und dem sicheren Browsing von Google können Unternehmen eine Zero-Trust-Strategie umsetzen, bei der Apple im Mittelpunkt steht. Dieser integrierte Ansatz schützt nicht nur Benutzer und Daten, sondern unterstützt die Belegschaft auch, flexibel, sicher und produktiv zu arbeiten, egal wo sie sich befinden.

Integrierte Zero-Trust Sicherheit, powered by Jamf und Google



Übersicht über die Integration	Beschreibung	Produktdokumentation oder Eintrag im Marketplace	Jamf Produkt	Google Produkt
Sicher LDAP für die Abfrage von Benutzern und Gruppen	Verzeichnisinformationen über die Benutzer einer Organisation (Name, E-Mail-Adresse, Rolle usw.). Diese Informationen können verwendet werden, um sicherzustellen, dass die richtigen Apps und Einstellungen an die richtigen Endbenutzer gelangen. Durch das Abrufen dieser Informationen muss der Admin diese Informationen nicht manuell neu erstellen.	Integration mit Google Secure LDAP	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity
Integrationen für Google Context Aware Access	Mithilfe der Integration können mobile und Mac Geräte den von Jamf festgelegten Compliance-Status mit BeyondCorp zu teilen. Sie können den Zugang zu Apps, die durch Context-Aware-Richtlinien geschützt sind, beschränken.	Google BeyondCorp Enterprise	Jamf Pro, Jamf Connect	Google Workspace, Google Cloud Identity, Google Cloud
Aktivierung von Chrome Enterprise Core und Premium	Chrome Enterprise verfügt über Funktionen, von denen ein Unternehmen in großem Umfang profitiert. Jamf Pro und Jamf School können dazu beitragen, die Unternehmensfunktionen in Google Chrome zu aktivieren.	Registrierung von Browsern auf macOS mit Jamf Pro Registrierung von Browsern auf Mobilgeräten mit Jamf Pro	Jamf Pro, Jamf School	Chrome Enterprise
SSO für Cloud Identity	Dadurch können sich die Admins in einem Unternehmen mit ihren Google-Anmeldedaten bei ihrer Jamf Pro Instanz, dem Jamf macOS Security Cloud Portal und dem Jamf Security Cloud Portal anmelden.	Konfiguration von Single Sign-On mit Google Workspace	Jamf Account	Google Workspace, Google Cloud Identity
Cloud-basierte Identität für Mac	Dadurch können sich die Endbenutzer eines Unternehmens mit ihren Google-Zugangsdaten bei ihrem Mac anmelden. Das Gleiche ist auch auf dem Chromebook oder bei Windows mit GCPW verfügbar.	Integration mit Google Identity	Jamf Connect	Google Workspace, Google Cloud Identity
Jamf Protect Parser für Google Security Operations	Durch die Integration von Jamf Protect und Google Security Operations können detaillierte Ereignisdaten, Warnmeldungen und Unified Logging-Ereignisse, die von Jamf Protect erfasst wurden, zur Protokollierung und Analyse an SecOps gesendet werden.	Google Security Operations	Jamf Protect	Google Security Operations
Jamf Pro Parser für Google Security Operations	Bestandsinformationen von Jamf Pro können von Google Security Operations ausgewertet werden	Google Security Operations	Jamf Pro	Google Security Operations
Kontobasierte Benutzeranmeldung mit Google Identity für iOS BYOD	Bereitstellung einer Geräteverwaltung, die die Privatsphäre der Benutzer auf persönlichen Mobilgeräten respektiert. Benutzer melden sich einfach über die Einstellungs-App an und nutzen ihre Google-Anmeldedaten, um sich für die Geräteverwaltung zu registrieren und Profile und Apps zu erhalten.	Benutzerregistrierung für BYOD	Jamf Pro, Jamf School	Google Workspace, Google Cloud Identity



www.jamf.com/de/

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

Wenn Sie mehr über die Partnerschaft zwischen Google und Jamf erfahren möchten, besuchen Sie unsere Seite mit den [Google-Integrationen](#). Sind Sie neugierig geworden? [Dann fordern Sie eine Testversion an](#).