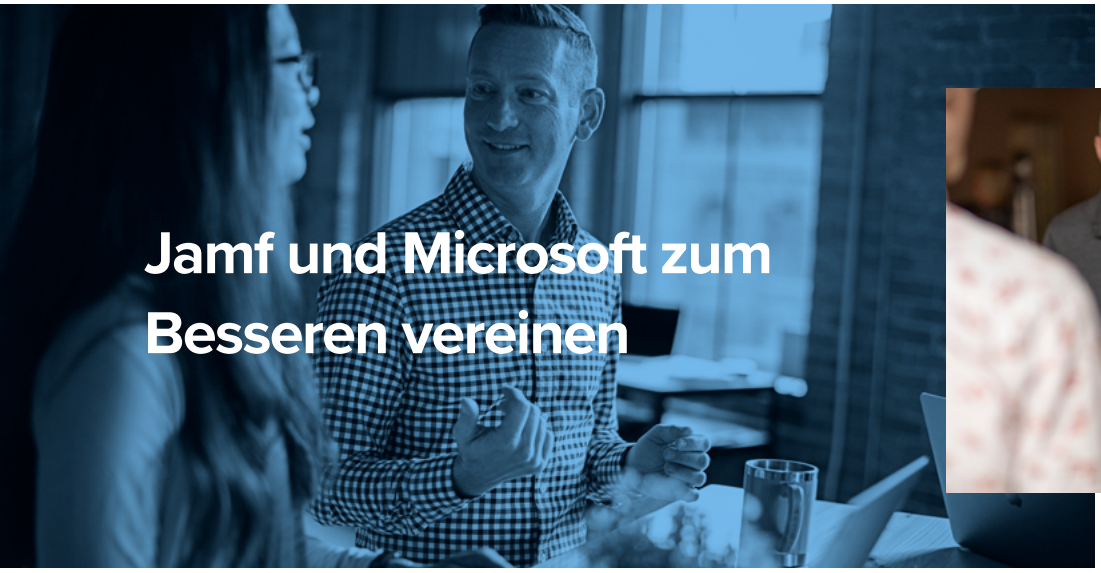
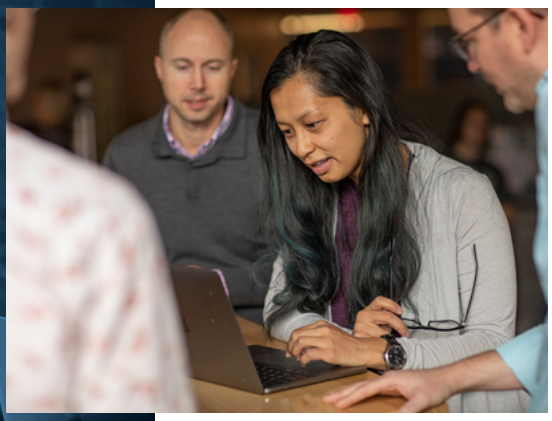
jamf

WHITEPAPER



Jamf und Microsoft zum Besseren vereinen



Die Unterstützung hybrider und dezentraler Arbeitsumgebungen ist von entscheidender Bedeutung, und Administrator*innen benötigen das beste zweckgebundene Verwaltungstool, um ihrem Unternehmen zum Erfolg zu verhelfen: Jamf für Apple und Microsoft für andere Geräte. Auf der Geräteverwaltung - der Grundlage der Unternehmenssicherheit - liegt die Endpoint- und Netzwerksicherheit, die das Beste aus der auf Apple fokussierten Bedrohungsanalyse von Jamf mit dem Identitätsmanagement und SIEM von Microsoft kombiniert.

Während viele denken, dass man sich für eine Plattform entscheiden muss, geht es nicht mehr um die Wahl des Gerätetyps, den man standardisieren möchte, und auch nicht um eine ineffektive Plattform, die die Verwaltung aller auf die gleiche Weise erzwingt. Diese Geräte funktionieren im Grunde ganz anders. Die Lösung besteht darin, sich mit den besten Optionen für jedes Gerät und sich selbst auszurüsten und dann Integrationen und Beziehungen wie die von Microsoft und Jamf den Weg weisen zu lassen.

In diesem Whitepaper behandeln wir Folgendes:

- Die Bedeutung der Geräteauswahl für Mitarbeiter*innen und Unternehmen
- Wie Jamf und Microsoft gemeinsam das Optimum an Benutzerfreundlichkeit, Effizienz und Flexibilität bieten

Die Macht der Wahl

Die Wahl der Arbeitstechnologie ist von entscheidender Bedeutung für Arbeitnehmer*innen bei der Wahl ihres Arbeitsplatzes, für den Erfolg von Arbeitgeber*innen bei der Einstellung und Bindung von Top-Talenten und für Unternehmen bei der Beurteilung ihres Wettbewerbsvorteils innerhalb ihrer Branche. In einer kürzlich durchgeführten weltweiten Studie* mit über 2000 Teilnehmer*innen gaben fast 9 von 10 Befragten an, dass die Wahl ihres Arbeitsgeräts für sie wichtig ist (87 %), und sie wären sogar bereit, einen Teil ihres Gehalts zu opfern (89 %), um die Möglichkeit zu haben, ihre Technologie selbst auszuwählen.

Die Studie ergab, dass die Wahlfreiheit der Mitarbeiter*innen einen erheblichen Einfluss auf die Mitarbeiterbasis eines Unternehmens hat, mit positiven Auswirkungen auf Wohlbefinden, Personalbeschaffung und Mitarbeiterbindung.

91 % der Befragten geben an, dass sie von einem Programm zur Mitarbeiterwahl profitieren. Die wichtigsten Gründe sind: Produktivität, Positivität und das Gefühl, mehr geschätzt zu werden.

Trotz der Bedeutung, die die Wahlfreiheit der Mitarbeiter*innen für sie hat, gab nur die Hälfte (54 %) der Befragten an, dass ihr Unternehmen ein Programm zur Wahlfreiheit der Mitarbeiter*innen und/oder eine BYOD-Strategie (Bring Your Own Device) hat.

Vor die Wahl gestellt, zeigen sowohl Apple als auch Nicht Apple Nutzer*innen Interesse an Apple

Apple Benutzer*innen haben eine starke Affinität zu ihren Produkten, und so ist es nicht überraschend, dass 98 % der regelmäßigen Apple Benutzer*innen Apple Geräte für die Arbeit wählen würden. Die Umfrage hat jedoch ergeben, dass die meisten Arbeitnehmer*innen Interesse daran haben, sich für Apple zu entscheiden. Hätten sie die Wahl, würden 62 % aller Befragten Apple für ihr Arbeitsgerät wählen.

Das Angebot von Apple Geräten hindert die Nutzer*innen nicht daran, die von ihnen geliebten Microsoft-Produktivitätswerkzeuge zu nutzen. Die Integrationen von Jamf und Microsoft ermöglichen eine breite Palette von Funktionen, die die Verwaltung, den Schutz und die Verbindung von Benutzern und Apple Geräten mit Microsoft-Software unterstützen.

Jamf und Microsoft: Zusammenarbeit

Es ist kein Geheimnis, dass Jamf und Apple eine sehr enge Beziehung haben, was noch mehr dafür spricht, Benutzer*innen durch eine sichere und strategische Integration in Microsoft zu unterstützen.

2017 kündigten Jamf und Microsoft eine Zusammenarbeit an, um Conditional Access (jetzt Geräte-Compliance genannt) auf macOS zu bringen. Dazu gehörte die Möglichkeit, Inventardaten von Jamf Pro an Microsoft Intune weiterzugeben, bedingte Zugriffsrichtlinien anzuwenden und Abhilfepfade anzubieten - so wird sichergestellt, dass nur vertrauenswürdige Benutzer*innen von vertrauenswürdigen Apps auf vertrauenswürdigen Geräten auf Unternehmensdaten zugreifen. Im Jahr **2018** hat Jamf die Integration von Microsoft-Technologien erneut erweitert, um ein nahtloseres Anmeldeerlebnis für Endbenutzer*innen zu schaffen, wobei Apps und benutzerdefinierte Einstellungen für Office für Mac **2019** folgen werden. Im Jahr **2020** kündigte Microsoft die Ausweitung von Conditional Access auf Apple Mobilgeräte an und ging eine Partnerschaft mit Jamf ein, um die Geräte-Compliance für iOS zu unterstützen. Zuletzt wurde im Jahr **2021** ein bedeutender Schritt in der Sicherheitspartnerschaft unternommen, indem Microsoft Sentinel und Jamf Protect integriert wurden, um Apple spezifische Bedrohungsdaten in Echtzeit direkt in das bevorzugte SIEM-Tool für IT und Sicherheit in einer Microsoft-Umgebung zu übertragen.

Da sich die Arbeitsabläufe und Benutzerprozesse im Laufe der Jahre verändert haben und sich weiterhin anpassen, arbeiten Jamf und Microsoft weiterhin daran, die Lücke zu schließen, um sowohl für Endbenutzer*innen als auch für die IT-Abteilung eine optimierte Erfahrung zu schaffen.

Aus der IT-Perspektive

Als IT-Administrator*in ist es wichtig, eine zuverlässige, sichere Geräteflotte zu schaffen, die einfach zu aktualisieren, zu schützen und zu warten ist.Benutzer*innen wollen den gleichen Service, Schutz sowie Verwaltbarkeit, ganz gleich, ob Sie sich für Mac oder Windows entscheiden.

Ganz gleich, ob Sie aus der Welt von Apple oder Windows kommen, kann ein Versuch, die andere Seite zu verstehen, manchmal zu Fehlerquellen führen. Viele Mac Administrator*innen sind an Jamf Pro gewöhnt, aber mit den neuen Integrationen und Partnerschaften zwischen Jamf und Microsoft gibt es viele, die aus der Microsoft-Welt kommen und Mac mit Intune verwalten und sich fragen, wann sie beides kombinieren sollen.

Mit der neuen Entra-Plattform hat Microsoft seine Zero-Trust-Lösung völlig unabhängig von einzelnen Management-Lösungen gemacht. Microsoft Entra ID Conditional Access stellt das Gerätevertrauen von Intune und Geräteverwaltungslösungen von Partnern wie Jamf Pro her.

Daher müssen Windows-Administrator*innen verstehen, wie das Apple Ökosystem funktioniert. Wie ist das verschlüsselt? Wie kann die Ausführung von Anti-Malware garantiert werden? Wie entdeckt man schädliches Verhalten und behebt Verstöße? Wie meldet man sich an?

Jamf Pro und Microsoft Entra ID Conditional Access

Jamf Pro ist die Engine, die das Gerät verwaltet und die Compliance-Richtlinien des Unternehmens berechnet. Aufbauend auf den nahezu unbegrenzten Möglichkeiten der Smart Computer Group- und Smart Device Group-Berechnungen meldet Jamf Pro an Microsoft, dass ein Gerät konform ist. Wenn ein Endbenutzer/eine Endbenutzerin von einem Gerät aus auf eine Cloud Ressource zugreift, verwendet Microsoft Entra ID Conditional Access diese Gerätekonformität zusammen mit den Risikostufen und dem Standort des Benutzers/der Benutzerin, um den Zugriff zu gewähren.

Die Compliance ist nicht völlig von den Administrator*innen abhängig. Spezielle Einstellungen, komplexe Passwörter, Verschlüsselung oder ein Ruhezustand nach einer bestimmten Zeit der Inaktivität können verlangt werden (oder auch nicht). Durch die Verlagerung der Compliance-Berechnung in Jamf Pro ist Microsoft nicht mehr durch die begrenzten Informationen eingeschränkt, die eine App auf einem Apple Gerät sammeln kann. Microsoft Entra ID kann flexibler agieren, indem es seine Entscheidungen einfach auf den Compliance-Status stützt. Und wenn das Gerät nicht konform ist, verweist es den Benutzer/die Benutzerin zurück an Jamf Self Service, damit er sich selbst reparieren kann, ohne dass die IT-Abteilung eingreifen muss.

Das ist das Schöne an dieser Beziehung. Mit Jamf Pro können Sie das gesamte Spektrum an Verwaltungsfunktionen nutzen und gleichzeitig Identitäten und Zugriffe auf die Dienste von Ihrem Mac aus mit Microsoft Entra ID schützen. Daher ist eine Standardisierung auf eine Plattform unnötig.

Microsoft Enterprise Mobility + Sicherheit & Geräte-Compliance

Die Notwendigkeit, Remote-Mitarbeiter*innen zu unterstützen, hat dazu geführt, dass sich der Fokus auf die Sicherheit nicht mehr nur auf die Grenzen des Unternehmensnetzwerks, sondern auch auf die Grenzen des Büros erstreckt. Unternehmen sind auf der Suche nach einer optimierten Methode zur Verwaltung und zum Schutz aller ihrer Geräte. Die Partnerschaft zwischen Microsoft und Jamf wurde auf die Geräte-Compliance ausgeweitet, mit dem gleichen Ziel: vertrauenswürdige Benutzer*innen, die auf vertrauenswürdige Apps auf vertrauenswürdigen Geräten zugreifen.

„Trends wie Programme zur Auswahl von Technologien durch Mitarbeiter*innen und die zunehmende Nutzung der IT durch die Verbraucher*innen nehmen weiter zu, und Unternehmen benötigen Management-Tools, die sich an hybride Umgebungen anpassen und auf diese umstellen können", sagte Brad Anderson, Corporate Vice President bei Microsoft. „Mit Microsoft und Jamf können IT Teams die Verwaltung von Mitarbeitergeräten konsolidieren, während sie nicht die Fähigkeit verlieren, wichtige ökosystem-spezifische Lösungen zu bieten."

Die Integration von Jamf Pro mit Microsoft Entra ID ermöglicht es Ihnen, die Einhaltung von Richtlinien auf institutionellen macOS, iOS und iPadOS Geräten durchzusetzen, die von Jamf verwaltet werden. So können Unternehmen sicherstellen, dass nur vertrauenswürdige Benutzer*innen mit konformen Geräten auf Unternehmensressourcen zugreifen können. Die Integration von Jamf Pro Geräte-Compliance mit Microsoft Intune nutzt die Partner Compliance Management API.

Jamf reagiert darauf, indem es von Benutzer*innen verlangt, dass sie Geräte registrieren, mit denen sie auf Apps zugreifen, die mit Azure Active Directory verbunden sind, einschließlich Microsoft 365 Apps. Zunächst werden die Compliance-Kriterien festgelegt und von Jamf an dem Gerät gemessen. Die von Jamf gesammelten Geräteinformationen werden dann an Microsoft gesendet. Wenn ein Benutzer/eine Benutzerin auf eine geschützte Ressource zugreift, überprüft Microsoft Entra ID den Compliance-Status des Geräts, um den Zugriff dynamisch zu gewähren oder zu verweigern.

Durch dieses Angebot können Organisationen Jamf für die iOS Verwaltung wählen, während sie wichtige Geräteinformationen, wie den Compliance-Status, mit Microsoft Endpoint Manager teilen. IT-Teams können Jamf Funktionen für die Verwaltung des Apple Ökosystems nutzen und gleichzeitig Conditional Access auf Basis von Entra ID und Microsoft Intune einsetzen, um sicherzustellen, dass nur vertrauenswürdige Benutzer*innen von konformen Geräten und mit zugelassenen Apps auf Unternehmensdaten zugreifen können.

Jamf Protect und Microsoft Sentinel

Da die Geräte und die Netzwerkinfrastruktur von Unternehmen immer komplexer werden, sind Sicherheitsteams zunehmend auf Tools wie Security Incident and Event Manager (SIEM) und Security Orchestration Automated Response (SOAR) angewiesen, um ihre Umgebung zu schützen. Um echte Sicherheit und Kontrolle in die Mac Welt zu bringen, hat Jamf sein Endpoint-Sicherheitstool Jamf Protect in den Datenfluss für Microsoft Sentinel integriert.

Jamf Protect ist ein reiner Mac Endpoint-Schutz, der alle Mac spezifischen Sicherheitsdaten und -warnungen mit minimaler Konfiguration direkt in Sentinel überträgt. Alle bösartigen oder verdächtigen Mac Aktivitäten sowie Malware-Benachrichtigungen lassen sich problemlos in bereits bestehende Arbeitsabläufe integrieren, sodass Ihr Sicherheitspersonal nur wenig Aufwand und Zeit benötigt. Mit den Angriffserkennungs- und Protokollinformationen von Jamf Protect kann Sentinel seine Fähigkeiten erweitern, um breit angelegte Angriffe auf alle Mac Geräte in der Umgebung eines Kunden zu erkennen und zu beheben und gleichzeitig die Sicherheit für das Unternehmen als Ganzes zu verbessern.

Durch die Kombination der Fähigkeiten von Microsoft und Jamf erhalten die Kund*innen einen vollständigen Überblick über die Sicherheitsaktivitäten in ihrem gesamten Mac Bestand, und zwar von ihrem vertrauten Microsoft Sentinel aus.

Schlussfolgerung

Durch derartige Integrationen und die Beziehung zwischen Jamf und Microsoft besteht kein Grund mehr dazu, den Mac nicht mit offenen Armen in Ihrer Umgebung zu begrüßen. Selbst als Windows-Administrator*in können Sie den Mac so sicher, verwaltbar und integriert machen, wie jedes Ihrer Windows Geräte.

Fordern Sie noch heute eine Testversion von Jamf an oder wenden Sie sich an Ihren bevorzugten autorisierten Reseller, um loszulegen .

Möchten Sie mehr über unsere Partnerschaften und Integrationen erfahren?
Besuchen Sie **jamf.com/de/integrationen/microsoft/**.

Quellen:

**https://www.jamf.com/de/ressourcen/e-books/internationale-studie-mitarbeiter-wahlprogramme-2021/*