jamf

WHITE PAPER

Zusammen werden Jamf und Microsoft noch besser

Da sich die Arbeitswelt in diesem Jahr geändert hat, trifft dies auch auf die tagtägliche Aufgabe zu, Apple Geräte in Unternehmen zu verwalten. Die Unterstützung von Mitarbeitern aus der Ferne war noch nie so wichtig, und viele Administratoren benötigen die besten speziell entwickelten Tools, um ihrer Organisation zum Erfolg zu verhelfen: Jamf für Apple und Microsoft für andere Geräte.

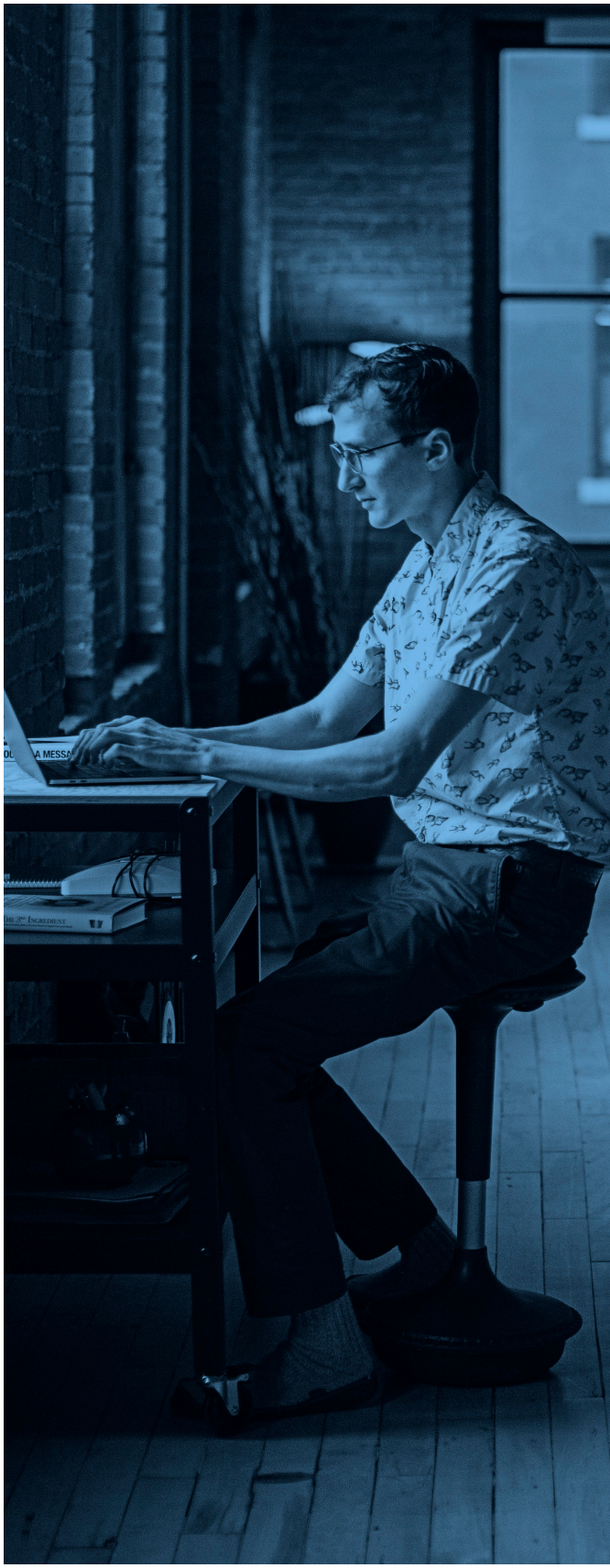
Auch wenn viele annehmen, dass man die eine oder andere Plattform wählen muss, geht es nicht mehr darum, den Gerätetyp zu wählen, den man standardisieren will, noch um eine ineffektive Plattform, die einen zwingt, alles auf die gleiche Art zu verwalten. Diese Geräte funktionieren im Grunde ganz anders. 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 White Paper behandeln wir Folgendes:

- Warum der Mac in Unternehmen zunehmend populär wird, und wie Sie darauf reagieren
- Wie Jamf und Microsoft gemeinsam das Optimum an Benutzerfreundlichkeit, Effizienz und Flexibilität bieten

Der Mac wird in Unternehmen zunehmend populär

Die Ansprüche der Anwender an die Technik ändern sich, denn sie möchten gerne mit der Hardware arbeiten, die ihnen am besten liegt. Oft ist das der Mac.



Die Macht der Wahl

In dem Maße, wie Mitarbeiter ihre Geräte am Arbeitsplatz wählen können, werden in Ihren Netzwerken immer mehr Macs auftauchen. Wie viele? Wenn sie die Wahl zwischen PC und Mac haben, wählen 72 %* den Mac. Warum sollte man sich in Unternehmen, insbesondere in den IT-Abteilungen, ernsthaft mit dem Einsatz von Macs beschäftigen? Weil zufriedene, effizient arbeitende Mitarbeiter produktiver sind. Die Ergebnisse stammen aus einer globalen Forschungsstudie** die sich auf den Mac in Unternehmen konzentriert. Und das sagen die Mac Anwender dazu:

97 %
berichten von höherer Produktivität

95%
berichten von mehr Kreativität

94 %
melden mehr Eigenständigkeit

91 %
berichten von einer verstärkten Zusammenarbeit

Der Mac wird auch am Arbeitsplatz als effektiver betrachtet als jede andere Marke. 79 % der befragten Mitarbeiter stimmen zu, dass sie ihre Arbeit nicht so effektiv erledigen könnten, wenn sie keinen Mac zur Verfügung hätten. Und 83 % der Befragten in den Bereichen Informationstechnologie und Personalwesen haben die Ansicht, dass die Nutzung eines Mac für ihre Arbeit unerlässlich ist.

Verbesserte Mitarbeiterbindung durch Macs

Gerätewahlprogramme für Mitarbeiter sowie das Angebot, mit einem Mac zu arbeiten, sind für die Mitarbeiter wichtige Faktoren bei der Entscheidung, ob sie weiterhin bei ihrem Arbeitgeber bleiben oder den Arbeitgeber wechseln.

95% der Befragten stimmen zu, dass sie eher zu einem Unternehmen gehen oder dort bleiben würden, wenn sie bei der Technologie am Arbeitsplatz eine Auswahlmöglichkeit haben.

Die Arbeit mit dem Mac hindert die Benutzer keineswegs daran, die ihnen vertraute Produktivitätssoftware von Microsoft weiterhin zu nutzen.

Jamf und Microsoft: Zusammenarbeit

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

2017 kündigten Jamf und Microsoft eine Zusammenarbeit an, um Bedingten Zugriff zu macOS zu bringen. Dazu gehörte die Fähigkeit, Bestandsdaten auf Jamf Pro mit Microsoft Intune zu teilen, Bedingten Zugriff zu verwenden und Abhilfemaßnahmen umzusetzen, damit der Zugriff auf Unternehmensdaten nur über vertrauenswürdige Anwendungen und Geräte erfolgt. Dann erweiterte Jamf 2018 die Integration in Microsoft Technologie erneut, um Benutzern eine nahtlosere Anmeldung zu ermöglichen. Die Partnerschaft wurde 2020 mit Geräte-Compliance für IoS fortgesetzt, das später in diesem Whitepaper noch detaillierter behandelt wird. 2021 hat Jamf die auf den Mac fokussierte Sicherheit, Transparenz, Erkennung und Behebung von Jamf Protect in die Cloud-nativen SIEM- und SOAR-Fähigkeiten von Azure Sentinel integriert, um Sicherheitsorganisationen eine umfassende Kontrolle und Sicherheitsdaten über ihre gesamte Mac Flotte zu bieten.

Da sich Workflows und Benutzerprozesse im Laufe der Jahre geändert haben und sich weiterhin an eine „neue Normalität“ im Unternehmen anpassen, schließen Jamf und Microsoft die Lücke weiter und entwickeln eine optimierte Erfahrung sowohl für Benutzer als auch IT-Experten.

Aus der IT-Perspektive

Für IT-Administratoren ist es wichtig, eine zuverlässige, sichere Geräteflotte zu erstellen, die sich einfach aktualisieren, schützen und warten lässt. Benutzer wollen den gleichen Service, die gleiche Sicherheit und Verwaltbarkeit, egal 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 IT-Administratoren kennen sich gut mit Jamf Pro aus und sind daran gewöhnt, aber aufgrund der neuen Integrationen und Partnerschaften zwischen Apple, Jamf und Microsoft gibt es zahlreiche, die aus der Welt von Microsoft stammen und sich bei der Verwaltung von Mac mit Intune fragen, wie sie die beiden miteinander kombinieren sollen.

Windows-Administratoren ist die Sicherheit in einer Zero-Trust-Umgebung wichtig. Microsoft Intune ist nicht da als ein Teil des Verfahrens, für eine bessere Mac Verwaltungsplattform sondern bietet es den Identitätsschutz von einem Mac zu einer beliebigen anderen App.

Daher müssen Windows-Administratoren 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 Intune

Jamf Pro ist die Engine zur Verwaltung des Geräts, die Meldedaten an Microsoft Intune sendet. Microsoft Intune ist dann dafür verantwortlich, diese Daten anzusehen und zu bestimmen, ob das Gerät die Vorschriften erfüllt oder nicht.

Die Compliance ist nicht völlig von den Administratoren abhängig. Bestimmte Einstellungen, komplexe Passwörter, Verschlüsselung oder ein Ruhemodus nach einer gemessenen Inaktivität können alle erforderlich sein (oder nicht). Diese Compliance-Einstellungen sind der Kommunikationspunkt zwischen Microsoft Intune und Jamf Pro. Die Anwendung dieser Richtlinien zeigt Administratoren, ob das Gerät korrekt konfiguriert ist oder ob Handlungsbedarf besteht.

Der Unterschied besteht darin, wie diese Compliance oder Nicht-Compliance mit einem Benutzer assoziiert wird. Das ist die Rolle von Bedingter Zugriff. Diese nur in Microsoft Intune vorhandene Funktion kann von anderen integriert werden, aber die Kontrolle geht von Intune aus. Mit diesen Richtlinien, Compliance- und Sicherheitsmaßnahmen, sehen wir, wie die Kommunikation zwischen Intune und Jamf Pro gebildet wird, eine Beziehung entsteht und eine Sicherheitsebene sich formt.

Das ist das Schöne an dieser Beziehung. Man kann das ganze Spektrum der Verwaltungsfunktionen durch Jamf Pro erhalten, während man Identitäten und den Zugriff seines Mac auf Services mit Microsoft Intune und Azure AD schützt. Daher ist eine Standardisierung auf eine Plattform unnötig.

Microsoft Enterprise Mobility + Security und Geräte-Compliance für iOS

Die Notwendigkeit zur Unterstützung von Remote-Mitarbeitern hat den Sicherheitsschwerpunkt vom Bereich innerhalb des Firmennetzwerks auf das Gebiet außerhalb des Büro-Perimeters verlegt. Deshalb suchen Organisationen nach einer optimierten Methode, um alle ihre Geräte zu verwalten und zu schützen. Um Organisationen optimal zu unterstützen, kündigte Jamf an, dass es die Zusammenarbeit mit Microsoft Enterprise Mobility + Security erweitern wird, indem es Geräte-Compliance für iOS herausbringt.

„Trends wie Geräteauswahlprogramme für Mitarbeiter und die Konsumerisierung von IT wachsen weiter an, und Organisationen benötigen Verwaltungstools, die sich an hybride Umgebungen besser anpassen", sagte Brad Anderson, Corporate Vice President 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."

Unternehmen genießen bereits die Möglichkeit, bedingten Zugriff auf macOS Geräte zu nutzen, indem Bestandsdaten aus Jamf mit Microsoft Endpoint Manager geteilt werden. Mit Geräte-Compliance für iOS können IT Teams jetzt auch verhindern, dass ein autorisierter Benutzer ein macOS oder iOS Gerät verwendet, das nicht den Sicherheitsrichtlinien entspricht. Dabei nutzen sie Jamf Self Service zur Behebung des Problems.

Jamf reagiert darauf, indem es von Benutzern verlangt, dass sie Geräte registrieren, mit denen sie auf Anwendungen zugreifen, die mit Azure Active Directory verbunden sind, einschließlich Microsoft 365 Apps. Zunächst werden von Jamf Compliance Kriterien auf dem iOS Gerät festgelegt und überprüft. Die von Jamf erfassten Geräteinformationen werden dann an Microsoft Endpoint Manager gesendet. Schließlich überprüft Endpoint Manager den Compliance-Status des Geräts, und nutzt Azure Active Directory zur dynamischen Gewährung oder Ablehnung des Zugriffs. Wenn das Gerät gegen die Compliance verstößt, wird eine Benachrichtigung an den Benutzer gesendet, die eine Behebung mithilfe von Jamf Self Service erfordert.

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 die Jamf Funktionen für die Verwaltung des Apple Ökosystems verwenden, während sie Bedingter Zugriff mit Azure Active Directory und Microsoft Endpoint Manager nutzen, um sicherzustellen, dass nur vertrauenswürdige Benutzer von konformen Geräten aus mithilfe von genehmigten Apps auf Unternehmensdaten zugreifen können.

Jamf Protect und Microsoft Azure Sentinel

In dem Maße, wie die Geräte und die Netzwerkinfrastruktur von Organisationen immer komplexer werden, müssen sich Sicherheitsteams zunehmend auf Tools wie SIEM (Security Incident and Event Manager) und SOAR (Security Orchestration Automated Response) verlassen, um ihre Umgebung abzusichern. Um der Mac Welt echte Sicherheit und Kontrolle zu bieten, hat Jamf sein Endpoint Security-Tool, Jamf Protect in den Datenfluss für Microsoft Azure Sentinel integriert.

Jamf Protect ist ein nur für Mac verfügbarer Endpoint-Schutz und überträgt nativ alle Mac spezifischen Sicherheitsdaten und Warnmeldungen direkt an Azure Sentinel, wobei nur minimale Konfiguration erforderlich ist.
Alle bösartigen oder verdächtigen Mac Aktivitäten sowie Malware-Benachrichtigungen können einfach in vorhandene Workflows integriert werden, was wenig Mühe und Zeit vom Sicherheits- und IT-Personal erfordert. Dank der Fähigkeiten von Jamf Protect zur Entdeckung und Protokollierung von Angriffen kann Azure Sentinel seine Fähigkeiten zur Identifizierung und Behebung von breitgefächerten Angriffen auf alle Mac Geräte in der Umgebung eines Kunden erweitern und der Organisation eine bessere Sicherheit bieten.

Durch die Kombination der Fähigkeiten von Microsoft und Jamf haben Kunden perfekten Einblick in die Sicherheitslage bei ihren Macs, wobei sie die vertraute Perspektive von Azure Sentinel verwenden.

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 können Sie den Mac so sicher, verwaltbar und integriert machen, wie jedes Ihrer Windows Geräte.

Fordern Sie noch heute eine kostenlose Testversion von Jamf an und überzeugen Sie sich selbst. Gerne können Sie sich auch an einen autorisierten Händler für Apple Geräte Ihrer Wahl wenden, um anzufangen.

Quellen:
**https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/*
***https://www.jamf.com/resources/e-books/global-survey-mac-in-the-enterprise/*