



Absicherung von macOS für ein modernes Arbeitsumfeld

In internationalen Unternehmen hat eine neue Ära der modernen Arbeit begonnen, in der einzelne Mitarbeiter fundierte Entscheidungen schnell treffen müssen und dazu die Tools einsetzen möchten, die sie am besten kennen und bevorzugen. Befördert wird dieser Trend durch die Millennial-Generation, die nun einen wachsenden Teil der Belegschaft in modernen Unternehmen ausmacht. Diese Mitarbeiter wollen selbst die Tools auswählen, die am besten geeignet sind, ohne auf ihr mobiles Benutzererlebnis oder ihre Privatsphäre zu verzichten, und fluten das Unternehmen mit den von ihnen bevorzugten Geräten und Apps. Die Beliebtheit von Apple unter den Millennials hat zu einer enormen Verbreitung



401 East Middlefield Road
Mountain View, CA 94043, USA
globalsales@mobileiron.com
www.mobileiron.com
Tel.: +1 877 819 3451
Fax: +1.650.919.8006

von iOS und seit kurzen auch von macOS-Desktops im Unternehmen geführt. Im 4. Quartal 2017 stiegen die Auslieferungen von Mac-Computern beispielsweise im Jahresvergleich um 7,30 % und übertrafen damit den PC-Markt als solchen insgesamt deutlich, der nur um 0,70 % wuchs.¹

Früher wurden Mac-Laptops und Mac-Desktops im Unternehmen vor allem in Nischen eingesetzt, beispielsweise durch Grafikdesigner und Videoproduzenten. Damals mussten nur wenige Mac-Workstations verwaltet werden. Daher ließen viele IT-Abteilungen diese Endgeräte entweder ungesichert oder sicherten sie mit einer Insel-Lösung ab, die von der Infrastruktur der vereinheitlichten Endgeräteverwaltung (UEM) getrennt war. Insel-Lösungen sind zwar kurzfristig eine attraktive Option, eignen sich jedoch nicht als langfristige Strategie oder als Sicherheitsmodell mit mehreren Schichten, wie es zur Skalierung aufgrund der wachsenden Zahl der Mac-Computer im Unternehmen erforderlich ist. Die Verwaltung von Mac-Workstations mit Insel-Lösungen kann diese Endgeräte daher gefährden und zu Sicherheitslücken im gesamten Unternehmen führen.

Was die Unternehmen brauchen, ist ein strategisches UEM-Konzept, das die Kosten für die IT reduziert und deren Arbeit vereinfacht, einen Mix unterschiedlicher Betriebssysteme wie iOS, macOS, Android und Windows 10 unterstützt und den Benutzern ein problemloses, sicheres und produktives Benutzererlebnis in einem zeitgemäßen, modernen Arbeitsumfeld zur Verfügung stellt. Benötigt wird dazu eine komplette UEM-Plattform wie MobileIron, mit der die Benutzer Innovationen in der Cloud und bei Mobilgeräten gefahrlos nutzen und zügig fundierte Entscheidungen treffen können, die im richtigen Moment die richtigen Aktionen auslösen. Es gibt keine Insel-Lösung, die all diese Anforderungen erfüllen kann.



¹ <https://9to5mac.com/2018/01/12/mac-market-share-2017/>

UEM als ideale Lösung für macOS-Sicherheit

Die Zeit ist reif für ein ausgereifteres Konzept zur Verwaltung von Mac-Computern im Unternehmen. Dies gilt insbesondere für Unternehmen, die bereits eine UEM-Lösung einsetzen, aber macOS bisher durch eine separate Insel-Lösung verwalten. Durch die Erfassung all dieser Geräte in der UEM-Lösung erreichen die IT-Abteilungen einen höheren Sicherheitsstandard bei der Verwaltung und können zwei wichtige Verwaltungsbereiche optimieren:

Steigerung der betrieblichen Effizienz

Mit UEM können IT-Administratoren bequem Geräte und Netzwerkeinstellungen, Apps, Zertifikate und Konfigurationen für Mac-Desktops über eine zentrale Konsole bereitstellen. Bei einer Verwaltung der Mac-Desktops mit Insel-Lösungen muss die IT-Abteilung diese Aufgaben mehrfach mit verschiedenen Verwaltungstools wiederholen, zwischen denen keine Transparenz besteht.

Mächtige und vollständige Compliance-Verwaltung

Bei einer gemeinsamen Plattform muss nur ein Regelsatz definiert werden. Sobald dieser Regelsatz durch den Sicherheitsbeauftragten des Unternehmens genehmigt ist, kann er zur Gewährleistung der Compliance für alle Endgeräte verwendet werden – dies vereinfacht den Prozess und die Arbeit der IT deutlich. Bei Insel-Lösungen muss die IT-Abteilung verschiedene Regeln in verschiedenen Systemen definieren, um die Sicherheits- und Compliance-Richtlinien des Unternehmens einzuhalten. Da jedes einzelne System anders funktioniert, kann es dazu kommen, dass die Compliance-Vorschriften nicht vollständig eingehalten werden. Wenn sich Bestimmungen ändern, sind die Richtlinien beispielsweise veraltet, ohne dass es der IT-Abteilung bewusst ist. Es kann außerdem eine Herausforderung sein, komplette Audit-Berichte ohne einheitliche Ansicht für jede Insel-Lösung zu generieren.

Entscheiden Sie sich für MobileIron, um Mac-Desktops sicher zu verwalten

MobileIron bietet ein mehrschichtiges Sicherheits- und Zugriffsmodell für macOS, das die Betriebseffizienz verbessert und die Einhaltung der Compliance erleichtert, da alle Endgeräte im Unternehmen unabhängig von ihrer Größe oder ihrem Betriebssystem verwaltet werden können. Der MobileIron macOS-Agent erleichtert den Benutzern die Registrierung bei der OEM-Lösung und die Skriptausführung für Aufgaben, die über das MDM-Protokoll nicht ausgeführt werden können. Er kann außerdem wie jede andere Anwendung per Push auf bereits registrierte Geräte übertragen werden, ohne die vorhandene Verwaltung zu beeinträchtigen, sodass Endgeräte mit Hilfe von Skripten verwaltet werden können.

Höhere Sicherheit

Dank der besseren granularen Transparenz und Kontrolle können Unternehmen die Compliance-Bestimmungen einhalten und Daten auf jedem unternehmenseigenen oder mitarbeitereigenen Mac-Desktop sowie auf anderen Geräten mit anderen Betriebssystemen schützen. Mit MobileIron können Unternehmen die Geräteverschlüsselung und die Einstellungen zur Vermeidung von Datenverlust umfassend nutzen sowie einen bedingten Zugriff auf Cloud-Dienste wie Office 365 und Salesforce.com erzwingen.

Einfachere Verwaltung

Die IT-Abteilung profitiert von der effizienteren Verwaltung mit einem geringen Anteil an Handarbeit. Die Administratoren können beliebige Geräte „Over the air“ konfigurieren und einen sicheren Zugriff auf Unternehmens-Apps, E-Mail, WLAN, VPN sowie andere Produktivitäts-Apps und Content-Repositories wie SharePoint und Box zur Verfügung stellen. Die Verwaltung von Mac-Desktops mit MobileIron

ist jetzt genauso einfach wie die Verwaltung von iOS oder anderen Gerätearten. Es sind weder eine Einarbeitungszeit, noch manuellen Eingriffe oder eine Administratorschulung erforderlich.

Die IT kann zudem die Produktivität im Unternehmen mit Rahmenbedingungen für Sicherheit mobiler Anwendungen steigern, um Apps in großem Maßstab zu verteilen, zu schützen und zu verwalten. Der Datenschutz für die Mitarbeiter ist ebenfalls gewährleistet, da Unternehmens- und private Apps und Daten auf den mitarbeitereigenen Desktops getrennt sind. Genauso wichtig für die IT ist die Möglichkeit, den gesamten Geräte-Lebenszyklus von der sicheren Bereitstellung über die Verwaltung und Abschaltung von Geräten bei Kündigung von Mitarbeitern oder Austausch der Desktops zu verwalten.

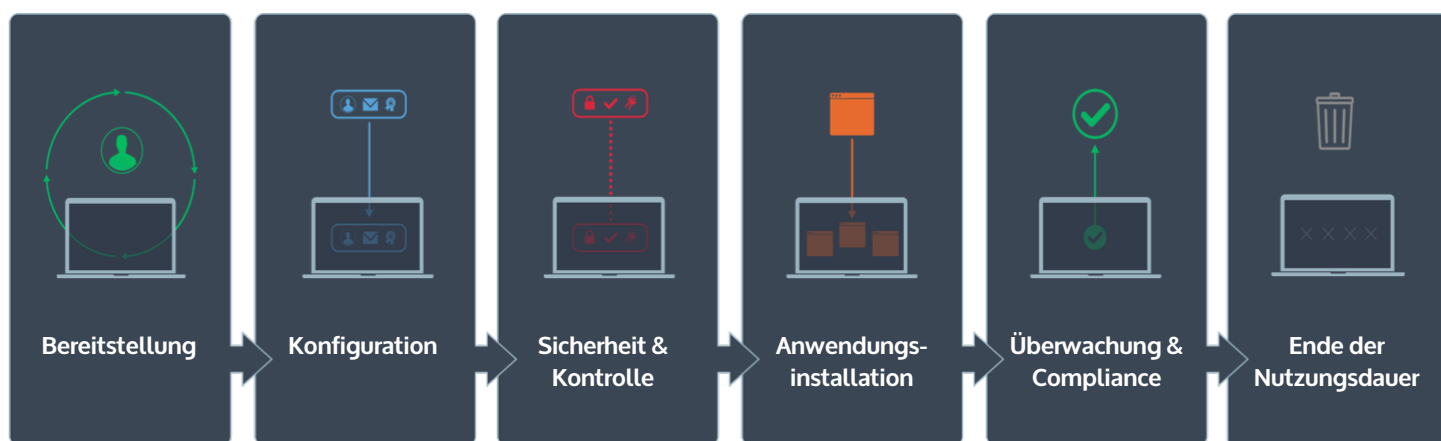
Besseres Benutzererlebnis

Dank MobileIron kann die IT-Abteilung die Produktivität steigern und Benutzer mit beliebigen Geräten innerhalb von Minuten arbeitsfähig machen. Selbst Telearbeiter und Leiharbeiter erhalten mit einem voll ausgestatteten Mac-Desktop unabhängig von ihrem Arbeitsort schnell einen Zugriff auf Unternehmens-Apps und Content. Mit den bequem

erreichbaren Optionen zur Fehlerbehebung und Selbstbedienung unterstützt MobileIron zudem die Benutzer bei der Beseitigung von Problemen und reduziert so die Zahl der Anrufe beim Helpdesk. Die Benutzer erhalten zudem das gleiche, von MobileIron bekannte intuitive Benutzererlebnis für alle Geräte, vom Smartphone über Tablets bis zu Desktops. Die Mitarbeiter müssen nicht zwischen verschiedenen Verwaltungsoberflächen auf verschiedenen Geräten wechseln. Durch die Registrierung von Unternehmensgeräten bei MobileIron erhalten die Benutzer ein einheitliches, störungsfreies Benutzererlebnis.

MobileIron sichert Mac-Computer während des gesamten verwalteten Geräte-Lebenszyklus

MobileIron bietet eine umfassende Desktop-Verwaltungslösung für Mac-Computer in jeder Phase der Geräteverwaltung während des gesamten Lebenszyklus. Wenn Unternehmen MobileIron bereits zur Absicherung und Verwaltung von Geräten mit iOS, Android oder Windows 10 einsetzen, können sie diese Funktionen problemlos auf Mac-Workstations erweitern.



Bereitstellung

MobileIron unterstützt das Geräte-Registrierungsprogramm (DEP) von Apple. Damit wird es für Unternehmen ganz einfach, neue, unternehmenseigene Geräte, also auch Mac-Desktops, bereitzustellen und zu konfigurieren. Wie bereits erwähnt, bietet der MobileIron macOS-Agent granulare Kontrollen an, die über die durch das MDM-Protokoll unterstützten Sicherheitsfunktionen hinausgehen, dient aber zugleich auch als Registrierungspunkt.

Konfiguration

IT-Administratoren können mit der benutzerfreundlichen MobileIron-Konsole alle modernen Endgeräte mit Einstellungen, Zertifikaten, WLAN, VPN usw. konfigurieren. Mit dem macOS-Agent können Administratoren komplexe Skripte starten, die sie vielleicht schon früher für alte Systeme oder Punktlösungen zur Unterstützung von Nischenanwendungen verwendet haben.

Sicherheit und Kontrolle

Die Absicherung von Mac-Desktops mit MobileIron unterscheidet sich nicht von der Absicherung anderer Geräte. Unternehmen können Daten in Cloud-Diensten wie Office 365 und Salesforce durch Sperrung nicht konformer Geräte mit MobileIron Access schützen. MobileIron schützt außerdem die Daten, die den Mac-Desktop verlassen, durch die sichere Vernetzung über MobileIron Tunnel. MobileIron Tunnel bietet eine App-spezifische VPN-Verbindung, sodass keine VPN-Lösung eines Drittanbieters benötigt wird. IT-Administratoren können außerdem Standard-Antivirus- und Antimalware-Anwendungen auf jedem Mac über die MobileIron-Konsole bereitstellen und aktualisieren.

Anwendungsinstallation

MobileIron unterstützt die gesamte Palette der App-Verteilung und Lebenszyklusfunktionen für macOS-Geräte, darunter auch das Volumen-Kaufprogramm (VPP) von Apple. Apps aus dem

Mac App Store sowie hauseigene Apps können in Apps@Work organisiert und per Push auf jeden Mac-Desktop übertragen werden. In Apps@Work können je nach den Richtlinien des Unternehmens verschiedene Apps verschiedenen Benutzern zur Verfügung gestellt werden. Die Endbenutzer laden einfach die relevanten Apps durch Auswahl in Apps@Work herunter und installieren sie. Über die MobileIron-Konsole können Administratoren mit Richtlinien festlegen, welche Apps Mitarbeiter auf ihre Geräte herunterladen können und verhindern, dass Apps bösartige Aktionen ausführen.

Monitoring und Compliance

Damit die Administratoren sicherstellen können, dass alle Geräte, auch Mac-Desktops, die Compliance erfüllen, muss der Compliance-Status jedes einzelnen Geräts für die Administratoren transparent sein. Mit MobileIron kann die IT konsistente Rahmenbedingungen für die Sicherheit von Mobilgeräten und Desktops definieren und mit einem intuitiven Richtlinienmodul durchsetzen. Ein nicht konformes Gerät lässt sich schnell identifizieren und gegebenenfalls der Zugriff auf Unternehmensressourcen unterbinden. Durch granulare Richtlinieneinstellungen und Compliance-Konfigurationen kann die IT-Abteilung zudem die Sicherheitsrichtlinien je nach den Anforderungen des Unternehmens und den Änderungen von Bestimmungen wie der Datenschutzgrundverordnung, PCI DSS und HIPAA anpassen und aktualisieren.

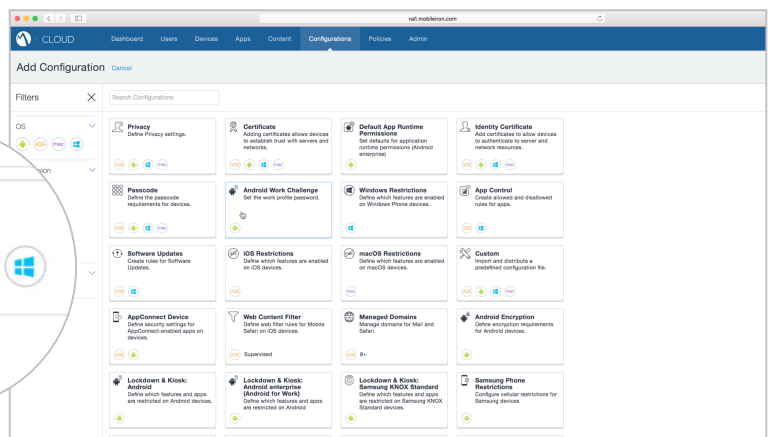
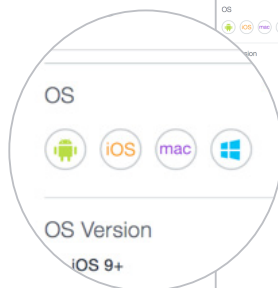
Ende der Nutzungsdauer

Wenn ein Mac-Desktop ausgesondert werden soll oder ein Mitarbeiter das Unternehmen verlässt, kann die IT-Abteilung aus der Ferne alle Unternehmens-Apps, Daten und Konfigurationen löschen und den Mac wieder auf die Werkeinstellungen zurücksetzen. Bei einem Mac-Desktop, der Eigentum des Mitarbeiters ist, kann die IT-Abteilung Unternehmens-Apps und Unternehmensdaten löschen, ohne die privaten Apps und den privaten Content des Benutzers auf dem Gerät zu verändern.

Ein modernes Arbeitsumfeld erfordert ein modernes Sicherheitsmodell

Das Arbeitsumfeld im Unternehmen hat sich durch den Eintritt der Millennials ins Arbeitsleben und deren bevorzugte Geräte deutlich verändert. Mac-Desktops, die einst vor allem Nischenprodukte waren, werden daher jetzt im Unternehmen immer häufiger eingesetzt. Bei diesen Geräten muss die gleiche Sicherheit und Kontrolle gewährleistet sein wie bei allen anderen Geräten im Unternehmen. Wenn Mac-Desktops nicht verwaltet oder nur durch Insel-Lösungen abgesichert werden, entstehen Sicherheitslücken, die das Unternehmen anfällig für Cyberattacken und Compliance-Verstöße machen.

Die gute Nachricht in diesem Zusammenhang ist, dass MobileIron die Absicherung von Mac-Desktops genauso einfach macht wie bei allen anderen im Unternehmen verwalteten Geräten. Es sind weder Integrationen noch zusätzlichen Schulungen oder eine Einarbeitung erforderlich. Die Zeit ist reif für ein modernes Konzept zur Mac-Verwaltung, das für die Endbenutzer problemlos ist, die Betriebseffizienz steigert und die IT-Arbeit während des gesamten Lebenszyklus des Geräts vereinfacht. Mit MobileIron wird all dies möglich.



Mit der MobileIron Cloud wird es ganz einfach, Mac-Desktops zusammen mit anderen Endgeräten verschiedener Betriebssysteme abzusichern.

Weitere Informationen

Weitere Informationen über moderne Endgerätesicherheit für macOS mit MobileIron finden Sie [hier](#).