jamf

Mac und iOS Ohne Kompromisse

in PC-lastigen Unternehmen

Einführung

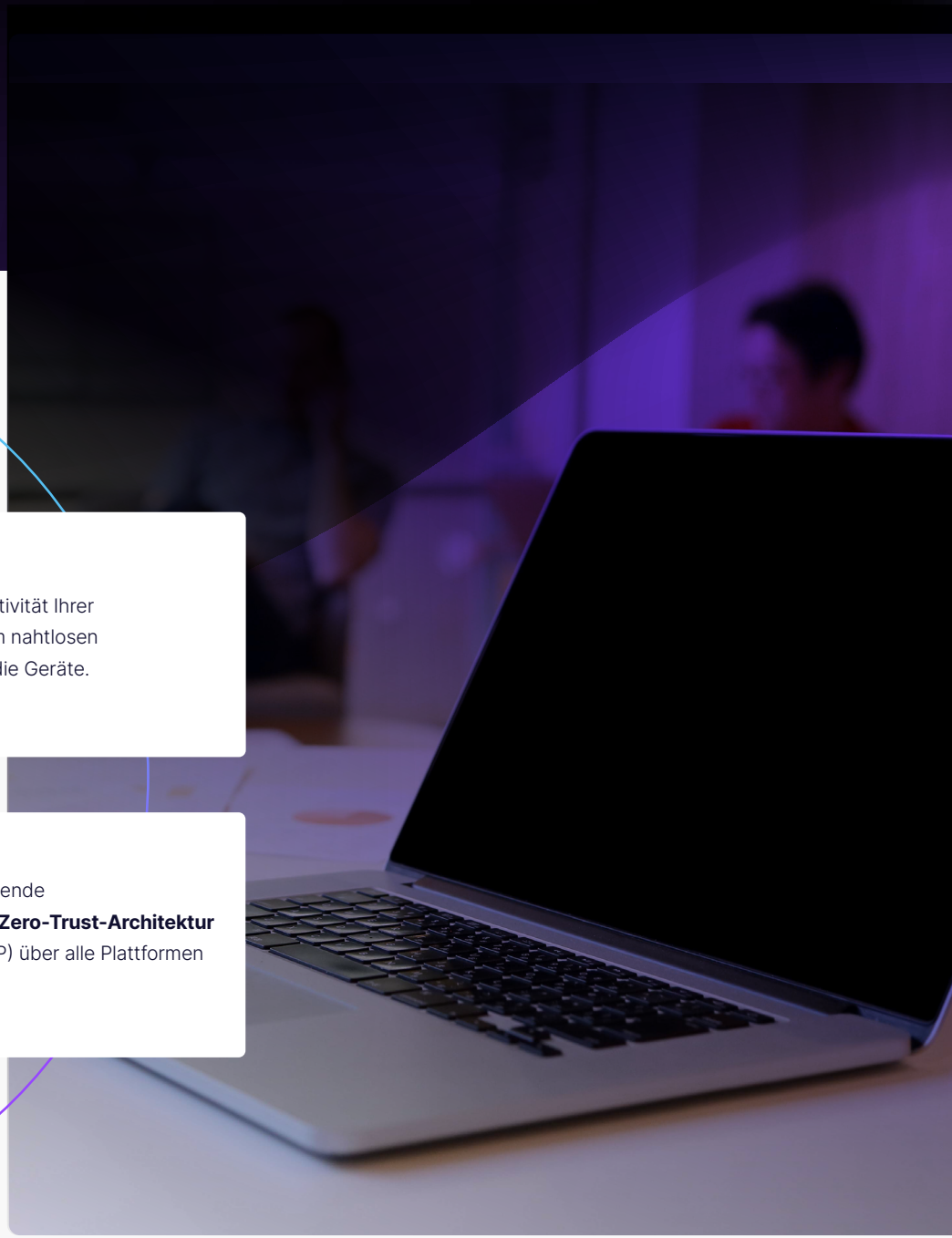
Wenn Apple Geräte in Windows-orientierten Unternehmen Einzug halten, entscheidet die Effizienz - und nicht zusätzlicher Personalbedarf - darüber, ob die IT-Abteilung weiterhin reibungslos funktioniert oder durch Mehrarbeit ins Stocken gerät.

Dieser Leitfaden ist der erste Teil der Serie *Warum Jamf*, die IT-Führungskräfte und Administratoren aller Kompetenzstufen mit den nötigen Informationen versorgt, um sicherzustellen, dass bestehende Investitionen in Identität, Sicherheit, Automatisierung und Beobachtbarkeit konforme Ergebnisse liefern und gleichzeitig die manuelle Arbeit reduzieren. Letztlich geht es darum, ein konsistentes Apple-Erlebnis zu schaffen, ohne den operativen Aufwand zu erhöhen.

Kurze Zusammenfassung

Mit dem zunehmenden Einsatz von Apple Geräten in Windows-orientierten Unternehmen entscheidet die betriebliche Effizienz über den Erfolg. In diesem E-Book wird beschrieben, wie Unternehmen Apple integrieren können, ohne die Zahl der Mitarbeiter:innen, die Betriebskosten oder die Komplexität zu erhöhen, indem sie wesentliche Schwachstellen angehen, die sich auf Prozesse und Arbeitsabläufe auswirken. Das Ergebnis ist eine schnellere Bereitstellung, eine bessere Transparenz und ein konsistentes, sicheres Apple Erlebnis, das mit dem Unternehmen skaliert.

Jamf löst die Integrationsprobleme



Beseitigen Sie Datensilos und ineffiziente Arbeitsabläufe durch die **Integration von Identitäts-**, **Sicherheits-** und **bestehenden IT-Lösungen**, um e eine ganzheitliche Strategie umzusetzen.

Automatisieren Sie den gesamten Lebenszyklus von Apple Geräten durch die **Integration in das Ökosystem** - von der Beschaffung über Patches bis zur sicheren Außerbetriebnahme.

Beschleunigen Sie die **Reaktion auf Vorfälle** durch die kontinuierliche Analyse umfangreicher Telemetriedaten, um die grundlegende Sicherheitslage zu standardisieren und aufrechtzuerhalten.

Optimieren Sie die Produktivität Ihrer Mitarbeiter:innen mit einem nahtlosen Onboarding-Workflow für die Geräte.

Vereinheitlichen Sie umfassende Zugriffsrichtlinien mit einer **Zero-Trust-Architektur** und **Identitätsdiensten** (IdP) über alle Plattformen hinweg.

Umfassende Integration in Ihr bestehendes System

Eine mangelnde Vernetzung zwischen der Geräteverwaltung und vorhandenen Sicherheits- und Identitäts-Tools führt zu Datensilos, ineffizienten Arbeitsabläufen und Lücken in der Konformität.

Oft herrscht die falsche Annahme vor, Apple-Geräte und klassische Windows-Netzwerke ließen sich nicht miteinander vereinbaren. Dies ist ein Mythos. Obwohl dieser Glaube auf Jahrzehnte zurückgeht, sieht die Realität moderner Unternehmenstechnologie anders aus: Plattformübergreifender Support ist nicht nur für die globale Geschäftskontinuität notwendig, sondern eine absolute Selbstverständlichkeit. Dies ist besonders wichtig, da Unternehmen zunehmend auf Cloud-basierte Architekturen, Apps und Dienste setzen, um Mehrwert zu generieren und die Produktivität der Mitarbeiter aufrechtzuerhalten – unabhängig von Gerätetypen, Plattformen oder Versionen, während gleichzeitig eine ganzheitliche Einheitlichkeit über verteilte Belegschaften hinweg gewährleistet wird.

Neben der plattformübergreifenden Unterstützung spielt die umfassende Integration eine entscheidende Rolle für die Kompatibilität zwischen Ihrem vorhandenen Tech-Stack und den Apple Geräten, die in großem Umfang eingeführt werden.

Wie gelingt es Jamf, Apple Geräte nahtlos in Ihrem Unternehmen zu integrieren?

Vier Worte: **Platform Application Programing Interface** (Platform API).

Der Schlüssel zu einer reibungslosen Kommunikation zwischen Apple Endgeräten und Ihrem Technologiepaket liegt in sicheren, standardbasierten Verbindungen zwischen Lösungen, die in Ihre Verwaltungs-, Identitäts- und Sicherheitsabläufe eingebunden sind.

Was bedeutet dies für die Konformität in einem Unternehmen angesichts der modernen Bedrohungslandschaft? Einfachere Lösungen und weniger Komplexität.

Durch die nahtlose Integration von Apple in Ihr bestehendes technisches System werden folgende Aspekte plattformübergreifend ermöglicht:

Automatisierung sorgt für einheitliche Workflows & Parität

Identitätsorientierte Sicherheit bietet einheitlichen Schutz vor Bedrohungen

Aufrechterhaltung der Konformität mit **Lösungen, die Sie bereits besitzen**

Optimierung der Reaktionszeiten, indem IT-Silos aufgebrochen werden

Warum Jamf?

Der Jamf Marketplace bietet über 300 (und mehr) vorgefertigte Integrationen, damit der Einführung von Apple in Ihrem Unternehmen problemlos umgesetzt werden kann.

Weniger Ausfallzeiten bei der Belegschaft durch eine optimierte Bereitstellung der Geräte

Jede Stunde, die jemand auf ein Gerät warten muss, bedeutet eine Stunde Produktivitätsverlust - und in PC-Umgebungen beträgt diese Wartezeit durchschnittlich 2-4 Stunden pro Gerät.

Bei der Integration von Apple Geräten in eine PC-Umgebung ist die Bereitstellung die kritischste Aufgabe im Projekt, dicht gefolgt von der Planung. Während dieser Phase warten die Mitarbeiter:innen in der Regel, bis ihre neuen oder aktualisierten Geräte von der IT-Abteilung bereitgestellt werden. Je nach den zu installierenden Einstellungen, der Anzahl der Apps und den rollenspezifischen Konfigurationen, die die Mitarbeiter:innen für ihre Arbeit benötigen, führt der Zeitraum zwischen der Ausgabe der Geräte an die Mitarbeiter:innen und dem Zeitpunkt, zu dem diese Geräte einsatzbereit sind, zu Produktivitätsausfällen.

Was wäre, wenn ich Ihnen sagen würde, dass diese Verzögerungen auf etwa 15 Minuten pro Apple Computer (und nur 5-7 Minuten für jedes iPad und iPhone) reduziert werden könnten?

Das Geheimnis dieser schnellen Bereitstellung liegt im Zero-Touch-Bereitstellung. Durch die Anbindung von Apple Business Manager (ABM) an eine speziell entwickelte Apple-Verwaltungslösung verfügt die IT-Abteilung über ein Automatisierungsframework, mit dem Windows-Umgebungen einfach nicht mithalten können. Man kann sich ABM als Apples Pendant zu Windows Autopilot vorstellen – allerdings mit einer tieferen Hardware-Integration, da Apple sowohl die Chips als auch den Registrierungsdienst kontrolliert. Die IT-Abteilung integriert ABM in Jamf und definiert die Bereitschaft der Geräte direkt in der Verwaltungskonsole: Apps, Konfigurationen, Sicherheitsrichtlinien und Identitätseinstellungen. Wenn dann Geräte von Apple beschafft werden, synchronisiert ABM diese Geräteinformationen mit Jamf und fügt sie einer Vorregistrierungsgruppe hinzu.

Ab da ist die Arbeit der IT im Wesentlichen erledigt.

Firmeneigene Geräte werden an die Benutzer:innen geliefert - im Büro oder an einem anderen Ort - wo sie ihre Geräte auspacken und einschalten, und das war's! Das Gerät wird automatisch in Jamf registriert, und der Workflow zur Vorregistrierung wird ausgeführt, wodurch das Gerät nahtlos bereitgestellt werden kann. Dank der Vollautomatisierung durch Zero-Touch muss der Endbenutzer keinerlei manuelle Schritte ausführen oder ein Helpdesk-Ticket erstellen.

Warum Jamf?

Mit den Entwürfen von Jamf und der deklarativen Geräteverwaltung konfigurieren sich Geräte selbständig, was die Einrichtung auf etwa 15 Minuten für Macs und auf weniger als 7 Minuten für mobile Geräte reduziert. Die verwaltete Gerätebeglaubigung liefert einen auf der Hardware basierenden Nachweis der Konformität, sodass die IT-Abteilung weiß, dass jedes Gerät echt ist, bevor es auf Unternehmensressourcen zugreift.

Apple integriert die Beglaubigung, Identität und Verwaltung in einem einheitlichen Rahmen - von der Hardware bis zur Software.

Mithilfe der deklarativen Geräteverwaltung (DDM) können Geräte alle Einstellungen asynchron übernehmen und den Status an den Geräteverwaltungsdienst melden, ohne ständig den Apple Support anzufragen. Das bedeutet, dass sich die Geräte schneller konfigurieren und auch dann konform bleiben, wenn sie nicht mit dem Internet verbunden sind.

Die verwaltete Gerätebeglaubigung liefert im Rahmen einer Vertrauensbewertung aussagekräftige Nachweise zu den Geräteeigenschaften. Dabei werden kryptografische Erklärungen auf Basis der Secure Enclave und der Apple Beglaubigungsserver verwendet, um die Echtheit des Geräts zu bestätigen, bevor es überhaupt auf Unternehmensressourcen zugreifen kann.

Platform SSO ermöglicht passwortloses Arbeiten durch Touch ID mit phishing-resistenten Anmeldedaten, die auf hardwaregebundenen Schlüsseln in der Secure Enclave basieren, so dass sich Mitarbeiter:innen nur einmal bei der Anmeldung authentifizieren müssen, um nahtlosen Zugriff auf Unternehmensanwendungen zu erhalten, ohne mit Passwörtern jonglieren zu müssen.

IT-Aufgaben und -Prozesse auf Unternehmensebene automatisieren

Laut Forrester belaufen sich die Kosten für das Zurücksetzen eines einzigen Passworts auf 70 US-Dollar; **ein durchschnittliches Unternehmen wendet jährlich über 1 Million US-Dollar** für die Bearbeitung manueller, passwortbezogener Aufgaben auf.

Automatisierung ist ein weit gefasster Begriff, der wie ein großer Topf wirkt, in den so gut wie alles hineinpasst, was man hineinsteckt. Es ist wichtig, die Beziehung zwischen Automatisierung und Zeit zu verstehen. Es geht nicht nur darum, dass die Automatisierung von Aufgaben der IT Zeit spart, sondern auch darum, wie lange es dauert, bis die IT-Mitarbeiter:innen eine Fertigkeit so weit beherrschen, dass sie über das nötige Wissen verfügen, um die Automatisierung zu entwickeln.

Durch die schiere Menge an Geräten, Technologien und Lösungen, die auf Unternehmensebene eingesetzt werden, wird dies für IT-Teams zu einem enormen Zeitaufwand. Die Vorteile der Automatisierung gehen über die Effizienz hinaus: Die IT-Abteilung kann sich auf die strategische Arbeit konzentrieren, anstatt ständig Brände löschen zu müssen. Es bietet:

Konsequente Durchsetzung

Die Richtlinien gelten für Mac, iPhone und iPad - kein Gerät fällt durchs Raster.

Weniger menschliche Fehler

Standardisierte Workflows beseitigen Risiken, die durch manuelle Abläufe entstehen.

Skalierbarkeit ohne mehr Mitarbeiter:innen einzustellen

Sie können kontinuierlich die wachsenden Verwaltungs- und Sicherheitsanforderungen erfüllen, auch wenn das Unternehmen expandiert.

Das richtige Automatisierungs-Framework übernimmt repetitive Aufgaben: die Bereitstellung von Geräten, die Durchsetzung von Richtlinien, die Installation von Software-Patches und das Zurücksetzen von Passwörtern. Aber Apple geht noch weiter. Bei der deklarativen Geräteverwaltung warten die Geräte nicht auf Serveranweisungen, sondern setzen Richtlinien eigenständig durch und melden Statusänderungen in Echtzeit. Das bedeutet weniger Supportanfragen, schnellere Konformität und weniger manuelle Eingriffe, sobald Ihre Apple Flotte wächst.

Warum Jamf?

Die intelligenten Automatisierungsworkflows von Jamf eliminieren manuelle Konfigurationen durch richtlinienbasierte Verwaltung, dynamische Gruppen und API-gesteuerte Prozesse, die entwickelt wurden, um eine konsistente, fehlerfreie Bereitstellung und Überwachung der Konformität im großen Maßstab zu gewährleisten.

Stärkung der Zugriffsrichtlinien durch die Implementierung von Zero-Trust

Die moderne Bedrohungslandschaft entwickelt sich ständig weiter. Cyberkriminelle nutzen fortschrittliche Technologien wie KI, um ihre Bedrohungen immer besser zu machen, den Schaden zu maximieren und sich durch Tarnmaßnahmen vor der Entdeckung zu schützen.

Es besteht kein Zweifel daran, dass Bedrohungsakteure es auf jede Plattform abgesehen haben - kein Betriebssystem ist unangreifbar. Deshalb ist es ein Eckpfeiler der modernen Geräteverwaltung, Endgeräte auf dem neuesten Stand zu halten und sicherzustellen, dass eine mehrschichtige Verteidigungsstrategie umgesetzt wird. Der Schlüssel liegt darin, jedes Gerät, jeden Benutzer und jede Anfrage so lange als nicht vertrauenswürdig zu behandeln, bis das Gegenteil bewiesen ist. Zero-Trust ist kein Produkt - es ist ein Framework. Und die Architektur von Apple ist dafür ausgelegt.

Die verwaltete Gerätebeglaubigung bestätigt auf kryptografischem Wege die Echtheit eines Geräts, bevor dieses auf Unternehmensressourcen zugreift. Das Platform SSO verknüpft die Benutzeridentität mit hardwaregebundenen Schlüsseln in der Secure Enclave, wodurch der Diebstahl von Anmeldedaten erheblich erschwert wird. Die deklarative Geräteverwaltung stellt sicher, dass die Geräte alle Sicherheitsrichtlinien selbständig durchsetzen, auch wenn sie offline sind. Zusammen bilden diese Elemente eine Grundlage, auf der Vertrauen kontinuierlich überprüft und nicht einfach vorausgesetzt wird.

Dadurch gewinnen die Unternehmen an Flexibilität und können schneller auf Vorfälle reagieren**, weil sie die Verwaltung, die Identität und die Sicherheit ihrer Geräteflotte auf folgende Weise vereinheitlichen:**

Implementierung von Zero-Trust-Netzwerkzugriff (ZTNA)

- Durchsetzung kontextbasierter Zugriffsrichtlinien, die bei jeder Anfrage den Zustand des Geräts und die Anmeldedaten überprüfen.
- Sitzungen können mithilfe von Mikrotunneln isoliert werden, um gängige Angriffe auf Geräte und im Netzwerk zu reduzieren.
- Verbesserter Schutz für macOS, iOS, iPadOS, Android und Windows

Nutzung von Baselines und Benchmarking der Konformität

- **Automatische Bereitstellung von grundlegenden Sicherheitskonfigurationen**, die die gesetzlichen Vorschriften oder die individuellen Anforderungen an die Konformität berücksichtigen
- **Überprüfung der Sicherheitslage von Geräten** und Unternehmen mithilfe von Benchmarking, um die Konformität zu validieren
- **Nutzung von KI/ML zur Bedrohungssuche, Reaktion auf Vorfälle und IT-Support**
- Proaktive Erkennung bekannter Bedrohungen bei gleichzeitiger Verbesserung der Fähigkeit, **unbekannte Bedrohungen** früher zu erkennen und zu stoppen
- **Verkürzung der Reaktionszeiten und Beschleunigung der Problembehebung** bei gleichzeitiger Schließung von Sicherheitslücken
- Nutzung des **KI-Assistenten von Jamf**, um Teams bei der Erkundung von Technologien, der Validierung von Konfigurationsempfehlungen und der Entwicklung schnellerer Korrekturmaßnahmen zu unterstützen

Warum Jamf?

GenAI verleiht Social Engineering neue Dynamik – Phishing-Nachrichten, synthetische Medien und KI-generierte Malware sind schwerer zu erkennen als je zuvor.

Secure Enclave und die verwaltete Gerätebeglaubigung von Apple überprüfen die Geräteidentität auf Hardwareebene, während Jamf Zero-Trust-Netzwerkkontrollen durch risikobasierte Zugriffsrichtlinien, die Überprüfung der Gerätekonformität und die Integration von bedingtem Zugriff durchsetzt, wodurch sensible Daten am Endpunkt geschützt werden.

Mehr Transparenz und bessere Reaktionszeiten während des gesamten Lebenszyklus eines Geräts

In den meisten Gesprächen über Sicherheit geht es hauptsächlich um aktive Bedrohungen. Doch einige der größten Risiken - und Kosten - verbergen sich in den Lücken: veraltete Bestände, ungenutzte Softwarelizenzen und Geräte, die vom Unternehmen ohne ordnungsgemäße Datenlöschung entsorgt werden.

IT- und Sicherheitsteams konzentrieren sich oft so sehr auf Fragen im Zusammenhang mit Bedrohungsakteuren, dass andere Aspekte völlig in den Hintergrund treten.

Bei der Transparenz geht es aber nicht nur darum, zu wissen, was in Ihrem Netzwerk passiert. Es geht darum, zu wissen, was installiert ist, was lizenziert ist, was den Vorschriften entspricht und was ausgemustert werden sollte. Kontextbezogene Endpunktdaten, wie aktuelle Geräteinventare oder Software-Wildwuchs , zeichnen ein lückenloses Bild der Endpunktintegrität über den gesamten Lebenszyklus hinweg. Mit der deklarativen Geräteverwaltung melden Apple Geräte proaktiv Statusänderungen - Betriebssystemversion, Sicherheitsstatus, installierte Apps - ohne dass die IT-Abteilung diese abfragen muss. Das bedeutet, dass der Bestand aktuell und nicht veraltet ist.

Wir werden hier einmal aufschlüsseln, wie sich mangelnde Transparenz auf Unternehmen auswirkt:

Ungenutzte Software-Lizenzen

Wenn Softwarelizenzen nicht genau nachverfolgt werden, bleiben 50 % der Softwarelizenzen ungenutzt, was einer **Verschwendung von ca. 45 Millionen US-Dollar pro Monat entspricht.**

Probleme bei der Außerbetriebnahme

10-20 % der Datenverstöße der letzten Jahre stehen im Zusammenhang mit Elektroschrott und Geräten, die nicht ordnungsgemäß entsorgt werden. Im Gegensatz zu den derzeit genutzten Endgeräten stellen sie für Unternehmen einen blinden Fleck dar.

Lücken in der Konformität

Unternehmen, die Geräte erneuern und umverteilen, riskieren, dass Daten in die falschen Hände geraten (Stichwort: Insider-Bedrohungen), wenn diese Geräte nicht ordnungsgemäß verwaltet werden. Zum Beispiel, wenn der Laptop eines Personalleiters an einen neuen Vertriebsmitarbeiter weitergegeben wird. Personenbezogene Daten auf diesem Gerät können immer noch vorhanden und für den neuen Benutzer einsehbar sein - und je nach den für Ihre Branche geltenden Vorschriften kann dies einen Verstoß gegen Datenschutzgesetze wie die DSGVO darstellen.

Mt dem Managementansatz von Apple ist dies ganz einfach zu handhaben. Die Geräte melden sich selbst und die Richtlinien werden eigenständig durchgesetzt. Und wenn das Gerät gelöscht oder an eine andere Person weitergegeben wird, sorgt die Integration zwischen Apple Business Manager und Ihrer Verwaltungslösung dafür, dass das Gerät automatisch erneut registriert wird - ohne manuelle Eingriffe und ohne Sicherheitslücken.

Warum Jamf?

Mit Jamf for Mac kann die IT-Abteilung überprüfen, ob die Apple Silicon Macs vor der Außerbetriebnahme im vollen Sicherheitsmodus laufen. So wird sichergestellt, dass die mit FileVault verschlüsselten Daten geschützt bleiben, auch wenn ein Gerät verloren geht oder unsachgemäß entsorgt wird. Da 10 bis 20 % aller Datenlecks mit Elektroschrott in Verbindung stehen, schließt die hardwaregestützte Transparenz hinsichtlich des Secure-Boot-Status eine Lücke, die die meisten Unternehmen erst erkennen, wenn es bereits zu spät ist.

Industrielle Workflows, die Ergebnisse liefern

Der eigentliche Maßstab für die Verwaltung von Geräten ist nicht das IT-Backend, sondern die Frage, ob die Belegschaft und Kunden besser mit der Technik arbeiten können. Diese Beispiele aus der Praxis zeigen, wie Geräte die Effizienz der Workflows steigern können:

Gesundheitswesen

Wenn der Status eines Patienten in der Krankenakten auf „entlassen“ gesetzt wird, löscht ein iPad am Krankenbett automatisch alle Daten des Patienten und bereitet sich auf den nächsten Patienten vor, ohne dass die Mitarbeiter:innen das Gerät berühren müssen. Das Klinikpersonal teilt sich iPhones für die Schichten, wobei je nach Rolle und Anmeldedaten personalisierte Apps aktiviert werden.

Luftfahrt

Piloten ersetzen schwere Checklisten, Karten und Handbücher durch ein einziges, auf dem iPad gehostetes Electronic Flight Bag. Mechaniker, Gate Agents und Flugbegleiter haben automatisch Zugriff auf die richtigen Apps, egal welches Gerät sie in die Hand nehmen.

Einzelhandel

iPads, die auf den Einzel-App-Modus festgelegt sind, dienen als Selbstbedienungskioske. Das bedeutet: keine Fehlerbehebung, keine unangemessenen Inhalte und kein Zurücksetzen am Ende des Tages. Die Mitarbeiter:innen bewegen sich nahtlos zwischen Point-of-Sale-, Bestands- und Kundeninformationen auf gemeinsam genutzten Geräten, die je nach Anmeldung konfiguriert sind.

Produktion

Die Mitarbeiter:innen in der Produktion verfügen häufig weder über Anmeldedaten für das Netzwerk noch haben sie viel Erfahrung mit mobiler Technik. Gesicherte Ladeschränke bieten Zero-Level-Support. Wenn ein iPad nicht funktioniert, schließen die Mitarbeiter:innen es einfach wieder ans Ladegerät an, und das Gerät wird automatisch zurückgesetzt und die Einrichtung abgeschlossen, während es sich selbst repariert. Dann nehmen sie sich einfach ein anderes iPad und machen sich wieder an die Arbeit, ohne ein IT-Ticket oder anderweitigen Support zu benötigen.

Finanzdienstleistungen

Schadenregulierer, Kreditsachbearbeiter und Berater im Außendienst benötigen sofortigen Zugriff auf sensible Daten auf gemeinsam genutzten Geräten, oft an unvorhersehbaren Standorten mit strengen Konformitätsanforderungen. Dafür nimmt sich ein Sachverständiger einfach ein iPad aus dem Bestand, tippt einmal auf seine Anmeldedaten und hat sofort Zugriff auf Schaden-Apps, Foto-Tools und Kundendaten. Nach Beendigung des Vorgangs werden die Anmeldedaten in Sekundenschnelle entfernt, und das Gerät ist für den nächsten Benutzer bereit, wobei die Konformität durch einen vollständigen Prüfpfad sichergestellt wird.

Schlussfolgerung

Die Integration von Apple in Windows-orientierte Unternehmen erfordert keine groß angelegte Umstellung oder zusätzlichen operativen Aufwand. Vielmehr ist eine Migration auf effiziente, automatisierte und standardisierte Arbeitsabläufe erforderlich. Durch die Vereinheitlichung von Lebenszyklusverwaltung, Identität und Sicherheit auf einer Apple-eigenen Grundlage, die sich in vorhandene Tools integrieren lässt, können IT-Teams die betriebliche Reife schrittweise verbessern. Dieser Ansatz reduziert den manuellen Aufwand, verbessert die Einheitlichkeit und ermöglicht einen proaktiven Betrieb. So können Unternehmen in ihrem eigenen Tempo modernisieren und gleichzeitig die plattformübergreifende Verfügbarkeit, Konformität und Kontrolle ihrer Desktop- und Mobilgeräteflotte aufrechterhalten.

Die wichtigsten Erkenntnisse

- Die Einbindung von Apple-Geräten ist eine Frage der Prozesseffizienz, nicht der Mitarbeiterzahl.
- Mit der Zero-Touch-Bereitstellung wird die stundenlange Einrichtung zu einer Sache von Minuten, was die Ausfallzeiten reduziert.
- Einheitliche Verwaltung, Identität und Sicherheit beseitigen operative Silos.
- Die Automatisierung standardisiert die Durchsetzung und reduziert menschliche Fehler in großem Umfang.
- Zero-Trust-Netzwerkzugriff erhöht die Sicherheit ohne zusätzliche Komplexität.
- Die Transparenz des Lebenszyklus schützt die Betriebszeit, die Konformität und die Softwareausgaben.
- Die deklarative Geräteverwaltung sorgt dafür, dass die Geräte konform bleiben, auch wenn sie offline sind.

Sind Sie bereit, dies in Aktion zu erleben?

Erleben Sie Jamf