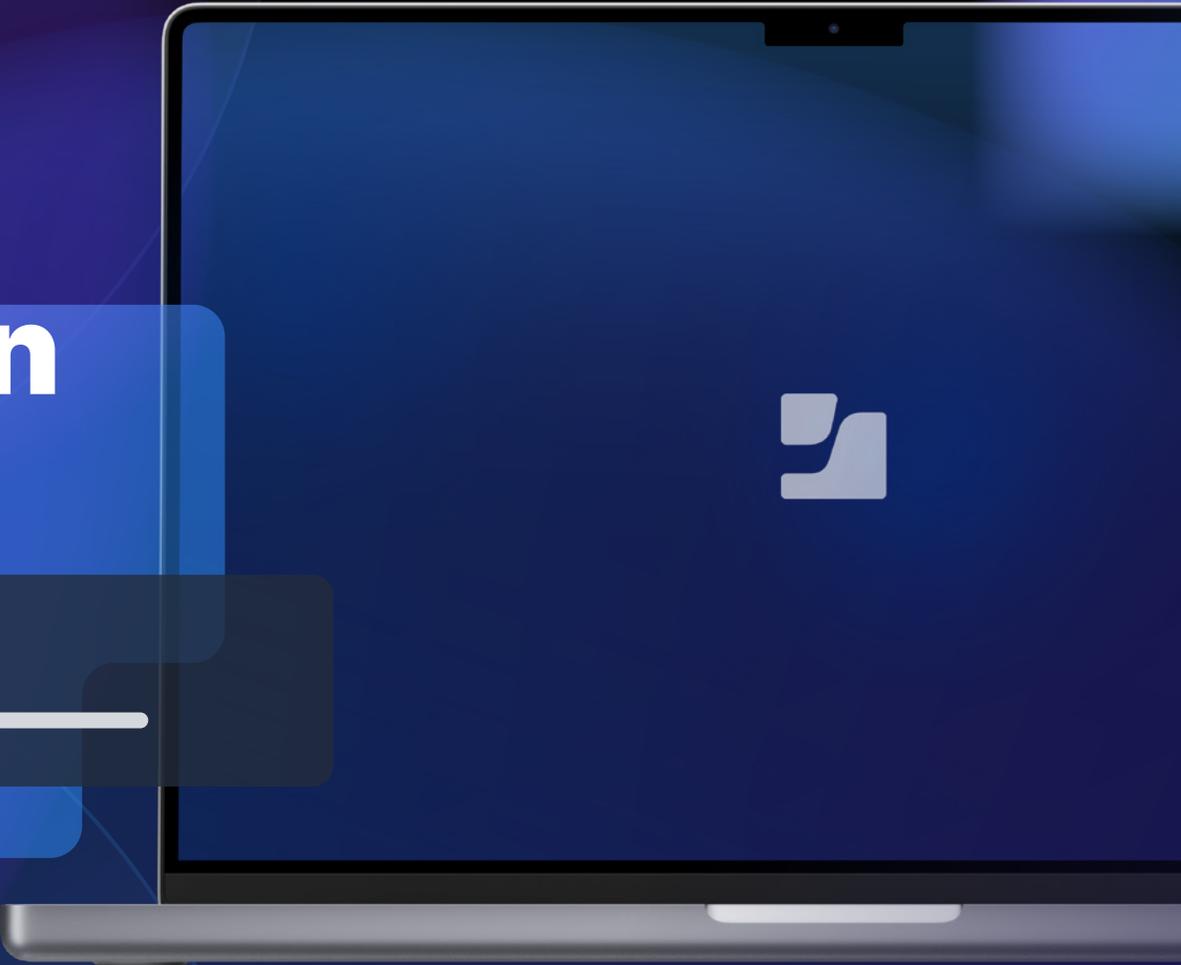


 jamf



Einführung von Macs im Unternehmen



Einführung

Mac Geräte machen derzeit 27 % aller Geräte im Unternehmen aus (gegenüber 24 % im Jahr 2024) und sind weiter auf dem Vormarsch. Trotz der zunehmenden Akzeptanz und der Erfolgsgeschichten von branchenführenden Organisationen weltweit zögern einige IT-Teams noch immer, macOS Produkte in ihrer Umgebung aufzunehmen.

Dieses Zögern rührt oft von der falschen Vorstellung her, dass die Verwaltung von Macs von Natur aus komplexer ist, dass macOS sich nicht gut in andere Plattformen integrieren lässt oder dass die Einführung von macOS die Sicherheit gefährden könnte.

Tatsache ist aber, dass Apple robuste Werkzeuge und Fähigkeiten entwickelt hat, wie den Apple Business Manager, das MDM Framework, die Endpunktsicherheit API und integrierte Sicherheitsfunktionen. Mit diesen Tools können IT-Teams ihre Mac Flotten nahtlos und sicher verwalten. In Kombination mit der richtigen Lösung im Unternehmen helfen diese Tools den IT-Teams, den Mac sicher und effizient neben anderen Plattformen zu integrieren.

In diesem Whitepaper wird untersucht, wie Organisationen häufige Herausforderungen überwinden und Macs in großem Umfang erfolgreich einführen und unterstützen können.

Schritte zur Einführung von Macs

Dieses Whitepaper bietet Anleitungen und Konfigurationen, die auf die speziellen Anforderungen von Unternehmen zugeschnitten sind. Die Compliance-Anforderungen variieren oft je nach Organisation, Industrie und Region.

Wir konzentrieren uns auf Best Practices und wichtige Aspekte, die Führungskräfte vor, während und nach der Einführung von Macs in ihren Umgebungen berücksichtigen sollten. Dieser Ansatz trägt dazu bei, das Risiko bei der Integration zu minimieren, und gibt Unternehmen die Flexibilität, Macs in einem Tempo einzuführen, das ihren Bedürfnissen entspricht.

Der Inhalt ist in drei Abschnitte organisiert:

1. **Wichtige Aspekte bei der Einführung von Macs (VORHER)**
2. **Best Practices für einen erfolgreichen Einsatz (WÄHREND)**
3. **Kontinuierliche Verwaltung, Sicherheit & Unterstützung (DANACH)**

„Ein Ziel ohne Plan ist nur ein Wunsch.“

- Antoine de Saint-Exupéry

Wichtige Aspekte bei der Einführung von Macs

Die Einführung von Macs im Unternehmen ist nicht nur eine technische, sondern auch eine strategische Entscheidung.

Geschäftsziele unterstützen

Um eine erfolgreiche Einführung zu gewährleisten, müssen die IT-Führungskräfte die Einführung von Macs zunächst mit den allgemeinen Unternehmenszielen abstimmen, z. B.:

- Verbesserung der Nutzerproduktivität
- Verbesserung des Sicherheitsstatus
- Anwerbung/Bindung von Spitzentalenten

Beurteilung der organisatorischen Bereitschaft

Als Nächstes müssen Führungskräfte **die Bereitschaft ihrer Organisation beurteilen**, um den Mac erfolgreich einzuführen:

- Infrastruktur
- Assets/Bestand
- Ressourcen (Daten/Dienste)
- IT-Unterstützungsfähigkeiten

Tools für die Kompatibilität optimieren

Die Integration einer **bewährten Lösung für Macs** gewährleistet die Unterstützung nativer Plattformen und optimiert die Abläufe. Durch die Maximierung der Kompatibilität zwischen der von den Stakeholdern verwendeten Software und den von ihnen genutzten Diensten können plattformübergreifend eingesetzte Ressourcen zur Unterstützung des Geschäftserfolgs genutzt werden – ohne ihn zu beeinträchtigen.

Sicherheit und Compliance

macOS bietet zwar starke native Funktionen, die mit vielen Standards und Frameworks der Industrie übereinstimmen, aber es erfüllt nicht alle Anforderungen. Jamf baut auf den nativen Funktionen von macOS auf und ermöglicht es Organisationen, diese zu nutzen:

- Erfüllung der gesetzlichen und branchenüblichen Compliance-Anforderungen
- Überwachung, Auditierung und Durchsetzung von Compliance-Richtlinien in großem Umfang
- Erreichung eines konsistenten Schutzes über alle Plattformen hinweg

Implementierung von Support und Training für die Nutzer:innen

Die effektive Unterstützung der Nutzer:innen ist ein wichtiger Faktor für den Erfolg. Schulungen und ein reibungsloses Onboarding erleichtern den Stakeholdern den Übergang. Weitere Vorteile sind:

- **kuratierte Unterstützung** befähigt zu unabhängiger Problemlösung
- mehr Zeit für IT-Teams, um sich auf strategische Aufgaben zu konzentrieren
- Steigerung der Produktivität der Stakeholder und Reduzierung von Fehlern

Leistung messen, um den Erfolg zu steigern

Das Verständnis der Fortschritte bei der Erreichung von Zielen ist ein wesentlicher Bestandteil jedes Geschäftsmodells. Nur durch eine Bewertung der Leistung können wir **die Risikofaktoren wirklich erkennen und abmildern**, um die gewünschten Ergebnisse zu erzielen. Die Messung von KPIs hilft bei:

- der Nachverfolgung der erfolgreichen Einführung
- Effizienzsteigerung
- Leitfaden für künftige Verbesserungen

Checkliste für die Bereitstellung von Macs in Windows-zentrierten Unternehmen

Bevor Mac Geräte in einer Windows-Umgebung bereitgestellt werden, ist es wichtig, einen Plan zu entwickeln, der Mac spezifische Tools und Arbeitsabläufe in den breiteren Technologie-Stack integriert. Dies gewährleistet die Kompatibilität mit Unternehmenssystemen, unterstützt die einzigartigen Stärken der macOS-Plattform und ermöglicht einen reibungslosen plattformübergreifenden Betrieb.

1. Die Einführung von Macs an den Unternehmenszielen ausrichten

- Wie kann der Mac die zentralen Unternehmensziele unterstützen (z. B. Produktivität, Talentbindung und Verbesserung der Sicherheit)?
- Holen Sie sich die Unterstützung der Geschäftsleitung und entwickeln Sie eine langfristige Strategie.
- Dokumentieren Sie messbare Erfolgskennzahlen in Bezug auf die Geschäftsergebnisse.

2. Beurteilung der organisatorischen Bereitschaft

- Auditieren Sie die Infrastruktur, um herauszufinden, ob sie für Macs kompatibel ist (Netzwerk, Identität, Sicherheit, Geräteverwaltung)
- Erfassen Sie Ihren Bestand und bewerten Sie plattformübergreifende Nutzungsszenarien.
- Überprüfen Sie die internen Support-Fähigkeiten für die Fehlerbehebung und die Eskalation von macOS.
- Identifizieren Sie wichtige Services und Datensysteme, die für den Betrieb des Macs wichtig sind.

3. Tools und Kompatibilität der Software optimieren

- Wählen Sie eine einheitliche Lösung für die Identitätsverwaltung, die sowohl macOS als auch Windows unterstützt (z. B. Identitätsprovider, Softwareverteilung und Sicherheitsgrundlagen)
- Sorgen Sie dafür, dass wichtige Apps verfügbar oder mit macOS kompatibel sind.
- Standardisieren Sie die Workflows und Services für eine plattformübergreifende Nutzbarkeit.
- Erstellen Sie eine auf macOS zugeschnittene Strategie für die Bereitstellung und das Patchen von Apps.

4. Angleichung an die Frameworks für Sicherheit und Compliance

- Integrieren Sie die Macs in den bestehenden Sicherheitsstatus (EDR, VPN/ZTNA, SSO, MDM).
- Übernehmen Sie Compliance-Standards (NIST, CIS, ISO) für die macOS-Flotte.
- Konfigurieren Sie Richtlinien zur Überwachung und zum Auditieren der Parität mit Windows-Systemen.
- Überprüfen Sie die Einstellungen für die Verschlüsselung, Authentifizierung und Endpunktsicherheit.

5. Vorbereitung von Schulungsprogrammen & Support für die Nutzer:innen

- Entwickeln Sie macOS-spezifische Onboarding- und Orientierungsressourcen.
- Führen Sie Schulungen für Support-Mitarbeiter zu Apple-spezifischen Tools und Verfahren zur Lösung von Tickets durch.
- Stellen Sie den Nutzer:innen Self-Service-Ressourcen und eine Wissensdatenbank zur Verfügung.
- Kommunizieren Sie die Vorteile von Mac und die Support Channels klar an Ihre Nutzer:innen.

6. Festlegung von Leistungs- und Erfolgskennzahlen

- Definieren Sie KPIs für die Einführung von Macs (z. B. Bereitstellungszeit, Nutzerzufriedenheit, Anzahl der Tickets).
- Überwachen Sie Nutzungstrends und die plattformübergreifende Leistung.
- Verfolgen Sie die Compliance, Sicherheitsvorfälle und Kennzahlen zum Zustand des Systems.
- Nutzen Sie die Ergebnisse, um die Roadmap für die Mac Integration zu verbessern.

Best Practices für einen erfolgreichen Einsatz

Die Einführung von Macs findet nicht in einem Vakuum statt - es gibt mehrere Aspekte, die zu einem nahtlosen Erlebnis für alle Stakeholder beitragen.

Planen Sie jeden Schritt, jedes Verfahren und jeden Workflow.

Die erfolgreiche Einführung des Macs in Ihrem Unternehmen beginnt mit einem gut ausgearbeiteten Plan. Die Abbildung der einzelnen Phasen im Lebenszyklus des Geräts - einschließlich der Prozesse und Workflows - hat folgende Vorteile:

- sorgt für plattformübergreifende Prozesse und Workflows
- verringert die Risiken durch die Parität der Plattformsicherheit
- hält die IT- und Sicherheitsteams funktional aufeinander abgestimmt

Automatisierte Bereitstellung und Nutzung

Durch die Bereitstellung können Geräte sofort nach dem Auspacken konfiguriert werden. Durch die Automatisierung wird der manuelle Aufwand eliminiert und jedes Gerät erhält eine konsistente Konfiguration, während gleichzeitig die Produktivität der Stakeholder beschleunigt wird. Darüber hinaus wird nicht nur die Fehlerwahrscheinlichkeit verringert, sondern es werden auch IT-Ressourcen für Aufgaben freigesetzt, die ihren Fähigkeiten entsprechen.

Nahtlose, sichere Integration mit Systemen

Durch die nahtlose und sichere Integration von Mac Geräten in Ihre Infrastruktur werden vorhandene Geräte, Services und Ausrüstungen zusammengeführt, was zu einem zentralisierten Betrieb führt, der als Grundlage für die IT und Unternehmen dient. Neben der Integration von Management, Identität und Sicherheit können Unternehmen:

- einheitliche Erfahrungen für die Stakeholder auf allen Plattformen gewährleisten
- Richtlinien durchsetzen und Bedrohungen schneller erkennen und darauf reagieren
- die Unterstützung der IT und ihre Ausrichtung auf die Unternehmensziele verbessern

Geräte überwachen und mit Patches auf dem neuesten Stand bleiben

Eine konsequente Überwachung und rechtzeitige Software-Updates sind entscheidend für die Aufrechterhaltung leistungsfähiger, sicherer Endpunkte. Eine zentrale Lösung für die Verwaltung, die macOS nativ unterstützt, ist hilfreich für:

- Festlegung von Baselines und Messung der Compliance anhand von Benchmarks
- Erfassung und Analyse von Telemetriedaten zum Zustand der Geräte in Echtzeit
- Automatisierung der Patch-Verwaltung zur Behebung von Schwachstellen/Bedrohungen

Kommunikation mit Stakeholdern und Dokumentation des Feedbacks

Die Stakeholder sind für den Erfolg von Mac-Initiativen von entscheidender Bedeutung. Durch regelmäßige Kommunikation bleiben alle Beteiligten während des gesamten Prozesses informiert und engagiert. Darüber hinaus trägt die Erfassung von Feedback nicht nur zur Identifizierung von Schmerzpunkten bei, sondern auch zur kontinuierlichen Verbesserung durch datengestützte Entscheidungsfindung.

„Tun Sie Ihr Bestes, bis Sie es besser wissen. Wenn Sie es dann besser wissen, machen Sie es besser.“

- Maya Angelou

Checkliste für Best Practices bei der Bereitstellung von Macs in Windows-orientierten Unternehmen

Bei der Bereitstellung von Mac Geräten in einer Windows-basierten Umgebung ist die Abstimmung mit Windows-Endpunkten entscheidend, um Sicherheitslücken zu minimieren und sicherzustellen, dass Compliance-Anforderungen nicht nur erfüllt, sondern auch unternehmensweit ganzheitlich durchgesetzt werden – unabhängig von der verwendeten Plattform.

1. Planen Sie jeden Schritt, jeden Prozess und jeden Workflow

- Bilden Sie jede Phase des Lebenszyklus eines Macs ab - von der Registrierung bis zur Außerbetriebnahme -, damit alle wissen, wie die Prozesse und die Abläufe sind.
- Definieren Sie plattformübergreifende Workflows, die nahtlos in macOS- und Windows-Umgebungen funktionieren.
- Stimmen Sie die IT- und Sicherheitsfunktionen aufeinander ab, um die Plattformparität aufrechtzuerhalten und Risiken zu reduzieren.

2. Automatisieren Sie die Bereitstellung und die Nutzung

- Implementieren Sie eine Zero-Touch-Bereitstellung mit dem Apple Business Manager und Tools für die Mobilgeräteverwaltung.
- Konfigurieren Sie automatisierte Workflows für die Bereitstellung, um eine konsistente Einrichtung von Geräten im großen Maßstab zu gewährleisten.
- Eliminieren Sie manuelle Schritte, um Fehler zu reduzieren. Dadurch kann das IT-Personal an strategischen Aufgaben arbeiten.

3. Integrieren Sie die Macs sicher in die Systeme im Unternehmen

- Integrieren Sie die Mac Geräte in Ihre Kernsysteme wie Identitätsprovider, Geräteverwaltung und Plattformen zur Endpunktsicherheit.
- Sorgen Sie dafür, dass Richtlinien in macOS- und Windows-Flotten konsistent durchgesetzt werden.
- Zentralisieren Sie den Betrieb für eine bessere Transparenz und schnellere Reaktion auf Sicherheitsereignisse.

4. Überwachen Sie Ihre Geräte und automatisieren Sie die Patch-Verwaltung

- Verwenden Sie Tools, die macOS nativ unterstützen, um den Zustand, die Compliance und Aktivitäten der Geräte in Echtzeit zu verfolgen.
- Automatisieren Sie die Bereitstellung von Software und Sicherheitspatches, um die Endpunkte auf dem neuesten Stand zu halten.
- Legen Sie Baselines für die Performance fest und messen Sie diese anhand von Compliance-Benchmarks

5. Kommunizieren Sie mit Stakeholdern und holen Sie Feedback ein

- Halten Sie die Stakeholder während des gesamten Prozesses der Einführung von Macs mit regelmäßigen Updates und Abstimmungsgesprächen auf dem Laufenden.
- Erstellen Sie Feedback-Schleifen, um Nutzererlebnisse und betriebliche Herausforderungen zu erfassen.
- Nutzen Sie Feedback, um Workflows zu verfeinern, die Nutzerzufriedenheit zu erhöhen und künftige Verbesserung einzuleiten.

Laufende Verwaltung, Sicherheit und Unterstützung

Eine engere Abstimmung mit den Unternehmenszielen bedeutet, dass Ihre Technologie im Einklang mit den Anforderungen der Organisation wächst und sich weiterentwickelt.

Best Practices für die Geräteverwaltung

Der Einsatz von MDM-Lösungen (Mobile Device Management) rationalisiert die IT-Verwaltung, während die Automatisierung den manuellen Aufwand reduziert. Die Aufrechterhaltung der Compliance ist für macOS genauso wichtig wie für andere Plattformen in Ihrer Umgebung, weshalb MDM die entscheidende Grundlage für diese Dinge bildet:

- Bereitstellung von sicheren Konfigurationen und Entwicklung von Baselines
- Nutzung einer richtlinienbasierten Verwaltung zur Durchsetzung der Compliance
- Patches für OS- und App-Schwachstellen, Abwehr von Bedrohungen

Nutzeridentitäten und Endpunktsicherheit verwalten

Sichere Identitäts-, Konfigurations- und Endpunktverwaltung fließen direkt in die Zugriffsverwaltung ein, die für den Schutz sensibler Daten auf allen Plattformen unerlässlich ist. Durch die Kopplung von Identitäts- und Endpunktsicherheit kann die IT ein umfassendes Sicherheitspaket implementieren, das es den Stakeholdern ermöglicht, sich auf die Produktivität zu konzentrieren:

- Ermöglichung von Single Sign-On mit starker MFA über alle Unternehmensressourcen hinweg
- Überprüfung des Gerätezustands mittels Telemetrie, bevor der Zugang gewährt wird
- Wahrung des Datenschutzes der Stakeholder ohne Beeinträchtigung der Datensicherheit

Wichtige Strategien für die Instandhaltung von Mac Geräten in großem Umfang

Die Verwaltung von Mac Geräten in einer wachsenden Organisation erfordert skalierbare Prozesse und eine ständige Kontrolle. Durch die Integration von Verwaltungs-, Identitäts- und Sicherheitslösungen werden fortschrittliche Automatisierungen ermöglicht, die plattformübergreifende Workflows standardisieren und eine stabile, mit dem Unternehmen mitwachsende IT-Umgebung gewährleisten.

Langfristigen Support und Instandhaltung etablieren

Eine langfristige Mac Strategie geht über die erstmalige Bereitstellung hinaus - sie erfordert einen kontinuierlichen Support, um sicherzustellen, dass Mac Geräte in gleicher Weise wie Windows Endpunkte verwaltet und gesichert werden.

Glücklicherweise ist dieser Prozess durch die Integration mit vorhandenen Tools wie Microsoft Entra ID, Splunk und anderen SIEMs-Plattformen sehr einfach. Die Ausweitung der Identitäts- und Sicherheits-Workflows auf Macs ermöglicht es der IT, den Betrieb ganzheitlich zu optimieren und sich gleichzeitig auf Schulungen zu konzentrieren, um einen reibungslosen Betrieb der Geräte und die Produktivität der Stakeholder gewährleisten.

Upgrades mit iterativem Feedback

Stakeholder spielen eine wichtige Rolle bei der Gestaltung von Mac Umgebungen, die der Produktivität dienen. Das Einholen von Feedback ist eine wichtige Voraussetzung für die Identifizierung von Problempunkten. Außerdem ermöglicht es Effizienzsteigerungen, wenn es mit bestehenden oder neuen Technologien kombiniert wird, was zu folgenden Ergebnissen führt:

- Leistungssteigerung durch erweiterte Workflows
- Maximierung der Nutzerzufriedenheit in der gesamten Organisation
- iterative Verbesserungen, die die Akzeptanz im Unternehmen fördern

Checkliste für fortlaufende Mac-Verwaltung und -Sicherheit für Windows-orientierte Unternehmen

Sobald Macs in einer Windows-Umgebung bereitgestellt werden, muss die IT mehrere Plattformen supporten. Durch sorgfältige Planung (vorher) und eine durchdachte Bereitstellung (während) werden kontinuierlicher Support und Compliance (danach) für die Geschäftsziele und die Produktivität der Stakeholder zu den entscheidenden Aufgaben der IT.

1. Standardisierung der Geräteverwaltung mit MDM

- Implementieren Sie eine macOS-native MDM-Lösung, um die Konfiguration und Compliance zu zentralisieren.
- Richten Sie sichere Konfigurationsbaselines ein, die mit den Endpunktrichtlinien von Windows übereinstimmen.
- Nutzen Sie die richtlinienbasierte Verwaltung, um Compliance durchzusetzen und Risiken zu reduzieren.
- Automatisieren von Patching-Workflows sowohl für Betriebssysteme als auch für Apps, um bekannte Schwachstellen zu beseitigen.

2. Sichere Identitäts- und Zugangskontrollen für Endpunkte

- Integrieren Sie Mac-Geräte in bestehende Identitätsrahmenwerke wie Microsoft Entra ID für eine einheitliche Zugriffskontrolle.
- Implementieren Sie starke MFA und Single Sign-On für macOS-Nutzer:innen, die auf Unternehmensressourcen zugreifen.
- Nutzen Sie die Gerätetelemetrie in ZTNA-Workflows, um den Zustand von macOS-Geräten zu überprüfen, bevor Sie Zugriff gewähren.
- Sorgen Sie für eine einheitliche Endpunktsicherheit, indem Sie Antiviren-, Überwachungs- und Verschlüsselungsrichtlinien für macOS durchsetzen.

3. Skalierung von plattformübergreifenden Verwaltungsworkflows

- Entwickeln Sie eine plattformübergreifende Automatisierung, die macOS in Workflows einbezieht, die traditionell auf Windows basieren.
- Zentralisieren Sie Identitäts-, Verwaltungs- und Sicherheitsplattformen für eine einheitliche Verwaltungserfahrung.
- Sorgen Sie für die Skalierbarkeit des Prozesses, um der steigenden Anzahl von Mac-Nutzer:innen gerecht zu werden, ohne den manuellen Arbeitsaufwand zu erhöhen.

4. Instandhaltung von Mac Geräten mit einer langfristigen Support-Strategie

- Erweitern Sie vorhandene Windows-basierte Support-Tools, um Mac-Umgebungen zu verwalten (z. B. Microsoft Sentinel).
- Bieten Sie Helpdesk-Schulungen mit Schwerpunkt auf macOS-spezifischer Fehlerbehebung und Benutzerunterstützung an.
- Passen Sie die routinemäßigen Wartungspläne für macOS an die Intervalle für Windows-Updates an, um das Patch-Management zu standardisieren.

5. Verbesserung der Abläufe mit iterativem Feedback der Stakeholder

- Holen Sie strukturiertes Feedback von Mac Nutzer:innen ein, um Lücken und Reibungspunkte zu identifizieren.
- Kombinieren Sie das Feedback mit Analysen, um Workflows zu optimieren und die Leistung der Geräte zu steigern.
- Wenden Sie die Ergebnisse in schrittweisen Iterationen an, um die Akzeptanz, die Zufriedenheit der Nutzer:innen und die betriebliche Effizienz zu steigern.

Warum Mac Geräte?

Die Einführung von Macs in Unternehmen stößt auf Widerstand seitens der IT-Abteilung. Da es viele Mythen über Kosten, Kompatibilität, Verwaltung, Sicherheit und Fachwissen gibt, kann es schwierig sein, sich für macOS im Unternehmen zu entscheiden.

Die wichtigsten Unterschiede, die die IT bei der Bereitstellung von Mac vs. Windows kennen sollte

Obwohl beide Plattformen in modernen Umgebungen in Unternehmen nebeneinander bestehen können, gibt es bei der Bereitstellung von Macs spezifische Merkmale, auf die sich IT-Teams einstellen müssen. Das Verständnis dieser Unterschiede trägt dazu bei, eine reibungslose Einführung, eine starke Sicherheitslage und eine optimierte Benutzererfahrung zu gewährleisten, neben einer gleichwertigen Verwaltung und Sicherheit wie bei den Entsprechungen unter Windows.

Was unterscheidet Mac-Bereitstellungen von Windows?

- Die Registrierung erfolgt identitätsgesteuert und automatisiert über den Apple Business Manager und MDM - keine Bildbearbeitung erforderlich.
- Mac Geräte verlassen sich auf eine deklarative Geräteverwaltung, bei der die Steuerlogik zur Durchsetzung der Richtlinien in Echtzeit auf das Gerät verlagert wird.
- OS- und Software-Updates werden standardmäßig von den Nutzer:innen genehmigt und müssen koordiniert werden, um die Zeitvorgaben für Patches einzuhalten.
- Hardware und Software sind eng miteinander verbunden, wodurch die Variabilität minimiert wird. Es sind jedoch Apple-spezifische Tools dafür erforderlich.
- macOS legt großen Wert auf die Privatsphäre und Sicherheit der Nutzer:innen und hat daher entsprechende Standardeinstellungen, die sich auf Telemetrie, Dateizugriff und Überwachungstools von Drittanbietern auswirken.
- Es ist keine Active Directory-Verbindung erforderlich, da Mac Geräte über SSO, SAML und Cloud Identity Anbieter integriert werden können.
- **Tools für den Lebenszyklus und Bereitstellungs-Workflows unterscheiden sich voneinander** und erfordern Skripting- und Automatisierungsstrategien, die nativ für macOS sind, um maximale Unterstützung zu gewährleisten.

Was tun, wenn Ihr Unternehmen noch unentschlossen ist, ob es Mac unterstützen soll?

Ganz gleich, ob Sie eine IT-Führungskraft sind, die für die Einführung des Macs plädiert, oder ein Mac Admin, der noch nie mit macOS gearbeitet hat - die **5 häufigsten Einwände der IT-Abteilung gegen den Mac im Unternehmen** helfen Ihnen, Fakten von Fiktion zu unterscheiden. Wenn Sie sich mit diesen Bedenken auseinandersetzen, werden Sie - gestützt durch Daten und Erfolge aus der Praxis - besser verstehen, warum die Einführung und Unterstützung von Macs viel einfacher ist, als es scheint.

TL;DR die folgenden Abschnitte enthalten die wichtigsten Vorteile für Organisationen bei der Verwaltung und Sicherung von Macs neben Windows in Umgebungen mit mehreren Plattformen.

Sicherheit

- Die Etablierung einer konsistenten Sicherheitsgrundlage gewährleistet einheitliche Sicherheitsstandards, reduziert die Komplexität und hält die Compliance für die gesamte Geräteflotte aufrecht.
- Das Bereitstellen kompatibler Apps aus vertrauenswürdigen Quellen optimiert die Software-Verteilung und sorgt dafür, dass die Anwendungen sicher und auf dem neuesten Stand sind.
- Die Überwachung in Echtzeit und die Analyse der Telemetrie standardisieren den Überblick über den Zustand der Geräte und erleichtern die Erkennung von Risiken, die Durchsetzung von Richtlinien und die schnelle Reaktion auf Bedrohungen.



Produktivität

- Die optimierte Bereitstellung von Macs durch Zero-Touch-Bereitstellung sorgt dafür, dass sie sofort nach der Auslieferung einsatzbereit und konform sind.
- Durch die Implementierung einer Zero-Trust-Architektur werden kompromittierte Geräte blockiert und das Risiko des Missbrauchs von Anmeldeinformationen beim Zugang zu geschützten Ressourcen im Unternehmen verringert.
- Sorgen Sie für eine standardisierte, nahtlose Benutzererfahrung, unabhängig vom Gerätetyp, der Betriebssystemplattform oder dem Nutzungsmodell.

Mitarbeiterzufriedenheit

- Minimieren Sie Ausfallzeiten für Stakeholder durch proaktives Verwalten des Gerätebestands und von Reparaturanfragen während des gesamten Lebenszyklus des Geräts.
- Das Kuratieren eines App-Katalogs für den Self-Service erlaubt es den Stakeholdern, häufige Probleme, wie z. B. die Installation von Apps oder das Zurücksetzen von Passwörtern, selbst zu lösen, ohne die IT zu belasten.
- Sie gewinnen und binden Top-Talente, indem Sie Mitarbeiterprogramme anbieten und sie dazu befähigen, störungsfrei mit der Plattform zu arbeiten, mit der sie sich am wohlsten fühlen.

Benutzerfreundlichkeit

- Sie erreichen einen umfassenden, ganzheitlichen Ansatz für die Zugangskontrolle und den Schutz vor Bedrohungen, wenn Sie die Endpunktsicherheit und IAM miteinander kombinieren.
- Durch kontinuierliches Verwalten des Gerätebestands und des Servicebedarfs unterstützen Sie die Effizienz im gesamten Lebenszyklus und die Betriebszeit der Geräte.
- Schalten Sie neue Funktionen frei und entwickeln Sie verbesserte Workflows, um die Geschäftskontinuität durch die Integration mit Tools und Lösungen besser zu unterstützen.

ROI/TCO

- **Sie können die Kosten für die Verwaltung und den Geräte-Support für Macs** um ein Drittel reduzieren im Vergleich zu Endpunkten von Windows
- **Durch eine höhere Leistung und Zuverlässigkeit der Geräte** steigern Sie die Produktivität der Mitarbeiter:innen um 3,5 %.
- Nach durchschnittlich vier Jahren der Nutzung liegt der Restwert eines Macs bei **30 % im Gegensatz zu 15 %** bei Windows PCs

5 wichtige Maßnahmen, die IT-Führungskräfte bei der Einführung von Macs in einer Windows-basierten Umgebung im Unternehmen priorisieren sollten

1.

Durch einheitliches Management können Sie eine Plattformparität herstellen.

Integrieren Sie Mac-spezifische Lösungen in bestehende Identitäts-, MDM- und Sicherheitsplattformen, um eine einheitliche Überwachung und Durchsetzung von Richtlinien unter macOS und Windows zu gewährleisten. Ein integrierter, auf erstklassigen Lösungen basierender Ansatz trägt dazu bei, die Gleichheit zu wahren, die Komplexität zu reduzieren und sowohl den Nutzer:innen als auch den Admins ein einheitliches Erlebnis zu bieten.

2.

Automatisiertes Bereitstellen und Zero-Touch-Nutzung

Nutzen Sie Apple Business Manager und MDM-Lösungen, um die Registrierung und Konfiguration von Geräten sowie die Anwendung von Richtlinien ab der Aktivierung der Macs zu automatisieren. Die Automatisierung eliminiert manuelle Fehler, beschleunigt die Zeit bis zur produktiven Nutzung und ermöglicht eine skalierbare, konsistente Bereitstellung im gesamten Unternehmen.

3.

Passen Sie die macOS Sicherheit an Standards im Unternehmen an.

Erweitern Sie die grundlegenden Sicherheitspraktiken - wie MFA, Endpunktsicherheit, Patch-Verwaltung und Compliance-Überwachung - auf macOS genauso stringent wie bei Windows. Dies schützt sensible Daten, gewährleistet die Einhaltung gesetzlicher Vorschriften und trägt dazu bei, unabhängig vom Gerätetyp ein hohes Maß an Sicherheit zu gewährleisten.

4.

Etablieren Sie eine Support-Infrastruktur und führen Sie Schulungen für die Belegschaft durch.

Schulen Sie die Teams vom IT-Support zu macOS-spezifischen Tools und unterstützen Sie die Nutzer:innen beim Onboarding und bei der Nutzung von Self-Service-Ressourcen. Ein proaktiver Support reduziert die Anzahl der Tickets, verbessert die Nutzerzufriedenheit und hilft den Stakeholdern, sich ohne Produktivitätsverlust auf der Plattform zurechtzufinden.

5.

Überwachen, messen und iterieren Sie kontinuierlich.

Überwachen Sie den Zustand der Macs, den Compliance-Status und das Feedback der Nutzer:innen zu nativen Tools und integrierten Lösungen. Iterative Verbesserungen auf der Grundlage von Daten in Echtzeit und Beiträgen der Stakeholder ermöglichen der IT eine schnelle Anpassung, eine Optimierung der Workflows und einen langfristigen Erfolg der Einführung.

Fazit

Obwohl dies ein weit verbreiteter Irrtum ist, ist die Einführung von Macs in Unternehmen keine Nischeninitiative – sie ist eine strategische Chance, die Infrastruktur zu modernisieren, Mitarbeiter:innen zu stärken und die Sicherheitslage plattformübergreifend zu verbessern. Mit einer durchdachten, bewussten Planung, der Anwendung von Best Practices und der Nutzung der richtigen Lösung können Organisationen Mac und Windows nahtlos integrieren und gleichzeitig eine Compliance-Parität in der gesamten Infrastruktur erreichen – und das alles ohne zunehmende Komplexität.

Ein konsistenter, sicherer und skalierbarer Verwaltungsansatz unterstützt die Flexibilität des Unternehmens und die Zufriedenheit der Stakeholder bei gleichzeitiger Senkung der Gesamtbetriebskosten und Maximierung der Investitionsrendite. Der Weg zu einer erfolgreichen Einführung von Macs ist nicht mit Kompromissen gepflastert – er basiert auf einer klaren Kommunikation mit den Stakeholdern, einer sicheren Integration von Tools und einer durchdachten, ganzheitlichen Vision der geschäftlichen Umgebung. Mit der richtigen Grundlage kann Ihre Organisation das gesamte Potenzial von Macs in großem Umfang ausschöpfen.



Die wichtigsten Punkte des plattformübergreifenden Supports

- Bringen Sie die Einführung von Macs mit den Unternehmenszielen in Einklang, um den Mehrwert für die Stakeholder zu steigern und deren Unterstützung zu erhalten.
- Standardisieren Sie Tools und Richtlinien zur Optimierung der Verwaltung und Sicherheit.
- Automatisieren Sie Bereitstellung, Patching und Updates, um Risiken und IT-Aufwand zu reduzieren.
- Implementieren Sie Zero-Trust durch die Integration bestehende Identitätsprovidern und Endpunktsicherheit.
- Schulen Sie die Nutzer:innen und etablieren Sie Self-Service-Tools zur Verbesserung der Produktivität und Zufriedenheit.
- Holen Sie Feedback ein und überwachen Sie den Zustand Ihrer Flotte, um kontinuierliche Verbesserungen zu erzielen.
- Reduzieren Sie die Gesamtbetriebskosten und entwickeln Sie langfristige Strategien, die die Unternehmensziele unterstützen.

Der Erfolg von morgen baut auf dem Fundament von heute auf.

Probieren Sie Jamf aus