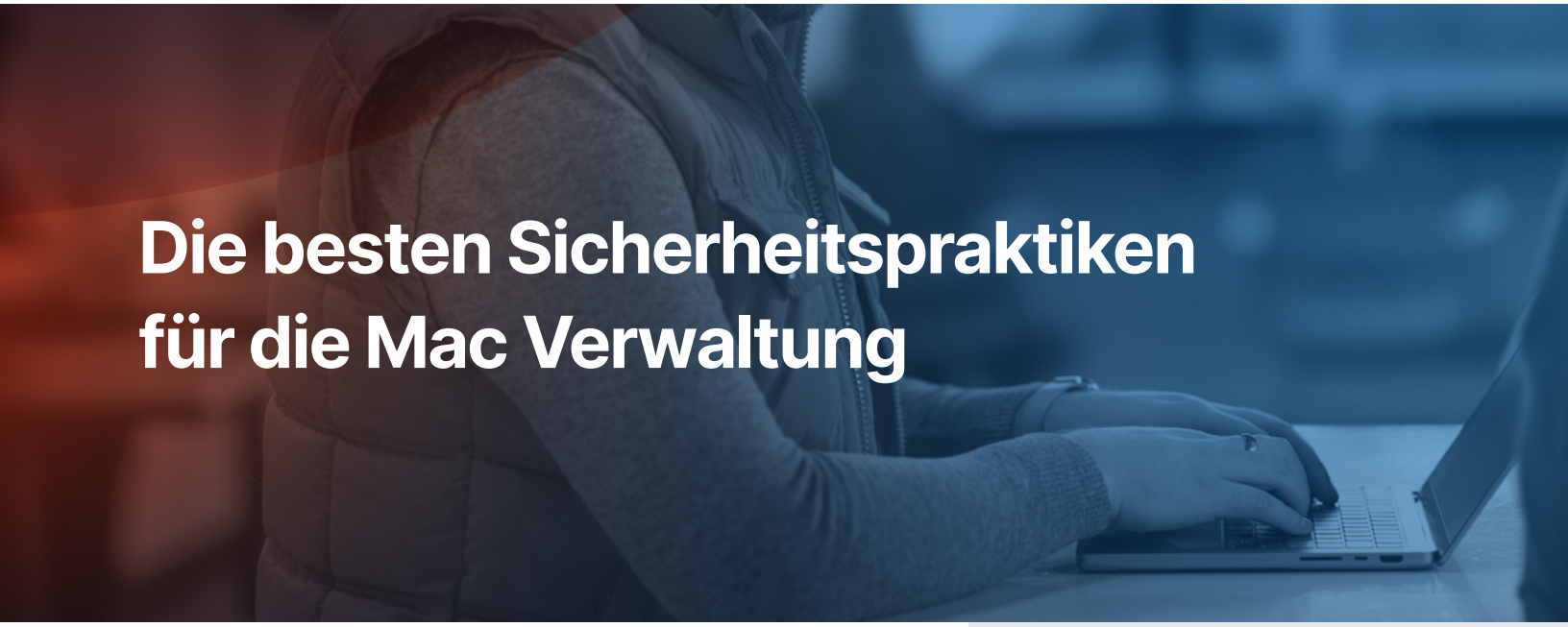
jamf



Die besten Sicherheitspraktiken für die Mac Verwaltung

Einführung

Die Weiterentwicklung der Geschäftsabläufe, wachsende Sicherheitsanforderungen und eine größere Auswahl für die Mitarbeiter:innen tragen auch weiterhin dazu bei, dass die **Mac Akzeptanzrate** in großen Unternehmen bei 76 % liegt. Laut einer Studie von Computerworld loben „neun von zehn IT-Fachleuten die geschäftlichen Vorteile von Macs, iPhones und iPads am Arbeitsplatz.“ Das ist eine gute Nachricht – sowohl für die Mitarbeiter:innen und als auch für Unternehmen! Durch die Diversifizierung der Auswahl an Technologien können Mitarbeiter:innen am produktivsten sein, wenn sie mit der Hardware und Software arbeiten, mit der sie sich am wohlsten fühlen.

Aus der Sicht des IT- und des Sicherheitsteams bringt jede Veränderung Variablen mit sich, die zu Risiken führen können, wenn sie nicht kontrolliert werden. Zum Glück für Unternehmen lassen sich die spezifischen Risiken von macOS durch proaktive, mehrschichtige Verteidigungsstrategien minimieren, die sich auf eine umfassende Lösung für die Verwaltung mobiler Geräte, Identitäts- und Zugriffskontrolle sowie Endpunktsicherheit konzentrieren. Diese Lösung erstreckt sich über Ihre gesamte Infrastruktur und schützt Geräte, Daten und Benutzer vor den sich ständig weiterentwickelnden Bedrohungen (mehr dazu im nächsten Abschnitt).

Die Integration von Lösungen eröffnet Möglichkeiten für detailliertere Sicherheitsmaßnahmen, um eine grundlegende Endpunktintegrität aufrechtzuerhalten. Dadurch wird die Konformität durchgesetzt und die Mitarbeiter:innen bleiben produktiv, während die IT-Abteilung mehr Zeit für die Entwicklung von Workflows hat, die die Geschäftsabläufe besser unterstützen. In diesem Dokument werden wir auf verschiedene kritische Sicherheitspraktiken eingehen:

- Patch- & Update-Verwaltung
- Erkennung von Bedrohungen & Reaktion auf Vorfälle
- Datenschutz & Verschlüsselung
- Netzwerk- & Anwendungssicherheit

Die Grundlage für Mac Verwaltung und Sicherheit

Bevor wir zu unserer Checkliste mit Sicherheitspraktiken kommen, sollte man sich bewusst machen, wie wichtig eine solide Grundlage ist, auf der die Prozesse und Workflows für die Mac Verwaltung aufbauen können. Eine skalierbare Lösung, die zum Beispiel keine taggleiche Unterstützung für die neuesten Patches bietet, kann sowohl die Geräte- als auch die Unternehmenssicherheit beeinträchtigen. Häufige Ursachen hierfür sind die verspätete Bereitstellung von Updates für die aktuellste macOS-Version durch die Entwickler sowie eine unzureichende Unterstützung wichtiger Features und Funktionalitäten.

Mobile Device Management (MDM)

Mit insgesamt 508 erfassten Sicherheitslücken rangierte macOS im Jahr **2024** auf Platz 9 der Top 50 CVEs (allgemeine Schwachstellen und Gefährdungen) und stellte damit eine nennenswerte Größe in der Statistik der Schwachstellen dar. Bis Mai 2025 ist macOS auf Platz 2 der Top 10 vorgerückt. Die **243 erfassten Schwachstellen** entsprechen bereits nahezu der Hälfte der Gesamtzahl aus dem Jahr 2024. Bitte beachten Sie, dass sich diese Rangliste im Laufe des Jahres verschieben kann, so dass sich die Anzahl der CVEs und ihre Position im Laufe der Zeit ändern können.

Dies unterstreicht, wie wichtig es ist, dass das Betriebssystem und die Apps auf dem neuesten Stand sind. Mithilfe von modernen Funktionen, wie der deklarativen Geräteverwaltung (DDM), können Geräte spezielle Einstellungen autonom durchzusetzen und Änderungen in Echtzeit zu melden. Dadurch wird nicht nur das MDM entlastet, sondern auch die Update-Geschwindigkeit und -Zuverlässigkeit verbessert, während IT-Teams umgehend über wichtige Statusänderungen informiert werden.

Obwohl MDM weit mehr als nur Patch-Management umfasst, ist seine Fähigkeit, Abläufe zu optimieren und die Effizienz bei Entscheidungsfindungen zu steigern, ebenso wichtig wie die zentrale Orchestrierung anderer entscheidender Aspekte der Mac Verwaltung. Zu den Fähigkeiten, die direkt auf den grundlegenden Charakter von MDM hinweisen, gehören:

- Bereitstellung sicherer Konfigurationen und Einstellungen
- Installation von verwalteten Apps
- Durchsetzung der Konformität auf der Grundlage von Richtlinien
- Pflege der aktuellen Bestände

Identität und Zugang

Der Schutz von Daten und die Sicherstellung, dass Mitarbeiter Zugriff auf die benötigten Ressourcen haben, um produktiv zu bleiben, mögen wie zwei separate Faktoren erscheinen, aber bei näherer Betrachtung sehen wir, dass sie untrennbar miteinander verbunden sind – und zwar durch ein gemeinsames Element: Berechtigungen. Laut dem **Verizon 2024 Data Breach Investigations Report** sind „68 % der Datenschutzverletzungen auf menschliches Versagen zurückzuführen." Diese Erkenntnis berücksichtigt keine bösartigen Insider, sondern konzentriert sich auf Vorfälle, die auf eine falsche Konfiguration von Berechtigungen (geringste Rechte) und auf Fehler der Endbenutzer in Bezug auf Anmeldeinformationen zurückzuführen sind.

Aus der Sicherheitsperspektive lässt sich dies nicht durch Schulungen zur Erkennung von Bedrohungen und deren Berichterstattung beheben. Um diese und ähnliche Sicherheitsbedenken erfolgreich zu bewältigen, benötigen Unternehmen eine Lösung, die über die Aktivierung von Cloud-basierten Identitäten hinausgeht. Zum Beispiel die Einführung von:

- risikobewussten Zugriffsrichtlinien, die den Zugang von kompromittierten Geräten und Accounts verweigern
- intelligentes Split-Tunneling verschlüsselt den geschäftlichen Datenverkehr unter Wahrung der Privatsphäre der Benutzer für den privaten Datenverkehr
- Multi-Faktor-Authentifizierung (MFA) erzwingt die Identitätsüberprüfung für Anfragen auf Ressourcen

Endpunktsicherheit

Über alle Plattformen hinweg machte **Malware, die auf macOS abzielte**, im Jahr 2024 etwa 11 % der weltweiten Malware-Erkennungen aus. Obwohl sie bei der Erkennung leicht hinter den anderen zurückliegen, sollten IT- und Sicherheitsteams diesen Trend nicht auf die leichte Schulter nehmen. Die Zahl hat sich im Vergleich zu vor zwei Jahren mehr als verdoppelt - und dank Malware-as-a-Service und anspruchsvoller, KI-gesteuerter Malware haben Bedrohungsakteure vermehrt Macs ins Visier genommen, was zu **einem deutlichen Anstieg** von Infostealer-Malware-Kampagnen geführt hat.

Zusätzlich zu anderem Schadcode, wie etwa Trojanern, die versuchen, die integrierten Code-Signing-Schutzmechanismen von macOS zu umgehen, sowie APTs, ist die Malware-Prävention eine kritische Notwendigkeit, um Geräte gegen die sich ständig weiterentwickelnde Bedrohungslage zu verteidigen. Darüber hinaus gibt es weitere Aspekte, die für die Aufrechterhaltung eines starken Sicherheitsstatus von Geräten und Organisationen unerlässlich sind.
Zum Beispiel:

- Identifizierung unbekannter Bedrohungen durch Verhaltensanalysen
- Verdächtige Apps und erkannte Bedrohungen in die Quarantäne verschieben und entfernen
- Aktive Überwachung, Warnmeldung und Berichte über Daten zum Zustand der Geräte (Telemetrie)
- Filtern des Zugangs zu riskanten Webinhalten, z. B. 0-Day-Phishing-URLs

Wichtige Sicherheitspraktiken für die Mac Verwaltung

Dieser Abschnitt ist sehr umfangreich, daher werden wir die wichtigsten Sicherheitspraktiken in Form einer Checkliste vorstellen. Dadurch erhalten IT- und Sicherheitsteams die nötige Flexibilität, um die erforderlichen Informationen anzuzeigen und umzusetzen. Dieses Format bietet den IT-Verantwortlichen eine klare, zusammengefasste Übersicht zu jedem Punkt, unterteilt in sieben Kategorien, die durch die Integration der drei Basislösungen ermöglicht werden.

Registrierung und Bereitstellung von Geräten

- Sichere Zero-Touch-Bereitstellungen von Geräten mit Registrierung im MDM
- Automatisierte Systemeinrichtung, einschließlich der Bereitstellung von verwalteten Apps und Konfigurationen
- Durchsetzung unternehmensweiter Standards und Sicherheitsrichtlinien über alle Besitzmodelle hinweg: firmeneigene Geräte und BYOD

Endpunktschutz und Konformität

- Härtung der macOS Sicherheitseinstellungen (FileVault, Gatekeeper, XProtect)
- Maßgeschneiderte Bedrohungsvermeidung auf dem Gerät und im Netzwerk durch individuelle Analysen
- Generierung von Sicherheitsrichtlinien zur Konfiguration von Endpunkten mit der gewünschten Konformitätsstufe, um individuelle Sicherheits-Baselines auf der Grundlage von Frameworks und Industriestandards zu erstellen

Identitäts- und Zugriffsverwaltung (IAM)

- Etablierung von rollenbasierten Zugangskontrollen (RBAC) für einen Zugang mit den geringsten Berechtigungen
- Minimierung des Risikos der Kompromittierung von Anmeldeinformationen durch SSO und passwortlose Authentifizierung
- Überwachung des Zustands von Geräten und Anmeldeinformationen mit der Zero-Trust-Architektur

Patch- und Update-Verwaltung

- Optimierung von OS- und App-Updates, um bekannte Schwachstellen automatisch zu beseitigen
- Tracking von Telemetriedaten und sicherer Austausch der Daten mit integrierten Lösungen in Echtzeit
- Sicherstellung der Konformität durch automatisierte, richtlinienbasierte Korrekturprozesse bei Erkennung von Verstößen

Erkennung von Bedrohungen und Reaktion auf Vorfälle

- Nutzung von ML, um die Erfassung und Analyse von Bedrohungsintelligenz zu automatisieren und datengestützte Anleitungen und Empfehlungen bereitzustellen
- Schnelle Behebung von Vorfällen mit nahtlosen Endpunkterkennungs- und Reaktions-Tools (EDR)
- Erweiterung der Bedrohungssuche und automatische Behebung mithilfe von KI und richtlinienbasierten Workflows

Datenschutz und Verschlüsselung

- Erzwingung einer FileVault-Verschlüsselung und automatische Schlüsselerfassung durch sichere Speicherung und Aktualisierung von Wiederherstellungsschlüsseln in Gerätedatensätzen
- Implementierung eines Zero-Trust-Netzwerkzugriffs (ZTNA) in der gesamten Infrastruktur und Überwachung des Gerätezustands und der Anmeldeinformationen, bevor der Zugang zu geschützten Unternehmensressourcen gewährt wird
- Speicherung der Daten auf geschützten Volumes und Verhinderung von unbefugter Weitergabe oder Kopieren an unsichere Orte per DLP (Data Loss Prevention)

Netzwerk- und Anwendungssicherheit

- Erzwingung einer netzwerkübergreifenden Sicherheit durch die ständige Verschlüsselung aller Netzwerkverbindungen und die Verwaltung von Firewall-Richtlinien
- Verwaltung von Apps von Drittanbietern und macOS Sicherheitsgrundlagen
- Segmentierung des Netzwerkverkehrs, um netzwerkbasierte Angriffe (Man-in-the-Middle) zu verhindern, indem jede Anfrage für Ressourcen durch einen eigenen Microtunnel geleitet wird

Jamf funktioniert! Echte Ergebnisse aus der Praxis

Effizienzsteigerung durch die Verkürzung der Bereitstellungszeiten für Geräte

„Wir sparen mehr als einen Tag pro Laptop im Vergleich zur manuellen Bereitstellung."

- Eigentümer des Produkts, Plattform für digitale elektronische Unterschriften und Automatisierung von Dokumenten.

Unternehmen, die Macs in großem Umfang einsetzen, erzielen **messbare Effizienzgewinne** und einen verbesserten Sicherheitsstatus.

Innovationen fördern, Routine minimieren

„Heute brauchen wir zehn Minuten pro Gerät. Das ist eine enorme Zeitersparnis."

- Leiter der Plattform für Informationstechnologie, Finanzverwaltung und Buchhaltung

Demonstrieren Sie die **spürbaren Zeiteinsparungen und die Ressourcenoptimierung**, die durch automatisierte Zero-Touch-Bereitstellungen erzielt werden.

Sichere Daten und produktive Benutzer – dank einer umfassenden Risikominimierung

„Die Funktionen zur Erkennung von Bedrohungen in Echtzeit, zur Überwachung der Einhaltung von Richtlinien und zur zentralen Durchsetzung von Richtlinien haben sich als entscheidend für den Schutz unserer Assets und die Einhaltung der Vorschriften erwiesen."

- Leiter der Informationstechnologie, digitale öffentliche Bibliothek

Optimieren Sie Ihre **Sicherheit** und Compliance durch die Mac Verwaltung. Setzen Sie dabei auf die Vorteile einer Bedrohungserkennung in Echtzeit sowie auf eine zentrale Durchsetzung Ihrer Sicherheitsrichtlinien.

Durchsetzung der organisatorischen Compliance während des gesamten Lebenszyklus der Geräte

„Diese Struktur erfüllt nicht nur die strengen Anforderungen von Standards wie SOC 2 Typ II, ISO und HIPAA, sondern unterstützte auch deren kontinuierliche Einhaltung. Dies verdeutlicht die Fähigkeit von Jamf, die organisatorische Sicherheit zu stärken und die Einhaltung von wichtigen Industrievorschriften zu gewährleisten."

- Senior Manager für Informationstechnologie, Unternehmen für digitale Gesundheit

Verbessern Sie proaktiv die Angleichung an Compliance-Benchmarks und **implementieren Sie Sicherheitsgrundlagen**, die auf branchenweit anerkannten Standards und Rahmenwerken basieren.

Fazit

Da die Nutzung von Macs in den Unternehmen weiter zunimmt, müssen Organisationen einen proaktiven, integrierten Ansatz für die Verwaltung und Sicherung ihrer Mac Flotte entwickeln. Angesichts neuer Bedrohungen und komplexer Arbeitsmodelle wie Hybrid- oder Remote-Work ist eine fokussierte Sicherheitsstrategie essenziell. Sie sollte sich eng an den Unternehmensabläufen orientieren und dennoch die nötige Flexibilität besitzen, um den individuellen Anforderungen der verschiedenen Stakeholder gerecht zu werden.

Dies erfordert mehr als nur eine Lösung, die für alle passt.

Vielmehr bedarf es einer mehrschichtigen Lösung, die den Mac in jeder Phase des Geräts und die Apps nativ unterstützt. Mit einem Mobile Device Management (MDM), einer Identitäts- und Zugriffsverwaltung (IAM) und einer Endpunktsicherheit schaffen Sie eine solide Grundlage. Dadurch können Unternehmen ihren Benutzern die Möglichkeit geben, sich ein Gerät auszusuchen, ohne sich zwischen Kompromissen bei der Sicherheit oder der Beeinträchtigung des Datenschutzes entscheiden zu müssen.

In einfachen Worten:

- **Geräte sind konform**
- **Daten sind sicher**
- **Benutzer sind geschützt**

In diesem Dokument wurden die wesentlichen Sicherheitspraktiken beschrieben, die erforderlich sind, um die Integrität der Endpunkte aufrechtzuerhalten und die Einhaltung von Vorschriften zu gewährleisten. Dadurch erhalten die Sicherheitsteams die nötigen Tools, um schnell auf Bedrohungen zu reagieren, und die IT-Teams können sich auf Innovationen konzentrieren, während sie den Stakeholdern erstklassigen Support bieten. Zusätzlich wird die Produktivität der Mitarbeiter:innen gestärkt, indem Unterbrechungen ihrer Arbeitsabläufe vermieden werden.

Wenn Lösungen nahtlos zusammenarbeiten, erhalten Unternehmen ein sicheres, skalierbares Mac Ökosystem, das neben Windows-PCs funktioniert und Produktivität, Benutzerfreundlichkeit und Schutz bietet und fördert - und so den Weg für Innovation und Widerstandsfähigkeit ebnet, wo auch immer Sie arbeiten.

Die wichtigsten Erkenntnisse

Die Akzeptanz des Macs in Unternehmen ist um **76 %** gestiegen, was auf die Präferenz der Mitarbeiter:innen und Produktivitätsvorteile zurückzuführen ist.

Endpunktsicherheit für macOS ist angesichts der zunehmenden Bedrohung durch Malware, einschließlich Infostealern und KI-gestützter Malware, wichtiger denn je.

90 % der IT-Fachleute erkennen die geschäftlichen Vorteile des Einsatzes von Apple Geräten am Arbeitsplatz.

Eine Zero-Trust-Architektur und Automatisierung spielen eine entscheidende Rolle bei der Einhaltung der Compliance, der Erkennung von Bedrohungen und der Verkürzung der Reaktionszeiten.

Die Integration grundlegender Lösungen sorgt für mehr Automatisierung und optimiert die Konformität bei minimaler Störung der Benutzer.

68 % der Sicherheitsvorfälle sind auf menschliches Handeln zurückzuführen – Berechtigungen und Zugriffskontrollen sind daher entscheidend.

Umfassende Lösungen müssen MDM, Identitäts- und Zugriffsverwaltung (IAM) und Endpunktsicherheit beinhalten.

IT- und Sicherheitsteams müssen sich auf neue Variablen einstellen, die durch Macs eingeführt werden, und benötigen integrierte, umfassende Verteidigungsstrategien, um die Risiken zu minimieren.

Mithilfe einer umfassenden und integrierten Strategie für die Sicherheit der Macs können Unternehmen sicher skalieren und die Produktivität maximieren.

Eine Defense-in-Depth-Strategie ist unerlässlich, um macOS-spezifische Risiken im gesamten Unternehmen zu minimieren.

jamf

Probieren Sie Jamf for Mac aus.

www.jamf.com/de/