

A silver MacBook laptop is shown from a three-quarter perspective, open. The screen displays a dark blue background with a white vertical line on the left side. The text 'Ein praktischer Leitfaden zur Konformität mit dem Mac' is overlaid on the screen in a large, white, sans-serif font.

Ein praktischer Leitfaden zur Konformität mit dem Mac

*Für IT-Teams, die immer mehr
Macs verwalten müssen*

Warum ist die Konformität bei Macs so wichtig?

Wachsende Unternehmen, die Macs und mobile Geräte verwalten, müssen Konformitätsanforderungen erfüllen und gleichzeitig einen effizienten und überschaubaren IT-Betrieb gewährleisten. Bei der Konformität geht es nicht nur um die Einhaltung rechtlicher oder regulatorischer Vorschriften. Sie spielt auch eine entscheidende Rolle bei der Stärkung der Sicherheit, der Verringerung von Risiken und dem Aufbau von Vertrauen, und das alles, ohne die ohnehin schon viel beschäftigten IT-Teams weiter zu belasten.

Zu verstehen, warum die Konformität mit Macs wichtig ist, bildet das Fundament für die Schaffung einer sicheren sowie skalierbaren Infrastruktur.

Die Konformität orientiert sich im Kern an Benchmarks. Ein Konformitäts-Benchmark in der IT-Sicherheit besteht aus einer Reihe von Standards, mit denen die Einhaltung von Vorschriften und Anforderungen durch eine Organisation gemessen wird, und bietet Best Practices für den Schutz sensibler Daten.

Die CIS-Kontrollen und -Benchmarks beispielsweise werden branchenübergreifend als Grundlage für bewährte Sicherheitsverfahren eingesetzt. Sie sind zwar nicht an eine einzelne Vorschrift gebunden, dienen aber häufig als Grundlage, auf der Unternehmen zusätzliche branchen- oder regionalspezifische Konformitätsmaßnahmen aufbauen, wie sie beispielsweise von GDPR oder HIPAA gefordert werden.

Wachsende Unternehmen nutzen diese Benchmarks, um Risiken zu reduzieren, Daten zu schützen und Sicherheitslücken zu vermeiden, während ihre Umgebungen wachsen. Denn die Nichteinhaltung einschlägiger Vorschriften kann zu hohen Geldstrafen, rechtlichen Schritten und Rufschädigung führen. Die regelmäßige Verfolgung und Einhaltung dieser Benchmarks hilft Unternehmen, in der digitalen Welt sicher und wettbewerbsfähig zu bleiben.



Was ist DDM?



Mit der deklarativen Geräteverwaltung (DDM) können Geräte proaktiv und autonom handeln, wenn sie aus der Konformität fallen. Dies erhöht die Systemzuverlässigkeit und reduziert gleichzeitig den manuellen Aufwand zur Durchsetzung der Konformität.

Wie können IT-Teams die Sicherheit für Macs aufrechterhalten?

IT-Admins lieben Apple unter anderem deshalb, weil der Mac über erstklassige, integrierte Sicherheitsfunktionen verfügt.

Für kleine IT-Teams, die sowohl für Macs als auch für mobile Geräte zuständig sind, sind diese integrierten Schutzmaßnahmen am effektivsten, wenn sie zentral verwaltet und automatisch durchgesetzt werden.

Mac Computer sind von Natur aus stabiler und effizienter als andere Geräte. Und mit den richtigen Tools kann die IT leistungsstarke, flexible Apple-spezifische Verwaltungs- und Sicherheitsmaßnahmen durchsetzen, ohne die hervorragende Apple-Benutzeroberfläche zu beeinträchtigen. Wenn Sie eine erstklassige MDM-Lösung mit dem DDM-Protokoll (Deklarative Geräteverwaltung) von Apple kombinieren, können Sie sicherstellen, dass sowohl die Unternehmensdaten als auch die Beschäftigten und die Netzwerke geschützt sind.

Rechtliche Konformität für Macs:

Was ist zu beachten?

Viele Organisationen müssen die gleichen Konformitätsanforderungen erfüllen wie größere Unternehmen, arbeiten aber mit schlankeren IT-Teams und weniger Ressourcen.

Infolgedessen bedeutet Konformität, sich mit mehreren Normen und Anforderungen gleichzeitig auseinanderzusetzen. Ihre Organisation hat wahrscheinlich mehrere Konformitätsstandards zu erfüllen. Diese Standards sorgen dafür, dass die Daten des Unternehmens und der Mitarbeiter:innen sicher bleiben. Das bedeutet, dass Sie diese ebenso umsetzen müssen wie die Benchmarks der Branche und der Behörden.

Wie viele Vorschriften gibt es eigentlich?

Jede Branche und Region hat ihre eigenen Vorschriften und Best Practices, die sich teilweise überschneiden. Eine kleine Auswahl aus aller Welt:

ISO

Die [ISO 27701-Zertifizierung](#) gewährleistet den ordnungsgemäßen Umgang mit personenbezogenen Daten im Gesundheitswesen weltweit



Die [deutschen IT-Sicherheitsgesetze 1.0 und 2.0](#) regulieren den IT-Schutz mit eigenen Sicherheitsanforderungen



Die [DORA](#)-Verordnungen betreffen die Regulierung der Finanzinstitute in der EU



[Cyber Essentials+](#) definiert minimale Sicherheitsstandards für alle Organisationen in Großbritannien



Die [CIS Benchmarks](#) des Zentrums für Internetsicherheit bieten präskriptive Empfehlungen für die Konfiguration, um die Sicherheit von Organisationen zu gewährleisten



Die [NIS2](#)-Anforderungen gewährleisten die Einhaltung der EU-weiten Rechtsvorschriften zur Cybersicherheit

Es gibt eine Menge komplexer Vorschriften, die es zu verfolgen und durchzusetzen gilt.

Sobald Sie herausgefunden haben, welche Anforderungen auf Ihr Unternehmen und Ihre Geräteumgebung zutreffen, besteht der nächste Schritt darin, die richtigen Prozesse zur Unterstützung dieser Anforderungen zu implementieren.

Mit einem modernen Ansatz für die Geräteverwaltung können IT-Teams einen Großteil dieser Arbeit automatisieren und die Konformität ihrer gesamten Flotte kontinuierlich überwachen.

Mit einer Geräteverwaltung können Sie:

- einheitliche Konfigurations- und Konformitätsrichtlinien verwenden
- dynamische Gruppierungen nutzen, um Einstellungen und Aktionen automatisch zuzuweisen
- Automatisierungen einsetzen, um den manuellen Aufwand zu reduzieren und die Konformität auf der Geräteebene aufrechtzuerhalten

Damit scheint alles unter Kontrolle zu sein. Sie könnten sich sogar für einen Moment zurücklehnen.

Außer...

Was sind dynamische Gruppen?



Mit **dynamischen Gruppen** können IT-Teams dynamisch aktualisierte Gruppen für verwaltete Computer, mobile Geräte oder Benutzer:innen auf der Grundlage definierter Kriterien erstellen. Diese Gruppen passen sich automatisch an, wenn Geräte oder Benutzer:innen die festgelegten Bedingungen erfüllen oder nicht mehr erfüllen, so dass keine manuellen Aktualisierungen mehr erforderlich sind.

Was sind die Entwürfe von Jamf?



Richtlinienbasierte Konfigurations-Workflows nutzen Apples Framework für die deklarative Geräteverwaltung, um Geräteeinstellungen, Befehle, App-Installationen und Beschränkungen effizienter und autonomer zu verwalten.

Erfahren Sie mehr über die [Entwürfe von Jamf](#)

In ihrer Gesamtheit unterstützen diese Funktionen IT-Teams dabei, Konformität und Konsistenz auch in großen Infrastrukturen bei minimalem laufendem Aufwand zu gewährleisten.

...bei der Konformität ist der Wandel die einzige Konstante.

Wenn sich die Technologie, Geschäftspraktiken und Vorschriften weiterentwickeln, müssen auch die Anforderungen an die Konformität mitwachsen. Das Ziel der Konformität besteht darin, die Sicherheit und den reibungslosen Betrieb in einer Organisation zu gewährleisten, auch wenn sich die Rahmenbedingungen ändern. Die kontinuierliche Anpassung an neue Sicherheitsrisiken und an die regulatorischen Anforderungen ist ein fortlaufender Prozess.

Dies beinhaltet in der Regel:

- ✓ **Regelmäßige Konformitätsaudits und Überprüfungen**
- ✓ **Zeitnahe Umsetzung von Updates für Betriebssysteme und die Sicherheit**
- ✓ **Laufende Überwachung auf Sicherheitsbedrohungen**
- ✓ **Anpassung an neue Vorschriften und Strategien**
- ✓ **Schnelles Reagieren auf Änderungen der Benutzerrollen oder des Zugriffs**

Diese Anforderungen klingen überwältigend und in der Tat ist die Umsetzung oft komplex.

An dieser Stelle wird eine strukturierte Checkliste für die Konformität unerlässlich:

Mit einem klaren, schrittweisen Ansatz können IT-Teams ihre Bemühungen in Bezug auf die Konformität optimieren und sich an neue Anforderungen anpassen.

Eine klar definierte Checkliste sorgt dafür, dass nichts übersehen wird und dass Sicherheitskontrollen, Überwachung und Durchsetzung konsequent berücksichtigt werden.

Vorbereitungsphase

- ✓ **Erstellen Sie Benutzerkonten und -profile.**
- ✓ **Legen Sie gemeinsam mit den Entscheidungsträgern in Ihrer Organisation Richtlinien und Berechtigungen fest.**
- ✓ **Definieren Sie externe Konformitätsvorgaben basierend auf den Branchen- oder gesetzlichen Vorschriften, denen Ihr Unternehmen unterliegt.**
- ✓ **Stellen Sie die Kompatibilität von Hardware und Software mit allen von Ihnen verwendeten Tools sicher.**

Was sind Konformitäts-Benchmarks?

Mithilfe von Konformitäts-Benchmarks können IT-Teams die Konformität auf strukturierte und wiederholbare Weise definieren, prüfen und durchsetzen.

Die Funktion:

- ✓ Reduziert den Zeitaufwand für die Prüfung und Durchsetzung der Konformität in der gesamten Geräteflotte
- ✓ Vereinfacht komplexe Sicherheitsstandards und Konfigurationsanforderungen
- ✓ Verbessert die allgemeine Sicherheit der Geräte

Konformitäts-Benchmarks automatisieren die Anwendung und Aufrechterhaltung von Sicherheitseinstellungen und tragen dazu bei, dass Geräte dauerhaft den definierten Standards entsprechen.

Beispiel:

Durchsetzung eines Konformitäts-Benchmarks, z. B. CIS Level 1

- 1 Wählen Sie die Art der Durchsetzung.
- 2 Wählen Sie die Geräte aus, für die dieser Benchmark gelten soll.
- 3 Passen Sie den Benchmark bei Bedarf an.
- 4 Speichern und bereitstellen.

Kontinuierliche Wartung und Überwachung

Konformitäts-Benchmarks geben Aufschluss über den Status der verwendeten Benchmarks und die allgemeine Konformität der Geräte. Und mithilfe der detaillierteren Ansichten können IT-Teams die Konformität auf der Ebene der einzelnen Regeln, z. B. der Kennwortanforderungen, genauer überprüfen.

Sehen Sie sich eine Demo zu Konformitäts-Benchmarks an:

Konformitäts-Benchmarks
in  Pro

Die Konformitäts-Benchmarks basieren auf dem macOS Security Compliance Project (mSCP), einem gemeinsamen Projekt von IT-Sicherheitsteams des National Institute of Standards and Technology (NIST), der National Aeronautics and Space Administration (NASA), der Defense Information Systems Agency (DISA) und des Los Alamos National Laboratory (LANL).

Einrichtung und Konfiguration

Durch die automatisierte Bereitstellung, können Sie dafür sorgen, dass jedes Gerät für seinen Benutzer korrekt konfiguriert ist und dass alle Apps und Zugriffseinstellungen auf Geräteebeane auf dem neuesten Stand sind.

- ✓ **Mit den Konformitäts-Benchmarks können Sie die Konfiguration vereinfachen und beschleunigen, indem Sie Anforderungen verwenden, die auf gemeinsamen Standards basieren, wie z. B. CIS Level 1 oder 2.**
- ✓ **Um Zeit zu sparen und die Konsistenz zu verbessern, könne Sie vordefinierte Konfigurationsvorlagen verwenden oder Ihre eigenen erstellen. Dies spart Zeit und erhöht die Sicherheit mit Richtlinien für Passwörter, Einstellungen für Service-Konfigurationsdateien und der Verwaltung von Hintergrundaufgaben.**
- ✓ **Wichtige Apps und Updates können Sie mit einer Kombination aus Self Service+ und dynamischen Gruppen installieren, so dass die Benutzer:innen auf die benötigten Tools zugreifen können, während die IT-Abteilung durch automatische Zuweisung die Kontrolle behält.**
- ✓ **Konfigurieren Sie die wichtigsten Sicherheitseinstellungen wie Festplattenverschlüsselung, Systemschutz und App-Kontrollen.**

Tests

- ✓ **Sie können die Funktionalität von Apps und Funktionen des Systems testen.**
- ✓ **Sie können Sicherheitsüberprüfungen und Audits zur Bestätigung der Konformität durchführen.**
- ✓ **Sie sollten in Erwägung ziehen, diese Änderungen zunächst einer kleineren Gruppe von Mitarbeiter:innen vorzustellen, die als „On-the-Job“-Tester fungieren können.**

Legen Sie einen guten Start hin

- ✓ **Geben Sie den Benutzer:innen klare Anweisungen.**
- ✓ **Planen Sie ein Kickoff-Meeting für Fragen und Fehlerbehebung.**
- ✓ **Stellen Sie sicher, dass automatisierte Aktualisierungen der Konformität aktiviert sind, damit die Systeme auch bei sich ändernden Anforderungen konform bleiben und der Aufwand für die Überwachung aktualisierter Konformitätsprotokolle minimiert wird.**

Was ist Self Service+ ?

Self Service+ ist ein Portal für die Endbenutzer:innen von macOS. Dadurch haben sie Zugang zu Inhalten und Updates, die in Jamf Pro vorkonfiguriert wurden. In Self Service+ können Benutzer:innen:

- 1 den Sicherheitsstatus ihrer Geräte einsehen**
- 2 nach Apps aus dem App Store und von Drittanbietern, Konfigurationsprofilen und Büchern suchen und diese installieren**
- 3 Identitätsbezogene Aufgaben wie das Ändern von Passwörtern durchführen**

Best Practices und künftige Überlegungen

Mit den richtigen Tools und Prozessen können Sie sicherstellen, dass Ihre Geräteflotte sicher konfiguriert ist und sowohl den gesetzlichen Anforderungen als auch den intern festgelegten Richtlinien entspricht.

Mit dem richtigen Ansatz lässt sich die Konformität mit minimalem Aufwand aufrechterhalten. Sicherheitsteams können außerdem problemlos Konformitätsdokumente und -Status erstellen und vorlegen, wenn dies für Audits oder Überprüfungen erforderlich ist.

Informieren Sie sich über Gesetzesänderungen, Vorschriften und Konformitätsstandards, indem Sie die Ankündigungen der Regulierungsbehörden verfolgen. IT-Teams sollten sich zwar immer über kommende Anforderungen im Klaren sein, aber Aktualisierungen von Konformitäts-Rahmenwerken und -Benchmarks können den manuellen Aufwand für die Einhaltung der Vorschriften verringern.

Wichtig ist, sich Folgendes vor Augen zu führen: Die Rolle der IT-Teams bei der zukunftssicheren Gestaltung und Aufrechterhaltung von Konformitätsbemühungen ist absolut entscheidend.

Um dieses Thema noch besser verstehen zu können, ist es ein guter Anfang, nach Informationen wie diesem E-Book zu suchen. Sie können auch diese Checkliste nutzen.

Und was ist vielleicht das Wichtigste von allem? Wenn Sie sich weiterhin für effiziente und verlässliche Konformitätspraktiken einsetzen, können Sie sicherstellen, dass Ihre Organisation auf künftige Veränderungen vorbereitet ist.



Wir zeigen Ihnen, wie Jamf die Verwaltung der Konformität vereinfachen kann.

Testversion anfordern