jamf

Die IT-Checkliste für die Mac Compliance

Bei Compliance geht es nicht nur um die Einhaltung gesetzlicher Vorschriften. Dabei geht es auch um mehr Sicherheit, weniger Risiken und mehr Vertrauen.

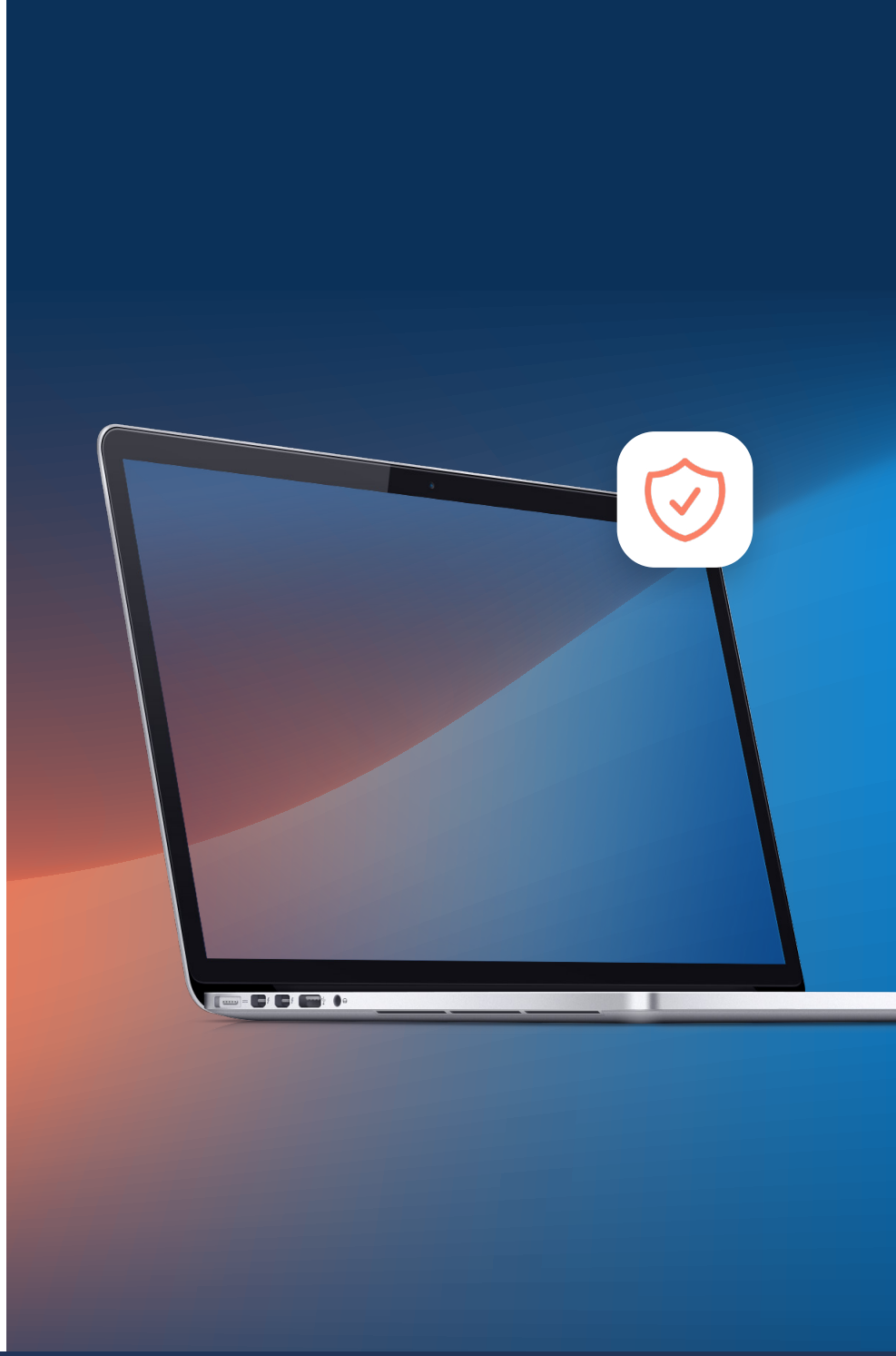
Warum ist die Mac Compliance wichtig?

Die meisten Organisationen, unabhängig von ihrer Größe oder Branche, müssen in irgendeiner Form Compliance-Vorschriften einhalten, insbesondere beim Umgang mit sensiblen Daten.

Ein Compliance-Benchmark in der IT-Sicherheit ist eine 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.

CIS Controls und CIS Benchmarks sind freiwillige Richtlinien des Zentrums für Internetsicherheit (CIS), die weithin übernommen werden, um Sicherheitsanforderungen wie die GSDVO oder HIPAA zu erfüllen.

Organisationen müssen sich an diese Benchmarks halten, um Sicherheitsrisiken zu verringern, das Vertrauen der Kunden zu stärken und Strafen zu vermeiden. 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.



Wie können IT-Admins die Sicherheit für Macs aufrechterhalten?

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

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 Compliance für Macs:
Was ist zu beachten?

Es gibt viel zu bedenken, wenn es um Compliance in Ihrer Organisation geht.

Ihre Organisation hat wahrscheinlich mehrere Compliance-Standards zu erfüllen. Diese Standards sorgen dafür, dass die Daten des Unternehmens und der Mitarbeiter:innen sicher bleiben. Das bedeutet, dass Sie Sie 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:

Die **ISO 27701-Zertifizierung** gewährleistet den ordnungsgemäßen Umgang mit personenbezogenen Daten im Gesundheitswesen weltweit

DORA-Verordnungen betreffen die Regulierung der Finanzinstitute in der EU

Die **CIS Benchmarks** des Zentrums für Internetsicherheit bieten präskriptive Empfehlungen für die Konfiguration, um die Sicherheit von Organisationen zu gewährleisten

NIS2 -Anforderungen gewährleisten die Einhaltung der EU-weiten Rechtsvorschriften zur Cybersicherheit

Die deutschen IT-Sicherheitsgesetze 1.0 und 2.0 regulieren den IT-Schutz mit eigenen Sicherheitsanforderungen

Cyber Essentials+ definiert minimale Sicherheitsstandards für alle Organisationen in Großbritannien

Dies sind sicherlich eine Menge komplexer Vorschriften, die es zu verfolgen und durchzusetzen gilt!

Nehmen wir an, Sie bleiben beharrlich; Sie recherchieren und ermitteln, welche Vorschriften für Ihre Organisation und Geräteumgebung gelten. Dank Ihres erstklassigen MDM und Ihres eigenen gründlichen QS-Verfahrens können Sie nun eine automatisierte Methode zur Umsetzung und kontinuierlichen Validierung der Compliance implementieren.

Mit der Geräteverwaltung haben Sie folgende Vorteile:

- **Ausgefeilte Konfigurationsprofile, Compliance-Erklärungen und Blueprints**
- **Einrichtung von Smart Groups für dynamische Zuweisungen von Profilen und Befehlen**
- **Automatisierungen, die Zeit sparen und die sofortige Einhaltung der Compliance auf der Geräteebene gewährleisten**

Dann können Sie sich gemütlich abmelden und vielleicht ein lang aufgeschobenes Nickerchen machen.

Außer...

...In der Compliance ändert sich immer alles.

Da sich das Internet, die IT, die Geschäftspraktiken und die Gesetze ändern, müssen sich auch Ihre Compliance-Konfigurationen ändern. Das Ziel der Compliance ist es, die Sicherheit und einen reibungslosen Betrieb des Unternehmens zu gewährleisten. Es ist Teil des Prozesses, immer auf dem Laufenden über neue Sicherheits- und IT-Themen zu sein.

Dies erfordert:

- ✓ **Regelmäßige Compliance Audits und regulatorische Überprüfungen**
- ✓ **Schnelle OS Updates**
- ✓ **Proaktive Überwachung von Cyberbedrohungen**
- ✓ **Einhaltung der sich ändernden Compliance-Vorschriften**
- ✓ **Rasche Reaktion auf Personal- und Richtlinienänderungen, die sich darauf auswirken, wer Zugang zu welchen Daten hat**

Wenn das alles wirklich überwältigend klingt, dann liegt das daran, dass es das auch ist.

Geben Sie die Mac Compliance Checkliste und Jamf ein.

Anhand einer strukturierten Checkliste kann die IT ihre Prozesse zur Compliance optimieren und den sich ändernden Vorschriften immer einen Schritt voraus sein. Der beste Weg, um sicherzustellen, dass Sie nichts übersehen, ist eine gründliche Checkliste, die detaillierte, spezifische Schritte enthält, um sicherzustellen, dass Sie die richtigen Sicherheitskonfigurationen sowie Überwachungs- und Durchsetzungsmaßnahmen eingerichtet haben.

Und vergessen Sie nicht den Einsatz von erstklassigen Lösungen, die helfen, all diese Bereiche zu tracken, zu überwachen, durchzusetzen und zu aktualisieren.

Vorbereitungsphase

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

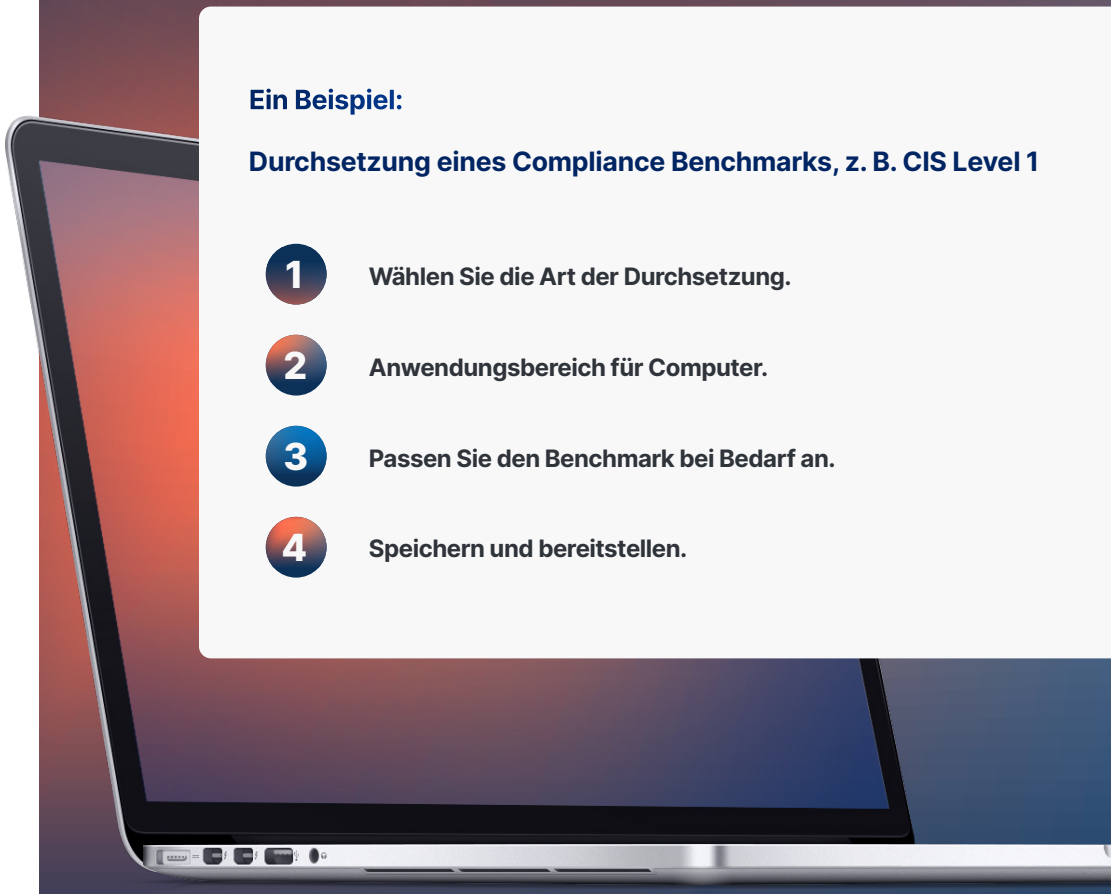
Was kann die Funktion „Compliance Benchmarks“?

Die in Jamf Pro integrierten Benchmarks für Compliance ermöglichen es der IT, Compliance zu definieren, zu auditieren und durchzusetzen.

Die Funktion:

- **verkürzt die Zeit, die ein IT Admin zum Auditieren und Durchsetzen eines Compliance Benchmarks in seiner Geräteflotte benötigt, von Wochen auf Minuten**
- **versteckt die Komplexität der Compliance-Standards, Regeln und Konfigurationskontrollen hinter einer einfachen und leicht verständlichen Benutzeroberfläche und einem Workflow**
- **erhöht den Sicherheitsstatus der Geräteflotte Ihrer Kunden**

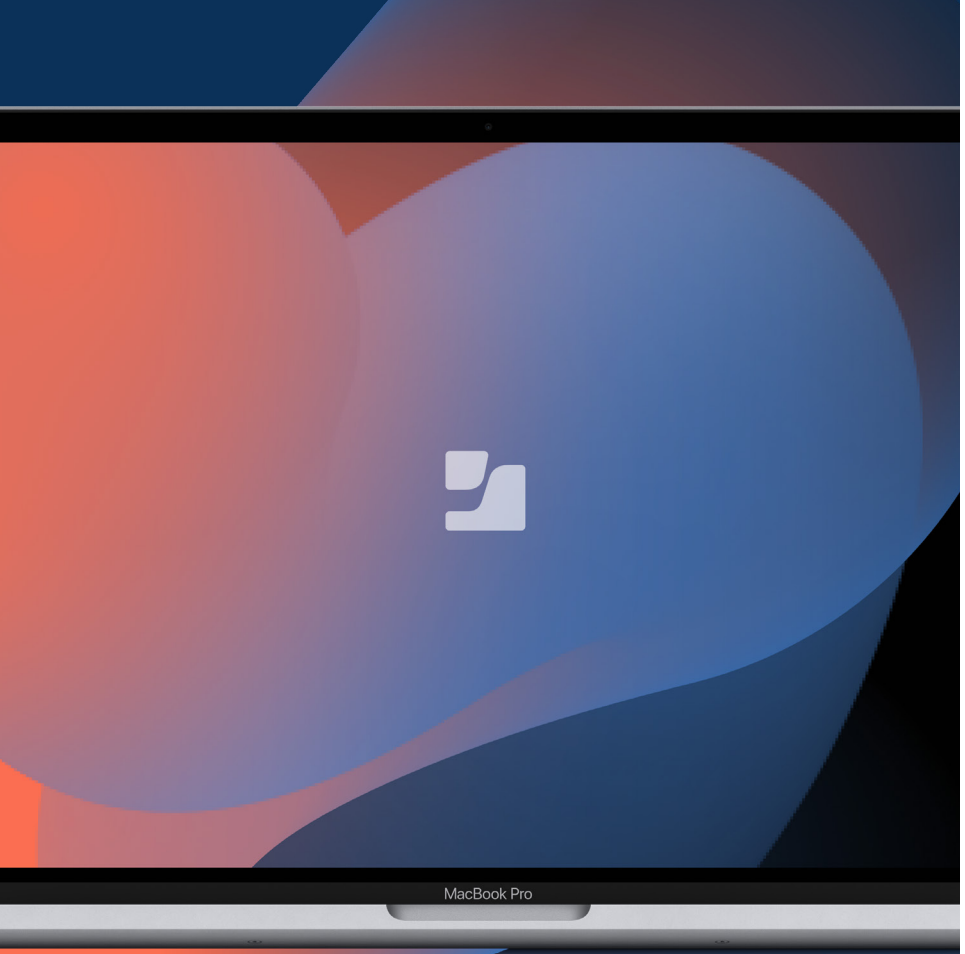
Compliance Benchmarks erstellen all dies automatisch und umfassen Profile, Richtlinien, Skripte, Erweiterungsattribute und vieles mehr. Sie erstellen Jamf Pro Konfigurationen, die die Gerätekonfigurationen ändern und aufrechterhalten, um die Compliance mit dem ausgewählten Benchmark zu gewährleisten.



Ein Beispiel:

Durchsetzung eines Compliance Benchmarks, z. B. CIS Level 1

1. **Wählen Sie die Art der Durchsetzung.**
2. **Anwendungsbereich für Computer.**
3. **Passen Sie den Benchmark bei Bedarf an.**
4. **Speichern und bereitstellen.**



Die Benchmarks für die Compliance wurden auf der Grundlage des macOS Sicherheits- und Compliance-Projekts (mSCP) erstellt. Es handelt sich um ein gemeinsames Bestreben von Bundesmitarbeiterinnen für IT-Sicherheit 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).

Kontinuierliche Wartung und Überwachung

Das Dashboard für Compliance Benchmarks zeigt alle erstellten Benchmarks und deren Status an. Detailliertere Ansichten zeigen die Compliance aller Geräte pro Compliance-Regel (z. B. Mindestlänge des Passworts) an, damit die Admins alles im Blick haben.

Sehen Sie sich eine Demo zu Compliance Benchmarks an:

Einrichtung und Konfiguration

Nutzen Sie die automatisierte Bereitstellung mit MDM und DDM, um sicherzustellen, dass jedes Gerät genau das hat, was die einzelnen Nutzer:innen brauchen, und dass die Apps und die Einstellungen für den Zugang proaktiv auf der Geräteebene aktualisiert werden.

- ✓ **Nutzen Sie die Compliance Benchmarks von Jamf, um Ihren Workflow zu vereinfachen und zu beschleunigen, indem Sie die von Jamf erstellten Anforderungen auf der Grundlage gängiger Benchmarks, wie CIS Level 1 oder 2, verwenden. Ihre Admins können jedoch auch benutzerdefinierte Benchmarks erstellen.**
- ✓ **Verwenden Sie eine der sechs Schnellstartvorlagen im Fenster der Jamf Blueprints oder erstellen Sie Ihre eigenen. Dies spart Zeit und erhöht die Sicherheit mit Richtlinien für Passwörter, Einstellungen für Service-Konfigurationsdateien und der Verwaltung von Hintergrundaufgaben.**
- ✓ **Sie können wichtige Apps und Updates mit einer Kombination aus Self Service+ (das bestimmten Nutzergruppen den Zugang und das Herunterladen von Apps und Ressourcen entsprechend ihrer Rolle ermöglicht) und Smart Groups installieren.**
- ✓ **Sie können die Sicherheitseinstellungen (FileVault, Gatekeeper, etc.) konfigurieren .**

Tests

- ✓ **Sie können die Funktionalität von Apps und Funktionen des Systems testen.**
- ✓ **Sie können Sicherheitsaudits durchführen; Jamf Protect speichert Auditprotokolle, die der IT bei dieser Aufgabe helfen können.**
- ✓ **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 Nutzer:innen klare Anweisungen.**
- ✓ **Planen Sie ein Onboarding-Meeting für Fragen und Fehlerbehebung.**
- ✓ **Stellen Sie sicher, dass alles richtig für die automatisierten Updates der Compliance-Einstellungen durch Jamf eingerichtet ist. Dadurch müssen Sie sich nicht mehr um die neuesten Entwicklungen für viele wichtige Compliance-Protokolle kümmern.**

Was ist Self Service+ ?

Self Service+ ist ein Portal für Nutzer:innen von macOS. Dadurch haben sie Zugang zu Inhalten und Updates, die in Jamf Pro vorkonfiguriert wurden. In Self Service+ können Nutzer: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. **Aufgaben der Identitätsverwaltung wie das Ändern von Passwörtern durchführen**

Best Practices und künftige Überlegungen

Mit dem richtigen Partner können Sie sicherstellen, dass Ihre Geräteflotte sicher konfiguriert ist und sowohl den gesetzlichen Anforderungen als auch den intern festgelegten Richtlinien entspricht: Jamf ist der richtige Partner.

Jamf stellt sicher, dass die Compliance der Geräteflotte mit minimalem Aufwand durch die IT-Admins erreicht wird. Sicherheitsteams können außerdem problemlos Compliance-Dokumente und -Status erstellen und Prüfern vorlegen.

Sie bleiben auf dem Laufenden über sich ändernde Gesetze, Vorschriften und Compliance-Standards, indem Sie die Ankündigungen der Regulierungsbehörden verfolgen. Obwohl Apple-Admins immer eine Vorstellung davon haben sollten, was in Sachen Compliance auf sie zukommt, aktualisiert Jamf Blueprints und Benchmarks für die Compliance, wenn sich diese Details ändern.

Wichtig ist, sich Folgendes vor Augen zu führen: Die Rolle der IT-Admins bei der zukunftssicheren Gestaltung von Compliance-Bemühungen ist absolut entscheidend. Um die Bedeutung dieses Themas besser zu verstehen, ist es ein guter Anfang, nach Informationen wie diesem E-Book zu suchen. Sie können auch diese Checkliste nutzen.

Vielleicht das Wichtigste von allem? Setzen Sie sich stets für schnellere und zuverlässigere Compliance-Strategien und -Taktiken ein. Dank Ihrer Arbeit ist Ihre Organisation zukunftssicher und für alle anstehenden Veränderungen gerüstet.