

Warum Jamf for Mac

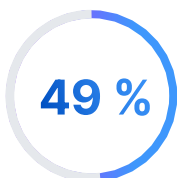
IT-Verantwortliche in Unternehmen haben die Aufgabe, Ausfallzeiten von Geräten zu begrenzen, die Produktivität und Zufriedenheit der Endbenutzer zu gewährleisten und gleichzeitig Risiken zu minimieren und Cyberbedrohungen abzuwehren.

Da sich immer mehr Mitarbeiter:innen für Macs entscheiden, wird von den IT-Teams erwartet, dass sie nahtlose Erlebnisse und Sicherheit auf Unternehmensniveau bieten - ohne Kompromisse und sie dürfen ihr Budget nicht überschreiten. Hier kommt Jamf ins Spiel.



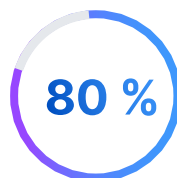
IT-Teams verbringen sehr viel Zeit mit Routineaufgaben.

In der modernen IT-Umgebung ist Schnelligkeit gefragt, aber veraltete Workflows, isolierte Tools und fehlende Daten in Echtzeit zwingen die Teams dazu, stundenlang an Lösungen zu basteln. Es ist nicht skalierbar.



der Organisationen geben an, dass sie nur begrenzten Zugang zu Informationen zum richtigen Zeitpunkt haben ⁽¹⁾

Ohne Einblick in die Geräte verschwenden IT-Teams Zeit damit, Daten mithilfe provisorischer Lösungen und manueller API-Aufrufe zusammenzufügen, nur um einfache Berichte zu erstellen. Das Fehlen von Daten in Echtzeit stellt ein noch größeres Risiko für die Sicherheit der Geräte dar.



der IT-Führungskräfte sagen, dass Probleme bei der Integration die Initiativen zur digitalen Transformation bremsen ⁽²⁾

Ohne eine klare Dokumentation, nativ eingebaute Integrationen oder ein Framework für nahtlose Integrationen verbringen IT-Teams unnötig viel Zeit damit, ihre Tools reibungslos miteinander zu verbinden.



der Macs wurde FileVault deaktiviert ⁽³⁾



der Macs wurde Firewall deaktiviert ⁽³⁾

IT-Teams verbringen zu viel Zeit damit, Geräte manuell zu sichern und zu reparieren, um die grundlegende Konformität einzuhalten. Andere Anbieter bieten Vorlagen für die Konformität an, die nicht vollständig sind oder nicht die Konformitätsgrundlagen des macOS Security Compliance Projects widerspiegeln. Dies bedeutet mehr Arbeit für IT-Teams.



Jedes Jahr erhöht sich das Risiko in allen Apple Umgebungen.

Die zunehmende Beliebtheit des Macs im Unternehmen ist ein zweischneidiges Schwert, denn auch Hacker sind nun der Meinung, dass es sich lohnt, Apple Geräte anzugreifen.

Der fehlende Schutz vor Apple-spezifischen Bedrohungen erhöht nur das Risiko. Telemetrie ohne Mac-spezifische Ereignisdaten (d. h. Gatekeeper und XProtect) bedeutet, dass Sie nur begrenzte Sichtbarkeit haben, bis Bedrohungsakteure andere Sicherheitskontrollen auslösen. Ohne spezielle Teams für die Suche nach Bedrohungen für Apple haben die meisten Sicherheitsanbieter Schwierigkeiten, Schritt zu halten.

Die durchschnittlichen Kosten für die Nichteinhaltung von Datenschutzbestimmungen belaufen sich auf 14,8 Millionen US-Dollar⁽²⁾.

Fehlende Protokollierung und Prüfprotokolle führen zu einer mangelhaften Auditbereitschaft, aber die Unterstützung von Integrationen mit SIEM-Anbietern bietet zusätzliche Transparenz für eine echte zentrale Sicherheitsübersicht.

39 % der Unternehmen verfügen über mindestens ein Gerät mit bekannten Schwachstellen.⁽³⁾ Begrenzte Transparenz hinsichtlich CVEs und fehlende automatisierte Workflows für Software-Patches setzen Sie dem Risiko durch angreifbare Software aus.



300

Jamf Threat Labs trackt über 300 Malware-Familien auf macOS⁽³⁾



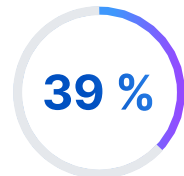
21

Jamf Threat Labs entdeckte allein im Jahr 2023 21 neue Malware-Familien (3)



14,8 Mio. USD

Die durchschnittlichen Kosten der Nichteinhaltung von Datenschutzbestimmungen



39 % der Unternehmen hatten mindestens ein Gerät mit bekannten Sicherheitslücken⁽³⁾



Warum also Jamf for Mac?

Jamf steigert die Produktivität um das Doppelte im Vergleich zu unseren Wettbewerbern⁽⁴⁾, indem es sich nahtlos in jede IT-Infrastruktur integriert. Dies reduziert den Zeitaufwand für die Datenerfassung, die Ausfallzeiten der Geräte, den First-Level-Support und manuelle Eingriffe.

Unsere Sicherheitslösungen reduzieren die Risiken zwei- bis dreimal stärker als die der Mitbewerber, indem sie Apple-spezifische Bedrohungen verringern, die Reaktionszeiten verkürzen, ungepatchte Schwachstellen reduzieren und die Konformitätsbereitschaft erhöhen.

Wir erreichen dies durch:

- Überwachung von Bedrohungen in Echtzeit über mehrere Vektoren mit speziellen Teams für die Suche nach Bedrohungen für Apple
- Umfassende Funktionen für Inventarisierung, Berichterstellung, Protokollierung und Prüfung

- Umfassende vorgefertigte IT- und InfoSec-Integrationen
- Ein robustes Framework für Richtlinien mit automatisierter Ausführung in Echtzeit und Self Service für Endbenutzer
- Automatisierte Beschaffung, Validierung, Neupaketierung und Bereitstellung von Apps

Unsere großen Support- und Service-Teams sind legendär. Außerdem bieten wir Jamf Nation an - das weltweit größte Forum für Apple Admins, in dem die Mitglieder ihr umfangreiches Fachwissen miteinander teilen.

„Der hervorragende technische Support, den ich von Julie [Technische Support-Ingenieurin] erhalte, ist ein wichtiger Beweis dafür, dass die Entscheidung für die Verwaltung von Jamf for Mac richtig war. Ich kann meinem Managementteam zeigen, dass Jamf eine zuverlässige Lösung ist.“

- IT-Analyst bei einer Regierungsbehörde



Jamf steigert die Produktivität mehr als andere Lösungen.

Jamf ist besser als die Konkurrenz aufgrund:

- weniger Ausfallzeiten des Geräts
- gesteigerter IT-Betriebseffizienz
- weniger Bedarf an direkter Unterstützung für Endbenutzer
- bessere Überwachung und Sichtbarkeit

schnellerer Einsatzbereitschaft

Der Zugang zu umfassenden Geräteinformationen in Echtzeit und automatisierte Workflows verringert den Bedarf an manueller Berichterstellung, Audits und Workflow-Management.

So geht's:

- **Automatisierte Workflows für das Onboarding**, die Konfigurationen auf der Grundlage von Rolle, Abteilung, Benutzer und Standort festlegen, ersparen der IT Zeit und sorgen dafür, dass neue Mitarbeiter sofort starten können.
- **Präzises Targeting** hilft bei der Automatisierung von Fehlerbehebung, Gerätehärtung und Software-Updates - und erspart den Benutzern und der IT viel Zeit.
- **Der First-Level-Support** geht bei der Fehlerbehebung über die grundlegenden Funktionen hinaus und ermöglicht den Benutzern ein Selbstbedienungsmodell für das Hinzufügen von Apps zur Produktivität.



Jamf reduziert mehr Risiken als andere.

Das robuste Richtlinien-Framework von Jamf umfasst Frameworks für die Geräteverwaltung, richtlinienbasierte Skriptausführung und Netzwerkkontrollen. Unser Expertenteam für die Suche nach Bedrohungen nutzt gut trainierte Verhaltensanalysen, um Apple-spezifische Angriffe zu stoppen.

Mit Jamf können IT-Verantwortliche:

- bekannte und neue Apple-spezifische Zero-Day-Bedrohungen blockieren
- schneller auf Sicherheitsrisiken reagieren – mit gezielter Abwehr in Echtzeit

- ungepatchte Schwachstellen mit CVE-Berichterstattung und automatisierten Software- und App-Updates reduzieren
- die Wahrscheinlichkeit von Datenverlusten durch eine sichere, speziell für Apple entwickelte Konnektivität mit dynamischer Risikobewertung anhand einer erhöhten Anzahl von Datenpunkten reduzieren
- die Absicherung von Geräten durch die Integration in das macOS Security Compliance Project automatisieren, wodurch das Risiko menschlicher Fehler eliminiert und die Auditbereitschaft durch detaillierte Protokollierung und Audit-Trails erhöht wird.

1. „Automation: Trends, Challenges and Best Practices“, IDC, 2023

2. "State of IT Report", dritte Ausgabe, Salesforce

3. „Jamf Security 360: Annual Trends Report 2024“, Jamf, 2024

4. „Driving ROI: The Case for a Proven Apple Enterprise Management Solution“, Jamf Whitepaper, 2021

**Jamf ist die richtige Wahl.
Überzeugen Sie sich selbst
von unseren Leistungen.**

G2-Bewertungen:

„Jamf Pro bleibt das *herausragende Mobile Device Management für Apple Macs.*“

„Jede Menge Unterstützung von den Anbietern. Jamf wird in der Regel explizit in der Dokumentation des Anbieters aufgeführt, da es *das beste Produkt für Apple MDM ist.*“



Probieren Sie Jamf aus