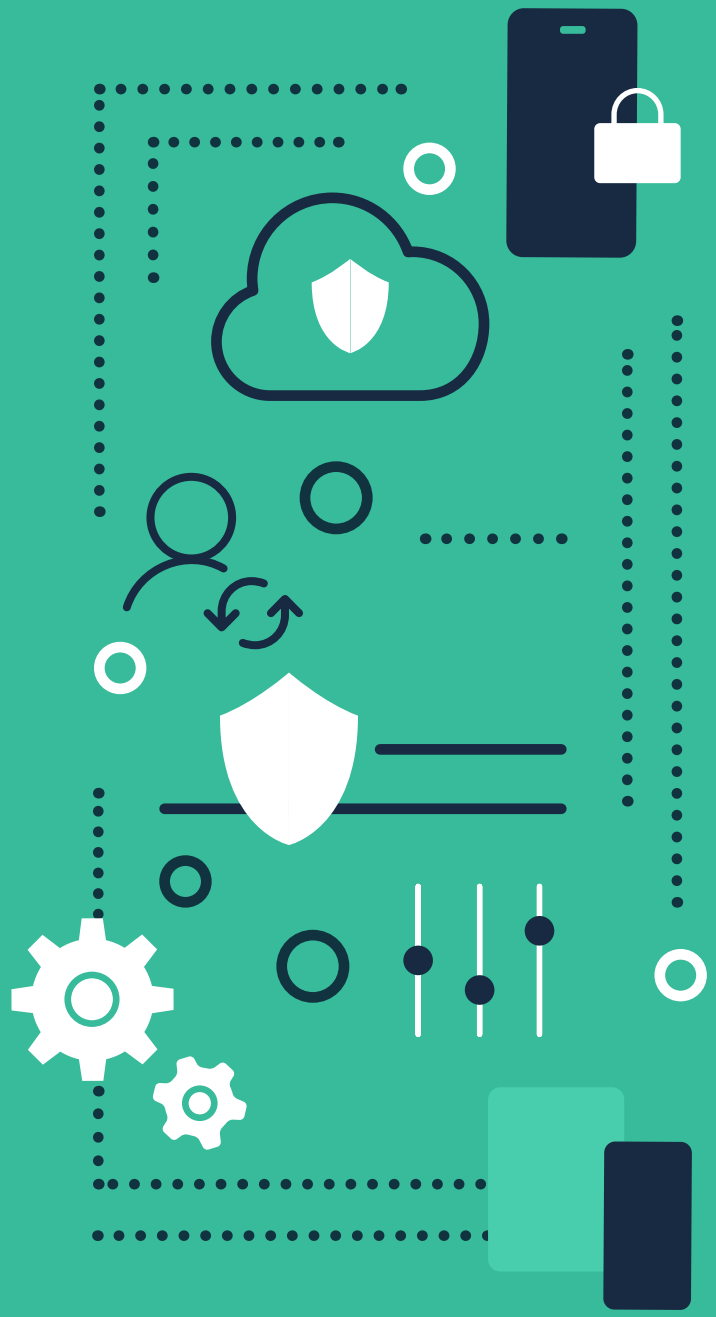


jamf

Mac Endgeräte-schutz

für Beginner

Native Sicherheit ist nicht das Ende (Punkt)

Es besteht kein Zweifel: Der Mac ist das sicherste Gerät auf dem Markt. Was seit Jahrzehnten gilt, hat auch heute noch Bestand. Wenn Unternehmen über die Zusammensetzung ihrer Flotte nachdenken, sind Sicherheitslösungen zum Schutz von Daten, Geräten und Benutzer*innen von entscheidender Bedeutung.

Nachlässigkeit kann zu nachteiligen oder kostspieligen Verstößen führen. Mit einer Endgerätesicherheitslösung für Mac können IT- und Sicherheitsteams nicht nur bekannte Bedrohungen abwehren, sondern sich auch an künftige Sicherheitsanforderungen Ihres Unternehmens anpassen und diese vorhersehen.

Egal, ob Sie ein Unternehmen mit einer Apple Fleet sind oder ein kleines Unternehmen, das eine Handvoll Mac Geräte verwaltet, Jamf erweitert den Endgeräteschutz über das hinaus, was Apple als native Funktionalität anbietet, um gemeinsam Ihre macOS Geräte, die Daten Ihres Unternehmens und Ihre Endbenutzer*innen zu schützen.

IN DIESEM LEITFADEN GEHEN WIR AUF FOLGENDE PUNKTE EIN:

- Mac Endgeräteschutz umfasst
- Warum der für mehrere Betriebssysteme konzipierte Endpunktschutz für Mac unzureichend ist

ENDGERÄTESICHERHEIT AUF MACS:

Den Apple eigenen Sicherheitsvorteil ausbauen und sich auf das Unbekannte vorbereiten

Mit der zunehmenden Verbreitung von Macs in Unternehmen, kleinen Betrieben, Schulen und Organisationen des Gesundheitswesens wird es immer wichtiger, sicherzustellen, dass Geräte und Daten für legitime Zwecke, korrekt und von autorisierten Benutzer*innen verwendet werden — hier kommt der Mac Endgeräteschutz ins Spiel.

Um dies zu erreichen, müssen viele Komponenten — Identitätsmanagement, Patching, Virenschutz (AV), Konfiguration, Endgeräteerkennung und -Reaktion — zusammenarbeiten, um die Anforderungen Ihres IT- und Sicherheitsteams zu unterstützen.

*Weitere Informationen über die Verwaltung von Unternehmensressourcen, Daten und Benutzer*innen finden Sie in unserem E-Book Identitätsverwaltung für Einsteiger.*

IDENTITY AND ACCESS MANAGEMENT (IAM)

Die durch das Identitätsmanagement implementierten Sicherheitsmaßnahmen betreffen sowohl die Endbenutzer*innen als auch die IT-Abteilung während des gesamten Lebenszyklus der Mitarbeiter*innen, unabhängig davon, ob sie vor Ort oder an einem anderen Ort arbeiten. Zero Trust Network Access (ZTNA)-Lösungen, virtuelle private Netzwerke (VPNs) und SaaS-Apps, die Mitarbeiter*innen mit Unternehmensressourcen verbinden, bieten Möglichkeiten, Ihren Endgeräteschutz

In einer zunehmend mobilen Belegschaft, in der die Mitarbeiter*innen von verschiedenen Standorten aus mit unterschiedlichen Geräten arbeiten, müssen Unternehmen in der Lage sein, diese Geräte und ihre Unternehmensdaten zu verwalten und zu sichern, ohne dass eine Bindung an ein lokales Active Directory erforderlich ist. Jamf Connect unterstützt Benutzer*innen von ihrem ersten bis zu ihrem letzten Arbeitstag.
Ein Nutzer/eine Nutzerin kann seinen Mac auspacken, einschalten und auf all seine Unternehmensapps zugreifen, nachdem er sich mit einem einzigen Satz von Anmeldeinformationen für die Cloudidentität angemeldet hat.
Mit Jamf Connect können Organisationen die Identität und den Zugriff mit minimalen Auswirkungen auf das Endbenutzererlebnis überwachen und sich auf die beständige Priorisierung von Gerät- und Datensicherheit verlassen.

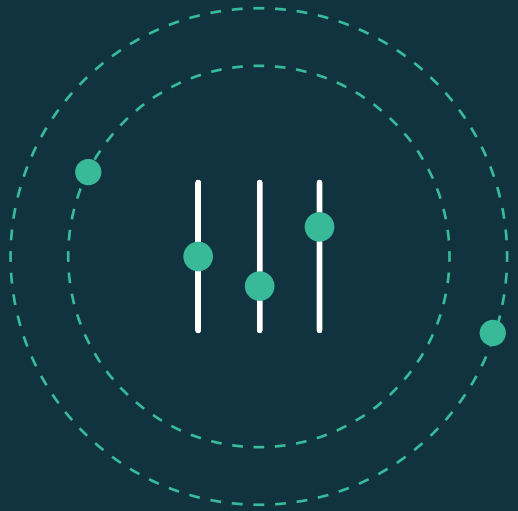
APP-VERWALTUNG

Die automatisierte Verwaltung von Apps vereinfacht die Arbeit und unterstützt effiziente, sichere Benutzer*innen.

Indem man sicherstellt, dass die Nutzer*innen die richtigen Apps über sichere Wege wie Jamf Self Service oder den Mac App Store erhalten:

- Apps können für die richtigen Benutzer*innen und Geräte bereitgestellt werden
- Benutzer*innen können benutzerdefinierte Titel und Apps abrufen, wenn sie sie benötigen
- Die IT-Abteilung kann iOS Aktualisierungen durchführen und Einstellungen vornehmen, die die Sicherheit der Organisation und der Benutzer*innen gewährleisten.

Integrieren Sie Jamf Pro in den Apple Business Manager, um Lizenzen für die Programme und Software Ihres Unternehmens zuzuweisen und zu verwalten. Außerdem kann Jamf Pro bei Patches und Software-Updates helfen. Auf diese Weise wird auch sichergestellt, dass Sie mögliche gefährdete Softwareversionen aktualisieren und verwalten können und den Status Ihrer gesamten Mac Fleet im Blick behalten. Sicherheits-Patches sollten häufig und einfach durchgeführt werden, um sicherzustellen, dass alle bekannten Schwachstellen der App entschärft werden. Mit Jamf können Sie den Aufwand für die Wartung oder Aktualisierung von Apps unter macOS optimieren und zusätzliche Transparenz für die Einhaltung von Richtlinien und die Kompatibilität schaffen, während Sie gleichzeitig eine hochwertige Endbenutzererfahrung bieten. Das bedeutet auch, dass Sie die neueste Version von macOS verwenden, sobald sie veröffentlicht wird, um Sicherheitslücken aufgrund von Verzögerungen bei der Aktualisierung zu vermeiden.



Sicherheits- und Verwaltungstools sollten kein Grund sein, Betriebssystem Updates oder Upgrades zu verschieben. Mit Jamf werden Sie nicht durch die Lösung aufgehalten, sondern erhalten ohne Verzögerung Unterstützung für neue macOS Versionen, sobald diese veröffentlicht werden. Sie bestimmen, wann Ihre Geräte aktualisiert werden.

ANTIVIRUS (AV)

AV scheint eine neue Notwendigkeit für Mac zu sein, aber es gibt eben auch eine neue Realität. Mac und macOS rücken immer mehr in den Mittelpunkt, da die Bedeutung von macOS im Unternehmen zunimmt.

AV ist eine Grundvoraussetzung für die meisten Unternehmensgeräte, um eine grundlegende Sicherheit zu gewährleisten. Apple bietet einen grundlegenden Virenschutz in macOS mit XProtect, Gatekeeper und MRT. Diese Tools werden jedoch nur sporadisch aktualisiert, und den Unternehmen fehlt der Überblick über ihre Aktionen. Jamf Protect bietet ausgefeilte AV-Funktionen, um Mac Malware zu verhindern und unter Quarantäne zu stellen, und geht weit über das hinaus, was Windows fokussierte Lösungen unter macOS bieten können.

Unternehmen sollten nicht warten, bis Probleme mit Malware, Adware oder anderer unerwünschter Software auftreten. Sie müssen AV implementieren, das Mac-spezifische Angriffe effektiv identifiziert und behebt, ohne wertvolle Ressourcen für die Suche nach Bedrohungen für Windows auf einem Mac auszugeben. Effektive, effiziente und umfassende Mac AV-Funktionen sind für die Sicherheit und die Benutzerfreundlichkeit von Geräten unerlässlich. Gleichzeitig führt jede AV-Lösung, die den Endbenutzer/die Endbenutzerin in seiner Produktivität behindert, nur zu Ärger für alle Beteiligten. Jamf Protect wurde entwickelt, um macOS vor Malware zu schützen, ohne die Erfahrung zu verändern, die Endbenutzer vom Mac erwarten.

Mac AV ist nicht mehr nur ein netter Bonus, sondern ein Muss. Allerdings benötigen Sie nicht einfach nur AV, sondern eine speziell für Mac entwickelte AV-Lösung – ohne die Einschränkungen einer AV-Lösung für die systemübergreifende Nutzung.

KONFIGURATION

Die Standard-Sicherheitsfunktionen für Mac sind großartig — sie sind die besten, die es gibt — aber angesichts der modernen und sich ständig weiterentwickelnden Bedrohungen in der Cybersicherheitslandschaft ist das nicht genug. Sie müssen Ihre Sicherheitsvorkehrungen bewerten und weiterentwickeln, um Ihre Geräte und Daten zu schützen. Und wenn es so einfach ist, Ihre Sicherheit zu erhöhen, warum tun Sie es dann nicht?

Es gibt einen umfangreichen Wissensschatz und Skripte, die in der Sicherheitsgemeinschaft bereits existieren, um dies zu tun.

Mit Jamf ist es einfach, diese zu implementieren und auszuführen und alle Benutzer*innen zu überwachen, die versuchen, diese Standards zu ändern. Jamf räumt die Hindernisse aus dem Weg, die Sie bisher vielleicht davon abgehalten haben, eine grundlegende Sicherheit für Ihre Geräte einzurichten.

FileVault, die Aktivierung von Firewall- und Kennwortanforderungen, die Einstellung von Bildschirmschoner- und Sperranforderungen - all das spielt eine Rolle bei der Festlegung Ihrer Sicherheitsanforderungen und Benchmarks.

Sie wissen nicht, wo Sie anfangen sollen? Das Center for Information Security liefert Branchen-Benchmarks, und Jamf ist CIS-zertifiziert. Mit Jamf sind Sie also bereits auf dem Weg, und wir haben Ressourcen, um Ihnen zu helfen.

Erfahren Sie mehr über CIS-Sicherheitsbenchmarks und Jamf mit unserer macOS Sicherheits Checkliste.

ERKENNUNG UND REAKTION SPEZIELL FÜR MAC

Herkömmliche EDR-Tools (Endpoint Detection and Response) gibt es für Mac schon seit geraumer Zeit, aber die meisten sind nicht darauf ausgelegt, Angriffe, die speziell auf Mac abzielen, effektiv zu erkennen. Vielmehr versuchen sie, Mac Geräten Windows Modelle aufzuzwingen. Da Jamf Protect sich ausschließlich auf Mac und macOS konzentriert, minimiert Jamf Falschmeldung und maximiert die Erkennungsraten auf Mac.

Wenn Sie Jamf Protect mit Jamf Pro kombinieren, erhalten Sie minimal-invasive Abhilfemaßnahmen, die weit über die durchschnittlichen EDR-Funktionen hinausgehen. Mit Jamf können IT- und Sicherheitsteams einen nahtlosen Vorfallsreaktionsplan erstellen, der Ihren Teams eine enge Zusammenarbeit ermöglicht.

JAMF STEHT FÜR ENDGERÄTESICHERHEIT.

Der Mac-Endpunktschutz mit Jamf Protect unterstützt die Einhaltung von Endpunktrichtlinien, erfüllt die Anforderungen an den Virenschutz, indem er macOS Malware verhindert, kontrolliert und sichert Mac Apps innerhalb des Unternehmens und erkennt und behebt Mac-spezifische Bedrohungen mit minimalen Auswirkungen auf die Benutzererfahrung.

In Verbindung mit Jamf Pro bietet Jamf umfangreiche Automatisierungs-, Untersuchungs- und Abhilfemöglichkeiten, um große und kleine Sicherheitsrisiken an Endpunkten zu minimieren.

Kostenlose Testversion anfordern

oder wenden Sie sich an Ihren bevorzugten Apple Partner, wenn Sie Ihre Sicherheit verstärken möchten.

Erfahren Sie mehr über die Endgeräteschutzfunktionen von Jamf.