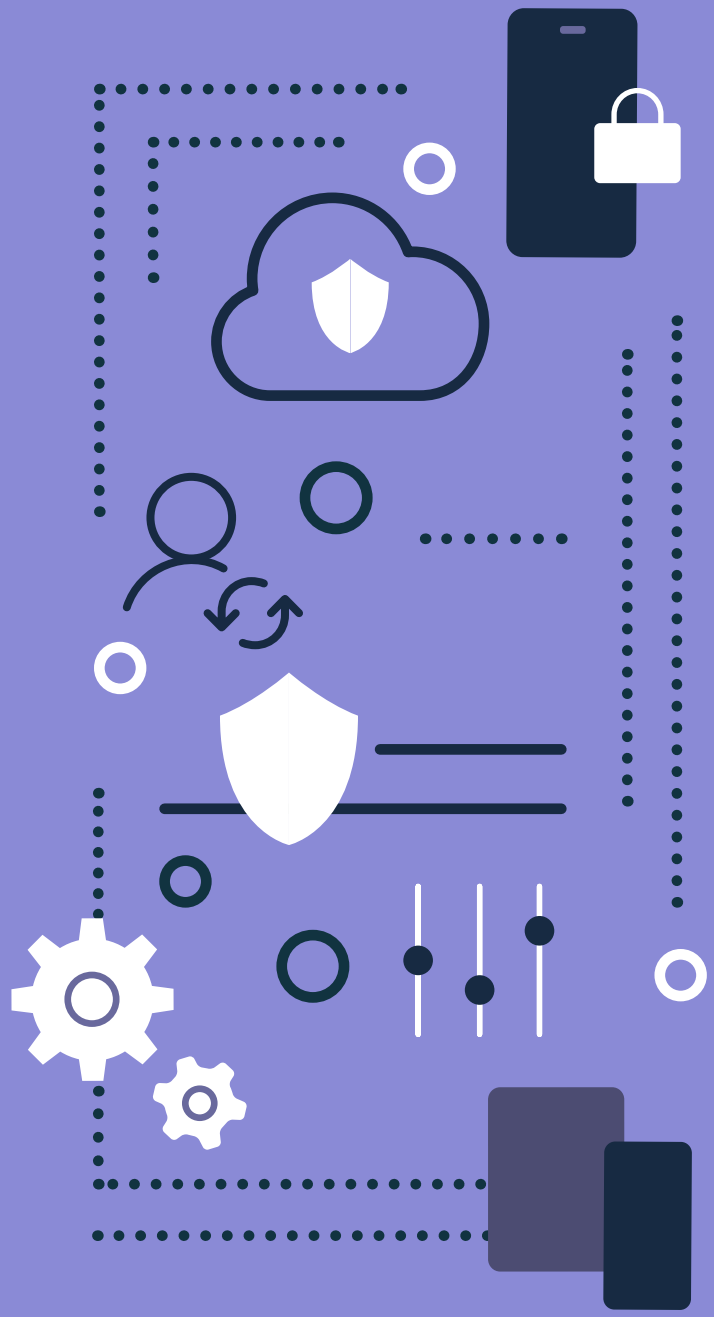


jamf

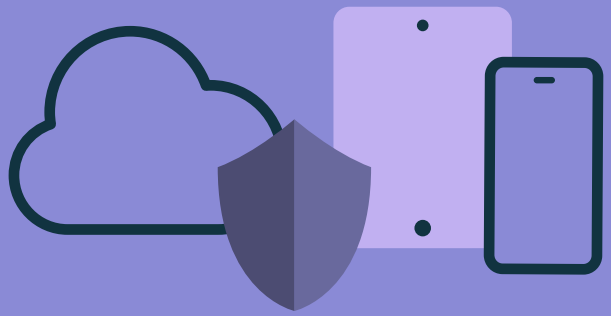
Unverzichtbarer Leitfaden für

Antivirus für Mac

MAC SPEZIFISCHE MALWARE IST UNERLÄSSLICH, DA UNTERNEHMEN IHRE APPLE FLEET WEITER AUSBAUEN.

Insgesamt betrachtet steht Apple gut da, obwohl Bedrohungen auf allen Computer-Plattformen im Anstieg sind. Apple hat sich besonders darauf konzentriert Malware-spezifische Erkennungen in dem nativen Apple Security Framework auszubauen.

Mit der Einführung von Remote- und Hybrid-Arbeitskräften in Unternehmen hat sich die Technologielandschaft drastisch verändert. Deshalb passen Malware-Autoren und Hacker sich an diese Änderungen an, indem sie den Bereich und die Größe der Malware-Tools in ihrem Arsenal ändern. Durch die gleichzeitige Nutzung mehrerer Bedrohungstypen erhöhen Angreifer die Komplexität, während eine zunehmende Automatisierung den Angriff auf weitere Ziele ermöglicht auf die Benutzer vertrauen.



IN DIESEM LEITFADEN BESPRECHEN WIR FOLGENDES:

- Definition von Mac-fokussierten Antivirus-Programmen (AV)
- Aufzeigen, wie Malware-Bedrohungen Mac Benutzer*innen zunehmend beeinträchtigen
- Erläutern Sie, warum das Verständnis dieser Trends so wichtig für die Sicherung privater Daten und...
- ...Teilen Sie, was Jamf bietet, damit Ihre Mac Geräte geschützt bleiben

MAC FOKUSSIERTE ANTIVIREN

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. Unternehmen benötigen ausgefeiltere AV-Funktionen, um Mac Malware zu verhindern und unter Quarantäne zu stellen, und das geht weit über das hinaus, was Windows fokussierte Lösungen unter macOS bieten können.
Und sie sollten nicht warten, bis Malware, Adware oder andere unerwünschte Softwareprobleme 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 sowohl für die Sicherheit als auch für die Benutzerfreundlichkeit der Geräte unerlässlich.

Beispiele wie die Weitergabe von GPS-Koordinaten, die entschlüsselte Protokollierung von Nachrichten und die Überwachung/Aufzeichnung von Telefongesprächen sind laut einem Bericht von Kaspersky Labs nur einige der vielen Datenschutzprobleme, die verletzt werden.

EINE SICH ÄNDERNDE BEDROHUNGSLANDSCHAFT

Die Zahl der Phishing-Kampagnen, die aktuelle Krisen ausnutzen und sich die Ängste und Sorgen der Menschen zunutze machen, hat deutlich zugenommen, insbesondere wenn es um Waren geht, die nur begrenzt verfügbar oder von weltweiten Engpässen betroffen sind, wie z. B. Betrug im Bereich des technischen Supports.

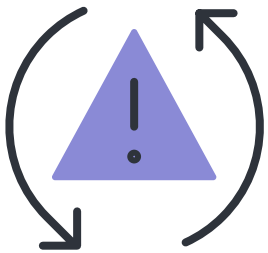
AUSSPIONIEREN ONLINE

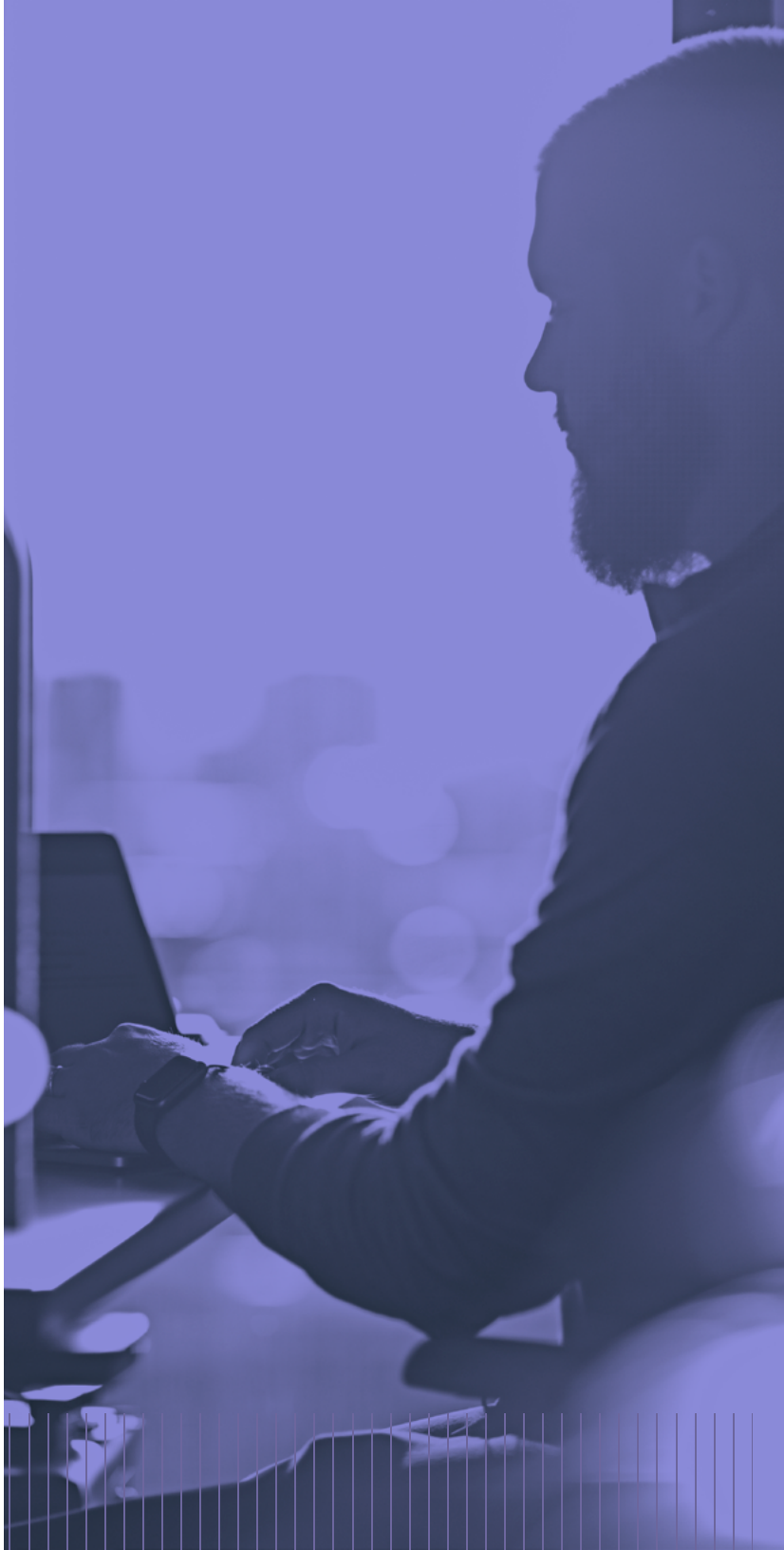
Adware, Spyware und Stalkerware sind allesamt Arten von Malware, die dazu dienen, Daten über Computerbenutzer*innen zu erlangen und auszuspionieren. Stalkerware wird auch als Online-Spionage bezeichnet, das es in Echtzeit alle Arten von personenbezogenen Daten ausnutzt.

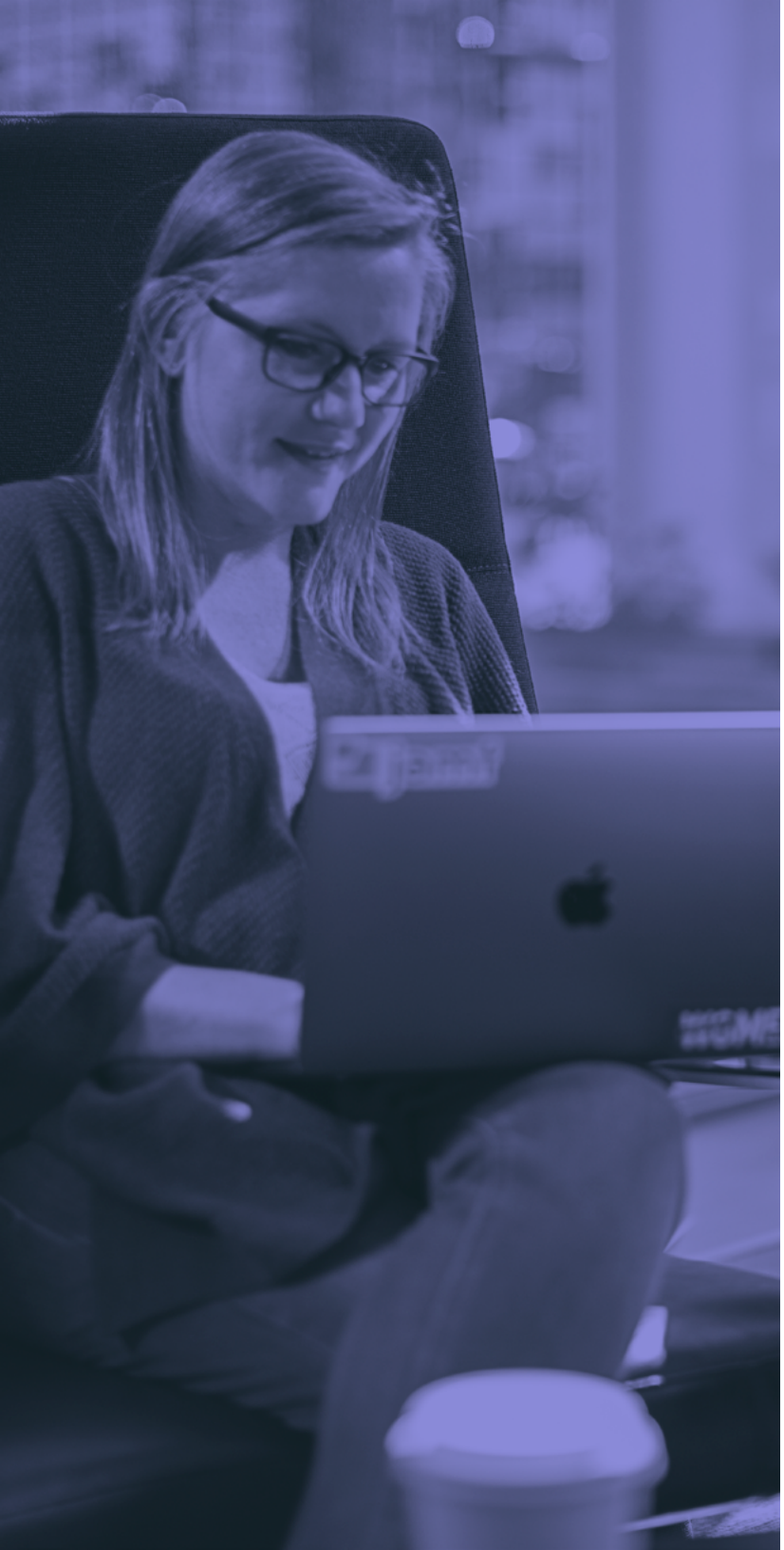
ES IST SCHACH, NICHT DAME

Bei der Auswertung dieser Informationen ist zu beachten, dass Bedrohungsakteure oft auf lange Sicht agieren, d. h., dass Angriffskampagnen so lange dauern können, wie sie für den Erfolg erforderlich sind. Sie sind nicht darauf begrenzt, ein Stück Malware in ein Gerät einzuschleusen, sondern versuchen oft, mehrmals Zugriff zu erhalten und existierende Schwachstellen zu nutzen. So haben sie Zeit, ihre Angriffsstrategie oder -tools zu ändern, so viele Informationen zu sammeln, wie sie möchten, und schließlich der Malware die Möglichkeit zu geben, sich tiefer in die betroffenen Systeme einzunisten.

Das ist zyklisch, und jede Facette hat direkt Auswirkungen auf die nächste und verstärkt sie.







ZUSTAND DER ANTIVIRUS-SOFTWARE FÜR DEN MAC

Das Wachstum von Malware setzt seinen allgemeinen Aufwärtstrend fort: AV-Test.org hat im Jahr 2022 insgesamt 1.227.048.144 Malware identifiziert - einschließlich potenziell unerwünschter Apps (PUA). Der Silberstreif am Horizont für Mac Nutzer*innen? Die Verteilung nach Betriebssystem ergab, dass nur 220 der gesamten Malware auf macOS abzielten!

Mehrere Faktoren beeinflussen diese deutliche Veränderung, darunter Folgendes:

- Das anhaltende Marktwachstum von Apple in der Geschäftswelt
- Verbraucher, die Apple Produkte im Rahmen von Programmen zur Mitarbeiterauswahl wählen (oder einfach ihre eigenen mitbringen)
- Verbraucher*innen, die Apple Produkte im Rahmen von Programmen zur Mitarbeiterauswahl wählen (oder einfach ihre eigenen mitbringen)

PACKEN SIE DIE PARTYHÜTE NOCH NICHT AUS!

Während Privatanwender diesen Rückgang als Grund zum Feiern sehen, zeigen Telemetriedaten, die von verschiedenen Quellen gesammelt wurden, dass Geräte, die im privaten Bereich genutzt werden, immer noch von potenziell unerwünschten Programmen (PUPs) befallen werden, wobei Adware an der Spitze steht.

Für Privatanwender von Mac-Produkten stellen PUPs und Adware jedoch einen Versuch dar, auf die persönlichen Daten des Anwenders abzuzielen - oder eine Vorbereitung auf etwas viel Schlimmeres, wenn bösartige Werbung geschaltet wird, private Daten verfolgt werden oder eine zweifelhafte App heruntergeladen wird, die behauptet, den Mac zu reinigen.

KOMBINERBARE MALWARE

Während die letzte bekannte neue Ransomware, die auf Macs abzielte, vor mehreren Jahren entdeckt wurde, brachte 2020 EvilQuest an die Spitze (auch als ThiefQuest bezeichnet). Diese Malware weist alle Merkmale von Ransomware auf, mit Ausnahme der Verschlüsselungswarnungen und der Aufforderung zur Zahlung für die Entschlüsselung von Dateien, die lediglich als Vorwand dienen, um ihre wahre Absicht zu verschleiern: den anhaltenden und gezielten Diebstahl von persönlichen und geschäftlichen Daten.

Malware wie diese kann sich im Laufe der Zeit weiterentwickeln — genau wie normale Software — und zusätzliche Funktionen enthalten, die mehr Schaden anrichten und gleichzeitig die Tarnkappe vergrößern, um der Entdeckung zu entgehen. Sie kann sich sogar aktualisieren, um sich weiterzuentwickeln, nachdem sie ein Gerät infiziert hat. EvilQuest weist alle Merkmale einer fortlaufenden Geschichte auf, die man im Auge behalten sollte, da sie sich in Zukunft verändern wird.

SELBST ALTE HUNDE KÖNNEN NOCH NEUE TRICKS LERNEN

Diese momentan nur lästige Malware, die an Adware erinnert, entwickelt sich ebenfalls. Angesichts der neueren macOS Versionen von Apple, bei denen die Signierung von Apps überprüft wird, bevor diese gestartet werden können, haben sich einige Malware-Autoren viel Mühe gegeben, um auf die wertvollen Daten auf Ihrem System zuzugreifen und die Werbung, die Sie beim Surfen im Internet sehen, zu Geld zu machen.

Beispiele für diese Angriffsarten sind: Duplizieren der Safari-App selbst, Ändern der App und Installieren nicht autorisierter Erweiterungen, um Benutzer zu verfolgen; Verwenden von Konfigurationsprofilen — der gleichen Art, die von IT-Administrator*innen zur Verwaltung von Geräteeinstellungen verwendet werden, um Benutzer dazu zu verleiten, diese auf ihren Geräten zu installieren; und effektives Gewähren von Zugriffsmöglichkeiten für Bedrohungsakteure, die sie für weitere Angriffe benötigen.

Es sollte auch beachtet werden, dass Adware zwar als weniger gefährlich angesehen wird, aber die Kombination aus der Tatsache, dass sie die häufigste Malware-Bedrohung unter macOS ist und gleichzeitig die fortschrittlichsten Formen der Innovation bei der Infektion von Systemen aufweist — ganz zu schweigen von der immer häufigeren Möglichkeit, neue Malware-Nutzlasten aus der Ferne hinzuzufügen - kann ihre Auswirkungen verstärken.

ARBEITEN SIE INTELLIGENTER, STATT MEHR

Leider gibt es keine Universallösung für die derzeitige Eskalierung von Bedrohungen Eine der wichtigsten Erkenntnisse ist, dass Bedrohungen nicht alle aus derselben Richtung kommen. Bedrohungsakteure variieren zunehmend ihre Taktiken und zielen auf Geräte und Dienste ab, die den größten Erfolg versprechen. Zudem zeigen die Daten, dass die Angriffe keinesfalls aufhören.

Was bedeutet das für alle, die sich privat und bei der Arbeit auf Computer verlassen? Vereinfacht ausgedrückt muss die Sicherheit so eingerichtet sein, dass sie alle Bedrohungen, die auf sie zukommen, abwehren, verhindern oder beseitigen kann. Wachsamkeit ist ein wichtiger Teil der Sicherheitsgleichung, sei es durch die Schulung der Benutzer*innen, wie sie gängige Bedrohungen wie Phishing-Versuche erkennen können, oder durch die Nichtinstallation unbekannter Software.

IT- und Sicherheitsteams müssen außerdem wachsame Praktiken in ihre Arbeitsabläufe integrieren, um die Sicherheitslage des Unternehmens zu stärken und jederzeit aufrechtzuerhalten. Der Einsatz von Erkennungssoftware, die Bedrohungen auf der Grundlage bekannter Signaturen oder Heuristiken aufspürt und Verhaltensanalysen durchführt, um unbekannte Bedrohungen zu erkennen, bevor sie auftreten, liefert die notwendigen Erkenntnisse, um nicht nur zu verstehen, woher die Bedrohungen kommen, die auf das Unternehmen abzielen, sondern auch, wie man sich vor ihnen schützen kann.

Schnelle Reaktion und Automatisierung gehen Hand in Hand, um schnell auf erkannte Bedrohungen zu reagieren und gleichzeitig alle gefundenen Probleme zu beheben. Beides trägt dazu bei, die Angriffsfläche zu minimieren und das Risiko effizienter zu verwalten, während es gleichzeitig eine weitere Ebene zur Defense-in-Depth-Strategie hinzufügt.

Schließlich benutzen wir Macs, um etwas zu erledigen – nicht, um durch Tausende Zeilen von Code nach Fehlern zu suchen, bevor wir eine App starten. In diesen Momenten erinnern wir uns daran, dass Apple bestrebt ist, seine Benutzererfahrung außergewöhnlich einfach zu gestalten, damit Apple Benutzer*innen etwas Außergewöhnliches schaffen können. Warum sollte Sicherheitssoftware nicht auch diesen Richtlinien folgen?

JAMF INTEGRATION + SUPPORT

Jamf Protect verhindert Malware und behebt schädliches Verhalten durch signaturbasierte Erkennung und Verhaltensanalysen auf dem Mac Mit einem granularen Top-Down-Einblick in die Geräte können die IT- und Sicherheitsabteilungen von Unternehmen erkennen, was die Geräteleistung unter dem Aspekt der Sicherheit beeinträchtigt. Zudem werden in Kombination mit Jamf Pro die zentralisierte Patch-Verwaltung und Behebung ermöglicht, um eine Lösung für fast alle auftretenden Probleme zu ermöglichen. Jamf Connect schließlich vervollständigt dieses hochsichere Dreiergespann. Die Lösung von Jamf Connect für die Identitäts- und Zugriffsverwaltung nutzt Cloud-basierte Identitätsdienste für den sicheren Zugriff auf Geräte und Ressourcen.

Eine gestaffelte Abwehr, die die integrierten Tools von Apple umfasst und durch die kombinierte Leistung von Jamf erweitert, hilft Ihnen dabei, eine effektive Mac Sicherheit zu gewährleisten, die sich nahtlos in die Endbenutzererfahrung integriert, während sie dennoch alle relevanten Einblicke und Analysen über Geräte bietet. Diese mehrschichtige Strategie ermöglicht es der IT-Abteilung, die beste Entscheidung zu treffen, wenn es um den Schutz ihrer Geräte und die Sicherung der Benutzerdaten geht.

Jamf — der Standard im Apple Enterprise Management— hat die Produkte und Lösungen, die Ihnen helfen, die beste Sicherheitsstrategie für Ihr Unternehmen und Ihre Benutzer*innen umzusetzen.

Wir nennen es Trusted Access. **Erfahren Sie mehr darüber.**

VERLASSEN SIE SICH NICHT NUR AUF UNSER WORT,

sondern stellen Sie AV- und Endpunktschutz auf die Probe.

Wenn Sie bereit sind, Ihre Mac Flotte vor eskalierenden Sicherheitsbedrohungen und bekannter Malware in freier Wildbahn zu schützen und bösartiges Verhalten zu beheben, testen Sie uns kostenlos oder wenden Sie sich an Ihren bevorzugten Fachhändler.

Kostenlose Testversion anfordern

oder wenden Sie sich an Ihren bevorzugten Reseller, wenn Sie bereit sind, Ihre Sicherheit zu verbessern.

Weitere Informationen über Jamf Protect und Mac Endgeräteschutz finden Sie auf jamf.com/de