SICHERHEIT IM GESUNDHEITSWESEN FÜR EINSTEIGER

Das Gesundheitswesen ist wie viele andere Organisationen auf der ganzen Welt auf Technologie angewiesen, um ihre Geschäftspraktiken zu verbessern. Die Fortschritte bestimmen – zumindest teilweise – die Art und Weise, wie die Kontinuität des Unternehmens fortgesetzt wird, und verändern oft die Art und Weise, wie Dinge erledigt, gespeichert und verwaltet werden – oder alle drei!

Es ist kein Geheimnis, dass, während die Welt insgesamt von COVID-19 und seinen Varianten erschüttert wurde, das Gesundheitswesen weiterhin unter seinen Auswirkungen zu leiden hat, sowohl direkt durch die Anzahl der Patienten, die eine Behandlung benötigen, als auch indirekt durch verschiedene verwandte, aber äußere Einflüsse, wie zum Beispiel:

- Laufende Verwaltung von Patientendaten und -aufzeichnungen, Nutzern und Endpunkten unter Einhaltung der gesetzlichen Vorschriften
- Umsetzung von Änderungen im Kerngeschäft, wie z. B. die Einführung von Telemedizin, unter Berücksichtigung der Sicherheit von Patienten und Pflegepersonal
- Aufrechterhaltung der Datensicherheit in allen Geschäftsmodellen und Schutz vor Bedrohungen und Angriffen durch böswillige Akteure, die immer mehr zunehmen

"DREI IST DIE MAGISCHE ZAHL"

Moderne Sicherheitspraktiken setzen sich aus vielen einzelnen Komponenten zusammen. Dieses E-Book ist kein Leitfaden für jede einzelne Hardware und Software, die es auf dem Markt gibt, sondern es geht vielmehr darum, die besonderen Anforderungen der Branche im Gesundheitswesen zu verstehen und die Werkzeuge und Verfahren zu ermitteln, die diesen Anforderungen am besten gerecht werden.

Beginnen wir mit einem Überblick über die Sicherheit im Gesundheitswesen, indem wir uns ansehen, in welche Bereiche die Komponenten, Tools und Best Practices fallen:

HARDWARE	SOFTWARE	KONFORMITÄT

Die Lösung für die Sicherheitsbedürfnisse im Gesundheitswesen ist nicht so einfach wie die Auswahl einer Lösung aus jeder Kategorie. Wenn es so einfach wäre, gäbe es keine Sicherheitsprobleme im Allgemeinen. Diese Kategorien zeigen, wie Lösungen für bestimmte Probleme aussehen können, einige besser als andere.

Jamf Protect zum Beispiel überwacht, erkennt, verhindert, behebt und berichtet über Malware-Vorfälle auf Ihrem Mac. Malware zielt größtenteils auf Software ab und erfordert eine softwarebasierte Lösung zum Schutz, sodass die Endgerätesicherheit in den Bereich Software fällt.

Hardware

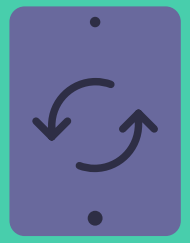
Bedrohungen und Angriffe, die direkt auf Ihre Apple-Geräte abzielen, fallen unter die Kategorie Hardware. Sicherheitspraktiken, die darauf abzielen, Schwachstellen zu schließen, die andernfalls physischen Zugriff auf Geräte ermöglichen würden — wie die Verschlüsselung der gesamten Festplatte zum Schutz von Daten im Ruhezustand, die Aktivierung von Startpasswörtern, um unbefugten Zugriff auf das Startmenü von macOS zu verhindern, oder die Entsperrung Ihres iOS-Geräts — fallen ebenfalls in diese Kategorie.

Software

Wenn Sie überlegen, was in den Bereich Software fällt, sollten Sie Bedrohungen und Angriffe in Betracht ziehen, die in erster Linie auf das Betriebssystem selbst abzielen und/oder dort operieren.

Beispiele für Kategorien:

- Endgeräteschutz
- Erfordert VPN (virtuelles privates Netzwerk) oder ZTNA (Zero-Touch-Netzwerkzugang)
- Apps Lifecycleund Patch-Management



Konformität

Die Konformität ist wohl die wichtigste Kategorie in dieser Dreifaltigkeit und auch diejenige, die bei allen Stakeholdern die größten Bedenken hervorruft. Konformität macht keinen Unterschied zwischen Hardware- oder Software-Lösungen. Die Stakeholder der Compliance-Kategorie befassen sich hauptsächlich mit der Prüfung, Erreichung und Aufrechterhaltung der Einhaltung von **Vorschriften, die das Gesundheitswesen regeln**, wie dem **Health Insurance Portability and Accountability Act von 1996 (HIPAA)** und dem **Health Information Technology for Economic and Clinical Health (HITECH) Act von 2009**.

Es gibt unzählige Möglichkeiten, das **Konformitäts-Management** zu unterstützen, aber es gibt gute Ansatzpunkte für jedes Team:

- Lösungen für das Sicherheitsinformations- und Ereignismanagement (SIEM), die Protokolle zentral verwalten
- Sicherheitsüberwachungs-Tools, die den Zustand des Geräts aktiv überwachen und es mit gängigen Sicherheitsrahmen vergleichen

Tipp für bewährte Praktiken:

Unternehmen sollten Sicherheitsmanagement-Frameworks wie die **SP 800-53-Reihe des National Institute of Standards and Technology (NIST)** und/oder die **Benchmarks des Center for Internet Security (CIS)** verwenden, um sicherzustellen, dass die Endpunkte gehärtet sind und die Unternehmen die Best Practices der Branche befolgen.

"UNSER WAHRER FEIND MUSS SICH ERST NOCH OFFENBAREN."

- Michael Corleone

Ähnlich wie die von Al Pacino in Der Pate, Teil III dargestellte Figur, die es mit einer Vielzahl von bekannten und unbekannten Feinden zu tun hatte, kämpft auch die Informationssicherheit gegen eine scheinbar nicht enden wollende Horde bösartiger Akteure.

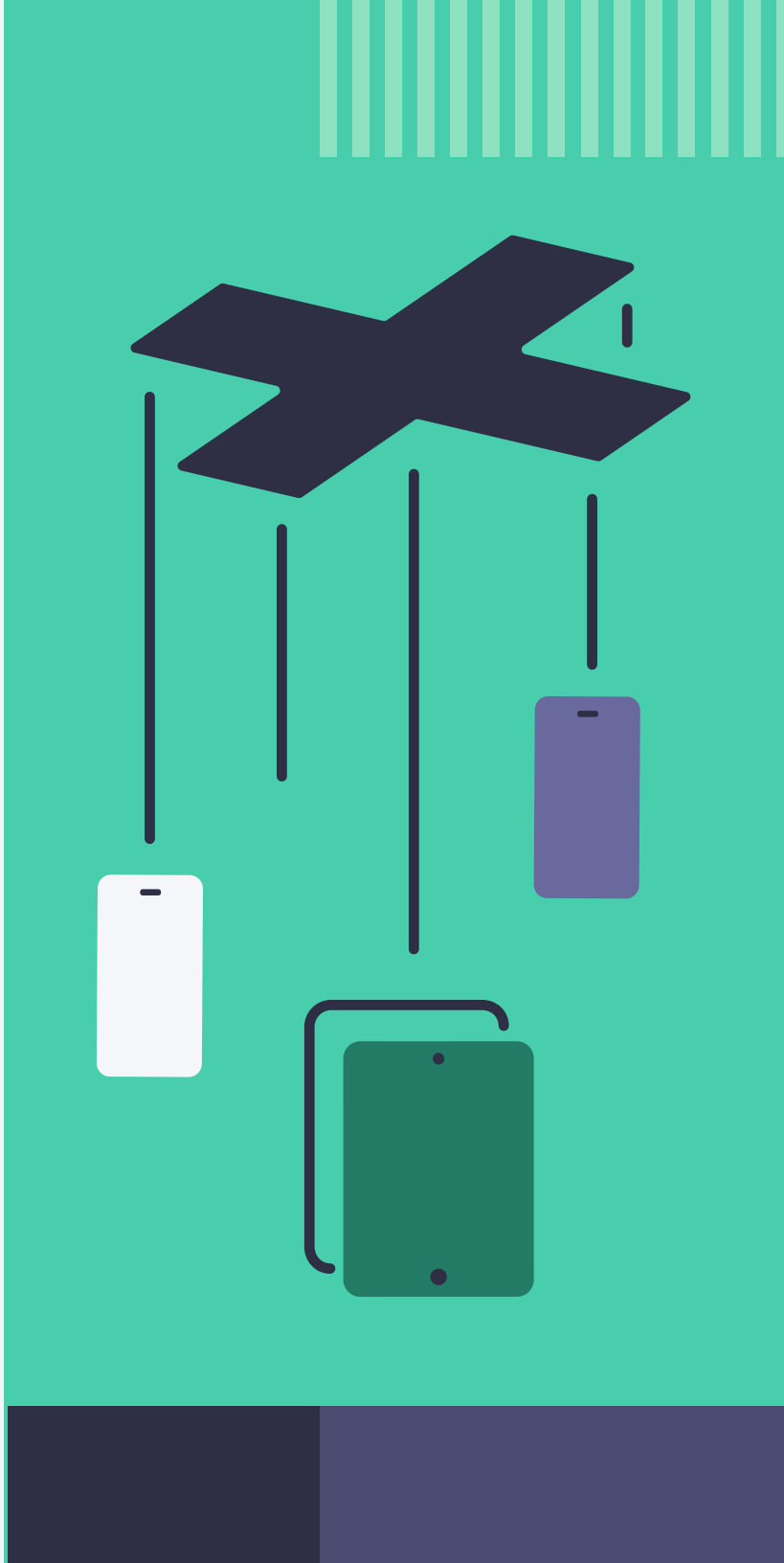
Während die Angreifer selbst "gesichtslos" sein mögen, sind die Bedrohungen, die sie für Angriffe und Kompromittierungen von Endgeräten einsetzen, bekannt. Mit diesen Informationen können Administrator*innen im Gesundheitswesen ihre Geräte am besten schützen:

- Einstellungen für das **Härten von** Geräten
- **Verwaltung** der Geräte
- **Implementierung** des Endpunktschutzes
- **Pflege** der Geräte mit aktuellen Patches
- **Überwachung** der Geräte in Echtzeit
- **Triagierung** erkannter Probleme
- **Behebung** von Risiken

UND

- **Aufrechterhaltung** der Geräte-Konformität...

...um alle Beteiligten vor Gerätekompromittierung, Datenverlust/-diebstahl, Sicherheitsverletzungen und Ereignissen zu schützen, die andernfalls die Leistung, die Erfahrung der Endbenutzer und das Niveau der Patientenversorgung beeinträchtigen würden.



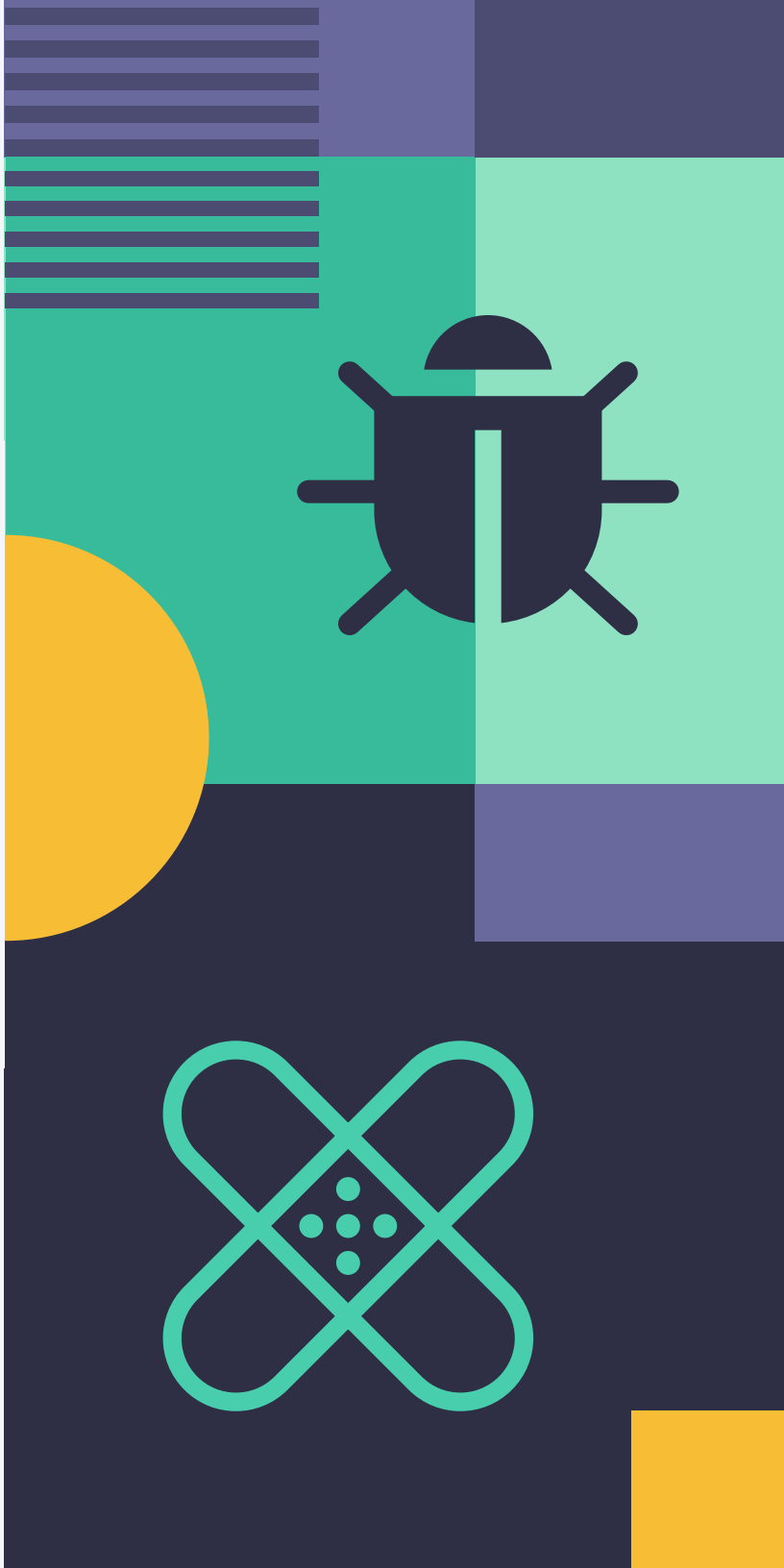
Die folgende Liste der potenziellen Bedrohungen enthält Bedenken, die speziell für Anbieter*innen im Gesundheitswesen gelten:

- Angriffe auf der Grundlage von Malware — wie Ransomware und Denial of Service (DoS) — können Systeme lahmlegen und Anbieter daran hindern, Geräte zur Verwaltung von lebenswichtiger Hilfe zu nutzen.

- Geräte, die nicht auf dem neuesten Stand sind, was Patches und System-/App-Updates angeht, lassen Organisationen bekannte Schwachstellen für spätere Angriffe offen, die zu Datenschutzverletzungen, Datenlecks und/oder Diebstahl von personenbezogenen Daten (PII) oder datenschutzrechtlich geschützten Datensätzen führen können.

- Die Anbieter sind darauf angewiesen, dass die von ihnen verwendete Technologie ein Mindestmaß an Benutzerfreundlichkeit aufweist. Zeit- und Minutenverluste auf Geräten, die nicht richtig funktionieren — sei es aufgrund fehlender Funktionalität oder nicht aktualisierter Apps — haben reale Konsequenzen. Ein Gerät, das für einen Mitarbeiter innen der Personalabteilung konfiguriert ist, wird für einen Arzt auf seiner Visite wenig bis gar nicht von Nutzen sein und umgekehrt.

- Staatliche Vorschriften geben Hinweise darauf, wie Daten- und Gesundheitsdaten erhoben, gespeichert, verwaltet, weitergegeben und entsorgt werden sollten. Jedes Daten-Leck kann die Aufsichtsbehörden auf den Plan rufen und zivil- und/oder strafrechtliche Sanktionen nach sich ziehen, ganz zu schweigen vom möglichen Verlust von Patienten oder der Schließung einer Einrichtung aufgrund eines beschädigten Rufs.



"DER GRÖSSTE SIEG IST DER, DER KEINEN KAMPF ERFORDERT." — Sun Tzu

Die Themen, die mit der Sicherheit im Gesundheitswesen und deren effektiver Verwaltung zusammenhängen, sind vielfältig. Sie sind nicht auf eine bestimmte Art der Bereitstellung beschränkt. Schädliche Akteure setzen mehrere Methoden ein, um die Verteidigungsmaßnahmen einer Organisation zu umgehen und ihr Ziel zu kompromittieren.

Die gute Nachricht? Auch die Sicherheit im Gesundheitswesen sollte nicht isoliert bereitgestellt werden. In der Tat ist die Strategie der "Verteidigung in der Tiefe" der beste Ansatz, um die Vielzahl der Bedrohungen abzuschwächen. Indem sie mehrere defensive Schutzmaßnahmen in einer konzertierten Aktion zur Vereitelung von Angriffen aufeinander abstimmen, können Organisationen Sicherheitsmängel erkennen und Workflows zur Behebung bereitstellen, um diese zu beheben und das Risiko zu minimieren.

Endgeräteschutz

Der Schutz vor Malware wird von vielen als das wichtigste Element in jedem Sicherheitskonzept zum Schutz von Geräten, Benutzer innen und Daten angesehen. Und obwohl diese Überlegung angesichts der Fähigkeiten von **Endgerätesicherheitssoftware** wie **Jamf Protect**, bekannte und neue Bedrohungen für Ihre gesamte Flotte von macOS-Geräten abzuwehren, nicht ganz unbegründet ist, ist dies in Wirklichkeit nur eine Variable in der Gesamtsicherheitslage Ihrer Organisation.

Der Schutz von Geräten vor Malware-Bedrohungen spielt eine wichtige Rolle bei der Reduzierung von Risiken, der Sicherung von Daten und der Minimierung von Ausfallzeiten für Ihre Endnutzer. Es gibt viele Software-Optionen zum Schutz von Endgeräten, aber es gibt bestimmte Funktionen, auf die Gesundheitsdienstleister*innen unbedingt achten sollten:

- Aktive Überwachung auf Bedrohungen in Echtzeit
- Signatur- und analytikbasierte Erkennung von bekannten und potenziellen Bedrohungen
- Vorbeugung gegen bekannte Malware zur Beseitigung von Bedrohungen
- Behebung festgestellter Bedrohungen und Malware
- Warnmeldungen, die den Endbenutzer über erkannte/behobene Bedrohungen benachrichtigen
- Reporting in Echtzeit, das Mac-Administrator*innen mehrere Einblicke bietet, von Zusammenfassungen auf hoher Ebene bis hin zu detaillierten Angaben
- Geringer Ressourcenbedarf für Agenten, die auf Endgeräten installiert sind: geringere Ressourcennutzung = bessere Leistung

Es gibt Funktionen, die nicht unbedingt erforderlich sind, aber den IT- und Sicherheitsteams das Leben erleichtern und gleichzeitig die Fähigkeit verbessern, auf festgestellte Probleme zu reagieren, sie zu bewerten und zu beheben:

1. Fähigkeiten zur Integration mit anderen Produkten. Ein Beispiel: Übermittlung von Ergebnissen zum Gerätezustand von Ihrem Endpunktschutz an Ihre MDM-Lösung, **um SOAR-Workflows (Security Orchestration, Automation and Response) zu ermöglichen, die automatisch erkannte Probleme** beheben, wie z. B. das Entfernen von Malware und die Durchführung von Bereinigungsaufgaben.
2. Besonders wichtig in stark regulierten Umgebungen ist die **Ausrichtung an Sicherheitsframeworks**, die von der Branche genehmigte Leitlinien auf der Grundlage bewährter Verfahren für die Einstellung von Geräten und die Messung der wichtigsten Kennzahlen zur Unterstützung des höchstmöglichen Sicherheitsniveaus bieten.

Geräteverwaltung

Der Einsatz einer MDM-Suite (Mobile Device Management) ist der Schlüssel zu einer effektiven, effizienten und proaktiven Verwaltung Ihrer Flotte von macOS- und iOS-Geräten. Es spricht zwar nichts dagegen, dass die IT-Abteilung das native Konfigurationsprogramm von Apple, den Apple Configurator 2, verwendet, um jedes Gerät manuell zu konfigurieren, aber die Realität dieses Prozesses ist, dass die App nur für die gleichzeitige Bearbeitung einiger weniger Geräte konzipiert wurde. Wenn es um die Bereitstellung und Verwaltung von Hunderten oder Tausenden von Geräten geht, ist die Geräteverwaltung über die MDM Software – wie **Jamf Pro** oder **Jamf Now**– eindeutig die erste Wahl.

Durch die Anpassung an die Verwaltungs-, Sicherheits- und Datenschutz-Frameworks von Apple ermöglicht Jamf Pro der IT-Abteilung die Verwaltung ganzer Flotten über ein einziges, benutzerfreundliches Dashboard. Dabei werden fortschrittliche Funktionen mit leistungsstarken Arbeitsabläufen kombiniert, um die Geräte konfiguriert zu halten und mit den Unternehmensrichtlinien in Einklang zu bringen, ohne die Apple-Endbenutzererfahrung zu beeinträchtigen.

Die Geräteverwaltung verbessert die allgemeine Sicherheit, indem sie Organisationen in die Lage versetzt:

- Vereinfachtes Onboarding/Offboarding durch standardisierte Geräteregistrierungen
- Standardisierte Konfigurationen, die als Vorlagen dienen, um den Anforderungen bestimmter Abteilungen, Benutzertypen oder Gruppen gerecht zu werden, z. B. wenn alle Ärzte dieselben Anwendungen für die Dokumentation von Patientengesprächen oder den Zugriff auf Peripheriegeräte wie Drucker und Scanner in der Abteilung verwenden
- Entwicklung von Richtlinien zur Durchsetzung von Unternehmensrichtlinien, wie z. B. einer Richtlinie zur akzeptablen Nutzung (AUP)
- Verteilen Sie Software und Updates auf Geräte und stellen Sie den Self Service so ein, dass vorautorisierte Apps angezeigt werden, die die Benutzer installieren können. Keine Fummelei mit Apple-IDs oder individuellen Abonnementkosten/pro Benutzer*in anfallende Gebühren für Apps
- Verwalten Sie Ihren Bestand, einschließlich Hardware, Software und Gesundheitszustand Ihrer Apple-Flotte
- Implementierungmoderner Verfahren zur Identitätsverwaltung, um zu verfolgen, welche Geräte welchen Benutzer*innen zugewiesen sind, einschließlich Seriennummern, Garantieinformationen und Servicestatus
- Verfolgungund Lokalisierung fehlender Geräte in Echtzeit bei gleichzeitiger Minimierung des Risikos von Datenverlusten durch Befehle zum Sperren und Löschen aus der Ferne

Verwaltung des Lebenszyklus von Apps und Patch-Unterstützung

Wie führt Ihre Organisation Aktualisierungen des Betriebssystems und der Apps durch? Werden Aktualisierungen in nicht produktiven Umgebungen auf Kompatibilität getestet, bevor sie auf produktiven Systemen bereitgestellt werden? Welches System zur Überprüfung der Aktualität der Patches für die Geräte in Ihrer Flotte gibt es außerdem? Wenn die Antwort auf eine dieser Fragen "?" lautet, gehört Ihre Organisation möglicherweise zu den 39 %.

Was sind die 39 %, fragen Sie? Das ist eine ausgezeichnete Frage!

Die 39 % beziehen sich auf den Prozentsatz der Unternehmen, die nach den in Jamf's **Security 360 veröffentlichten Schlüsselergebnissen: Annual Trend Report** veröffentlicht wurden, **"Geräte mit bekannten Betriebssystemschwachstellen in einer Produktionsumgebung ohne Einschränkung der Privilegien oder des Datenzugriffs betrieben haben".**

Dies ist problematisch, da eine beträchtliche Anzahl von **Common Vulnerabilities and Exposures** (CVE) auf ungepatchte Schwachstellen zurückgreift, um Endgeräte anzugreifen und zu gefährden. Die CVE-Liste der öffentlich bekannt gegebenen Cybersicherheitsschwachstellen wird von der **MITRE Corporation** geführt und vom US-Heimatschutzministerium (DHS) und der **Agentur für Cybersicherheit und Infrastruktursicherheit** (CISA) gesponsert. Sie enthält über 160.000 einzigartige CVE-Einträge, die sich in ihrem Schweregrad unterscheiden.

Auch hier ist eine MDM-Lösung unerlässlich, die Versionsstufen für die installierte Software auf Ihrer Geräteflotte und Funktionen für die Verwaltung des Lebenszyklus von Apps bietet, die es der IT-Abteilung ermöglichen:

- Bestimmen Sie, für welche Geräte Aktualisierungen für Betriebssysteme, Apps und Peripheriegeräte erforderlich sind
- Identifizieren Sie, welche Patches im Vergleich zu einer aktualisierten Liste der aktuellen iOS-Versionen erforderlich sind
- Apps und Services deaktivieren, für die keine Patches verfügbar sind oder die vom Entwickler nicht mehr unterstützt werden und die eine Bedrohung darstellen
- Nutzen Siedie "Smart Groups" von Jamf in Verbindung mit "Richtlinien", um Aktualisierungen effizient an die Geräte zu liefern, und zwar nur an die, die sie benötigen

Härtende Geräte

Die Sicherung von Geräten ist keineswegs eine triviale Aufgabe. Abhängig von Ihrer Umgebung, den organisatorischen Anforderungen, den gesetzlichen Vorschriften und der Anzahl und Art der zu konfigurierenden Geräte kann die Erstkonfiguration zwischen einigen Minuten und mehreren Stunden pro Gerät dauern. Je größer die Flotte, desto komplexer sind in der Regel die Anforderungen an die Benutzer innen und die Konformität. Je größer die Flotte ist, desto länger braucht die IT-Abteilung natürlich, um die Geräte zu sichern. Hundert Geräte innerhalb einer Abteilung zu sichern, nimmt weit weniger Zeit in Anspruch als fünfzig Geräte in fünf verschiedenen Abteilungen zu konfigurieren, von denen sich die Hälfte außerhalb des Standorts befindet.

Dies zeigt, wie wichtig es ist, die richtigen Werkzeuge für die jeweilige Aufgabe zu beschaffen. In diesem Fall stellt die Härtung eine "Sperrung" von Funktionen dar, die entweder unnötig sind oder für einen bestimmten Zweck konfiguriert werden müssen, um den Richtlinien des Unternehmens zu entsprechen. Sie dient auch dazu, die Angriffsfläche von Geräten zu begrenzen, um schädlichen Akteuren **weniger Angriffsvektoren zu bieten**.

Ein Großteil dieser Funktionen ist über die MDM-Lösung konfigurierbar, mit der Sie Ihre Flotte verwalten. Der Schlüssel zu einer maximalen Unterstützung von macOS und iOS liegt darin, sicherzustellen, dass Ihre Lösung **noch am selben Tag Unterstützung** für die neuesten Apple-Betriebssysteme bietet, was auch die Unterstützung der Apple-Geräteverwaltung, der Sicherheit und der Frameworks für den Datenschutz beinhaltet. Dies bietet umfassende Unterstützung für:

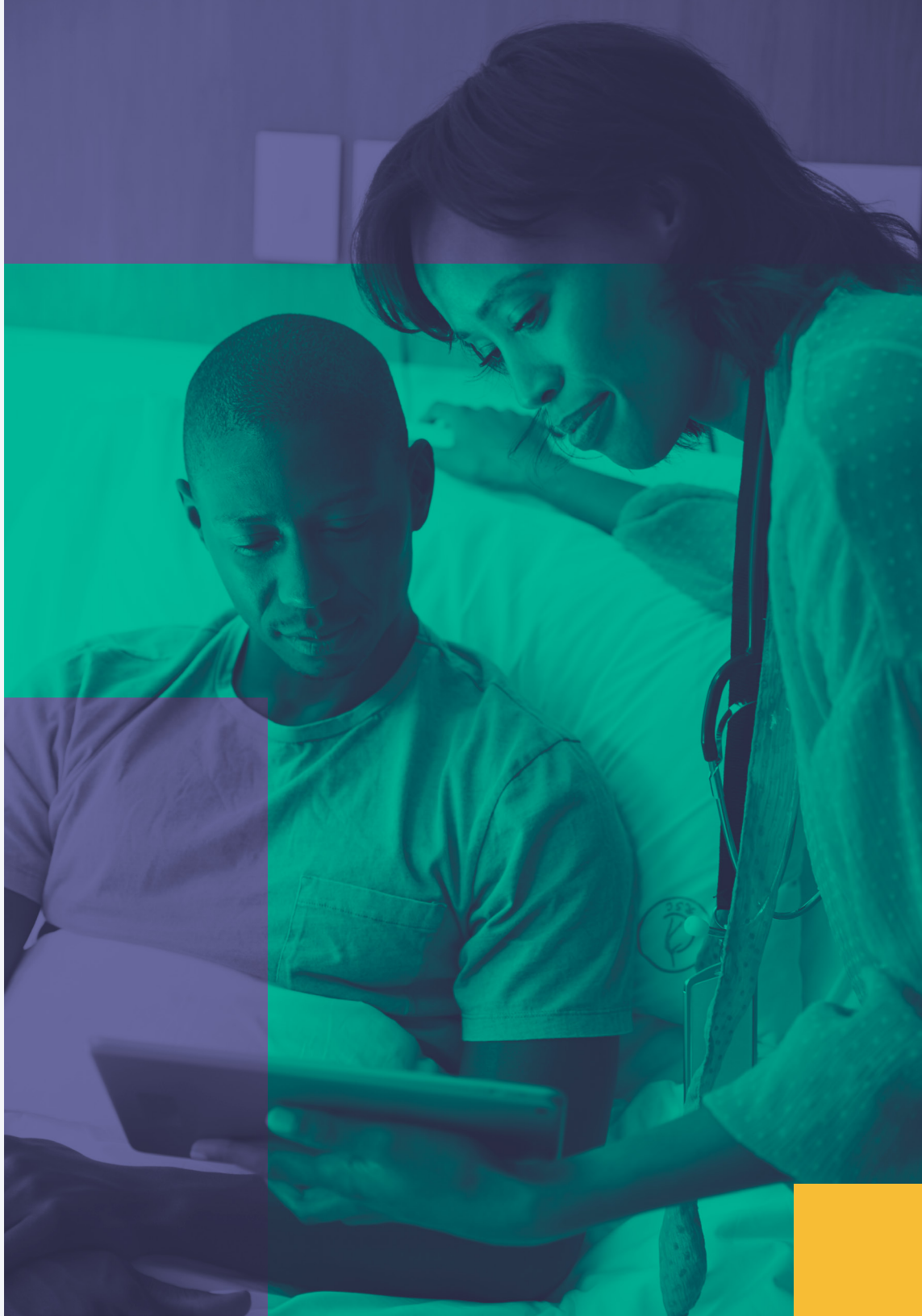
- Befehle zum Verwalten von Geräten
- Konfigurierbare Einstellungen für mehr Sicherheit der Geräte
- Einhaltung der Kontrollen des Benutzerdatenschutzes durch alle Apps

Die Aktivierung der FileVault-Vollverschlüsselung ist beispielsweise notwendig, um Daten im Ruhezustand vor unbefugten Benutzern zu schützen und um im Falle des Verlusts oder Diebstahls eines Geräts sicherzustellen, dass die auf dem Gerät gespeicherten privaten Daten ohne den Entschlüsselungsschlüssel für niemanden lesbar sind. Ohne die entsprechende Unterstützung können jedoch selbst Benutzer*innen mit gültigen Accounts den Inhalt des Laufwerks möglicherweise nicht entsperren, wenn ihr Account nicht der Sicherheitsgruppe des FileVault-Benutzers für dieses Gerät hinzugefügt wurde. Wenn Ihre **MDM-Lösung FileVault korrekt verwaltet**, fügt sie den Benutzer der entsprechenden Gruppe hinzu, damit Benutzer innen auf die gesicherten Daten zugreifen können. Und im Notfall wird automatisch ein Wiederherstellungsschlüssel generiert und im Gerätedatensatz innerhalb des MDM zum Abruf gespeichert.

Sicherer Zugriff und Kommunikation

Wir haben uns mit der Bedeutung des Schutzes von Endgeräten, der Verwaltung und Absicherung von Geräten und der Aktualisierung von Geräten befasst. Gehen Sie nun zur Sicherung von Netzwerkverbindungen mit **Lösungen über, die für die moderne Datenverarbeitung entwickelt wurden**, und erfahren Sie, wie dies eine entscheidende Rolle für die Sicherheit von Daten, die Aufrechterhaltung ihrer Integrität und den Schutz vor unbefugten Bedrohungen spielt, ohne dass Endnutzer davon betroffen sind.

Vor fünf bis zehn Jahren, als VPN die wichtigste Methode zur Sicherung der Kommunikation war, wäre das ein vernünftiger Ansatz gewesen. VPN war — und ist für einige vielleicht immer noch — der De-facto-Standard für die Verschlüsselung von Netzwerkverbindungen, insbesondere wenn es um Fernverbindungen zu Unternehmensressourcen geht. In modernen Umgebungen aus der Ferne und in hybriden Arbeitsumgebungen wie Telehealth ist das VPN-Sicherheitsmodell jedoch veraltet und bietet einfach nicht **die Flexibilität und den zusätzlichen Sicherheits- und Zugriffsschutz**, den ZTNA bietet.



Laut **Gartner** ist Zero Trust Network Access (ZTNA) ein Produkt oder Service, der **eine identitäts- und kontextbasierte, logische Zugriffsgrenze um eine App oder eine Reihe von Apps erzeugt**. Kurz gesagt, das Sicherheitsmodell schafft anwendungsbasierte Mikrotunnel. Daher können sich die Stakeholder auf die gleichen Vorteile verlassen:

- Nur autorisierte Benutzer können sich mit Gesundheitsanwendungen verbinden.
- Die Durchsetzung von Richtlinien ist über alle Ressourcen und Clouds hinweg einheitlich.
- Mikrotunnel gewährleisten den Zugang mit geringstem Recht und verhindern seitliche Bewegungen
- Aktivieren Sie die Single-Sign-On (SSO)-Authentifizierung für eine einheitliche Authentifizierung über alle Geräte hinweg.

VPN macht zwar einiges richtig, aber auf Kosten einiger erheblicher Sicherheitsprobleme, wie z. B. der Tatsache, dass der Benutzer bei der Gewährung des VPN-Zugangs auf alle Ressourcen zugreifen kann – und nicht nur auf die, die er speziell benötigt. Ein weiteres großes Problem, das nicht in der Hand der IT-Abteilung liegt, ist die Tatsache, dass sich die Benutzer für eine VPN-Verbindung entscheiden müssen, bevor der Schutz der Daten aktiviert wird. Dies zeigt **eine von security.org durchgeführte Umfrage**, bei der 43 % der Benutzer*innen auf die Frage "Benutzen Sie ein VPN?" antworteten: "Ich weiß, was das ist, aber ich benutze keines."

Hinter den Kulissen stellt **ZTNA sicher, dass der Benutzer authentifiziert und autorisiert ist und dass das Gerät vertrauenswürdig ist und direkt auf die Daten zugreifen kann**.

Bereitstellung von Identitäten

Die Art und Weise, **wie Sie Benutzeridentitäten verwalten und den Zugriff auf Unternehmensressourcen bereitstellen**, ist für das Sicherheitsmanagement in jeder Umgebung entscheidend. Wenn es um die Sicherheit im Gesundheitswesen und die Einhaltung von Vorschriften geht, ist es absolut entscheidend, alles richtig zu machen. Von der kritischen Arbeit des Pflegepersonals bis hin zu den behördlichen Anforderungen, die die Datenrichtlinien, den Zugriff und die Verwendung vorschreiben, bleibt nur wenig Spielraum für Zeit — und noch weniger Raum für Fehler.

Warum also Benutzerkonten manuell oder ad hoc verwalten, wenn diese Methode stark von manuellen Eingriffen abhängt und daher sehr anfällig für menschliche Fehler ist? Das sollten Sie nicht tun; es ist weder effizient noch effektiv. In dynamischen, sich schnell verändernden Umgebungen profitieren Organisationen von einer standardisierten Bereitstellung von Accounts und Zugängen, um Workflows zu automatisieren. Mit den richtigen Standards für die Bereitstellung von Identitäten und Workflows haben Endnutzer*innen sicheren Zugriff auf das, was sie brauchen, wann sie es brauchen und von jedem Gerät aus, überall.

Die Nutzung von Cloud-basierten Identity Anbietern (IdP), zusammen mit Single-Sign-On (SSO) Technologie erlaubt es der IT-Abteilung, automatisierte Workflows zu erstellen, die als Vorlagen dienen:

- Standardisierung des Onboardings für neue Mitarbeiter*innen
- Streamline Hardware-Bereitstellungen
- Bereitstellung des Zugangs zu Ressourcen, einschließlich Apps und Services
- Umsetzungund Durchsetzung von Richtlinien für Passwörter
- Synchronisierung von Passwörtern über alle Gerätetypen hinweg
- Integration mit ZTNA, um den Zugriff auf Ressourcen zu beschränken, wenn der Zugang gefährdet ist, ohne den Zugriff auf nicht betroffene Services zu verhindern

Bereitstellung von Hardware

Der Einsatz neuer Geräte wie MacBook Pro Laptops und mobiler Geräte wie iPad oder iPhone scheint auf den ersten Blick eine einfache Angelegenheit zu sein: Geräte kaufen, Geräte konfigurieren und Geräte einsetzen. Allerdings gibt es in diesem Verfahren häufig Hindernisse oder Hemmnisse. Unabhängig davon, ob es sich um Beschaffungsprobleme oder um Probleme bei der Koordinierung der Logistik handelt, um die Geräte in die Hände der Nutzer zu bekommen, sind die Chancen ziemlich groß, dass die größte (zeitliche) Hürde der Bereitstellungsprozess sein wird.

Das muss aber nicht so sein. Tatsächlich hat Apple große Anstrengungen unternommen, um sicherzustellen, dass seine Geräte fast berührungslos eingesetzt werden können (Zero-Touch-Deployment). Mit dem Zero-Touch-Bereitstellungsmodell kann die IT-Abteilung Geräte innerhalb kürzester Zeit bereitstellen:

- ☑ Registrieren Sie sich für einen Apple Business/School Manager Account
- ☑ Verknüpfen Sie Ihren Apple Business/School Manager Account mit Ihrer MDM-Lösung
- ☑ Konfigurieren Sie die Einstellungen für das Pre-Stage Enrollment Profile

Das war´s!

Wenn Ihre Organisation Geräte von Apple (oder dessen autorisierten Partnern) kauft, werden die Geräte-Datensätze Ihrem ASM/ABM Account hinzugefügt. Sobald Sie bei Apple registriert sind, kann Ihr MDM den Rest erledigen.

Durch Hinzufügen einer IdP-Lösung wie Jamf Connect **kann der Bereitstellungsprozess weiter automatisiert werden, indem die Cloud-basierte, SSO-fähige Authentifizierung** erweitert wird, so dass die Geräte direkt von Apple an den Endbenutzer geliefert werden können, was eine erhebliche Zeit- und Arbeitsersparnis bedeutet. Damit entfällt der Aufwand für die manuelle Konfiguration durch die IT-Abteilung, und die Benutzer können ihre neuen Geräte auspacken, einschalten und den Registrierungsprozess abschließen. Während die Benutzer*innen dem optimierten Benutzerregistrierungsprozess folgen, werden im Hintergrund sichere und benutzerdefinierte Workflows ausgeführt, um ihre Geräte mit den wichtigsten Anwendungen, dem Zugang zu Diensten und den Sicherheits- und Konfigurationseinstellungen für Endgeräte auszustatten, die sie benötigen, um mit minimalem Zeitaufwand produktiv zu sein.

Konformitätsberichte

Im Gesundheitswesen wird die Last der Einhaltung der Vorschriften und der vorgeschriebenen Berichterstattung auf Daten gelegt: Gesundheitsakten, Datenschutzdaten von Patienten oder alle Informationen, die zur Identifizierung eines Patienten verwendet werden können, oder Details zu seiner Krankengeschichte. Die Art und Weise, wie diese Daten erhoben, verwaltet, weitergegeben, gespeichert und entsorgt werden, unterliegt den Bestimmungen des HIPAA.

Es handelt sich dabei um Richtlinien, an die sich die Gesundheitsorganisationen halten müssen. Es ist jedoch Sache jeder Organisation, zu bestimmen, wie sie diese Anforderungen einhält und die erforderlichen Schutzmaßnahmen umsetzt und verwaltet. Organisationen des Gesundheitswesens müssen wissen, dass PII/PHI geschützt sind und geschützt bleiben, und für den Fall, dass sie nicht mehr geschützt sind, müssen sie Maßnahmen ergreifen, um zu reagieren und das Problem zu beheben, z. B. indem sie die betreffende App, den Dienst oder das Gerät wieder in Übereinstimmung mit den Vorschriften bringen — und zwar schnell!

Bei der Bewertung von Software für die Erstellung von Berichten über die Einhaltung von Vorschriften und bei der Prüfung, wie sie die **Sicherheit erhöhen und gleichzeitig die Arbeit bei der Überprüfung der Einhaltung von Vorschriften verkürzen kann**, sollten Sie Folgendes beachten:

- Logs können gesammelt und in Echtzeit von jedem Endpunkt zu einem zentralen Punkt zur Überprüfung durch IT- und Sicherheitsteammitglieder gestreamt werden.
- Integrierte Ereignisfilter untersuchen Protokolle, um nach Schweregrad geordnete Probleme zu erkennen.
- Konfigurierbare Ausführlichkeitsstufen für Überwachungsprotokolle zur Anwendung von Vorlagen für eine Vielzahl von Gerätetypen und Compliance-Stufen
- Mehrere Methoden zur Bereitstellung und Konfiguration von Compliance-Software auf Endgeräten entsprechend den Anforderungen Ihres Unternehmens
- Anpassbare Erkennungspräferenzschlüssel zur Anpassung der Datenerfassung an gesetzliche Anforderungen
- Ausrichtung auf vertrauenswürdige Compliance-Rahmenwerke wie NIST SP 800-53r4, NIST SP 800-171 und Cybersecurity Maturity Model Certification (CMMC) für die Verwaltung kontrollierter, nicht klassifizierter Informationen (CUI) in nicht-bundesstaatlichen Systemen und Organisationen
- Integration mit Softwarelösungen zur zentralen Erfassung von Streaming-Protokollen (SIEM), Entwicklung von Richtlinien, um die Konformität von Geräten zu gewährleisten (MDM) und Ausführung von Abhilfeworkflows, um Risiken durch Malware und unerwünschte Anwendungen zu mindern (Endpunktschutz)

"DER BESTE WEG, DIE ZUKUNFT VORHERZUSAGEN, IST, SIE ZU GESTALTEN."

– Abraham Lincoln

In diesem Fall liegt die Zukunft in technologischen Fortschritten, die den Zugang zum Gesundheitswesen aus der Ferne und Telehealth-Medizin ermöglichen. Obwohl die Telemedizin bereits von Gesundheitsdienstleistern auf der ganzen Welt genutzt wird, bringt die Ausweitung der Telemedizin von reinen Fernkonsultationen zu hybriden Modellen, die persönliche Besuche einschließen, viele Möglichkeiten und eine Reihe von Sicherheitsbedenken mit sich.

Es sollte nicht überraschen, dass ein Gerät wie ein MacBook Pro oder ein iPad, das im Außendienst verwendet wird, mit größerer Wahrscheinlichkeit verloren geht oder gestohlen wird und/oder eher Opfer von Datenlecks durch schlecht entwickelte Apps oder von Man-in-the-Middle (MitM)-Angriffen wird, wenn es sich mit nicht vertrauenswürdigen Wi-Fi-Hotspots verbindet.

Schädliche Akteure wird es immer geben. Es gibt kein Patentrezept oder eine magische Lösung, um sie davon abzuhalten, Schwachstellen auszunutzen oder PHI zu kompromittieren. Dies soll Sie nicht erschrecken, sondern vielmehr über eine sehr reale Bedrohung informieren, die ständig und überall lauert — online, offline, in der Krankenhauscafeteria, in den Wohnungen der Patienten oder auf dem Arbeitsweg. Ob Gesundheitsdienstleister*innen von Sicherheitsverletzungen betroffen sein werden, ist keine Frage des "**ob**", sondern des "**wann**".

Für diejenigen, die angegriffen werden, ist dies eine unbekannte Größe. Aber es muss auch nicht alles so düster sein...

- ☑ Bleiben Sie informiert
- ☑ Fortlaufende Schulungen für Mitarbeiter*innen zur **Erkennung von Phishing-Versuchen** und zum Reporting von Sicherheitsbedenken
- ☑ Zusammenarbeit mit vertrauenswürdigen Partnern, um die **sichersten Softwarelösungen und Dienstleistungen zu nutzen**
- ☑ Anpassung der Gesundheitsfürsorgerichtlinien an die gesetzlichen Anforderungen und an die Industriestandards für Gerätemanagement, Sicherheit und Datenschutz
- ☑ Erwägen Sie Risikobewertungsprozesse und eine mehrgleisige, eingehende Verteidigungsstrategie
- ☑ Angriffsflächen verkleinern
- ☑ Risiken minimieren, Bedrohungen eindämmen und Probleme beheben
- ☑ Aufrechterhaltung der Gerätekonformität
- ☑ Schutz von Benutzer*innen, Geräten und sensiblen Daten
- ☑ Schulung der Endbenutzer, um die Bedrohungen von heute... und morgen zu erkennen.

"...DAS MORGEN GEHÖRT DENEN, DIE SICH HEUTE DARAUF VORBEREITEN."

– Malcolm X

Angesichts der Ausweitung der Gesundheitsdienste, der bekannten und unbekannten Bedrohungen, denen die Branche ausgesetzt ist, und der Worte von Malcom X und Abraham Lincoln — im Wesentlichen heute kluge Entscheidungen zu treffen, die das Morgen Ihrer Organisation formen und effektiv gestalten — besteht Hoffnung und die Möglichkeit für Gesundheitsdienstleister, die modernen Sicherheitsanforderungen von heute zu erfüllen.

Jamf ist bereit, Ihnen bei der Erfüllung Ihrer Sicherheitsanforderungen zu helfen. Probieren Sie es mit einer kostenlosen Testversion aus.

Testversion anfordern

Oder wenden Sie sich an Ihren bevorzugten Apple Partner, um Jamf kostenlos zu testen.