jamf

Verwalten und schützen Sie Ihre anfälligsten Endpoints: mobile Geräte

Wenn wir von mobilen Geräten sprechen, denken wir an Laptops, Tablets und Smartphones. Obwohl jedes Gerät in die Kategorie der mobilen Geräte fällt, konzentriert sich dieser Beitrag auf Smartphones und Tablets. Millionen von Nutzer:innen weltweit verlassen sich auf diese Geräte, um ihre täglichen Aufgaben bei der Arbeit, in der Schule und im Privatleben zu bewältigen. Diese Abhängigkeit von mobilen Geräten hat jedoch auch erhebliche Bedenken hinsichtlich der mobilen Sicherheit aufgeworfen.

Es ist möglich, Ihre mobilen Endgeräte zu sichern und gleichzeitig die Compliance aufrechtzuerhalten und ein unvergessliches Benutzererlebnis zu schaffen. Nach der Lektüre wissen Sie, wie Sie den Schutz mobiler Geräte effektiv und effizient an die gleichen Standards anpassen können wie den Rest Ihrer Flotte.

Stand der mobilen Sicherheit

Mithilfe von Mobilgeräte können Organisationen die Abläufe in verschiedenen Geschäftsbereichen optimieren. Dank ihrer Benutzerfreundlichkeit, Portabilität und der Möglichkeit, von überall aus auf Apps und Ressourcen zuzugreifen, helfen sie sowohl Außendienstmitarbeitenden als auch Unternehmensteams, konnektiv und produktiv zu bleiben.

Tauchen Sie ein und erfahren Sie mehr über:

Organisationen nutzen häufig eine Reihe von Modellen für den Besitz von Mobilgeräten, wie z. B. gemeinsame oder individuelle Bereitstellungen für Mitarbeiter:innen an vorderster Front (z. B. Krankenschwestern oder Mitarbeiter:innen im Einzelhandel) und unternehmenseigene, personalisierte (COPE) oder Bring-Your-Own-Device (BYOD)-Programme für die Beschäftigten des Unternehmens. IT-Teams, die für die Bereitstellung und das Management verantwortlich sind, müssen maßgeschneiderte Konfigurationen für die Sicherheit auf der Grundlage der individuellen Anforderungen des jeweiligen Modells anbieten. Unabhängig davon, ob die Geräte gemeinsam genutzt und streng kontrolliert werden oder ob sie sich in persönlichem Besitz befinden und dem Datenschutz unterliegen, ist es wichtig, auch das Nutzererlebnis insgesamt zu verbessern.

Die zunehmende Akzeptanz und Abhängigkeit von mobilen Geräten bedeutet aber auch, dass die Sicherheit eine größere Rolle spielt. Einige der häufigsten Auswirkungen auf das Unternehmen sind:

- Zusätzliche Risiken von Datenlecks
- Unbefugter Zugriff auf private Nutzerinformationen
- Mangelnde Vereinbarkeit zwischen Mobilgeräten und dem Nutzererlebnis
- Umsetzung und Einhaltung der Compliance

Die Lücken zwischen den Sicherheitsrichtlinien, die für den Schutz von Computern entwickelt wurden, und der Wirksamkeit ihrer Durchsetzung auf mobilen Geräten können die Sicherheitslage von mobilen Geräten schwächen und die Sicherheitslage des Unternehmens insgesamt verringern. Ein anderer Aspekt ist die Komplexität, die mit der Unterstützung mehrerer Plattformen einhergeht, was sich auf die Geschwindigkeit der mobilen Bereitstellung auswirkt - sowohl bei der Bereitstellung unternehmenseigener Geräte für die Nutzer:innen als auch bei der Gewährleistung der Sicherheit von Unternehmensdaten auf privaten Geräten, die für die Arbeit genutzt werden. All dies ohne Beeinträchtigung der Privatsphäre des Nutzers/der Nutzerin oder der Benutzerfreundlichkeit seines Geräts.

Eine weitere wichtige Überlegung ist, ob Ihr Unternehmen Richtlinien hat, die die Nutzung von Mobilgeräten einschränken, die nicht unter ein BYOD-Programm fallen. Wenn Sie glauben, dass Ihr Unternehmen gegen mobile Bedrohungen immun ist, sollten Sie das unbedingt überdenken. Stellen Sie sich zunächst die Frage, ob wir die private Nutzung von Mobilgeräten erlauben

Geräte können sensible Daten enthalten oder werden zur Durchführung wichtiger geschäftlicher Workflows benötigt. Zum Beispiel Mobilgeräte, die von Direktor:innen oder Vizepräsident:innen für normale Geschäftsaufgaben verwendet werden. Diese Geräte werden häufig für die organisatorische Kommunikation eingesetzt, dienen aber auch als offensivere Vektoren für Angriffe. Oder denken Sie an Geräte, die für bestimmte Anwendungsfälle bereitgestellt werden, wie iPads für Vertriebsmitarbeiter:innen im Außendienst oder in der Fertigung. Diese Geräte sind „im Außeneinsatz“, stellen aber auch besondere Anforderungen an die Compliance und die Benutzerfreundlichkeit.

Mobilitätstreiber

Das herkömmliche Konzept der Unternehmensmobilität, das sich auf die Entwicklung unserer Arbeitsweise bezieht, stand vor erheblichen Herausforderungen, die eine rasche Veränderung der Organisationsmodelle erforderlich machten. Dieser Wandel wurde durch verschiedene Faktoren vorangetrieben, darunter:

- Die Migration von Operationen zu Cloud Diensten
- Die Einführung von verteilten Arbeitsplätzen
- Die zunehmende Verbreitung von nativen, mobilen Apps

Die Entwicklung und Nutzung mobiler Geschäftsapps passt sich nahtlos an die sich ständig verändernden Arbeitsumgebungen an und macht mobile Geräte zu unverzichtbaren Werkzeugen. Dies ist vor allem auf ihre Bequemlichkeit, Anpassungsfähigkeit, ihr Engagement und ihre Kosteneffizienz zurückzuführen.

Der Schwerpunkt liegt dabei auf der Bedeutung mobiler Geräte und Geschäftsapps für den modernen, globalen Arbeitsplatz:

Mobile Geräte für effizientes Arbeiten:
Mobilgeräte sind unverzichtbar für den Zugang zu geschäftlichen Apps und Netzwerken an jedem Ort und ermöglichen ein intelligenteres, effizienteres Arbeiten.

Beliebtheit von Apps für Mobilgeräte:
Mobile Geräte unterstützen kritische Workflows und enthalten sensible Daten, was sie zu bevorzugten Zielen für Angriffe macht. Geräte, die von Führungskräften oder Teams im Außendienst verwendet werden, müssen ein Gleichgewicht zwischen Benutzerfreundlichkeit und Compliance herstellen.

Vielseitige Workflows:
Mobile Geräte ermöglichen effiziente Arbeitsabläufe, bei denen die Nutzer:innen unterwegs Videokonferenzen abhalten, Nachrichten versenden, den Bestand verwalten, auf Kundeninformationen zugreifen, Dokumente bearbeiten und E-Mails bearbeiten können.

Erwartung an die mobile Leistung:
Da sich viele Nutzer:innen neben oder anstelle von Desktops auf Mobilgeräte verlassen, wächst die Erwartung, dass die mobile Technik nahtlos und effizient als Erweiterung ihrer Arbeit funktioniert.

Innovation am Arbeitsplatz:
Mobile Geräte fördern die Innovation am Arbeitsplatz, indem sie die Zufriedenheit, Produktivität und Bindung der Mitarbeiter:innen steigern und gleichzeitig Organisationen helfen, effizienter zu arbeiten und sich an Veränderungen anzupassen.

Vermehrter Einsatz von Mobilgeräten:
Mobilgeräte dominieren die Internet- und Arbeitsnutzung und werden im Jahr 2024 einen weltweiten Marktanteil von 62,22 % erreichen – laut Statcounter GlobalStats übertreffen sie Desktops und Tablets bei weitem.

Remote- und Hybridarbeit:
Der Einsatz von Mobilgeräten ist nach wie vor entscheidend für Remote-Arbeit und Hybridarbeit. 95 % der Mitarbeiter:innen bevorzugen Remote-Optionen. Mobile Geräte fördern die Zusammenarbeit und Flexibilität, unabhängig vom Standort.

Globale Durchdringung mit Mobilgeräten:
Im Jahr 2024 besaßen weltweit 7,4 Milliarden Menschen ein Mobiltelefon. Smartphones machten dabei 71 % aus – das entspricht etwa 6,7 Milliarden Abonnements – was das globale Ausmaß der mobilen Nutzung verdeutlicht.

Die Landschaft der mobilen Unternehmensbereitstellung

In der Vergangenheit haben sich Unternehmen in der Regel bewusst dafür entschieden, ihre geschäftlichen Anforderungen auf eine einzige Plattform auszurichten, bei der es sich häufig um Microsoft Windows handelte. Dazu gehörte die Beschaffung von Computern, die mit dem gewählten Betriebssystem kompatibel waren. Durch Unternehmensvereinbarungen mit Microsoft konnten Unternehmen die Bereitstellung der neuesten Windows Version so lange hinauszögern, bis sie auf den Übergang vorbereitet waren. Der Vorteil war, dass ältere Betriebssystemversionen über einen längeren Zeitraum weiter unterstützt wurden, um den Bedürfnissen dieser Organisationen gerecht zu werden.

Doch genau hier liegt die Herausforderung: Die mobile Landschaft, die traditionell als verbraucherorientiert gilt, betrachtet Betriebssystem-Patches als Aktualisierungen, die implementiert werden sollten, sobald sie verfügbar sind. Da die Nutzer:innen selbst bestimmen können, wann und wie schnell nach der Veröffentlichung von Aktualisierungen diese installiert werden, hat sich dies in den Unternehmen als Hindernis für die Akzeptanz erwiesen:

- Vielfältige Auswahl an mobilen Betriebssystemen
- Fragmentierung zwischen unterstützten Versionen innerhalb jedes Betriebssystems
- Entwicklung von Bereitstellungsmethoden für verschiedene Betriebssysteme
- Unterschiedliche Unterstützung führt zu verzögerten Upgrades
- Unterschiedliche Unterstützung für Unternehmensanwendungen in verschiedenen Betriebssystemversionen
- Unterschiedliche Aktualisierungszeitpläne und Funktionsunterstützung durch die Entwickler:innen
- Unterschiedliche Eigentumsmodelle mit Auswirkungen auf die Verwaltung (z. B. BYOD vs. COPE)
- Unterstützte vs. nicht unterstützte Funktionen in MDM-Lösungen (nativ vs. nicht-nativ für Frameworks)
- Unterschiedliche Sicherheitsstufen für verschiedene Betriebssysteme
- Begrenzte richtlinienbasierte Durchsetzung von Compliance-Anforderungen

Zunehmende Besorgnis

Wir haben die Sicherheitsbedenken im Zusammenhang mit der raschen Zunahme der Nutzung mobiler Geräte in Unternehmen bereits angesprochen. In diesem Abschnitt befassen wir uns eingehender mit den Bedrohungen, die auf mobile Geräte abzielen, und den Risiken, die mit ihrer Nutzung verbunden sind. Außerdem werden wir uns mit häufigen Missverständnissen über die Sicherheit mobiler Geräte am Arbeitsplatz befassen.

Das erste Problem ergibt sich aus der mobilen Natur dieser Geräte, die aus mehreren Gründen ein attraktives Ziel für Cyberkriminelle sind:

Wertvolle Datenspeicherung:
Mobile Geräte enthalten eine Fülle von persönlichen, geschäftlichen und gesetzlich geregelten Daten wie PHI (persönliche Gesundheitsinformationen) - sogar nicht gesetzlich geregelte, aber sensible Daten wie PII (persönlich identifizierbare Informationen). Cyberkriminelle können diese Informationen für verschiedene Zwecke ausnutzen und möglicherweise Angriffe auf Nutzer:innen oder Organisationen starten. Es ist wichtig, diese Daten auf mehreren Ebenen zu schützen, um sicherzustellen, dass nur autorisierte Nutzer:innen Zugriff haben.

Anfällig für Verlust oder Diebstahl:
Die Mobilität mobiler Geräte ermöglicht es den Nutzer:innen, von verschiedenen Orten aus zu arbeiten, erhöht aber auch das Risiko des Diebstahls oder des Verlegens. Cyberkriminelle können die Gelegenheit nutzen, um Geräte zu stehlen, was eine direkte Bedrohung für die Datensicherheit darstellt. Selbst ein kurzer unbeaufsichtigter Zugriff auf ein Gerät kann es gefährden oder anfällig für künftige Angriffe machen.

Missverständnisse über Sicherheit:
Einige glauben, dass mehr als verschiedene Sicherheitslösungen erforderlich sind. Die sich schnell entwickelnde mobile Bedrohungslandschaft erfordert jedoch eine native Unterstützung für Endpoint-Frameworks. Der Rückgriff auf Lösungen, die diese Unterstützung nicht bieten, kann die Anfälligkeit erhöhen, da Angriffsvektoren in nicht unterstützten Funktionen und Merkmalen offen gelassen werden.

Übermäßig geschützt oder zu wenig verwaltet: das Gleichgewicht finden

Das Gleichgewicht zwischen Geräteverwaltung und Sicherheit ist ein entscheidendes Konzept im Zusammenhang mit der Optimierung mobiler Technologien zur Unterstützung von Mitarbeitenden an vorderster Front. Auch wenn es wie ein Konflikt zwischen IT- und Sicherheitsprioritäten aussieht, ist es in Wirklichkeit unzureichend, sich nur auf die Verwaltung oder die Sicherheit zu konzentrieren. Organisationen müssen beide Elemente nahtlos integrieren, um eine mobile Sicherheitslösung zu schaffen, die Effizienz und Effektivität unterstützt.

Die Herausforderung besteht darin, das richtige Gleichgewicht zu finden. Die übermäßige Sperrung von Geräten mit starren Sicherheitsmaßnahmen kann das Nutzererlebnis beeinträchtigen und die Produktivität der Belegschaft verringern. Andererseits gefährdet die Vernachlässigung der Sicherheit wertvolle Daten und Abläufe. Der Schlüssel liegt nicht darin, sich zwischen Sicherheit und Produktivität zu entscheiden, sondern beides in Einklang zu bringen, um sicherzustellen, dass das Management von Mobilgeräten und die Sicherheit zusammenarbeiten, um Teams an vorderster Front zu unterstützen und gleichzeitig die Unternehmensgeräte zu schützen.

Ausgaben	Übermäßiger Schutz	Unterverwalten
Beeinträchtigte Leistung		✓
Benutzerfreundlichkeit		✓
Schatten-IT (Bedenken hinsichtlich des Datenschutzes können Mitarbeiter:innen dazu bewegen, persönliche Geräte zu verwenden)		✓
Umgehung von Sicherheitsmaßnahmen des Unternehmens		✓
Untergräbt das Potenzial des mobilen Arbeitsplatzes		✓
Einhaltung der rechtlichen Compliance	✓	
Entschärft sich entwickelnde mobile Bedrohungen	✓	
Trennung der Geschäftsdaten von den persönlichen Daten in einem separaten, verschlüsselten Volumen	✓	
Sicherstellen, dass die Patches in regelmäßigen Abständen korrigiert werden	✓	
Optimiert die Bereitstellung von mobilen Endpoints	✓	
Verhindert unbefugten Zugriff auf Unternehmensressourcen	✓	
Angemessener Schutz der Privatsphäre der Nutzer:innen bei gleichzeitigem Schutz der Unternehmensressourcen		✓

Im Folgenden finden Sie einige Strategien, die Unternehmen bei der Umstellung auf ein mobiles Sicherheitskonzept helfen können, bei dem die Privatsphäre der Nutzer:innen im Vordergrund steht und gleichzeitig die Sicherheitsmaßnahmen verbessert werden:

1. Priorisieren Sie benutzerfreundliche Sicherheits-Workflows: Integrieren Sie Benutzerfreundlichkeit und Einfachheit in die Sicherheitsprozesse. Davon profitieren sowohl die Nutzer:innen als auch die Teams, die für die Verwaltung und den Schutz mobiler Geräte zuständig sind.

2. Umstellung auf datenzentrierte Sicherheit:
Anstatt sich ausschließlich auf die Gerätesicherheit zu konzentrieren, sollten Sie sich auf die Datensicherheit konzentrieren. Der Schutz von Geräten ist zwar wichtig, aber sie sind austauschbar. Sensible Daten hingegen müssen immer geschützt werden.

3. Akzeptieren Sie unterschiedliche Eigentumsmodelle:
Seien Sie offen für unterschiedliche Eigentumsmodelle und passen Sie die Sicherheitsmaßnahmen so an, dass sie die Unternehmensressourcen schützen, die von verschiedenen Benutzergeräten aus zugänglich sind. Das Ignorieren bestimmter Geräte kann zu Schwachstellen in Ihrer gesamten Sicherheitsstrategie führen.

4. Umfassender Datenschutz:
Sorgen Sie dafür, dass die Daten in all ihren Formen sicher sind. Dazu gehört die Verschlüsselung von Datenträgern, die Trennung von geschäftlichen und persönlichen Daten und die Sicherung von Daten, die über eine beliebige Netzverbindung übertragen werden.

5. Moderne mobile Technologien einsetzen:
Setzen Sie auf Technologien, die den Anforderungen moderner mobiler Geräte gerecht werden. Herkömmliche Sicherheitstools sind oft nicht in der Lage, sich gegen neue Bedrohungen für Mobilgeräte zu wehren, da sie nur einen teilweisen und keinen umfassenden Sicherheitsschutz bieten.

6. Split-Tunneling einführen:
Erkennen Sie, dass mobile Effizienz entscheidend ist. Geschäftsdaten, die geschützt werden müssen, werden sicher weitergeleitet, während geschäftsfremde Daten, wie z. B. persönliche Informationen, die Sicherheitsprotokolle des Unternehmens umgehen können. Durch diesen Split-Tunneling-Ansatz wird die Datensicherheit aufrechterhalten und gleichzeitig die Privatsphäre der Nutzer:innen auf BYO-Geräten geschützt.

Was passiert, wenn man Mobilgeräte wie Computer behandelt

Welche Auswirkungen hat die zunehmende Integration von macOS und iOS auf die Zukunft der Mobil- und Endpoint-Sicherheit?

Der Vergleich von Mac, einem Desktop-Betriebssystem, mit mobilen Geräten mag zwar wie der Vergleich von Äpfeln mit Birnen erscheinen, aber Tatsache ist, dass jede neue Version von macOS und iOS eine größere Konvergenz zwischen diesen Betriebssystemen mit sich bringt. Mit jeder neuen Version wird die Frage nach der Bedeutung dieser Integration immer wichtiger.

Die wichtigere Frage ist jedoch, wie Unternehmen diese tiefere Integration nutzen können. Im Folgenden finden Sie einige Möglichkeiten, wie sich diese Integration auf verschiedene Gerätetypen erstreckt:

- Rasche Behebung von Sicherheitslücken
- Nahtlose Rückkehr zu mehr Produktivität
- Verbesserte Mitarbeitererfahrung
- Mehr Vertrauen der Belegschaft
- Infrastrukturweite Durchsetzung der Vorschriften
- Stärkere Anpassung an die Unternehmensrichtlinien
- Umfassende, mehrstufige Sicherheitsprozesse
- Bilaterale App-Verwaltung
- Defense-in-Depth-Strategie, unabhängig vom Eigentumsmodell
- Flexible und dennoch robuste Sicherheits- und Verwaltungslösungen, die zusammenarbeiten und umfassende Unterstützung bieten

Mobile Compliance

Die Einhaltung von Vorschriften ist nicht auf regulierte Branchen beschränkt. Für Organisationen in Bereichen wie Finanzen, Gesundheitswesen und Bildung ist sie unerlässlich. Sie umfasst aber auch die Einhaltung von Regeln und Richtlinien, die innerhalb einer Organisation festgelegt wurden, um die speziellen Geschäftsanforderungen zu erfüllen und gleichzeitig die Risiken für die Geschäftskontinuität zu minimieren. In Anbetracht dessen spielt die Implementierung und Durchsetzung einer unternehmensweiten Richtlinie für mobile Geräte, ähnlich wie bei der heutigen Handhabung von Mac Geräten, eine zentrale Rolle bei der Einführung einer umfassenden Strategie für die mobile Sicherheit in Ihrem Gerätepark.

Nehmen wir dieses Beispiel: Mobile Geräte sind in hybriden und dezentralen Arbeitsszenarien einem erhöhten Risiko von Diebstahl, Verlust oder Kompromittierung ausgesetzt, wodurch sensible Unternehmensdaten gefährdet werden können. Die IT-Abteilung kann Verschlüsselungsstandards und sichere Authentifizierungsprotokolle für Geräte und Nutzer:innen durchsetzen, indem sie einen MDM-Workflow zur Bereitstellung standardisierter Sicherheitskonfigurationen nutzt. Darüber hinaus können mit der Fernlöschfunktion bei Bedarf Daten sicher von den betroffenen Geräten gelöscht werden.

Organisationen können einen Compliance Plan für Nutzer:innen von Mobilgeräten entwickeln, unabhängig von ihrem Anwendungsfall.

Dieser Ansatz geht auf inhärente Risiken ein und bietet gleichzeitig eine solide Grundlage, auf der man aufbauen kann. Dies ist besonders wertvoll, wenn es darum geht, Risiken zu mindern, die mit neuen Paradigmen verbunden sind, **wie z. B. neu entwickelte mobile Apps im Vergleich zu einer ausgereiften Website, die** bereits mit Vorschriften wie dem California Consumer Privacy Act (CCPA) konform ist.

Darüber hinaus geht es bei der Einhaltung von Vorschriften darum, Probleme zu entschärfen und zu erkennen, bevor sie sich zu kritischen Schwachstellen oder Verstößen gegen Vorschriften auswachsen. Hier arbeitet die Kombination aus Sicherheit (Überwachung) und Verwaltung (Durchsetzung) zusammen, um Bedrohungen zu erkennen und zu entschärfen und sicherzustellen, dass mobile Geräte die Vorschriften einhalten.

Angesichts der Vielseitigkeit mobiler Geräte kann es vorkommen, dass Nutzer:innen versehentlich zugelassene Dienste für private Aufgaben oder nicht zugelassene Apps für geschäftsbezogene Aufgaben verwenden. Beide Szenarien bergen Risiken, wie z. B. die Vermischung von Daten, die Beeinträchtigung der Privatsphäre der Nutzer:innen oder die Gefährdung des Unternehmens durch Datenschutzverletzungen und Verstöße gegen Vorschriften.

Wenn Unternehmen die Einhaltung von Richtlinien für mobile Geräte mit der gleichen Ernsthaftigkeit behandeln wie andere Endgeräte, können sie sicherstellen, dass alle Endgeräte, die auf Unternehmensressourcen zugreifen, über den gleichen Schutz vor den neuesten Bedrohungen verfügen, und genaue Aufzeichnungen über den Gerätebestand, die Gerätenutzung, die bereitgestellten Geräte, den Zugang der Mitarbeiter:innen zu Unternehmensdaten und die bereitgestellten Sicherheitsmaßnahmen führen.

Ein letzter Aspekt bei der Einhaltung der Vorschriften für mobile Geräte ist die laufende Schulung der Nutzer:innen in Sachen Sicherheit. Dieser Aspekt, der oft übersehen wird, aber für einen umfassenden Plan für mobile Sicherheit unerlässlich ist, **vermittelt den Nutzer:innen Kenntnisse über bewährte Sicherheitspraktiken**, sichere Arbeitsabläufe und Verfahren, die bei potenziellen Sicherheitsbedrohungen zu befolgen sind. Diese Ausbildung ist eine wichtige Schutzmaßnahme, die die Verwaltungs- und technischen Sicherheitsmaßnahmen ergänzt.

Einfach ausgedrückt: Cybersicherheit liegt nicht nur in der Verantwortung der IT-Abteilung oder des Unternehmens - sie liegt in der Verantwortung aller.

Schlüssel zur Vereinheitlichung der Verwaltung und Sicherheit von Mobilgeräten

Falls es noch nicht klar ist, lassen Sie es uns klar sagen: Der Schlüssel zur Sicherheit ist die Vereinheitlichung von Verwaltung und Sicherheit für Ihre gesamte Flotte.

1. Konvergenz:

Der Erfolg stellt sich ein, wenn Verwaltung und Sicherheit nahtlos mit robusten Sicherheitsprotokollen in einem modernen, mobilzentrierten Arbeitsbereich integriert werden.

2. Überwindung:

Die Überwindung mobiler Sicherheitsprobleme erfordert eine umfassende Lösung im Gegensatz zu den traditionellen Einzelansätzen, bei denen mehrere Tools zusammengefügt werden, ohne dass sich ein einzelnes Tool als besonders effektiv erweist.

3. Konsistenz:

Zur Sicherstellung der Einheitlichkeit gehört die Messung der Sicherheitsgrundlagen auf allen Geräten und die proaktive Überwachung der Endpoints auf Veränderungen, die auf das Vorhandensein von Problemen hindeuten könnten, und ob Sicherheitsbedrohungen, Schwachstellen oder Anomalien untersucht werden müssen.

4. Benutzerfreundlichkeit:

Die Priorisierung der Benutzerfreundlichkeit und deren Abstimmung mit dem Schutz ist ein wesentlicher Bestandteil einer umfassenden Strategie, die das empfindliche Gleichgewicht zwischen Effektivität und Einfachheit für IT, Sicherheitsteams und Nutzer:innen betont.

5. Reaktion:

Eine schnelle Reaktion auf Sicherheitsbedrohungen ist unabdingbar, wobei der Schwerpunkt auf der Priorisierung, Untersuchung und Lösung liegt, die alle Gerätetypen, verschiedene Plattformen und die gesamte Infrastruktur umfasst.

6. Gleichgewicht:

Das richtige Gleichgewicht zu finden bedeutet, Sicherheit zu erreichen, ohne das Nutzererlebnis zu beeinträchtigen, und die Möglichkeit zu bekräftigen, Sicherheit und Nutzerzufriedenheit nahtlos miteinander zu verbinden.

Wir stellen uns eine Zukunft vor, in der jedes Gerät kompromisslosen Schutz genießt, ohne Kompromisse eingehen zu müssen. Diese Vision ist das ultimative Ziel: ein ausgewogener, umfassender Schutz von Daten und Datenschutz, der sich auf alle Geräte in Ihrer Infrastruktur erstreckt.

Lassen Sie sich von Jamf dabei helfen, den Sicherheitsbedarf Ihres Unternehmens zu ermitteln und herauszufinden, wie Sie

alle Ihre Endpoints verwalten und schützen können.

jamf

www.jamf.com/de/

Los geht's

Oder kontaktieren Sie Ihren bevorzugten Reseller, um Jamf kostenlos zu testen.