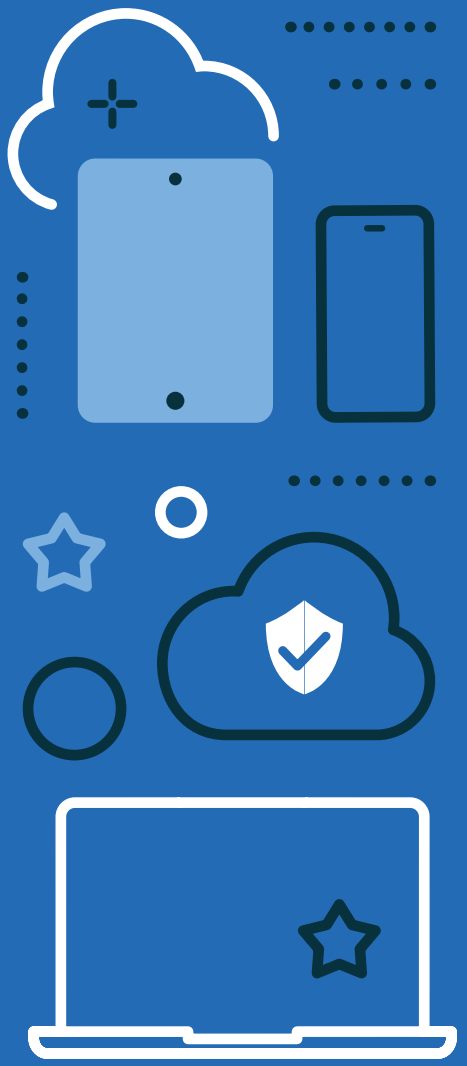


Datenrichtlinien und Verwaltung

für Beginner

jamf

Heute unterstützen Unternehmen mehr denn je Tele- und Hybrid-Mitarbeiter, und sie benötigen mehr als nur die Grundlagen der Geräteverwaltung. Mobilgeräte von Unternehmen bieten die Freiheit, jederzeit und überall zu arbeiten. Aber diese Flexibilität bringt das Problem der persönlichen Nutzung von Firmengeräten, selbst auf persönlichen Geräten ihres Mobilfunkplans.

Jamf Data Policy hilft Organisationen dabei, das Home-Office zu ermöglichen und zu unterstützen, indem sichergestellt wird, dass Benutzer produktiv bleiben, egal wo sie sich befinden und welche Geräte sie verwenden, während sie zu hybriden und Remote-Umgebungen wechseln.

Durch Nutzung der folgenden Technologien können Organisationen Folgendes tun:

- Implementierung von anpassbaren Richtlinien zur Sicherstellung der Compliance
- Datenhöchstgrenzen und Warnschwellen konfigurieren
- Ausfiltern von unangemessenen Inhalten
- Erweitern der Richtlinien auf die gesamte Netzwerkkommunikation
- Überwachung und Eliminierung der Schatten-IT
- Nutzung in Echtzeit verwalten

Erfahren Sie, was Sie für eine Richtlinie für einen akzeptablen Gebrauch wissen müssen und verwalten Sie die Daten und Geräte Ihres Unternehmens auf eine Weise, die die Anforderungen der Firma und der Endbenutzer unterstützt.

Die Verwaltung von Geräten wird oft als eine hohe Wissenschaft betrachtet. Das wird mit allen möglichen Daten unterstützt, um die optimale Verwaltungsebene zu erreichen, und sicherzustellen, dass Geräte, Benutzer und Daten geschützt sind und geschützt bleiben. Und während das nicht umstritten ist, gehört zu einem erfolgreichen Administrator doch auch etwas „Magie." Das geht auf die Erfahrung und ein gründliches Verständnis der einzigartigen Anforderungen Ihres Netzwerks zurück. Schließlich ist jedes Netzwerk, trotz aller Standards und Best Practices, seine eigene Insel und folgt den spezifischen Richtlinien seiner Organisation.

„Es gibt keine Magie!" *– Onkel Vernon*

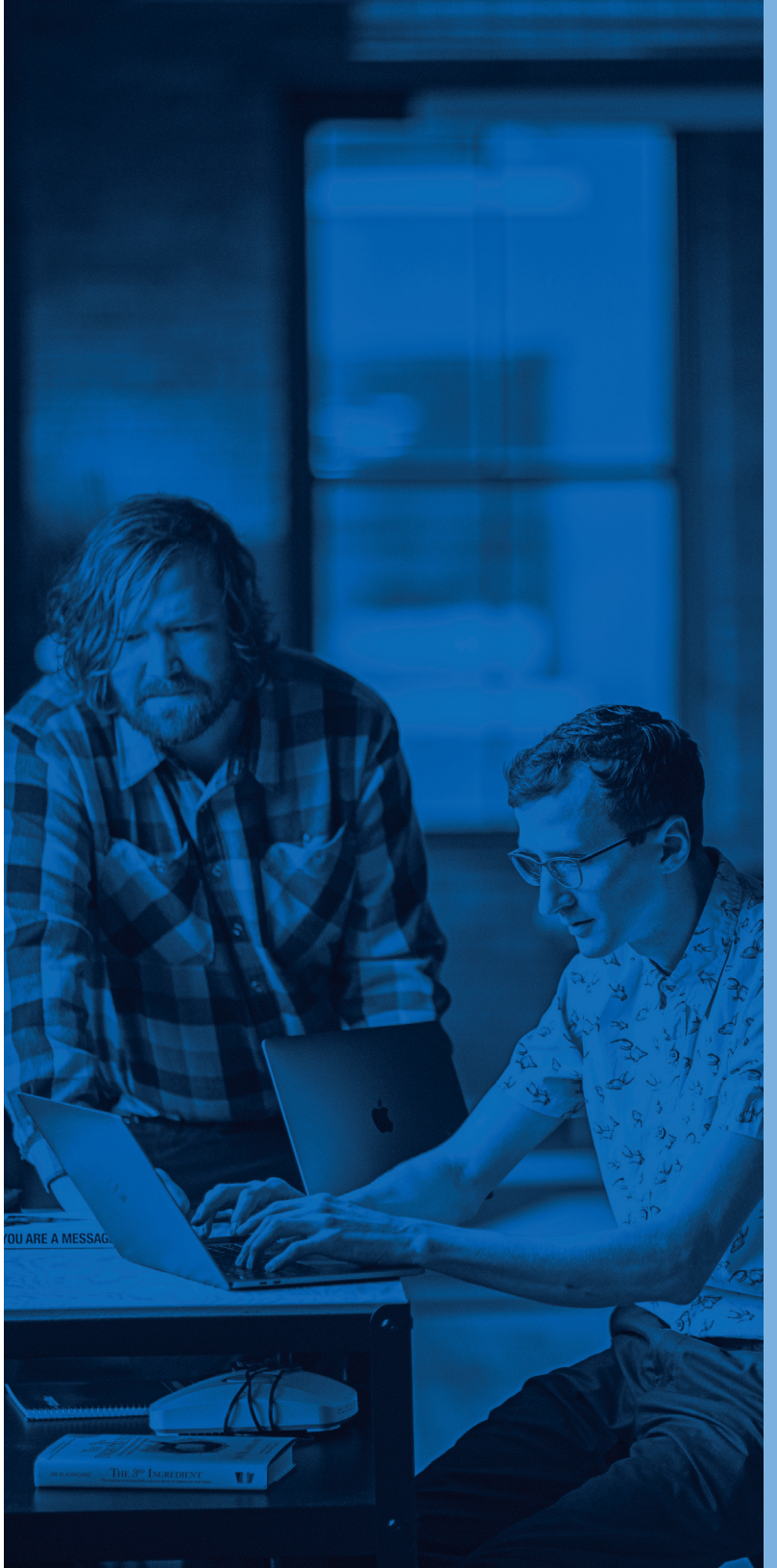
Fühlt es sich nicht magisch an, wenn alle Ihre Geräte optimal funktionieren?

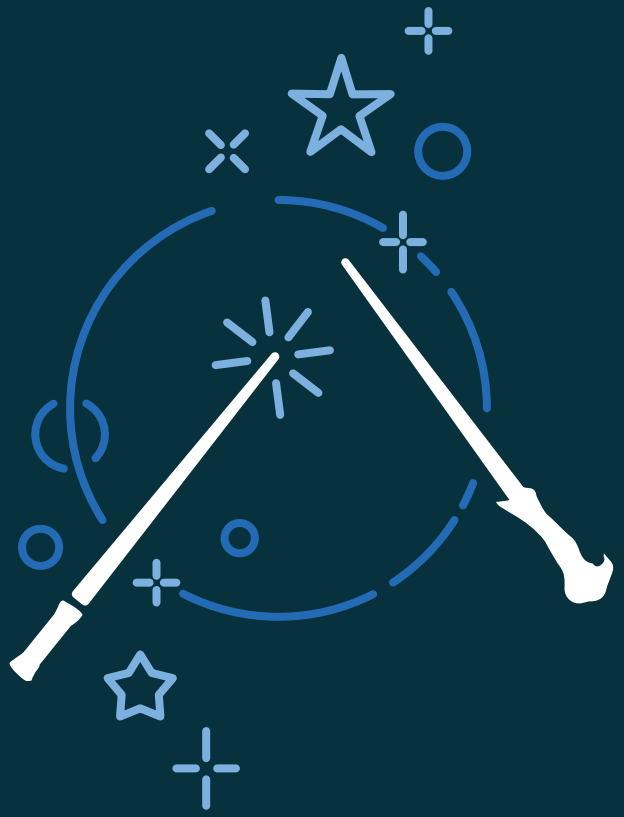
Die Daten sind sicher, Firmen-Apps und Ressourcen sind zugänglich und dennoch geschützt. Und die Benutzer sind glücklich über die Fähigkeit, gesicherte Geräte für die Ausführung von beruflichen und persönlichen Aufgaben zu verwenden, ohne strikte Verwaltungspraktiken, die sie daran hindern, produktiv zu sein oder ihre Freizeit zu genießen. Was passiert, wenn Probleme erkannt werden, aber das Risiko durch Automatisierung gemildert wird, ohne dass die IT-Abteilung einen Finger heben muss oder das Erlebnis des Endbenutzers beeinträchtigt wird?

Das ist die Art von Magie, die Administratoren von Mobilgeräten einsetzen, die Jamf Data Policy nutzen. Jamf Data Policy geht über die Grundlagen hinaus und hilft Organisationen, Geschäftspraktiken in Tele- und Hybridarbeit-Umgebungen zu unterstützen. Unabhängig vom Gerätetyp, oder ob es sich um persönliche Geräte als Teil einer BYOD (Bring Your Own Device) Initiative handelt oder um Firmengeräte, die sowohl für die Arbeit als auch für persönliche Aufgaben verwendet werden, ist es wichtig, eine Richtlinie für den akzeptablen Gebrauch zu haben und sie auch zu verwalten und durchzusetzen.

Hier ist ein Ausgangspunkt für die Erstellung oder Bewertung Ihrer Nutzungsrichtlinie. Überlegen Sie, wie Ihre Organisation Folgendes tun kann:

- Es den Administratoren ermöglichen, den Datenverbrauch mit Echtzeitanalysen und detailliertem Reporting zu überwachen
- Durchsetzung von Nutzungsrichtlinien
- Eliminierung der Schatten-IT
- Inhalte filtern
- Implementierung von maßgeschneiderten Richtlinien zur Erfüllung der Anforderungen Ihrer Benutzer und der Organisation
- Ganzheitliche Unterstützung für Ihr Netzwerk – unabhängig vom Gerät oder der Besitzart



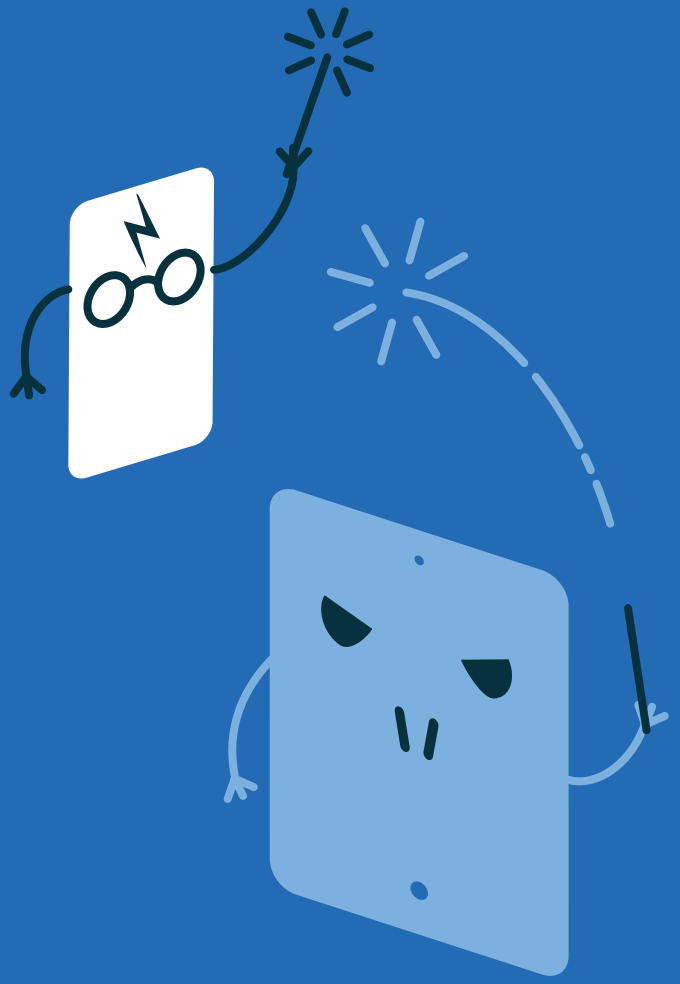


HARRY POTTER GEGEN VOLDEMORT

Bevor Sie sich die Funktionen von Jamf Data Policy genauer ansehen, sollten wir einige der Gründe erwähnen, warum es notwendig ist, um Ihrer Organisation bei der Verwaltung der Mobilgeräte in Ihrem Netzwerk zu helfen. Und wie kann man den Anwendungsfall besser beschreiben als durch einen Hinweis auf den größten modernen Magier, Harry … Potter, das ist richtig!

In den Büchern von J.K. Rowling ähneln die Zauberer des Pottermore-Universums in gewisser Weise IT-Administratoren, da sie die Wahl hatten, wie Voldemort zu sein, oder wie Harry – hören Sie uns bitte weiter zu.

Wenn Sie sich für den Weg von Voldemort entscheiden, würde Ihre Organisation mit einer eisernen Faust regiert, und die Benutzer dazu gezwungen, sich an Ihre Richtlinien anzupassen, unabhängig von ihren Anforderungen oder den unbeabsichtigten Folgen.



Aber wenn Sie Harry nachahmen, würde Ihre Organisation alle fair behandeln und eher Kompromisse suchen, während alle danach streben, das Gesamtproblem zu lösen.

„Bald müssen wir alle die Entscheidung fällen, zwischen dem, was richtig ist und dem was einfach ist“
– Albus Dumbledore

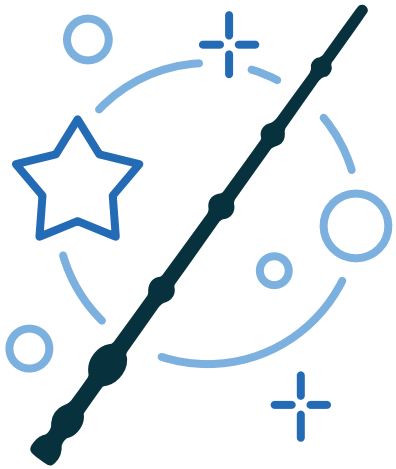
Auch wenn es für die IT-Abteilung einfach ist, dem Pfad Voldemorts im Namen der Sicherheit und des Schutzes der Benutzer zu wählen, bleibt die traurige Realität, dass oft der zweite Weg mehr Optionen bietet, Datensicherheit zu erreichen und Benutzer zu schützen. Dabei arbeiten nämlich alle Beteiligten zusammen, ein gemeinsames Ziel zu erreichen und kämpfen nicht gegen übermäßige oder einschränkende Kontrollen an, die lediglich die Produktivität behindern und die Benutzer vor den Kopf stoßen.

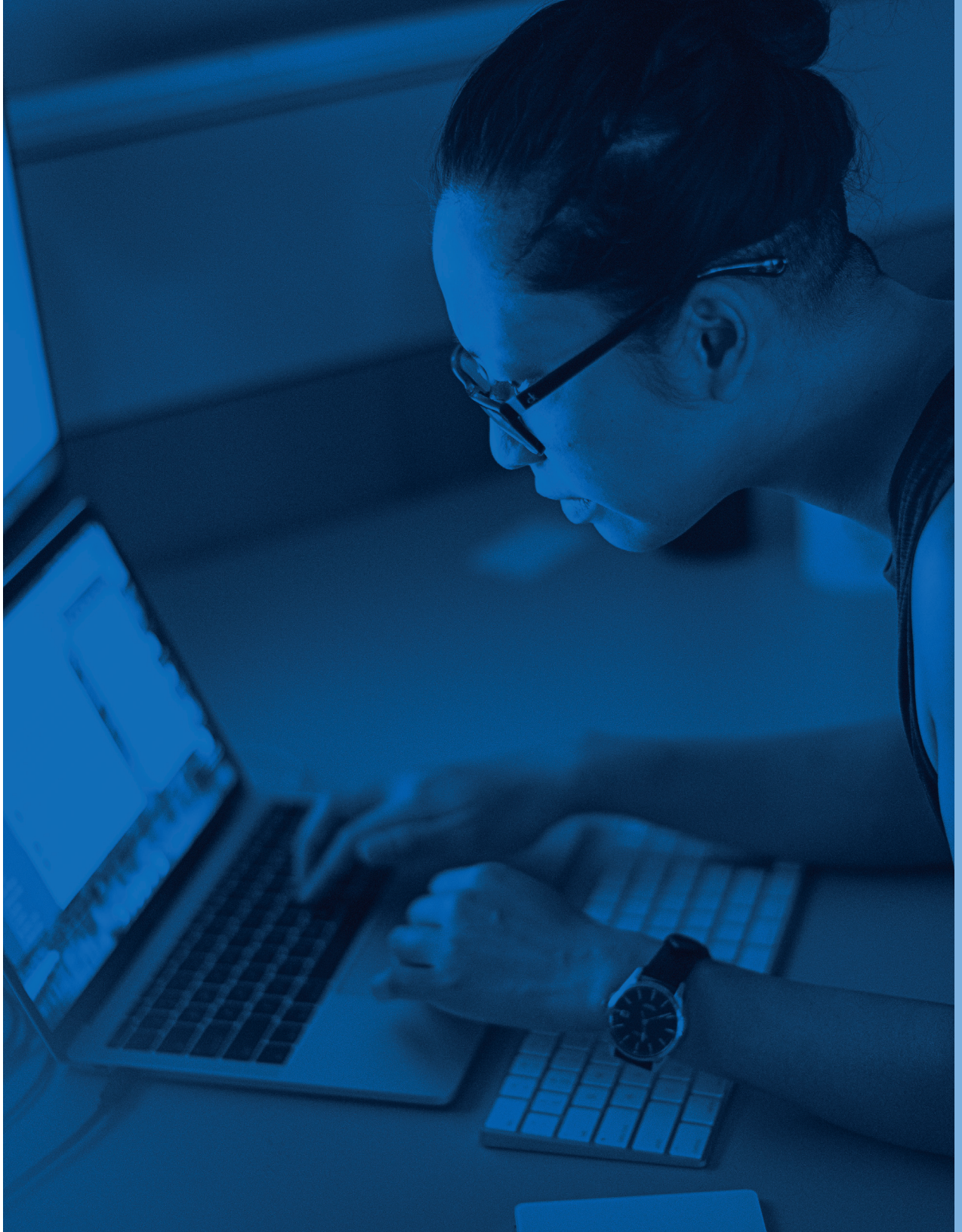
Wie bereits erwähnt ist jedes Netzwerk anders und folgt verschiedenen Regeln, Richtlinien, Gesetzen und Vorschriften. Wenn es also um Datenrichtlinien und Verwaltung geht, gibt es keine Antwort in Einheitsgröße. Wenn man das bedenkt, wird die Verwaltung von Geräten nach der Voldemort-Methode lediglich die IT-Abteilung einengen und die Flexibilität eliminieren, die nötig ist, um potenzielle Probleme in der dynamischen Welt der Informationstechnologie zu überwachen, zu erkennen, darauf zu reagieren und sie zu lösen. Würden Sie nicht zustimmen?

DER ELDERSTAB

Wie Harry Potter sind IT-Administratoren auch nur Menschen. Ganz normale Menschen mit Fähigkeiten, die zwar beträchtlich sind, aber kanalisiert werden müssen, um effektiv zu sein. Harry hatte den Elderstab. Sie haben Jamf Data Policy.

Vor allem wenn wir uns auf zwei Funktionen konzentrieren, die Organisationen den erforderlichen Schutz bieten, um ihr Mobilgeräte auf eine einheitliche und effiziente Weise zu verwalten.





POLICY CONTROL IN ECHTZEIT

Diese umfasst die Konfiguration von Höchstwert-Richtlinien für die Datennutzung und deren Anwendung bei Erreichen von Schwellenwerten, sowie die Transparenz bei der Nutzung durch kategoriebasierte Kontrollen. Darüber hinaus kann das angepasst werden, um die automatische Durchsetzung der Richtlinie auszulösen. Dies zeigt, wie man mit organisatorischen IT-Richtlinien den Zugriff auf unangemessene Inhalte und auf Apps einschränken kann, die nicht als arbeitsrelevant betrachtet werden.

Über 50 % der Datennutzung in Unternehmen ist laut Jamf nicht geschäftlich wichtig. Diese beispiellose Transparenz bezüglich der Datennutzung ermöglicht Organisationen die präzise Konfiguration von Datenpools und netzwerkbasiertem Datenverkehr, damit Mobilgeräte als Werkzeuge verwendet werden, statt als Objekte, die aufgrund eines Mangels an Einsicht oder Kontrolle missbraucht werden.

„Der Lauf der Zeit verlangsamt sich nicht, wenn etwas Unangenehmes auf einen zukommt“

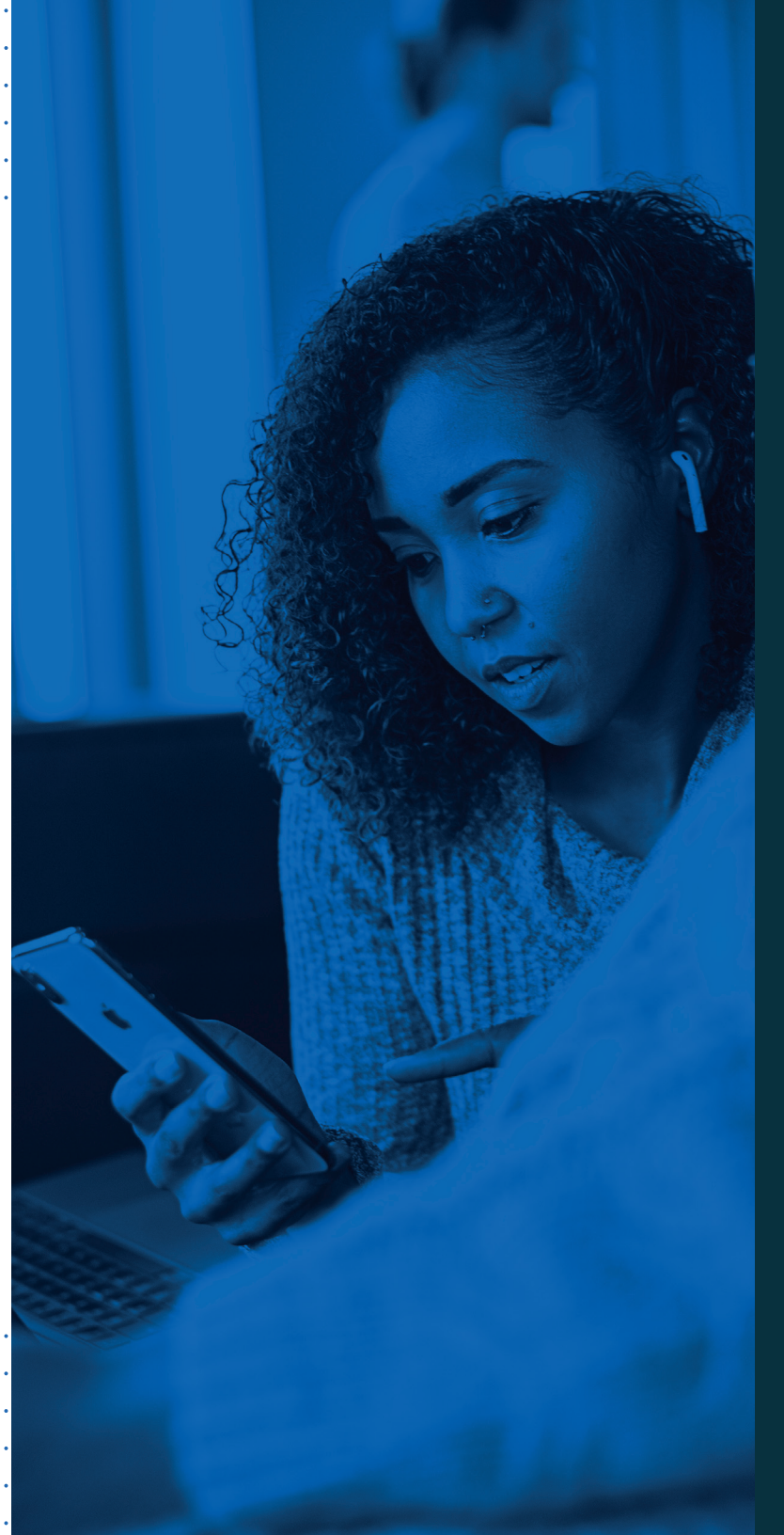
– Harry Potter und der Feuerkelch

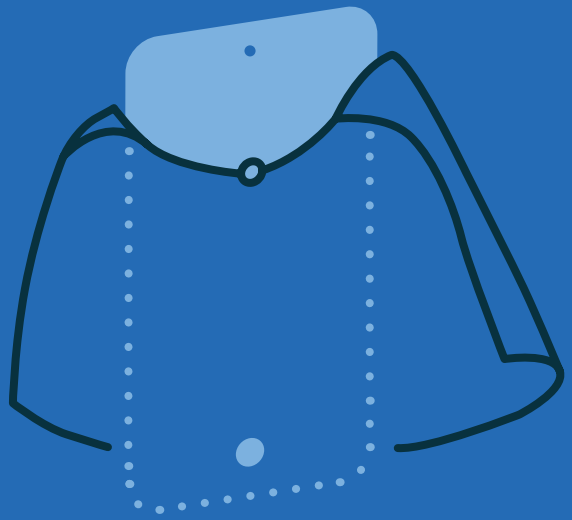
JEDES MOBILGERÄT, JEDES BESITZMODELL

BYOD. CYOD. COPE. Dieses Mischmasch aus Akronymen bezieht sich auf Mobilgerät-Programme, die auf unterschiedliche Weise unterstützt werden. Wenn es noch nicht schwierig genug wäre, sich für ein Besitzmodell zu entscheiden, dann macht die Vielfalt der verschiedenen Mobilgerätetypen, Anbieter und Netzwerkbetreiber alles noch komplizierter, oder?

Nicht für Jamf Data Policy, nein.

Die einzige Entscheidung, die Ihre Organisation treffen muss, ist die Wahl der am besten für das Unternehmen geeigneten Geräte. Unabhängig vom Gerätetyp, Besitzmodell oder Betriebssystem unterstützt Jamf den Großteil dieser Optionen. Dadurch kann sich die IT-Abteilung auf die Verwaltung der Mobilgeräte konzentrieren, mit Schwerpunkt auf der Sicherheit und den Compliance Richtlinien. Sie müssen sich nicht darüber Sorgen machen, schlecht zueinander passende Teile zu kombinieren, wie das in heterogenen Systemen oft der Fall ist.





DER TARNUMHANG

Aus der IT-Perspektive könnte ein Umhang, der einen unsichtbar macht, hilfreich sein, wenn zu viele Tickets gleichzeitig eingereicht werden. Stellen Sie sich sich vor, dass Sie den Kopf senken und sich ausschließlich auf die Lösung von Problemen konzentrieren, statt auf die endlosen E-Mails, Texte, Anrufe und „schnellen Fragen“ zu reagieren.

Wenn Ihnen das zusagt, gibt es einige Funktionen in Jamf Data Policy, die dabei helfen könnten, die Flutwelle an Anfragen durch die Standardisierung der Ressourcennutzung, der Durchsetzung der Compliance und der Kontrolle der Nutzererwartungen aufzuhalten.

UMFASSEND KONFIGURIERBAR

Keine zwei Netzwerke sind identisch, und keine zwei Organisationen werden ihre Infrastruktur ähnlich verwalten oder die gleichen Anforderungen für die Unternehmenskontinuität identifizieren. Größtenteils hängt das von der Risikobereitschaft der Organisation ab. Und so wie Großunternehmen den Sicherheitsstatus ändern, um das Risiko anzugehen, ermöglicht auch Jamf Data Policy eine vollständige Anpassung der Richtlinien und wie sie für die Verwaltung implementiert werden.

Von der Anpassung der Content-Filterkategorien bis zur Veränderung von Positiv- und Negativlisten, können Richtlinien ganzheitlich (die Organisation insgesamt betreffend) oder spezifisch angewendet werden, und zwar auf einen Benutzer – oder durch Gruppenmitgliedschaft – und die Entscheidungen sind flexibel und versuchen, die Anforderungen Ihrer Organisation zu erfüllen. Und am wichtigsten ist, dass Sie die Entscheidung treffen.

CONTENT-FILTER

Jamf entdeckte, dass Erotik-Apps und Glücksspiele wesentlich häufiger auf unverschlüsselte Verbindungen angewiesen sind, die Organisationen durch Datenlecks und Compliance-Verstöße gefährden können. Wenn wir über die oben genannten Kategorien hinausgehen, kann der Zugriff auf Inhalte, die Waffen, Hassrede oder andere Formen von Volksverhetzung enthalten, auch zivil- oder strafrechtliche Konsequenzen für Benutzer und/oder die Organisation haben.

Ganz abgesehen von Sicherheitsbedrohungen aus Web-Inhalten wie Phishing-Websites und anderen Formen von Malware, die überall im Internet auftauchen. Bei der Content-Filterung geht es nicht nur darum, schlechte Inhalte proaktiv fernzuhalten. Das kann auch lediglich die autorisierten Daten zulassen, indem es sicherstellt, dass akzeptable Websites, Services und Apps erreichbar sind.

Darüber hinaus ist es wichtig, das juristische Risiko zu reduzieren, indem Sie eine den Vorschriften entsprechende Datennutzung verwalten und den Zugriff auf nicht genehmigte Services überwachen und blockieren. Services wie Schatten-IT können den Sicherheitsstatus Ihrer Geräte und Ihres Netzwerks untergraben, indem sie versehentlich vertrauliche Firmendaten enthüllen.

DER STEIN DER WEISEN

Dieser Abschnitt bespricht leider nicht die Formel für das Elixier des Lebens, oder wie man unedle Metalle in Gold verwandeln kann. Stattdessen wird er das nächstbeste Thema diskutieren: zwei weitere Funktionen in Jamf Data Policy, die auf ihre Weise auch magisch sind, indem sie Echtzeit-Erkenntnisse sammeln, was es IT-Administratoren ermöglicht, Daten in umsetzbare Aufgaben zu verwandeln, um Ihre Geräte besser anzupassen und zu verwalten.

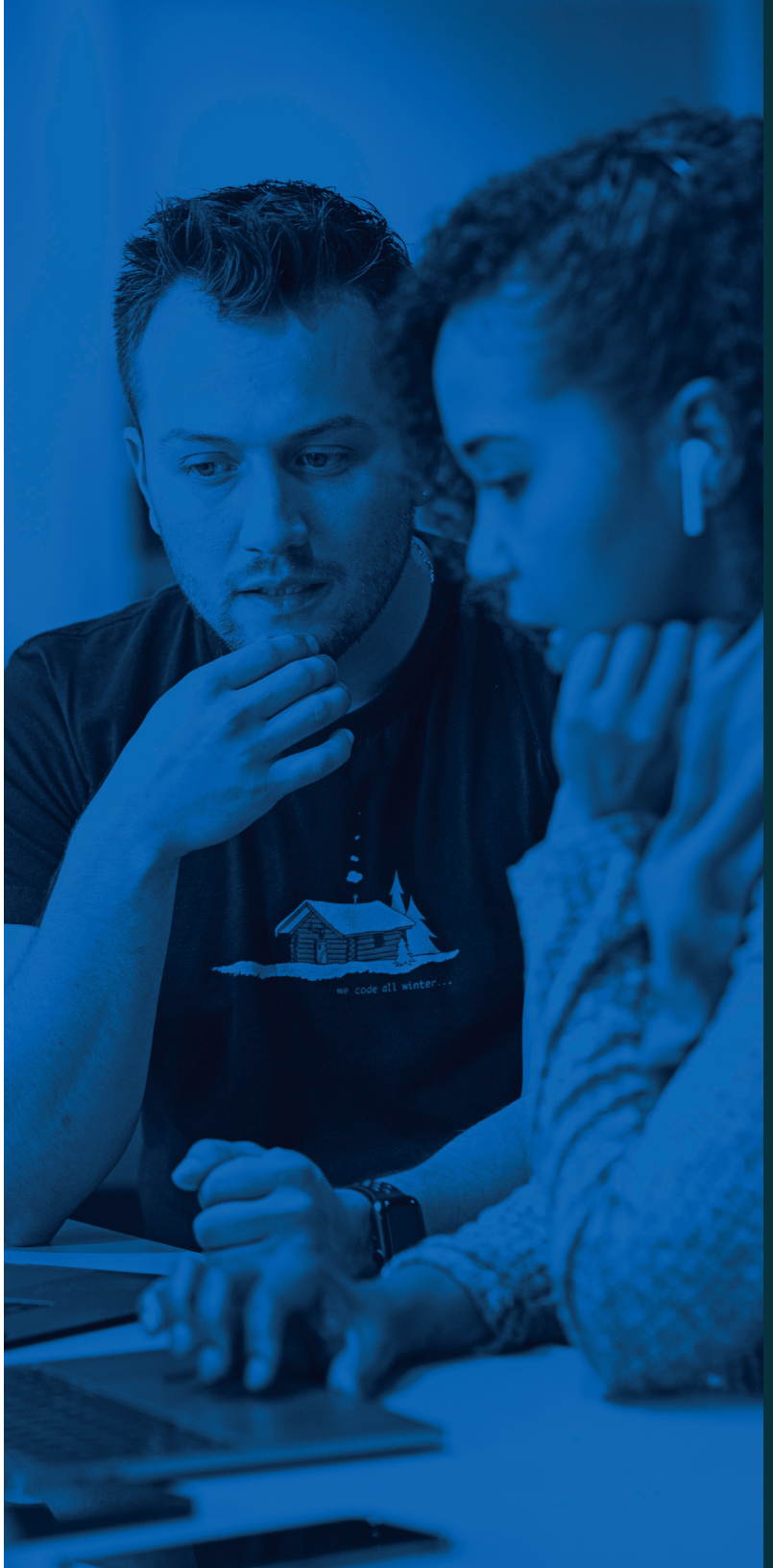
Darüber hinaus machen diese Funktionen die Schutzmaßnahmen netzwerkbewusst. Das bedeutet, dass Ihre Geräte und Benutzer über alle Arten von Netzwerkverbindungen hinweg geschützt und konform bleiben, egal, ob neue Sitzungen eröffnet oder existierende Verbindungen unterbrochen werden.

FÜR ALLE NETZWERKE

Wie erwähnt reicht dabei eine Einheitslösung definitiv nicht. Nichts passt besser zu diesem Konzept als die Netzwerkverbindungen auf Ihrem Mobilgerät. Wenn Benutzer beispielsweise gemessene Mobilfunkverbindungen verwenden müssen, sind sie sich oft mehr der Nutzungsgrenzen bewusst, da Roaming- oder Überschussgebühren zu zahlen sind. Aber wenn sie sich mit einem WLAN-Hotspot verbinden können, dürften sie wohl keine Bedenken bezüglich der Bandbreite haben.

Jamf Data Policy löst diese Probleme, indem es Administratoren ermöglicht, Richtlinien für verschiedene Netzwerk-Verbindungstypen und ihre speziellen Variablen zu erstellen und durchzusetzen.

Nehmen wir beispielsweise an, dass Ihre Organisation das COPE-Modell (Corporate-Owned, Personally Enabled) unterstützt und den Mitarbeitern Mobilgeräte für die Arbeit und die persönliche Nutzung zur Verfügung stellt, dass aber der Mobilfunkplan ein Teil des Datenpools ist, den alle Benutzer teilen. Ihre Organisation könnte die genutzte Bandbreite einschränken, damit es über Mobilfunk genug Daten für alle gibt, ohne Bandbreitenbeschränkungen auf WLAN einzusetzen. Jamf Data Policy ermöglicht es, Richtlinien genau dafür zu implementieren – um die Bandbreite auf Mobilfunk, aber nicht auf WLAN zu begrenzen. Darüber hinaus sind die Richtlinien intelligent genug, um zu erkennen, welche Verbindung momentan verwendet wird und sich automatisch anzupassen, ohne dass die IT-Abteilung aktiv werden muss oder die Benutzererfahrung beeinträchtigt wird.



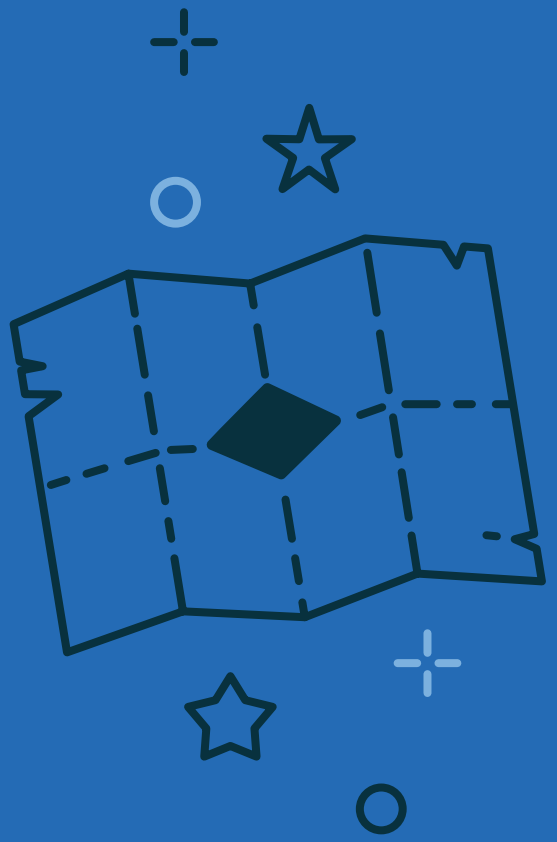
EINBLICKE IN ECHTZEIT

„Ich schwöre feierlich, ich bin ein Tunichtgut.“ *– Harry Potter*

Fragen Sie Administratoren, ob sie lieber vorher wissen möchten, dass etwas ausfallen wird (proaktiv) oder danach (reaktiv). Höchstwahrscheinlich werden alle die gleiche Antwort geben – sie wollen das vorher wissen.

Wenn man die Wahl hat, würden alle lieber vorher gewarnt werden. Selbst wenn man das Ereignis nicht verhindern kann, würde man es dann wenigstens möglichst schnell abmildern.

Hurra! Die Echtzeit-Erkenntnisse von Jamf Data Policy bieten genau das: eine Vorwarnung durch detaillierte Berichte, welche der IT-Abteilung zeigen, wie Geräte Daten über welche Verbindungen benutzen. Administratoren können Richtlinien proaktiv ändern, die mehr (oder weniger) streng sein müssen. Sie können Änderungen an existierenden Datenpools vornehmen, Content-Filterung konfigurieren, um den Zugriff auf Apps und Services zu aktivieren oder zu deaktivieren, oder einfach nur den Sicherheitsstatus eines Geräts im Auge behalten.



ABFAHRT AUF BAHNSTEIG 9¾

Wenn Sie Ihre firmeneigenen Mobilgeräte oder die persönlichen Geräte der Benutzer bei Jamf Pro registrieren, ist das eine hervorragende Grundlage für die Geräteverwaltung. Aber in heutigen modernen Arbeitsumgebungen, die sich um Hybrid- oder Telearbeit zentrieren, erfordert die Verwaltung des Geräts ein sehr spezialisiertes Tool.

Jamf Data Policy ist dieses Tool:

- Verwalten Sie durch intelligente und netzwerkbewusste Richtlinien, wie Daten auf dem Gerät gesendet und empfangen werden.
- Compliance-Regeln werden über jede Netzwerkverbindung eingehalten.
- Filtern sie Inhalte mit siebzig intelligenten Vorlagen aus, um zu verhindern, dass Geräte sich mit verwundbaren, kompromittierten oder bösartigen Websites, Apps und Services oder nicht zugelassenen Inhalten verbinden.

Schließlich vereinfacht Jamf Data Policy die Aufgabe der IT-Abteilung, indem es Schatten-IT eliminiert und Nutzungsrichtlinien für alle Geräte durchsetzt – unabhängig vom Besitzerstatus – um nicht nur Daten zu schützen, sondern auch Geräte und Benutzer, ohne dabei das Erlebnis der Beteiligten zu beeinträchtigen.

Testversion anfordern

Beginnen Sie noch heute mit einer Testversion oder kontaktieren Sie Ihren Apple Partner.