jamf

Außergewöhnliche Anwendererfahrungen für Apple Geräte in einem PC-dominierten Unternehmen

Einführung

Erfahrung bedeutet Produktivität.

Die Übertragung der Apple Nutzererfahrung auf IT-Abläufe minimiert operative Widerstände und optimiert damit die Produktivität sowie den ROI des Unternehmens.

Dieser Leitfaden ist der zweiteTeil der Serie „Warum Jamf“, die IT-Führungskräfte und Administratoren aller Kompetenzstufen mit den nötigen Informationen versorgt, um sicherzustellen, dass bestehende Investitionen in Identität, Sicherheit, Automatisierung und Beobachtbarkeit die Mitarbeiter dabei unterstützen, produktiv zu bleiben, Herausforderungen zu meistern und Blockaden effektiv zu reduzieren.

Kurze Zusammenfassung

Die Produktivität sinkt, wenn die Bereitstellung der Geräte, die Zugriffsverwaltung, Software-Updates und die Abwehr von Bedrohungen auf manuellen Prozessen beruhen. In diesem Leitfaden wird erläutert, wie die Integration von Geräteverwaltung, Identität und Sicherheit den IT-Betrieb rationalisiert und gleichzeitig die Benutzerfreundlichkeit verbessert. Mit Zero-Touch-Bereitstellung, rollenbasierten Zugriffskontrollen und automatisiertem App-Lifecycle-Management beschleunigt Jamf den Onboarding-Prozess und sorgt für sichere und konforme Geräte. Self Service+ ermöglicht es den Mitarbeitern, genehmigte Apps zu installieren und allgemeinegängige Probleme bei Bedarf selbst zu lösen, wodurch die Anzahl der Helpdesk-Tickets reduziert wird, während die Richtliniendurchsetzung gewahrt bleibt. Das Ergebnis ist ein skalierbarer Workflow, der die Sicherheit erhöht, die Verwaltung vereinfacht und es den Mitarbeitern ermöglicht, vom ersten Tag an produktiv zu sein.

Produktivitätsprobleme, die Jamf löst

Ein nahtloser Onboarding-Prozess der neuen Mitarbeiter mit Geräten, die sofort nach dem Auspacken einsatzbereit sind

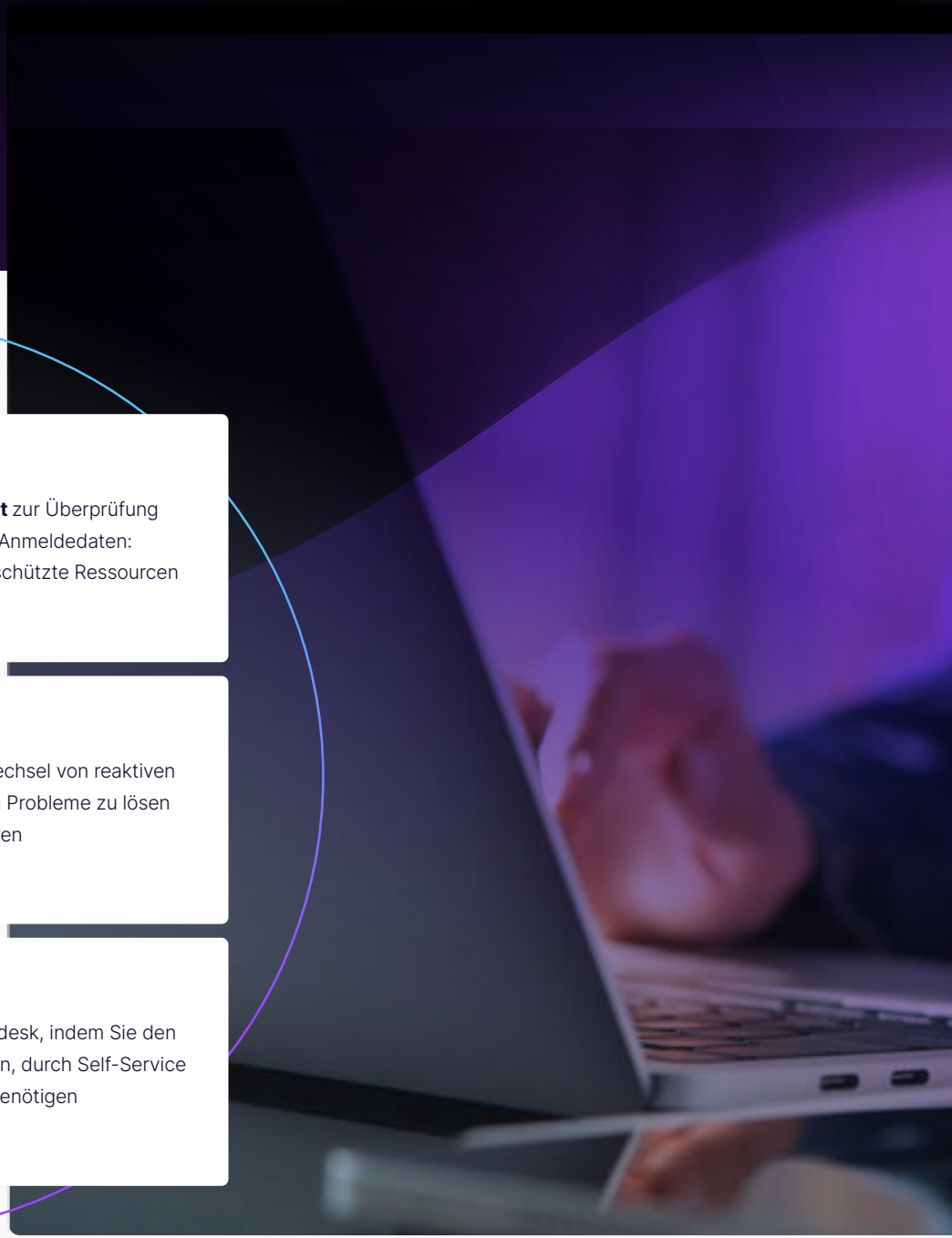
Implementierung von **Zero Trust** zur Überprüfung des Zustands von Geräten und Anmeldedaten: Reduzierung des Risikos für geschützte Ressourcen

Nutzung sicherer Basiskonfigurationen und rollenspezifischer Optimierungen ab der ersten Anmeldung

Transparenz **in Echtzeit** und Wechsel von reaktiven zu einem proaktiven Ansatz, um Probleme zu lösen und nicht auf Vorfälle zu reagieren

Automatische **Aktualisierungen der Software**: Minimierung der Ausfallzeiten und Maximierung der Konformität

Weniger Aufwand für den Helpdesk, indem Sie den Benutzern die Möglichkeit geben, durch Self-Service Hilfe zu erhalten, wenn sie sie benötigen



Nahtloses Onboarding, Produktivität von null auf hundert

Für die IT sieht ein typischer manueller Bereitstellungsprozess etwa so aus:

1. **Beschaffung der Hardware**
2. **Auspacken jedes Geräts**
3. **Zentrale Bereitstellung der Geräte**
4. **Ersteinrichtung**
5. **Installation:**
   - Betriebssystem-Updates
   - Apps
   - Endpunktsicherheit
6. **Konfiguration:**
   - Hardware-Einstellungen
   - Software-Einstellungen
   - Sichere Baselines
7. **Check: Werden die Endpunkte überwacht?**
8. **Zuweisung zu einem Endbenutzer**
9. **Check: Kann sich der Endbenutzer authentifizieren?**
10. **Check: Hat der Endbenutzer Zugang zu den erforderlichen Tools?**

In der Theorie mögen zehn Schritte als viel Arbeit erscheinen, um ein Gerät für einen neuen Mitarbeiter vorzubereiten. In der Praxis schrecken viele Unternehmen, die mehr als 1.000 Geräte verwalten, verständlicherweise davor zurück, auch nur zehn Geräte auf diese Weise manuell zu einzurichten, da dies Auswirkungen auf Zeit, Produktivität und Budget hat.

Abhängig von Ihren individuellen Anforderungen können allein die Schritte 5-6 mehrere Stunden pro Gerät in Anspruch nehmen. Das bedeutet, dass etwas so Einfaches wie das Aufspielen von Betriebssystem- und Software-Patches, die Installation einer Produktivitätssuite und die Konfiguration von Software-Einstellungen für die Konformität leicht einen halben Tag in Anspruch nehmen kann - mit all den Starts und Stopps für Neustarts und der Zeit, die damit verbracht wird, darauf zu warten, dass der Vorgang abgeschlossen wird.

Wie kann man diese Verschwendung der Ressourcen vermeiden?

Eine Onboarding-Strategie, die Verwaltung, Identität und Sicherheit als Grundgerüst integriert, um den Einrichtungsprozess basierend auf der Rolle des Endbenutzers mittels Zero-Touch-Bereitstellung zu automatisieren. Dies verkürzt nicht nur die Wartezeit neuer Mitarbeiter auf einsatzbereite Hardware von Stunden auf Minuten, sondern reduziert auch erheblich die Zeitspanne bis zur vollen Produktivität.

Das bedeutet:

- **Keine Wartezeiten beim Onboarding**, weil die IT-Abteilung keine Unterstützung leisten muss.
- Die Mitarbeiter müssen ihr Gerät nicht im Büro abholen.
- Menschliche Fehler oder Ermüdung durch sich Routineaufgaben sind ausgeschlossen.
- Die Mitarbeiter könne vom ersten Tag an produktiv arbeiten und einen aktiven Beitrag leisten.
- Mit effizienten Arbeitsabläufen sparen Unternehmen Zeit und Geld - und verschwenden sie nicht.

Warum Jamf?

Jamf bietet flexible, leistungsfähige Workflows, die die IT-Ressourcen entlasten, indem sie die Bearbeitungszeit für Support-Tickets während der Onboarding-Phase verkürzen. Durch die Automatisierung standardisierter Aufgaben zur Einrichtung schafft die IT bessere, unterstützende Arbeitsabläufe für Endbenutzer, damit diese ihre Geräte selbst registrieren und über den Self Service auf die Software, Tools und Konfigurationen zugreifen können, die sie benötigen, und zwar dann, wenn sie diese benötigen.

Zugriffsrichtlinien, die Daten schützen, ohne die Menschen zu behindern

Ein Eckpfeiler der Datensicherheit sind Zugriffskontrolllisten (Access Control Lists, ACL) bzw. die Berechtigungen, die einem Benutzerkonto für eine geschützte Ressource gewährt (oder verweigert) wurden. Während es üblich ist, bei der Festlegung von IT-Support-Verhältnissen die Anzahl der Geräte zu berücksichtigen, verschiebt sich der Fokus beim Thema Identität auf die Anzahl der von der IT unterstützten Benutzer, um die Datensicherheit strategisch zu planen.

Bei der manuellen Konfiguration sind vor allem die erforderlichen Berechtigungen multipliziert mit der Gesamtzahl der Endbenutzer zu berücksichtigen. Mit zunehmender Mitarbeiterzahl steigt auch die Zahl der Berechtigungen, die die IT-Abteilung manuell bearbeiten muss. Dies beeinträchtigt die Leistung massiv, führt zu erheblichen Verzögerungen und erhöht die Wahrscheinlichkeit, dass Risiken durch menschliches Versagen und Ermüdung durch sich wiederholende Prozesse entstehen. Da die IT-Abteilung Änderungen manuell verarbeiten muss, sind bei jeder Änderung - wie etwa ein Rollenwechsel oder einer Änderung der Risikotoleranz - Änderungen pro Account und oft auch pro Gerät erforderlich, was die Skalierbarkeit dieser Methode erschwert.

Wie sieht eine optimale, skalierbare Lösung aus?

Die Integration einer Identitäts- und Zugriffsverwaltung (IAM) mit der Geräteverwaltung und der Endpunktsicherheit bietet die größte Anpassungsfähigkeit an die Bedürfnisse des Unternehmens. Außerdem verlagert es die manuelle Arbeit von Änderungen pro Account/pro Gerät auf ein zentralisiertes Sicherheitsmodell, das die rollenbasierte Zugriffskontrolle (RBAC) nutzt, um den Zugriff der Benutzer auf gesicherte Ressourcen über ihre Rolle zu definieren, anstatt über ihre individuelle Identität und/oder jedes einzelne Gerät, das sie für ihre Arbeit verwenden.

Das bedeutet:

- Die **Zuweisung von Berechtigungen** wird auf der Grundlage von Rollen und Gruppenmitgliedschaften in einem zentralen Repository verwaltet.
- Es gilt das Prinzip des geringsten Privilegs, das **den Zugriff** auf das Notwendige beschränkt.
- Die Zugriffsrechte gelten, sobald sich der **Benutzer authentifiziert**, danach auf jedem Gerät und bei Rollenänderungen.
- **Geringerer Verwaltungsaufwand**, auch bei umfangreicheren Änderungen, da die IT-Abteilung die Änderung nur einmal bearbeiten muss.
- Das Auditieren von Kontrollmechanismen wird durch zentrale Transparenz und die Protokollierung der Richtlinieneinhaltung erheblich **erleichtert**.

Warum Jamf?

Native Unterstützung für Cloudidentitätsanbieter (IdP) bedeutet, dass die gleichen zentralisierten identitätsbasierten Sicherheitskontrollen, die für Anmeldedaten und Endpunkte gelten, auch für Ihre Jamf-Instanz gelten. Jamf baut auf der Identitätsintegration auf, um ein nahtloses Benutzererlebnis zu bieten, wendet aber IAM-Strategien auf Unternehmensressourcen an und unterstützt neben Windows-PCs auch Mac- und mobile Geräte - für ein einheitliches Identitätsparadigma, das sowohl anpassbar als auch skalierbar ist.

Strukturiertes App-Lebenszyklusmanagement

Einer der wichtigsten Faktoren für die Benutzererfahrung sind die Softwarelösungen, die zur Erledigung der Arbeit eingesetzt werden. Diese Faktoren müssen berücksichtigt werden:

- **Anforderungen des Unternehmens**
- **Präferenzen der Benutzer**
- **Mehrere Betriebssysteme**
- **Verschiedene Gerätetypen**

Das bedeutet, dass der Weg zur Konformität nicht gerade einfach ist. Die Unterstützung von nativen Apps, internem Code und/oder in der Cloud gehosteter Software ist ein weiterer Stolperstein auf diesem Weg.

Die Patch-Verwaltung für mehrere Betriebssysteme, einschließlich Sicherheitsversionen und App-Updates, kann sich leicht von einer Aufgabe, die nur wenige Minuten dauert, zu einem stunden- oder tagelangen Projekt ausweiten, wenn Umfang und Komplexität den IT-Teams über den Kopf wachsen.

Die manuelle Aktualisierung von Apps oder die flottenweite Aktualisierung eines Betriebssystems - selbst bei einem geringen Verhältnis von IT zu Geräten - führt dazu, dass Endbenutzer nicht mehr arbeiten können und Unternehmen Risiken ausgesetzt sind, die von einer Vielzahl von Vektoren herrühren, z. B:

- **Ungepatchte Schwachstellen** aufgrund von fehlenden Updates
- **Fehlerhafte Software** aufgrund unvollständiger oder nur teilweiser Updates
- **Schwächung des Sicherheitsstatus** durch unzusammenhängende Patch-Bereitstellungen
- **Nicht genehmigte oder nicht autorisierte** App-Nutzung (Schatten-IT)
- **Gefährdete** App-Integrität oder unsichere App-Installationen

Welche Lösung harmonisiert das Lebenszyklusmanagement von Apps?

Eine Strategie, die Apps zentralisiert und nativ bereitstellt und gleichzeitig die Sichtbarkeit der Endgeräte, die Durchsetzung von Richtlinien und die Automatisierung von Software-Updates integriert, sobald diese verfügbar sind, stellt sicher, dass die Geräte auf dem neuesten Stand bleiben und dass bekannte Schwachstellen, die die Daten des Unternehmens gefährden könnten, in der gesamten Infrastruktur gleichwertig beseitigt werden - unabhängig von Betriebssystem oder Gerätetyp.

Das bedeutet:

Inventarinformationen werden **in Echtzeit aktualisiert** und bieten einen Überblick darüber, welche Apps und welche Versionen auf den verwalteten Geräten installiert sind.

Die Apps **stammen von seriösen Entwicklern**, deren Authentifizierung und Integrität durch digitale Signaturen überprüft wird.

Die Software wird nativ installiert und **automatisch aktualisiert**, was den IT-Aufwand reduziert, weil der Lebenszyklen der verwalteten Apps optimiert werden.

Die **Konformität** wird über Richtlinien durchgesetzt, die sicherstellen, dass die verwalteten Apps auf allen unterstützten Geräten verfügbar und gleich konfiguriert sind.

Die Prüfpfade werden **vereinfacht**. Dank der einheitlichen Protokollierung lässt sich die Einhaltung von Vorschriften nachweisen und den Prüfern leicht zur Verfügung stellen.

Warum Jamf?

Um erfolgreich zu sein, müssen die Strategien zur Patch-Verwaltung sicher, effektiv, skalierbar und konsistent sein. Mit den Jamf App-Installationsprogrammen werden alle diese Anforderungen erfüllt und durch Automatisierung ergänzt, um die Vorschriften einzuhalten und bei der Bereitstellung von Drittanbietersoftware sichere Endpunkt-Baselines zu gewährleisten. Dies lässt sich mit leistungsstarken und zugleich flexiblen Richtlinien kombinieren, die Benchmarks nutzen, um Betriebssystem- und Systemsicherheitspatches auf dem neuesten Stand zu halten. So wird ein erstklassiger Sicherheitsstatus der Geräte gewährleistet, der im Einklang mit der allgemeinen Sicherheitsstrategie des Unternehmens steht.

Abwehr von Bedrohungen, bevor sie den Benutzer erreichen

Nichts bringt die Produktivität schneller zum Erliegen als eine bösartige Bedrohung, die den Zugriff auf Daten verhindert, die Konnektivität auf ein unbrauchbares Niveau verlangsamt oder die Integrität von Unternehmensdaten gefährdet - oder alles zusammen.

Die drei vorangegangenen Abschnitte befassen sich mit der Bereitstellung von Geräten, Zugriffsrechten und der Verwaltung des Lebenszyklus von Apps. In diesem Abschnitt werden Bedrohungsabwehr und Prävention als wesentliche Faktoren hervorgehoben, um die Produktivität der Mitarbeiter angesichts moderner Bedrohungen aufrechtzuerhalten. Insbesondere hochentwickelte Bedrohungen, die sich auf unterschiedliche Mobilgeräte, unterschiedliche Plattformen und die Abhängigkeit moderner Unternehmen von cloudbasierten Diensten stützen, um Endbenutzer im Büro und im Home-Office anzugreifen.

Eine effektive Reaktion auf Vorfälle ist zwar entscheidend, um zu verhindern, dass sich bestehende Bedrohungen zu etwas viel Schlimmerem ausweiten. Doch in der Realität sieht es so aus, dass zu dem Zeitpunkt, an dem ein Endpunkt kompromittiert wird, die Auswirkungen für den Endbenutzer bereits spürbar sind. Darüber hinaus erfordert die Behebung des Problems einen größeren Aufwand und führt zu Betriebsunterbrechungen, was die Auswirkungen durch zusätzliche Verzögerungen weiter verschärft. **Dies führt zu:**

- Ein **Verlust** an **Produktivität**,
- Dies führt zu verlängerten **Ausfallzeiten**,
- Das **wirkt sich** teamübergreifend negativ aus,
- Hat **negative** Auswirkungen auf den Unternehmensbetrieb,
- Dies führt zu einer **Gewinnminderung**,
- **Schwindendes** Vertrauen der Kunden,
- Und es entstehen höhere **Kosten für** die Behebung.

Welche Lösung hilft der IT, den Bedrohungen einen Schritt voraus zu sein?

Um eine Bedrohung wirksam zu stoppen, muss die IT-Abteilung sie zunächst identifizieren können. Ganz gleich, ob es sich um eine nicht richtlinienkonforme App oder eine vom Benutzer deaktivierte Einstellung handelt – der Schlüssel zur Vermeidung von Risiken für Unternehmensdaten liegt darin, die Bedrohung von vornherein zu verhindern.

Das bedeutet:

- **Aktive Überwachung** kontextbezogener Telemetriedaten, einschließlich des Zustands der Endgeräte
- Umfassender Überblick über die Risikomatrizen der Endpunkte zur Bewertung**und Priorisierung des Schweregrads von Bedrohungen**
- **Die Transparenz über Geräte**, die auf gesicherte Ressourcen zugreifen, ist von entscheidender Bedeutung – für verwaltete und nicht verwaltete Geräte gleichermaßen.
- **Integration von**Lösungen zur Schaffung einer nahtlosen Strategie zur Geräteverwaltung, Identität und Endpunktsicherheit
- **Nutzung von** Technologien des **maschinellen Lernens (ML), um die Identifizierung und Behebung unbekannter Bedrohungen zu verbessern und effizient zu skalieren**

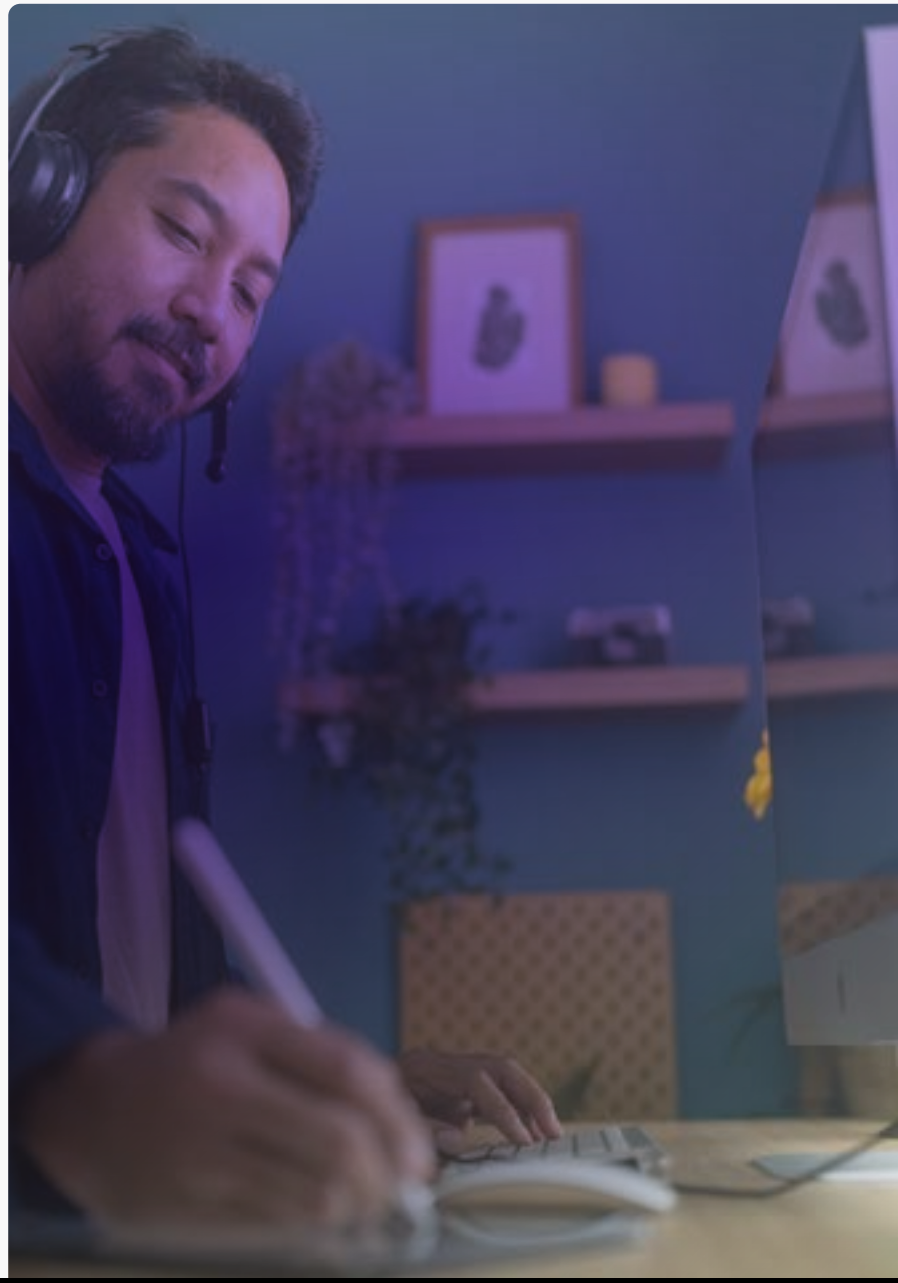
Warum Jamf?

Jamf überprüft die Konformität der Endgeräte mithilfe mehrerer Schutzebenen. Durch Echtzeitüberwachung wird der Zustand des Geräts kontrolliert. Die Ergebnisse werden protokolliert und der IT-Abteilung gemeldet, um eine Gefährdung der Unternehmensressourcen zu verhindern. Diese Daten werden genutzt, um Risiken zu beseitigen, indem das Gerät automatisch wieder in einen richtlinienkonformen Zustand versetzt wird – so wird das Problem für den Endbenutzer unsichtbar und ohne Eingreifen der IT gelöst.

Keine Ausfallzeiten: Mitarbeiter bleiben produktive und der Umsatz ist gesichert

Faktoren wie:

- **Plattformübergreifende Unterstützung**
- **Desktop und mobile Geräte**
- **Hybride Cloud-Technologien**
- **Verteilte Belegschaften**
- **Eigentumsmodelle**



stellen Herausforderungen für umfassende Managementstrategien dar. Von der Aufrechterhaltung der Produktivität hybrider Teams über die nahtlose Integration von Lösungen verschiedener Anbieter bis hin zur ganzheitlichen Ausweitung der Sicherheit auf die gesamte Infrastruktur – die Unternehmens-IT muss viele Komplexitätsfaktoren berücksichtigen, um den Geschäftsbetrieb auf Erfolgskurs zu halten.

Moderne Unternehmen, die auf globaler Ebene tätig sind, sind facettenreich wie ein Oktopus. Jeder Arm steht für ein strategisches Vorhaben, das Teil des Ganzen ist, das als digitale Transformation bezeichnet wird.

Vorbei sind die Zeiten, in denen eine Firewall, ein Virenschutz, eine lokale Domain und eine VPN-Verbindung ausreichten, um den Datenverkehr innerhalb der sicheren Mauern des Netzwerks zu schützen. Heutzutage erfordert jeder dieser „Arme“ oder spezifischen Bereiche dynamische, flexible Lösungen zur effektiven Verwaltung und Absicherung, und zwar von jedem Gerät aus, mit jedem Betriebssystem und von jedem Ort der Welt aus. Gleichzeitig muss dem Benutzer genau der Komfort, Zugriff und Schutz geboten werden, den er erwartet und benötigt, um Endgeräte, Unternehmensressourcen und die Privatsphäre der Benutzer zu schützen.

Welche Lösung sichert die geschützten Ressourcen dynamisch und plattformübergreifend?

Ältere Lösungen weisen Sicherheitslücken auf, die das Risiko von Datenverletzungen mit sich bringen. Unternehmen benötigen heute adaptive Technologien, die auf Zero-Trust-Architekturen basieren, um IAM, Geräteverwaltung und Endpunktsicherheit zu nutzen und eine umfassende Lösung bereitzustellen, die nicht nur moderne Bedrohungen und Angriffe abwehrt, sondern auch dafür sorgt, dass die Konformität sichergestellt wird.

Das bedeutet:

- Wechsel von einem impliziten Vertrauensmodell zu einem Modell, bei dem **der Zugang standardmäßig verweigert wird** - niemals vertrauen, immer überprüfen
- Explizite **Überprüfung der Anmeldedaten** und des **Zustands des Geräts** jedes Mal, bevor eine Zugriffsanfrage genehmigt wird
- Hinzufügen einer Ebene **kontextbezogener Intelligenz**, um hochentwickelte Bedrohungen mittels Verhaltensanalysen zu bekämpfen
- Implementierung **netzwerkinterner Schutzmaßnahmen**, die den Datenverkehr in einzelnen Mikrotunneln isolieren und so Abhörversuche und Seitwärtsbewegungen verhindern
- **Beschleunigte** Reaktion auf Vorfälle und automatisierte Workflows zur Behebung von Problemen, um Ausfallzeiten zu reduzieren.

Warum Jamf?

Mit Zero-Trust-Netzwerkzugriff (ZTNA) von Jamf wird moderner Bedrohungsschutz auf alle unterstützten Gerätetypen ausgeweitet. Dies bietet eine plattformübergreifende Unterstützung mit Funktionsparität, um Sicherheitsstrategien über gesamte Geräteflotten hinweg zu optimieren – unabhängig von deren Standort oder der verwendeten Netzwerkverbindung. Durch die Integration von mehrschichtigen Schutzmechanismen erhalten Endbenutzer nativen Zugriff auf Unternehmensressourcen, während die IT-Teams von einer besseren Abstimmung zwischen Geschäftsabläufen und Konformitätsanforderungen profitieren.

Weniger Helpdesk-Tickets und mehr Produktivität der Benutzer

Eine Kernaufgabe der IT besteht darin, die Anforderungen der Benutzer zu unterstützen. In den meisten Unternehmen übersteigt die Zahl der Mitarbeiter bei weitem die Zahl der IT-Fachleute im Unternehmen. Aus diesem Grund wird die Fähigkeit der IT-Abteilung, auf Probleme zeitnah, effizient und erfolgreich zu reagieren und sie zu lösen, durch Faktoren wie diese erheblich beeinträchtigt:

- **Durchschnittliche Bearbeitungszeit von Tickets**
- **Effizienz der Arbeitsabläufe**
- **Größe des IT-Teams**
- **Unternehmensweite Kultur**
- **Kenntnisse der Teammitglieder**

Jede potenzielle Unzulänglichkeit bei einem oder mehreren dieser Faktoren wird durch eine mangelnde Abstimmung zwischen ihnen noch verstärkt. Dies führt zu einer Verringerung der Effizienz betrieblicher Abläufe, was mangelnde Kontinuität bei der Verfolgung der Geschäftsziele zur Folge hat.

Dies sind zwar langfristige Auswirkungen, doch die Betroffenen spüren die unmittelbaren Folgen in Form von Verzögerungen bei der Erledigung arbeitsbezogener Aufgaben:

- Software **nicht installiert**
- **Unkonfigurierte** Einstellungen
- **Falsche** Berechtigungen
- **Fehlermeldungen** des Systems
- **Hardware-Inkompatibilitäten**

Mit welcher Lösung wird die IT zum Motor für gesteigerte Produktivität?

Erfahrungsgemäß lassen sich Defizite in der Benutzererfahrung nicht durch eine bloße Erweiterung der Zugriffsrechte beheben. Bei dem Versuch, ein Problem zu „lösen“, erhöht die IT das Risikoprofil und damit die Gefahr von Beeinträchtigungen der Datenintegrität sowie die Häufigkeit von Sicherheitsvorfällen.

Durch die Einrichtung einer zentralen Wissensbasis, die es auch technisch nicht versierten Beteiligten ermöglicht, Probleme eigenständig zu beheben, erhalten die Benutzer schnell Hilfe. Gleichzeitig gewinnt die IT wertvolle Kapazitäten zurück, um durch die Optimierung von Arbeitsprozessen die Produktivität zu steigern und die IT-Strategie konsequenter mit den übergeordneten Geschäftszielen zu harmonisieren.

Das bedeutet:

- Einbeziehung der **Betroffenen als Teil der Lösung** - nicht als Problem, das es abzuwehren gilt
- Endbenutzer können **zugelassene Apps installieren** und **sanktionierte Einstellungen konfigurieren**, ohne die Berechtigungsstandards zu ändern.
- Automatisierte **Aktualisierungen der Apps** über ein benutzerfreundliches Portal, das die Updates mit einem einzigen Mausklick durchführt
- Die Verknüpfung des unternehmenseigenen App-Portals mit **cloudbasierten IdPs,** um die Benutzer dort abzuholen, wo sie sind
- Bereitstellung eines **nativen Portals,** das auf die Erfahrung des Benutzers abgestimmt ist und auch Benachrichtigungen über App-Updates bereitstellt

Warum Jamf?

Self-Service+ für Mac, iPhone und iPad stellt ein Apple-eigenes, durch das Unternehmen verwaltete Portal zur Verfügung, das so angepasst ist, dass Apps, Tools, Skripte, Verbrauchsmaterialien wie Drucker und Updates nur einen Mausklick entfernt sind - ohne dass administrative Berechtigungen erforderlich sind. Durch die Integration mit dem IdP kann die IT-Abteilung problemlos Anfragen vorübergehend genehmigen, ohne dass die Konformität dauerhaft beeinträchtigt wird – dafür wird ein vollständiger Prüfpfad bereitgestellt.

Schlussfolgerung

Produktive Unternehmen beseitigen Reibungsverluste sowohl im IT-Betrieb als auch bei den Mitarbeitern. Durch die Vereinheitlichung von Geräteverwaltung, Identitäts- und Endpunktsicherheit können Unternehmen den Onboarding-Prozess automatisieren, konsistente Zugriffskontrollen durchsetzen, den Sicherheitsstatus der Apps aufrechterhalten und Bedrohungen abwehren, bevor sie die Arbeit stören. Jamf stellt diese Fähigkeiten durch Workflows bereit, die für die Skalierung über verschiedene Geräteflotten hinweg entwickelt wurden, während die Benutzer produktiv und sicher bleiben. Mit der Zero-Touch-Bereitstellung, dem proaktiven Schutz und dem Self Service, der die Mitarbeiter dabei unterstützt, allgemeine Probleme zu lösen, reduziert die IT-Abteilung den betrieblichen Aufwand und stärkt gleichzeitig die Konformität und Ausfallsicherheit. Das Ergebnis ist eine sichere, optimierte Umgebung, in der sich die Mitarbeiter vom ersten Tag an auf sinnvolle Aufgaben konzentrieren können.

Die wichtigsten Erkenntnisse

- **Beschleunigtes Onboarding großer Geräteflotten:** Die Zero-Touch-Bereitstellung ermöglicht die direkte Auslieferung vorkonfigurierter Geräte und ersetzt die manuelle Einrichtung
- **Skalierung des Zugriffs ohne Beeinträchtigung der Benutzergeschwindigkeit**: rollenbasierte Zugriffskontrolle passt Berechtigungen bei wachsenden Organisationen automatisch an die Identität an
- **Verwaltung des App-Status über Tausende Endpunkte hinweg:** automatische Patches und Updates halten die Software sicher, ohne die Arbeitsabläufe zu unterbrechen
- **Stoppen von Bedrohungen, bevor sie den Betrieb unterbrechen**: kontinuierliche Überwachung und Durchsetzung der Konformität reduzieren Ausfallzeiten bei einer verteilten Belegschaft
- **Benutzer unterstützen und die IT entlasten:** dank Self Service installieren Mitarbeiter genehmigte Apps selbst und lösen Standardprobleme selbständig, was das Ticketaufkommen reduziert
- **Plattform- und standortübergreifende konsistente Erlebnisse**: einheitliche Workflows sorgen dafür, dass Geräte sicher und produktiv bleiben, egal ob die Mitarbeiter im Büro oder an einem anderen Ort arbeiten.

Sind Sie bereit, dies in Aktion zu erleben?

Erleben Sie Jamf