

Evaluierung der Endpunktverwaltung:

Warum ältere Lösungen nicht
den modernen Anforderungen
entsprechen



Einführung

Die moderne Belegschaft ist mobil, arbeitet nicht mehr nur vom Büro aus und verlangt ein hohes Maß an Flexibilität.

Die Nutzung von Mobilgeräten ist mittlerweile unerlässlich für die Aufrechterhaltung des Geschäftsbetriebs, unabhängig davon, ob Ihre Mitarbeiter:innen aus der Ferne, hybrid oder im Büro arbeiten. Smartphones, Tablets und andere mobile Endpunkte sind in der gesamten Industrie unverzichtbare Werkzeuge, die Workflows optimieren, den Zugang zu Daten in Echtzeit ermöglichen und die Produktivität von praktisch überall aus steigern.

Mit der zunehmenden Verbreitung mobiler Geräte stellt sich nicht nur die Frage, ob diese Geräte ins Unternehmen gehören, sondern auch, ob die Organisationen in der Lage sind, sie effektiv zu verwalten und zu sichern.

Während sie sich in Branchen wie dem Gesundheitswesen, dem Finanzsektor, dem Bauwesen und dem Transportwesen zu unverzichtbaren Geschäftswerkzeugen entwickeln, bringt diese Evolution neue Komplexitäten mit sich: Die IT steht unter wachsendem Druck, eine fragmentierte Gerätelandschaft zu verwalten, die Konformität bei unterschiedlichen Eigentumsmodellen durchzusetzen und die Produktivität zu fördern, ohne dabei die Sicherheit oder die Privatsphäre der Benutzer zu gefährden – und das alles bei gleichzeitiger Ausrichtung von Mobiltechnologie und IT-Prozessen an den übergeordneten Geschäftszielen.

Dieses E-Book befasst sich mit dem kritischen Wandel in der Unternehmensverwaltung für mobile Geräte und Sicherheit und erklärt, warum ältere Tools oder der „One-Size-Fits-All“-Ansatz den Anforderungen moderner Unternehmen nicht mehr gerecht werden. Es stellt die Bedeutung skalierbarer, integrierter Lösungen dar, die moderne Workflows unterstützen, intuitiv zu bedienen sind und der IT die nötige Kontrolle und Transparenz geben, um mobile Flotten im Einklang mit strategischen Prioritäten zu halten.

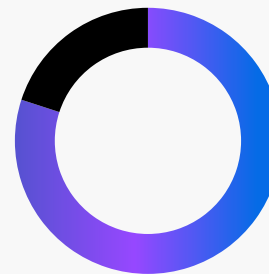
Wenn Ihre aktuellen Tools nicht für Mobil-first oder hybride Arbeitsumgebungen entwickelt wurden, hilft Ihnen dieser Leitfaden bei der Analyse, ob sie noch einen Mehrwert bieten können – oder ob es an der Zeit ist, Ihren Ansatz zu überdenken.

Arbeit ohne Grenzen

Unabhängig davon, ob Ihr Unternehmen komplett remote arbeitet oder eine Rückkehrpflicht ins Büro besteht – und ganz egal, wo man sich physisch befindet – die Allgegenwärtigkeit mobiler Geräte in unserem Privatleben ist unbestreitbar. Tatsächlich ist dieser Trend so stark, dass er die Schwelle zur professionellen Nutzung überschritten hat. Dank der Kombination aus Funktionsvielfalt, Leistung, Mobilität und Effizienz wurde das mobile Endgerät in vielen Branchen zum Werkzeug der Wahl und lässt die Grenzen zwischen privater und beruflicher Nutzung zunehmend verschwimmen.

Wie wichtig ist die Mobilität für die Geschäftskontinuität?

Laut dem [Verizon 2024 Mobile Security Index](#),



„sind 80 % der Befragten der Meinung, dass Mobilgeräte für das reibungslose Funktionieren ihrer Organisationen entscheidend sind.“

Da Mobilgeräte ein so entscheidendes Instrument für die Aufrechterhaltung des Geschäftsbetriebs sowie für die Bereitstellung von Produkten und Dienstleistungen Ihrer Branche sind, ist es für Unternehmen unerlässlich, mobile Endgeräte nicht nur zu verwalten und abzusichern. Sie müssen zudem eng an den Geschäftszielen ausgerichtet werden. Nur so bleibt die mobile Flotte konform, unterstützt die sich wandelnden Anforderungen des Unternehmens sowie der Benutzer vollumfänglich und ist gleichzeitig vor einer sich ständig verändernden Bedrohungslage geschützt.

Entwicklung der Rollen und der Art und Weise, wie die Aufgaben abgearbeitet werden

In den letzten Jahren haben viele Industrien auf Mobilgeräte gesetzt, um Geschäfte voranzutreiben und Wachstum auf neuartige Weise zu ermöglichen, was erst durch die zunehmende Nutzung mobiler Geräte möglich wurde. Beispiele für einige dieser Industrien, Rollen und die Art und Weise, wie sie von der Effizienzsteigerung durch die Einführung mobiler Geräte profitiert haben, sind:

Luftfahrt

Mobilgeräte optimieren die Flugzeugwartung, den Flugbetrieb und den Service für Passagiere, indem der **Zugang zu Daten und Kommunikation in Echtzeit ermöglicht wird** - vom Flugsteig bis zum Cockpit. Der Umstieg von konventionellen Flight Bags auf elektronische Lösungen ermöglicht es Piloten, massives Gewicht einzusparen: Statt rund 20 Kilogramm an Karten und Handbüchern tragen sie nur noch ein einziges iPad (ca. 2,3 kg) bei sich. Das optimiert nicht nur die Betriebsabläufe, sondern stellt auch die Einhaltung gesetzlicher Richtlinien sicher.

Bauwesen

Tablets und Smartphones verbessern die Zusammenarbeit, **reduzieren Verzögerungen und stärken die Projektübersicht** durch digitale Dokumentation sowie den Zugriff auf Projektmanagement-Tools – sowohl vor Ort als auch remote. iPads ermöglichen den Teams den Zugriff auf Baupläne, während Vorgesetzte Papierkram erledigen und Dokumente direkt vor Ort unterzeichnen können. Das Ergebnis: Kürzere Wartezeiten und eine lückenlose Kommunikation mit allen Projektbeteiligten und Lieferanten.

Finanzdienste

Smartphones steigern den Service für die Kunden, erhöhen die Produktivität und unterstützen die Konformität durch mehrere verschlüsselte Kommunikationsplattformen. Dadurch erhalten Finanzfachleute sicheren Zugang zu Kundendaten und können gleichzeitig die Marktaktivitäten jederzeit überwachen. Ganz ähnlich profitieren auch Broker von der Freiheit, Geschäfte von überall aus abzuschließen – sicher und direkt mit ihren verwalteten iPhones. So können sie ihren **Service perfekt an die spezifischen Anforderungen ihrer Klienten anpassen**.

Hotelgewerbe

Mit Smartphones und Tablets **heben Hotels den Gästeservice auf ein neues Level und gestalten abteilungsübergreifende Workflows effizienter**. Vernetzte mobile Lösungen ermöglichen es dem Team, individueller und zügiger auf Wünsche einzugehen. Und mithilfe von iPads im Kiosk-Modus können Gäste den Check-in selbst erledigen und so ohne Wartezeit direkt in ihren Urlaub starten. Darüber hinaus bieten verwaltete iPads in den Zimmern einen einfacheren Roomservice, während spezielle Apps detaillierte Informationen und Concierge-Support auf Knopfdruck zur Verfügung stellen.

Einzelhandel

Mobilgeräte bieten sowohl den Einzelhändlern als auch den Gästen Vorteile in Form von schnelleren Transaktionen, besserer Kundenbindung und **flexibleren Abläufen in physischen und digitalen Geschäften**. Durch die Umstellung von herkömmlichen Point-of-Sale-Systemen (PoS) auf mobile Systeme können die Verkäufer ihren Bestand problemlos verwalten und gleichzeitig die Kunden vor Ort betreuen, ohne von ihrer Seite zu weichen. Außerdem können sie alle benötigten Informationen auf einen Blick einsehen, einschließlich der Möglichkeit, Kundendaten zu aktualisieren und Zahlungen mit mobilen Checkout-Optionen abzuwickeln – alles von ihrem iPhone oder iPad aus.

Herausforderungen im Unternehmen

Der traditionelle Ansatz, mit einer einzigen Verwaltungslösung eine einheitliche Flotte von Geräten zu verwalten, entspricht nicht mehr der Realität der heutigen Unternehmenslandschaft, die zunehmend von unterwegs arbeitet. Angesichts eines breiten Mixes aus Gerätetypen, Eigentumsmodellen und Betriebssystemen wächst der Druck auf die IT: Sie muss in einer stark fragmentierten Landschaft sicherstellen, dass die Technologie mit den Unternehmenszielen im Einklang steht, die Konformität erfüllt wird und die Produktivität hoch bleibt. Da sich die Bedrohungslandschaft kontinuierlich weiterentwickelt und die Diversität der Endpunkte zunimmt, müssen Organisationen prüfen, ob ihre derzeitige Lösung den immer komplexer werdenden Anforderungen noch gerecht wird (oder sich an sie anpassen kann) und gleichzeitig einen Mehrwert für ihr Unternehmen bietet.

Eine Größe passt nicht allen

Früher verfolgte die IT den Ansatz, dass die Verwaltung eines einzigen Gerätetyps mit nur einem Betriebssystem im gesamten Unternehmen durch eine einzige Management-Lösung machbar sei. Unabhängig davon, ob die Aufgabe darin bestand, 100, 1000 oder Zehntausende von Geräten zu verwalten – es gab eine gewisse Logik, die der IT half, homogene Endpunkte zu verwalten und zu sichern.

Hier ist ein Überblick über die Vielfalt der Geräte, die unter den Begriff „Mobilgeräte“ fallen:

- Smartphones
- Tablets
- Laptops
- Wearables
- Internet der Dinge (IoT)
- E-Reader
- Spielkonsolen
- Digitalkameras

Betrachten Sie die Vielzahl dieser Gerätetypen unter Berücksichtigung der **durchschnittlichen Anzahl von Geräten** pro Kopf weltweit (3,6) und vergleichen Sie diese mit Unternehmen aus der Vergangenheit. Sie werden feststellen, dass sie mit der modernen Computerlandschaft – und damit auch mit der Erweiterung der modernen Bedrohungslandschaft – wenig gemeinsam hat.



„85 % der Befragten geben an, dass die Bedrohung durch mobile Geräte im letzten Jahr zugenommen hat.“

– Verizon 2024 Mobile Security Index

Das wirft zwangsläufig die Frage auf: Entspricht Ihre aktuelle Management- und Sicherheitslösung noch Ihren strategischen Zielen, Ihren Konformitätsanforderungen und dem Bedürfnis nach produktivem Arbeiten?

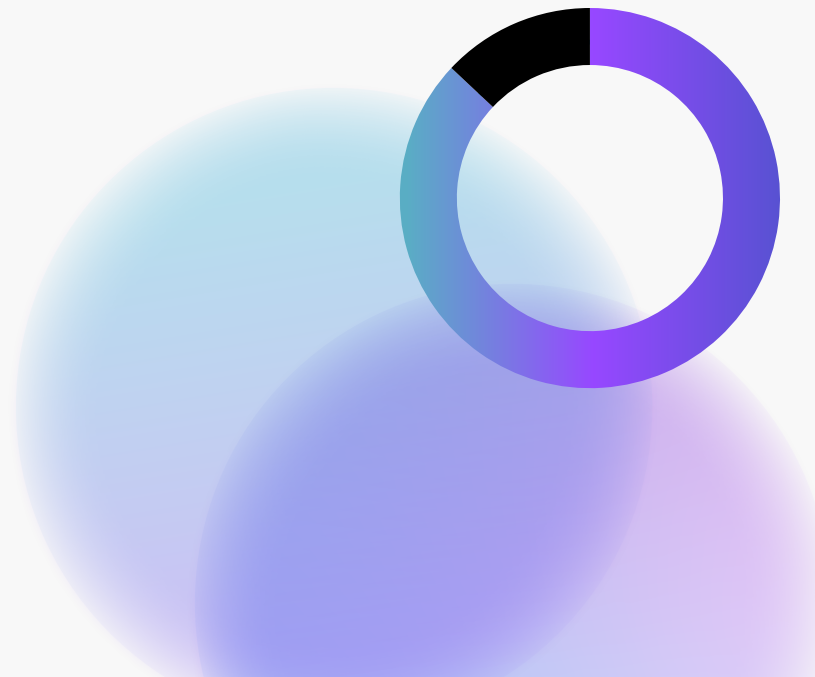
Aufrechterhaltung der Konformität bei unterschiedlichen Besitzverhältnissen

Bevor wir versuchen, die im vorangegangenen Abschnitt gestellte Frage zu beantworten, sollten wir uns mit den Auswirkungen der unterschiedlichen Besitzmodelle auf die Gerätenutzung von Mobilgeräten im Unternehmen befassen.

In diesem Abschnitt geht es insbesondere darum, **die Sicherheit im Unternehmen aufrechtzuerhalten**, wenn die für die Arbeit genutzten Mobilgeräte eine Mischung aus unternehmenseigenen und persönlichen Geräten sind. Zusätzliche Komplexität bedeutet, dass man Folgendes unterstützen muss:

- **unterschiedliche Gerätetypen** (Laptops, Smartphones, Tablets, Wearables)
- **von verschiedenen Anbietern** (Apple, Microsoft, Samsung usw.)
- **mehrere Betriebssysteme** (Apple, Android, ChromeOS und Windows)
- **unterschiedliche Software-Versionen** (Apps und OS)
- **verteilte Arbeitskräfte** (Rückkehr ins Büro, remote und hybride Umgebungen)

Moderne Unternehmen gleichen einem Schmelztiegel aus verschiedensten Geräten, Besitzmodellen und IT-Umgebungen, was sich in vielfältiger Weise auf die jeweiligen Bedürfnisse und Anforderungen auswirkt. Dadurch muss die IT dafür zu sorgen, dass die Benutzer - unabhängig vom Besitzverhältnis - Zugang zu Unternehmensressourcen haben, um produktiv zu bleiben. Außerdem muss die Produktivität der Mitarbeiter:innen mit Mobilgeräten im Unternehmen umfassend geschützt werden. Und schließlich muss sichergestellt werden, dass die Mobilgeräte so eingesetzt werden, dass sie mit den Geschäftszielen übereinstimmen und die Geschäftsabläufe so unterstützen, dass Wachstum und Skalierbarkeit im Einklang mit den organisatorischen Anforderungen stehen.



„87 % der Befragten aus dem Bereich der kritischen Infrastrukturen glauben, dass eine Sicherheitsverletzung auf Mobil- und IoT-Geräten erhebliche Auswirkungen auf ihr Unternehmen haben würde.“

– Verizon 2024 Mobile Security Index

Lösen für X

Ältere Tools wurden nicht dafür entwickelt, mit der heutigen mobilen und hybriden Arbeitsumgebung Schritt zu halten. IT-Teams brauchen integrierte Lösungen, die skalierbar und sicher sind und die Verwaltung optimieren. Moderne Verwaltungslösungen helfen Organisationen, die gewünschten Geschäftsergebnisse zu erzielen, indem sie die Zero-Touch-Bereitstellung vereinfachen, das Patching automatisieren und Compliance-Baselines plattformübergreifend durchsetzen. Die umfassende Integration von Identitätsdiensten ermöglicht eine Zero-Trust-Architektur und einen sicheren Zugriff über jede Netzwerkverbindung. Eine verhaltensbasierte Bedrohungserkennung und die Endpunktüberwachung in Echtzeit verbessern die Reaktion auf Sicherheitsvorfälle. Die Kombination mit der Unterstützung von CIS-Benchmarks versetzt die IT in die Lage, die Konformität kontinuierlich zu prüfen und nachzuweisen, während gleichzeitig die Produktivität und Performance über alle Gerätetypen, Eigentumsmodelle und Arbeitsumgebungen hinweg aufrechterhalten wird.

Technische Prozesse an Geschäftszielen ausrichten

Die IT ist, wie jeder andere Unternehmensbereich auch, entscheidend für den Unternehmenserfolg. Um erfolgreich zu sein, müssen IT-Prozesse über die klassische Geräteverwaltung hinauswachsen und Lösungen für mobile Geräte, verteiltes Arbeiten und moderne Cyberbedrohungen bieten.

Um wettbewerbsfähig zu bleiben, muss sich die IT an den Kernzielen des Unternehmens orientieren und einen direkten Beitrag zu folgenden Dingen leisten:

1. **Strategisches Wachstum**
2. **Steigerung der betrieblichen Effizienz**
3. **langfristige Widerstandsfähigkeit**

Zusätzlich zur Unterstützung des Unternehmens muss sie flexibel sein, die Produktivität verbessern und Risiken minimieren, ohne dabei das Benutzererlebnis zu beeinträchtigen.

Wenn Sie eine Verwaltungslösung einsetzen, die der Diversität mobiler Geräte gerecht wird und diese an Ihrer Unternehmensstrategie ausrichten, erzielen Sie messbare Erfolge in Kernindustrien. Beispiele für moderne Einsatzszenarien sind:

Produktion

Mithilfe von iPads haben die Mitarbeiter:innen in der Produktion Zugang zu Daten der Lieferkette in Echtzeit und digitalisieren Workflows. Eine IDC-Studie ergab, dass 85 % der Unternehmen, die **in Technologien für die digitale Transformation (DX) investiert** haben, einen direkten Zusammenhang feststellten: „Eine verbesserte Mitarbeitererfahrung und ein höheres Mitarbeiterengagement führen zu einem besseren Kundenerlebnis, höherer Kundenzufriedenheit und steigenden Umsätzen für das Unternehmen.“

Gesundheitswesen

Durch iPads und iPhones haben Pflegekräfte einen sofortigen, sicheren Zugang zu elektronischen persönlichen Gesundheitsinformationen (PHI) und Telemedizin-Tools. Gemäß den National Institutes of Health (NIH) belegen 70 % der im Fachartikel **Smartphone and Mobile App Use Among Physicians in Clinical Practice** ausgewerteten Studien den *Einsatz mobiler Apps*. Diese dienen dazu, Patientenergebnisse zu verbessern und Abläufe in der Versorgung effizienter zu gestalten – insbesondere durch den Zugriff auf evidenzbasierte medizinische Daten als Grundlage für klinische Entscheidungen.

Regierung

iPhones ermöglichen einen sicheren Zugang aus der Ferne zu den Ressourcen der Regierungsbehörden und unterstützen die Datenerfassung vor Ort. Laut dem **Verizon 2024 Data Breach Investigations Report** führen etwas mehr als 90 % der als verloren oder gestohlen gemeldeten Mobilgeräte zu einer ‚bestätigten Offenlegung von Daten‘. Eine skalierbare, umfassende Sicherheitslösung passt sich wachsenden Geräteflotten und sich ändernden Richtlinien an und gewährleistet dabei einen konsistenten, ganzheitlichen Schutz.

Optimierte Unterstützung für Ihre Mobilgeräte

Moderne Strategien für Mobilgeräte sind für IT-Teams unerlässlich, um den Support zu skalieren, die Konformität durchzusetzen und die Privatsphäre der Benutzer auf persönlichen und unternehmenseigenen Geräten zu wahren. Eine plattformübergreifende Sicherheit gewährleistet die Erreichung gleicher Sicherheitsstandards und die Einhaltung der Vorschriften, während die optimierte Neukonfiguration gemeinsam genutzter Geräte das Risiko verringert und die Verfügbarkeit erhöht – wodurch Mitarbeiter:innen ohne festen Arbeitsplatz produktiver arbeiten können. Dieser Ansatz verbessert die betriebliche Effizienz und gewährleistet einen einheitlichen Schutz, so dass IT-Führungskräfte die Verwaltung der mobilen Flotte an die sich verändernden Anforderungen von Unternehmen und Arbeitskräften anpassen können.

Skalierbare Unterstützung für verschiedene Besitzmodelle

Moderne Unternehmen stehen vor der Herausforderung der Skalierbarkeit, wenn sie eine hybride Flotte von persönlichen und unternehmenseigenen Geräten unterstützen. Spezifische Lösungen, wie z. B. die **Unterstützung verschiedener Modelle für die Registrierung**, sind für IT-Teams unerlässlich, um Folgendes zu erreichen:

- weniger Komplexität
- Sicherheit auf ganzer Linie
- getrennte, geschäftliche und personenbezogene Daten
- Konformität
- Schutz der Privatsphäre

Eine Schlüsselfunktion zur Aufrechterhaltung der Sicherheit bei gleichzeitiger Wahrung der Privatsphäre besteht darin, **Geschäftsdaten zu schützen und gleichzeitig Netzwerkverbindungen** zu/von Unternehmensressourcen zu verschlüsseln, während der private Datenverkehr über persönliche Geräte direkt ins Internet geleitet wird. Dieser Ansatz gewährleistet einen konsistenten Sicherheitsstatus der Geräte sowie eine skalierbare Durchsetzung von Richtlinien über verschiedenste Eigentumsmodelle hinweg.

Parität der plattformübergreifenden Endpunktsicherheit

Zusätzlich zur Herausforderung durch unterschiedliche Eigentumsmodelle arbeiten moderne Unternehmen häufig in heterogenen oder gemischten Umgebungen. Diese bestehen aus verschiedenen Betriebssystemen wie iOS/iPadOS, Windows und Android, die von den jeweiligen Stakeholdern genutzt werden. Multipliziert man die Komplexität mit der Anzahl der Geräte, wird die Risikominimierung aufgrund der vielen Variablen immer schwieriger.

Mit einer Mischung aus Defense-in-Depth-Strategien und den richtigen Kontrollmechanismen, wie:

- moderne Telemetrie
- verhaltensbasierte Erkennung von Bedrohungen
- einheitliche Richtlinien für den Zugang

und plattformübergreifende Unterstützung werden mobile Endpunkte konsistent abgesichert. Dies geschieht sowohl auf dem Gerät als auch im Netzwerk, **unabhängig vom jeweiligen Betriebssystem**. Diese plattformübergreifende Unterstützung ermöglicht es IT-Teams, die Fragmentierung zu verringern und gleichzeitig **strenge Sicherheitsstandards für die gesamte mobile Flotte aufrechtzuerhalten**.

Gemeinsam genutzte Geräte und schreibtischlose Mitarbeiter:innen

In Branchen, in denen eine gemeinsame Nutzung der Geräte zum Alltag gehören, ist es entscheidend, die Ausfallzeiten beim Benutzerwechsel so gering wie möglich zu halten. Dazu gehören:

- ein schnelles Einrichten eines iPhones zur Unterstützung der Kunden während einer geschäftigen Einkaufssaison
- die Bereitstellung von iPhones für die Flugbesatzung, um den Einkauf von Lebensmitteln und Getränken an Bord zu optimieren
- das Umkonfigurieren eines iPads im Kioskmodus, um die Pflegekräfte bestmöglich zu unterstützen

In Situationen, in denen es auf Sekunden ankommt, ist eine einfache Gerätekonfiguration entscheidend. Wenn **Benutzer Rollenwechsel selbstständig durchführen** oder **Geräte ohne IT-Unterstützung zurücksetzen und neu registrieren können**, spart dies im Ernstfall lebenswichtige Zeit. Spezifische Lösungen sorgen dafür, dass gemeinsam genutzte Geräte sicher und für den nächsten Benutzer einsatzbereit bleiben, während gleichzeitig die Zahl der Supportanfragen sinkt und die betriebliche Effizienz insgesamt verbessert wird.

Neue Workflows zur Steigerung der Produktivität

Die Optimierung der Mobilgeräteverwaltung steigert die Effizienz der IT und die Benutzerproduktivität im Unternehmen. Die nahtlose Integration von Identitäts- und Sicherheitstools ermöglicht eine schnellere Bereitstellung, Berichterstattung über die Compliance und Zugangskontrolle. Durch eine automatisierte Bereitstellung werden Einrichtungszeit und manuelle Fehler reduziert, während Self-Service-Funktionen die Benutzer befähigen, bei Bedarf eigenständig auf wichtige Apps und Ressourcen zuzugreifen. Letztendlich sorgen diese Workflows dafür, dass die Ausfallzeiten reduziert werden und die IT-Teams die Möglichkeit bekommen, sich auf die Entwicklung von Prozessen zu konzentrieren, die einen direkten Mehrwert für die Geschäftsziele schaffen.

Nahtlose Integration von bestehenden Tools

„Patentrezepte“ gibt es nicht.

Deshalb ist die **Integration ein wichtiger Bestandteil für die erfolgreiche Verwaltung und Sicherung mobiler Geräte:**

- Erweiterung der Dienste
- Hinzufügen von umfassenden Sicherheitsebenen
- Nutzung von bestehenden Tools
- Anpassung der Workflows an die Konformitätsanforderungen

Die **Integration von Identitätsanbietern** wie Microsoft Entra ID und Okta beispielsweise zentralisiert die Zugangskontrolle, setzt Richtlinien für Conditional Access durch und ergänzt Authentifizierungsverfahren um eine phishing-resistente Multi-Faktor-Authentifizierung. Die Minimierung des Risikos eines unbefugten Zugriffs auf geschützten Ressourcen ist nur eines von zahllosen Beispielen, bei denen die Integration mit Sicherheitsplattformen der IT Folgendes ermöglicht:

- optimiertes Onboarding von Geräten
- eine schnellere Bereitstellung
- einfachere Berichterstattung über die Konformität
- weniger Reibungsverluste im gesamten Technologiebereich
- Anpassung an geschäftliche Workflows

Automatisierte Gerätebereitstellung und -nutzung

Je nach Unternehmen kann das manuelle Onboarding von Mobilgeräten bis zu 30 Minuten pro Gerät in Anspruch nehmen, was zu Produktivitätsverzögerungen und einem erhöhtem Aufwand für die IT führt.

Eine **automatisierte Bereitstellung mobiler Geräte mit Zero-Touch** und dem Apple Business Manager (ABM) verkürzt die Provisionierungszeiten erheblich, indem sie den Bereitstellungsprozess optimiert und Ausfallzeiten effektiv reduziert. Dieser Ansatz **steigert die Effizienz der IT** und bietet Organisationen folgende Vorteile:

- macht die manuelle Einrichtung überflüssig und verringert das Risiko menschlicher Fehler
- beschleunigt das Onboarding, einschließlich der Installation und Konfiguration von Apps
- stellt sicher, dass jedes Gerät die Sicherheits- und Konformitätsstandards erfüllt - vom ersten Tag an
- Benutzer verfügen über die benötigten Ressourcen und sind nach der Aktivierung sofort einsatzbereit

Zugang zu benötigten Ressourcen - wenn Ihre Benutzer es brauchen

Eine **gute Reaktionszeit** für eine IT-Anfrage liegt in der Regel im Bereich von 24 Stunden oder einem Werktag. Wenn jemand jedoch eine App oder eine Konfiguration braucht, um eine Aufgabe zu erledigen, bedeutet jede Minute Verzögerung einen Produktivitätsverlust, der sich möglicherweise auf die Abläufe der Organisation und letztendlich auf das Endergebnis auswirkt.

Self Service bietet viele Vorteile, weil die Benutzer Zugang zu folgenden Funktionen erhalten:

- ein kuratierter Katalog genehmigter Apps
- Unternehmensressourcen und -services
- sichere Konfigurationen und Einstellungen

- und das alles, ohne ein Support-Ticket einreichen zu müssen!

Die Benutzer können sicher auf die Ressourcen zugreifen, die sie benötigen, um produktiv zu bleiben, während die IT die Kontrolle über die verfügbaren Ressourcen behält. Dadurch wird das Volumen der Helpdesk-Tickets reduziert und die Mitarbeiter:innen können selbständig aktiv werden.

Umsetzung einer umfassenden Sicherheitsstrategie

Unternehmen müssen ihre Sicherheitspraktiken weiterentwickeln und skalieren, um sich effizient gegen moderne Bedrohungen in unterschiedlichen mobilen Umgebungen zu schützen. Die Automatisierung der Patch-Verwaltung minimiert Schwachstellen, indem sie dafür sorgt, dass Geräte und Apps auf dem neuesten Stand bleiben, und gleichzeitig der Aufwand für die IT reduziert wird. Eine fortschrittliche Erkennung von Bedrohungen erfordert Analysen in Echtzeit, eine umfassende Integration und mehrschichtige Verteidigungsmechanismen, um die Risiken zu erkennen und zu minimieren. Eine Zero-Trust-Strategie, die den Zustand der Geräte überwacht und die Identität der Benutzer verifiziert, bietet einen sicheren Zugang zu Ressourcen unabhängig von Standort, Plattform oder Besitzmodell.

Automatisierte Patch-Verwaltung

Faktor Mensch stellt die größte vermeidbare Gefahrenquelle innerhalb der Cybersicherheitsstrategie eines Unternehmens dar. Veraltete Software, die in diesen Bereich fällt, macht mobile Geräte anfällig und untergräbt die Konformitätsziele eines Unternehmens. Die gute Nachricht ist, dass durch die **Automatisierung der Patch-Verwaltung sowohl für Betriebssysteme als auch für Apps** diese Art von Bedrohung auf folgende Weise entschärft werden kann:

- Überwachung und Warnmeldungen in Echtzeit
- proaktive Überprüfung von Unified Logs
- Nutzung von **dynamischen Gruppen**
- Durchsetzung dynamischer Richtlinien
- **App-Installationsprogramme**
- Mindestversionseinstellung für Apps

Durch die Automatisierung reduziert sich der manuelle Aufwand für die IT. Außerdem wird dafür gesorgt, dass die Geräte stets auf dem neuesten Stand sind und die internen und gesetzlichen Anforderungen erfüllen. Und die Unterbrechungen und Ausfallzeiten für die Benutzer werden minimiert.

Erkennung und Prävention von Bedrohungen

Cyberangriffe erreichten 2020 ihren Höhepunkt und gingen danach zurück - bis **die Angriffe auf Mobilgeräte laut Kaspersky von Q1 bis Q4 2023 um 147 %** anstiegen. Bedrohungen für Mobilgeräte sind anspruchsvoller geworden und umgehen häufig die Abwehr herkömmlicher Malware-Tools. Eine wirksame mobile Sicherheit muss bekannte Bedrohungen verhindern und Verhaltensanalysen auf dem Gerät und im Netzwerk durchführen, um erweiterte Risiken in Echtzeit zu erkennen. Die umfassende Integration von Management, Identität und Sicherheit bietet IT-Teams folgende Vorteile:

- mehr Transparenz über die Aktivitäten von Mobilgeräten
- Bewertung des Risikostatus in Echtzeit
- schnellere Reaktionszeiten bei Vorfällen über mehrere Plattformen, Besitzmodelle und Arbeitsumgebungen hinweg
- nahtlose Integration in SIEMs von Drittanbietern
- umfassende, mehrstufige Kontrollen ohne Beeinträchtigung der Leistung des Geräts

Zero-Trust-Netzwerkzugriff (ZTNA)

Die Arbeitsumgebungen und die Gerätenutzung haben sich weiterentwickelt. Sollten sich die Unternehmen also immer noch auf ältere Tools verlassen, die für eine andere Ära entwickelt wurden, um die heutige mobile Flotte zu verwalten und zu sichern?

Die Antwort ist einfach: nein.

Die Umstellung auf Cloud Computing, hybride Arbeitsumgebungen und mobile Geräte macht die Kontrolle des Zugangs auf der Grundlage der Identität des Benutzers und des Zustands des Geräts zu einer unabdingbaren Voraussetzung für die Einhaltung der Konformität. Heutige Unternehmen erreichen dies, indem sie diese Maßnahmen umsetzen:

- Ersetzen von klassischen VPNs durch verschlüsselte Microtunnel zur Isolierung des Netzwerkverkehrs
- Umsetzung von Richtlinien für den Conditional Access, die nur sanktionierten Benutzern und verifizierten Geräten Zugang gewähren
- nahtlose Integration der Identität in das Management- und Sicherheitssystem des Unternehmens
- Entwicklung einer Zero-Trust-Strategie, die Unternehmensressourcen ganzheitlich absichert - unabhängig davon, wo die Mitarbeiter:innen arbeiten, welches Gerät sie nutzen oder wer es besitzt

Konformität ganzheitlich standardisieren und durchsetzen

Eine wirksame Konformität beginnt mit der Implementierung von Sicherheitsgrundlagen, die auf Industriestandards basieren und sicherstellen, dass alle Mobilgeräte vom ersten Tag an durchsetzbare Richtlinien erfüllen. Die aktive Überwachung des Zustands der Endgeräte bietet Transparenz in Echtzeit und KI-gesteuerte Erkennung von Risiken. Dies hilft der IT, die Konformität aufrechtzuerhalten und schnell auf Bedrohungen zu reagieren. Die Überprüfung der Konformität durch Benchmarks wie CIS ermöglicht es Organisationen, die Einhaltung der Vorschriften zu auditieren, bei Bedarf anzupassen und darüber zu berichten.

Stärkung des Sicherheitsstatus durch die Einführung von Baselines

Technische Kontrollen und Richtlinien sind für die Konformität und die Durchsetzung der Vorschriften unerlässlich, aber wo fängt man an und welche Anforderungen gibt es in Ihrer Branche? Fangen Sie mit den Grundlagen an, die auf von der Industrie akzeptierten Standards und Frameworks basieren.

Die Festlegung von Konfigurations-Baselines stellt sicher, dass jeder Endpunkt – ob unternehmenseigen oder im Privatbesitz – **bei der Registrierung der mobilen Geräte im MDM die erzwingbaren Sicherheitsanforderungen erfüllt**. Dies ist ein grundlegender Schritt und entscheidend für die Entwicklung und Implementierung einer umfassenden Sicherheitsstrategie. Eine, die der IT bei folgenden Aspekten hilft:

- Sicherstellung der Konformität durch strukturierte Bereitstellung von Konfigurationsprofilen für bestimmte dynamische Gruppen
- Automatisierung der konsistenten Bereitstellung und Reduzierung von Abweichungen von der Konfiguration im großen Maßstab
- Angleichung der Prozesse für mobile Geräte an die Datensicherheit zur Unterstützung der Geschäftskontinuität
- Anpassung der Sicherheitsstrategien an die individuellen Bedürfnisse des Unternehmens und die Vorschriften der Industrie

Aktive Überwachung des Zustands der Endpunkte

Der nächste wichtige Schritt nach der Implementierung von Baselines ist die aktive Überwachung von Geräteflotten, bei der eine kontinuierliche Transparenz über den Zustand für eine nachhaltige Compliance unerlässlich ist, einschließlich einer schnellen Reaktion auf Vorfälle, wenn kompromittierte Endpunkte entdeckt werden. Dank der engen Integration von Management-, Identitäts- und Sicherheitslösungen werden die Silos zwischen den IT-Teams aufgebrochen. Dabei wird **KI genutzt, um das Sicherheitsniveau des Unternehmens zu verbessern** und zusätzlich Folgendes zu ermöglichen:

- **Nutzung von Echtzeitlemetrie und Einblicke in das Verhalten von Endpunkten**
- **Maschinelles Lernen (ML) für die Erkennung von Risiken und noch schnellere Abwehr**
- **proaktive Bedrohungssuche auf mobilen Endpunkten**, Analyse und Reaktion auf anspruchsvolle Bedrohungen

Überprüfen und Durchsetzen der Konformität mit Benchmarks

Der dritte wichtige Schritt schließt die Lücke im Lebenszyklus der Gerätekongformität, indem er die Lücke zwischen Durchsetzung, Überprüfung und Verbesserung schließt und den Organisationen ein Tool an die Hand gibt, um die Kongformität kontinuierlich zu auditieren. Außerdem erleichtert es den **Nachweis der Compliance, wie er in regulierten Industrien vorgeschrieben ist**.

Moderne Management-Lösungen unterstützen Unternehmen nicht nur bei der Standardisierung und Überwachung der Compliance, sondern bieten auch die erforderlichen nativen Werkzeuge, um diese Kongformität anhand branchenweit anerkannter Benchmarks wie CIS Level 1 und 2 zu verifizieren. Dies stärkt die interne Governance und die regulatorische Compliance durch:

- **flexible Anpassung der Benchmarks an die individuellen Anforderungen des Unternehmens** durch die IT
- **automatisierter Abgleich der Baselines, um etwaige Abweichungen von den Benchmarks automatisch zu eliminieren**
- **Erstellung von Anleitungen mit einem Klick in den Formaten PDF, HTML und Adoc für die Auditprüfung**

Bequemlichkeit vs. Sicherheit: die Zahlen im Überblick

Die Entscheidung für bequeme oder kostengünstige Tools geht oft zulasten der Sicherheit, was langfristig zu größeren Risiken und Betriebsunterbrechungen führt. Uneinheitliche Schutzmaßnahmen für verschiedene Gerätetypen schwächen den allgemeinen Sicherheitsstatus und führen zu Lücken, die Cyberkriminelle ausnutzen können. Cyberangriffe haben nicht nur Auswirkungen auf die Sicherheit, sondern beeinträchtigen auch die Leistung von Geräten, behindern die Produktivität und stören die Geschäftskontinuität. Um diese Fallstricke zu vermeiden, sollten IT-Verantwortliche Sicherheitslösungen priorisieren, die alle Endpunkte schützen – unabhängig von den Eigentumsverhältnissen oder dem Betriebssystem. Dies gewährleistet Effektivität, Resilienz, Effizienz und eine nachhaltige organisatorische Stabilität.

Billig gekauft ist teuer bezahlt: Warum ‚einfach‘ am Ende teurer ist als ‚sicher‘

Die Kosten sind ein entscheidender Faktor für Organisationen, die sich für eine Verwaltungs- und Sicherheitslösung von Mobilgeräteflotten entscheiden. Das Festhalten an Altsystemen oder die Entscheidung für Standardlösungen mag zwar die anfänglichen Einrichtungszeiten und Anschaffungskosten senken, geht jedoch oft zulasten einer umfassenden mobilen Sicherheit – ein Kompromiss für die Bequemlichkeit und die Preisvorteile dieser Tools.

Leider können solche Lücken in der Sicherheit zu kostspieligen Verstößen führen. Laut dem IBM-Bericht „Cost of a Data Breach 2025“ liegen **die durchschnittlichen Kosten für eine Datenverletzung weltweit bei 4,44 Millionen US-Dollar** und in den USA bei 10,22 US-Millionen Dollar.

Im Gegensatz dazu zeigt eine Analyse des IBM-Berichts, dass Sicherheitsteams durch KI und Automatisierung Kosten in Höhe von 1,9 Millionen US-Dollar einsparen konnten. Diese Technologien verkürzten die Reaktionszeit bei Datenpannen um signifikante 80 Tage und reduzierten die Durchschnittskosten pro Angriff deutlich gegenüber Organisationen, die nur auf Basislösungen in den Bereichen Verwaltung, Identität und Sicherheit setzen.

Das Fazit: Investitionen in die Cybersicherheit sind untrennbar mit dem Geschäftsbetrieb, dem öffentlichen Ruf und der regulatorischen Compliance verbunden – Faktoren, die allesamt auf unterschiedliche Weise zum Gesamtergebnis eines Unternehmens beitragen.

Mangelnde Parität schwächt den Sicherheitsstatus der Organisation

Wenn die Sicherheit mobiler Geräte plattformabhängig ist, anstatt die Sicherheitsfunktionen selbst plattformunabhängig zu unterstützen, entstehen für Unternehmen Sicherheitsungleichheiten.

Dies hat zur Folge, dass einige Mobilgeräte nicht so gut geschützt sind wie andere.

Laut einem kürzlich im **Infosecurity Magazine** erschienenen Artikel nannten 41 % der Befragten gestohlene Geräte mit sensiblen Daten als Hauptursache für Datenverluste – noch vor schwachen und gestohlenen Passwörtern (36 %) und Ransomware-Angriffen (32 %). Dieses Szenario ist auf uneinheitliche Kontrollmechanismen auf den unterstützten Plattformen zurückzuführen, was zu einem falschen Gefühl des Schutzes vor ausnutzbaren Sicherheitslücken führt und die allgemeine Widerstandsfähigkeit untergräbt.

Die Unternehmenssicherheit muss alle Endpunkte umfassen, die auf die organisatorische Infrastruktur zugreifen. Da jedes Gerät ein potenzielles Risiko darstellt, muss dieser Schutz unabhängig von Gerätetyp, Betriebssystem oder Eigentumsverhältnis gelten. Risiko ist Risiko.

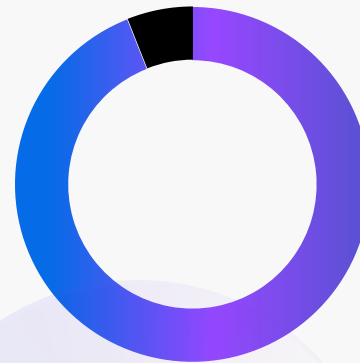
Auswirkungen auf die Leistung der Geräte und die Produktivität der Mitarbeiter

Cyberfälle haben nicht nur finanzielle Auswirkungen (wie bereits erwähnt). Sie beeinträchtigen zwar die Sicherheitslage der Geräte und der gesamten Organisation, verschlechtern aber auch die Performance und die Benutzerproduktivität – was sich wiederum negativ auf den gesamten Geschäftsbetrieb auswirkt.

Unter Berücksichtigung von Sicherheitsverletzungen in verschiedenen Umgebungen (öffentliche und private Clouds sowie vor Ort) fand IBM heraus, dass die durchschnittliche Zeit bis zur Identifizierung einer Datenverletzung 207 Tage beträgt. Die durchschnittliche Zeit bis zur Eindämmung (Mean Time to Contain, MTTC) erforderte zusätzliche 70 Tage. Damit stieg die durchschnittliche Gesamtdauer für die Identifizierung und Eindämmung einer Datenverletzung über verschiedene Umgebungen hinweg auf 276 Tage – eine Zeitspanne, die sowohl finanzielle Verluste als auch Opportunitätskosten durch Leistungseinbußen bei den betroffenen Geräten und Unternehmenssystemen vereint.

Obwohl der vorherige Aspekt sowohl direkte als auch indirekte Auswirkungen auf die Mitarbeiter:innen hat, können die Folgen bestimmter Bedrohungen und Angriffe die Benutzerproduktivität stärker beeinträchtigen. Nehmen wir zum Beispiel einen Ransomware-Angriff. In einem Artikel über die Folgen verlängerter Ausfallzeiten von Netzwerken und Unternehmen stellte [Help Net Security](#) fest, dass

„94 % der Unternehmen, die von einem Ransomware-Angriff betroffen waren, mit erheblichen Ausfallzeiten und Produktivitätseinbußen zu kämpfen hatten. 40 % der Opfer gaben an, dass es bei ihnen eine Zeit lang zu einem totalen Arbeitsstopp und einem vollständigen Produktivitätsverlust kam.“



Cyberangriffe haben Auswirkungen, die über die unmittelbaren Kosten hinausgehen, wie z. B. entgangene Geschäftsmöglichkeiten, verringerte Produktivität, untergrabenes öffentliches Vertrauen und sinkender Marktwert. Diese Folgen hallen oft noch lange nach der Eindämmung einer Sicherheitsverletzung nach.

Die wichtigsten Erkenntnisse

1.

Mobilität ist geschäftskritisch:

Mobile Geräte sind unverzichtbare Werkzeuge in allen Branchen, da sie Echtzeitkommunikation, flexible Arbeitsabläufe und Geschäftskontinuität in Remote-, Hybrid- und Vor-Ort-Umgebungen ermöglichen.

2.

Ältere Tools sind unzureichend:

Traditionelle und einheitliche Verwaltungslösungen können die Sicherheit angesichts der Komplexität moderner mobiler Flotten, unterschiedlicher Besitzmodelle und plattformübergreifender OS nicht aufrechterhalten.

3.

Sicherheit muss umfassend sein:

Moderne Unternehmen benötigen plattformübergreifende, identitätsbasierte Sicherheitsstrategien, die die Erkennung von Bedrohungen in Echtzeit, Richtlinien für Conditional Access und eine automatisierte Patch-Verwaltung beinhalten

4.

Konformität ist nicht verhandelbar:

Eine effektive Verwaltung von Mobilgeräten unterstützt die auditfähige Konformität, indem sie sichere Baselines bereitstellt, die den Zustand der Endpunkte überwacht und die Einhaltung der Branchenstandards überprüft.

5.

Skalierbarkeit und Automatisierung sind der Schlüssel:

Speziell entwickelte Lösungen optimieren die Nutzung, vereinfachen die Bereitstellung und reduzieren den manuellen Aufwand, sodass die IT den Support über verteilte Teams hinweg ganzheitlich skalieren kann.

6.

Benutzererlebnisse sind wichtig:

Die Unterstützung der Mitarbeiter durch Self-Service-Tools und einen konsistenten Zugriff auf Unternehmensressourcen steigert die Produktivität, ohne die Privatsphäre oder Sicherheit zu beeinträchtigen, und reduziert gleichzeitig die Arbeitsbelastung der IT.

7.

Die unternehmerische Ausrichtung schafft Mehrwert:

Die Anpassung der Mobilgeräteverwaltung an strategische Zielen verbessert die betriebliche Effizienz, unterstützt das Wachstum und positioniert die IT als Innovationsmotor.

Fazit

Die zunehmende Nutzung von mobilen Geräten zur Steigerung der Produktivität ermöglicht das Arbeiten am Schreibtisch oder von unterwegs. Das Erzielen von Geschäftsergebnissen ist nicht länger ein Trend - es ist ein bestimmendes Merkmal des modernen Unternehmens.

Aufgrund der zunehmenden Komplexität von Gerätetypen, Besitzmodellen und der Unterstützung mehrerer Betriebssysteme sind ältere Verwaltungstools nicht mehr in der Lage, einige der grundlegendsten Anforderungen moderner Unternehmen in Bezug auf Sicherheit, Konformität und Benutzerfreundlichkeit zu erfüllen.

Die IT-Abteilung soll nicht mehr nur Geräte verwalten.

Sie müssen vielmehr die Technologie und die Verwaltungsprozesse mit der Unternehmensstrategie in Einklang bringen, um die Unternehmensziele zu erreichen. Sie müssen kritische Assets schützen und die Belegschaft unterstützen, denn diese erwartet nahtlosen Zugang von überall, auf dem Gerät ihrer Wahl und mit dem Betriebssystem, mit dem sie am besten arbeiten können.

1.

**Es steht sehr viel
auf dem Spiel.**

2.

**Die Risiken sind
größer.**

3.

**Und der Spielraum für
Fehler wird immer kleiner.**





Moderne Lösungen für die Endpunktverwaltung sind darauf ausgelegt, diesen wachsenden Anforderungen gerecht zu werden. Von Zero-Touch-Bereitstellung und fortschrittlicher Erkennung von Bedrohungen bis hin zu plattformübergreifender Unterstützung und Zero-Trust-Sicherheit. Dank spezifischer Tools können IT-Teams die Geschäftsabläufe auf Mobilgeräten skalieren, sichern und optimieren, ohne die Sicherheit, Effizienz oder Produktivität zu beeinträchtigen.

Doch eine Frage bleibt:

Entspricht Ihre derzeitige Lösung für die Unternehmensverwaltung noch den sich entwickelnden Anforderungen Ihres Unternehmens, Ihrer IT und Ihrer Mitarbeiter:innen? Wenn die Antwort nicht klar ist, ist es jetzt an der Zeit, Ihren Ansatz zu überdenken ... der Erfolg Ihres Unternehmens hängt davon ab.

Probieren Sie Jamf aus