

Ein Leitfaden für Käufer:innen: Mobilität im Unternehmen

Entdecken Sie, was mit Mobilgeräten bei der Arbeit alles möglich ist

Mobile Arbeitskräfte sind mit immer neuen Bedrohungen konfrontiert.

Erfolgreiche Bereitstellungen erfordern detaillierte Einblicke, sicheren Zugang zu Apps und Geräte, die den Anforderungen der Endbenutzer:innen und des Unternehmens entsprechen.

Ob an der Frontlinie oder im Büro – Mitarbeiter:innen verlassen sich immer stärker auf mobile Geräte, um ihre Aufgaben erfolgreich zu erledigen. Die Verteidigung mobiler Endpoints kann eine Herausforderung sein, vor allem weil Benutzer:innen mit neuen Bedrohungen konfrontiert sind und die Geräte in einer Vielzahl von Umgebungen eingesetzt werden. Organisationen müssen heute neue Workflows und Produktivität in einem benutzerfreundlichen Umfeld ermöglichen.

Zu einem robusten Programm für den Mobilschutz gehören:

Verhinderung von mobilem Phishing



Phishing-Angriffe sind auf Mobilgeräten um **50 %** wahrscheinlicher.

Das Blockieren von Angriffen

Erkennung von Kompromissen mit robuster Forensik

Festlegung von Grundlagen für Mobilgeräte und Einhaltung von Compliance

Durchsetzung von Nutzungsrichtlinien

Registrierung von Geräten und Benutzer:innen in Produktivitäts-Workflows

Kontrolle der mobilen Datennutzung zur Reduzierung von Datenüberlastungen

Sichere Verbindung zwischen Arbeiter:innen und kritischen Apps und Arbeitsbelastungen

Vorbeugung von App-Risiken, von der Verwaltung von Schwachstellen bis zur Malware-Prävention

Die Verhinderung von Sicherheitsfehlkonfigurationen



WichtigsteFunktionen

Die wichtigsten Fähigkeiten, um mehr aus Ihrer mobilen Flotte zu machen.



Sichere Konfigurationsverwaltung

Abhärtung mobiler Geräte

- Einführung einer guten Sicherheitshygiene
- Durchführung von Compliance-Audits
- Überwachung auf Schwachstellen in der Konfiguration

Patch-Verwaltung

- Priorisieren Sie Patches mit detaillierten Berichten über Schwachstellen
- Entschärfen Sie Schwachstellen in OS und Apps

Beugen Sie Datenverlusten vor

- Kontrollieren Sie den Fluss von Unternehmensdaten zwischen Apps
- Schränken Sie den Zugang zu einer App basierend auf dem Sicherheitsstatus von Benutzer:innen und deren Geräten

Richtlinie zur akzeptablen Nutzung

- Schränken Sie die Webnutzung mit dynamischen kategoriebasierten Richtlinien ein
- Setzen Sie AUP nach Benutzer, Gruppe, Region oder globaler Konfiguration durch



Angriffsprävention

Malware und andere App-Risiken

- Blockieren Sie Malware
- Identifizieren Sie Schwachstellen und riskante Apps
- Verhindern Sie das Durchsickern wichtiger Daten während der App-Nutzung
- Überwachung der Nutzung alternativer Apps auf dem Marketplace

Adversary-in-the-Middle

- Identifizieren Sie abtrünnige Hotspots und Protokollangriffe
- Entschärfen Sie Adversary-in-the-Middle-Angriffe mit verschlüsselten Tunneln

Web-Bedrohungen

- Verhindern Sie Phishing-Versuche, einschließlich Zero-Day-Angriffen
- Blockieren Sie bösartigen Netzwerkverkehr, einschließlich C2 und Datenexfiltration
- Neutralisieren Sie das Risiko von Kryptojacking, Spam und anderen webbasierten Bedrohungen



Geräteverwaltung

Bereitstellung und Registrierung

- Lassen Sie Geräte direkt an Benutzer:innen oder Standorte schicken
- Registrierung von Geräten für jedes Besitzmodell
- Integrieren Sie Geräte, Benutzer:innen und Apps nahtlos in Produktivitäts-Workflows.

Konfiguration & Einstellungen

- Automatisieren und skalieren Sie Aufgaben der Geräteverwaltung
- Beschränken Sie die Verwendung des Geräts auf seinen spezifischen Zweck
- Wenden Sie Richtlinien an, um sicherzustellen, dass Geräte die Sicherheitsanforderungen einhalten

Berichterstattung über den Bestand

- Erfassen Sie Daten über Benutzer:innen, Hardware, Software und Geräte-Sicherheit
- Passen Sie Bestandsspezifikationen für maximale Sichtbarkeit an

Inhalte auf Abruf

- Befähigen Sie Mitarbeiter:innen, genehmigte Apps anzufordern, herunterzuladen und zu aktualisieren



Benutzerdefinierte Workflows

Workflows für gemeinsam genutzte Geräte

- Bereitstellung, Personalisierung und Aktualisierung von Geräten je nach Anwendungsfall
- Unmittelbarer Zugang für Benutzer:innen zu Apps im Unternehmen
- Anpassung des Geräts mit rollenspezifischen Konfigurationen
- Befähigung von Frontline-Managern zur Bereitstellung von Tier-Zero-Support ohne IT-Hilfe

Partner-Integrationen und API

- [Jamf Marketplace](#) für vorgefertigte Lösungen und Integrationen
- Führende Anbieter für Organisationen aus den Bereichen Gesundheitswesen, Einzelhandel, Hartwaren und Luftfahrt
- EHR/EMR-Integrationen zur Optimierung der Geräteverwaltung für Gesundheitsorganisationen
- Jamf API erlaubt Organisationen die Integration von Jamf in jede Plattform oder jeden Workflow



Secure Access nicht übersehen

Schützen Sie Daten bei der Übermittlung

- Einrichtung verschlüsselter Tunnel zu wichtigen geschäftlichen Anwendungen und Daten

Audit der Nutzung kritischer Apps

- Erhalten Sie eine Berichterstattung über alle Apps, auf die mobile Arbeiter:innen zugreifen

Setzen Sie Richtlinien für den Zugang in Echtzeit durch

- Erstellen Sie Richtlinien für den Zugang, die Benutzer:innen und die Haltung der Geräte einbeziehen.



Erkennung von und Reaktion auf Bedrohungen

Reichhaltige Telemetrie sammeln

- Sammeln detaillierter Protokolle für die Offline-Analyse

Erkennung von Anomalien

- Aktivieren Sie die Bedrohungssuche und suchen Sie nach Anomalien, die auf bösartige Aktivitäten hinweisen.
- Binden Sie Indicators of Compromise sowie neue Erkenntnisse in die Threat Intelligence ein, um künftige Erkennungen zu optimieren

Bedrohungsbehebung

- Verweigern Sie den Zugang zu kritischen Apps und Workloads, wenn eine Gefährdung erkannt wird
- Entfernen Sie Malware und versetzen Benutzer:innen in einen produktiven Zustand zurück.



Zero-Trust-Ergebnisse mit Jamf erreichen

Jamf hilft Organisationen, ihre wertvollsten Güter zu schützen, indem es sicherstellt, dass nur autorisierte Benutzer:innen auf registrierten Geräten, die den Sicherheitsanforderungen der Organisation entsprechen, Zugang zu sensiblen Geschäftsanwendungen erhalten.



Wählen Sie Ihre mobilen Sicherheitsfähigkeiten mit Bedacht

Die Bedrohungslandschaft und unsere Arbeitsmethoden entwickeln sich ständig weiter. Angemessene Schutzmaßnahmen von gestern sind keine Garantie für die Sicherheit von heute. Und so wie wir heute arbeiten, werden wir morgen nicht mehr arbeiten. Im Folgenden finden Sie einige Überlegungen zur Auswahl Ihrer Sicherheitslösungen für Mobilgeräte.

Untersuchen Sie die Fähigkeiten der Lösung.

Es ist wichtig zu prüfen, über welche Fähigkeiten Ihre Lösung tatsächlich verfügt. Es reicht nicht aus, dass sie eine Funktion für „Mobilschutz“ vorgibt. Ihre Lösung sollte die einzigartigen Bedrohungen für mobile Geräte berücksichtigen und nicht einfach nur Computer-Sicherheitskonzepte auf ein Mobilgerät anwenden.

Sicherheit erfordert Geräteverwaltung.

Eine einzige Sicherheitslösung kann nicht alle Ihre Anforderungen erfüllen, und auch eine Software allein reicht nicht aus. Die Geräteverwaltung ist auf den Schutz bezogen von entscheidender Bedeutung, denn was man nicht sehen kann, kann man auch nicht sichern. Ihre Verwaltungssoftware hilft Ihnen, die Geräte-Compliance aufrechtzuerhalten und potenzielle Probleme zu beheben.

Das Erlebnis Ihrer Benutzer:innen ist wichtig.

Mitarbeiter:innen nutzen Mobilgeräte, weil ihre Mobilität ihnen hilft, produktiv zu bleiben. Sicherheitsrichtlinien, die die Funktionalität von Geräten zu sehr einschränken, sind für Benutzer:innen nicht hilfreich, da sie möglicherweise auf nicht genehmigte Lösungen setzen könnten, um diese zu umgehen.

Mobile Geräte haben sich zu unverzichtbaren Arbeitsmitteln entwickelt, auf die sich Benutzer:innen verlassen, um produktiv zu bleiben.

Wenn Geräte von der Aktion einer Richtlinie betroffen sind, müssen unbedingt Workflows eingerichtet werden, damit der/die Benutzer:in so schnell wie möglich wieder arbeiten kann.

Nicht alle Geräte benötigen die gleichen Sicherheits-Tools.

Berücksichtigen Sie das Bereitstellungsszenario und den Anwendungsfall, bevor Sie Tools und Richtlinienkonfigurationen anwenden. Zum Beispiel:

- Überlegen Sie, wie Ihre Mitarbeiter:innen ihre Geräte nutzen. Ihre Rollen beeinflussen ihre Risiken. Ein Beispiel: Standard-Mitarbeiter:innen mit Zugang zu einigen sensiblen Daten und dem Internet müssen vor allgemeinen Bedrohungen geschützt werden. Ihre Geräte sollten die Compliance einhalten und vor Phishing und Malware geschützt werden. Die Filterung von Inhalten, die Abwehr von Bedrohungen und der Zero-Trust-Netzwerkzugriff tragen dazu bei, sie noch sicherer zu machen.
- Schreibtischlose Arbeiter:innen, wie im Einzelhandel, profitieren von der Filterung von Inhalten und der Sicherheit von Apps. Wenn ihr Gerät keinen Zugang zu einem Browser hat, ist die Gefahr des Phishings geringer.
- Führungskräfte und Arbeitsfunktionen mit Zugang zu kritischeren Daten sind oft das Ziel. Sie erfordern zusätzliche Schutzmaßnahmen und müssen häufig gesetzliche Anforderungen erfüllen.