jamf

Beabsichtigen Sie die Integration von Apple Geräten in eine PC-basierte Umgebung?

Ihre Umgebung verfügt bereits über ausgereifte Systeme für **Identität**, **Sicherheit** und **Transparenz**.

Jetzt möchten Sie Apple Geräte mit einer **beschleunigten Bereitstellung** + **weniger Aufwand** + **geringerem Risiko** hinzufügen.

Nutzen Sie unsere Selbsteinschätzung, um herauszufinden, wie schnell Sie Apple in Ihre bestehenden Systeme integrieren können, ohne eine parallele Infrastruktur aufbauen zu müssen.

jamf

Zugriff + Vertrauen

Apple Geräte sollten sichnahtlos in Ihr Zugangsmodell integrieren lassen - ohne manuelle Ausnahmeregeln.

Stellen Sie sich folgende Fragen:

1. Können wir einheitliche **Zugriffsrichtlinien** für Mac Benutzer und Windows Benutzer durchsetzen?

2. Können wir die Zugriffsrichtlinien auf Basis von **Identitätsgruppen** festlegen, ohne die bestehende Organisationsstruktur neu aufbauen zu müssen?

3. Können wir den Zugriff an die **Konformität des Geräts** koppeln (nicht nur an den Benutzernamen/Passwort)?

jamf

Sicherheitsstatus + Bedrohungserkennung + Reaktion auf Vorfälle

Apple-Geräte sollten ein fester Bestandteil Ihres Sicherheitsbetriebsmodells sein.

Stellen Sie sich folgende Fragen:

1. Können wir die Risiken bei Apple in der **gleichen Konsole** sehen wie die Risiken bei Windows?

2. Sind die **Warnmeldungen umsetzbar** oder nur informativ?

3. Können wir die **Antwort automatisieren** oder ist bei Apple alles manuell?

jamf

Assets + Workflow

Apple Geräte sollten vollständig in Ihrem IT-Betrieb und den gesamten Asset-Lebenszyklus integriert sein - mit präziser Datenerfassung.

Stellen Sie sich folgende Fragen:

1. Haben wir einen **vollständigen Überblick über das Inventar** (Apps, Betriebssystem, Verschlüsselung, Eigentumsmodell)?

2. Können wir Apple **Endpunkte ohne zusätzlichen Aufwand in bestehende ITSM-Abläufe** integrieren?

3. Erfolgen die **Integrationen bidirektional** (Synchronisierung + aktive Steuerung) oder handelt es sich lediglich um einen Datenexport?

jamf

Bereitschaft zur Systemintegration Selbsteinschätzung

Bewerten Sie jede Kategorie auf einer Skala von 1-5

Identität

- [ ] Wir können einen konsistenten Zugriff und ein gerätebasiertes Vertrauensmodell für Apple erzwingen
- [ ] Eine gruppenbasierte Steuerung und Automatisierung des Lebenszyklus ist unkompliziert
- [ ] Für Apple Benutzer sind nur minimale manuelle Ausnahmebehandlungen erforderlich

Sicherheit:

- [ ] Die Sicherheitsrisiken und der Status von Apple werden in unseren Security-Operations-Workflows angezeigt
- [ ] Wir können Reaktionsmaßnahmen automatisieren (nicht nur Warnungen), indem wir die deklarative Geräteverwaltung (DDM) von Apple nutzen
- [ ] Die Berichte sind auf unsere internen Kontrollen und Prüfungen abgestimmt

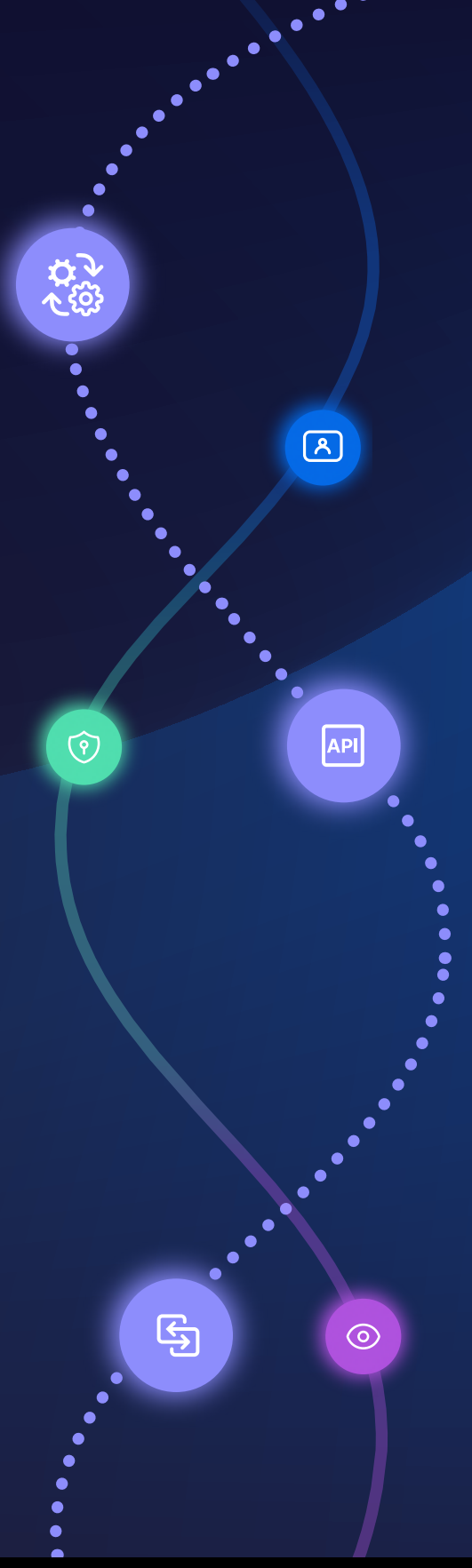
Transparenz:

- [ ] Das Apple-Inventar ist vollständig, genau und kann in CMDB/ITSM verwendet werden
- [ ] Wir können Workflows anhand des Zustands der Geräte (nicht anhand von Tabellenkalkulationen) in Echtzeit auslösen
- [ ] Daten bleiben konsistent, ohne dass eine manuelle Bereinigung notwendig ist

Wenn einer der Bereiche mit < 3 bewertet wurde, ist die Wahrscheinlichkeit groß, dass Sie auf manuelle Übergangslösungen, Integrationsrückstände und eine erschwerte Skalierbarkeit zusteuern.

jamf

Unternehmen erreichen erfolgreiche Integrationen mit Jamf



Jamf beschleunigt die Einführung von Apple mithilfe von unterstützten **Marketplace-Integrationen** und **flexiblen APIs** in den Bereichen Identität, Sicherheit und Transparenz. Dadurch werden Arbeitsabläufe rationalisiert, Integrationsschulden reduziert und Teams bei der Implementierung und Erweiterung von Apple mit Tools unterstützt, denen sie bereits vertrauen.

Verlassen Sie sich nicht nur auf unser Wort: Finden Sie heraus, warum Jamf in der IDC MarketScape als **Leader** eingestuft wurde: Worldwide Unified Endpoint Management Software for Apple Devices 2025-2026 Vendor Assessment