jamf

Mac Verwaltung und Sicherheit im Unternehmen

Das moderne Unternehmen entwickelt sich ständig weiter, und die Wahl der Technologie spielt eine entscheidende Rolle bei der Steigerung der Produktivität der Belegschaft und der Sicherheit des Unternehmens. Untersuchungen zeigen, dass Mitarbeiter:innen, die ihre Geräte selbst auswählen können, zufriedener, effizienter und engagierter sind - und dass mehr Fachleute als je zuvor Macs im Unternehmen bevorzugen.

Für die IT bringt dieser Wandel sowohl Chancen als auch Herausforderungen mit sich: Wie unterstützt man die Nutzer:innen mit der von ihnen bevorzugten Technologie und gewährleistet nahtloses Management und maximale Sicherheit bei gleichzeitiger Minimierung der Betriebsrisiken?

Obwohl macOS mit robusten, integrierten Sicherheitsfunktionen ausgestattet ist, erfordern Unternehmensumgebungen einen strukturierteren Ansatz für Verwaltung, Compliance und Risikominimierung. Wenn Ihre Geräteflotte schnell wächst, stehen IT-Teams vor der Herausforderung, ein nahtloses Nutzererlebnis aufrechtzuerhalten und gleichzeitig Sicherheitsbedenken auszuräumen. Sicherheitsteams verlassen sich oft auf Tools, die ursprünglich nicht für macOS entwickelt wurden, was eine angemessene Überwachung und Reaktion auf Vorfälle erschwert. Mit der richtigen Strategie lassen sich Workflows optimieren, die Produktivität steigern und Sicherheitsrisiken verringern. Gleichzeitig erhalten die Sicherheitsteams die nötige Transparenz in die Mac Flotte, um proaktiv und effektiv handeln zu können.

jamf

Dieser Leitfaden bietet IT-Führungskräften eine strategische Grundlage für die Verwaltung und Sicherung von Macs in großem Maßstab. Wir werden Folgendes behandeln:

Grundlagen der Mac Verwaltung: Grundprinzipien für die nahtlose Bereitstellung, Konfiguration und Verwaltung

Erweiterte Sicherheitsstrategien: Erweiterung des Schutzes über die nativen Funktionen von macOS hinaus, um die sich ständig weiterentwickelnden Sicherheitsrisiken im Unternehmen zu minimieren

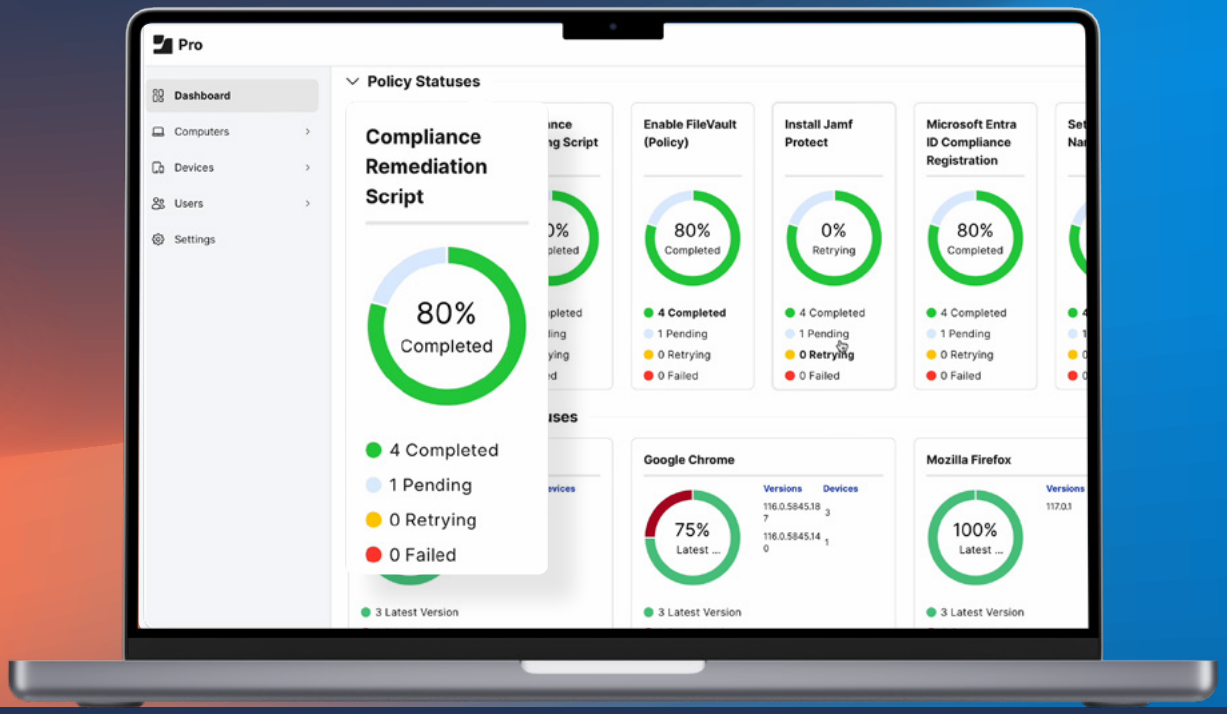
Lebenszyklus-Management: Einfacherer Umgang mit dem Mac von der Zero-Touch-Bereitstellung bis zum sicheren Offboarding

Integration der Infrastruktur: Gewährleistung einer reibungslosen Koexistenz mit Windows-Umgebungen und IT-Ökosystemen im Unternehmen

Best Practices für die Unternehmenssicherheit: Schutz von Unternehmensdaten, Geräten und Nutzer:innen mit Mac-optimierten Tools

Ganz gleich, ob Sie Macs in einer traditionell Windows-basierten Organisation einführen oder eine bestehende Apple Bereitstellung erweitern: Dieser Leitfaden vermittelt Ihnen die nötigen Kenntnisse, um die IT-Effizienz zu verbessern, die Sicherheit zu erhöhen und die Rentabilität Ihrer Mac-Investitionen zu maximieren - und das alles bei gleichzeitiger Minimierung der Betriebsrisiken.

Die moderne Mac Verwaltung: Grundprinzipien und Technologien



Die Entwicklung der Mac Verwaltung im Unternehmen

Macs sind zu einem Eckpfeiler des modernen Unternehmens geworden und bieten Sicherheit, Leistung und ein ausgezeichnetes Nutzererlebnis. Was einst als Nischenprodukt galt, das vor allem von kreativen Köpfen genutzt wurde, ist heute ein fester Bestandteil von IT-Ökosystemen im Unternehmen. Aufgrund der zunehmenden Verbreitung setzen IT-Führungskräfte auf fortschrittlichere Verwaltungsstrategien, um eine nahtlose Integration und Sicherheit zu gewährleisten, und wenden sich Mobile Device Management (MDM)-Lösungen zu, mit denen die Mac Verwaltung rationalisiert und automatisiert werden konnte.

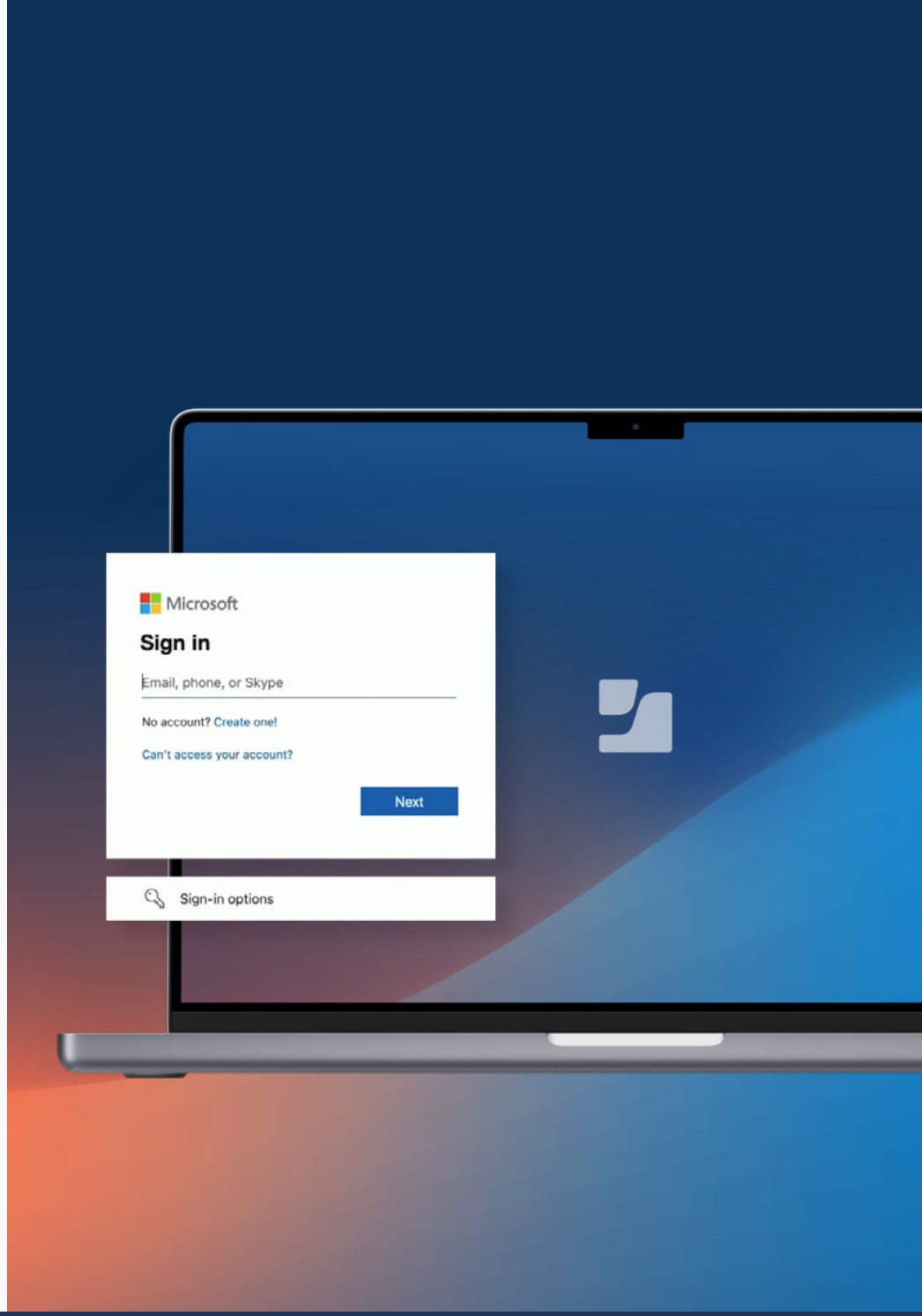
Doch durch den zunehmenden Einsatz von Macs stoßen die IT-Teams jedoch an die Grenzen der bisherigen MDM-Lösungen. Diese wurden in erster Linie für Windows entwickelt und haben Schwierigkeiten, sich vollständig an das sich schnell entwickelnde Ökosystem von Apple anzupassen. Die nahtlose Integration mit macOS Updates, die Unterstützung von Sicherheitsfunktionen und neuen Funktionalitäten ab dem ersten Tag sowie die Kompatibilität mit Apple-eigenen Workflows erfordert einen zielgerichteten Ansatz, der nur durch den Einsatz einer Apple-zentrierten Lösung möglich ist.

Diese Probleme machen deutlich, warum IT-Führungskräfte moderne Verwaltungslösungen benötigen, die sich nahtlos integrieren lassen, effizient skalierbar sind und die Sicherheit verbessern, während sie gleichzeitig ein reibungsloses Nutzererlebnis bieten. Obwohl viele IT-Experten mit der traditionellen PC-Verwaltung unter Verwendung von Microsoft-nativen Lösungen vertraut sind, bietet das macOS-Ökosystem viele Vorteile durch einen Ansatz, der die Produktivität steigert und gleichzeitig die Sicherheit auf dem Mac maximiert. Da Unternehmen ihre Windows-zentrierten Strategien hinter sich lassen, erkennen sie Macs zunehmend als Motor für Effizienz und Mitarbeiterzufriedenheit an. Um diese Vorteile voll ausschöpfen zu können, muss die IT jedoch eine proaktive, skalierbare und auf Apple zugeschnittene Verwaltungsstrategie einführen, die die sich ständig weiterentwickelnde Unternehmenslandschaft unterstützt.

Für IT-Führungskräfte muss eine effektive Mac Verwaltung mit den wichtigsten Geschäftszielen in Einklang stehen:

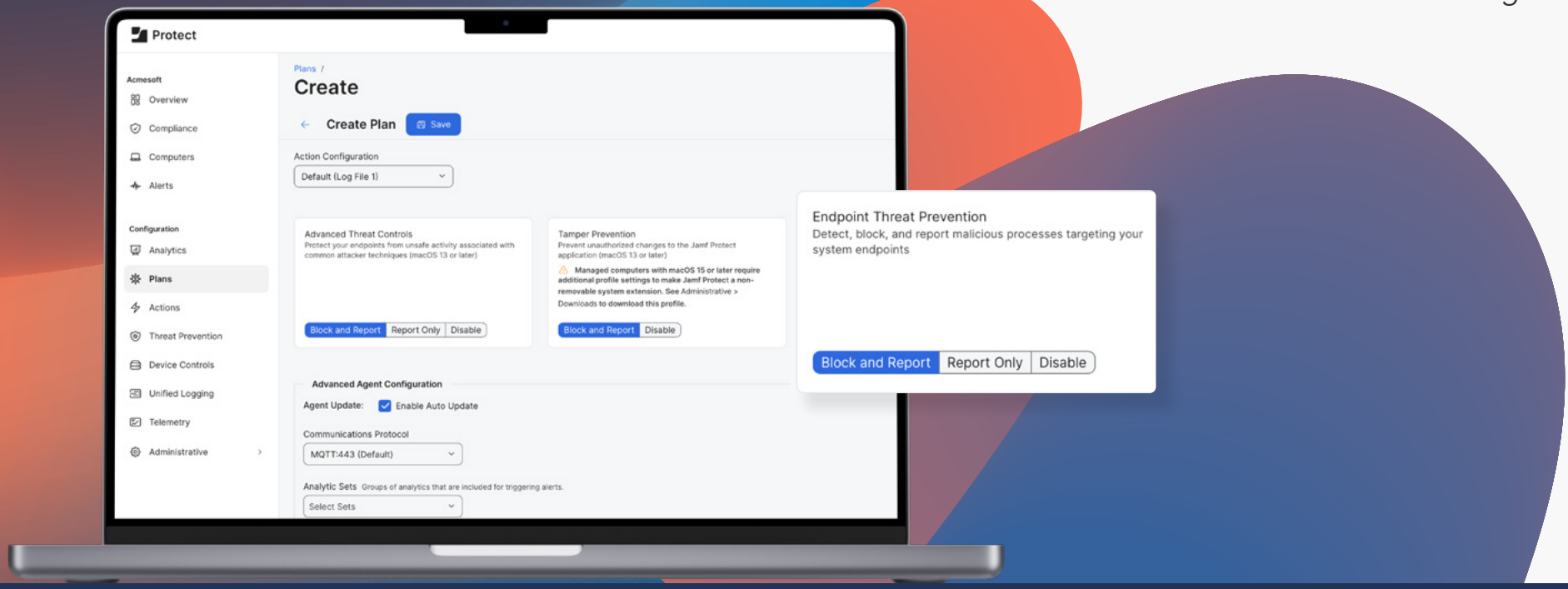
- **Produktivitätssteigerung:** Durch die optimierte Einrichtung von Geräten, Updates und Support werden Ausfallzeiten reduziert und die Mitarbeiter:innen können effizienter arbeiten.
- **Risikominimierung:** Die aktive Überwachung von Endpoints, das Aufrechterhalten der Compliance durch Sicherheitsrichtlinien und das Automatisieren von Aufgaben zur Wiederherstellung nach einem Vorfall minimieren Bedrohungen für das Unternehmen.

Unter Berücksichtigung dieser Grundsätze dreht sich eine moderne Mac-Verwaltungsstrategie um die MDM- und Sicherheitsframeworks von Apple, die einen strukturierten Ansatz für die Bereitstellung, Sicherung und Wartung von Mac-Geräten im großen Maßstab bieten.



Grundlagen der Mac Verwaltung: **Ein strategischer Ansatz für Unternehmen**

Mit den folgenden Grundprinzipien können IT-Führungskräfte eine nahtlose Bereitstellung, Konfiguration und Verwaltung von Macs sicherstellen und gleichzeitig die erwartete Benutzerfreundlichkeit und Sicherheit aufrechterhalten, ohne die Privatsphäre der Nutzer:innen zu beeinträchtigen.



Zero-Touch-Bereitstellung: Automatisieren und skalieren

Ein optimierter Onboarding-Prozess ist entscheidend für die Effizienz, die Sicherheit und die Benutzerzufriedenheit. Mithilfe der Zero-Touch-Bereitstellung kann die IT die Macs konfigurieren und bereitstellen, noch bevor das Gerät ausgepackt wurde. Dadurch entfällt die manuelle Einrichtung und der IT-Aufwand wird reduziert. Zu den wichtigsten Faktoren gehören:

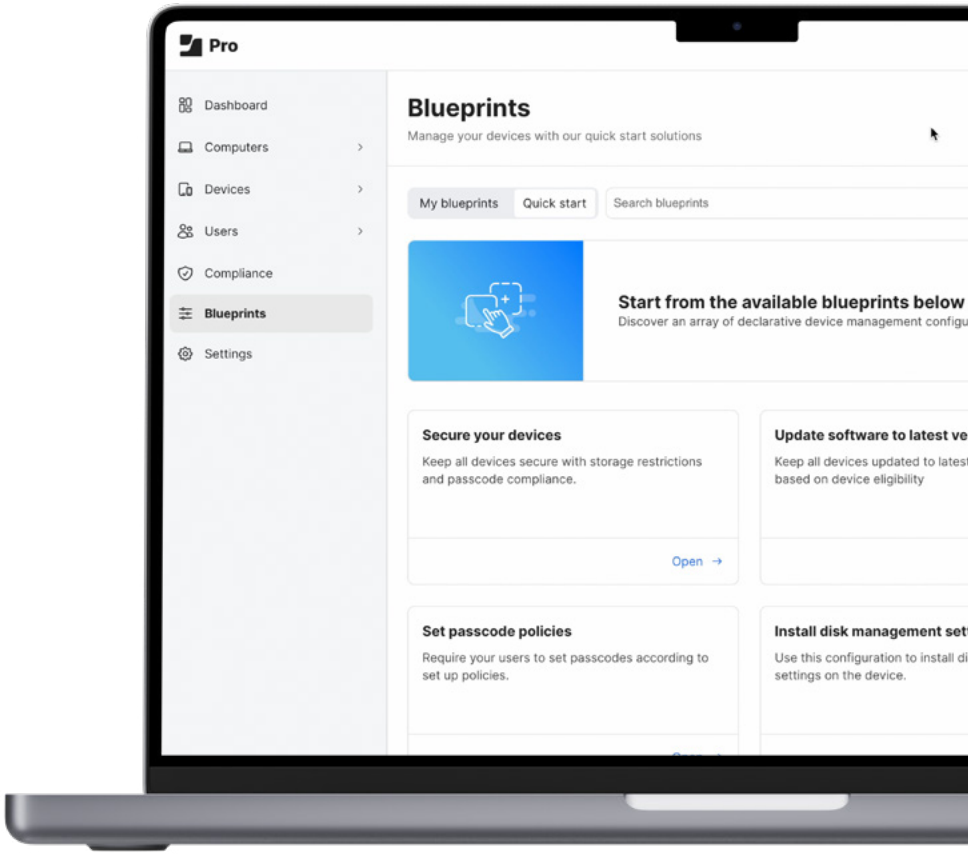
- **Automatisierte Registrierung und Anpassung**
- **Account-Bereitstellung und -Verwaltung**
- **Just-in-time-Onboarding für macOS**

Durch die Automatisierung kann die IT die Mitarbeiter:innen schneller einbinden, die Sicherheit ab dem ersten Einschalten des Geräts verbessern und die freigeetzten Ressourcen für strategische Initiativen nutzen, die den Geschäftsbetrieb unterstützen und steigern, und gleichzeitig ein einwandfreies Onboarding-Erlebnis bieten, das die Produktivität umgehend steigert.

Zentralisierte Einstellungen und Konfiguration: Wahrung der Konsistenz bei Skalierung

Um die Sicherheit und Konformität einer wachsenden Mac Flotte zu gewährleisten, ist ein zentralisierter, richtliniengesteuerter Ansatz erforderlich. Die IT muss Konfigurationen einrichten und durchsetzen, die die Einheitlichkeit wahren und gleichzeitig die Geschäftsanforderungen unterstützen. Zu den wichtigsten Strategien gehören:

- **Blueprints**
- **Smart Groups**
- **Sicherheitsbefehle und Beschränkungen aus der Ferne**
- **Integration von Apple Business Manager (ABM)**



App- und Patch-Verwaltung: Risiko reduzieren + Produktivität steigern

Durch die Standardisierung von Software-Bereitstellung und Patch-Verwaltung reduziert die IT Sicherheitslücken, minimiert Ausfallzeiten und unterstützt neue Funktionen und Funktionalitäten zur Unterstützung und Steigerung der Produktivität der Nutzer:innen Erschließen Sie die Leistungsfähigkeit von Apps für Ihre Nutzer:innen mit:

- **Automatisierter App-Bereitstellung**
- **Durchsetzung von Patches**
- **App-Katalog**
- **Sicherheit von Inhalten und Geräten auf Abruf**

Sicherheit und Compliance auf Unternehmensebene: Schützen Sie, was wichtig ist

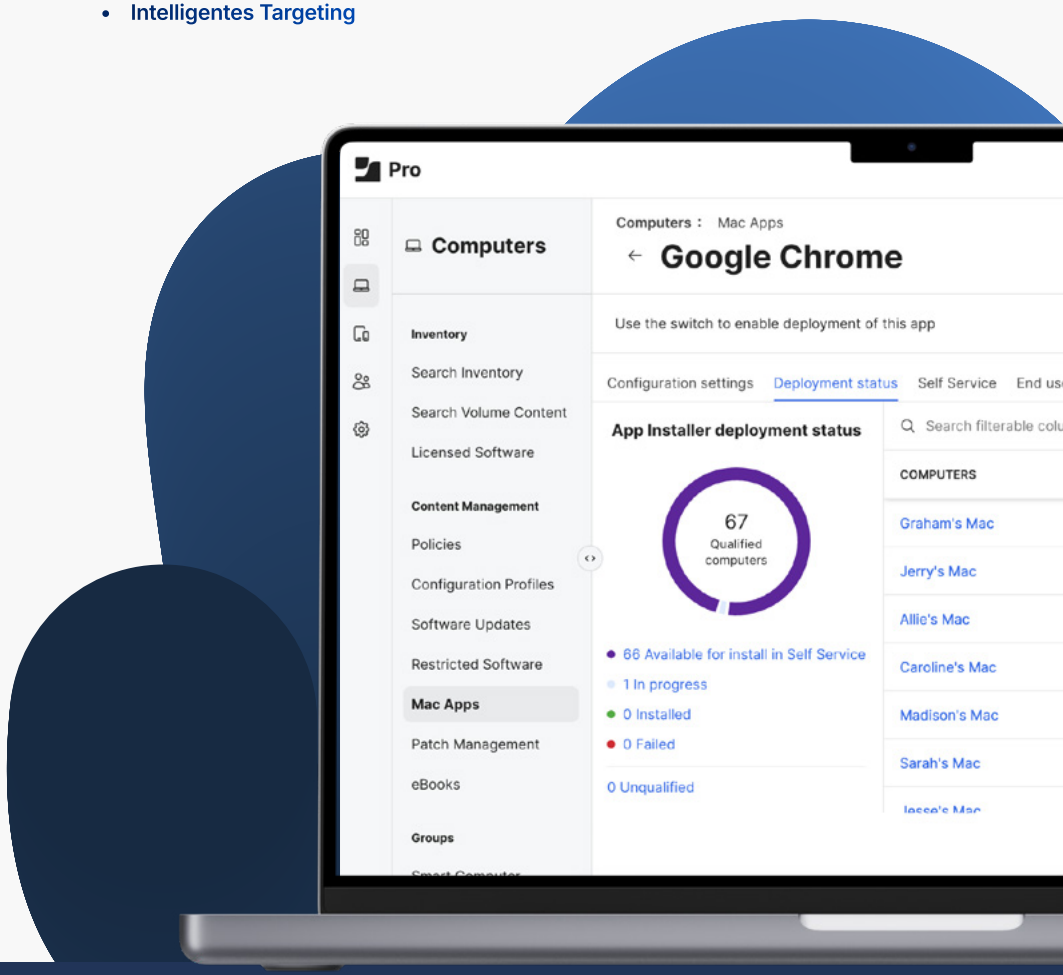
Trotz der starken Sicherheits- und Datenschutzfunktionen von macOS sind zusätzliche Schutzmaßnahmen erforderlich, um den Sicherheitsstandards im Unternehmen und den Compliance-Bestimmungen der jeweiligen Industrie gerecht zu werden. Eine moderne Strategie für Mac Sicherheit beinhaltet:

- **Endpoint-Schutz und Compliance**
- **Identitäts- und Zugangsverwaltung (IAM)**
- **Erkennung von Bedrohungen und Reaktion auf Vorfälle**
- **Schutz vor netzwerkbasierten Bedrohungen**
- **Zero-Trust-Netzwerkzugriff (ZTNA)**

Berichterstattung und Sichtbarkeit

Die Verwaltung des gesamten Lebenszyklus eines Macs, von der Beschaffung bis zur Außerbetriebnahme, sorgt für langfristige Kosteneinsparungen und Betriebseffizienz. Außerdem wird das Risiko von Datenverlusten durch verloren gegangene Geräte minimiert. Zu den wichtigsten Faktoren gehören:

- **Bestandsverwaltung**
- **App-Berichte**
- **Intelligentes Targeting**



Vorteile im Unternehmen: **Warum die IT bei der Umstellung eine Vorreiterrolle spielen muss**

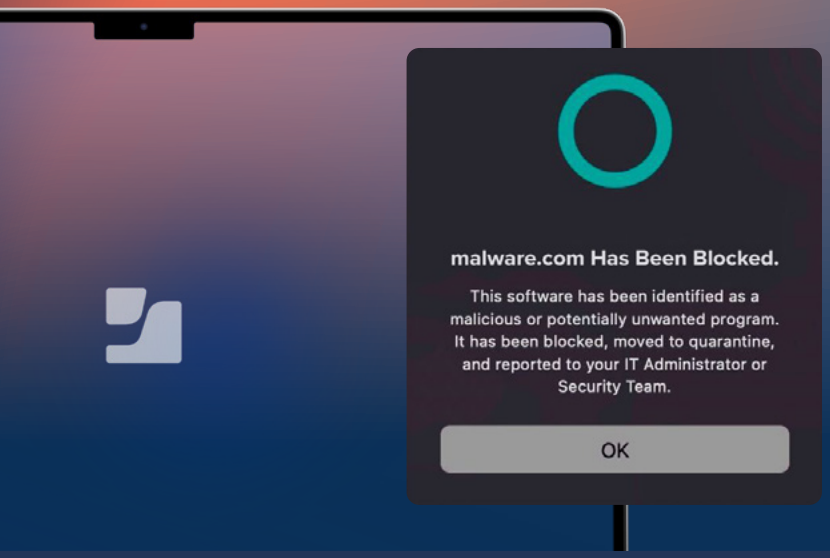
Durch den zunehmenden Einsatz von Macs im Unternehmen haben IT-Führungskräfte die Möglichkeit, die Strategien für die Unternehmensverwaltung neu zu definieren. Durch die Implementierung eines Apple-nativen, proaktiven und automatisierten Ansatzes kann die IT:

- die Sicherheit verbessern und die Compliance durchsetzen, während die Komplexität minimiert wird
- die Nutzerproduktivität durch nahtlose Workflows steigern, die das Macs-Erlebnis aufrechterhalten
- den IT-Overhead durch Automatisierung und optimierte Abläufe reduzieren

Wenn IT-Führungskräfte diese Grundlagen der Mac Verwaltung beherzigen, können sie die Einführung des Macs zu einem strategischen Vorteil machen und von weiteren Vorteilen profitieren, z. B:

- Höhere Effizienz und Sicherheit bei gleichzeitiger Unterstützung der Geschäftsabläufe.
- **Senkung der Gesamtbetriebskosten** (TCO) im Vergleich zu anderen Anbietern von Hardware
- **Erhöhung des Return On Investment** (ROI) durch die Verwaltung und Sicherung von Macs in großem Umfang

Erweiterte Sicherheitsstrategien: **Ausweitung des Schutzes über die macOS-eigenen Funktionen hinaus, um die Risiken im Unternehmen zu minimieren**



Die Bedeutung von Sicherheit bei der Verwaltung von Macs in Unternehmen

Mit der zunehmenden Verbreitung von Macs in Unternehmen steigen auch die Herausforderungen für die Sicherheit, die mit der Verwaltung einer vielfältigen und verteilten Belegschaft einhergehen. Auch wenn macOS einen starken integrierten Schutz bietet, reicht es nicht aus, sich auf die standardmäßigen Sicherheitsmaßnahmen zu verlassen, um Daten im Unternehmen zu schützen, zumal Cyberkriminelle immer häufiger Macs angreifen. IT-Führungskräfte müssen eine umfassende, mehrschichtige Sicherheitsstrategie umsetzen, die Folgendes umfasst:

- **Endpoint-Schutz**
- **Identity and Access Management (IAM)**
- **Grundlegende Sicherheitskonfigurationen**
- **Aktive Überwachung und Berichterstattung**
- **Durchsetzung der Compliance**

Durch einen proaktiven Schutz der Macs mit automatisierten Patches, Zero-Trust Frameworks und Erkennung von Bedrohungen in Echtzeit können Organisationen Risiken minimieren, die Einhaltung von Vorschriften durchsetzen und Unternehmensressourcen schützen. Eine umfassende Sicherheitsstrategie ist nicht nur eine Priorität der IT, sondern auch eine wesentliche Voraussetzung für die Schaffung einer Grundlage, die die Cyber-Resilienz gegenüber einer sich ständig weiterentwickelnden Bedrohungslandschaft stärkt und mit der Geschäftskontinuität in Einklang steht und diese unterstützt.

Verwalteter Lebenszyklus des Geräts: Von Anfang bis Ende

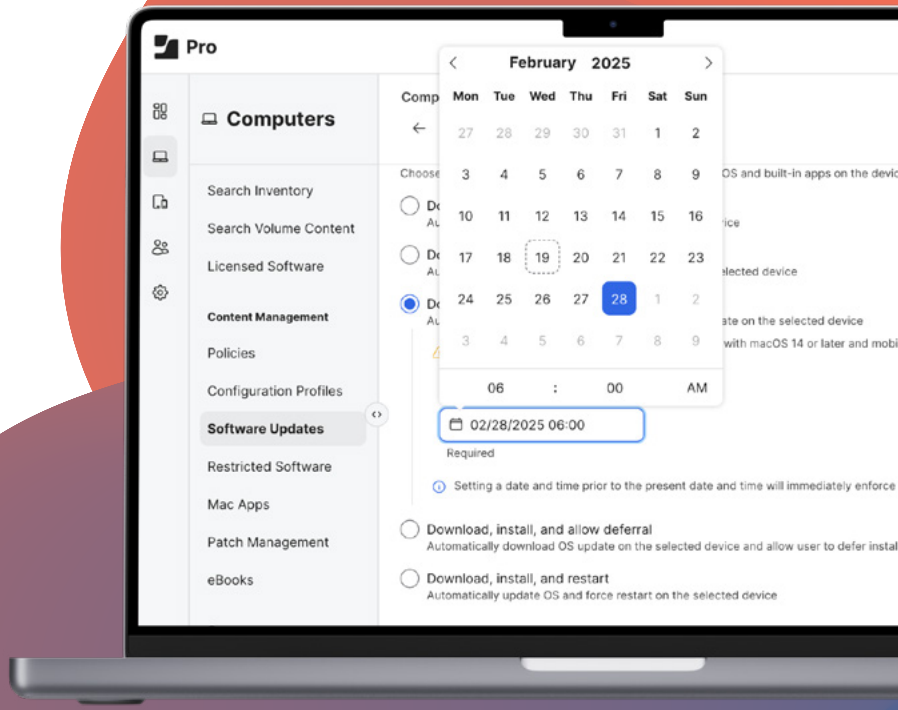
Die Sicherheit im Unternehmen erfordert, dass alle Geräte, die für die Arbeit verwendet werden und eine Verbindung zu Unternehmensressourcen herstellen, hinsichtlich des Risikos, das sie für die Unternehmensressourcen darstellen, gleich behandelt werden. Der Schlüssel dazu ist die Konsistenz während des gesamten Lebenszyklus des Geräts, um sicherzustellen, dass keine Sicherheitslücken entstehen, von der Beschaffung über die Bereitstellung der Konfiguration bis hin zur Überwachung der Compliance, zur kontinuierlichen Patch-Verwaltung und schließlich zur Außerbetriebnahme, wo der Lebenszyklus von neuem beginnt. IT-Vorteile, die durch die Konsistenz ermöglicht werden, sind:

- **Sicherheit auf ganzer Linie**
- **Aufrechterhaltung der Kontrollparität**
- **Vorgaben für Workflows**
- **Konstante Bescheinigung für das Gerät**

Festlegung eines grundlegenden Sicherheitsstatus

Die Festlegung der Grenzen dessen, was in Ihrem Unternehmen als normaler Betrieb angesehen wird, bietet einen verifizierten Abgrenzungspunkt. Darüber hinaus müssen IT-Verantwortliche in regulierten Industrien sicherstellen, dass Geräte und die Mitarbeiter:innen, die sie für die Arbeit mit geschützten Datentypen verwenden, bestimmte Gesetze einhalten, die regeln, wie Daten, Prozesse und Arbeitsabläufe gesichert werden müssen, um Verstöße zu vermeiden. Zu den wichtigsten Compliance-Faktoren gehören:

- **Anpassung an Standards und Frameworks**
- **Dokumentation der Compliance gegenüber Auditor:innen**
- **Benachrichtigungen in Echtzeit**
- **Richtlinienbasierte Durchsetzung**



Stoppen Sie anspruchsvolle Bedrohungen mit anspruchsvollen Technologien

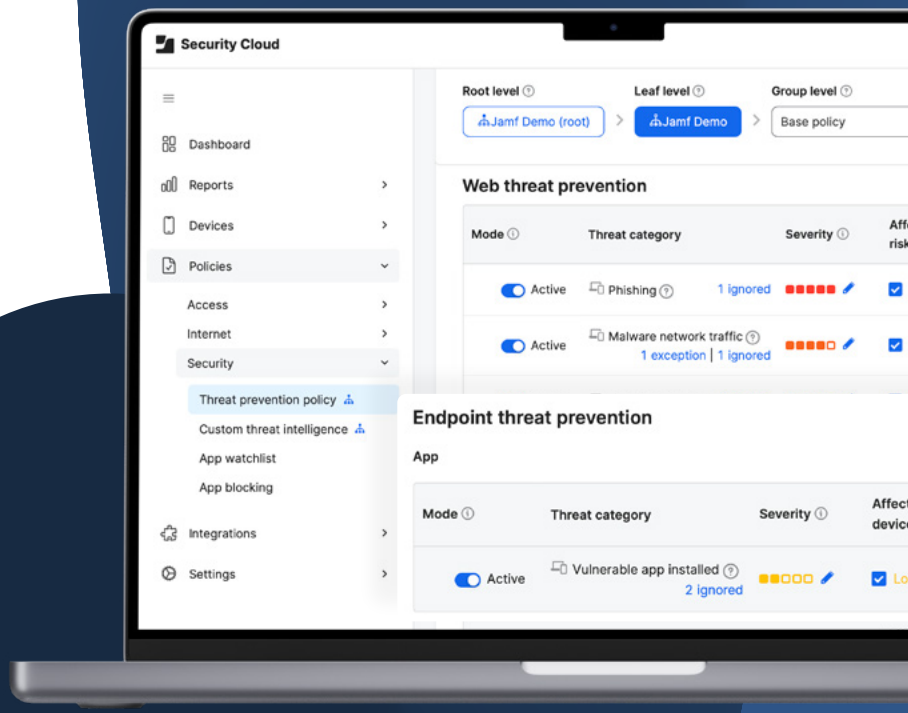
Bedrohungsakteure entwickeln ihre Tools ständig weiter und nutzen die Vorteile der künstlichen Intelligenz (KI), um fortschrittliche Bedrohungen zu entwickeln, die mit herkömmlichen Endpoint-Schutzmaßnahmen nur schwer zu erkennen und zu bekämpfen sind. Moderne Bedrohungsprävention und -abwehr erfordert fortschrittliche Technologien wie Maschinelles Lernen (ML), um Unternehmen dabei zu helfen, immer einen Schritt voraus zu sein. Mithilfe von KI-Technologien können Admin-Teams anspruchsvolle Bedrohungen schneller und einfacher erkennen und abwehren:

- **Zero-Day-Bedrohungen entdecken**
- **netzwerkbasierte Angriffe blockieren**
- **dynamische Anpassung der Schutzmaßnahmen**
- **Telemetrie im großen Maßstab skalieren**

Zero Trust, um Cyberkriminellen keine Angriffsfläche zu geben

IT-Führungskräfte wissen, dass es nur eine einzige Kompromittierung braucht, um eine Datenverletzung zu verursachen. Angesichts derart hoher Risiken ist es von entscheidender Bedeutung, dass jede Zugangsanfrage überprüft wird, um sicherzustellen, dass die Anmeldeinformationen des Benutzers oder des Geräts jedes Mal den grundlegenden Sicherheitsstatus aufrechterhalten. Beispiele dafür, wie Zero-Trust-Netzwerkzugriff (ZTNA) einen starken Sicherheitsstatus aufrechterhält, sind:

- **Zustand des Endpoints überprüfen**
- **netzwerkbasierte Bedrohungen stoppen**
- **Verbindungen isolieren und verschlüsseln**
- **Automatische Workflows für die Wiederherstellung nach einem Cyberangriff**



Durchsetzung der Compliance: Damit die Technik sicher bleibt

Die Anpassung der Geschäftsabläufe an organisatorische Standards oder Industrievorschriften gibt Unternehmen die Gewissheit, dass Geräte, Daten, Nutzer:innen, Prozesse und Workflows den etablierten Richtlinien entsprechen, die für ihre Sicherheit sorgen. Die Einhaltung von Richtlinien liefert der IT-Abteilung wertvolle Anhaltspunkte dafür, dass die Endgeräte ordnungsgemäß konfiguriert und die Sicherheitskontrollen aktiviert sind:

- Härtungskonfigurationen
- Sicherheitsanalytik
- Festlegung von Baselines
- Auditberichte

Erweiterungen der Lösungen durch Deep Integration

Entscheidungen werden nicht oft im luftleeren Raum getroffen. Genauso ist es mit der Sicherheit. Eine Lösung, egal wie leistungsstark sie ist, reicht nicht aus, um die verschiedenen Arten von Bedrohungen abzuwehren, denen Unternehmen heute ausgesetzt sind, und gleichzeitig die Funktionen des Betriebssystems nativ zu unterstützen. Beides ist erforderlich, und oft sind zusätzliche Lösungen notwendig, um die besonderen Anforderungen im Unternehmen zu erfüllen. Entscheidende Vorteile, die Unternehmen durch die Integration von Lösungen erzielen können, sind:

- Zentralisierung der Bedrohungsanalysen
- Automatisierte Behebung von Schwachstellen
- Implementierung von Conditional Access
- Anpassung von Support-Workflows

Schnellere Reaktionszeiten auf Vorfälle + Bedrohungssuche = Weniger Risiko

Sicherheitsstrategien sind nicht narrensicher und manchmal kommen Bedrohungen durch. In diesen Fällen ist die Zeit entscheidend. Sie stellt die Verbindung zwischen Risikominimierung und Datenverlust dar. Ein umfassender Sicherheitsplan beinhaltet Strategien zur Reaktion auf Vorfälle und zur Erkennung von Bedrohungen, um bekannte Risiken zu minimieren und unbekannte Bedrohungen, die sich traditionellen Endpoint-Security-Lösungen entziehen können, zu erkennen Zu den wichtigsten Strategien zur beschleunigten Reaktion auf Vorfälle und der Suche nach Bedrohungen gehören:

- Einrichtung sicherer Basislines
- Sicherer Austausch von Telemetriedaten
- Automatisierte Triage und Reaktion
- Integration von AI/ML Technologien

Schulungen für Mitarbeiter:innen zu Best Practices im Bereich Sicherheit

IT-Führungskräfte wissen, dass jede Kontrolle, Konfiguration und Richtlinie nur ein Teil eines größeren Sicherheitspuzzles ist. Jedes Puzzle ist einzigartig für das Unternehmen. Jede Kontrolle ist auf die jeweiligen Anforderungen und Risikobewertungsbedürfnisse zugeschnitten.

Eine Maßnahme, die für eine Defense-in-Depth-Strategie von entscheidender Bedeutung ist, die aber keine Sicherheitskontrolle, sondern eine administrative Kontrolle darstellt, ist die Schulung der Endnutzer:innen. Obwohl die Nutzer:innen oft als Schwachstellen in der Sicherheitskette angesehen werden, können sie auch eine wirksame erste Verteidigungslinie darstellen. Mit den richtigen Schulungen und der richtigen Sensibilisierung können die Nutzer:innen einen wichtigen Beitrag zu einer stärkeren, widerstandsfähigeren Sicherheitsumgebung leisten. Obwohl die Nutzer:innen oft als Schwachstellen in der Sicherheitskette angesehen werden, können sie auch eine wirksame erste Verteidigungslinie darstellen. Mit den richtigen Schulungen und der richtigen Sensibilisierung können die Nutzer:innen einen wichtigen Beitrag zu einer stärkeren, widerstandsfähigeren Sicherheitsumgebung leisten. Und selbst wenn eine Bedrohung die Unternehmensabwehr durchbricht, bietet die Kombination aus einem umfassenden Sicherheitsplan und Schulungen zum Sicherheitsbewusstsein den Unternehmen die Möglichkeit, Bedrohungen schnell zu entschärfen, da die Mitarbeiter:innen wissen, was sie tun und was sie nicht tun dürfen.

IT-Führungskräfte, die ihre Sicherheitspläne durch Schulungen für Endnutzer:innen ergänzen, schaffen eine Sicherheitskultur, die alle Aspekte der Unternehmensverwaltung und -sicherheit im Unternehmen abdeckt. Diese Kultur macht den Unterschied aus, wenn es darum geht, bestimmte Arten von Angriffen zu stoppen, bevor sie ausgeführt werden können, doch dazu müssen die Nutzer:innen nur geschult werden in:

- **Bereitstellung von Informationen über aktuelle Bedrohungen**
- **Proaktive Verbesserung der Sicherheitshygiene**
- **Durchführung von regelmäßigen Backups und Datenschutz**
- **Festlegung von Sicherheitsrichtlinien und Leitlinien für Nutzer:innen**
- **die Mitarbeiter:innen zu einem Teil der Lösung machen, z. B. durch Verbesserung der Reaktion auf Zwischenfälle**

Fazit und nächste Schritte

Die Rolle der IT-Führungskräfte entwickelt sich ebenso weiter wie die Verwaltung und Sicherheit für Macs. Es erfordert einen scharfen Blick und ein klares Verständnis der Risiken, um ihre Strategien bestmöglich an die sich ständig verändernde Landschaft anzupassen. Nur wenn Sie verstehen, dass sich Risiken ständig ändern, und dieses Verständnis mit nativen Technologien kombinieren, die speziell für macOS entwickelt wurden, können Sie die effektivsten Lösungen für die Verwaltung und Sicherung Ihrer Mac Flotte im Unternehmen entwickeln.

Lösungen, die die einzigartigen Bedürfnisse und Anforderungen Ihres Unternehmens und damit auch seiner Geräte, Daten und Stakeholder übertreffen - und nicht nur minimal unterstützen.

Zusammenfassung der wichtigsten Tipps für die Mac Verwaltung und Sicherheit

Das Schließen von Sicherheitslücken erfordert ein modernes Cybersicherheitskonzept. Umfassende Schutzmaßnahmen, die die Sicherheit und den Datenschutz auf alle Geräte, Nutzer:innen und Daten in Ihrer gesamten Infrastruktur ausweiten. Eine leistungsstarke Defense-in-Depth-Lösung, die Verwaltung, Identität und Sicherheit beinhaltet.

Die wichtigsten Aspekte für eine ausgeglichene Mac Verwaltung und Sicherheit sind:

- **Entwicklung ganzheitlicher Strategien, die sich über den gesamten Lebenszyklus der Geräte erstrecken**
- **Integration von Verwaltungs-, Identitäts- und Sicherheitslösungen zur Automatisierung umfassender Verwaltungs- und Sicherheitsworkflows**
- **Automatisierung des Onboardings von Geräten zur Skalierung durch Zero-Touch-Bereitstellungen**
- **Schaffung einer Baseline von sicheren Konfigurationen, die sich an Standards und Frameworks orientieren**
- **Standardisierung von App-Bereitstellungen und Patch-Verwaltungszyklen**
- **Abwehr von geräte- und netzwerkbasierten Bedrohungen mit Endpoint-Schutz und ZTNA**
- **Überwachung des Zustands von Endpoints mit Sichtbarkeit in Echtzeit zur Abwehr bekannter Bedrohungen**
- **Durchsetzung der Compliance durch automatisierte richtlinienbasierte Verwaltungsworkflows**
- **Datengestützte Entscheidungen durch gemeinsame Telemetrie, um Risiken zu minimieren**
- **Identifizierung unbekannter Bedrohungen und schnelle Reaktion auf Vorfälle durch KI/ML-basierte fortschrittliche Technologien und Automatisierung, um Schwachstellen zu entschärfen und zu beheben**
- **Schulungen der Nutzer:innen zum Sicherheitsbewusstsein als Teil einer umfassenden Lösung, damit sie nicht zur Ursache des Problems werden**