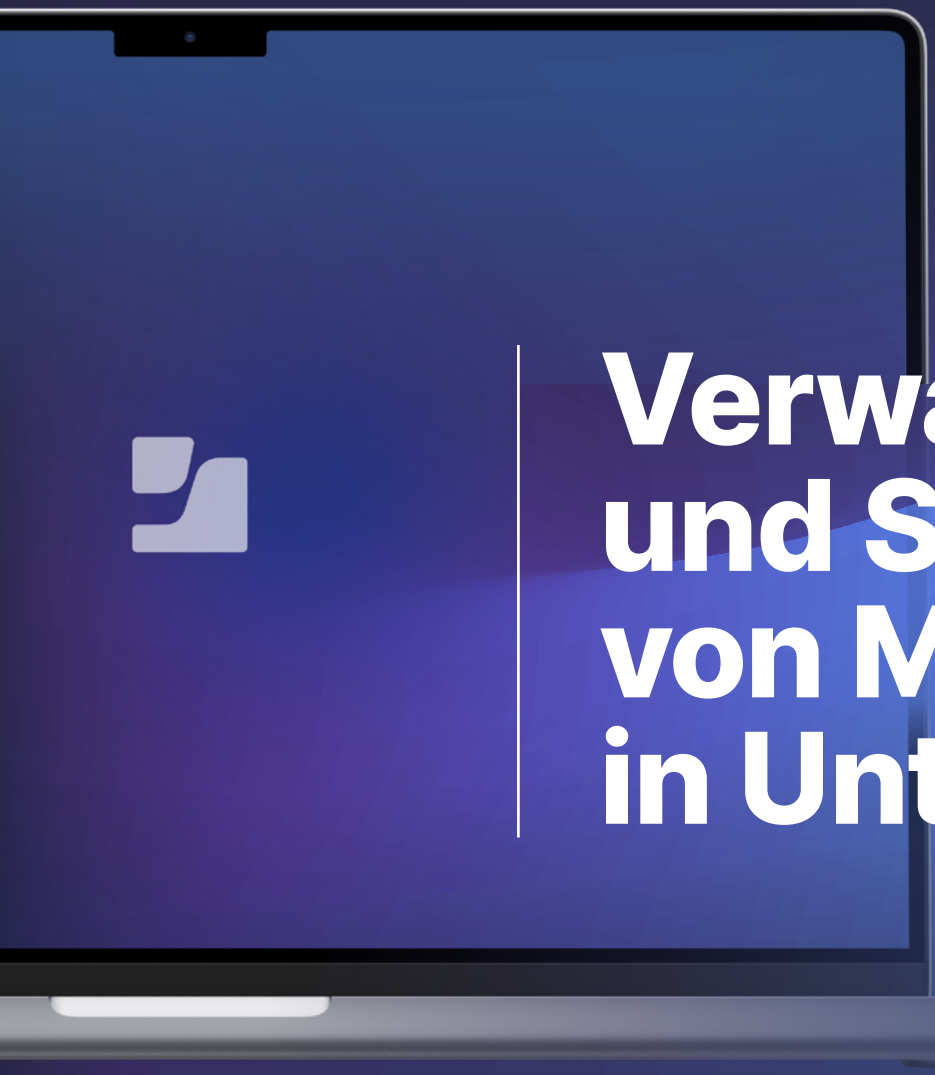
jamf



Verwaltung und Sicherheit von Macs in Unternehmen

Florierende Unternehmen passen sich an neue Arbeitsweisen an, und die Wahl der Technologie spielt heute eine wichtige Rolle, wenn die Produktivität gesteigert und die Sicherheit verbessert werden sollen Untersuchungen zeigen, dass Mitarbeiter, die ihre Geräte frei wählen können, zufriedener, effizienter und engagierter sind - und dass immer mehr Menschen einen Mac für die Arbeit bevorzugen.

Für die IT bringt dieser Wandel sowohl Chancen als auch Herausforderungen mit sich: Wie unterstützt man die Benutzer 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 moderne Umgebungen einen einfachen, konsistenten Ansatz für Verwaltung, Konformität und Sicherheit. Wenn sich die Anzahl Ihrer Geräte erhöht, müssen die IT-Teams dafür sorgen, dass die Geräte einwandfrei funktionieren und dass sie sicher sind. Die Unternehmen verlassen sich dabei oft auf Tools, die nicht von Haus aus für macOS entwickelt wurden, was es schwieriger macht, eine angemessene Geräteüberwachung und Reaktion auf Vorfälle sicherzustellen. 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-Teams eine strategische Grundlage für die Verwaltung und den Schutz 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

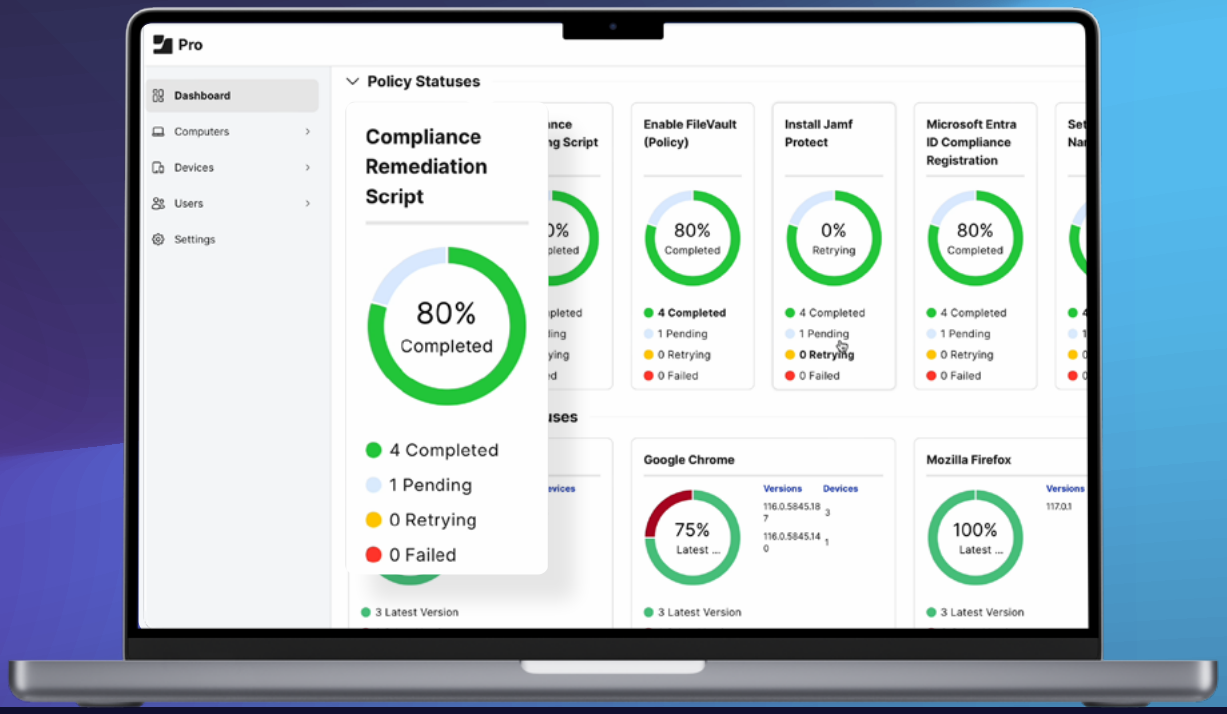
Lebenszyklus-Management: Einfacherer Umgang mit dem Mac von der Zero-Touch-Bereitstellung bis zum sicheren Offboarding

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 Benutzern mit Mac-optimierten Tools

Ganz gleich, ob Sie Macs in einer traditionell Windows-basierten Organisation einführen oder eine bestehende Apple Umgebung erweitern: Dieser Leitfaden vermittelt Ihnen die nötigen Kenntnisse, um die IT-Effizienz und die Benutzerfreundlichkeit 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 in Unternehmen

Macs sind zu einem Eckpfeiler des modernen Unternehmens geworden und bieten Sicherheit, Leistung und ein ausgezeichnetes Benutzererlebnis. Was einst als Nischenprodukt galt, das vor allem von kreativen Köpfen genutzt wurde, ist heute ein fester Bestandteil in modernen IT-Umgebungen. Aufgrund der zunehmenden Verbreitung setzen IT-Admins 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.

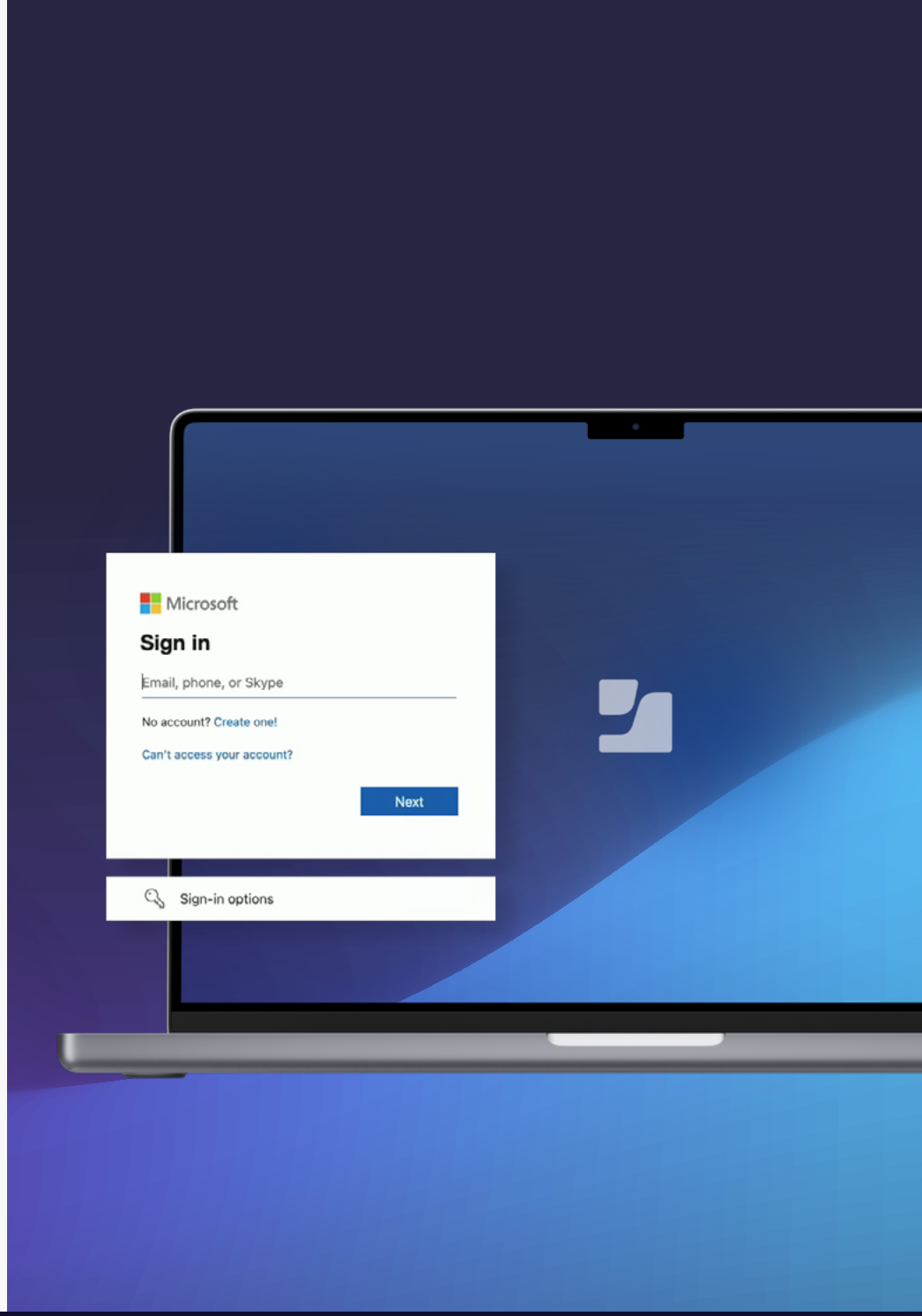
Doch durch den zunehmenden Einsatz von Macs stoßen die IT-Teams jedoch an die Grenzen der bisherigen MDM-Lösungen. Diese wurden in erster Linie für Windows entwickelt und haben Schwierigkeiten, sich vollständig an das sich schnell entwickelnde Ökosystem von Apple anzupassen. Die nahtlose Integration 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-Teams moderne Verwaltungslösungen benötigen, die sich nahtlos integrieren lassen, effizient skalierbar sind und die Sicherheit verbessern, während sie gleichzeitig ein reibungsloses Benutzererlebnis 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-Abteilung jedoch eine proaktive, skalierbare und auf Apple zugeschnittene Verwaltungsstrategie einführen, die den Anforderungen wachsender Unternehmen gerecht wird.

Eine effektive Mac Verwaltung muss mit den wichtigsten Geschäftszielen in Einklang stehen:

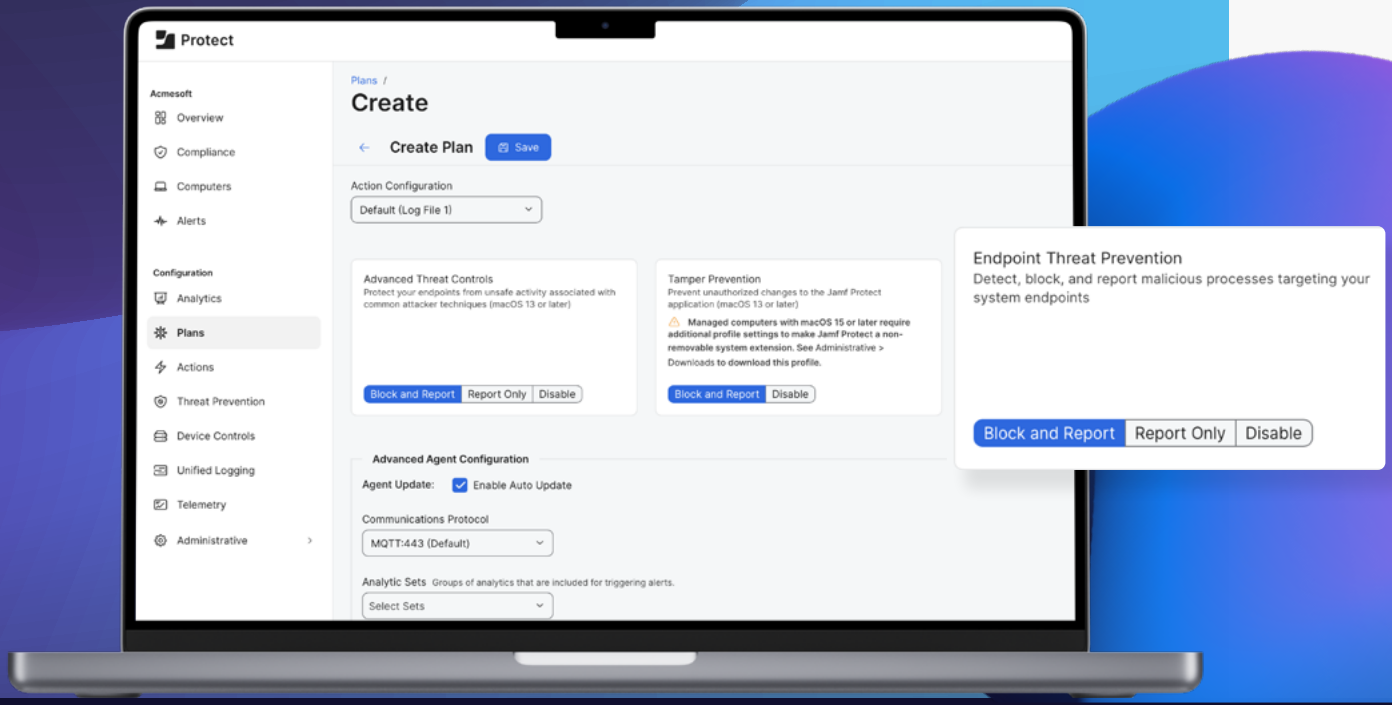
- **Produktivitätssteigerung:** Durch die optimierte Einrichtung von Geräten, Updates und Support werden Ausfallzeiten reduziert und die Mitarbeiter:innen können effizienter arbeiten.
- **Risikominimierung:** Die aktive Überwachung von Endpunkten, das Aufrechterhalten der Konformität durch Sicherheitsrichtlinien 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 bieten, wenn Ihr Unternehmen expandiert.



Grundlagen des Mac Managements: **Ein strategischer Ansatz für wachsende Unternehmen**

Mit den folgenden Grundprinzipien können IT-Teams eine nahtlose Bereitstellung, Konfiguration und Verwaltung von Macs sicherstellen und gleichzeitig die von den Mitarbeitern erwartete Benutzerfreundlichkeit sowie ein hohes Maß an Sicherheit gewährleisten, ohne die Privatsphäre der Benutzer 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:

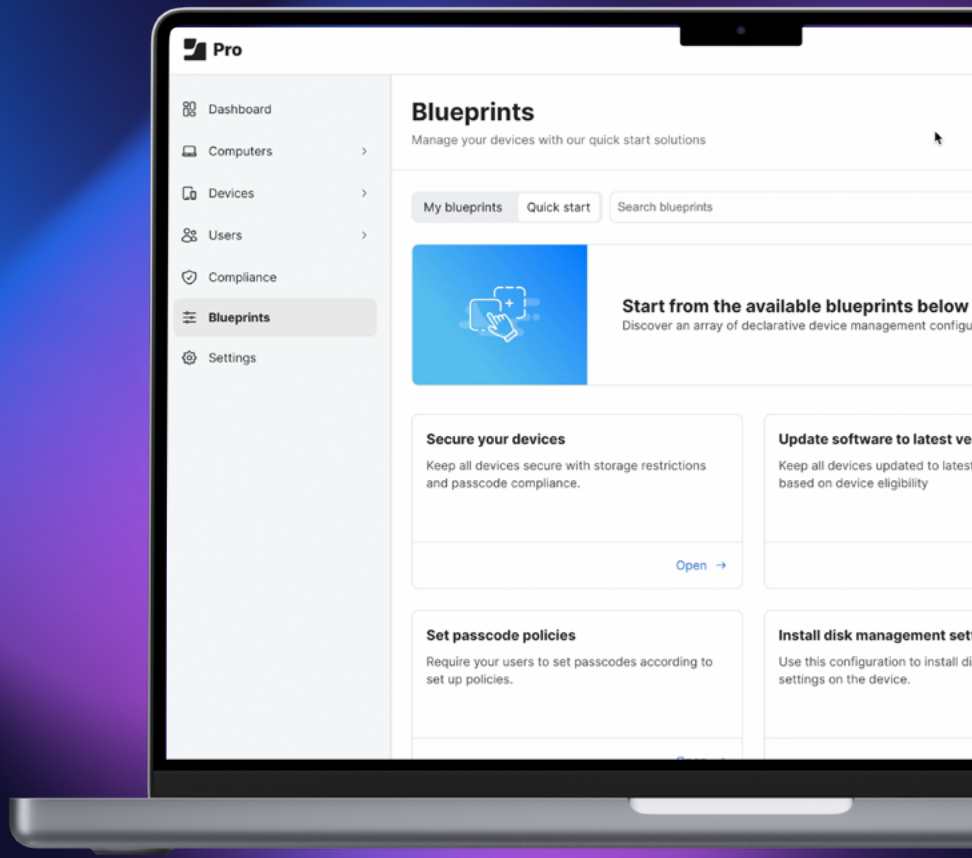
- **Automatisierte Registrierung und Anpassung**
- **Account-Bereitstellung und -Verwaltung**
- **Just-in-time-Onboarding für macOS**

Durch die Automatisierung kann die IT-Abteilung neue Mitarbeiter schneller einarbeiten, die Sicherheit ab dem ersten Einschalten des Geräts verbessern und ihre Zeit für strategischere IT-Aufgaben nutzen. Außerdem verläuft das Onboarding viel reibungsloser und die Mitarbeiter können gleich viel produktiver arbeiten.

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:

- **Entwürfe**
- **Dynamische Gruppen**
- **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 Profitieren Sie von leistungsfähigen Apps für Ihre Benutzer mit:

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

Grundlegenden Sicherheit und Konformität: Schützen Sie, was wichtig ist

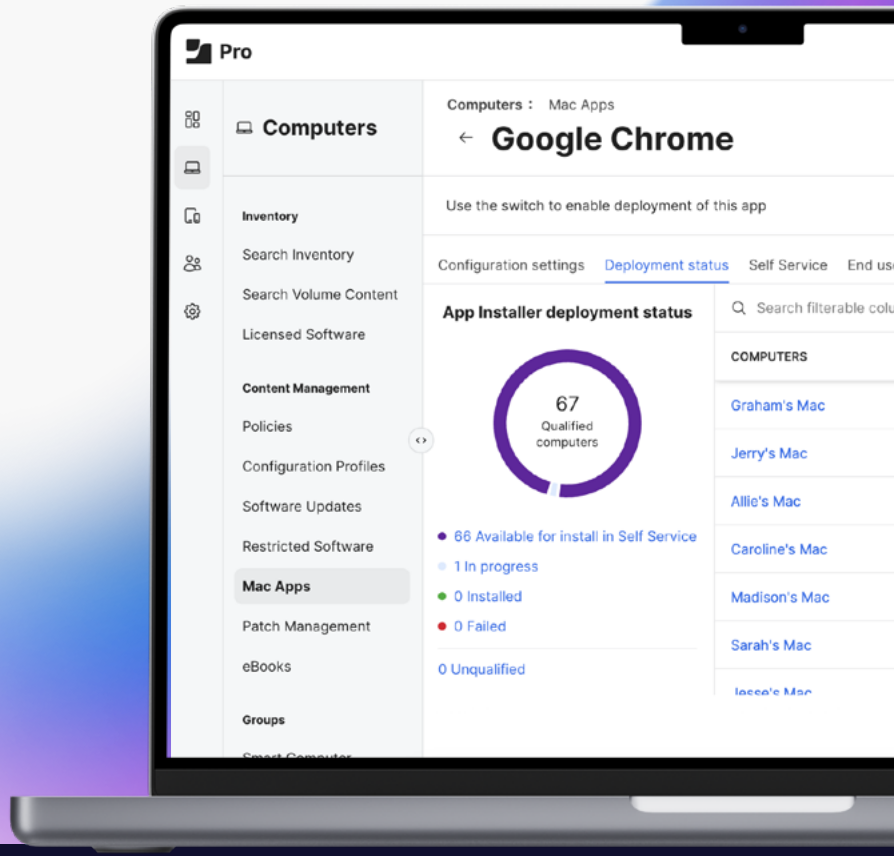
Trotz der leistungsfähigen Sicherheits- und Datenschutzfunktionen von macOS sind zusätzliche Schutzmaßnahmen erforderlich, um die Sicherheitsstandards von Unternehmen einzuhalten. Zu den wesentlichen Konformitätsanforderungen einer modernen Mac Sicherheitsstrategie gehören:

- Endpunktschutz und Konformität
- Identitäts- und Zugriffsverwaltung (IAM)
- Erkennung von Bedrohungen und Reaktion auf Vorfälle
- Schutz vor netzwerkbasierten Bedrohungen
- Zero-Trust-Netzwerkzugriff (ZTNA)

Berichte 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 für Unternehmen: **Warum die IT bei der Umstellung eine Vorreiterrolle spielen muss**

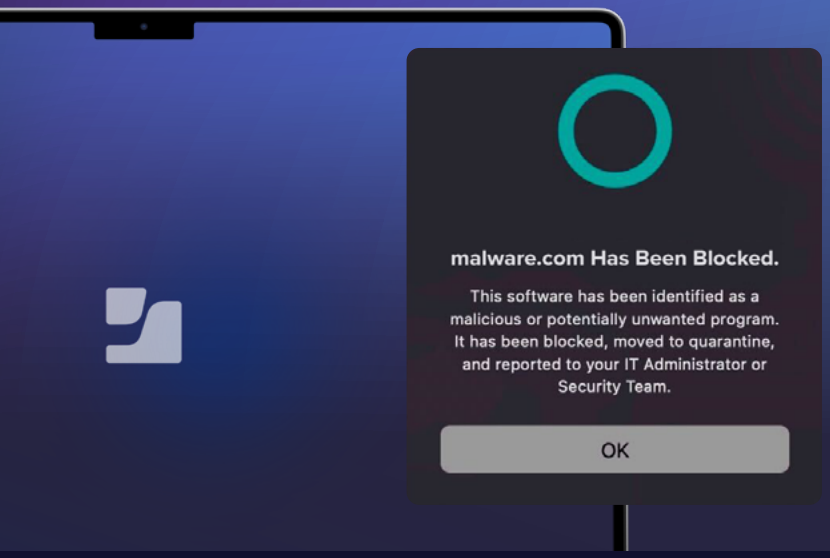
Durch den zunehmenden Einsatz von Macs in Unternehmen haben IT-Teams die Möglichkeit, die Verwaltungsstrategien neu zu definieren. Durch die Implementierung eines Apple-nativen, proaktiven und automatisierten Ansatzes kann die IT:

- die Sicherheit verbessern und die Compliance durchsetzen, während die Komplexität minimiert wird
- die Benutzerproduktivität durch nahtlose Workflows steigern, damit die Macs einwandfrei funktionieren
- den IT-Overhead durch Automatisierung und optimierte Abläufe reduzieren

Wenn IT-Teams 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
- **Höherer Return on Investment** (ROI) durch die Verwaltung und Sicherung von Macs, wenn Ihr Unternehmen wächst

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



Warum die Sicherheit bei der Verwaltung von Macs in Unternehmen so wichtig ist

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 Geschäftsdaten zu schützen, zumal Cyberkriminelle immer häufiger Macs angreifen. IT-Teams profitieren von einem umfassenden Sicherheitsansatz, der Folgendes umfasst:

- **Endpunktsicherheit**
- **Identitäts- und Zugriffsverwaltung**
- **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 Konformitätsanforderungen durchsetzen und Unternehmensressourcen schützen. Eine gut definierte Sicherheitsstrategie ist nicht nur eine Priorität der IT, sondern eine wesentliche Voraussetzung für die Schaffung einer Grundlage, die Ihren Sicherheitsstatus stärkt und die Geschäftskontinuität unterstützt.

Verwalteter Lebenszyklus des Geräts: Von Anfang bis Ende

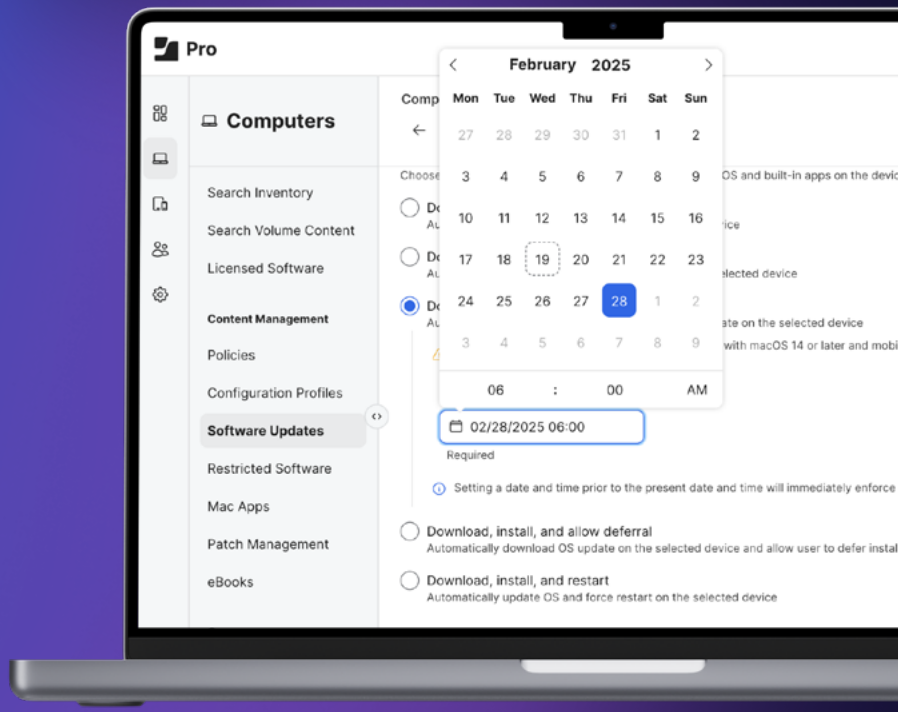
Eine effektive Sicherheit verlangt, dass alle Geräte, die für die Arbeit verwendet werden und eine Verbindung zu Unternehmensressourcen herstellen, hinsichtlich des Risikos, das sie für die Unternehmensressourcen darstellen, gleich behandelt werden. Der Schlüssel dazu ist die Konsistenz während des gesamten Lebenszyklus des Geräts, um sicherzustellen, dass keine Sicherheitslücken entstehen, von der Beschaffung über die Bereitstellung der Konfiguration bis hin zur Überwachung der Konformität, 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-Teams sicherstellen, dass die Geräte und die Mitarbeiter, die diese Geräte für die Arbeit mit geschützten Datentypen verwenden, den internen Richtlinien oder externen Anforderungen entsprechen, die den Schutz von Daten regeln. Zu den wichtigsten Konformitätsfaktoren gehören:

- **Anpassung an Standards und Frameworks**
- **Erstellung von Berichten über die Konformität**
- **Benachrichtigungen in Echtzeit**
- **Richtlinienbasierte Durchsetzung**



Bedrohungsabwehr mit KI/ML und Sicherheit auf Geräten

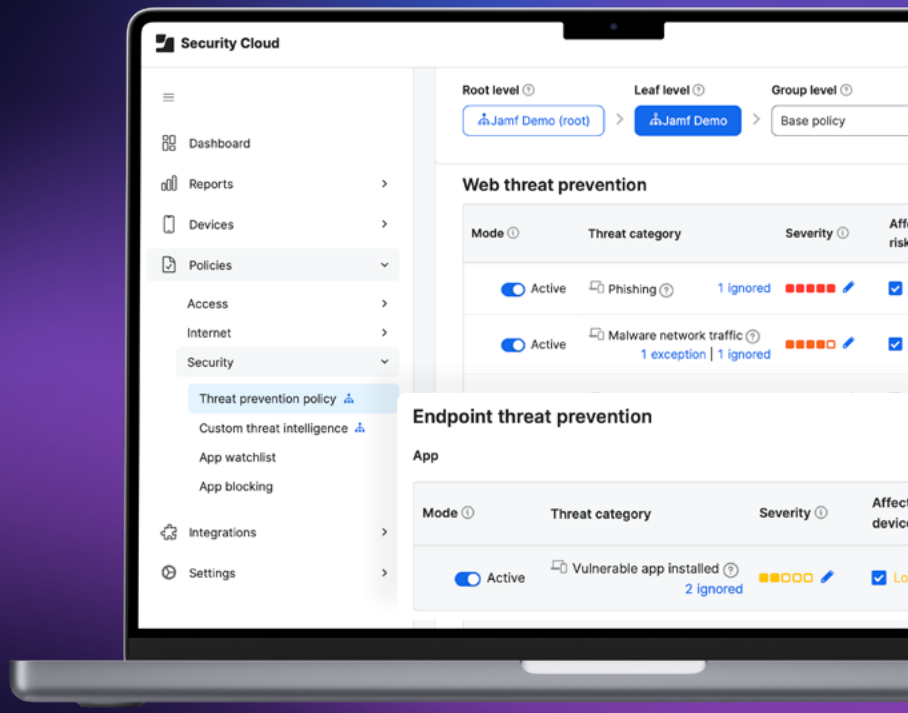
Die Bedrohungsakteure entwickeln ihre Methoden ständig weiter, wodurch es für die IT-Teams schwierig wird, nicht den Anschluss zu verlieren. Echtzeitanalysen auf der Grundlage von KI und maschinellem Lernen helfen dabei, anomales Verhalten zu erkennen, bekannte und unbekannte Bedrohungen zu verhindern und bösartige Aktivitäten zu blockieren, bevor sie die Produktivität der Benutzer beeinträchtigen. EDR-Tools bieten die nötige Transparenz, um die Untersuchung von Bedrohungen und die Reaktion darauf zu verbessern, so dass die IT-Abteilung verstehen kann, was passiert ist, und schnell Abhilfemaßnahmen ergreifen kann.

- **Erkennung von Bedrohungen in Echtzeit**
- **KI/ML-gesteuerte Prävention**
- **Schutz auf dem Gerät**
- **Transparenz zur Untersuchung der Vorfälle**

Zero-Trust-Prinzipien

Unternehmen wissen, dass schon ein einziges kompromittiertes Gerät ein Risiko darstellt. Zero Trust stärkt die Sicherheit durch kontinuierliche Überprüfung der Identität, des Zustands des Geräts und den Grund für den Zugriff. Dies ermöglicht eine kontextbasierte Zugriffskontrolle, die sicherstellt, dass nur vertrauenswürdige Benutzer und Geräte Zugriff auf sensible Daten erhalten, unabhängig davon, ob sie sich im Netzwerk oder remote befinden.

- **Kontinuierliche Identitäts- und Gerätekontrollen**
- **Kontextbezogener Zugang**
- **Datenschutz im und außerhalb des Netzwerks**
- **Reduzierte Angriffsfläche**



Durchsetzung der Konformität: Damit die Technik sicher bleibt

Die Anpassung der Geschäftsabläufe an organisatorische Standards oder Industrievorschriften gibt Unternehmen die Gewissheit, dass Geräte, Daten, Benutzer, 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**
- **Berichte zur Konformität**

Erweiterungen der Lösungen durch Deep Integration

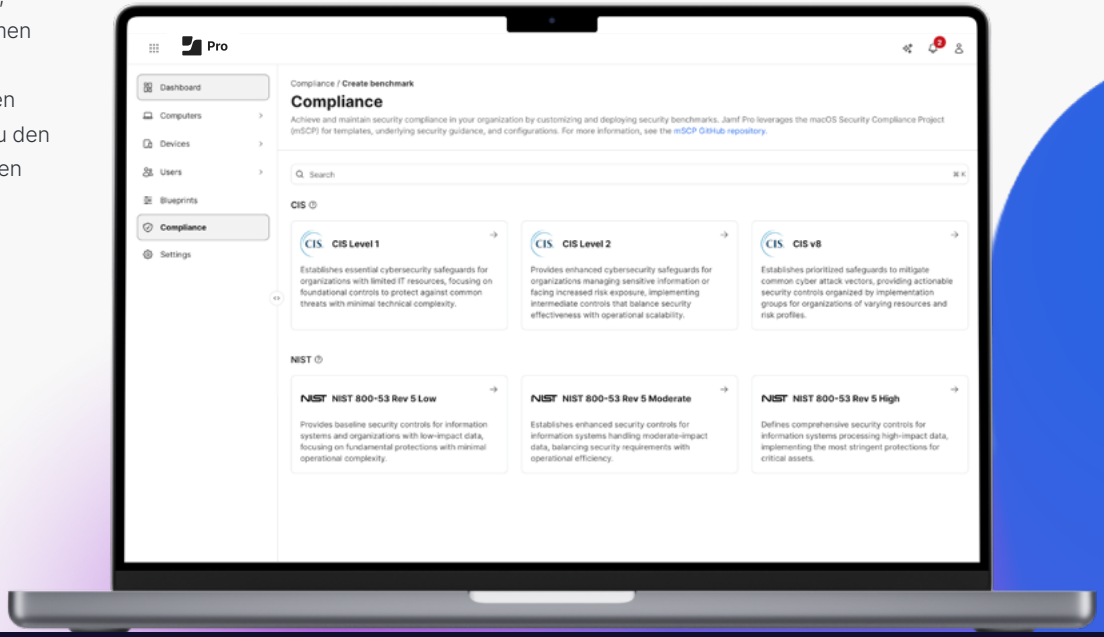
Entscheidungen werden nicht oft im luftleeren Raum getroffen. Genauso ist es mit der Sicherheit. Eine Lösung, egal wie leistungsstark sie ist, reicht nicht aus, um die verschiedenen Arten von Bedrohungen abzuwehren, denen Unternehmen heute ausgesetzt sind, und gleichzeitig die Funktionen des Betriebssystems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

- **Zentralisierung der Bedrohungsanalysen**
- **Automatisierte Behebung von Schwachstellen**
- **Implementierung eines bedingten Zugriffs**
- **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 kann Strategien zur Reaktion auf Vorfälle und zur Erkennung von Bedrohungen beinhalten, um bekannte Risiken zu minimieren und unbekannte Bedrohungen, die sich traditionellen Endpunktsicherheitslösungen entziehen können, zu erkennen. Zu den wichtigsten Strategien zur beschleunigten Reaktion auf Vorfälle und der Suche nach Bedrohungen gehören:

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



Schulungen für Mitarbeiter:innen zu Best Practices im Bereich Sicherheit

IT-Teams wissen, dass jede Kontrolle, Konfiguration und Richtlinie nur ein Teil eines größeren Sicherheitspuzzles ist. Jedes Puzzleteil 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 Endbenutzer. Obwohl die Benutzer 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 Benutzer 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-Teams, die ihre Sicherheitspläne durch Schulungen für Endbenutzer 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 Benutzer 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 Benutzer**
- **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-Teams 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 einzige, leistungsstarke Defense-in-Depth-Lösung, die Management, Identität und Sicherheit integriert, hilft wachsenden Unternehmen, eine stärkere Sicherheitsgrundlage zu schaffen.

Die wichtigsten Aspekte für eine effektive 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 der Endgeräte 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 Benutzer zum Sicherheitsbewusstsein als Teil einer umfassenden Lösung, damit sie nicht zur Ursache des Problems werden**