jamf

Mobile Threat Defense

für Beginner

Das ist eine Tatsache: Apple hat eine der stärksten sofort einsetzbaren sicheren Plattformen auf dem Markt. Allerdings stellt es in zunehmenden Maße ein Ziel als Plattform für entschlossene Angreifer*innen dar. Aus diesem Grund müssen Organisationen darauf reagieren können und die Bedrohungen heute und in Zukunft abwehren.

Häufige Angriffskampagnen wie Phishing, Malware und anfällige Apps werden benutzt, um Geräte auszunutzen und Zugriff auf Unternehmensressourcen und vertrauliche Daten zu gewinnen. Hierzu gehören:

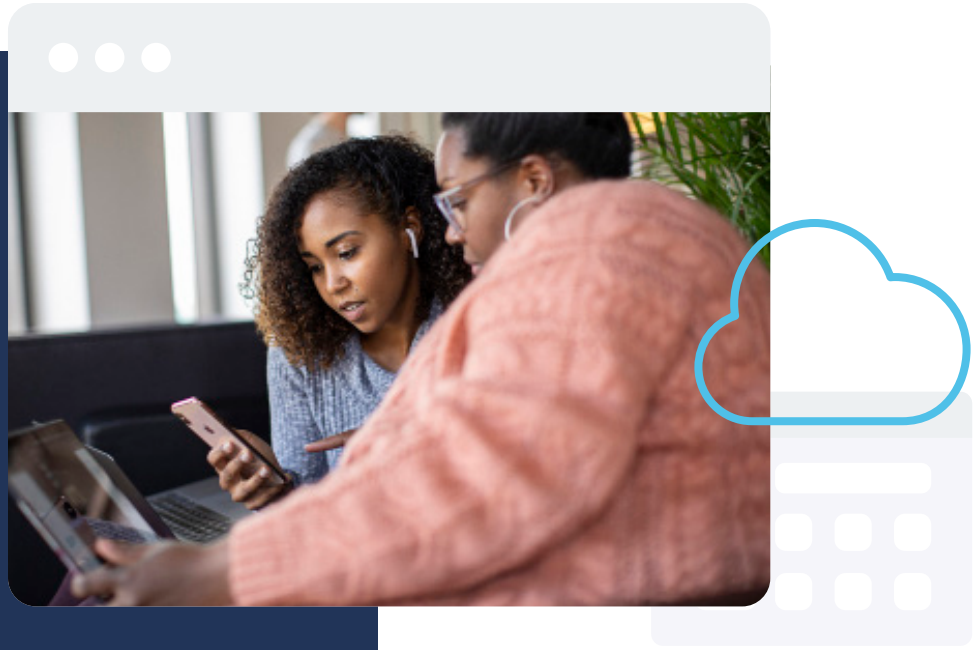
- Raub von vertraulichen Informationen
- Zugriff auf Unternehmensdienste
- Sammeln vertraulicher Benutzerdaten
- Abfangen von Netzwerkkommunikation

Jamf schützt Ihre mobilen Endgeräte durch Erkennung von Bedrohungen und Verhinderung von Zero-Day-Phishing- und Malware-Angriffen vor Kompromittierung. Das bereitet allen Organisationen große Sorge, vor allem jenen, die Tele- oder Hybridarbeit eingeführt haben, da sich derartige Angriffe zunehmend auf Mobilgeräte richten.

IN DIESEM LEITFADEN BESPRECHEN WIR FOLGENDES:

1. Umfassende Bedrohungserkennung und -prävention
2. Starker Schutz für jeden Anwendungsfall
3. Echtzeit-Reporting Funktion
4. Richtlinienkontrolle und bedingter Zugriff
5. Einheitliche Betriebsverwaltung

APPLE IST EIN WACHSENDES PLATTFORMZIEL FÜR ENTSCHLOSSENE ANGREIFER*INNEN...

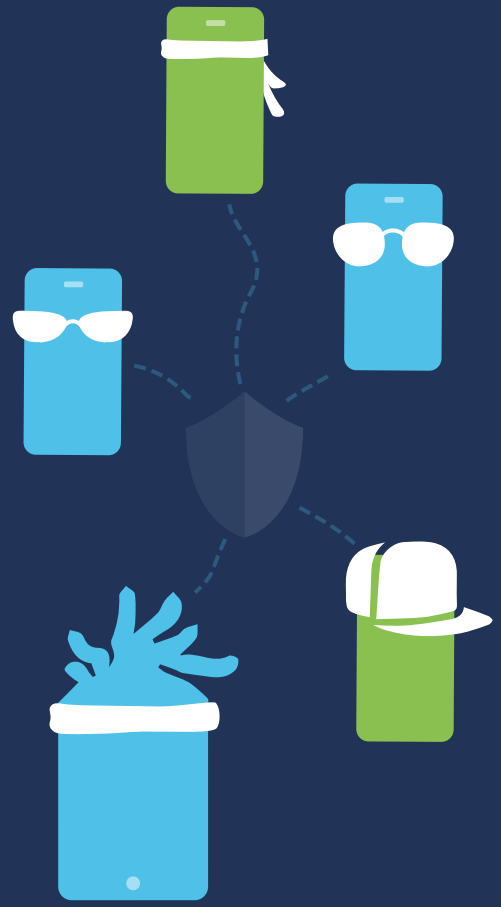


...UND SIE DISKRIMINIEREN NICHT.

Hier kommt **Jamf Protect** ins Spiel - die speziell entwickelte Lösung zum Schutz mobiler Geräte und Ihrer Benutzer*innen vor bösartigen Bedrohungen bei gleichzeitig geringem Overhead und kleinem Netzwerk-Footprint mit minimalen Auswirkungen auf die Geräteleistung und die Erfahrung der Endbenutzer*innen.

Organisationen, die für ihre Benutzer*innen macOS Geräte bereitstellen, verlassen sich darauf, dass Jamf Protect Endpoint-Schutz bietet, um die Geräte vor Sicherheitsbedrohungen zu schützen, Malware zu verhindern und Daten über den Gerätestatus zu liefern. Aber was ist mit mobilen Geräten, wie iOS, iPadOS und Android-Geräten? Welche Art von Sicherheitssystem für mobile Geräte ist verfügbar, das nicht nur die speziellen Anforderungen erfüllt, sondern auch mit **Jamf Pro** integriert werden kann, um eine umfassende Verwaltungslösung zu erhalten?

„SCHÜTZE DEIN INNERES“



Schütze dein Inneres. Dieser Spruch bezieht sich in diesem Zusammenhang auf den Schutz sensibler Güter durch den Schutz des Inneren, also des Kerns. Im Kontext dieses Leitfaden sind die Mobilgeräte der Kern. Schließlich sind sie der Weg, über den Angreifer*innen auf vertrauliche Daten zugreifen wollen.

41 % der Unternehmen erlebten einen Malware-Vorfall auf Remote-Geräten, was nicht nur ein erschreckender Wert ist, sondern auch ein beträchtlicher Anstieg im Vergleich zum Vorjahr, so der Cloud Security Report 2021. **Lesen Sie unseren Bericht Security 360, um mehr über die diesjährigen Sicherheitstrends und -risiken zu erfahren.**

Für alle, die nicht verstehen, was hinter dem Anstieg dieser Vorfälle steht, haben wir eine Antwort, die sowohl einfach als auch komplex ist. Die Erosion des Netzwerkperimeters aufgrund eines Wechsels zu Tele- und Hybridwarbeit führt dazu, dass Benutzer*innen zunehmend Mobilgeräte einsetzen, um auch außerhalb des Büros produktiv zu bleiben. Das ist der einfache Teil. Der komplexe Teil besteht darin, wie Unternehmen ihre Infrastruktur umgestalten, um Geräte zu schützen und Daten zu sichern.

Um die damit verbundene Komplexität zu minimieren, verfolgt Jamf einen cloudbasierten Ansatz, der leistungsstarke, fortschrittliche Sicherheitstechnologien mit extremer Flexibilität und Skalierbarkeit kombiniert. Das umfasst Echtzeitüberwachung, Erkennung und Reporting, was es IT- und Sicherheitsteams ermöglicht, den Status aller ihrer Geräte zu überwachen.

NETZWERK-SCHUTZ

Unter den zahlreichen Bedrohungen, mit denen moderne Unternehmen umgehen müssen, stellt das Phishing nur eine dar, aber sie ist vermutlich die gefährlichste, da sie auf das schwächste Glied in der Kette der Sicherheit abzielt – die Benutzer*innen. Die traurige Wahrheit ist, dass selbst bei wohlmeinenden und geschulten Nutzer*innen die Fehlerquote zu hoch ist, was bedeutet, dass die Erfolgsquoten bei der Kompromittierung hoch sind und Angreifer*innen sie daher weiterhin in ihrer Angriffskette nutzen werden.

Mit dem netzinternen Schutz können Sie Zero-Day-Bedrohungen wie Phishing-Websites aktiv und in Echtzeit blockieren. Auf diese Weise werden die Geräte vor den Auswirkungen dieser Kampagnen geschützt, bevor es zu einem ausbeuterischen Angriff kommt. Indem das Gerät daran gehindert wird, auf diese bösartigen Domänen zuzugreifen, und zwar über alle Kommunikationsarten hinweg (kabelgebunden, Wi-Fi oder Mobilfunk), können Unternehmen ihre Benutzer*innen und Endpoints schützen.

ERWEITERTE FUNKTIONA-LITÄTEN

Jamf Protect wurde mit Blick auf die Erweiterung der Funktionalität durch die Integration mit dem API-Framework eines Anbieters /einer Anbieterin entwickelt und verfügt über mehr Unified Endpoint Management (UEM) und Security Information and Event Management (SIEM) Partnerschaften als andere Sicherheitslösungen. In Bezug auf die IT- und Sicherheits-Teams bedeutet das, dass sie die bestehenden Investitionen in Sicherheits- und Geräteverwaltungs-Appliances, Apps und Services nutzen können, um Bedrohungen, Behebungs-Workflows und Automatisierung zu nutzen.

Ein hervorragendes Beispiel für eine solche Integration ist die Nutzung der Jamf Risk API zusammen mit den Funktionen von Jamf Protect, um eine beispiellose Kommunikation zu ermöglichen. Auf diese Weise werden die Daten zwischen beiden Systemen in Echtzeit ausgetauscht, was individuelle Berichte und Abhilfemaßnahmen zum Zustand der mobilen Geräte in Ihrem Unternehmen ermöglicht.

ADAPTIVER ZUGRIFF

Jamf Protect arbeitet unermüdlich daran, die unzähligen Angriffe auf die Cybersicherheit zu vereiteln, die keine Anzeichen einer Verlangsamung zeigen und die mobile Sicherheitslandschaft weiterhin plagen.

Einer der Hauptgründe, warum zugriffsbezogene Bedrohungen so effektiv sind, besteht darin, dass der Benutzer/die Benutzerin immer noch Zugriff auf eine Ressource hat, wenn ein Gerät kompromittiert wurde und es keine für den Benutzer/die Benutzerin sichtbaren Anzeichen gibt (das Gerät funktioniert scheinbar normal weiter). Das Gerät wird die Anfrage bearbeiten und den Zugang gewähren, wodurch die Ressource gefährdet wird.

Jamf bekämpft dies und erhöht gleichzeitig Ihre Sicherheitslage, indem es nur sichere Verbindungen und vertrauenswürdige Geräte für den Zugriff auf Unternehmensressourcen zulässt. Wie, fragen Sie?

> **Durch die kontinuierliche Überwachung von Telemetriedaten und kontextbezogenen, gerätespezifischen Inputs auf Anomalien.**

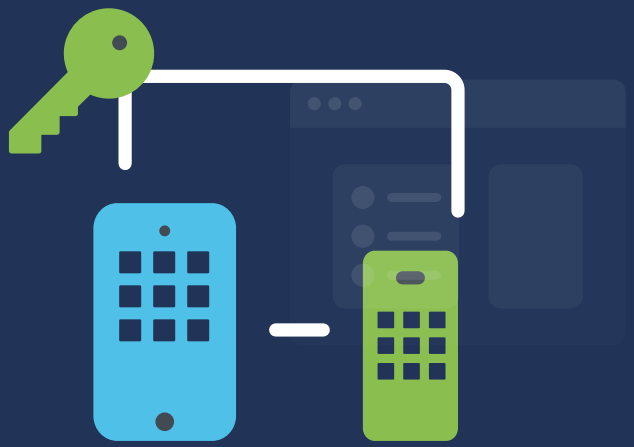
Wenn festgestellt wird, dass der Endpoint ein hohes Risiko darstellt oder kompromittiert ist, verhindert Jamf Protect den Zugriff auf die Ressource(n) durch die Durchsetzung von benutzerdefinierten Richtlinien.

FORTGE-SCHRITTENES MASCHINELLES LERNEN

Nachdem wir gelesen haben, was Jamf zum Schutz Ihres Unternehmens und Ihrer mobilen Geräteflotte beitragen kann, werden wir etwas tiefer in die Grundlagen der Software eintauchen, um Ihnen einen besseren Einblick zu geben, wie Jamf die Geräte vor Bedrohungen schützt. Dabei sehen wir uns keine Funktionen an, sondern die integrierten zentralen Verteidigungstechnologien, welche die oben erwähnten Funktionen unterstützen.

Wir stellen Ihnen vor. MI:RIAM: Eine fortgeschrittene Intelligenz-Engine, die in Echtzeit das breiteste Spektrum an bekannten und Zero-Day-Bedrohungen identifiziert. Durch die Nutzung der größten Gruppe an Bedrohungsdaten sammelt MI:RIAM Informationen von 425 Millionen Sensoren weltweit als Input für ihre Algorithmen. Dann nutzt sie fortschrittliche Datenwissenschaft, um Echtzeiteinblicke in die neuesten Bedrohungsdaten und aktiven Risiken zu bieten.

ALLE GERÄTE WILLKOMMEN



Sie haben nur iOS- und iPadOS-Geräte in Ihrer Flotte? Das ist perfekt. Jamf Protect bietet genau die Art von Sicherheitsschutz, die erforderlich ist, um Ihre Apple Geräte und Ihre Benutzer*innen vor aktuellen und neuen Bedrohungen zu schützen.

Haben Sie auch andere Geräte in Ihrer mobilen Geräteflotte? Auch das ist großartig! Jamf sichert Android- und Windows-Betriebssysteme und arbeitet ebenso hart daran, alle Ihre mobilen Geräte zu schützen. Jamf ermöglicht es Unternehmen, verschiedene Eigentumsmodelle zu unterstützen, z. B. unternehmenseigene oder BYOD-Programme, ohne dabei Kompromisse bei der Sicherheit einzugehen.

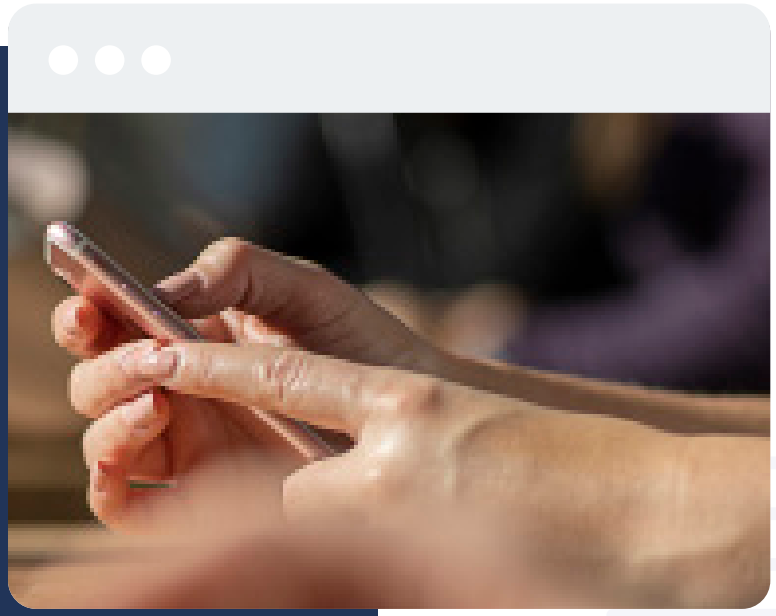
Als Benutzer*in möchten Sie wissen, dass Sie geschützt sind. Als Mitglied Ihres IT- oder Sicherheitsteams möchten Sie wissen, auf welche Weise Ihre Benutzer*innen geschützt sind. Aber wenn es um Hacker geht, dann ist es besser, dass sie möglichst wenig wissen, damit Sie den Sicherheitsstatus Ihres Netzwerks aufrechterhalten und letztlich Informationen schützen können. Und es gibt verschiedene Arten von Informationen, die Sie um jeden Preis schützen müssen, um ihre Integrität zu bewahren und IT- und Sicherheitsteams über die neuesten Zustandsdaten der Unternehmensendgeräte zu informieren.

PRIVATSPHÄRE DER NUTZER*INNEN

Persönliche Identifizierbare Informationen (PII), einschließlich persönlicher Gesundheitsinformationen (PHI) sind die meistgesuchten Datentypen, auf die Hacker*innen abzielen. Das ist ein zyklischer Effekt. Je mehr sie direkt einsammeln, umso mehr werden sie den Angriff fortsetzen wollen, und letztlich werden sie ihre kriminelle Bemühungen durchführen.

Glücklicherweise schützt Jamf die Online-Privatsphäre durch verschlüsselte Kommunikation und Schutz vor Phishing-Angriffen. Dies gilt nicht nur für die persönlichen Daten Ihrer Nutzer*innen, sondern auch für sensible Informationen, die zur Einhaltung gesetzlicher Vorschriften erforderlich sind. Die erweiterten Datenschutzfunktionen und Richtlinienkontrollen verhindern den Zugriff auf Unternehmensressourcen und -daten durch riskante Benutzer*innen oder Geräte.

ERKENNTNISSE IN ECHTZEIT



IT- und Sicherheitsteams können detaillierte Berichte über den Endpointstatus erhalten, indem sie die standardmäßigen Reporting-Funktionen verwenden, oder diese Funktionen an die spezifischen Anforderungen der Organisation anpassen. Mit den maßgeschneiderten Berichtsfunktionen geht Jamf Protect noch einen Schritt weiter und bietet Administrator*innen Echtzeitdaten in der Konsole oder exportiert sie über die integrierte Integrationsfunktion an einen SIEM-Partner, um Daten auf Dashboards zu visualisieren. Oder man nutzt die API zur Integration mit einer Unified-Management-Lösung, z. B. durch Kopplung mit Jamf Pro, um Daten zwischen der Software zu streamen und so ein automatisiertes Gerätemanagement und die Behebung erkannter Endpoint-Probleme zu ermöglichen.

Es gibt so viel, das Sie für Ihre Organisation und Ihre Benutzer tun können, um Daten, Geräte und Personen zu schützen. Es gab zu viel, als dass wir das alles in diesem E-Book erwähnen könnten. Das ist Ihr nächster Schritt:

Erfahren Sie mehr, indem Sie eine kostenlose Testversion ausprobieren. Sie können auch mit Ihrem bevorzugten Reseller zusammenarbeiten, um zu sehen, was mit Jamf möglich ist.

Testversion anfordern

Wir freuen uns darauf, dass Sie loslegen können.