jamf

Die Lücke schließen: macOS Sicherheit

Das Bedürfnis nach Sicherheit erstreckt sich über alle Betriebssysteme und macOS ist keine Ausnahme. Apple hat hart dafür gearbeitet, um native Datenschutz- und Sicherheitsfunktionen bereitzustellen, doch die Mac-Plattform wird für Angreifer aufgrund eines wachsenden Marktanteils in Unternehmen immer lukrativer. Dies macht sie zu einem begehrten Ziel für Schadsoftware, Datendiebstahl und die Identifizierung von Schwachstellen. Zudem setzen immer mehr Unternehmen auf Wahlfreiheit bei der Hardware und integrieren macOS in ihre Infrastruktur. Dabei mussten sie feststellen, dass, wie bei jeder anderen Plattform auch, zusätzliche Sicherheit und Transparenz erforderlich sind.

Mehrere Sicherheitsanbieter bieten zusätzliche Lösungen zum Schutz von Macs an, aber viele dieser Lösungen verwenden ein für den Anbieter und sein Windows Produkt spezifisches Sicherheitsmodell, anstatt mit modernen Frameworks zu arbeiten, die macOS bietet. Dadurch wird es schwierig, mit den ständigen Änderungen des Betriebssystems Schritt zu halten. Die beste Vorgehensweise besteht jedoch darin, das bestehende macOS Sicherheitsmodell zu erweitern, die Lücken zu schließen und den macOS spezifischen Mehrwert hinzuzufügen, den Sicherheitsteams benötigen, um effektiv zu arbeiten und ihr Unternehmen vor Bedrohungen zu schützen.

Bei den Apple Betriebssystemen sind Datenschutz und Sicherheit von grundlegender Bedeutung für die Plattform – der Schutz wurde bereits in die Hardware und Software integriert. Gleichzeitig legt Apple großen Wert auf eine intuitive Bedienung, die Benutzerfreundlichkeit und Produktivität in den Vordergrund stellt. Infolgedessen sind viele Funktionen in erster Linie auf den einzelnen Benutzer ausgerichtet und nicht auf die umfassenderen Bedürfnisse eines Unternehmens, was zusätzliche Transparenz und Sicherheitskontrollen erforderlich macht.

In unserem Whitepaper geben wir einen Überblick über den aktuellen Stand der macOS Sicherheit und zeigen auf, wie Apples Sicherheitsgrundlagen auf effiziente, effektive und benutzerfreundliche Weise verbessert werden können.

Wir werden Folgendes behandeln:

- Details zu verfügbaren, integrierten Sicherheitsfunktionen beim macOS
- Wie Jamf diese Funktionen im Unternehmen verbessert
- Wie Jamf die Bedrohungserkennung über Signaturen und integrierte Funktionen hinaus erweitert
- Zusätzliche Möglichkeiten zur Erweiterung des Apple-Sicherheitsmodells für fortgeschrittene Unternehmenssicherheit

Apps unter macOS

Apple hat viel Arbeit in die Entwicklung von Sicherheitsfunktionen gesteckt, um den Benutzer und die von ihm genutzten Drittanbieterprogramme zu schützen. In diesem Abschnitt werden wir einige dieser Funktionen vorstellen und darüber sprechen, wie sie strategisch verbessert und erweitert werden können. Weitere Informationen zu den Sicherheitsfunktionen von Apple finden Sie in **Apples umfassendem Sicherheitsleitfaden für die Plattform**.

Überprüfen Sie die Vertrauenswürdigkeit mit Gatekeeper.

Die von Apple bevorzugte und vertrauenswürdigste Methode zur Installation von Drittanbieteranwendungen ist der App Store. Auf diese Weise kann Apple Programme überprüfen und aussortieren, die nicht den Standards in Bezug auf Datenschutz, Sicherheit und Benutzerfreundlichkeit entsprechen. Allerdings schränkt Apple auch die Funktionen von Apps im App Store ein, wodurch viele geschäftskritische Apps für diese Art der Distribution nicht gut geeignet sind.

Wenn die Verteilung über den App Store nicht in Frage kommt, erlaubt Apple den Entwicklern von macOS, ihre Apps direkt über gehostete Downloads und andere traditionelle Distributionsmethoden zu vertreiben. Um diese ‚Ad-hoc'-Distributionen zu unterstützen, hat Apple zusätzliche Prüfmechanismen in das Betriebssystem integriert, um das Risiko einer unkontrollierten Verbreitung von Software auf macOS-Geräten zu verringern. Dabei ist das Feature „Gatekeeper" verantwortlich für die Verifizierungsprüfungen von Apple. Was in macOS als Option begann, um Programme je nach Risikobereitschaft laufen zu lassen, hat sich zu einem erweiterten und strengen Satz von Anforderungen und Abhilfemaßnahmen entwickelt. Die grundlegenden Zulassungsstufen für Apps, die aus dem ‚App Store' oder von ‚verifizierten Entwicklern' stammen, existieren weiterhin; allerdings wird die Option, problematischen oder riskanten Code auszuführen, zunehmend eingeschränkt.

Beachten Sie, dass diese Prüfungen nur für Apps gelten, die aus dem Internet heruntergeladen wurden. Apple trackt diese Apps, indem es zusätzliche Metadaten an die heruntergeladene Datei anhängt, die als Quarantäne-Attribut bezeichnet werden. Wenn ein Programm ausgeführt wird, führt Gatekeeper eine Reihe von Prüfungen durch, wie z. B. die Überprüfung des Quarantäneattributs, um festzustellen, ob es ausgeführt werden kann. Eine dieser grundlegenden Überprüfungen ist, ob die App von einem legitimen Entwickler signiert wurde oder ob sie über den App Store vertrieben wurde, abhängig von der zuvor besprochenen Einstellung.

Wenn die App von einem Entwickler signiert ist, wird das Zertifikat mit einer Datenbank für widerrufene Signaturen abgeglichen, um zu überprüfen, ob der Unterzeichner in der Vergangenheit mit Malware in Verbindung gebracht wurde. Auf diese Weise kann Apple ein Zertifikat schnell widerrufen und eine weite Verbreitung von Malware verhindern.

Mit Veröffentlichung von macOS Catalina erfordert das Bestehen der Gatekeeper-Prüfung außerdem, dass die App von Apple notariell beglaubigt wird. Damit eine App die Prüfung besteht, muss sie zur Analyse bei Apple hochgeladen werden. Nach erfolgreicher Analyse werden die Beglaubigungsdokumente mit der App verknüpft, um zu vermerken, dass sie diese zusätzliche Prüfstufe bestanden hat.

Das endgültige Urteil liegt beim Benutzer.

Im Rahmen der Benutzerfreundlichkeit erlaubt macOS dem Endbenutzer in vielen Situationen, Gatekeeper „außer Kraft zu setzen". Dazu kann der Benutzer einfach mit der rechten Maustaste auf die App klicken und „Öffnen" oder „Öffnen mit" wählen. Anstatt die Ausführung der App pauschal zu verweigern, wird der Benutzer in einer neuen Eingabeaufforderung lediglich gewarnt, dass er eine unbekannte oder potenziell bösartige App startet, aber Gatekeeper erlaubt ihm dies. Hierbei ist es wichtig zu beachten, dass Malware, die eindeutig von XProtect identifiziert wurde, nicht vom Benutzer verwendet werden kann.

Sobald die App zum ersten Mal ausgeführt wurde, wird die Quarantänekomponente aktualisiert, damit Gatekeeper beim nächsten Öffnen der App nicht erneut tätig wird.

⚠ Blockieren Sie Bedrohungen mit XProtect und MRT.

In der Gatekeeper-Suite sind außerdem die signaturbasierten Erkennungsmechanismen von Apple enthalten, die als XProtect und Malware Removal Tool (MRT) bekannt sind. Gemeinsam sind sie in der Lage, Dateien auf dem Betriebssystem zu scannen und nach Merkmalen in Dateien zu suchen, die mit bekannter Malware in Verbindung stehen. XProtect wird beim Start der App getriggert, während MRT das Dateisystem wiederkehrend scannt.

XProtect arbeitet mit einer Binärsignatur-Scan-Engine namens Yara. Yara unterstützt flexible und leistungsfähige binäre Signaturdefinitionen und eine effiziente Ausführungsmaschine. Um eine App zu überprüfen, scannt XProtect jeden ausführbaren Download bei der ersten Ausführung und bei jeder weiteren Aktualisierung. Werden übereinstimmende Signaturen gefunden, kann das Programm nicht ausgeführt werden. Die Datei mit bekannten, schlechten Signaturen wird über unabhängige Updates von Apple für macOS bereitgestellt. Apple definiert und stellt diese Signaturen nach eigenem Ermessen zur Verfügung, unabhängig von der Yara-Ausführungsmaschine selbst. Genau wie Gatekeeper wird dieser Scan nur durchgeführt, wenn eine App das richtige erweiterte Quarantäneattribut besitzt, das nach der ersten erfolgreichen Ausführung der App aktualisiert wird.

MRT wiederum läuft nach einem festen Zeitplan ab und nicht erst beim Start eines Programms. Dabei wird das Dateisystem auf spezifische Merkmale und Spuren früherer Malware-Infektionen untersucht; bei einem Treffer werden diese automatisch gelöscht. Diese Funktion ist hauptsächlich dazu gedacht, bekannte Bedrohungen, die möglicherweise bereits in der macOS-Population ausgeführt werden, zu finden und zu beseitigen.

⚙ Erweitern Sie Gatekeeper auf das Unternehmen.

Gatekeeper funktioniert tatsächlich so, wie es sein soll. Es blockiert die Ausführung nicht vertrauenswürdiger Apps und benachrichtigt den Benutzer, wenn es eine App als verdächtig oder bösartig identifiziert. IT- und Sicherheitsadmins müssen darüber Bescheid wissen, wenn versucht wird, nicht vertrauenswürdige Software auf einem unternehmenseigenen Gerät auszuführen. Noch wichtiger ist, dass sie erfahren, wenn ein Benutzer mit der rechten Maustaste auf eine App geklickt und diese gestartet hat, womit er eine Sicherheitskontrolle des Unternehmens umgangen hat. Um diese Unternehmensanforderungen zu erfüllen, überwacht Jamf for Mac - mit seiner speziell für Mac entwickelten Endpunktsicherheitslösung - Anzeichen für Gatekeeper-Aktionen und meldet die Ergebnisse an eine zentrale Stelle, damit IT- und Sicherheitsteams ihre Risiken genau einschätzen und fundierte Entscheidungen treffen können.

Jamf bietet nicht nur Einblick in die Gatekeeper-Aktivitäten, sondern ermöglicht es Unternehmen auch, die Kontrolle über das Vertrauensmodell für Entwickler zu übernehmen, indem es zusätzliche Signierinformationen als ‚nicht vertrauenswürdig' in der Unternehmensumgebung registriert. Unter Verwendung der neuesten Endpoint Security API von Apple verweigert Jamf proaktiv die Ausführung jeder App, die auf der unternehmensspezifischen Sperrliste steht. Dies kann auf Anwendungsebene (Anwendungs-ID) oder auf Herstellerebene (Entwicklerteam-ID) definiert werden.

Des Weiteren bietet macOS keine Signaturen oder Blockierungen für eine Vielzahl von Grayware (potenziell unerwünschte oder nicht genehmigte Software) an. Dazu gehören viele Adware- und Krypto-Miner-Anwendungen, die ein unerwünschtes und potenziell invasives Verhalten aufweisen. Oft wurden diese Programme rechtmäßig von einem Apple Entwickler signiert und der Benutzer stimmt bei der Installation zu, dass seine Daten gesammelt oder Ressourcen verwendet werden dürfen - meist ohne es zu merken. Daher greift Apple in vielen Fällen nicht in die Nutzung dieser Apps ein.

Allerdings ist die Risikobewertung in Unternehmen einfach anders, und es sollte ein strengerer und gezielterer Ansatz verfolgt werden. Daher setzt Jamf seinen eigenen Satz an verwalteten Yara-Regeln, binären Signaturen und nicht vertrauenswürdigen Entwickler-Zertifikaten durch. Diese werden verwendet, um Prozesse bei der Ausführung zu scannen, unabhängig davon, ob das erweiterte Quarantäneattribut vorhanden ist oder nicht. Dadurch wird gewährleistet, dass bei einer Aktualisierung der Sicherheitslage und dem Hinzufügen neuer Signaturen auch bereits vorhandene Apps beim nächsten Start erneut gescannt werden – und nicht nur bei der ersten Ausführung.

Jamf kuratiert diesen Feed bekannter Mac-Malware auf der Grundlage seiner umfangreichen Analysen zu macOS-Bedrohungen sowie Daten zu Mac-Bedrohungen von Drittanbietern. Unternehmen, die eine noch genauere Überwachung der in ihrer Umgebung ausgeführten Software wünschen, können die Liste der von Jamf blockierten Apps um ihre eigene Liste mit binären Hashes, Team-IDs usw. erweitern. Wenn eine App ausgeführt wird, deren mit dem Verhalten oder

der Signatur mit bekannter Malware unter macOS 10.15 (Catalina) oder höher übereinstimmt, verhindert Jamf die Ausführung dieses Prozesses, stellt die angreifende Datei unter Quarantäne und registriert eine Warnung, dass Malware verhindert wurde. Dieser Vorgang erfolgt unabhängig von den Gatekeeper/XProtect-Aktionen und ist als funktionale Erweiterung dieser Features gedacht. Jamf identifiziert bekannte Malware, ohne dabei die Quarantänekomponente zu berücksichtigen. Dadurch können unsichere Binärdateien identifiziert werden und die Wissensbasis über Malware wird kontinuierlich erweitert.

Erweitern Sie das Vertrauensmodell des App Store mit Self Service.

In bestimmten Situationen kann es sinnvoll sein, die Programme, die Ihre Benutzer installieren können, über einen Self-Service-App-Store zu bestimmen, der mit von der IT-Abteilung genehmigten Ressourcen bestückt ist.

Jamf Self Service+ ermöglicht einen sicheren und sofortigen Ressourcenzugriff, indem es der IT-Abteilung die Möglichkeit gibt, einen eigenen App-Katalog für Unternehmen zu erstellen, in dem Benutzer selbständig Apps installieren, Konfigurationen aktualisieren und allgemeine Probleme beheben können - ohne ein IT-Hilfeticket erstellen zu müssen.

Steuern und überwachen Sie das Verhalten der Apps.

Limitieren und bestätigen Sie das Verhalten der Apps mit Datenschutzkontrollen.

Die Systemsteuerungen für den Datenschutz wurden mit macOS Mojave eingeführt. Diese Kontrollen erfordern, dass Benutzer (oder Unternehmen) den Zugriff auf bestimmte Aktionen und Ordner pro App zulassen. Sobald den Apps Zugriff auf bestimmte Aktionen gewährt wurde, werden sie nicht mehr gefragt, wenn die Aktion in Zukunft von derselben App aus ausgeführt wird. Diese Funktion stellt sicher, dass den Apps ausdrücklich der Zugriff auf potenziell sensible Teile des Betriebssystems (Webcam, Mikrofon, Tastatureingaben, Downloads) gestattet wird, und veranlasst Benutzer dazu, sich Zeit zu nehmen und zu bestätigen, dass sie den Apps Zugriff auf private Daten gewähren.

Gehen Sie über reine Kontrollmechanismen hinaus, um das Verhalten von Apps zu auditieren und zu analysieren.

Obwohl Datenschutzkontrollen die Berechtigungen von Apps limitieren, werden Nutzer Fehler machen und Berechtigungen missbrauchen. Wie bereits erwähnt, bietet Jamf Einblick in die Arbeitsweise der nativen Apple Sicherheitsfunktionen und klassische Schutzmechanismen gegen Malware/Adware, damit Unternehmen stets informiert und geschützt bleiben. Wir bei Jamf sind jedoch der Meinung, dass der Endpunktschutz noch weitaus mehr beinhaltet. Deshalb bietet Jamf zusätzliche Audit- und Überwachungsfunktionen, die traditionell den EDR-Produkten (Endpoint Detection and Response) vorbehalten sind - allerdings mit einem Apple-first-Ansatz und mit Blick auf die Standards für Datenschutz und Sicherheit, die macOS Benutzer erwarten.

Erkennungstechnik mit Jamf for Mac

DasHerzstück des Endpunktschutzes von Jamf bildet ein Agent, der als leichtgewichtiger Sensor im User-Mode fungiert und auf eine von Apples eigenen Logik-Engines, GameplayKit, zurückgreift. Obwohl die Verwendung einer Game-Engine für die Analyse von Sicherheitsereignissen unüblich ist, ermöglicht sie Jamf eine enge Integration in das Ökosystem von Apple und die Analyse von Daten auf dem Gerät, bis diese gesammelt oder gemeldet werden müssen. Game-Engines sind außerdem dafür ausgelegt, eine große Anzahl von Ereignissen in Echtzeit zu verarbeiten, was sie perfekt für die Analyse von Aktivitäten auf dem Gerät macht. Im Gegensatz dazu gibt es viele Sicherheitslösungen, die sich zunächst auf die Windows-Plattform konzentrieren und dann nachträglich für macOS angepasst werden – oder solche, die verlangen, dass alle Daten in der Cloud gesammelt und analysiert werden.

Ein zusätzlicher Vorteil von GameplayKit ist, dass es, wie Yara, die Ausführungsmaschine von den Erkennungsdefinitionen trennt, so dass Erkennungen aktualisiert und erweitert werden können, ohne dass der Kernagent aktualisiert werden muss. Die Erkennungsdefinitionen sind ebenfalls Apple-eigen und verwenden NSPredicate, einen leistungsstarken logischen Abfragemechanismus, der typische Abfragesyntax sowie reguläre Ausdrücke unterstützt. Das Datenmodell von Jamf wurde so konzipiert, dass es die umfangreichen Funktionen von NSPredicate nutzen kann, einschließlich der Möglichkeit, native Funktionen aufzurufen und Datenmodelle miteinander zu verknüpfen. Dadurch erhält man Funktionen, die auf andere, traditionellere Weise nur umständlich oder mit hohem Rechenaufwand zu implementieren sind.

Zum Beispiel können wir das Datenmodell von Jamf und NSPredicate für folgende Aspekte verwenden:

- Warnmeldung, wenn sich eine Datei selbst löscht, eine gängige Technik, um seine Spuren zu verwischen. Bei diesem scheinbar einfachen Anwendungsfall werden sowohl die gelöschte Datei als auch der Löschvorgang untersucht, ohne aufwendige Join-Operationen oder fest codierte Erkennung.
- Warnmeldung, wenn eine unsignierte oder verdächtig signierte Binärdatei als Start-Daemon bestehen bleibt. Dazu gehört das Parsen einer Konfigurationsdatei, das Extrahieren eines eingebetteten Binärpfads aus dem Inhalt und die Verwendung von Metadaten über diese Binärdatei in der Analyse.
- Warnmeldung, wenn eine Microsoft Office-Anwendung ein unerwartetes untergeordnetes Element erstellt hat, um die Ausnutzung von Office-Makros zu identifizieren. Dieses Beispiel verdeutlicht die Fähigkeit, untergeordnete/übergeordnete Beziehungen zu verstehen und die Ausnutzung von Anwendungsfunktionen aufzudecken.
- Warnmeldung, wenn andere „Live-off-the-Land"-Aktivitäten in einer Weise genutzt werden, die auf Angriffe hindeutenb. Für diese Art von Aktivitäten ist der Zugriff auf untergeordnete/übergeordnete und Prozessgruppenbeziehungen, Befehlszeilenparameter usw. erforderlich, um den Missbrauch von ansonsten harmlosen Aktivitäten (curl, ssh, python usw.) aufzudecken.
- USB-Nutzung im gesamten Unternehmen tracken und Metadaten über Dateien melden, die auf Wechselmedien gespeichert werden.

Um die Auswirkungen dieser Erkennungen leicht verständlich zu machen, ordnet Jamf identifizierte Angriffe – sofern zutreffend – dem MITRE ATT&CK-Framework zu. Die aktuelle Abdeckung umfasst Anwendungsfälle aus dem gesamten Framework, einschließlich der Erkennung von Techniken in den folgenden Kategorien:

- Persistenz
- Erstzugang
- Befehl & Kontrolle
- Verteidigung & Ausweichen
- Entdeckung
- Privilegienerweiterung
- Zugang über Anmeldedaten

Verbesserte Transparenz mit Mac-nativer Telemetrie

Da die Unternehmen ihre macOS-Sicherheitslage zunehmend verstärken, wird ein tieferer Einblick in die System- und Benutzeraktivitäten immer wichtiger. Die nativen Apple-Frameworks bieten eine solide Grundlage, aber viele Sicherheitsteams benötigen häufig umfangreichere, korrelierte Signale, um anomales Verhalten zu erkennen, Vorfälle zu untersuchen und die Konformität in großem Umfang aufrechtzuerhalten.

Die Telemetriefunktion von Jamf baut auf Apples Endpoint Security API auf, um detaillierte, macOS-spezifische Signale von jedem Gerät zu sammeln. So können Unternehmen System-, Benutzer-, App- und Netzwerkaktivitäten genau analysieren und dabei Daten verwenden, die die Funktionsweise von macOS widerspiegeln. Die Telemetrie ist leichtgewichtig und leistungsstark, um das Benutzererlebnis nicht zu beeinträchtigen, und zudem manipulationssicher, damit Protokolle und Sicherheitsereignisse für Untersuchungen und Konformitätsanforderungen zuverlässig bleiben.

Durch die Korrelation von Ereignissen bei Prozessen, Apps, Authentifizierung, Konfigurationsänderungen und Benutzeraktionen hilft Jamfs Telemetrie den Sicherheitsteams, detaillierte Zeitpläne zu rekonstruieren und Verhaltensweisen zu erkennen, die auf Missbrauch oder aufkommende Bedrohungen hindeuten können.

Mit der Telemetrie von Jamf können Organisationen:

- gesetzliche und interne Konformitätsanforderungen mithilfe von präzisen, hochwertigen Ereignisdaten erfüllen
- Konfigurationsabweichungen, Schatten-IT und Richtlinienabweichungen erkennen
- die Reaktion auf Vorfälle durch Analyse korrelierter Ereignisse und Angriffspfade beschleunigen
- die proaktive Bedrohungssuche mit angereicherten, macOS-spezifischen Erkenntnissen unterstützen
- Nahtlose Integration in SIEM-Plattformen für zentralisierte Transparenz

Diese Funktionen bieten den Umfang und die entsprechenden Informationen, die für die Verwaltung und Sicherung von Mac-Geräten im großen Maßstab erforderlich sind, und bilden eine solide Grundlage für fortschrittliche Erkennungs- und Analysefunktionen. Telemetrie arbeitet auch mit dem macOS Unified Log System zusammen und ermöglicht es Unternehmen, sowohl erweiterte Sicherheitssignale als auch gezielte Protokolldaten für Audits, Untersuchungen und Konformität zu sammeln.

Einfache Erfassung und Berichterstattung mit Unified Log

Die meisten Sicherheitsanalysten und IT-Admins haben einen großen Bedarf an Endpunktprotokollen als Teil eines Audits zur Konformität oder wenn sie Lücken in anderen Sicherheitskontrollen schließen wollen. Als macOS von Syslog-Dateien auf Unified Logging umstieg, wurde es schwieriger, diese Informationen unternehmensweit zu sammeln, zu inventarisieren und zu prüfen. Die macOS Console.app bietet einen großartigen Zugang und Einblick in die Unified Log-Infrastruktur auf einem lokalen Mac, aber diese Daten können von einem Unternehmen nicht ganz so einfach zentralisiert werden.

Dank Jamf lassen sich Client-Protokolle an ein zentrales Aufzeichnungssystem weiterleiten, unmittelbar nachdem sie im Unified Log erfasst wurden. Um sicherzustellen, dass nur spezifische Daten erfasst werden, verwenden Jamf Admins die gleiche Prädikatfiltersprache (NSPredicate) wie das integrierte Befehlszeilen-Dienstprogramm „Log Stream“. Damit wird der Aufbau von Aufzeichnungssystemen für Mac-Protokolldaten zu einer einfachen Konfiguration anstelle einer mühsamen Erfassung von Daten für jede einzelne Maschine. Beispiele sind An- und Abmeldung, SSH, AirDrop und Autorisierungsereignisse. Wenn Daten im Unified Log protokolliert werden, kann Jamf sie sammeln.

Angleichung an die Standards von Apple

Unterstützung am Tag der Veröffentlichung

Um eine Schnittstelle zu macOS zu schaffen und Daten zu sammeln, die für Sicherheitsentscheidungen erforderlich sind, nutzt Jamf native Apple-Technologien. Zu diesen Technologien gehören aufkommende Frameworks wie die Endpoint Security API von Apple und das deklarative Geräteverwaltungsprotokoll (eine Weiterentwicklung des Geräteverwaltungs-Frameworks). Durch die Verwendung dieser Mechanismen minimiert Jamf die Belastung auf das Gerät und wird nicht durch Änderungen in macOS beeinträchtigt, die durch Patches oder größere Betriebssystemversionen eingeführt werden. Frühzeitiges und häufiges Patchen ist das am häufigsten empfohlene Sicherheitsprotokoll. Sicherheitstools, die sich strikt an die Unterstützung am Tag der Veröffentlichung halten, sind für die Einhaltung dieses Protokolls von zentraler Bedeutung und eine wichtige Komponente in einer umfassenden Defense-in-Depth-Sicherheitsstrategie.

Benutzererfahrung als Feature

Während Jamf die Apps und die Aktivitäten des Benutzers kontinuierlich auf potenzielle Bedrohungen überwacht, sucht es bewusst nicht nach ruhender oder Microsoft Windows-bezogener Malware. Das Scannen von Dateien, die sich lediglich im Dateisystem befinden, auf eine Vielzahl von Malware-Signaturen ist oft ein Hauptgrund für eine schlechte Benutzererfahrung. Dieser Ansatz stimmt mit Gatekeeper/XProtect insofern überein, als dass Bedrohungen zum Zeitpunkt ihrer potenziellen Ausführung erkannt werden, so dass die Benutzererfahrung und die Produktivität der Benutzer so wenig wie möglich beeinträchtigt werden.

Rahmenwerk für die deklarative Geräteverwaltung

Die auf der WWDC 21 angekündigte deklarative Geräteverwaltung (DDM) ist die Weiterentwicklung und Aktualisierung des Protokolls zur Geräteverwaltung. Durch DDM können Geräte proaktiv Verwaltungseinstellungen übernehmen, Zustandsänderungen autonom melden und asynchron mit dem MDM-Server kommunizieren. Dies bedeutet eine deutliche Abkehr vom traditionellen Command-and-Response-Modell hin zu einem effizienteren, autonomen Ansatz.

Datenschutz

Jamf analysiert die Daten auf dem Gerät und sammelt nur dann relevante Informationen, wenn es dafür konfiguriert wurde, d. h. wenn eine potenziell bösartige oder verdächtige Aktivität in Echtzeit erkannt wird. Dadurch werden die Anforderungen des Unternehmens und die Privatsphäre der Benutzer in Einklang gebracht, da weniger Benutzerdaten vom Gerät erfasst und in der Cloud gespeichert werden. Sobald eine bösartige Aktivität erkannt wird, werden die identifizierte Aktivität und die zugehörigen Daten an die Jamf Cloud-Konsole oder konfigurierte SIEM-Systeme (Security Information and Event Management) weitergeleitet. Alle speziell angeforderten Daten, die darüber hinausgehen, werden ebenfalls an Jamf oder das SIEM übermittelt. Durch das Herausfiltern aller unwichtigen Daten erhält ein Sicherheitsanalytiker, der mit der Überwachung und Untersuchung von Vorfällen betraut ist, eine qualitativ hochwertige Sammlung von nutzbaren Daten.

Andere Erweiterungen des Apple Sicherheitsmodells

Best Practices: Härtung von macOS

Obwohl Apple einige der sichersten und zuverlässigsten Betriebssysteme auf dem Markt anbietet und unterstützt, stellt sich häufig die Frage, welche zusätzlichen Schritte unternommen werden können, um macOS noch besser für Ihre Unternehmensumgebung zu machen.

Der beste erste Schritt besteht darin, das Mobile Device Management (MDM) von Apple für die automatisierte Verwaltung im Unternehmen zu nutzen. MDM hilft Ihnen nicht nur, Ihr Unternehmen besser zu schützen, sondern entlastet auch die IT-Abteilung bei der Verwaltung und Sicherung Ihrer Flotte.

Das mit OS X 10.7 (‚Lion') eingeführte MDM-Framework ermöglicht eine enorme Vielzahl an Workflows, um die Funktionalität der Geräte präzise auf die spezifischen Anforderungen eines Unternehmens zuzuschneiden. Konfigurationsprofile und Verwaltungsbefehle sind die beiden gängigsten Möglichkeiten, ein MDM zu nutzen, damit die Teams sicher arbeiten können, unabhängig von ihrem Aufenthaltsort.

Heben Sie die Sicherheit mit MDM auf ein neues Level, indem Sie sie mit der Leistungsfähigkeit des Apple Business Manager kombinieren – einer kostenlosen Lösung von Apple für Unternehmen, die dabei hilft, die Beschaffung, Verwaltung und Bereitstellung von Hardware zu automatisieren.

Beginnen Sie mit Apple ...

Im Laufe der Jahre hat sich Apple einen guten Ruf als sicherheitsbewusstes Unternehmen aufgebaut, und das zeigt sich in macOS. Native Funktionen wie die FileVault 2-Verschlüsselung, die Zwei-Faktor-Authentifizierung, die Funktion zum Sperren/Löschen aus der Ferne und die Möglichkeit, Passcode-Standards durchzusetzen, sind auf jedem neuen Mac verfügbar, der der Unternehmensumgebung hinzugefügt wird.

Moderne Verwaltungs- und Sicherheitsplattformen wie Jamf nutzen die neuesten Technologien von Apple, um diese Funktionen weiterzuentwickeln und die Implementierung, Durchsetzung und Berichterstattung über wertvolle Sicherheitswerkzeuge wie Verschlüsselung anzupassen.

...Verbessern mit Jamf.

MDM ist zwar ein hervorragender Eckpfeiler für jedes Unternehmen, aber viele fragen sich, was sie sonst noch tun können, um ihre Sicherheitslage weiter zu verbessern und den Datenschutz der Mitarbeiter:innen zu stärken. Hier kommt Jamf ins Spiel.

Es ist kein Geheimnis, dass die Geräteverwaltung ab einer bestimmten Größe die Ressourcen des Teams stark beansprucht. Mehr Mitarbeiter:innen bedeuten mehr Hardware, und mehr Hardware bedeutet mehr IT-Aufwand.

Zumindest war das so, bevor es Plattformen wie Jamf gab.

Mit patentierten Technologien wie Entwürfen und dynamischen Gruppen, die bei der Organisation von Geräten im Unternehmen und der automatischen Ausführung von Verwaltungsfunktionen helfen, müssen IT-Teams weniger Zeit mit der Geräteverwaltung verbringen und haben mehr Zeit für andere alltägliche IT-Aufgaben. Dynamische Gruppen behalten den Gerätebestand im Auge und fügen in Echtzeit Geräte aus einer vordefinierten Gruppe hinzu oder entfernen sie, wenn sich der Gerätestatus ändert.

Moderne Identitätsverwaltung unter macOS

Im Zentrum moderner Sicherheit steht die Identität - ein sicherer und individueller Zugang für Endbenutzer. Traditionelle IT verlässt sich auf lokale Verzeichnisdienste, die als zentraler Datensatz für Mitarbeiterinformationen wie Name und Abteilung dienen. Da sich die Sicherheits- und Bereitstellungsanforderungen weiterentwickeln, müssen Unternehmen einen neuen Ansatz für die Identitäts- und Zugriffsverwaltung als Teil ihrer Unternehmensstrategie wählen. Mit einem vollständigen cloudbasierten Identitäts-Stack vereinheitlichen Unternehmen Identitäten über Hardware und Software hinweg, um Funktionen und fortschrittliche Workflows zu erschließen und letztendlich ihr Unternehmen zu transformieren.

Auf der Grundlage von Informationen aus Verzeichnisdiensten stellt das cloudbasierte Single Sign-On (SSO) sicher, dass Endbenutzer sichere Anmeldedaten eingeben, um auf Unternehmensressourcen zuzugreifen.

Jamf erweitert diese gängigen Formen der Identitätsverwaltung.

Jamf vereinheitlicht die Identität in allen Unternehmensanwendungen und auf dem Mac des Benutzers mit nahtlosen Authentifizierungs-Workflows. Endbenutzer nutzen eine einzelne Cloud-Identität, um einfach und schnell Zugang zu den Ressourcen zu erhalten, die sie für ihre Produktivität benötigen.

Mit Jamf erhalten Organisationen:

- eine optimierte Bereitstellung und Authentifizierung für die vollständige Unterstützung von Mitarbeiter:innen an entfernten Standorten und vor Ort
- automatisierte Synchronisierung von Benutzeridentitäten und Anmeldedaten für Geräte
- IT mit umfassenden Funktionen für die Identitätsverwaltung für ihre Dienste und Geräte
- eine ZTNA-Lösung, die herkömmliche VPNs ersetzt und die Anforderungen moderner, hybrider Unternehmen erfüllt

Reaktion auf und Beseitigung von Bedrohungen auf dem Mac

Jamf stellt Dashboards zur Verfügung, die Unternehmen dabei helfen, den Zustand ihrer Mac-Geräte zu überwachen und Hardware zu melden, die Aufmerksamkeit benötigt. Durch die patentierte Funktion der dynamischen Gruppen können IT-Admins Geräte identifizieren, die aktualisiert oder gepatcht werden müssen, um ihre Sicherheit zu verbessern. Dies alles geschieht aus der Ferne und kann automatisiert werden, so dass die IT-Abteilung das Gerät nie physisch in die Hand nehmen muss.

Wenn die Bedrohungsbeseitigung mit Jamf Protect mit Jamf Pro kombiniert wird, geht sie noch einen Schritt weiter. Durch den Einsatz dieser dynamischen Gruppentechnologie können alle MDM- und Jamf-Befehle als Reaktion auf eine aktivitätsbasierte Warnmeldung orchestriert werden. Dazu gehören die automatisierte Isolierung des Netzwerks, fehlgeschlagener bedingter Zugriff, Benachrichtigungen der Benutzer oder eine Reihe anderer gezielter Formen der Beseitigung und Abwehr.

Sicherheit über das Gerätemanagement hinaus

Lesen Sie unseren Bericht über den Stand der Apple Sicherheit in Unternehmen, für den 1.500 IT- und InfoSec-Experten befragt wurden. Er beleuchtet die aktuelle Gerätenutzung und Sicherheitsansätze, Herausforderungen bei der Gerätesicherheit sowie die Zukunft der Endpunktsicherheit.

Jamf for Mac

Moderne Unternehmen benötigen einen einheitlichen Ansatz für die Verwaltung und Sicherung von macOS-Geräten in der gesamten Organisation. Jamf for Mac unterstützt dies durch die Integration von Apples integriertem Schutz mit fortschrittlichen Funktionen wie Identitäts- und Berechtigungsmanagement, Kontrolle von Wechseldatenträgern und Bedrohungsabwehr. So entsteht eine mehrschichtige, auf Apple ausgerichtete Sicherheitsstruktur, die Ihre Geräte in Echtzeit schützt, ohne die gewohnte macOS Erfahrung zu stören, die die Benutzer erwarten.

Mit Jamf for Mac erhalten Unternehmen einen besseren Einblick in die Aktivitäten der Geräte, eine stärkere Ausrichtung an den Konformitätsrichtlinien und die Möglichkeit, die geringsten Rechte durchzusetzen, Wechselmedien zu kontrollieren und webbasierte Bedrohungen abzuwehren. Diese Funktionen tragen dazu bei, die Risiken in der gesamten Mac Flotte zu reduzieren und gleichzeitig die Benutzerproduktivität aufrechtzuerhalten und die Apple Erfahrung zu bewahren.

Indem Jamf for Mac Verwaltung, Identitätsmanagement und Endpunktsicherheit in einer einzigen, auf Apple spezialisierten Lösung vereint, können Organisationen ihre macOS-Geräte ganzheitlich schützen und sicher agieren, während ihre Mac Flotten kontinuierlich wachsen.

jamf

Erste Schritte

Oder Sie kontaktieren Ihren bevorzugten Händler, um Jamf kostenlos zu testen.

www.jamf.com/de/