jamf

WHITE PAPER

macOS Sicherheit

Apple bietet nativen Schutz der Privatsphäre und der Geräte, aber kein Betriebssystem ist perfekt.

Die hohen Anforderungen an Sicherheit erstrecken sich über jedes Betriebssystem, und macOS ist keine Ausnahme. Apple hat viel investiert, um native Datenschutz- und Sicherheitsfunktionen bereitzustellen. Mit zunehmendem Marktanteil von Mac im Unternehmen steigt jedoch auch die Gefahr von schädlicher Software, Sicherheitsverletzungen und Sicherheitslücken. Unternehmen erlauben ihren Mitarbeitern mehr denn je, macOS über Mitarbeiterauswahlprogramme zu nutzen. Dabei stellten sie fest, dass wie bei jeder anderen Plattform zusätzliche Sicherheit und Transparenz erforderlich sind.

Einige Anbieter von Sicherheitslösungen liefern zusätzliche Lösungen zum Schutz des Mac. Viele dieser Lösungen verwenden jedoch ein Windows-spezifisches Sicherheitsmodell, anstatt mit modernen Frameworks wie Apple's macOS Framework zu arbeiten. Dies macht es schwierig, mit den ständigen Änderungen des Betriebssystems Schritt zu halten. Die bewährte Vorgehensweise ist es jedoch, das vorhandene macOS-Sicherheitsmodell zu erweitern, die Lücken zu schließen und den macOS-spezifischen Nutzen hinzuzufügen, den Sicherheitsteams für ein effizientes Arbeiten und den Schutz ihrer Organisation vor Bedrohungen benötigen.

Während Apple Betriebssysteme sowohl den Benutzer als auch seine Privatsphäre schützen, haben Benutzerfreundlichkeit und Produktivität stets oberste Priorität. Die Apple Erfahrung konzentriert sich stark auf die Benutzer anstatt auf die Arbeit desselben. Dasselbe gilt für viele der Sicherheits- und Datenschutzfunktionen in macOS.

Unser White Paper enthält einen Überblick über den aktuellen Stand der macOS Sicherheit sowie Anleitungen dazu, wie die sicherheitsrelevanten Apple Basiswerte auf effiziente, effektive und benutzerfreundliche Weise verbessert werden können.

Lernen Sie die folgenden Sachverhalte kennen:

- Details zu den verfügbaren integrierten Mac Sicherheitsfunktionen
- Wie Jamf diese Funktionen im Unternehmen verbessert
- Wie Jamf die Bedrohungserkennung über Signaturen und integrierte Funktionen hinaus erweitert
- Weitere Möglichkeiten zur Erweiterung des Apple Sicherheitsmodells zur Verbesserung der Unternehmenssicherheit

Vertrauen in macOS

Apple hat große Anstrengungen in dem Gebiet der Entwicklung von Sicherheitsfunktionen unternommen, um das Vertrauen zwischen den Benutzern und den von ihnen ausgeführten Anwendungen Dritter zu stärken. In diesem Abschnitt werden wir einige dieser Funktionen vorstellen und erörtern, wie sie strategisch verbessert und erweitert werden können. Weitere Informationen zu den Sicherheitsfunktionen von Apple finden Sie im vollständigen Sicherheitsleitfaden für Apple Plattformen unter **support.apple.com/de-de/guide/security/welcome/web**

Gatekeeper

Die von Apple bevorzugte und vertrauenswürdigste Methode für die Installation von Anwendungen Dritter ist über den App Store. Auf diese Weise kann Apple Programme überprüfen und aussieben, die nicht den Standards für Datenschutz, Sicherheit oder die Benutzererfahrung entsprechen. Apple schränkt jedoch auch die Funktionen von Anwendungen im App Store ein, und viele geschäftskritische Anwendungen sind für diese Art des Vertriebs nicht geeignet.

Wenn der Vertrieb über den App Store keine Option ist, ermöglicht Apple den macOS Entwicklern, ihre Anwendungen direkt über gehostete Downloads und andere traditionelle Distributionswege zu vertreiben. Um eine solche „Ad-hoc“-Distribution zu unterstützen und gleichzeitig das Risiko einer weiten Verbreitung nicht vertrauenswürdiger Software auf macOS Geräten zu verringern, hat Apple weitere Überprüfungen in das Betriebssystem integriert. Gatekeeper ist der Name der Funktion im Zentrum der Vertrauens- und Verifizierungsprüfungen von Apple. Diese Funktion wurde ursprünglich als Option für macOS eingeführt, damit Programme je nach Vertrauensstufe ausgeführt werden können, und hat sich mittlerweile zu einem erweiterten und strengen Satz von Anforderungen und Maßnahmen zur Risikominimierung entwickelt. Die grundlegenden Vertrauensstufen beim Herunterladen von Apps aus dem „App Store“ oder dem „App Store und von identifizierten Entwicklern“ sind weiterhin vorhanden, die Option zum Ausführen von nicht vertrauenswürdigem Code wird jedoch weiterhin an den Rand gedrängt.

Beachten Sie, dass diese Überprüfungen nur für Anwendungen gelten, die aus dem Internet heruntergeladen werden. Apple verfolgt diese Anwendungen, indem zusätzliche Metadaten an die heruntergeladene Datei angehängt werden, die als Quarantäneattribute bezeichnet werden. Wenn ein Programm ausgeführt wird, überprüft Gatekeeper das Quarantäneattribut,um festzustellen,ob die Anwendung eine Reihe von Überprüfungen durchläuft, bevor sie ausgeführt werden kann.

Eine der grundlegendsten Überprüfungen besteht darin zu untersuchen, ob die Anwendung von einem legitimen Entwickler signiert oder über den App Store vertrieben wurde, abhängig von der zuvor beschriebenen Einstellung.

Wenn die Anwendung von einem Entwickler signiert ist, wird das Zertifikat anhand einer widerrufenen Signaturdatenbank überprüft, um sicherzustellen, dass der Signierende in der Vergangenheit nicht mit Malware assoziiert wurde. Auf diese Weise kann Apple ein Zertifikat schnell widerrufen und eine weite Verbreitung der Malware stoppen. Ab macOS Catalina müssen Anwendungen von Apple beglaubigt werden, um die Gatekeeper Überprüfung zu bestehen. Damit eine Anwendung die Prüfung bestehen kann, muss sie zur Analyse auf Apple hochgeladen werden. Nach erfolgreicher Analyse wird die Anwendung mit Beglaubigungsdaten verknüpft, die darauf hinweisen, dass dieser zusätzliche Schritt der Überprüfung bestanden wurde.

Das ultimative Vertrauen liegt beim Benutzer

Im Namen der Benutzerfreundlichkeit ermöglicht macOS dem Endbenutzer die „Übersteuerung“ von Gatekeeper. Ein Benutzer kann einfach mit der rechten Maustaste auf die Anwendung klicken und „Öffnen“ oder „Öffnen mit“ auswählen. Anstatt den Start der Anwendung strikt abzulehnen, werden die Benutzer lediglich mit einer neuen Warnung darauf hingewiesen, dass sie eine nicht vertrauenswürdige Anwendung starten, aber Gatekeeper dies zulässt.

Nachdem die Anwendung zum ersten Mal ausgeführt wurde, wird die Quarantänekomponente aktualisiert, sodass die Gatekeeper-Aktionen beim nächsten Öffnen der Anwendung nicht wiederholt werden.

Blockieren von Bedrohungen mit XProtect und MRT

Das Technologiepaket von Gatekeeper umfasst auch die signaturbasierten Erkennungsmechanismen von Apple, die als XProtect und Malware Removal Tool (MRT) bekannt sind. Gemeinsam können sie Dateien auf dem Betriebssystem scannen und nach Merkmalen in Dateien suchen, die mit bekannter Malware assoziiert werden. XProtect wird beim Start der Anwendung aktiviert, während MRT das Dateisystem regelmäßig scannt.

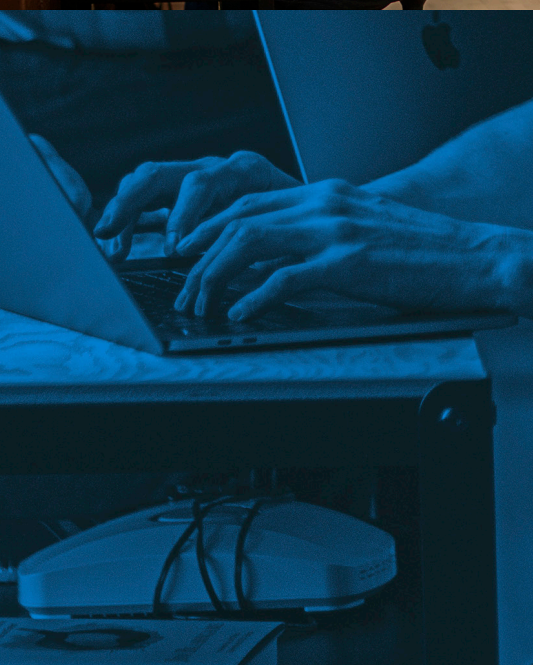
XProtect arbeitet mit einer binären Signatur-Scanengine namens Yara. Yara unterstützt flexible und leistungsstarke binäre Signaturdefinitionen und eine effiziente Ausführungsengine. Um die Vertrauenswürdigkeit einer Anwendung zu überprüfen, scannt XProtect jeden ausführbaren Download nur bei der ersten Ausführung. Wenn übereinstimmende Signaturen erkannt werden, kann das Programm nicht ausgeführt werden. Die bekannte Datei mit fehlerhafter Signatur wird über unabhängige Updates für macOS von Apple bereitgestellt. Apple definiert und liefert diese Signaturen nach eigenem Ermessen, und zwar getrennt von der Yara-Ausführungsengine selbst. Genau wie Gatekeeper wird dieser Scan nur durchgeführt, wenn eine Anwendung das richtige erweiterte Quarantäneattribut enthält, das nach der ersten erfolgreichen Ausführung der Anwendung aktualisiert wird.

MRT hingegen wird nicht bei Programmausführung, sondern planmäßig ausgeführt und durchsucht das Dateisystem nach bestimmten Dateinamen und Artefakten, die mit früherer Malware assoziiert werden, und entfernt sie, wenn sie entdeckt werden. Diese Funktion dient hauptsächlich dem Auffinden und Beseitigen bekannter Bedrohungen, die möglicherweise bereits in der gesamten macOS-Population ausgeführt werden.

Erweiterung von Gatekeeper auf das Unternehmen

Gatekeeper arbeitet effektiv und wie beabsichtigt. Die Funktion blockiert den Start nicht vertrauenswürdiger Anwendungen und benachrichtigt den Benutzer, wenn eine Anwendung als verdächtig oder bösartig erachtet wird. IT-/InfoSec-Experten benötigen Einblick in Versuche, nicht vertrauenswürdige Software auf einem Unternehmens-Asset auszuführen. Noch wichtiger ist, dass sie sich darüber im Klaren sein müssen, dass ein Benutzer mit der rechten Maustaste auf eine Anwendung geklickt und diese gestartet hat, um eine Sicherheitskontrolle für Unternehmen effektiv zu umgehen. Um diesen Unternehmensanforderungen gerecht zu werden, überwacht Jamf Protect – eine speziell für Mac entwickelte Endpoint-Sicherheitslösung – auf Anzeichen von Gatekeeper Aktionen und meldet die Ergebnisse an eine zentrale Stelle, damit IT- und Sicherheitsteams ihre Risiken genau einschätzen und fundierte Entscheidungen treffen können.

Jamf Protect bietet nicht nur Einblick in die Gatekeeper Aktivitäten, sondern ermöglicht es Unternehmen auch, Eigentümer des Entwickler-Vertrauensmodells zu werden, indem zusätzliche Signaturinformationen in der Unternehmensumgebung als nicht vertrauenswürdig registriert werden. Mit dem neuesten Endpoint Security



Framework von Apple verweigert Jamf Protect proaktiv die Ausführung von Anwendungen in der unternehmensspezifischen Blockierliste. Dies kann auf Anwendungsebene (Anwendungs-ID) oder auf Anbieterebene (Entwicklerteam-ID) definiert werden.

Darüber hinaus bietet macOS keine Signaturen oder Blockierungen für eine Vielzahl von Grayware (potenziell unerwünschte oder nicht genehmigte Software), einschließlich vieler Adware- und Crypto-Miner-Anwendungen mit unerwünschtem und potenziell invasivem Verhalten. Oft werden diese Programme von einem Apple Entwickler rechtmäßig signiert, und der Benutzer erklärt sich zum Zeitpunkt der Installation damit einverstanden, dass seine Informationen gesammelt oder Ressourcen verwendet werden können – normalerweise ohne es zu bemerken. Daher stört Apple in vielen Fällen den Betrieb dieser Anwendungen nicht.

Die Risikoermittlung ist jedoch im Unternehmen anders, sodass ein strengerer und gezielterer Ansatz möglicherweise gewünscht wird. Daher erzwingt Jamf Protect einen eigenen Satz verwalteter Yara-Regeln, binärer Signaturen und Zertifikate nicht vertrauenswürdiger Entwickler, die zum Scannen von Prozessen bei der Ausführung verwendet werden, unabhängig davon, ob das erweiterte Quarantäneattribut vorhanden ist oder nicht. Auf diese Weise wird sichergestellt, dass beim Hinzufügen neuer Signaturen und Aktualisieren der Sicherheitseinstellungen des Unternehmens vorhandene Anwendungen bei der nächsten Ausführung erneut gescannt werden, nicht nur beim ersten Mal.

Jamf kuratiert diesen Feed bekannter Malware, die auf Mac abzielt, basierend auf der intensiven Forschung von Jamf zu macOS Bedrohungen sowie auf Mac Bedrohungsdaten Dritter. Unternehmen, die eine noch detailliertere Kontrolle über die in ihrer Umgebung ausgeführte Software wünschen, können die Liste der von Jamf Protect blockierten Anwendungen um eine eigene Liste mit binären Hashes, TeamIDs usw. erweitern. Wenn eine Anwendung ausgeführt wird, die mit dem Verhalten oder der Signatur bekannter Malware unter macOS 10.15 (Catalina) oder höher übereinstimmt, verhindert Jamf Protect die Ausführung dieses Prozesses, stellt die fehlerhafte Datei unter Quarantäne und registriert eine Warnung, dass Malware verhindert wurde. Dieser Vorgang findet außerhalb von Gatekeeper/XProtect-Aktionen statt und ist als Obermenge ihrer Funktionalität konzipiert. Jamf Protect identifiziert bekannte Malware ohne Berücksichtigung des Quarantäne-Bits, um potenziell unsichere Binärdateien zu identifizieren, und verwaltet ein viel breiteres Spektrum an Malware-Wissen.

Erweiterung des App Store Vertrauensmodells durch Self Service

In bestimmten Situationen kann es angebracht sein, die Programme vorzugeben, die Ihre Benutzer installieren können. Dazu können Sie einen Self-Service App-Store nutzen, der mit von der IT genehmigten Ressourcen gefüllt ist.

Jamf Self Service ermöglicht einen sicheren und sofortigen Ressourcenzugriff. Dazu erhält die IT-Abteilung die Möglichkeit, einen eigenen Unternehmens App-Katalog zu erstellen, in dem Benutzer Apps installieren, Konfigurationen aktualisieren und häufig auftretende Probleme selbst beheben können – ohne dass ein IT-Hilfeticket erforderlich ist.

Kontrollieren und Überwachen des Verhaltens von Anwendungen

Datenschutzkontrollen zur Beschränkung und Bestätigung des Verhaltens von Anwendungen

Kontrollen zum Systemdatenschutz wurden in macOS Mojave eingeführt. Für diese Kontrollelemente müssen Benutzer (oder Unternehmen) den anwendungsbasierten Zugriff auf bestimmte Aktionen und Ordner gewähren. Sobald Anwendungen Zugriff auf bestimmte Aktionen erhalten haben, werden sie nicht mehr gefragt, wann die Aktion in Zukunft von derselben Anwendung ausgeführt wird. Diese Funktion stellt sicher, dass Anwendungen explizit auf potenziell sensible Teile des Betriebssystems (Webcam, Mikrofon, Tastenanschläge, Downloads) zugreifen dürfen. Außerdem bremst sie das Tempo der Benutzer und verlangt ihre Bestätigung, dass sie Anwendungen Zugriff auf private Daten gewähren.

Gehen Sie über Kontrollen hinaus, um das Anwendungsverhalten zu überwachen und zu analysieren

Während Datenschutzkontrollen die Berechtigung von Anwendungen einschränken, machen Benutzer Fehler, und Berechtigungen werden missbraucht. Wir haben bereits erläutert, wie Jamf Protect Einblick in die Aktionen der integrierten Apple Sicherheitsfunktionen und traditionellen Funktionen zur Verhinderung von Malware/Adware bietet, damit Unternehmen stets informiert und geschützt sind. Wir bei Jamf sind jedoch der Meinung, dass eine Lösung für den Endgeräteschutz hier nicht aufhören sollte. Jamf Protect bietet auch Prüf- und Überwachungsfunktionen, die traditionell für Endpoint Detection and Response (EDR) -Produkte reserviert sind – jedoch mit einem Apple-First-Ansatz und einem Blick auf die Datenschutz- und Sicherheitsstandards, die macOS Benutzer erwarten.

Erkennungstechnologie mit Jamf Protect

Das Herzstück des Jamf Protect Agent ist ein leichter Sensor im Benutzermodus (ohne Begleitschlüssel), der eine der Apple Engines zur Logikausführung, das Gameplay Kit, nutzt. Die Verwendung einer Spiel-Engine zur Analyse von Sicherheitsereignissen ist kein traditionelles Vorgehen, aber ein solches Vorgehen ermöglicht die enge Integration von Jamf in das Apple Ökosystem sowie die Analyse von Daten auf dem Gerät, bis sie erfasst oder gemeldet werden müssen. Außerdem sind Spiel-Engines so konzipiert, dass sie eine Vielzahl von Ereignissen in Echtzeit verarbeiten können. Dadurch sind sie perfekt für die Analyse der Aktivitäten geeignet, die auf dem Gerät stattfinden. Vergleichen Sie dieses Design mit den vielen Sicherheitslösungen, die sich zuerst auf die Windows Plattform konzentrieren und nachträglich auf macOS portiert werden – oder solchen, bei denen alle Daten in der Cloud gesammelt und analysiert werden müssen.

Ein zusätzlicher Vorteil des Gameplay-Kits besteht darin, dass es wie Yara die Ausführungsengine von den Erkennungsdefinitionen trennt. Dadurch können Erkennungen aktualisiert und erweitert werden, ohne dass der Core Agent aktualisiert werden muss. Die Erkennungsdefinitionen stammen ebenfalls von Apple. Sie verwenden NSPredicate, eine leistungsstarke Logiksprache, die neben regulären Ausdrücken auch die typische Abfragesyntax unterstützt. Das Datenmodell von Jamf Protect wurde speziell entwickelt, um die umfangreichen Funktionen von NSPredicate zu nutzen, einschließlich der Möglichkeit, native Funktionen aufzurufen und Datenmodelle miteinander zu verketten. Dadurch werden Funktionen freigeschaltet, deren Implementierung auf andere, traditionellere Weise chaotisch oder rechenintensiv ist. Mit dem Datenmodell von Jamf Protect und der NSPredicate-Sprache können wir beispielsweise folgende Aufgaben erledigen:

- Benachrichtigung, wenn sich eine Datei selbst löscht; dies ist eine gängige Technik zum Verwischen der eigenen Spuren. In diesem scheinbar einfachen Anwendungsfall werden sowohl die gelöschte Datei als auch der Löschvorgang ohne teure Verknüpfungsoperation oder fest codierte Erkennung analysiert.
- Warnung, wenn eine nicht signierte oder verdächtig signierte Binärdatei als Startdaemon beibehalten wurde. Dies beinhaltet die Analyse einer Konfigurationsdatei, die Extrahierung eines eingebetteten Binärpfads aus dem Inhalt und die Verwendung von Metadaten zu dieser Binärdatei in der Analyse.
- Benachrichtigung, wenn eine Microsoft Office Anwendung ein unerwartetes untergeordnetes Element erstellt hat, um die Ausnutzung von Office-Makros zu identifizieren.

Dieses Beispiel zeigt die Fähigkeit, übergeordnete und untergeordnete Beziehungen zu verstehen, um die Ausnutzung von Anwendungsfunktionen aufzudecken.

- Benachrichtigung, wenn andere opportunistische Aktivitäten auf eine Weise verwendet werden, die auf mögliche Angriffe hinweist. Diese Aktivitätsklasse erfordert Zugriff auf untergeordnete/übergeordnete und Prozessgruppen beziehungen, Befehlszeilenparameter usw., um Missbräuche ansonsten harmloser Aktivitäten (Curl, SSH, Python usw.) aufzudecken.
- Verfolgen Sie die USB-Nutzung im gesamten Unternehmen und melden Sie Metadaten zu Dateien, die auf Wechseldatenträger geschrieben werden.

Um die Auswirkungen dieser Arten der Erkennung besser zu verstehen, ordnet Jamf Protect identifizierte Angriffe gegebenenfalls dem Mitre Att&ck-Framework zu. Darunter fallen heutzutage viele Anwendungsfälle aus dem gesamten Framework, einschließlich der Erkennung von Techniken in den folgenden Kategorien:

- Genauigkeit
- Erstzugriff
- Befehl und Kontrolle
- Abwehrumgehung
- Entdeckung
- Rechteausweitung
- Zugang zu Anmeldeinformationen

Einfache Erfassung und Berichterstellung für Unified Log

Im Rahmen eines Compliance-Audits oder wenn Lücken in anderen Sicherheitskontrollen geschlossen werden sollen, benötigen die meisten Sicherheitsanalysten und IT-Administratoren dringend Endpunktprotokolle. Der von macOS vollzogene Wechsel von Syslog-Dateien zu Unified Logging erschwerte das Sammeln, Inventarisieren und Überprüfen dieser Informationen im gesamten Unternehmen. Die macOS Console.app bietet einen hervorragenden Zugriff auf und Einblick in die Unified Log-Infrastruktur auf einem lokalen Mac, aber sie lässt nicht zu, dass die Organisation diese Daten einfach zentralisiert.

Mit Jamf Protect können Client-Protokolle in ein Aufzeichnungssystem gestreamt werden, sobald sie in das Unified Log geschrieben werden. Um sicherzustellen, dass nur Zieldaten erfasst werden, verwenden Jamf Protect-Administratoren dieselbe Prädikatfiltersprache (NSPredicate) aus dem integrierten Befehlszeilenprogramm „log stream“. Auf diese Weise wird das Erstellen von Aufzeichnungssystemen für Mac Protokolldaten zu einer einfachen Konfiguration anstelle einer mühsamen Erfassung von Maschine zu Maschine. Beispiele hierfür sind An- und Abmelden, SSH-, AirDrop- und Autorisierungsereignisse. Wenn Daten im Unified Log protokolliert werden, kann Jamf Protect sie erfassen.

Ausstattung mit dem Standard der Apple Verwaltung

Support am Tag der Veröffentlichung

Jamf Protect nutzt native Apple-Technologien, um eine Schnittstelle zu macOS herzustellen und die für Sicherheitsentscheidungen erforderlichen Daten zu sammeln. Zu diesen Technologien gehören neue Frameworks wie das Enterprise Security Framework (ESF) für Catalina+ und das Open BSM Audit Framework. Durch die Verwendung dieser Mechanismen minimiert Jamf Protect mögliche Gerätebeeinträchtigungen. Außerdem kollidiert Jamf Protect nicht mit Änderungen in macOS, die in Patches oder größeren Betriebssystemversionen eingeführt wurden. Das frühzeitige und regelmäßige Patchen ist das am häufigsten empfohlene Sicherheitsprotokoll. Sicherheitstools, die den Support zum Zeitpunkt der Veröffentlichung gewährleisten, sind für die Einhaltung dieses Protokolls von zentraler Bedeutung.

Benutzererfahrung als Leistungsmerkmal

Jamf Protect überwacht die Anwendungs- und Benutzeraktivität kontinuierlich auf potenzielle Bedrohungen, unterlässt jedoch absichtlich die Suche nach ruhender oder auf Microsoft Windows abzielender Malware. Das Scannen von im Dateisystem befindlichen Dateien auf eine Vielzahl von Malware-Signaturen trägt häufig zu einer schlechten Benutzererfahrung bei. Dieser Ansatz steht insofern im Einklang mit Gatekeeper/XProtect, als dass Bedrohungen zum Zeitpunkt der potenziellen Ausführung erkannt werden, sodass die Benutzererfahrung und die Benutzerproduktivität nur minimal beeinträchtigt werden.

Datenschutz

Jamf Protect analysiert Daten auf dem Gerät und sammelt relevante Informationen nur, wenn diese Funktion konfiguriert wurde; dies ist normalerweise der Fall, wenn eine potenziell bösartige Aktivität oder eine Aktivität von großem Interesse in Echtzeit erkannt wird. Dadurch werden die Unternehmensanforderungen mit der Privatsphäre der Benutzer in Einklang gebracht, da weniger Benutzerdaten vom Gerät abgerufen und in der Cloud gespeichert werden. Wenn eine bösartige Aktivität identifiziert wird, werden die identifizierte Aktivität und die zugehörigen Daten an die Cloud-Konsole von Jamf Protect oder an konfigurierte SIEM-Systeme (Security Information and Event Management) weitergeleitet. Alle darüber hinaus speziell angeforderten Daten werden ebenfalls an Jamf Protect oder das SIEM weitergeleitet. Durch Herausfiltern aller unnötigen Daten erhalten Sicherheitsanalysten, die mit der Überwachung und Untersuchung von Vorfällen beauftragt sind, eine qualitativ hochwertige Sammlung anwendbarer Daten.

Weitere Erweiterungen des Apple Sicherheitsmodells

Bewährte Vorgehensweise: Abhärtung von macOS

Während Apple einige der sichersten und zuverlässigsten verfügbaren Betriebssysteme bereitstellt und unterstützt, lautet eine häufig gestellte Frage: Welche zusätzlichen Schritte können unternommen werden, um macOS noch besser an Ihre Unternehmensumgebung anzupassen.

Als erster Schritt wird empfohlen, das MDM-Framework (Mobile Device Management) von Apple für die automatisierte Verwaltung in großem Maßstab zu nutzen. Mit MDM können Sie nicht nur Ihr Unternehmen besser schützen, sondern auch die Verwaltung und Sicherung Ihrer Geräte außerhalb der IT erheblich entlasten.

Das mit OS X 10.7 („Lion“) eingeführte MDM-Framework bietet eine unglaubliche Anzahl von Workflows, um die Gerätefunktionalität an die spezifischen Anforderungen des Unternehmens anzupassen. Konfigurationsprofile und Verwaltungsbefehle sind die zwei gängigsten Methoden, um mithilfe von MDM sicherzustellen, dass Teams in jeder Arbeitsumgebung geschützt sind.

Steigern Sie Ihre Sicherheitsstufe: Kombinieren Sie MDM mit der Leistung von Apple Business Manager, einer kostenlosen Lösung von Apple for Business, mit der Sie die Beschaffung, Verwaltung und mehr von Hardware automatisieren können.

Starten mit Apple

Im Laufe der Jahre hat sich Apple einen Namen als Security-First-Unternehmen gemacht, was sich in macOS widerspiegelt. Native Funktionen wie FileVault 2-Verschlüsselung, Zwei-Faktor-Authentifizierung, Fernsperrungs-/Fernlöschungsfunktion und die Möglichkeit, Passcode-Standards zu erzwingen, sind mit jedem neuen Mac verfügbar, der der Umgebung eines Unternehmens hinzugefügt wird.

Moderne Verwaltungsplattformen wie Jamf Pro nutzen MDM, um diese Funktionen weiterzuentwickeln und die Implementierung, Durchsetzung und Berichterstellung für wertvolle Sicherheitstools wie Verschlüsselung anzupassen.

Erweitern Sie Ihre Lösungen mit Jamf

MDM ist ein wichtiger Eckpfeiler für jedes Unternehmen. Dennoch fragen sich viele, welche weiteren Maßnahmen die Sicherheit verbessern und die Privatsphäre der Mitarbeiter stärken können. Hier kommt Jamf ins Spiel.

Es ist kein Geheimnis, dass die Geräteverwaltung an einem bestimmten Punkt zu einer starken Belastung der Teamressourcen führt. Eine höhere Anzahl von Mitarbeitern bedeutet mehr Hardware, und mehr Hardware bedeutet mehr IT-Aufwand.

Zumindest war dies vor der Einführung von Plattformen zur Geräteverwaltung wie Jamf Pro der Fall.

Durch die Verwendung patentierter Technologien wie Smart Groups – eine Lösung zur Organisation von Unternehmensgeräten und automatischen Ausführung von Verwaltungsfunktionen – wird die Zeit reduziert, die IT-Teams für die Geräteverwaltung aufwenden müssen, und sie haben mehr Zeit für andere alltägliche IT-Aufgaben. Smart Groups überwacht die Gerätebestände aufmerksam und fügt Geräte in Echtzeit zu einer vordefinierten Gruppe hinzu und entfernt sie, wenn sich der Gerätestatus ändert.

Modernes Identitätsmanagement unter macOS

Im Zentrum der modernen Sicherheit steht die Identität, d. h. ein sicherer und individueller Zugriff für Endbenutzer. Legacy-IT stützt sich auf lokale Verzeichnisdienste, um als zentralisierte Aufzeichnungen der Mitarbeiterinformationen wie Name und Abteilung zu fungieren. Da sich die Sicherheits- und Bereitstellungsanforderungen ändern, müssen Unternehmen im Rahmen ihrer Unternehmensstrategie einen neuen Identitätsansatz verfolgen. Mit einem vollständig Cloud-basierten Identity-Stack vereinheitlichen Unternehmen die Identität von Hardware und Software, um Funktionen und erweiterte Workflows zu ermöglichen und letztendlich das Geschäft zu transformieren.

Cloud-basiertes SSO baut auf Informationen aus Verzeichnisdiensten auf und stellt sicher, dass Endbenutzer sichere Anmeldeinformationen eingeben, um auf Unternehmensressourcen zuzugreifen.

Jamf Connect erweitert diese gängigen Formen des Identitätsmanagements.

Jamf Connect vereinheitlicht die Identität aller Unternehmensanwendungen und des Mac des Benutzers, ohne das Vertrauen zu beeinträchtigen. Endbenutzer nutzen eine einzige Cloud-Identität, um einfach und schnell Zugriff auf Ressourcen zu erhalten, die sie für ihre Produktivität benötigen.

Jamf Connect bietet Unternehmen folgende Vorteile:

- Optimierte Bereitstellung und Authentifizierung ohne Konfigurationsaufwand für die vollständige Unterstützung von dezentral und vor Ort tätigen Mitarbeitern
- Automatisierte Synchronisierung von Benutzeridentitäten und Geräteanmeldeinformationen
- IT mit umfassenden Identitätsverwaltungsfunktionen für alle ihre Dienste und Geräte

Reagieren auf und Beheben von Bedrohungen auf dem Mac

Jamf Pro – der Standard bei der Apple-Verwaltung – bietet Dashboards, mit denen Unternehmen über den Status ihrer Mac Geräte informiert werden können, und kennzeichnet Hardware, die Aufmerksamkeit erfordert. Mithilfe der patentierten Smart Group-Funktionalität können IT-Administratoren auf Geräte abzielen, die zur Verbesserung der Sicherheit aktualisiert oder gepatcht werden müssen. Dies alles erfolgt dezentral und kann automatisiert werden, sodass die IT das Gerät niemals physisch berühren muss.

Durch die Kombination von Jamf Protect mit Jamf Pro wird die Beseitigung von Bedrohungen noch einen Schritt weiter vorangetrieben. Mithilfe dieser Smart Group-Technologie können alle MDM- und Jamf Pro-Befehle als Reaktion auf eine aktivitätsbasierte Warnung von Jamf Protect koordiniert werden. Dies umfasst die automatisierte Netzwerkisolation, „Reimaging“, fehlgeschlagenen bedingten Zugriff, Benutzerbenachrichtigungen sowie eine beliebige Anzahl anderer gezielter Formen der Wiederherstellung und Reaktion. Jamf Pro und Jamf Connect können bei Angriffen auf einen Benutzer oder ein Gerät eine Sperrung der Anmeldeinformationen, Zugriffsänderungen und eine Vielzahl anderer Abhilfemaßnahmen im Zusammenhang mit der Identität veranlassen.

Ergänzung von Apple für beispiellose Vorteile

Apple wird nur dann im Unternehmen an Zugkraft gewinnen, wenn die Mac Nachfrage der Benutzer steigt. Mit den richtigen Tools können IT-Teams und Teams für Datensicherheit zuversichtlich eine Mac-Initiative einführen, die Benutzern die erforderlichen Ressourcen und den benötigten Zugriff bieten – und zwar ohne Abstriche in Bezug auf Datensicherheit und Datenschutz.

Nutzen Sie noch heute die Vorteile der Jamf Unternehmenslösungen die Ihr modernes Unternehmen benötigt.

Erste Schritte

Gerne können Sie sich auch an einen Händler für Apple Geräte Ihrer Wahl wenden, um Jamf kostenlos zu testen.