jamf

WHITEPAPER

Sicherheits-erweiterungen: macOS

Native Privatsphäre und Sicherheit, aber kein Betriebssystem ist perfekt.

Das Bedürfnis nach Sicherheit erstreckt sich über alle Betriebssysteme und macOS ist keine Ausnahme. Apple hat viel in die Bereitstellung nativer Datenschutz- und Sicherheitsfunktionen investiert, aber der Wert eines Angriffs auf die Mac-Plattform steigt mit dem wachsenden Marktanteil in Unternehmen, was sie zu einem begehrten Ziel für Malware, Sicherheitsverletzungen und die Entdeckung von Sicherheitslücken macht. Mehr denn je erlauben Unternehmen ihren Mitarbeiter*innen die Nutzung von macOS im Rahmen von Programmen, die von den Mitarbeiter*innen selbst gewählt werden können. Dabei stellten sie fest, dass wie bei jeder anderen Plattform zusätzliche Sicherheit und Transparenz erforderlich sind.

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

Und während die Apple Betriebssysteme sowohl den Benutzer/die Benutzerin als auch seine Privatsphäre schützen, hatten Benutzerfreundlichkeit und Produktivität schon immer oberste Priorität. Die Apple Experience konzentriert sich stark auf den Benutzer/die Benutzerin und nicht auf das Unternehmen, in dem er tätig ist. Das Gleiche gilt für viele der Sicherheits- und Datenschutzfunktionen in macOS.

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

Sie werden lernen:

- Details zu verfügbaren integrierten macOS 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

Apps auf macOS

Apple hat große Anstrengungen unternommen, um Sicherheitsfunktionen zu entwickeln, die den Benutzer*innen und die von ihm ausgeführten Drittanbieterprogramme 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 dem umfassenden Sicherheitsleitfaden von Apple für die Plattform unter: **support.apple.com/guide/security** (auf Englisch).

Überprüfen Sie das Vertrauen mit Gatekeeper.

Der von Apple bevorzugte und vertrauenswürdigste Weg zur Installation von Drittanbieterprogrammen ist der 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 Apps im App Store ein, und viele geschäftskritische Apps sind für diese Art des Vertriebs nicht geeignet.

Wenn der Vertrieb über den App Store nicht in Frage kommt, erlaubt Apple den macOS Entwickler*innen, ihre Programme direkt über gehostete Downloads und andere traditionelle Vertriebsmethoden zu vertreiben. Um diese „Ad-hoc"-Verteilungen zu unterstützen, hat Apple weitere Kontrollen in das Betriebssystem eingeführt, um das Risiko einer weit verbreiteten Verteilung von Software auf macOS Geräten zu verringern. Gatekeeper ist der Name der Funktion, die im Mittelpunkt der Verifizierungsprüfungen von Apple steht. 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 Akzeptanzstufen für die Zulassung von Apps, die aus dem „App Store" oder dem „App Store und identifizierte Entwickler*innen" heruntergeladen wurden, bestehen nach wie vor, aber die Möglichkeit, problematischen oder riskanten Code auszuführen, wird weiterhin marginalisiert.

Beachten Sie, dass diese Überprüfungen nur für Apps gelten, die aus dem Internet heruntergeladen werden. Apple verfolgt 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 Quarantäne-Attributs, um festzustellen, ob es ausgeführt werden kann.
Eine dieser grundlegenden Überprüfungen ist, ob die Apps von einem legitimen Entwickler*innen signiert ist oder ob sie über den App Store vertrieben wurde, je nach der zuvor besprochenen Einstellung.

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

Ab macOS Catalina müssen Apps von Apple beglaubigt werden, um die Gatekeeper Überprüfung zu bestehen. Damit eine App die Prüfung bestehen kann, muss sie zur Analyse auf Apple hochgeladen werden. Nach erfolgreicher Analyse wird die App mit Beglaubigungsdaten verknüpft, die darauf hinweisen, dass dieser zusätzliche Schritt der Überprüfung bestanden wurde.

Das ultimative Vertrauen liegt beim Benutzer/bei der Benutzerin

Im Namen der Benutzerfreundlichkeit erlaubt macOS dem Endbenutzer/der Endbenutzerin in vielen Situationen, Gatekeeper „außer Kraft zu setzen". Der Benutzer/die Benutzerin kann einfach mit der rechten Maustaste auf die App klicken und „Öffnen" oder „Öffnen mit" wählen. Anstatt den Start der Apps pauschal zu verweigern, wird der Benutzer/die Benutzerin in einer neuen Eingabeaufforderung lediglich gewarnt, dass er eine unbekannte oder potenziell bösartige Apps startet, aber Gatekeeper erlaubt ihm, dies zu tun. Es ist wichtig anzumerken, dass Malware, die XProtect definitiv identifiziert hat, nicht von einem Benutzer/einer Benutzerin zur Ausführung autorisiert werden kann.

Nachdem die App zum ersten Mal ausgeführt wurde, wird die Quarantänekomponente aktualisiert, sodass die Gatekeeper Aktionen beim nächsten Öffnen der App 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 Appaktiviert, während MRT das Dateisystem regelmäßig scannt.

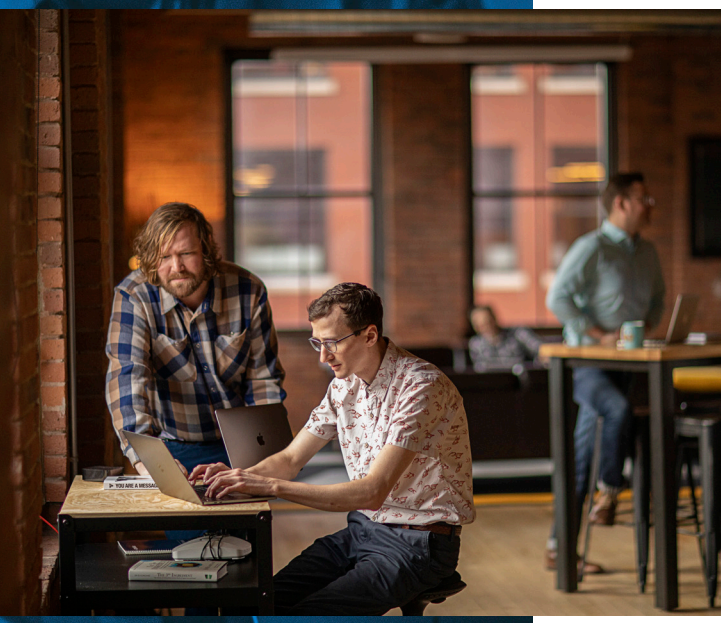
XProtect arbeitet mit einer binären Signatur-Scanengine namens Yara. Yara unterstützt flexible und leistungsstarke binäre Signaturdefinitionen und eine effiziente Ausführungsengine. Um eine App zu überprüfen, scannt XProtect jeden ausführbaren Download bei der ersten Ausführung und nach nachfolgenden iOS Aktualisierungen. Werden übereinstimmende Signaturen erkannt, wird die Ausführung des Programms nicht zulässig sein. 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 App das richtige erweiterte Quarantäneattribut besitzt, das nach der ersten erfolgreichen Ausführung der App aktualisiert wird.

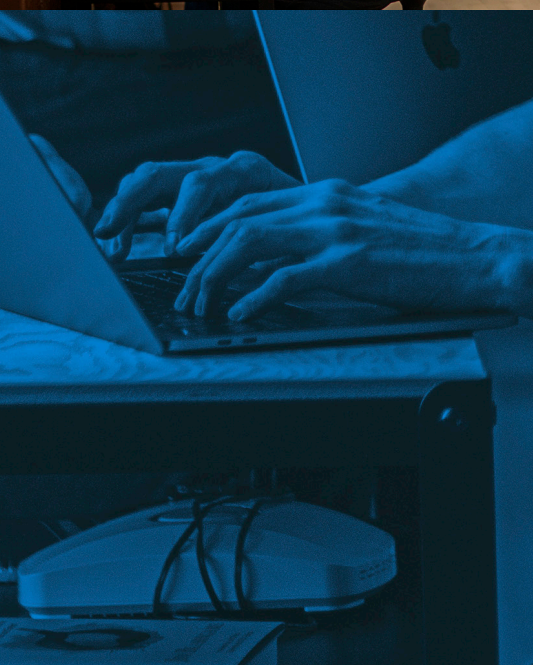
MRT hingegen wird nicht zur Programmlaufzeit, sondern nach einem Zeitplan ausgeführt und durchsucht das Dateisystem nach bestimmten Dateinamen und Artefakten, die mit früherer Malware in Verbindung gebracht werden, und entfernt sie, wenn sie entdeckt werden. Diese Funktion ist hauptsächlich dazu gedacht, bekannte Bedrohungen zu finden und zu beseitigen, die möglicherweise bereits in der macOS Population ausgeführt werden.

Erweitern Sie Gatekeeper auf das Unternehmen.

Gatekeeper arbeitet effektiv und wie beabsichtigt. Die Funktion blockiert den Start nicht vertrauenswürdiger Apps und benachrichtigt den Benutzer/die Benutzerin, wenn eine App als verdächtig oder bösartig erachtet wird. IT-Administrator*innen und Sicherheitsbeauftragte benötigen Transparenz bei Versuchen, nicht vertrauenswürdige Software auf einer Unternehmensanlage auszuführen. Noch wichtiger ist, dass sie sich darüber im Klaren sein müssen, dass ein Benutzer/eine Benutzerin mit der rechten Maustaste auf eine App geklickt und diese gestartet hat, um eine Sicherheitskontrolle für Unternehmen effektiv zu umgehen. Um diese Unternehmensanforderungen zu erfüllen, überwacht Jamf Protect — eine speziell für Mac entwickelte Endpunkt Sicherheitslösung — Hinweise auf 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, das Vertrauensmodell für Entwickler*innen zu übernehmen, indem sie zusätzliche Signierinformationen als nicht vertrauenswürdig in der Unternehmensumgebung registrieren. Mit dem neuesten Endpoint Security Framework von Apple verweigert Jamf Protect proaktiv die Ausführung von Apps in der unternehmensspezifischen Blockierliste. Dies kann auf Anwendungsebene (Anwendungs-ID) oder auf Hersteller-Ebene (Entwicklerteam-ID) definiert werden.





Darüber hinaus bietet macOS keine Signaturen oder Blockierung für eine Vielzahl von Grayware (potenziell unerwünschte oder nicht genehmigte Software), zu der viele Adware- und Krypto-Miner-Apps gehören, die unerwünschtes und potenziell invasives Verhalten zeigen. Oft sind diese Programme rechtmäßig von einem Apple Entwickler/einer Apple Entwicklerin signiert und der Benutzer/die Benutzerin 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 den Betrieb dieser Apps ein.

Die Risikoermittlung ist jedoch im Unternehmen anders, sodass ein strengerer und gezielterer Ansatz möglicherweise gewünscht wird. Daher setzt Jamf Protect seinen eigenen Satz an verwalteten Yara Regeln, binären Signaturen und nicht vertrauenswürdigen Entwicklerzertifikaten durch, die zum Scannen von Prozessen bei der Ausführung verwendet werden, unabhängig davon, ob das erweiterte Quarantäneattribut vorhanden ist oder nicht. Dadurch wird sichergestellt, dass bestehende Apps bei der nächsten Ausführung erneut gescannt werden, wenn neue Signaturen hinzugefügt werden und das Unternehmen seine Sicherheitslage aktualisiert.

Jamf kuratiert diesen Feed bekannter Mac Malware auf der Grundlage von Jamfs umfangreichen Recherchen zu macOS Bedrohungen sowie Daten zu Mac Bedrohungen von Dritten. Organisationen, die eine noch genauere Kontrolle über die in ihrer Umgebung ausgeführte Software wünschen, können die Liste der von Jamf Protect blockierten Apps um ihre eigene Liste mit binären Hashes, TeamIDs usw. erweitern. Wenn eine App 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 angreifende 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.

Erweitern Sie das Vertrauensmodell des App Stores mit Self Service.

In bestimmten Situationen kann es sinnvoll sein, die Programme vorzuschreiben, die Ihre Benutzer installieren können, indem sie einen Self-Service-App-Store nutzen, der mit von der IT-Abteilung genehmigten Ressourcen vorbesetzt ist.
Jamf Self Service ermöglicht einen sicheren und sofortigen Ressourcenzugriff, indem es der IT-Abteilung die Möglichkeit gibt, einen eigenen Katalog für Unternehmensapps zu erstellen, in dem Benutzer*innen Apps installieren, Konfigurationen aktualisieren und allgemeine Probleme selbständig beheben können — ohne ein IT-Hilfeticket zu benötigen.

Steuerung und Überwachung des Appverhaltens.

Begrenzen und bestätigen Sie das Verhalten von Apps mit Datenschutzkontrollen.

Kontrollen zum Systemdatenschutz wurden in macOS Mojave eingeführt. Bei diesen Kontrollen müssen Benutzer*innen (oder Unternehmen) den Zugriff auf bestimmte Aktionen und Ordner pro Apperlauben. Sobald den Applikationen der Zugriff auf bestimmte Aktionen gewährt wurde, werden sie nicht mehr gefragt, wenn die Aktion in Zukunft von derselben Applikation ausgeführt wird. Diese Funktion stellt sicher, dass Apps ausdrücklich der Zugriff auf potenziell sensible Teile des Betriebssystems (Webcam, Mikrofon, Tastatureingaben, Downloads) gestattet wird, und veranlasst die Benutzer*innen dazu, die Geschwindigkeit zu verringern und zu bestätigen, dass sie den Apps Zugriff auf private Daten gewähren.

Gehen Sie über die Kontrollen hinaus und auditieren und analysieren Sie das Applikationsverhalten.

Während Datenschutzkontrollen die Berechtigung von Apps einschränken, machen Benutzer*innen Fehler, und Berechtigungen werden missbraucht. Wir haben bereits darüber berichtet, wie Jamf Protect einen Einblick in die Aktionen der integrierten Apple Sicherheitsfunktionen und der herkömmlichen Malware/Adware-Präventionsfunktionen bietet, um Unternehmen zu informieren und zu schützen. 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 Endpunkt Erkennungs- und Reaktionsprodukte (EDR) reserviert sind – jedoch mit einem Apple First Ansatz und einem Blick auf die Datenschutz- und Sicherheitsstandards, die MacOS Benutzer*innen erwarten.

Erkennungstechnik mit Jamf Protect

Das Herzstück des Jamf Protect Agent*innen ist ein leichtgewichtiger Sensor für den Benutzermodus (ohne Begleittext), der eine von Apples eigenen Logikausführungsmaschinen, GameplayKit, nutzt. Obwohl die Verwendung einer Spiele-Engine für die Analyse von Sicherheitsereignissen unüblich ist, ermöglicht sie Jamf, eng in das Apple Ökosystem integriert zu bleiben und Daten auf dem Gerät zu analysieren, bis sie gesammelt 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. Dieses Design steht im Gegensatz zu vielen Sicherheitslösungen, die sich zunächst auf die Windows Plattform konzentrieren und dann nachträglich auf macOS portiert werden — oder zu denen, die verlangen, dass alle Daten in der Cloud gesammelt und analysiert werden.

Ein zusätzlicher Vorteil von GameplayKit ist, dass es, wie Yara, die Ausführungsengine von den Erkennungsdefinitionen trennt, sodass 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 Protect wurde speziell entwickelt, um die umfangreichen Funktionen von NSPredicate zu nutzen, einschließlich der Möglichkeit, native Funktionen aufzurufen und Datenmodelle miteinander zu verknüpfen. Dadurch werden Fähigkeiten freigesetzt, die auf andere, traditionellere Weise nur umständlich oder mit hohem Rechenaufwand zu implementieren sind. Zum Beispiel können wir das Daten Modell von Jamf Protect und NSPredicate verwenden:

- 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 unsignierte oder verdächtig signierte Binärdatei als Start-Daemon bestehen bleibt. 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.

- Warnung, wenn eine Microsoft Office Apps ein unerwartetes Kind erstellt hat, um die Ausnutzung von Office-Makros zu erkennen. Dieses Beispiel verdeutlicht die Fähigkeit, Kind-Eltern-Beziehungen zu verstehen und die Ausnutzung von Appfunktionen aufzudecken.

- Alarmieren Sie, wenn andere „Leben-am-Land”-Aktivitäten in einer Weise genutzt werden, die auf Angriffe hinweist. Für diese Art von Aktivitäten ist der Zugang zu Kind/Eltern- und Prozessgruppenbeziehungen, Befehlszeilenparametern usw. erforderlich, um den Missbrauch von ansonsten harmlosen 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 von Erkennungen leicht nachvollziehen zu können, ordnet Jamf Protect die erkannten Angriffe dem MITRE ATT&CK™ Framework zu, falls zutreffend. Die Abdeckung umfasst heute Anwendungsfälle aus dem gesamten Framework, einschließlich der Erkennung von Techniken in den folgenden Kategorien:

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

Einfache einheitliche Protokollerfassung und Berichterstattung

Im Rahmen eines Compliance-Audits oder wenn Lücken in anderen Sicherheitskontrollen geschlossen werden sollen, benötigen die meisten Sicherheitsanalysten und IT-Administrator*innen 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 Administrator*innen 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 sammeln.

Angleichungan die Standards von Apple.

Day-of-Release-Unterstützung

Um eine Schnittstelle zu macOS zu schaffen und die für Sicherheitsentscheidungen erforderlichen Daten zu sammeln, nutzt Jamf Protect native Apple Technologien. Zu diesen Technologien gehören aufkommende Frameworks wie Apples Endgerätesicherheits-API und das OpenBSM Audit-Framework prior. Durch die Verwendung dieser Mechanismen minimiert Jamf Protect die Auswirkungen auf das Gerät und wird nicht durch Änderungen in macOS beeinträchtigt, die durch Patches oder größere Betriebssystemversionen eingeführt werden. Das frühzeitige und regelmäßige Patchen ist das am häufigsten empfohlene Sicherheitsprotokoll. Sicherheitstools, die sich strikt an den Tag der Veröffentlichung halten, sind der Schlüssel zur Einhaltung dieses Protokolls und eine entscheidende Komponente in einer umfassenden Sicherheitsstrategie.

Benutzererfahrung als Leistungsmerkmal

Jamf Protect überwacht zwar kontinuierlich die App und Benutzeraktivitäten auf potenzielle Bedrohungen, sucht aber bewusst nicht nach ruhender oder Microsoft Windows bezogener Malware. Das Scannen von Dateien, die sich einfach nur 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 der potenziellen Ausführung identifiziert werden, sodass die Benutzererfahrung und die Benutzerproduktivität möglichst wenig beeinträchtigt werden.

Datenschutz

Jamf Protect analysiert die Daten auf dem Gerät und sammelt nur dann relevante Informationen, wenn es so konfiguriert ist, d. h. wenn eine potenziell bösartige oder hochinteressante Aktivität in Echtzeit erkannt wird. Dadurch werden die Unternehmensanforderungen mit der Privatsphäre der Benutzer*innen in Einklang gebracht, da weniger Benutzerdaten vom Gerät abgerufen und in der Cloud gespeichert werden. Wenn eine bösartige Aktivität erkannt wird, werden die identifizierte Aktivität und die damit verbundenen Daten an die Jamf Protect Cloud Konsole oder konfigurierte SIEM-Systeme (Security Information und 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.

Andere Erweiterungen des Apple Sicherheitsmodells

Bewährte Vorgehensweise: Abhärtung 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.

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 die FileVault 2-Verschlüsselung, die Zwei-Faktor-Authentifizierung, die Funktion zum Sperren/Löschen aus der Ferne und die Fähigkeit, Passcodes zu erzwingen, sind mit jedem neuen Mac, der zur Umgebung einer Organisation hinzugefügt wird, verfügbar.

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*innen 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 Mitarbeiter*innen 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.

Mit patentierten Technologien wie Smart Groups, die bei der Organisation von Unternehmensgeräten und der automatischen Ausführung von Verwaltungsfunktionen helfen, können IT-Teams weniger Zeit mit der Geräteverwaltung verbringen und 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

Der Kern moderner Sicherheit ist die Identität — ein sicherer und individueller Zugang für Endbenutzer*innen. LegaLegacy 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 das Identitäts- und Zugriffsmanagement als Teil ihrer Unternehmensstrategie wählen. Mit einem vollständigen Cloud basierten Identitätsstack können Unternehmen die Identität über Hardware und Software hinweg vereinheitlichen, um Funktionen und erweiterte Arbeitsabläufe freizuschalten und letztendlich das Geschäft zu transformieren.

Cloud basiertes Single Sign-On (SSO) baut auf Informationen aus Verzeichnisdiensten auf und gewährleistet, dass Endbenutzer sichere Anmeldedaten eingeben, um auf Unternehmensressourcen zuzugreifen.

Jamf Connect erweitert diese gängigen Formen des Identitätsmanagements.

Jamf Connect vereinheitlicht die Identität in allen Apps des Unternehmens und auf dem Mac des Benutzers/der Benutzerin mit nahtlosen Workflows zur Authentifizierung. Endbenutzer*innen nutzen eine einzige Cloud Identität, um einfach und schnell Zugang zu den Ressourcen zu erhalten, die sie für ihre Produktivität benötigen.
Jamf Connect bietet Unternehmen folgende Vorteile:

- Optimierte Bereitstellung und Authentifizierung für die vollständige Unterstützung von Mitarbeiter*innen vor Ort und an anderen Standorten
- Automatisierte Synchronisierung von Benutzeridentitäten und Geräteanmeldeinformationen
- IT mit umfassenden Identitätsverwaltungsfunktionen für alle ihre Dienste und Geräte
- Eine Zero Trust-Netzwerkzugriff (ZTNA)-Lösung, die ältere VPNs (virtuelle private Netzwerke) ersetzt und die Anforderungen moderner, hybrider Unternehmen erfüllt

Reagieren auf und Beheben von Bedrohungen auf dem Mac

Jamf Pro stellt Dashboards zur Verfügung, die Organisationen über den Zustand ihrer Mac Geräte auf dem Laufenden halten und Hardware markieren, die Aufmerksamkeit erfordert. Mithilfe der patentierten Smart Group Funktionalität können IT-Administrator*innen auf Geräte abzielen, die zur Verbesserung der Sicherheit aktualisiert oder gepatcht werden müssen. Dies alles geschieht aus der Ferne und kann automatisiert werden, sodass die IT-Abteilung das Gerät nie 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. Dazu gehören automatische Netzwerkisolierung, fehlgeschlagene Zugangskontrollen, Benutzerbenachrichtigungen oder andere gezielte Formen der Abhilfe und Reaktion. Jamf Pro und Jamf Connect können bei Angriffen auf einen Benutzer/eine Benutzerin oder ein Gerät eine Sperrung der Anmeldeinformationen, Zugriffsänderungen und eine Vielzahl anderer Abhilfemaßnahmen im Zusammenhang mit der Identität veranlassen.

Sicherheit über die Geräteverwaltung hinaus

Lesen Sie unseren Bericht über den Stand der Apple Sicherheit in Unternehmen, für den 1.500 IT- und InfoSec-Expert*innen befragt wurden. Er umfasst die aktuelle Gerätenutzung und -nutzung, Herausforderungen für die Gerätesicherheit und den zukünftigen Stand der Endgerätesicherheit.

Trusted Access

ist die Lösung von Jamf für Sicherheit jenseits des Sicherheitsmanagements. Trusted Access ist ein einzigartiger Arbeitsablauf, der Gerätemanagement, Benutzeridentität und Endgerätesicherheit zusammenführt, um Unternehmen dabei zu helfen, eine Arbeitsumgebung zu schaffen, die von den Benutzer*innen geschätzt wird, und einen sicheren Arbeitsplatz zu schaffen, dem Unternehmen vertrauen.

Durch die Verwendung von Jamf Protect mit Jamf Pro und die Nutzung von Jamf Connect können Administrator*innen sicherstellen, dass nur vertrauenswürdige Benutzer*innen auf Unternehmensapps über vertrauenswürdige und konforme Geräte zugreifen. Wenn es ein Problem mit einem infizierten Gerät gibt, kann es mit Jamf Pro schnell behoben und wieder in Betrieb genommen werden.

Trusted Access mit Jamf erhöht die Sicherheit Ihres modernen Arbeitsplatzes drastisch, während die Arbeit für Ihre Benutzer*innen rationalisiert wird — unabhängig davon, wo die Arbeit stattfindet.

Verwalten und sichern Sie Apple mit ungeahnten Vorteilen.

Mit den richtigen Tools können IT- und Informationssicherheitsteams eine Mac Initiative einführen, die Identität und den Zugriff verifizieren und authentifizieren und den Benutzer*innen die benötigten Ressourcen und den Zugriff gewähren — und das alles unter Berücksichtigung von Sicherheit und Datenschutz.

Nutzen Sie noch heute die Vorteile der Jamf Unternehmenslösungen und profitieren Sie von der Transparenz und den Abhilfemaßnahmen, die Ihr modernes Unternehmen benötigt.

Los geht's

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

jamf

www.jamf.com/de/