jamf

WHITE PAPER

Kernel Extensions: Übergang zu einem KEXT-losen Workflow

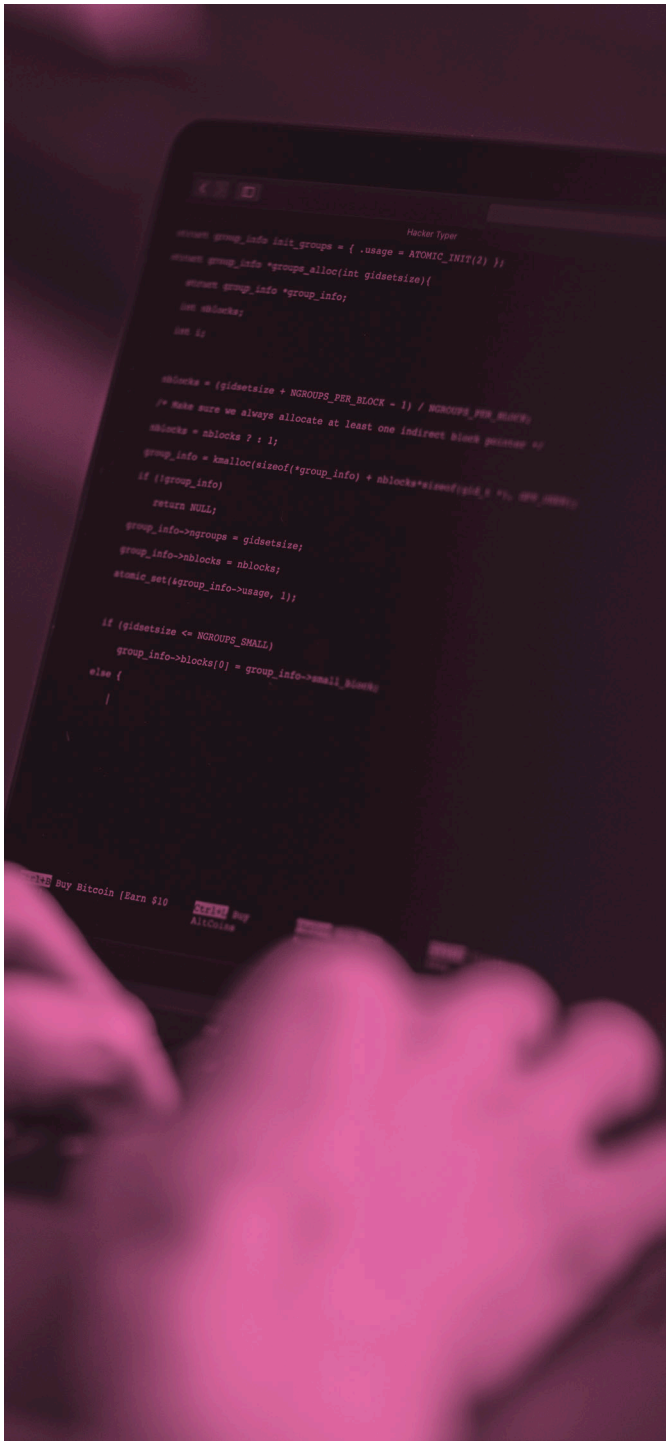
Auf der Apple Worldwide Developers Conference (WWDC) 2019 gab Apple bekannt, den Einsatz von Kernel Extensions (KEXTs) nicht mehr unterstützen zu wollen. Dies ist Teil ihrer laufenden Bemühungen, macOS zu modernisieren, die Sicherheit zu verbessern und Vertrauenswürdigkeit für Software und Sicherheitslösungen von Drittanbietern zu schaffen, um eine Kompatibilität mit aktualisierten Betriebssystemen zu gewährleisten.

Mit der Veröffentlichung von macOS Big Sur fing Apple an, Kernel Extensions (Kexte) nicht mehr zu unterstützen. Daher sollten Sie sich jetzt mit den Auswirkungen auseinandersetzen, die diese Änderung auf Ihre Umgebung hat, und entsprechende Partner suchen, die Ihnen bei einem Übergang helfen.

In diesem White Paper behandeln wir Folgendes:

- Was sind Kernel Extensions und warum werden sie nicht mehr unterstützt
- Warum Jamf Protect als „kextless“ entwickelt wurde
- Die Vorteile von „kextless“ für die IT, Informationssicherheit und Nutzer

Was sind Kernel Extensions?



Innerhalb eines Systems gibt es zwei Ebenen oder Modi – Nutzermodus und Kernelmodus. Im Nutzermodus existieren viele Anwendungen gleichzeitig mit inhärenten Grenzen zwischen ihnen. Diese Grenzen schränken den Zugriff ein, den Apps innerhalb ihrer spezifischen, vordefinierte Grenzen haben. Im gesamten Nutzermodus ist eine Interaktion mit allem, was im Kernelmodus und außerhalb bestimmter Fähigkeiten (APIs) ausgeführt wird, nicht möglich. Auch Änderungen können nicht vorgenommen werden. Auf diese Weise wird sichergestellt, dass keine Anwendung das gesamte System lahmlegt sowie, dass Anwendungen es schwer haben andere Anwendungen zu beeinträchtigen, welche innerhalb der festgelegten Grenzen agieren.

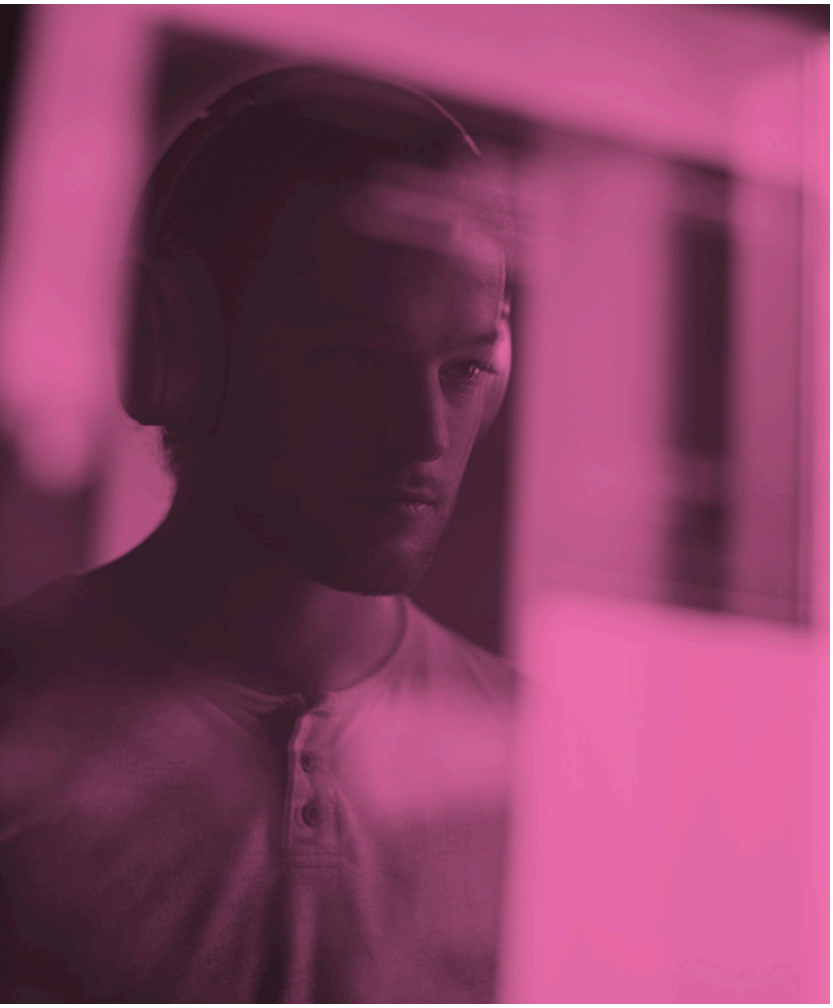
Im Kernelmodus gibt es hingegen keine Grenzen. Er kann in jede ausgeführten Anwendung eingreifen, jegliche Daten modifizieren, hat bestimmte Verwaltungsrechte und kann sogar das Betriebssystem selbst beeinträchtigen. Schließlich ist der Kernelbereich konzipiert, um nur das Betriebssystem zu enthalten. Daher stellt alles, was im Kernelmodus ausgeführt wird, ein Stabilitätsrisiko, ein Sicherheitsrisiko und ein Datenschutzrisiko dar. Software für den Kernelmodus hat strengere Anforderungen an die Qualitätskontrolle als normale Anwendungen.

Kexte bieten Entwicklern die Möglichkeit, sich den Kernelbereich zunutze zu machen und im Kernel zu entwickeln. Von dort aus können Entwickler Prozesse überwachen, verhindern, dass Anwendungen ausgeführt werden und im Allgemeinen alle Aktionen auf einem Gerät überwachen. In älteren Betriebssystemen nutzten viele Implementierungen von Sicherheitsüberwachung und Anwendungssteuerungen diese Technologie. Allerdings sind Anbieter immer noch fehlbar.

Warum unterstützt Apple Kernel Extensions nicht mehr?

Die Codierung im Kernel ist ein zweischneidiges Schwert. Dadurch haben Apps und Software von Drittanbietern direkten Zugriff und können wesentliche Änderungen vornehmen. Wenn jedoch etwas schiefläuft, läuft es meistens so richtig schief. Erweiterungen im Kernel zu entwickeln wird von Apple nicht unterstützt, weil man oft das Betriebssystem selbst beeinträchtigt – und zwar so, dass es möglicherweise nicht mehr ordnungsgemäß funktioniert. Da es im Kernel keine Grenzen gibt, gibt es fast nichts, was im Falle einer Störung verhindert, dass Aspekte betroffen sind, die die Funktionsfähigkeit des Geräts beeinträchtigen. Darüber hinaus hängen alle Änderungen davon ab, dass Apple die Kernel-Anteile zukünftiger Betriebssystemversionen nicht auf eine Weise ändert, die Drittanbieter-Anwendungen nicht erwarten.

Apple empfiehlt mit der Verwendung von KEXT vorsichtig zu sein, da das Unternehmen vorhat, das Betriebssystem in zukünftigen Versionen zu verändern. Wenn Apple einen Aspekt des Betriebssystems ändert, von dem ein KEXT abhängig ist, und das Gerät auf die neue Version aktualisiert wird, könnte das viele Probleme und eine Sicherheitslücke zur Folge haben und sogar dazu führen, dass das Gerät unbenutzbar wird – unabhängig davon, ob es sich um ein wesentliches Upgrade, ein kleines Update oder einen ergänzenden Patch handelt.



Einige Hauptnutzer von KEXT-Dateien sind Drittanbieter von Sicherheitslösungen. Aufgrund des Zugriffs und der Fähigkeiten, die Kexte zu bieten haben, setzen viele Sicherheitsanbieter auf KEXT. Dadurch kann Sicherheit wesentlich zur Instabilität beitragen und frustrierend für Unternehmen sein, die einen Sicherheitsanbieter nutzen, der sich auf Kexte verlässt. Denn wenn es Zeit für einen Patch oder ein Upgrade des Betriebssystems ist, brauchen Anbieter Zeit, um ihr Produkt auf dem neuen Betriebssystem zu verifizieren.

Dieses Modell von Kernelmodus, Nutzermodus und Kernel Extensions gibt es nicht nur bei Apple. Windows nennt Kernel Extensions „Treiber“. Sie sind die einzige unterstützte Art und Weise, wie viele Anwendungen funktionieren. Daher ist es einleuchtend, dass Sicherheitsanbieter mit KEXT arbeiten. Viele Sicherheitsanbieter haben ein Hauptprodukt, das zuerst für Windows entwickelt wurde. Dann wollten sie dasselbe Framework auf Apple Geräte anwenden. Mit der einheitlichen Endgeräteverwaltung wurde klar: Man kann nicht ein Tool nutzen und davon ausgehen, dass es auf magische Weise für alle Betriebssysteme funktioniert. Nur wenn man ein Produkt direkt für Apple entwickelt (in diesem Fall für die Sicherheit von Apple), kann man sich die unzähligen Vorteile von Apple zunutze machen.

Es gibt eine Alternative, mit der diese Sicherheitsmaßnahmen getroffen werden kann, ohne dabei ein großes Risiko einzugehen. Eine Alternative, deren höchste Priorität die Sicherheit von Apple Geräten ist. Nachdem Anwendungen im Nutzermodus nie mit diesen internen Strukturen und Systemen interagieren, sind sie vor diesen Änderungen sicher.

Eine fortschrittliche Lösung, die ohne KEXT entwickelt wurde

Am Anfang war Jamf Protect, eine Sicherheitslösung für Endgeräte speziell für Mac, darauf ausgerichtet, Aspekte mit Apple Unterstützung zu nutzen und war nie auf den Einsatz von Kernel Extensions angewiesen. Als Apple auf der WWDC19 verkündet hat, dass sie KEXT nicht mehr unterstützen und eventuell eliminieren werden, hat das Unternehmen auch die neuen Systems Extensions mit dem Endpoint Security Framework, den Network Extensions und dem DriverKit vorgestellt. Jamf konnte dieses neue Konzept willkommen heißen, ohne zuvor Abhängigkeiten von Kernel Extensions rückgängig machen zu müssen. Das führte zu geringeren Auswirkungen auf Geräte, einer besseren Stabilität und starkem Datenschutz für alle Anwendungen, die diese neuen Frameworks übernahmen.

Mit den System Extensions unterstützte Apple das erste Mal eine Methode, mit der Software ohne Zugriff auf den Kernelmodus entwickelt werden kann und dabei ähnliche Ergebnisse erzielt wie Kernel Extensions. Dadurch konnten Sicherheitsanbieter die vielen Informationen und Daten, die sie benötigten, auf sichere Weise erfassen und gleichzeitig das Anliegen von Apple unterstützen, dass Organisationen mit Drittanbietern arbeiten sollten, die keine KEXT nutzen.

Das sind fantastische Neuigkeiten für Jamf Kunden, aber ein kleines Dilemma für viele Anbieter, denen gesagt wurde, dass sie ihr Produkt für Apple Geräte überholen müssten. Jamf Protect musste nicht das Geringste für seine Kunden ändern und konnte die neue Power von Apple direkt nutzen.

jamf | PROTECT

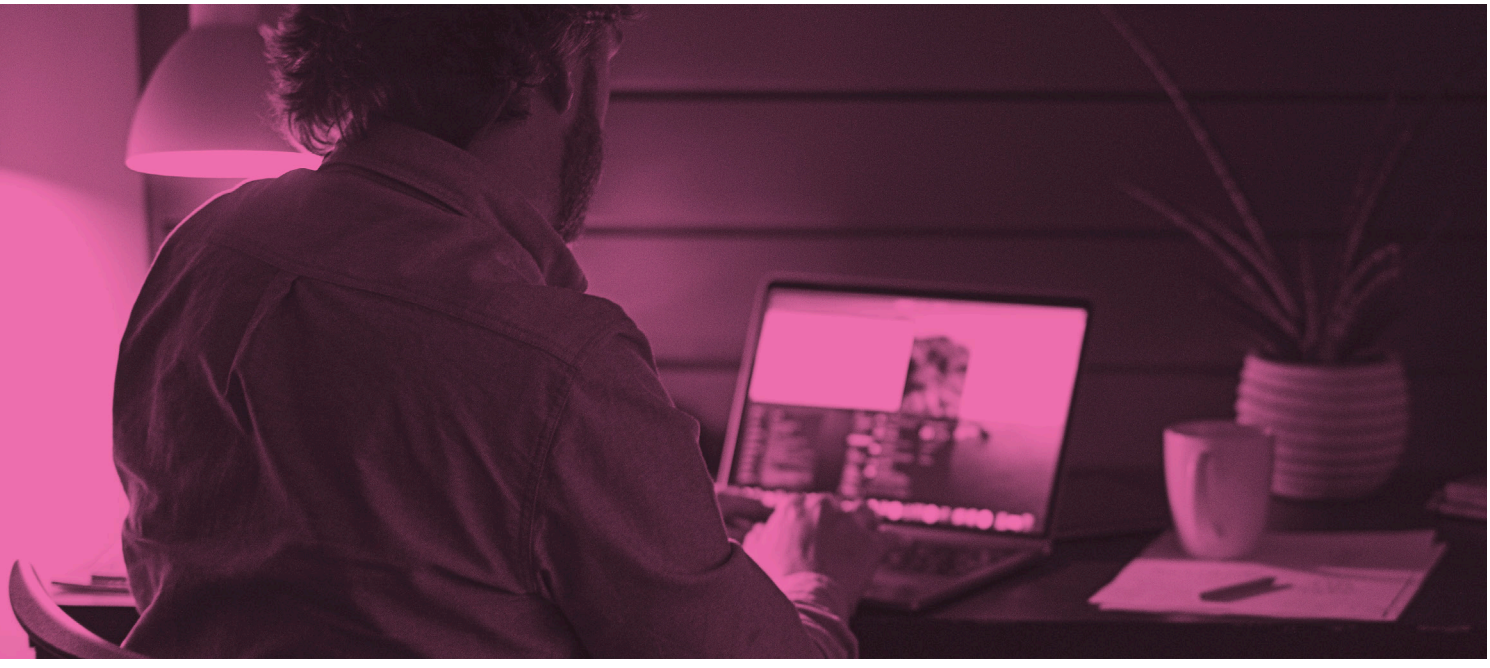
Jamf Protect wurde für Apple Geräte entwickelt und auf die Bedürfnisse von Apple Nutzern und Mac Administratoren zugeschnitten. Deshalb baut Jamf Protect auf dem zentralen Sicherheitskonzept von Apple für macOS auf und verstärkt es mit besserer Prävention, strengeren Kontrollen, mehr Transparenz und Gegenmaßnahmen, die sich Ihrer Umgebung anpassen.

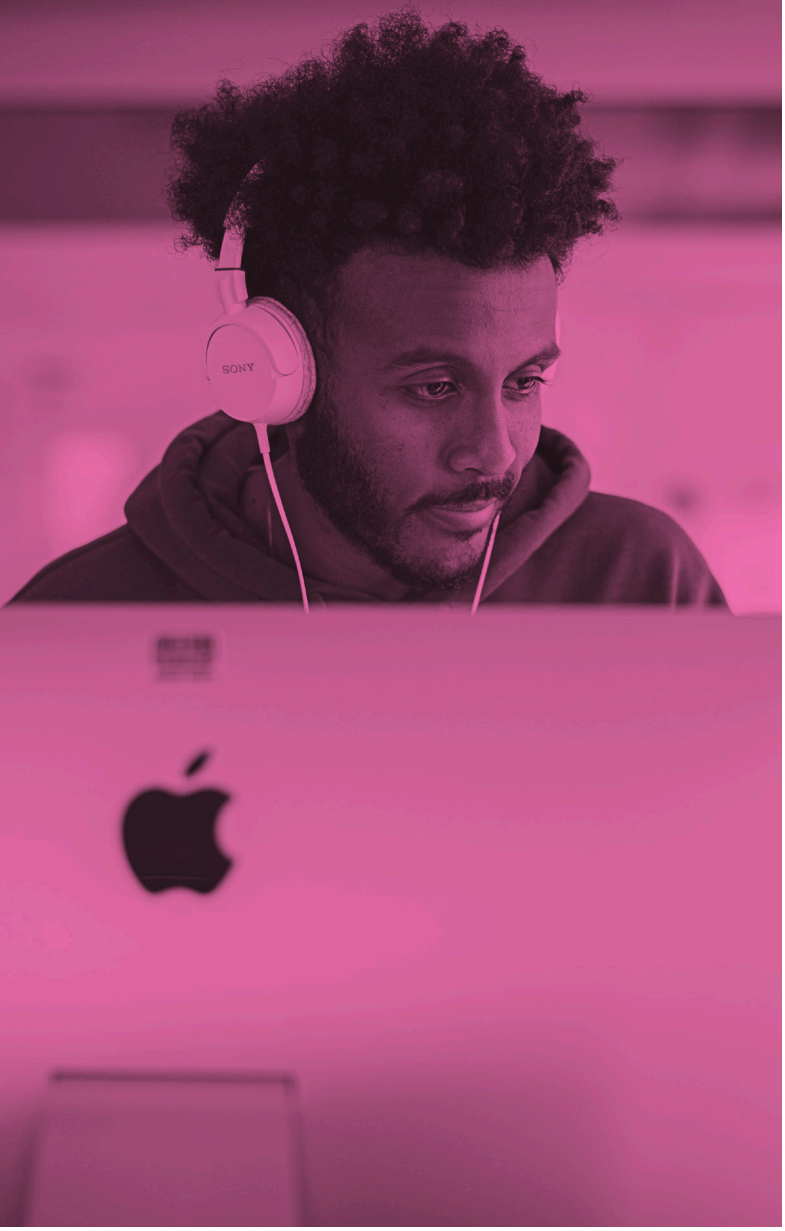
Eine Testversion anfordern oder **mehr erfahren**

Warum ein Anbieter, der nicht mit KEXT arbeitet, die erste Wahl sein sollte

Apple hat angekündigt, dass sie KEXT eliminieren werden. Ob in den nächsten Jahren oder den nächsten Versionen von macOS – es wird geschehen. Es wird also bald der Punkt kommen, an dem es zwingend notwendig sein wird, von KEXT auf die neuen Nutzermodus-Frameworks zu wechseln. Apple hat während der WWDC 2020 deutlich gemacht, dass Anbieter jetzt umsteigen müssen. Das Unternehmen hat sogar Kunden dazu angehalten, Anbieter zu wechseln, wenn diese das neue Modell nicht unterstützen.

Wie bereits erwähnt kann es zu großen Problemen führen, wenn bei Kernel Extensions etwas schiefläuft. Solche Probleme sind aus der Ferne unter Umständen äußerst schwierig festzustellen und zu beheben. Das Ganze ist auch noch zeitraubend. Manche Probleme können womöglich gar nicht aus der Ferne behoben werden. In solchen Fällen müssen die betroffenen Geräte an eine IT-Abteilung oder Apple zur Wiederherstellung geschickt werden. Das führt zu mehr IT-Tickets, längerer Auflösung von IT-Tickets und kann das Nutzererlebnis mit Mac drastisch beeinträchtigen.





Im Zuge der Veröffentlichung von macOS Big Sur, dem neuesten Mac Betriebssystem, soll erwähnt sein, dass Kextless-Sicherheitsanbieter und Kextless-Drittanbieter-Apps den Stress rund um die Aktualisierung von Geräten erheblich reduzieren. Da viele Sicherheitsanbieter ihre Plattformen noch testen, um ihre einwandfreie Funktion auf dem neuen Betriebssystem sicherzustellen, stellt es für Unternehmen einen unnötigen Stressfaktor dar. Unternehmen möchten, dass ihre Geräte kompatibel bleiben, und müssen dafür oftmals kostspielige Ausfallzeit in Kauf nehmen. Jamf hat dieses Problem nicht. Jamf bietet Unterstützung für das Apple Betriebssystem noch am selben Tag, ebenso wie Compliance mit jedem Produkt, einschließlich Jamf Protect.

Hinzu kommt, dass Apple jetzt seine eigene Halbleitertechnik in Form des M1 Chips eingeführt hat: Dadurch stehen Tools, die von Kexten abhängig sind, vor neuen Herausforderungen bezüglich der Endbenutzererfahrung. Jedes macOS Big Sur Gerät, das eine KEXT-Datei ausführte, erforderte bereits, dass entweder ein Endbenutzer die Ausführung der KEXT-Datei bei jedem Start des Geräts bestätigte oder dass eine Lösung für das Mobile Device Management (MDM) verwendet wurde, um die KEXT-Datei über ein Profil zu autorisieren. Mit M1 Geräten müssen Nutzer jedoch zuerst den Wiederherstellungsmodus ihres Gerätes starten, damit es Kexte laden kann, und Anbieter müssen M1 spezifische Versionen der KEXT bereitstellen. Es ist ein mühsamer Prozess, der Kexte auf macOS ihrem Ende näher bringt.

Bereit für einen besseren und sichereren Workflow ohne Kexte?

Abhängigkeit und Nutzung von Kernel Extensions waren immer nur eine kurzfristige Lösung, die zu Instabilität und Unsicherheit in Ihrer Umgebung führte. Damals war es für viele Sicherheitsanbieter ausreichend, aber jetzt gibt es eine effizientere Lösung. Nachdem Apple KEXT nun nicht mehr unterstützt, ist diese überlegene Methode gefragter denn je. Wenden Sie sich an einen Sicherheitsanbieter, der Endgerätesicherheit speziell für Mac bietet und dabei auf die Bedürfnisse der Apple Nutzer achtet – so sind Sie Sicherheitsbedrohungen einen Schritt voraus und dem Erfolg Ihres Teams steht nichts mehr im Wege.

Jamf Protect testen