Wie man die Safari-Startseite auf dem Mac anpasst

Quelle: osxdaily.com, Übersetzung: KJM

Verwenden Sie Safari als Standard-Webbrowser auf Ihrem Mac? Wenn ja, könnte es Sie freuen zu erfahren, dass die Startseite von Safari jetzt anpassbar ist, sofern Sie eine neue Version von Safari auf dem Mac verwenden.

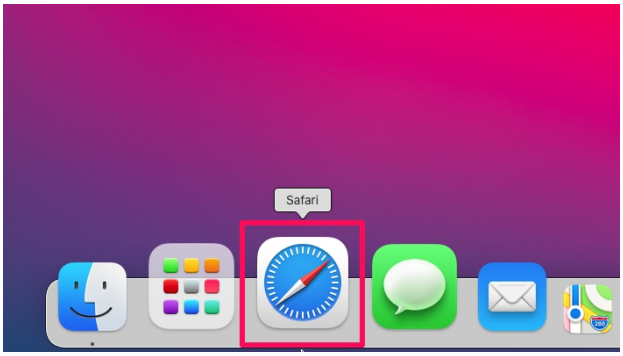
Bei Safari 14 und neueren Versionen ermöglicht die Anpassung der Startseite das Einstellen eines Hintergrundbildes, das Auswählen der angezeigten Abschnitte wie Favoriten oder häufig besuchte Seiten und vieles mehr. Diese modernen Safari-Versionen sind auf macOS Big Sur, macOS Catalina und macOS Mojave verfügbar, so dass Sie loslegen können, wenn Sie eine moderne macOS-Version verwenden.

Schauen wir uns an, wie Sie die Startseite in Safari für Mac anpassen können.

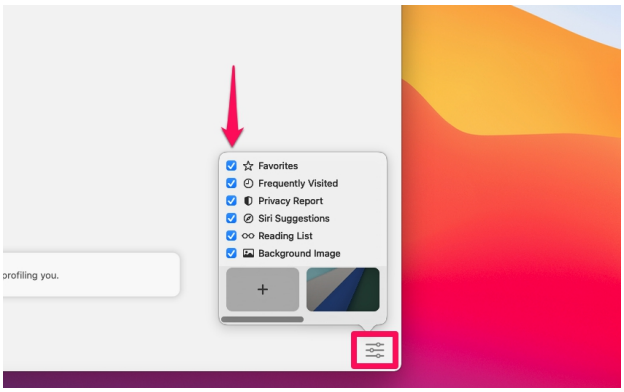
So passen Sie die Safari-Startseite unter macOS an

Das Anpassen der Startseite ist eigentlich ein ziemlich einfaches und unkompliziertes Verfahren, hier ist, was Sie tun möchten:

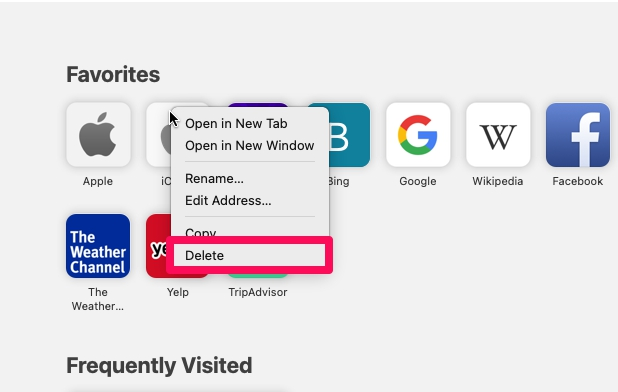
1. Starten Sie "Safari" auf Ihrem Mac über das Dock, Spotlight oder den Ordner "Programme".



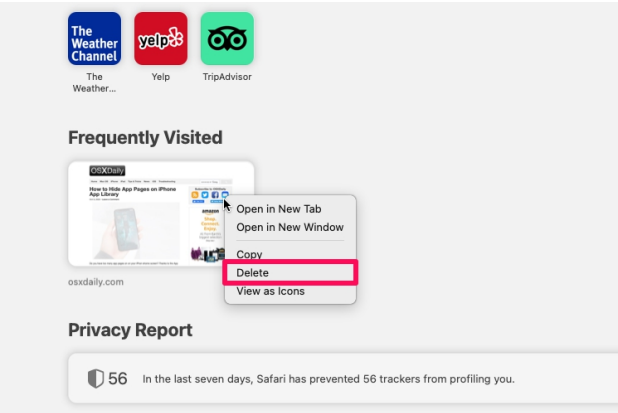
2. Zuerst lernen wir, wie man bestimmte Abschnitte ein-/ausblendet. Klicken Sie dazu auf die Schaltfläche „Anpassen“, die sich in der rechten unteren Ecke des Safari-Fensters befindet. Hier deaktivieren oder aktivieren Sie einfach die Abschnitte, die Sie auf der Startseite ein- oder ausblenden möchten.



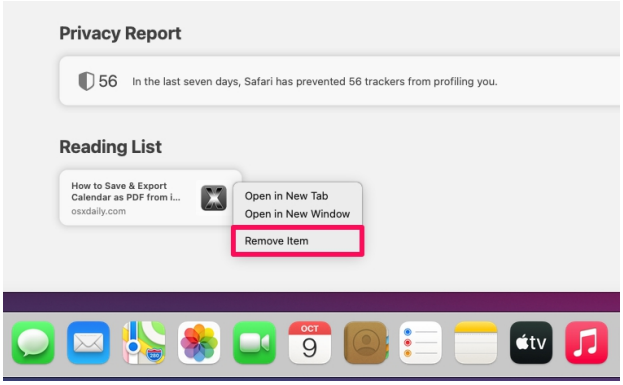
3. Als nächstes sehen wir uns an, wie Sie unerwünschte Favoriten aus Safari entfernen und Ihre Startseite aufräumen können. Klicken Sie dazu mit der rechten Maustaste auf ein beliebiges Symbol unter der Rubrik „Favoriten“ und wählen Sie „Löschen“.



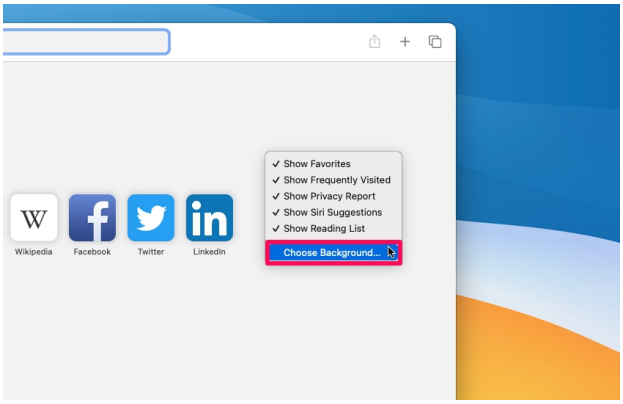
4. Wenn Sie eine der häufig besuchten Websites nicht mehr auf dem Startbildschirm anzeigen möchten, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Löschen“.



5. Auf ähnliche Weise können auch Leselisten entfernt werden. Sie werden am unteren Rand Ihrer Startseite angezeigt. Klicken Sie mit der rechten Maustaste auf eine der Leselisten und wählen Sie „Element entfernen“.



6. In diesem Schritt lernen wir, wie Sie den Safari-Hintergrund ändern können. Klicken Sie dazu einfach mit der rechten Maustaste auf den leeren Bereich der Startseite und klicken Sie auf „Hintergrund auswählen“. Daraufhin öffnet sich der Finder und Sie können ein beliebiges Bild als Hintergrund einstellen.



Und schon haben Sie die Safari-Startseite an Ihre Wünsche angepasst.

Egal, ob Sie Safari 14+ verwenden, das auf macOS Big Sur vorinstalliert ist, oder ob Sie eine eigenständige Version von Safari 14 auf einer älteren Version von macOS wie Catalina oder Mojave verwenden, die obigen Schritte werden identisch sein. Solange Sie eine moderne Safari-Version haben, werden Sie diese Optionen zur Verfügung haben.

Abgesehen von den neuen Anpassungsoptionen können Sie in neueren Versionen von Safari auch den **Datenschutzbericht** für Websites überprüfen, um zu sehen, wie viele Tracker von einer bestimmten Website kontaktiert wurden. Diese Tracker werden automatisch blockiert und daran gehindert, Sie im gesamten Web zu verfolgen.

Safari verfügt außerdem über eine native **Übersetzung** mit Unterstützung für sieben verschiedene Sprachen, wobei weitere Sprachen wahrscheinlich bald folgen werden.

Safari 14 bringt auch einige Leistungsverbesserungen. Nach Angaben von Apple ist Safari nun in der Lage, häufig besuchte Websites im Durchschnitt 50 Prozent schneller zu laden als Google Chrome. Auch die Energieeffizienz wurde verbessert: Im Vergleich zu Drittanbieter-Browsern wie Chrome oder Firefox kann Safari nun bis zu drei Stunden länger Videos streamen und eine Stunde länger im Web surfen.

Fehlersuche unter macOS: Beobachtung und das Protokoll

Quelle: Howard Oakley, eclecticlight.com. Übersetzung: KJM

An einem guten Tag bekomme ich nur zwei oder drei Fragen zu Problemen, die Mac-Anwender haben, gestellt. Wenn viel los ist — normalerweise, wenn es gerade ein macOS-Update gegeben hat und ich verzweifelt versuche, sowohl das Update zu installieren als auch herauszufinden, was darin enthalten ist — kann das auf zwanzig oder mehr ansteigen. Es gibt nur wenige gemeinsame Faktoren in diesen Fragen, abgesehen von zwei, die in fast jeder wiederkehren: Beobachtung und das Protokoll.

Genau beobachten

Einige Fragen sind so allgemein und vage wie „Warum stürzt mein Mac ständig ab?“ Diese sind oft der Beginn eines langen Austauschs von Nachrichten, in denen ich versuche, Beobachtungen zu entlocken, die die Liste der Ursachen von Millionen auf weniger als ein Dutzend eingrenzen können. Sie offenbaren in der Regel, dass der Benutzer außer, dass er bemerkt hat, dass etwas Ernsthaftes schief gelaufen ist, und dies weiterhin tut, nicht beobachtet hat, was tatsächlich passiert. Ein „Absturz“ kann alles sein, von einer App, die plötzlich beendet wird, wenn man es nicht erwartet, bis hin zum unerwarteten Herunterfahren des Macs, der sich tot stellt. Zwischen diesen beiden Fällen gibt es große Unterschiede, und eine sorgfältige Beobachtung ist unerlässlich.

Zu erkennen, wann Ihr Mac eine Kernel-Panik erlitten hat, ist eine grundlegende Fähigkeit für alle. Im Gegensatz zu einem Programmabsturz, bei dem der Mac noch läuft, folgt auf eine Kernel-Panik ein erzwungener Neustart oder ein Herunterfahren. Wenn Ihr Mac wieder hochfährt, sollte er Ihnen einen Dialog präsentieren, der in einem Panik-Protokoll Details zu den Ereignissen enthält. Wenn Sie dessen Inhalt nicht sofort kopieren und in eine Textdatei einfügen (TextEdit sollte ausreichen), ist er für immer verloren und Sie können von Glück sagen, wenn Sie die Ursache herausfinden.

Panikprotokolle sind nicht so schwer zu interpretieren, und ich und andere helfen Ihnen gerne, zu verstehen, was passiert ist und was Sie dagegen tun können. Leider hilft es nicht weiter, wenn Sie den Dialog an Apple senden: Apple analysiert sie zwar, aber nicht so, dass es Ihnen eine Antwort bringt, selbst wenn Sie AppleCare haben.

Voreilige Schlüsse

Manchmal sind die Beobachtungen zwar detailliert, aber unvollständig, und die Benutzer ziehen die falschen Schlüsse. Mein bestes Beispiel dafür stammt nicht aus der Computerbranche, sondern von einem schlimmen Tauchunfall, der sich vor vielen Jahren im Hafen von Hongkong ereignete. Ein Einheimischer tauchte allein von einem kleinen Schlauchboot aus, das einen Luftkompressor enthielt — eine fast selbstmörderische Lebensweise, aber irgendwie schaffte er es, sie durchzuhalten, bis eines Tages, als er in der Tiefe war, sein Kompressor nicht mehr funktionierte und die Luftzufuhr abbrach.

Seine einzige Wahl war es, an die Oberfläche durchzubrechen und zu hoffen, dass die Taucherkrankheit ihn nicht umbringen würde. An diesem Tag hatte er Glück, denn eine vorbeifahrende Dschunke fand ihn schwimmend und immer noch atmend, wenn auch etwas angeschlagen durch die Dekompression. Einer der Besatzungsmitglieder der Dschunke hatte eine Erste-Hilfe-Ausbildung absolviert und beobachtete die Vitalzeichen des Tauchers: Er lief blau an, hatte einen starken Anfall (von Taucherkrankheit) und sein Kiefer war sehr fest zusammengepresst. Gute Beobachtungen, aber die Schlussfolgerungen waren falsch. Der Ersthelfer entschied, dass die Atemwege des Tauchers durch seine Zähne blockiert wurden, also zog er sie mit einer handlichen Zange alle heraus, einen nach dem anderen.

Neulich bemerkte ich einen Tweet von jemandem, der sehr geschickt darin ist, Mac-Software zu analysieren und rückwärts zu programmieren. Er hat gesehen, wie Time Machine auf APFS (TMA) sichert, und bemerkte lange Perioden, in denen das Time Machine-Symbol in der Seitenleiste des Finders rotierte, was mit einer erheblichen CPU-Auslastung einherging. Er ging der Sache auf den Grund und fand den Prozess, der für das Drehen des Symbols verantwortlich zu sein schien und offenbar diese CPU-Zeit beanspruchte. Er änderte ein oder zwei Einstellungsdateien, und der verschwenderische Spinner war weg.

Ich fragte ihn einfach, ob es sich dabei um Spotlight handelte, das seine Indizes von Backups aufbaut, etwas, das mehrere von uns mit TMA beobachtet haben. Er sagte mir, dass das passiert, während Backups erstellt werden (in TMA passiert das nicht), und dass dieser sich drehende Cursor erschien, als noch kein Backup erstellt wurde. Ich erkannte, dass dies wahrscheinlich mit dem Indizierungsprozess zusammenfiel, und fragte ihn, ob er überprüft hatte, was zu der Zeit im Protokoll vor sich ging. Das hatte er nicht.

Verwendung des Logs zur Diagnose

Bei all den unaufhörlichen Meldungen, die in das Unified Log geschrieben werden, enthält es wichtige Informationen über fast alles, was in, auf und mit Ihrem Mac passiert. Das Überprüfen des Protokolls ist eines der wichtigsten Dinge, die man tun muss, wenn man versucht, ein Problem auf dem Mac zu diagnostizieren. Wenn man es versäumt, das Protokoll zu studieren, werden die Beobachtungen immer unvollständig und die Schlussfolgerungen meist fehlerhaft sein. Die Ausnahme ist eine Kernel-Panik: Meistens ist die Auswirkung davon so schwerwiegend, dass die Protokolleinträge lange vor der Panik aufhören und keine nützlichen Informationen aus ihnen entnommen werden können, daher die Bedeutung des Panik-Protokolls.

Im Fall des sich drehenden Time Machine-Symbols, das mit der Indizierung zusammenfiel, hätte der Untersucher gesehen, dass die TMA-Backups nacheinander gemountet wurden, damit die Indizierung stattfinden konnte. Das beweist zwar nicht, dass die Indizierung die Ursache für dieses Verhalten war, aber es zeigt zumindest, wo man als nächstes nachschauen muss, um zu einer fundierten Schlussfolgerung zu kommen.

Nur wenige Benutzer wagen es, in das Protokoll zu schauen, und ich kann diese Angst nachvollziehen, wenn man bedenkt, welches Werkzeug in macOS zur Verfügung steht, um dies zu versuchen. Console ist keine App, die dafür gedacht ist, schnell zu überprüfen, was kürzlich im Log passiert ist, sondern um dessen Live-Stream zu betrachten. Es kann verwendet werden, um vergangene Log-Einträge zu durchsuchen, aber es ist ein ungeschicktes Werkzeug dafür: Sie müssen ein Log-Archiv erstellen, das Ihr aktuelles Log enthält, und dieses durchsuchen. Die mitgelieferte Alternative, der Befehl `log show`, ist weit weniger attraktiv, es sei denn, Sie sind ein Terminal-Assistent, und selbst dann haben Sie vielleicht Schwierigkeiten, geeignete Prädikate zum Filtern von Einträgen zusammenzustellen.

Es ist kein Geheimnis, dass ich eine ganze Reihe von Log-Browsern und -Tools habe, von denen ich zwei besonders hervorheben möchte:

- Mints, eine Sammlung von verschiedenen kleinen Tools für die Arbeit mit macOS. Dazu gehören vorkonfigurierte Log-Browser für iCloud, Datenschutz (TCC), Time Machine, DAS-Planung und Spotlight-Suche.
- Ulbow, das mein neuer Log-Browser ist und so ziemlich alles aus dem Log holen kann, was man will.

Beide sind auf ihrer Produktseite erhältlich, wo Sie ein ganzes Kompendium an einführenden und fortgeschrittenen Artikeln und anderen Links finden. Wie bei all meinen anderen Tools sind auch diese völlig kostenlos, und ich nerve Sie nicht einmal mit Spenden oder schiebe Ihnen Werbung unter.

Bevor das Unified Log in Sierra eingeführt wurde, war es für die meisten fortgeschrittenen Benutzer üblich, sowohl mit der Konsole als auch mit dem Log vertraut zu sein. Es gibt keinen Grund, warum das jetzt eine aussterbende Kunst sein sollte. Das Protokoll ist heute so zugänglich wie seit Ende 2016 nicht mehr, und die Hinweise, die es geben kann, wenn Sie versuchen, ein Problem zu diagnostizieren, sind nirgendwo anders verfügbar.

Wie Apple den Mac vor Malware schützt und was Admins darüber wissen sollten

Quelle: Jesus Vigo auf jamf.com/blog/ , Übersetzung KJM

Es wird viel über die Werkzeuge und Prozesse geschrieben, die zum Schutz von Computergeräten vor den unzähligen Bedrohungen in freier Wildbahn eingesetzt werden. Von Firewalls bis hin zu Schutzmaßnahmen für Geräte — eine schnelle Suche zeigt eine Fülle von *Best Practices* für die Absicherung von Macs durch spezifische Konfigurationen und verwaltete Einstellungen. Aber was ist mit den eingebauten Malware-Schutzfunktionen, die Apple direkt in macOS integriert hat?

Diese werden von Administratoren manchmal nur oberflächlich betrachtet, wenn nicht sogar ganz übersehen, um anderen, wichtigeren Begriffen wie *„defense-in-depth“* und „filling the gap“ den Vorzug zu geben. Letzteres hilft dabei, die Ressourcen so auszurichten, dass die Strategie des Ersteren gestärkt wird. Leider sind die unten genannten Tools recht harmlos und nicht die aufregendsten. Das liegt zum Teil daran, dass sie dazu gedacht sind, verdeckt im Hintergrund zu arbeiten, um den Mac ohne großes Aufsehen zu sichern. Oder anders ausgedrückt: „Es funktioniert einfach“, wie es der verstorbene Steve Jobs so treffend formulierte.

Dieser Blog befasst sich mit den folgenden nativen Sicherheitstools, was sie tun und wie sie zusammenarbeiten, um den Mac zu schützen: Gatekeeper, XProtect und YARA.

Ein wachsamer Wächter

Apples **Gatekeeper**-Werkzeug, wie der mythologische Heimdall aus der nordischen Sage, der über Asgard wacht und es vor Eindringlingen schützt, indem er ihnen keinen Zutritt zu seinen heiligen Stätten gewährt, verhindert, dass Softwareprogramme ausgeführt werden, bevor sie durch die Erzwingung der Code-Signierung verifiziert wurden. Durch die Erzwingung dieses Beglaubigungsprozesses für jede App, bevor sie ausgeführt wird, wird die Möglichkeit der Ausführung von Malware eingeschränkt, ebenso wie die Möglichkeit, dass die Integrität der Software durch einen böswilligen Akteur beeinträchtigt wird.

Standardmäßig ist macOS so konfiguriert, dass heruntergeladene Apps mit einem Quarantäne-Flag gekennzeichnet werden. Dies signalisiert Gatekeeper, dass es prüfen soll, ob die blockierte Anwendung von einem Entwickler mit einem gültigen Zertifikat signiert wurde und ob die signierten Dateien mit der Signatur übereinstimmen. Wenn eine dieser beiden Überprüfungen fehlschlägt, darf die App nicht ausgeführt werden. Dieser Prozess wird in modernen Versionen von macOS durch die Pfad-Randomisierung verstärkt, die einen zweigleisigen Schutzansatz bietet:

1. Zertifizierung der Integrität aller gebündelten Dateien, um Angreifer daran zu hindern, Apps (oder gebündelte Dateien) zu infizieren und weiterzuverbreiten.
2. Nicht verifizierte Apps werden von versteckten, randomisierten Pfaden im Hintergrund ausgeführt und können nicht auf externe Dateien zugreifen oder mit ihnen interagieren.

Der geschickte Detektiv

Ob Sie es glauben oder nicht, die Mac-Hardware hat einen eigenen Superhelden zur Verbrechensbekämpfung (ok, Malware-Bekämpfung) namens **XProtect** eingebaut. Wie der sagenumwobene Kreuzritter Batman, der einen Bösewicht nach dem anderen aufspürt, um Gotham City zu verteidigen, bietet XProtect eine signaturbasierte Erkennung von Malware, um bösartige Inhalte zu identifizieren und deren Ausführung zu blockieren, damit der Mac optimal läuft und gleichzeitig vor einer nicht enden wollenden Vielzahl von Bedrohungen geschützt ist.

Auf modernen Versionen von macOS erhält XProtect Updates für sein signaturbasiertes Erkennungssystem und nutzt diese Intelligenz, um bekannte Malware automatisch zu erkennen und zu blockieren, wenn die folgenden Bedingungen eintreten:

- Apps werden zum ersten Mal gestartet
- Apps werden aktualisiert oder anderweitig modifiziert
- Neue Signaturen werden dem System hinzugefügt

Nach der Erkennung werden infizierte Apps sofort blockiert, und die Benutzer erhalten eine Benachrichtigung, um Maßnahmen zu ergreifen, z. B. das Verschieben in den Papierkorb, um die Bedrohung zu entfernen.

Allwissendes Orakel

O | ra | kel *(Substantiv)*
„eine Person, die weise oder autoritative Entscheidungen oder Meinungen abgibt“

YARA ist der Name eines Tools, das von Malware-Forschern verwendet wird, um bei der Kategorisierung von entdeckter Malware zu helfen. Die Sprache ermöglicht die Klassifizierung der Ergebnisse in ein organisiertes Muster oder einen Ausdruck, dessen Beschreibung eine Regel bildet. Der resultierende Code oder die YARA-Regeln werden dann von zahlreichen Sicherheitstools weltweit verwendet, um die Signatur zu erstellen, die zur Identifizierung bekannter Malware-Bedrohungen verwendet wird. Ähnlich wie das Orakel in der Matrix, das Neo bei der Verteidigung — und später bei der Auslöschung — gegen den lästigen Programmiercode Agent Smith hilft, ergänzen die YARA-Regeln Apples Sicherheits-Frameworks, indem sie einen Einblick in den zugrunde liegenden Code von Malware-Bedrohungen geben. Wie ein allsehendes Auge vergleicht es die von Sicherheitsanwendungen durchgeführten Scans mit den eindeutigen Signaturen, die durch die YARA-Regeln ermöglicht werden und die in der Bedrohungsdatenbank enthalten sind, auf Übereinstimmungen mit bekannten Malware-Fingerabdrücken.

Da es sich um eine Open-Source-Plattform handelt, ist die YARA-Plattform in einer Reihe von Sicherheitsanwendungen und Appliances verfügbar und wird durch die Erkenntnisse unzähliger Sicherheitsforscher ermöglicht, die aktiv Malware jagen, identifizieren und verfolgen. Diese Regeln tragen zur Fülle der Erkennungen in Programmen wie XProtect bei, die den Mac heute und morgen vor den allerneuesten — und schlimmsten — Malware-Bedrohungen (einschließlich ihrer Varianten) schützen!

Nutzen Sie die Macht

Jedes der oben aufgelisteten Werkzeuge arbeitet, um ein bestimmtes Bedürfnis zu befriedigen, allein sind sie stark und erfüllen ihre Aufgabe auf bewundernswerte Weise. Und doch, erst, wenn sie kombiniert werden, sind sie wie ein Jedi-Meister, der die Macht ausübt! Der stärkste, mächtigste Verbündete der Jedi und einer, dessen Stärke noch viel größer wird, wenn sich immer mehr mit ihm zusammentun.

Apples Dreifaltigkeit beim Schutz vor Bedrohungen, die mit Gatekeeper beginnt, um die Code-Signierung zu verifizieren, und an XProtect weitergibt, um laufende Bedrohungen durch Erkennung und Beglaubigung zu beseitigen, wird durch ständig aktualisierte YARA-Regeln verstärkt, die die neuesten Hinweise auf Bedrohungen liefern. Zyklisch fließt YARA direkt in beides ein, und zwar in Verbindung mit dem Malware Removal Tool (MRT) — der Engine in macOS, die regelmäßig nach Malware scannt und Infektionen entfernt — um Bedrohungen automatisch auf Basis von Erkennungen zu beseitigen.

Aber kein Betriebssystem ist perfekt...

Und selbst Yoda ist nicht unfehlbar. An dieser Stelle kommt eine Lösung wie **Jamf** ins Spiel. Jamf überbrückt die Lücke zwischen dem, was Apple bietet, und dem, was ein Unternehmen benötigt — ein Unternehmen, das immer mehr Macs einsetzt und optimierte Arbeitsabläufe benötigt, um die Benutzer zu sichern und zu schützen, egal wo sie sich befinden.