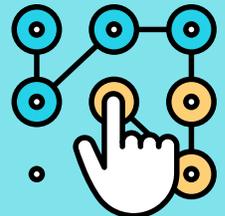
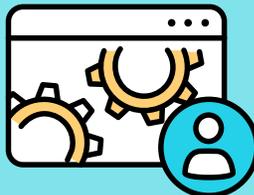


Mac Endgeräte- sicherheit

für
Beginner

Sicherheit direkt aus der Box – das ist nur der Anfang



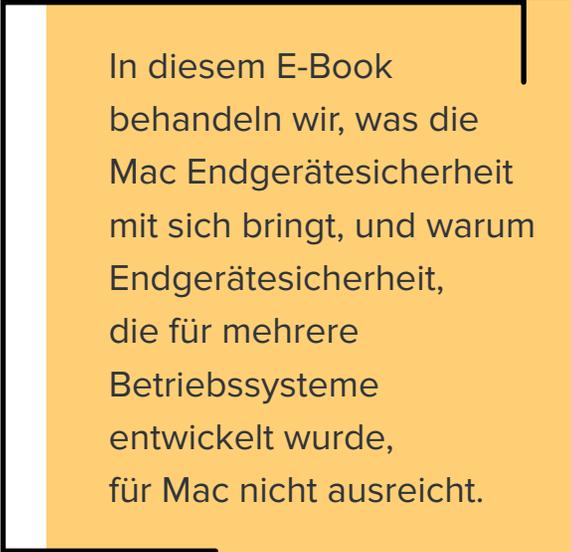


Mac Geräte sind zweifelsohne die sichersten Geräte auf dem Markt. Das war schon immer so, und gilt auch heute noch. Wenn Organisationen ihren Gerätebestand zusammenstellen, sind Sicherheitslösungen zum Schutz von Daten, Geräten und Anwendern von entscheidender Bedeutung.

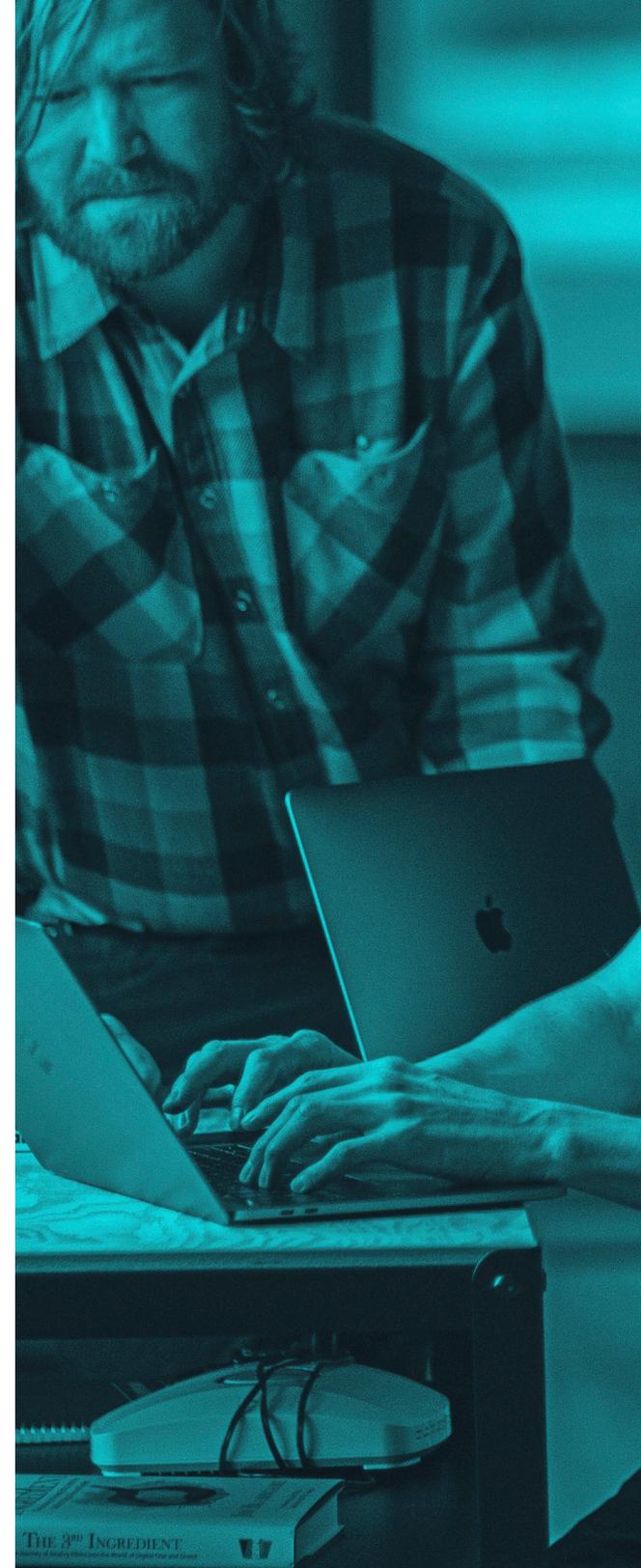
Selbstgefälligkeit kann zu schädlichen oder hochpreisigen Sicherheitsverletzungen führen. Mit einer Endgerätesicherheitslösung für Mac können IT- und Sicherheitsteams nicht nur vor bekannten Bedrohungen schützen, sondern sich auch laufend anpassen und zukünftige Sicherheitsanforderungen Ihrer Organisation voraussehen.



Ganz gleich, ob Sie ein großes Unternehmen sind, das ausschließlich mit Apple Geräten arbeitet, oder eine kleine Firma mit ein paar Mac Geräten – Jamf bietet Endgerätesicherheit, die über die native Funktionalität von Apple hinausgeht, um Ihre macOS Geräte, Daten und Endbenutzer zu schützen.



In diesem E-Book behandeln wir, was die Mac Endgerätesicherheit mit sich bringt, und warum Endgerätesicherheit, die für mehrere Betriebssysteme entwickelt wurde, für Mac nicht ausreicht.

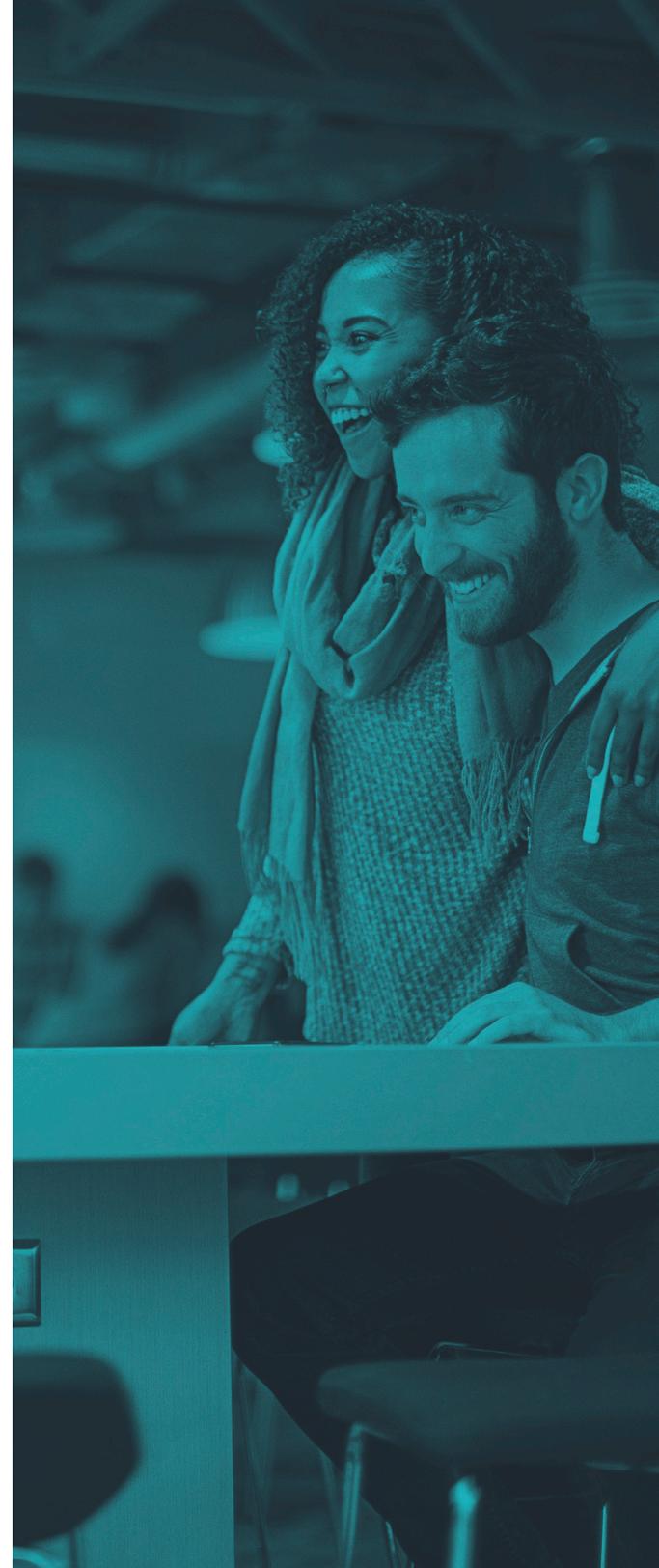


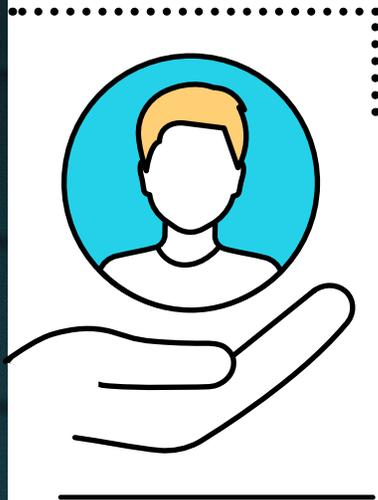
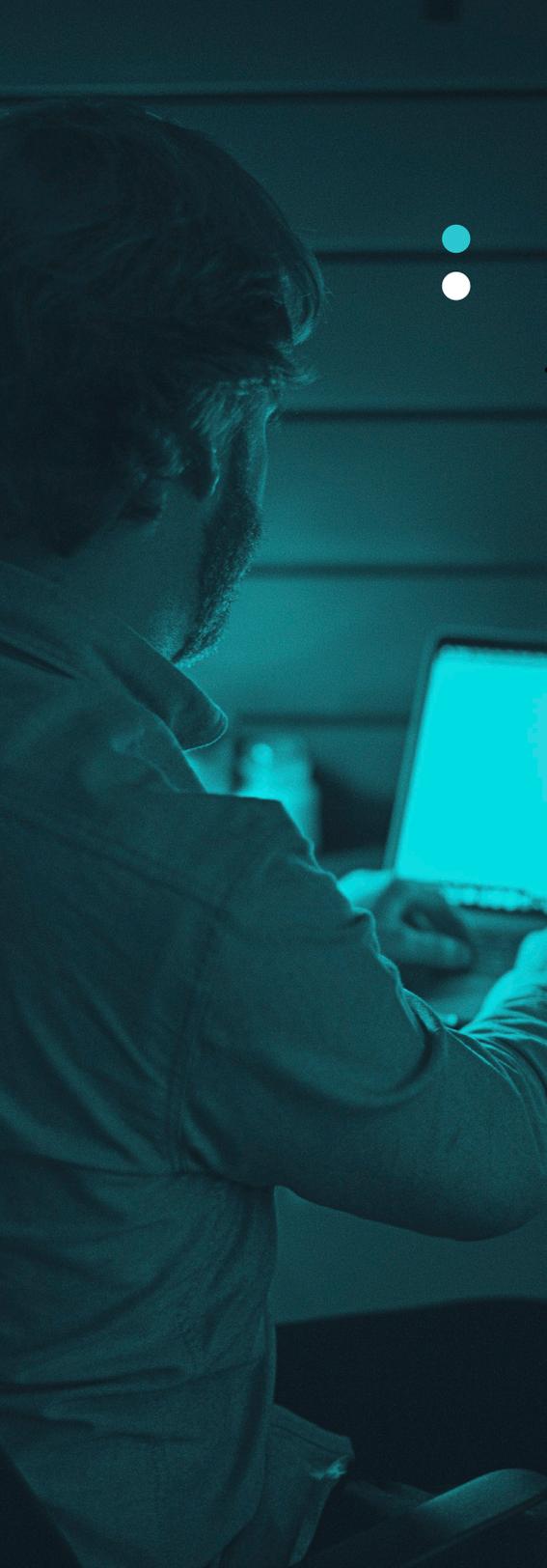
Endgerätesicherheit auf Macs:

Erweitern Sie die nativen Sicherheitsvorteile von Apple und schützen Sie sich vor dem Unbekannten. ● ●

Immer mehr Großunternehmen, Kleinunternehmen, Schulen und Gesundheitsinstitutionen verwenden Mac. Die rechtmäßige und korrekte Nutzung von Daten und Geräten durch autorisierte Benutzer ist dabei von zunehmender Bedeutung. [Hier kommt die Mac Endgerätesicherheit ins Spiel.](#)

Dazu arbeiten viele bewegliche Teile
– **Identitätsverwaltung, Patching,
Antivirus (AV), Konfiguration,
Endgeräteerkennung und -reaktion**
– zusammen, um die Anforderungen
Ihres IT- und Sicherheitsteams zu
unterstützen.





IDENTITÄTS- VERWALTUNG

Sicherheitsmaßnahmen, die durch die Identitätsverwaltung umgesetzt werden, beeinflussen sowohl Endbenutzer als auch IT im gesamten Lebenszyklus von Mitarbeitergeräten, unabhängig davon, ob vor Ort oder aus der Ferne gearbeitet wird. VPNs, SaaS-Anwendungen und Zugriff für Mitarbeiter auf Unternehmensressourcen sind Möglichkeiten zur Verstärkung Ihrer Endgerätesicherheit.

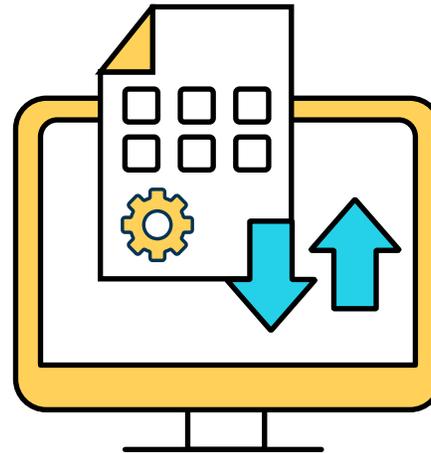
Bei einer zunehmend mobilen Belegschaft und mit Mitarbeitern, die von verschiedenen Standorten aus auf verschiedenen Geräten arbeiten, müssen Organisationen diese Geräte und deren Unternehmensinformationen verwalten und sichern können, ohne dass sie an ein Active Directory vor Ort gebunden sind. Jamf Connect unterstützt Anwender ab dem Moment, an dem sie ihren Mac auspacken und einschalten, bis hin zum Zugriff auf Unternehmensanwendungen, Ressourcen und Daten mit einem einzigen Satz von Anmeldeinformationen für die Cloudidentität. Ein Nutzer kann seinen Mac auspacken, einschalten und auf all seine Unternehmensanwendungen zugreifen, nachdem er sich mit einem einzigen Satz von Anmeldeinformationen für die Cloudidentität angemeldet hat.

Mit Jamf Connect können Organisationen die Identität und den Zugriff mit minimalen Auswirkungen auf das Endbenutzererlebnis überwachen und sich auf die beständige Priorisierung von Geräte- und Datensicherheit verlassen.

PATCHING



Sicherheits-Patching sollte regelmäßig und einfach durchgeführt werden, um jegliche bekannte Schwachstelle auszubessern. Jamf spart der IT-Abteilung wichtige Zeit durch Optimierung der folgenden erforderlichen Prozesse: Wartung oder Aktualisierung von Anwendungen auf macOS, Bereitstellung zusätzlicher Transparenz für Compliance und Kompatibilität sowie die Aufrechterhaltung einer nahtlosen Endbenutzererfahrung. Dies beinhaltet auch die Ausführung der aktuellsten Version von macOS, sobald diese veröffentlicht wird, um Sicherheitslücken aufgrund von verspäteten Aktualisierungen zu vermeiden.



Sicherheits- und Management-Tools sollten nicht der Grund dafür sein, OS-Updates oder Upgrades zu verschieben. Jamf unterstützt Sie ohne Verzögerung auf neuen macOS Versionen ab ihrem Erscheinungstag, damit Ihnen nichts mehr im Weg steht. Sie bestimmen, wann Ihre Geräte aktualisiert werden.



ANTIVIRUS (AV)

AV scheint eine neue Notwendigkeit für Mac zu sein, aber es gibt eben auch eine neue Realität. Mac und macOS wird immer mehr Aufmerksamkeit geschenkt, da Unternehmen vermehrt darauf zählen.

AV ist eine wichtige Anforderung für die meisten Geräte in einer Organisation, um eine grundlegende Sicherheit zu bieten. Apple bietet einen grundlegenden Virenschutz in macOS mit XProtect, Gatekeeper und MRT. Diese Tools werden jedoch nur sporadisch aktualisiert, und Organisationen können nicht genau verfolgen, was sie tun. Jamf Protect bietet hochentwickelte AV-Funktionen, um Mac Schadsoftware zu verhindern und unter Quarantäne zu stellen, und übertrifft damit die Möglichkeiten, die Windows-orientierte Lösungen auf macOS bereitstellen.

Organisationen sollten nicht warten, bis Malware, Adware oder andere unerwünschte Softwareprobleme auftreten. Sie müssen ein AV-Programm implementieren, das Mac spezifische Angriffe effektiv identifiziert und behebt, ohne wertvolle Ressourcen mit der Suche nach Bedrohungen für Windows auf einem Mac zu verschwenden. Effektive, effiziente und umfassende Mac AV-Funktionen sind für die Sicherheit und die Benutzerfreundlichkeit von Geräten unerlässlich. Eine AV-Lösung darf jedoch die Produktivität Ihrer Endbenutzer nicht beeinträchtigen, denn das führt nur zu Frust für alle Beteiligten. Jamf Protect schützt macOS vor Malware, ohne dabei das gewohnte Benutzererlebnis, das Benutzer von Mac erwarten, zu verändern.



Mac AV ist nicht mehr nur ein netter Bonus, sondern ein Muss. Allerdings benötigen Sie nicht einfach nur AV, sondern eine speziell für Mac entwickelte AV-Lösung – ohne die Einschränkungen einer AV-Lösung für die systemübergreifende Nutzung.

KONFIGURATION

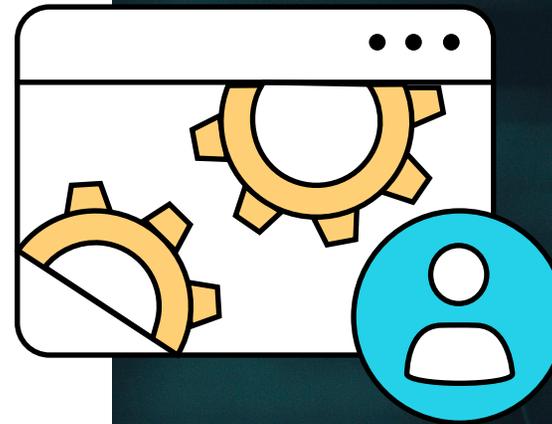
Die Sicherheit, die bei Mac direkt aus der Box kommt, ist großartig, sie ist die beste auf dem Markt. Aber wir können die Sicherheit Ihrer Geräte und Daten ganz einfach noch weiter verbessern. Wenn bessere Sicherheit also einfach ist, worauf warten Sie dann noch?

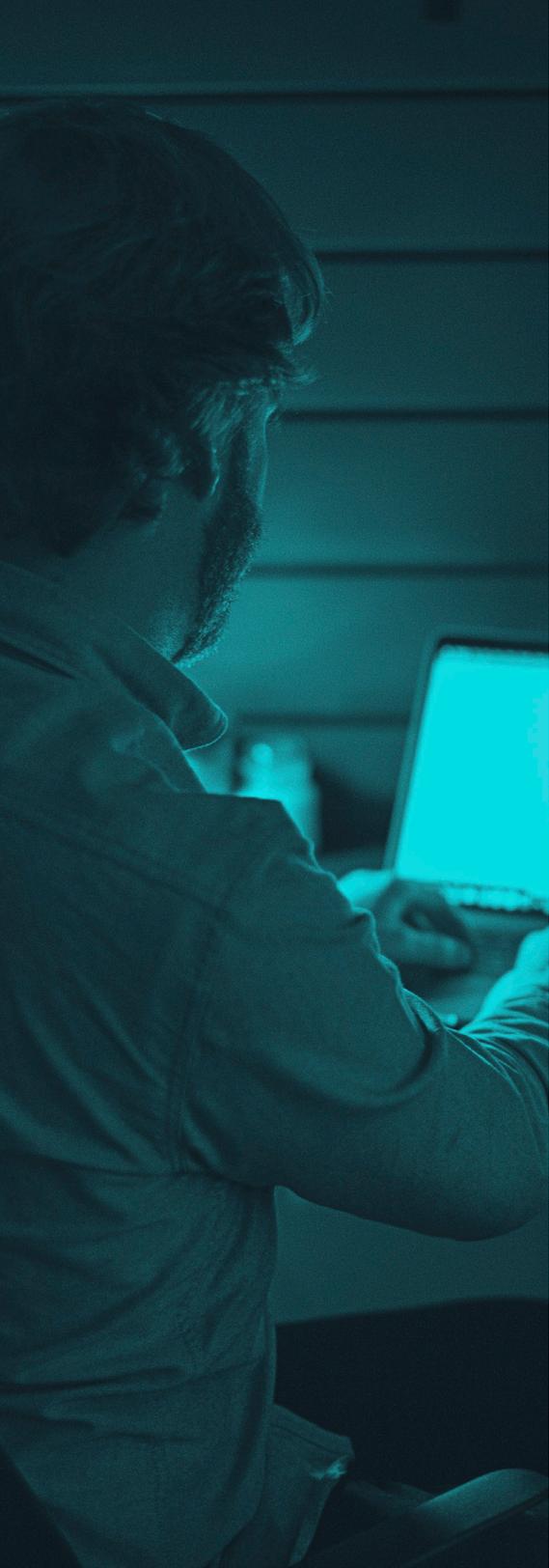
In der Sicherheits-Community stehen umfangreiches Wissen und viele Skripts zur Verfügung.

Jamf macht die Umsetzung, Ausführung und Überwachung für alle Nutzer, die diese Standards modifizieren möchten, zum Kinderspiel. Jamf räumt die Hindernisse aus dem Weg, um eine grundlegende geräteübergreifende Sicherheit zu etablieren.

FileVault, Firewall- und Passwortanforderungen, Bildschirmschoner- und Sperranforderungen spielen alle eine Rolle bei der Positionierung Ihrer Sicherheitsanforderungen und Ihrer Benchmarks.

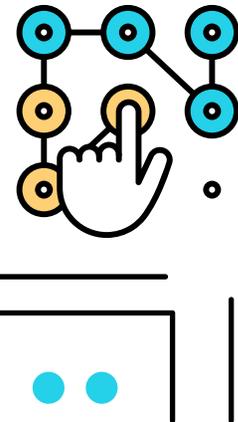
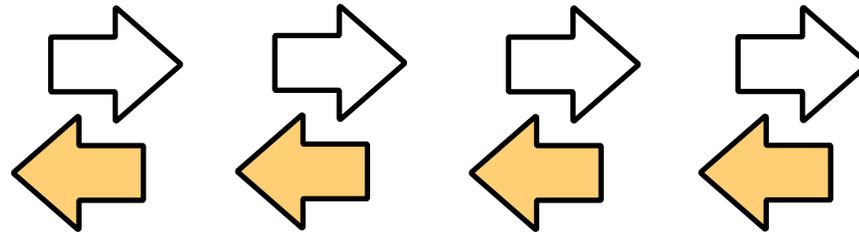
Doch wo fängt man an? Das Center for Information Security bietet Branchen-Benchmarks und Jamf ist CIS-zertifiziert. Mit Jamf sind Sie also bereits auf dem richtigen Weg, und unsere Ressourcen werden Ihnen noch weiter helfen. In unserer [macOS Sicherheits-Checklist](#) erfahren Sie mehr über die CIS-Sicherheits-Benchmarks und Jamf.





ERKENNUNG UND REAKTION SPEZIELL FÜR MAC

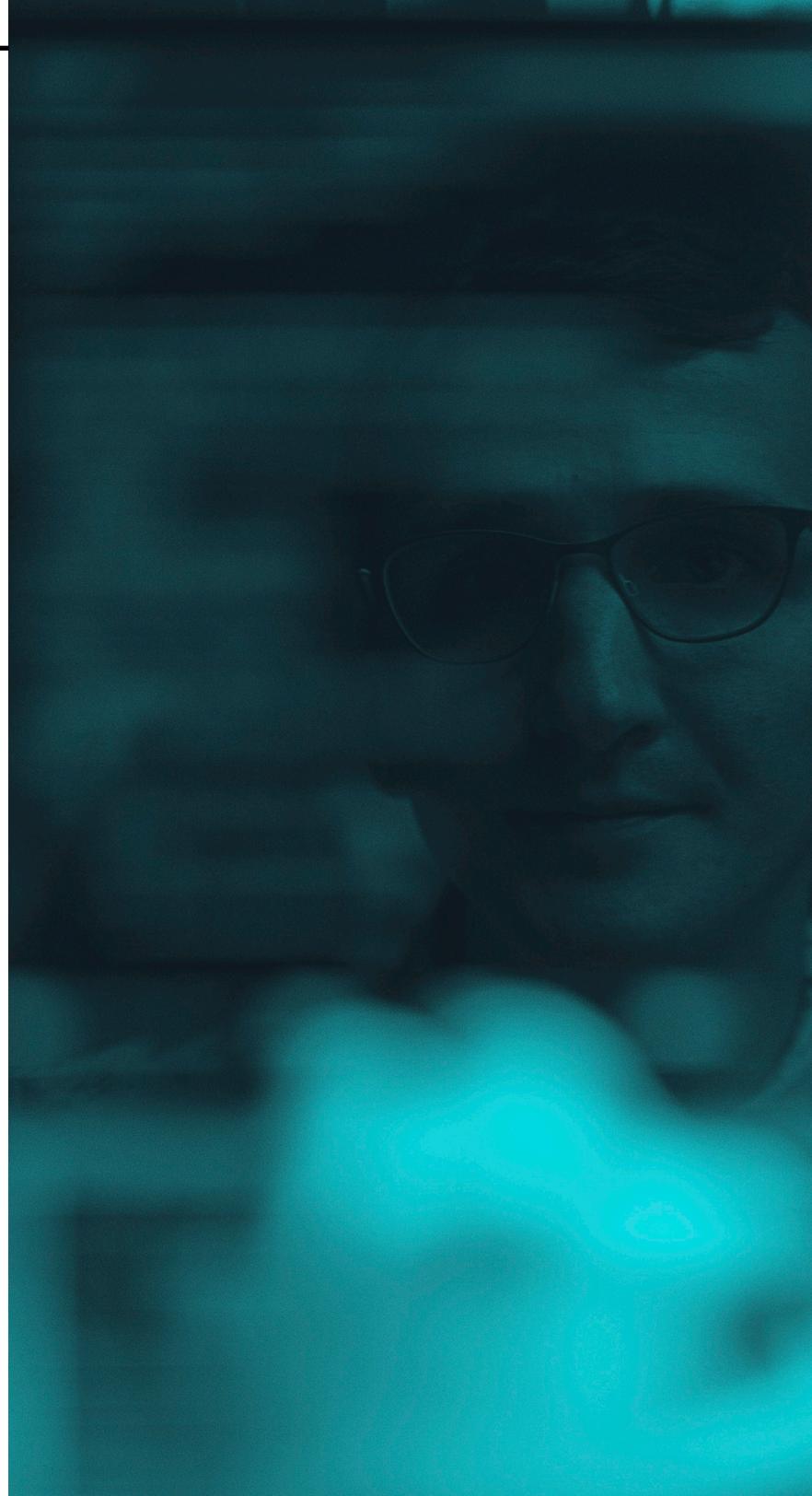
Traditionelle EDR-Tools (Endpoint Detection and Response) gibt es für den Mac seit einiger Zeit, aber die meisten sind nicht dafür konzipiert, spezifisch auf den Mac ausgerichtete Angriffe effektiv zu entdecken. Vielmehr versuchen sie, Mac Geräten Windows Modelle aufzuzwingen. Da Jamf Protect sich ausschließlich auf Mac und macOS konzentriert, minimiert Jamf Falschmeldung und maximiert die Erkennungsraten auf Mac.



Wenn Sie Jamf Protect mit Jamf Pro kombinieren, erhalten Sie Fähigkeiten für Gegenmaßnahmen, die nur geringfügig intrusiv sind und die durchschnittlichen EDR-Fähigkeiten übertreffen. Mit Jamf können IT- und Sicherheitsteams einen nahtlosen Vorfallsreaktionsplan erstellen, der Ihren Teams eine enge Zusammenarbeit ermöglicht.

APPLICATION LIFECYCLE MANAGER

Durch die Integration von Jamf Pro in Apple Business Manager können Sie Lizenzen der Anwendungen und Software Ihrer Organisation zuweisen und verwalten. Darüber hinaus hilft Jamf Pro bei Patching und Softwareaktualisierungen. So ist auch sichergestellt, dass Sie etwaige anfällige Softwareversionen aktualisieren und verwalten sowie die Transparenz des Status Ihrer gesamten Mac Geräte aufrechterhalten können.



Jamf bietet End- gerätesicherheit für Mac

Mac Endgerätesicherheit mit Jamf Protect unterstützt die Endgeräte-Compliance, kümmert sich um Antivirus-Anforderungen durch Vermeiden von macOS Malware, steuert und sichert Mac Anwendungen innerhalb der Organisation und erkennt und behebt Mac spezifische Bedrohungen mit minimalen Auswirkungen auf die Endbenutzererfahrung.

In Verbindung mit Jamf Pro nutzt Jamf extensive Möglichkeiten für die Automatisierung, Untersuchung und Behebung zur Entschärfung von großen und kleinen Risiken für die Endgerätesicherheit.

Fordern Sie eine kostenlose Testversion an oder kontaktieren Sie Ihren bevorzugten Apple Händler, wenn Sie bereit sind, Ihre Sicherheit mit Mac Endgerätesicherheit zu verstärken.

Erfahren Sie mehr über Jamfs **Endgerätesicherheits-Funktionen** für Mac.