Endpunktsicherheit für modernes Arbeiten

Endgerätesicherheit wird allgemein als Schutz Ihrer Geräteflotte vor Cyberangriffen verstanden.

Obwohl dies ein wesentlicher Bestandteil **ist, gehört zur erfolgreichen Implementierung und Gewährleistung der Endpunktsicherheit in Unternehmen noch mehr.** Dabei handelt es sich nämlich um eine Reihe von Funktionen, die Ihre Geräte (sowie Benutzer*innen) vor einer sich ständig weiterentwickelnden Bedrohungslage schützen. In dem Sinne müssen auch Sie handeln und die richtigen Tools für Ihre Geräte auswählen.

Und noch vieles mehr.

Wenn Sie neu im Apple Ökosystem sind oder sich zum ersten Mal mit der Endpunktsicherheit in der modernen Bedrohungslandschaft für Macs oder mobile Geräte befassen, müssen Sie sich keine Sorgen machen, denn Jamf zeigt Ihnen, wie moderne Verwaltung und Endpunktsicherheit aussehen und was dies für Ihre Remote oder hybride Umgebung und Ihre Endbenutzer*innen bedeutet, und zwar im Hinblick auf alte Lösungen und altbewährte Konzepte, die für diese modernen Plattformen einfach nicht geeignet sind.

Mit diesem White Paper können Sie:

- Unternehmensrisiken verstehen
- Endgerätesicherheit modernisieren
- Basislinien etablieren
- Vor moderner Malware schützen
- Native Apple Sicherheit erweitern
- Mehrschichtigen Ansatz zum Endgeräteschutz einsetzen
- Schwächen von All-in-One-Lösungen erkennen
- Lösungsübergreifende Integrationen verwenden
- Sicherheit und Leisung vereinbaren
- Nutzer*innen helfen, sich selbst zu helfen

Was kann schiefgehen?

Für viele Unternehmen auf der ganzen Welt kann die Verwaltung von Apple Geräten und die Gewährleistung der Endgerätesicherheit bei gleichzeitiger Gewährleistung der Benutzerfreundlichkeit eine schwierige Aufgabe sein. Wenn man bedenkt, dass von tausend installierten Geräten zweihundert über eine unsichere Konfiguration verfügen, kann dies Anlass zu großer Sorge geben.

Wenn spätestens an dieser Stelle aber keine Alarmglocken läuten, deutet dies auf ein größeres Problem hin. Außerdem wird ein umfassenderes Bild der Bedrohungen gezeichnet, die auf Unternehmen abzielen, wie z. B. Datendiebstahl — entweder durch Datenexfiltration über USB-Laufwerke oder über das Netzwerk, durch den Verlust von Anmeldeinformationen, indem man Opfer von Phishing-Angriffen wird, oder durch Schwachstellen in Anwendungen und im Betriebssystem, die ausgenutzt werden, weil die Patches nicht auf dem neuesten Stand sind.

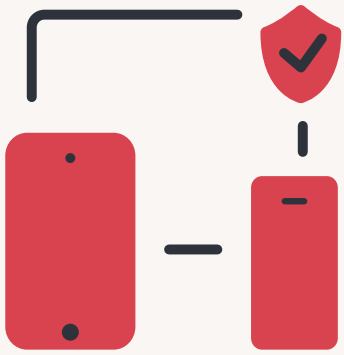
Damit ist die Risikominimierung bei gleichzeitiger ordnungsgemäßer Verwaltung der Geräte gleichbedeutend mit Yin und Yang. Es entsteht ein Gleichgewicht zwischen zwei scheinbar unverbundenen Aspekten, die zusammenkommen, um die Einhaltung der Vorschriften zu gewährleisten, indem sie harmonisch zusammenarbeiten — zum Nutzen des Ganzen.

Darüber hinaus verhindert die Abstimmung von Sicherheit und Verwaltung mit der Compliance, wie z. B. die Durchsetzung von Richtlinien zur akzeptablen Nutzung (AUP), andere Formen von Schäden, die zwar nicht rein technischer Natur sind, aber dennoch potenziell verheerend sein können. Beispiele hierfür sind die Anfälligkeit von Unternehmen für Haftungsfragen aufgrund von Verstößen gegen die für Ihre Branche geltenden Vorschriften oder die Schädigung der Marke und/oder des Rufs Ihres Unternehmens, z. B. durch eine öffentlich bekannt gewordene Datenschutzverletzung.

39 % der Unternehmen gestatteten den Betrieb von Geräten mit bekannten Sicherheitslücken im Betriebssystem **in einer Produktionsumgebung ohne Einschränkung der Berechtigungen oder des Datenzugriffs, gegenüber 28 % im Jahr 2020.**

— Jamf Security 360: jährlicher Trendberich

Gute Gerätehygiene aufrechterhalten



Wo können wir also ansetzen, um Geräte auf klare, übersichtliche und organisierte Weise wirksam zu schützen? Alles beginnt mit einem Rahmenwerk. Hierbei setzt man auf einen durch drei zentrale Säulen aufgebauten, mehrschichtigen Schutz im Rahmen einer Defense-in-Depth-Strategie, der Sie vor Fallstricken wie diesen bewahrt:

Mangelnder Einblick in den Zustand der Endgeräte: Nicht verwaltete Geräte stellen eine erhebliche Bedrohung für die Unternehmensressourcen und die Sicherheit von Unternehmensdaten und Endbenutzer*innen dar, da Geräte mit fragwürdigem oder unbekanntem Gesundheitszustand auf Ressourcen zugreifen können und so möglicherweise Daten und Informationen preisgeben.

Bedrohungen und Schwachstellen unkontrolliert: Bekannte und unbekannte Malware-Bedrohungen sowie netzbasierte Angriffe beeinträchtigen die Datensicherheit und -integrität. Ohne die Möglichkeit, regelmäßig mit den Endgeräten zu kommunizieren, kann es vorkommen, dass die Patches für die Geräte nicht mehr aktuell sind und/oder nicht mehr den Vorschriften entsprechen, ohne dass die IT- oder Sicherheitsteams dies bemerken, bevor es zu spät ist.

Von Benutzer*innen verursachte Risiken und Sicherheitsbedenken: Die Sicherheit Ihrer Geräte und/oder die Privatsphäre Ihrer Nutzer wird oft durch riskantes Verhalten gefährdet, z. B. durch das Herunterladen verdächtiger Apps oder die Verletzung von Benutzerrichtlinien, die nicht durchgesetzt werden.

Jede der drei nachstehenden Säulen dient als Dach, das abdeckt, wie Sicherheitskontrollen, Best Practices und Richtlinien, die für die Endpunktsicherheit wichtig sind, verwendet werden sollten, um Ihre Apple Flotte - sowohl macOS als auch iOS basierte Geräte — vor modernen Bedrohungen zu schützen, während gleichzeitig Daten geschützt und die Privatsphäre der Benutzer*innen gewahrt wird.

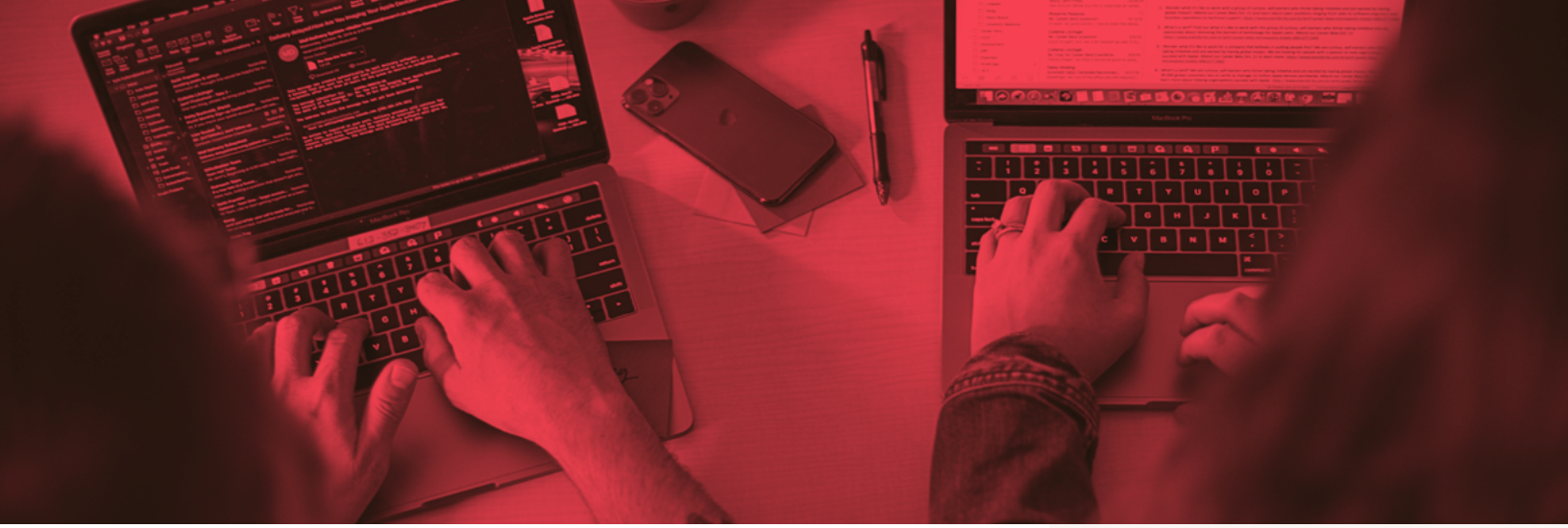
Darüber hinaus bilden diese Säulen die andere Hälfte des Ganzen: die Verwaltung und die Art und Weise, wie die Integration von Sicherheit und Verwaltung einen umfassenden Arbeitsablauf bildet, um die Endgeräte auf dem neuesten Stand zu halten, ständig auf Konformität zu überwachen und bereit zu sein, erkannte Bedrohungen in einem sich wiederholenden Zyklus zu entschärfen.

1 Sichere Basislinien einrichten

Die Standardisierung der Endgerätesicherheit hilft Unternehmen, die besonderen Anforderungen ihrer Geräteflotte zu erkennen. Dadurch wird das Management direkt informiert, indem der Gerätehygiene Vorrang eingeräumt wird, während die Kodifizierung bewährter Sicherheitspraktiken in Unternehmensrichtlinien dazu beiträgt, die Anforderungen mit den Härtungsstandards abzustimmen, die das Risiko schnell und auf leicht verständliche Weise beseitigen.

Durch die Prüfung von Anwendungen vor der Bereitstellung und die Aktualisierung des Betriebssystems und der Anwendungen wird nicht nur sichergestellt, dass die Anwendungen und unterstützten Betriebssysteme die besten Sicherheitsverfahren einhalten, sondern auch, dass sowohl die IT — als auch die Sicherheitsteams Software unterstützen, die den Anforderungen Ihres Unternehmens entspricht — und nicht dagegen verstößt -, wodurch Schwachstellen auf ein Minimum reduziert und der Support des Unternehmens standardisiert wird.

Ein wichtiger Aspekt dabei ist die Verwaltung von Benutzerrechten, wie z. B. Berechtigungen. Durch die Einschränkung der Zugriffsrechte nach dem Prinzip der geringsten Privilegien und die Verwaltung der Geräteeinstellungen sind die Benutzer*innen nur auf den Zugriff auf Daten und die Ausführung von Aufgaben beschränkt, die für ihre Produktivität erforderlich sind — alle anderen Rechte sind gesichert, um Missbrauch zu verhindern.

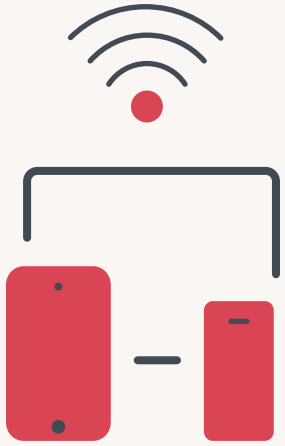


2 Verteidigen Sie das Gerät vor modernen Bedrohungen

Die Integration der Endgerätesicherheit in die Verwaltung — und nicht die Isolierung der beiden Bereiche — ist eine Grundvoraussetzung dafür, dass sowohl Apple Computer und mobile Geräte als auch Benutzer*innen und Daten sicher vor modernen geräte- und netzwerkbasierten Bedrohungen geschützt sind. Bedrohungsdaten, die von der Verwaltung und der Sicherheitsbehörde gemeinsam genutzt werden — wobei beide auf das Endpoint Security Framework (ESF) von Apple ausgerichtet sind — zentralisieren die Verwaltungsrichtlinien und lösen automatisch Arbeitsabläufe zur Behebung von Problemen aus, während gleichzeitig die IT-Abteilung und die Sicherheitsteams benachrichtigt werden.

Durch die konsequente Überwachung auf CVE-Bedrohungen kategorisieren und verhindern signaturbasierte Analysen, dass bekannte Bedrohungen Ihre Endpunkte beeinträchtigen. In ähnlicher Weise identifizieren und entschärfen Verhaltensanalysen und fortschrittliche ML unbekannte Bedrohungen oder Zero-Day-Angriffe, bevor sie eine Chance haben Durch die ständige Überwachung des Gerätezustands und die Erstellung von Berichten halten Sicherheitslösungen IT- und Sicherheitsteams mit Hilfe detaillierter Berichte auf dem Laufenden. Darüber hinaus schalten Warnmeldungen in Echtzeit Support-Teams ein, wenn Endgeräte eine Triage oder Behebung benötigen.

Und schließlich liefert die Zentralisierung des Austauschs von Bedrohungsdaten zwischen Management und Sicherheitsbehörden den Unternehmen Compliance-relevante Daten. Dieser Informationsstand ermöglicht es den Support-Teams, Risiken zu minimieren, wenn sie erkannt werden, und die Konformität der Endgeräte wiederherzustellen, bevor Bedrohungen zu größeren Sicherheitsproblemen führen, wie z. B. seitliche Verschiebungen oder Datendiebstahl, die den Ruf des Unternehmens schädigen oder zu rechtlicher Haftung führen können.



7% der kompromittierten Geräte griffen auf Cloud-Speicherdienste (wie OneDrive, Google Drive und DropBox) und 25% auf E-Mail-Dienste zu

Quelle: Jamf's Sicherheit 360: Jährlicher Trendbericht

3 Management von nutzerinduzierten Risiken

Benutzer*innen stellen die mit Abstand größte Bedrohung für die Endpunktsicherheit dar. Unabhängig davon, ob die Aktionen böswillig oder unbeabsichtigt durchgeführt werden, führt das Ergebnis oft zu derselben Schlussfolgerung: Riskante Verhaltensweisen stellen eine echte Bedrohung für die Sicherheit Ihrer Apple Flotte und kritischer oder sensibler Unternehmensdaten dar.

Die Abstimmung von Sicherheit und Management befasst sich mit Benutzerverhalten, das potenziell ein Risiko darstellen könnte, indem es sich auf Verhaltensanalysen stützt, um festzustellen, ob risikoreiches Verhalten, wie bösartige Downloads oder der Zugriff auf Websites, die für Phishing-Angriffe verwendet werden, unabhängig vom Modell des Gerätebesitzes vorliegt.

Daher müssen Sicherheitsprozesse in der Lage sein, Endpunkte zu schützen, während das Management die Einhaltung von Unternehmensrichtlinien, wie z. B. einer Acceptable Use Policy, durchsetzt.

Apropos Schutz der Privatsphäre: Moderne Computerumgebungen unterstützen oft eine Mischung aus verschiedenen Eigentumsmodellen, einschließlich BYOD. Verwaltung und Sicherheit müssen flexibel sein, um nicht zu weit zu gehen, und sich stattdessen darauf konzentrieren, die Privatsphäre der Endbenutzer*innen zu schützen, ohne die Sicherheit zu beeinträchtigen — und umgekehrt.

1 von 10

Menschen klicken auf Phishing-Links, während sie ihr Mobilgerät benutzen

Quelle: Wandera,
ein Jamf Unternehmen

Die Zahl der Mobilfunknutzer*innen, die auf Phishing-Angriffe hereinfallen, ist im Vergleich zum Vorjahr um 160 % gestiegen

Quelle: Wandera,
ein Jamf Unternehmen

Warum werden zusätzlich zu den nativen Apple Funktionen Sicherheitstools benötigt?

Apple gilt als Entwickler einiger der sichersten, sofort einsatzbereiten Geräte. Der Mac stützt sich auf seine Unix-Grundlagen und kombiniert sie mit Apples historischem Engagement für Sicherheit und Datenschutz. Er ist vollgepackt mit nativer Schutzsoftware und Technologien, die seine Anfälligkeit für Sicherheitsbedrohungen einschränken:

XProtect: Antivirus-Software mit signaturbasierter Erkennung von Malware

Malware-Entfernungs-Tool (MRT): Automatisierte Entfernung von erkannter Malware

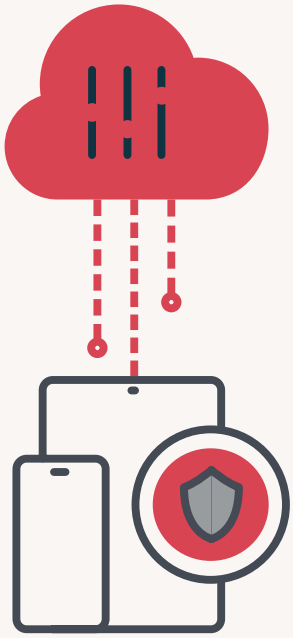
Notarielle Beglaubigung: App-Scandienst, der ein digitales Ticket für eine als kostenlos befundene Software ausstellt

Gatekeeper: Arbeitet mit Notarisierung, um sicherzustellen, dass nur vertrauenswürdige Software auf Ihrem Mac läuft

Sandbox (Containerisierung): Begrenzt den Schaden an Ihrem Mac, falls Benutzer*innen-Daten kompromittiert werden

App Store: Sichere Methode zur Verteilung von vertrauenswürdigen Apps, verwaltet von Apple

Anders gefragt: Haben IT- und Sicherheitsteams einen Überblick über die neuesten Bedrohungen, die auf den Mac in Ihrem Unternehmen abzielen? Ohne speziell entwickelte Sicherheits- und Verwaltungslösungen ist die Antwort ein klares **Nein**. Die Menge und die Art der Bedrohungen, die auf Apple abzielen, erfordern mehrschichtige Verteidigungsstrategien, flexible Unterstützung für verschiedene Eigentumsmodelle und eine zentrale Verwaltungsfunktion, um den vielfältigen und wachsenden Anforderungen der modernen Bedrohungslandschaft gerecht zu werden.

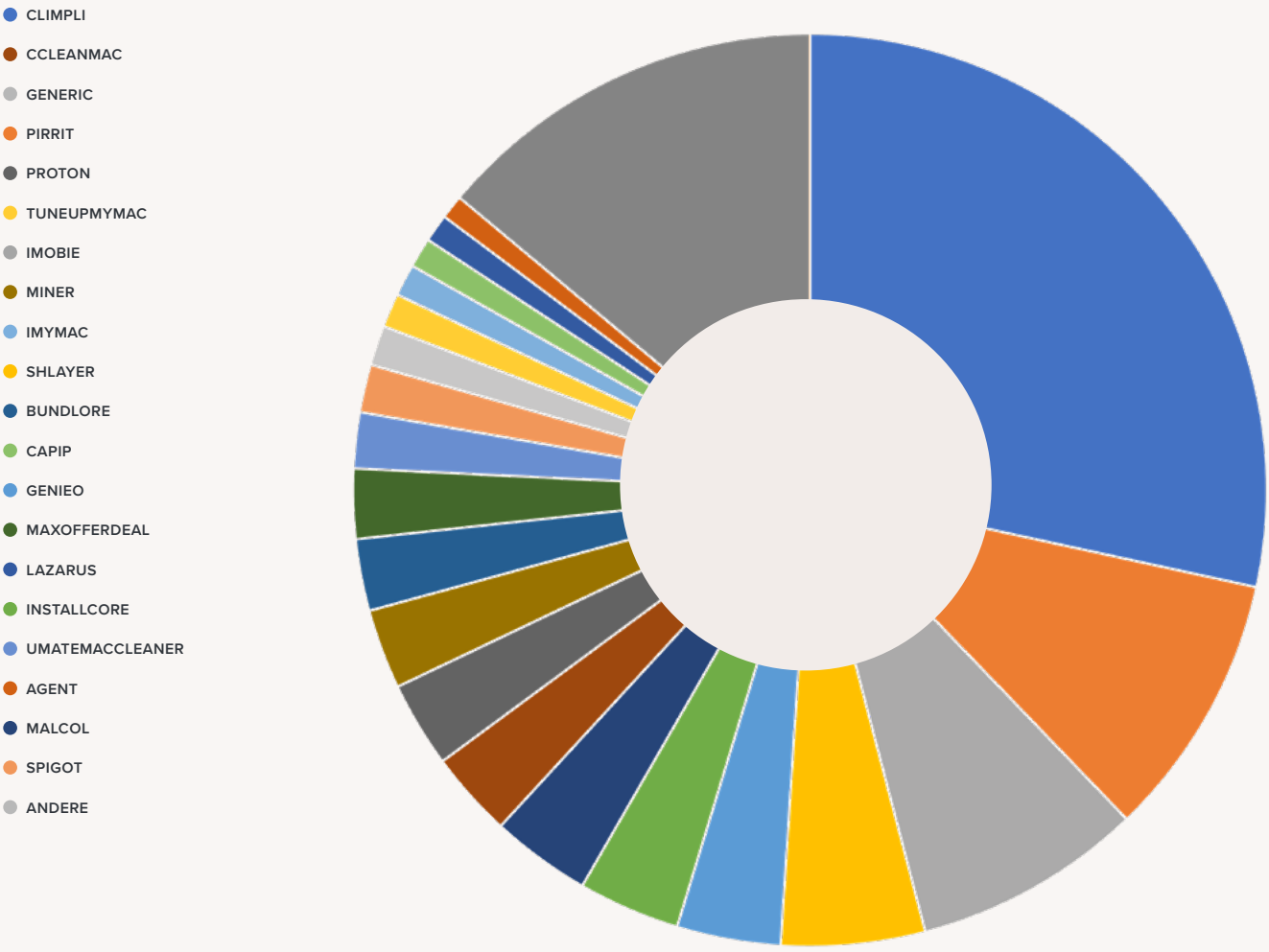


Lustige Tatsache:

Im Jahr 2021 wurde bei **6 % der** Organisationen eine Malware auf einem Gerät aus der Ferne installiert, **gegenüber 3 % im Jahr 2020.**

Quelle: Jamf's Sicherheit 360: Jährlicher Trendbericht

Der Anteil der im Jahr 2021 entdeckten Mac Malware-Familien



Quelle: Jamf Threat Labs

Schichten der Verteidigung

Bislang haben wir das potenzielle Risiko für Unternehmensdaten sowie die drei Säulen erörtert, die die Grundlage für eine moderne, mehrschichtige Verteidigungsstrategie bilden, bei der Verwaltung und Sicherheit gleichberechtigte Anker für Ihren Endpunktsicherheitsplan sind.

Wir setzen diesen Weg fort, indem wir zusätzliche Konzepte, Komponenten, Technologien und Praktiken einbeziehen, um einen Sicherheitsplan für Endgeräte zu entwickeln, der die besonderen Anforderungen Ihres Unternehmens erfüllt. Wir arbeiten daran, die Sicherheit in Ihrer gesamten Flotte umfassend zu gewährleisten, indem wir die besten Lösungen einbeziehen, die speziell für Apple zentrierte Endgeräte entwickelt wurden, und gleichzeitig die Wahlmöglichkeiten der Benutzer unterstützen.

Der Schlüssel liegt darin, die Integration zu einer natürlichen Erweiterung der Sicherheits- und Verwaltungsfunktionen zu machen, die mit den bestehenden Sicherheits-Workflows zusammenarbeitet und diese erweitert, während die Benutzererfahrung verbessert und nicht beeinträchtigt wird.

Wahl des Benutzers/der Benutzerin

COPE/BYOD/CYOD sind Besitzstände im modernen Computing, aber die Sicherheit und Verwaltbarkeit der Endgeräte muss gleich bleiben, wenn Daten gesichert und Bedrohungen abgewehrt werden sollen. Ziel sollte es sein, eine Lösung zu finden, die leistungsfähig und gleichzeitig flexibel genug ist, um der Risikobereitschaft gerecht zu werden und es den Nutzer*innen zu ermöglichen, bequem von jedem Ort aus mit jedem Gerät zu arbeiten.

Wählen Sie das Beste seiner Art

Geben Sie sich nicht mit einer Lösung zufrieden, die nur minimale Unterstützung für das Apple Ökosystem bietet, nur weil sie auch Windows Geräte verwaltet. Der vermeintliche Vorteil des Wegfalls des Verwaltungsaufwands verliert schnell an Wert, wenn man ihn mit den besten Lösungen vergleicht, die speziell auf Apple Geräte zugeschnitten sind und alle Funktionen vom ersten Tag an unterstützen. Sie sollten entscheiden, wann und wie Sie Ihre Endgeräte verwalten — und sich dies nicht von Ihrer Sicherheits- oder Verwaltungssoftware vorschreiben lassen.

Integration in bestehende Infosec-Workflows

Es ist nicht nötig, das Rad neu zu erfinden, vor allem dann nicht, wenn Sie über ausgereifte Arbeitsabläufe verfügen, die den Anforderungen Ihres Unternehmens und Ihrer Benutzer*innen entsprechen. Dies ist ein Punkt, an dem sich die Integration für IT- und Sicherheitsteams auszahlt, indem sie ihre bestehenden Workflows mit erstklassigen Lösungen verbinden, um die grundlegende Sicherheit und Verwaltung zu verbessern — und nicht aufgrund von Inkompatibilität oder mangelndem Entwicklersupport abreißen.

Erhöhen Sie das Benutzererlebnis zu einer Schlüssellösung

Seien wir ehrlich, die Benutzer*innen werden oft darauf verwiesen, was sie tun können und was nicht. In der modernen Computerlandschaft mit Remote-Arbeit und BYOD-Programmen müssen die Endbenutzer*innen als Teil der Lösung betrachtet werden — nicht als Problem, das vor sich selbst geschützt werden muss.

Endpunktsicherheit ist eine grundlegende Fähigkeit

Denken Sie an Yin und Yang — Endpunktsicherheit geht über einen auf Ihrem Mac installierten Virenschutz oder ein auf Ihrem iOS basierten Gerät konfiguriertes VPN hinaus. In der modernen Bedrohungslandschaft arbeiten Sicherheit (Yin) und Management (Yang) nahtlos als eine ganzheitliche, auf Apple ausgerichtete Lösung zusammen, die als Grundlage für die unzähligen Technologien, Praktiken und Richtlinien dient, die Ihren Defense-in-Depth-Plan ausmachen und gleichzeitig die Einhaltung der Endpunkt-Compliance sicherstellen.

Missverständnisse über All-in-One-Lösungen

Ein zentralisierter Stack bezieht sich auf die Fähigkeit beider Lösungen, als eine zusammenhängende Einheit zu arbeiten (wieder denken Sie an Yin und Yang) und bietet ganzheitliche Vorteile durch die Einbeziehung beider Hälften. Es sollte nicht als eine einzige Lösung missverstanden werden, die die schwere Arbeit anstelle von beiden übernimmt, normalerweise unter dem Deckmantel einer „einzigen Glasscheibe", da diese Einheitslösungen oft mehrere Betriebssysteme verwalten, aber auf Kosten der vollen Unterstützung für jede Lösung, was zu einem Mangel an Effizienz und Wirksamkeit führt, wenn es um Apple zentrierte Endpunktsicherheit geht.

Integration zwischen Lösungen - Win-Win

Die Vereinheitlichung von Management und Sicherheit, die als eine undurchdringliche Kraft agieren, beginnt mit der gemeinsamen Nutzung der Daten, auf die beide Teams angewiesen sind, um ihre jeweiligen Aufgaben zu erfüllen. Darüber hinaus hilft die Integration aller erforderlichen Tools und Workflows in eine einzige Lösung den Support-Teams, sich auf die Unterstützung der Benutzer*innen zu konzentrieren, anstatt sich mit der Suche nach Problemen und deren Behebung abzumühen. Von der Datenerfassung bis hin zur Bewertung des Gerätestatus, der Erstellung von Berichten und der Verwaltung von Echtzeitwarnungen – all dies kann einfach verwaltet werden, während gleichzeitig Arbeitsabläufe implementiert werden, um erkannte und/oder vermutete Probleme zu sortieren und zu beheben, bevor Bedrohungen zu etwas viel Schlimmerem führen können, wie z. B. zu einer Datenverletzung.

Sicherheit oder Leistung? Warum nicht beides?!

Sicherheit wird oft durch das Prisma der Kompromittierung betrachtet. Um mehr Schutz zu erhalten, müssen die Betroffenen auf bestimmte Freiheiten verzichten. Neue Technologien wie Zero Trust-Netzwerkzugriff (ZTNA) mit seinen kontextbewussten Richtlinien stellen diesen Gedanken jedoch auf den Kopf, indem sie weder Endgeräten noch ihren Verbindungen vertrauen. Stattdessen konzentriert sich ZTNA darauf, die Daten vor unbefugtem Zugriff und Bedrohungen der Datenintegrität zu schützen und sowohl Sicherheit als auch Leistung zu bieten, ohne die Benutzerfreundlichkeit zu beeinträchtigen.

Die Zahl der Unternehmen, die eine potenziell unerwünschte Anwendung in ihrer Flotte installiert haben, hat sich von 5 % auf 11 % mehr als **verdoppelt.**

36 % der Unternehmen werden im Jahr 2021 auf Indikatoren für **bösartigen Netzwerkverkehr** auf einem **Remote-Gerät stoßen"**, was die Frage aufwirft: **Sind Ihre IT- und Sicherheitsteams in der Lage, schnell auf Anzeichen einer Gefährdung zu reagieren?**

Wusssten Sie schon:

34 % der kompromittierten Geräte werden 2021 auf Konferenzdienste **(wie Zoom, Skype und Microsoft Teams)** zugreifen. Diese Zahl stieg auf **64 %.**

Quelle: Jamf's Sicherheit 360: Jährlicher Trendbericht

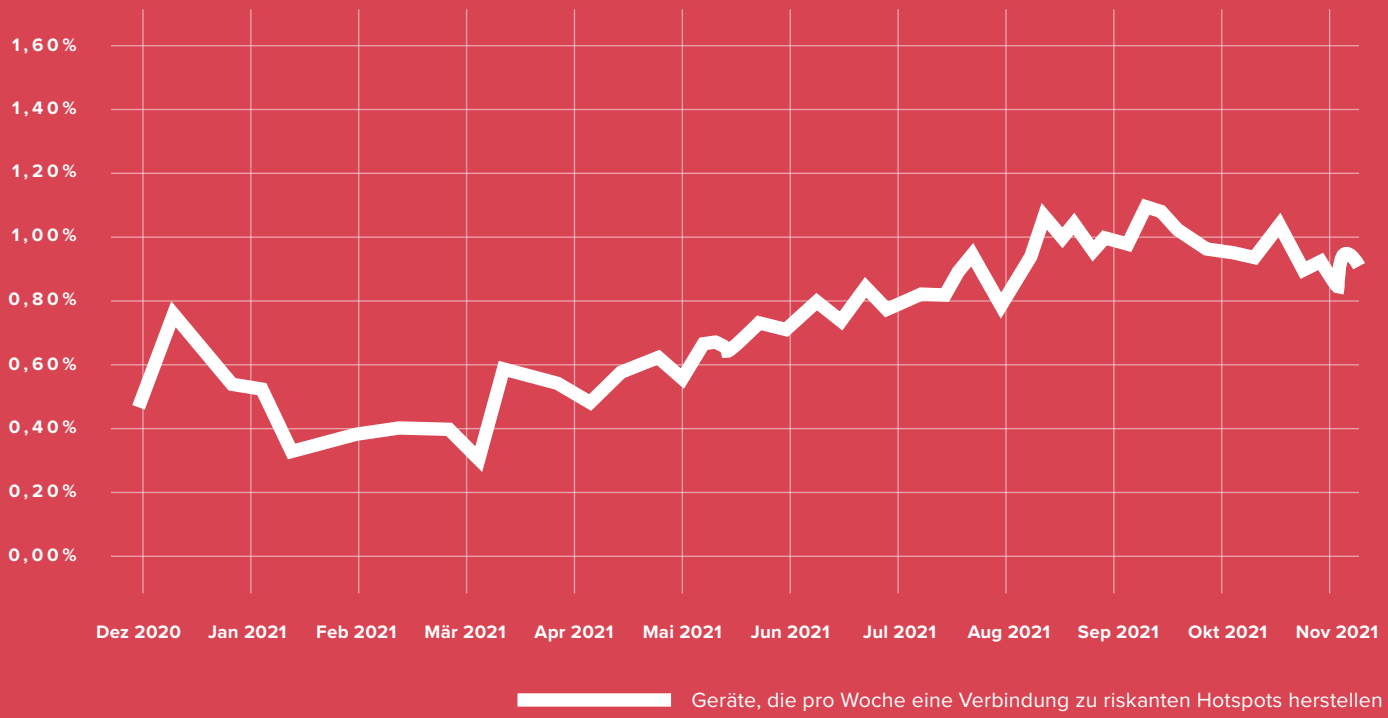
Befähigung Ihrer **Nutzer*innen**

Der Benutzer/die Benutzerin ist wichtig. Die Technologie sollte die Benutzer*innen unterstützen, sie befähigen und sie nicht in ihrer Produktivität einschränken oder blockieren, sondern sich in den Kontext einfügen, in dem sie sich am wohlsten fühlen. Schließlich trägt ihr Komfort dazu bei, dass sie zufriedene Benutzer*innen sind, und ein zufriedener Benutzer/eine zufriedene Benutzerin wird immer produktiver sein als ein unzufriedener/eine unzufriedene. Dies gilt umso mehr, wenn man moderne Umgebungen betrachtet, die auf Programmen zur Mitarbeiterauswahl und BYOD-Initiativen basieren. Dies wird mit der Verlagerung der Infrastruktur in die Cloud kombiniert, um die Remote- und Hybrid-Arbeitsumgebung zu unterstützen.

Den Daten von Jamf Threat Labs zufolge ist die Zahl der Benutzer*innen, die auf Phishing-Angriffe hereinfallen, im Vergleich zum Vorjahr um 160 % gestiegen."

Quelle: Jamf's Sicherheit 360: Jährlicher Trendbericht

Geräte, die pro Woche eine Verbindung zu riskanten Hotspots herstellen



Quelle: Jamf's Sicherheit 360: Jährlicher Trendbericht

Die wichtigsten Erkenntnisse:

- Bewerten Sie Ihre Endgeräte, um festzustellen, welche modernen Schutzmaßnahmen erforderlich sind, um die Sicherheitsanforderungen zu erfüllen.
- Führen Sie ein Framework ein, das speziell für den Schutz von Apple Geräten entwickelt wurde und als Grundlage für Ihre Sicherheitsstrategie für Endgeräte dient.
- Vorbeugung von Malware, Erkennung von Schwachstellen und Überwachung von verdächtigem und riskantem Verhalten bei gleichzeitiger Risikominderung und Bereitstellung von Patches durch richtlinienbasierte Workflows, um die Konformität der Geräte zu gewährleisten
- Einrichtung und Aufrechterhaltung sicherer Basislinien, die den Standard für Gerätehygiene setzen
- Erweitern Sie den Apple eigenen Schutz, damit Sicherheitsteams einen Überblick über Bedrohungen haben, die sich auf das Unternehmen auswirken.
- Integration von Sicherheit und Management zur nahtlosen Bereitstellung von Lösungen und zur raschen Beseitigung von Bedrohungen, wenn diese entdeckt werden
- Entscheiden Sie sich für erstklassige Lösungen, die das Apple Ökosystem vom ersten Tag der Veröffentlichung an vollständig unterstützen und mit den von Apple entwickelten Frameworks übereinstimmen – so können die Benutzer*innen eine großartige Erfahrung genießen und die IT-Abteilung kann nach ihrem Zeitplan aktualisieren.
- Beibehaltung des Apple Erlebnisses bei gleichzeitiger Erhöhung der Sicherheit und Beibehaltung der Leistung
- Unterstützung aller Gerätebesitzmodelle, um die Sicherheit von Benutzer*innen, Geräten und Daten zu maximieren und gleichzeitig die Privatsphäre des Endbenutzers/der Endbenutzerin zu schützen
- Ermöglichen Sie Ihren Nutzer*innen, mit dem Gerät produktiv zu sein, mit dem sie sich am wohlsten fühlen und von dem aus sie am liebsten arbeiten

Erfahren Sie, wie Jamf eine komplette, zweckgerichtete Lösung zum Schutz der Benutzer*innen vor böswilligen Absichten anbietet — und das bei minimaler Beeinträchtigung der Endbenutzererfahrung. Oder fordern Sie eine Testversion an und sehen Sie, wie Sie Ihre Benutzer*innen schützen können.

Testversion anfordern