jamf

Bewertung der Sicherheitsanforderungen Ihrer Organisation

Warum dies für Ihre allgemeine Sicherheitslage Entscheidend ist

Die einzigartigen Sicherheitsanforderungen Ihres Unternehmens zu verstehen, ist eine Kunstform, die teils theoretisch, teils praktisch ist. Obwohl es sich um eine duale Lösung handelt, ist sie fest in der Logik verwurzelt, indem sie wichtige Schwachstellendaten aus Risikobewertungen und Endpoint-Telemetrie, die durch Sichtbarkeit und Überwachung gesammelt werden, nutzt - in Verbindung mit der Kenntnis geltender gesetzlicher Anforderungen. Alle diese Komponenten zusammen bilden die Grundlage für die Entwicklung von Sicherheitstools und helfen Unternehmen, ihre Compliance-Ziele zu erreichen (und zu halten).

Den Finger am Puls des Unternehmens zu haben, ist für den anhaltenden Erfolg des Unternehmens von größter Bedeutung. Fragt man ein Unternehmen: „Wie bleiben Sie erfolgreich?“, so wird man Ihnen sicher sagen, dass es darauf ankommt, die Bedürfnisse des Unternehmens zu verstehen und diese Informationen so zu nutzen, dass Risiken minimiert und gleichzeitig die Chancen maximiert werden, um das Unternehmen voranzubringen. Dies gilt vor allem für diejenigen, denen es gelungen ist, ihren Betrieb auch in Zeiten des wirtschaftlichen Abschwungs, in Gesundheitskrisen oder einfach durch eine jahrzehntelange Langlebigkeit aufrechtzuerhalten.

In diesem Papier, diskutieren wir:

- Was ein Risiko ist und wie die gesammelten Telemetriedaten einen Einblick in den Zustand des Geräts und die allgemeine Sicherheitslage geben
- Warum die Risikobewertung in regelmäßigen Abständen und iterativ als Teil des Sicherheitskonzepts durchgeführt werden muss
- Wie diese Daten Ihrem Unternehmen nicht nur dabei helfen, seine Sicherheitsbedürfnisse zu bestimmen, sondern auch, wie es sie zum Schutz vor aktuellen und zukünftigen Risiken einsetzen kann
- Warum die Integration von Risikodaten in Endpoint-Sicherheitslösungen Unternehmen dabei hilft, eine starke Sicherheitslage aufrechtzuerhalten und gleichzeitig Compliance-Ziele zu erfüllen

Diese Überzeugung gilt unabhängig davon, welche Art von Unternehmen Sie führen. Zum Beispiel mit Filmen und Musik. Unterhaltung gibt es seit Jahrhunderten. Und in unterschiedlichem Maße hat sie sich im Laufe der Zeit bewährt, weil sie in der Lage war, die Wünsche ihrer Zielgruppe zu erkennen und ihr Angebot entsprechend anzupassen.

Es ist ein fortlaufender und evolutionärer Prozess.

Und ähnlich verhält es sich mit der Cybersicherheit. Anstatt die Anforderungen ihrer Kund*innen zu bewerten, müssen Unternehmen jedoch nach innen schauen, um festzustellen, was erforderlich ist, um einen sicheren Geschäftsbetrieb aufrechtzuerhalten. Die Risikobewertung umfasst alles, von Geräten über Software bis hin zur Infrastruktur, den Daten, Prozessen und Richtlinien Ihres Unternehmens. Diese Teile fügen sich zu einem Gesamtbild der Sicherheitslage eines Unternehmens zusammen.

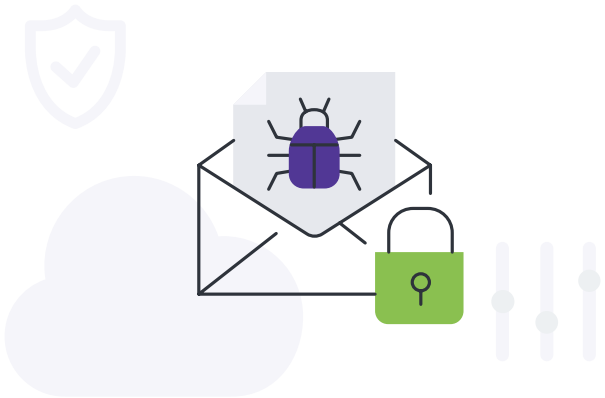
Anhand dieser Informationen können Unternehmen die Risiken und Verbindlichkeiten ihrer aktuellen Cybersicherheitsstrategie bewerten und die notwendigen Schritte unternehmen, um diese zu korrigieren, Risiken zu minimieren und Bedrohungen abzuschwächen.

Die Risikobewertung ist kein einmaliger Vorgang.
In Übereinstimmung mit bewährten Praktiken sollten Risikobewertungen in regelmäßigen Abständen durchgeführt werden. Aufgrund des dynamischen Charakters der Technologie befindet sich alles immer in einem vorübergehenden Zustand. Für die Sicherheit ist dies sogar noch wichtiger, da Bugs ein natürlich wiederkehrendes Problem sind, das zu Schwachstellen führt, die die Sicherheitslage verschlechtern und letztlich Geräte, Benutzer und Daten dem Risiko einer Kompromittierung aussetzen.

Dabei werden die Bedrohungsakteur*innen nicht berücksichtigt, die die Verteidigung Ihres Netzwerks aktiv auf Anzeichen von Schwachstellen und Angriffsvektoren untersuchen und testen.

Vereinfacht ausgedrückt: Die Risikobewertung sollte regelmäßig als Teil einer umfassenden Cybersicherheitsstrategie durchgeführt werden, wobei die gewonnenen Bewertungsdaten nicht nur dazu dienen, den aktuellen Stand der Sicherheit zu ermitteln, sondern auch, um iterativ den ganzheitlichen Sicherheitsplan des Unternehmens für eine umfassende Verteidigung zu erstellen, z. B:

- Etappen im Lebenszyklus von Geräten und Apps
- Beschaffung, Konfiguration und Einsatz von Sicherheitskontrollen
- Erreichen von Regulierungszielen und Durchsetzung der Compliance
- Identifizierung bestehender und neuer Bedrohungen und Zuweisung von kritischen Werten und Schweregraden
- Aufrechterhaltung der Abstimmung zwischen Risikobereitschaft und Risikominderungsstrategien
- Überarbeitung und Umsetzung von Verfahren zur Reaktion auf Vorfälle
- Aktualisierung und Einführung von Strategien zur Bedrohungsabwehr, z. B. Schulungen für Endnutzer*innen



Risikobewertung

Wir haben erörtert, warum Risikobewertungen wichtig sind, aber wie sieht eine solche Bewertung aus? Und was ist tatsächlich gefährdet? Die genauen Einzelheiten können zwar von Branche zu Branche oder von Unternehmen zu Unternehmen variieren, aber im Grunde geht es um Verständnis:

- Die Bedrohungslandschaft
- Die Schwachstellen Ihrer Organisation
- Die Wahrscheinlichkeit eines Angriffs
- Welche Auswirkungen ein Angriff auf Ihr Unternehmen haben wird
- Wie schnell sich Ihr Unternehmen von einem schweren Angriff erholen kann

> *„Um deinen Feind zu kennen, musst du dein Feind werden“* **- Sun Tzu**

Sehen wir uns einige Fragen an, die eine Risikobewertung beantworten muss.

Wo ist meine Organisation anfällig?

Ein Angreifer/eine Angreiferin kann viele Einstiegspunkte nutzen, um Ihr System auszunutzen, z. B. Hardware, Software, Schnittstellen und Herstellerinteraktionen mit Ihrer Netzwerkinfrastruktur sowie jeden Benutzer/jede Benutzerin, der Zugriff auf diese Komponenten hat. Schwachstellen können auch in Ihren Geschäftsprozessen und Richtlinien auftreten.

Die Klassifizierung und Inventarisierung dieser Komponenten ist notwendig, um ein solides Verständnis für Ihre Infrastruktur zu erhalten. Das sollten Sie wissen:

- Welche Geräte auf Ihr Netzwerk zugreifen
- Wer hat Zugang zu Ihren Daten?
- Wenn Sie bewährte Sicherheitspraktiken befolgen (z. B. Zugriff mit geringsten Rechten, strenge Kennwortrichtlinien usw.)
- Wenn Ihre Anbieter*innen Schwachstellen in Ihre Systeme einführen
- Wenn die Benutzer*innen darin geschult werden, potenzielle Bedrohungen zu erkennen und eine gute Sicherheitshygiene zu praktizieren

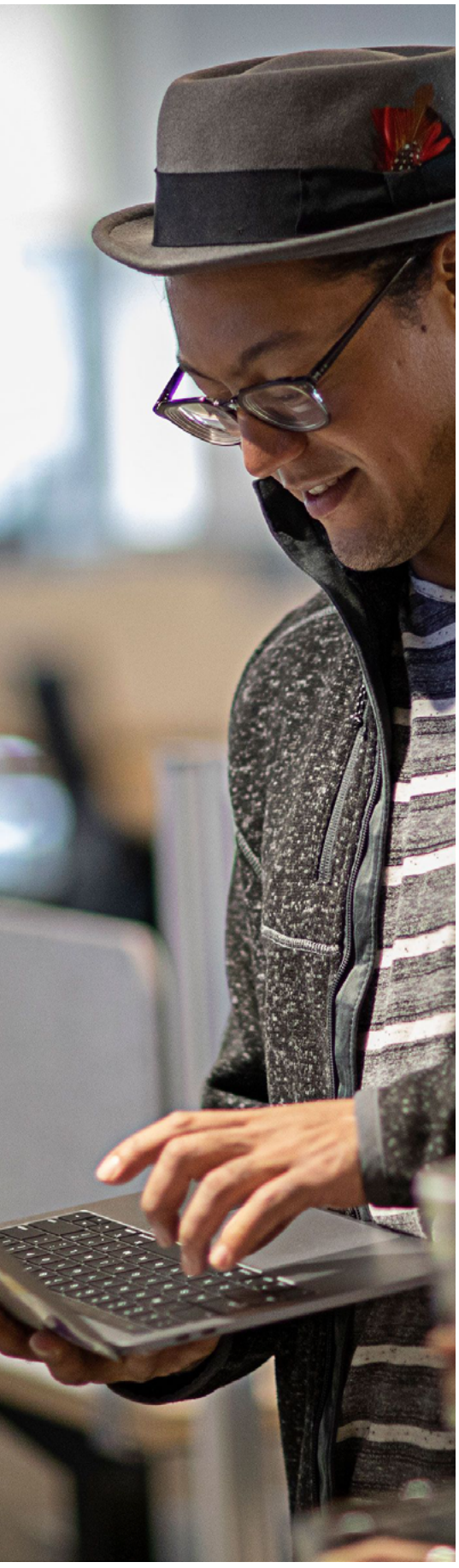
Welche Bedrohungen gibt es?

Risikobewertung bedeutet auch, zu wissen, welche Bedrohungen es gibt und wie sie Ihr System beeinträchtigen können. Auf diese Weise können Ihre IT- und Sicherheitsteams einschätzen, welcher Teil Ihres Unternehmens am anfälligsten ist, wie wahrscheinlich ein Angriff ist und welche Auswirkungen er auf Ihr Unternehmen haben könnte.

BEISPIEL

Durch die Verwendung des MITRE ATT&CK-Frameworks erhalten Sicherheitsteams die Informationen, die sie benötigen, um zu verstehen, wie bösartige Akteur*innen Ihr System angreifen könnten. Und bei unbekannten Bedrohungen können Teams die Bedrohungsjagd und den Einsatz von KI- und Machine-Learning-Software (ML) in Betracht ziehen, um verdächtiges oder bösartiges Verhalten zu erkennen. KI und ML arbeiten unermüdlich hinter den Kulissen, um Anomalien außerhalb des Grundverhaltens Ihres Netzwerks zu erkennen. Ihre Fähigkeit, enorme Datenmengen an Bedrohungsinformationen und Daten zum Musterabgleich zu verarbeiten, macht sie zu wichtigen Werkzeugen in Ihrem Arsenal der Cybersicherheit. Darüber hinaus können die mit dieser Software gesammelten Daten mit der gesamten Sicherheitsgemeinschaft geteilt werden, wodurch die Wissensbasis von Cyber-Sicherheitsexpert*innen überall verbessert wird.

Die Kenntnis gängiger Bedrohungsvektoren kann Ihnen helfen, Prioritäten zu setzen, welche Bereiche Ihres Unternehmens am meisten geschützt werden müssen. Bedrohungen gibt es in vielen Formen - laut dem **2023 Data Breach Investigation Report von Verizon** dringen Angreifer*innen mit gestohlenen Zugangsdaten, Phishing und unter Ausnutzung von Sicherheitslücken in Unternehmen ein. Im Allgemeinen stammen die Datenverletzungen aus völlig externen Quellen, aber ein nicht unerheblicher Anteil (bis zu 40 %) stammt aus der Ausnutzung von Partnersoftware. Der Schutz vor diesen Bedrohungen erfordert eine sorgfältige Analyse Ihrer aktuellen Einstellungen und Richtlinien - mehr dazu später.



Welche Auswirkungen hätte ein Cyberangriff auf mein Unternehmen?

Das Wissen um die Wahrscheinlichkeit einer Bedrohung hilft bei der Festlegung von Prioritäten in Ihrer Verteidigungsstrategie. Ein weiterer Aspekt ist das Verständnis der Auswirkungen, die eine Bedrohung auf die Mission Ihres Unternehmens hat, die auch finanzieller Art sein können, da die durchschnittlichen Gesamtkosten einer Datenschutzverletzung laut **IBMs Cost of a Data Breach Report** im Jahr 2022 bei 4,35 Millionen USD liegen. Mit durchschnittlich 277 Tagen für die Erkennung und Eindämmung einer Sicherheitsverletzung kann viel Zeit verloren gehen. Oder es kann Ihrer Beziehung zu den Kund*innen schaden, sei es durch Reputationsverluste oder durch Preiserhöhungen aufgrund von Datenschutzverletzungen, wie es 60 % der betroffenen Unternehmen im Jahr 2022 taten. Ganz zu schweigen von den Geldstrafen, die von den zuständigen Organisationen verhängt werden, wenn Ihr Unternehmen die geltenden Normen nicht einhält.

Was kommt als Nächstes?

Je größer die Auswirkungen eines Angriffs sind, desto höher ist natürlich die Priorität für den Schutz der betreffenden Systeme. Dies gilt auch für Angriffe mit höherer Wahrscheinlichkeit. Die Kombination dieser beiden Messgrößen - Auswirkung und Wahrscheinlichkeit - hilft bei der Quantifizierung des Risikos, das bestimmte Bedrohungen für Ihr Unternehmen darstellen. Ein solides Verständnis des Risikos gibt Ihnen das nötige Wissen, um Prioritäten zu setzen und Folgendes zu bestimmen:

- Welche kritischen Systeme am meisten geschützt werden müssen (d. h. den größten Verlust an geschäftskritischen Funktionen verursachen werden)
- Welche Kontrollen sind für die beste Verteidigungsstrategie erforderlich?
- Welche Software-Tools können Ihre Sicherheitslage verbessern?
- Wie viel Risiko können Sie tolerieren (d. h. Ihre Risikobereitschaft)

Sobald Sie die Informationen aus Ihrer Risikobewertung haben, ist es an der Zeit, das Gelernte umzusetzen. In den folgenden Abschnitten befassen wir uns mit der Bewertung Ihres Netzwerks und der Gerätetelemetrie sowie mit den Richtlinien, die Sie bei der Entwicklung oder Überarbeitung Ihrer Sicherheitsrichtlinien anwenden können.

Sichtbarkeit und Überwachung

Sie haben also die Risiken bewertet, sie identifiziert und Ihre Risikobereitschaft an Ihre Toleranzgrenze angepasst. Außerdem haben Sie die notwendigen Änderungen vorgenommen, um Sicherheitskontrollen zu beschaffen und zu konfigurieren, die das Risiko mindern. Sie verfügen über eine solide Sicherheitslage, und die Beteiligten haben die erforderlichen Schulungen erhalten, um aktuelle Bedrohungen zu erkennen und zu verstehen, dass diese gemeldet und entsprechend gehandelt werden müssen. Die Endpoints sind vor Bedrohungen geschützt und die Compliance-Ziele wurden erreicht, da alle Geräte in den Geltungsbereich fallen. Was nun?

Sind IT- und Sicherheitsteams einfach mit ihrer Arbeit fertig und können einen frühen (und wahrscheinlich dringend benötigten) Urlaub nehmen? Leider nein.

Die Dynamik der Technologie ist allgegenwärtig, und in diesem Fall bedeutet dies, dass etwas, das heute sicher ist, nicht für immer sicher bleibt. Der Schlüssel zum Schutz Ihrer Geräte, Ihrer Infrastruktur und Ihres Unternehmens vor allgegenwärtigen Sicherheitsbedrohungen liegt darin, dass Sie den Gesundheitszustand Ihrer Endpoints zu jedem Zeitpunkt kennen.

> *„Wir sind nicht in der Lage, eine Armee auf dem Marsch zu führen, wenn wir nicht mit dem Gesicht des Landes vertraut sind...“* **- Sun Tzu, Die Kunst des Krieges**

Die bei der aktiven Überwachung des Gerätezustands aufgezeichneten Telemetriedaten enthalten eine Fülle von Informationen zur Aufrechterhaltung der Geräte- und Unternehmenssicherheit. Telemetriedaten sind nicht nur der Schlüssel, um sicherzustellen, dass die Endpoints ordnungsgemäß konfiguriert sind, um die gesetzlichen Anforderungen zu erfüllen, sondern sie liefern auch die Metriken, mit denen Unternehmen nachweisen können, dass die Endgeräte zu einem bestimmten Zeitpunkt konform waren. Dies ist eine wichtige Voraussetzung für den Nachweis der Konformität, wenn Unternehmen eine gesetzliche Zertifizierung wie **PCI-DSS** anstreben, um Kartenzahlungen sicher akzeptieren und verarbeiten zu können.

Darüber hinaus ist es wichtig, dass die durch die Überwachung gewonnene Transparenz die Entscheidungsfindung auf allen Geräteebenen und Applebenszyklen unterstützt. Der Überwachungsprozess dient dazu, IT- oder Sicherheitsteams mit aktuellen Informationen über den Zustand ihrer Geräte, die darauf laufende Software und die von den Endbenutzer*innen durchgeführten Aktionen zu versorgen. Darüber hinaus erhalten Administrator*innen und die Geschäftsführung umfangreiche Telemetriedaten, um iterativ fundierte Entscheidungen über notwendige Anpassungen treffen zu können, damit die Konformität der Geräte und die Sicherheit von Benutzer*innen und Daten gewährleistet bleiben.

Welche Art von Daten werden bei der Überwachung erfasst?

Bevor wir uns mit den Arten von Telemetriedaten beschäftigen, die durch die Überwachung erfasst werden, sollten wir zunächst die beiden Arten der Überwachung erörtern:

- **Passiv:** Gesundheitsdaten werden langsam erfasst, in der Regel über einen bestimmten Zeitraum, um die Auswirkungen auf den Endnutzer/die Endbenutzerin oder die Leistungsfähigkeit des überwachten Geräts zu minimieren. Die unregelmäßige Datenerfassung bedeutet, dass die Erfassung von Telemetriedaten mehr Zeit in Anspruch nehmen kann, wodurch sich die Erstellung einer vollständigen Geräte-Basislinie verzögert. Außerdem könnten sich Verzögerungen bei der Datenerfassung direkt auf die Genauigkeit oder Aktualität der Daten auswirken, insbesondere wenn Tage oder Monate zwischen den Datenerfassungen vergehen.

- **Aktiv:** Gesundheitsdaten werden häufig von Endpoints übermittelt. Die Abfrage der Endpunkte erfolgt regelmäßig und wird oft in Echtzeit an ein zentrales Repository übermittelt.

Obwohl die erfassten Daten nahezu identisch sind, bestehen die größten Unterschiede zwischen beiden:

- **Wie** die Telemetriedaten erfasst werden
- Die **Zeit** , die für die Erstellung eines Basisprofils benötigt wird
- Die **Genauigkeit** der Informationen
- Und die **Häufigkeit der Aktualisierung** der Telemetriedaten

Beide Arten der Überwachung haben ihre Vor- und Nachteile, aber die Tatsache bleibt bestehen, dass die moderne Bedrohungslandschaft zu umfangreich ist und sich zu schnell verändert, als dass etwas anderes als die aktive Überwachung ein effektives Mittel sein könnte, um die aktuellsten Daten über den Zustand der Geräte zu sammeln und diese in verwertbare Daten umzuwandeln, um die Lücken in Ihrem Sicherheitsplan zu schließen, wie es das Sicherheitsaxiom „Man kann nicht schützen, was man nicht sehen kann“ in dem SecurityWeek-Artikel über **aktive vs. passive Überwachung zusammenfasst: Nicht länger ein Entweder-oder.**

Arten der erfassten Telemetriedaten und ihre Bedeutung für Ihre Sicherheitslage:

- **Betriebssystem-Aktualisierungen:** Ermitteln Sie den Aktualisierungsgrad des Betriebssystems (OS), um zu wissen, ob die Geräte die neuesten Funktionen unterstützen und ob die Geräte über den neuesten Schutz vor bekannten Bedrohungen verfügen, um Schwachstellen zu minimieren.
- **App-Patch-Stufen:** Wie das Betriebssystem benötigen auch Apps Patches, um Daten während der Verarbeitung zu schützen und gleichzeitig Fehler zu beheben und Schwachstellen zu entschärfen, die andernfalls ein Risiko darstellen könnten.
- **Konfigurationseinstellungen:** Die Härtung von Geräten ist für die Sicherheitslage von entscheidender Bedeutung. Nicht nur deshalb, weil Sie sie für maximale Sicherheit korrekt konfigurieren wollen, sondern auch, um die Möglichkeit von Fehlkonfigurationen zu minimieren, die **zu 21 % der fehlerbedingten Datenschutzverletzungen beitragen (Verizon Data Breach Investigation Report 2023).**
- **Netzwerkaktivität:** Mit welchen webbasierten Inhalten kommunizieren die Geräte? Werden nicht vertrauenswürdige Verbindungen gesichert? Über welche Anschlüsse werden Daten übertragen? Die Antworten auf diese und andere wichtige Fragen zur Netzwerknutzung sind entscheidend für die Bestimmung der Sicherheitslage Ihrer Geräte.
- **Verhaltensanalyse:** Die Benutzer*innen gelten nicht umsonst als das schwächste Glied in der Sicherheitskette. Unterschiedliche Kenntnisstände tragen zum anhaltenden Erfolg von Social-Engineering-Angriffen bei. Indem sie verstehen, wie Benutzer*innen ihre Geräte nutzen, erhalten Administrator*innen ein klareres Bild davon, wie benutzerinduzierte Risiken auftreten und wie sie sich daher besser davor schützen können.
- **Überprüfung der Authentifizierung:** Authentifizierungsprotokolle und Passwortverwaltung sind die Schlüssel, die ein Gerät und seine sensiblen Daten freischalten. Auch ein größeres, stärkeres Schloss oder ein komplexes Kennwortschema gibt keinen Aufschluss darüber, ob Benutzer*innen ihre Anmeldedaten gemeinsam nutzen oder ob ihre Konten kompromittiert wurden. Dies gilt auch für Remote- und hybride Arbeitsumgebungen, in denen eine verteilte Belegschaft auf eine richtlinienbasierte Verwaltung angewiesen ist, um die Sicherheit auf Remote-Endpoints durchzusetzen.
- **Bösartiger Code:** Das Vorhandensein von bösartigem Code kann in verschiedenen Formen auftreten. Das Herunterladen eines Trojaners, der als legitime App getarnt ist, oder von Sideloaded-Apps, der unwissentliche Besuch einer kompromittierten Website oder scheinbar schlummernde Bedrohungen, die im Hintergrund laufen - all dies kann die Einhaltung der Vorschriften gefährden, insbesondere angesichts der zunehmenden Verbreitung und der Angriffstrends im Zusammenhang mit mobilen Geräten.
- **Fehlerprotokollierung:** Geräte protokollieren alles, und je mehr Geräte die Administrator*innen betreuen, desto schwieriger ist es, jedes protokollierte Problem zu lösen. Das ist gut für Bedrohungsakteure und schlecht für Administrator*innen. Doch das muss nicht sein. Bei ordnungsgemäßer Verwaltung und dem Einsatz von SIEM-Lösungen (Sicherheitsinformations- und Eventmanagement) zur Sortierung und sinnvollen Nutzung des potenziell überwältigenden Telemetriedatenstroms ist die Fehlerprotokollierung und Bedrohungserkennung nicht nur effektiv, sondern auch effizient.
- **Systemprozesse:** Endpoint-Sicherheits Administrator*innen müssen wissen, welche Apps auf ihren Geräten laufen. Dies bezieht sich auf die durchschnittliche Basislinie des Geräts selbst und warnt Administrator*innen vor der Verwendung nicht genehmigter (Schatten-IT) oder nicht zugelassener (eingeschränkter) Tools, die andernfalls die Sicherheit verringern könnten, indem sie Datenlecks ermöglichen oder **Risiken für die Privatsphäre der Benutzer*innen erhöhen.**
- **Einhaltung von Audit-Vorschriften:** Bei der Transparenz des Endpunktzustands geht es sowohl um das, was bekannt ist, als auch um das, was nicht bekannt ist. In regulierten Branchen muss ein Unternehmen wissen, wo es auf dem Weg zur Compliance steht. Das bedeutet, dass es verstehen muss, was notwendig ist, um die Compliance-Ziele zu erreichen und gleichzeitig Nachweise für das Erreichen dieser Ziele zu sammeln.

Aber können Telemetriedaten zur automatischen Risikominderung verwendet werden?

Ja, das kann sie. In der Tat gibt es mehrere Faktoren, die die Risikoverwaltung erheblich erschweren, z. B.:

- Bestellung großer Mengen von Geräten, verschiedener Gerätetypen
- Aufrechterhaltung der Sicherheit in einer Flotte von persönlichen und unternehmenseigenen Geräten
- Unterstützung verteilter Arbeitskräfte in entfernten und hybriden Umgebungen
- Konvergenz von zwei oder mehr Bedrohungsarten zur Durchführung komplexer, mehrgleisiger Angriffe auf Ziele
- Durchsetzung von Sicherheitseinstellungen zur Aufrechterhaltung der Endpoint-Compliance

Die Automatisierung der Erfassung, Analyse und Sortierung von Telemetriedaten ist dem manuellen Durchlaufen der einzelnen Schritte vorzuziehen. Aufgrund der schieren Menge an Daten, die es zu durchforsten gilt, der Menge an Zeit, die es braucht, um jede Aufgabe so schnell wie möglich zu erledigen, und natürlich der Tatsache, dass der Mensch nur so viel tun kann, bis er Pausen zum Essen und Ausruhen benötigt.

Keine dieser wesentlichen Einschränkungen gilt für Computer.

Der Einsatz von Systemen, die durch Automatisierung die „schwere Arbeit“ übernehmen, spart Unternehmen wertvolle Zeit und Geld - Ressourcen, die besser dazu genutzt werden können, Angriffe erfolgreich zu verhindern, als sich mit den Aufräumarbeiten im Nachhinein zu beschäftigen.

Die aktive Überwachung ist die zweite Ebene (nach der Risikobewertung) in Ihrem Sicherheitsplan, um den Sicherheitsbedarf Ihres Unternehmens zu verstehen. Die Telemetriedaten werden durch die kontinuierliche Überwachung Ihrer Flotte in Echtzeit erfasst und bereitgestellt. Sie liefern aktuelle Daten zum Zustand der Endgeräte, die von Ihrer Endpoint-Sicherheits Lösung analysiert und verarbeitet werden, um zu ermitteln, wie es um die einzelnen Geräte bestellt ist. Alle erkannten Mängel oder anomalen Verhaltensweisen können automatisiert werden, um Warnungen an IT- oder Sicherheitsteams zu senden (zumindest), um die nächsten Schritte festzulegen. Die Ergebnisse können auch dazu verwendet werden, automatisierte Workflows für die Reaktion auf Vorfälle zu initiieren, wie z. B. die automatische Entfernung bekannter verdächtiger Software von Geräten oder die Quarantäne von Endpoints, die mit Ransomware infiziert sind.

Weitere, fortschrittlichere Workflows sind durch die Integration von Endpoint-Sicherheitslösungen mit anderen Tools, wie Identitäts- und Mobilgeräteverwaltung (MDM), möglich, um robuste Workflows zu erstellen, die mehr Automatisierungsmöglichkeiten bieten

Compliance

Verschiedene Zitate aus Sun Tzu's „Die Kunst des Krieges“ sind in diesem Dokument verstreut, um einige zentrale Themen zusammenzufassen, die IT- und Sicherheitsexpert*innen bei der Durchführung von Due-Diligence-Prüfungen zur Risikobewertung und bei der Vorbereitung eines besseren Verständnisses der Sicherheitsanforderungen ihres Unternehmens nützlich sein können. Damit sollen etwaige Lücken geschlossen und gleichzeitig das Verständnis dafür geschaffen werden, dass jede Phase für sich genommen entscheidend ist. Darüber hinaus führt jede Phase direkt zur nächsten Phase, indem die vorhandenen Informationen für die nächsten Schritte genutzt werden.

Das Verständnis für Ihre Sicherheitsbedürfnisse bedeutet nicht nur, dass Sie wissen, welche Sicherheitsprobleme zu einem bestimmten Zeitpunkt bestehen. Dies bedeutet, dass Sie herausfinden müssen, welche Maßnahmen erforderlich sind, um Probleme zu lösen, und welche Strategien Sie wählen müssen, um sicherzustellen, dass Ihre Endpoints den Compliance-Anforderungen entsprechen - unabhängig davon, ob Ihr Unternehmen zu einer regulierten Branche gehört oder nicht. Das Ziel ist es, die Einhaltung der gesetzlichen Vorschriften zu gewährleisten oder - bei nicht regulierten Unternehmen - die Übereinstimmung mit den Unternehmensrichtlinien aufrechtzuerhalten. Beides dient der Sicherheit und dem Schutz der Privatsphäre der Benutzer*innen, indem Risiken mithilfe eines strukturierten Rahmens minimiert werden, der die Sicherheit Ihrer Geräte und Ihres Unternehmens gewährleistet.

> *„Die höchste Kunst des Krieges besteht darin, den Feind zu unterwerfen, ohne zu kämpfen.“* **- Sun Tzu**

Die „Feinde“ sind in diesem Fall Bedrohungsakteur*innen und alles und jeder, der ein Risiko für Ihr Unternehmen darstellen kann. Schließlich ist das Risiko gleichbedeutend mit einer Haftung, die andernfalls zur Ausnutzung einer Schwachstelle oder zu weitaus schlimmeren Folgen führen könnte. Wenn es darum geht, Ihre Sicherheitsbedürfnisse zu verstehen, ist es jedoch müßig, sich über die Vielzahl potenzieller „Feinde“ Gedanken zu machen, die über den unmittelbaren, konkreten Zustand Ihres Netzwerks hinausgehen. Ihr Augenmerk sollte besser auf die Vielfalt der Risiken selbst gerichtet sein und nicht darauf, woher sie kommen. Dadurch können sich die Administrator*innen darauf konzentrieren, wie sie am besten vorgehen, um die Compliance zu wahren, indem sie Geräte, Benutzer*innen und Daten sowohl vor aktuellen als auch vor wachsenden und sich weiterentwickelnden Bedrohungen schützen.

Welche branchenspezifischen Leitlinien helfen bei der Identifizierung und Minimierung der verschiedenen Arten von Risiken?

Es ist wichtig, zwischen Leitlinien, Rahmenwerken und Grundlinien zu unterscheiden, bevor man fortfährt. Leitlinien haben eine Affinität zu bewährten Verfahren. Es gibt keine festen Regeln, die zu befolgen sind, sondern eher eine Gruppierung von Branchenpraktiken, die Organisationen dabei helfen, verschiedene Formen von Risiken in einer allgemeinen Kapazität zu verwalten.

Andererseits zielen Frameworks, die eine ähnliche DNA wie Best Practices haben, darauf ab, alle Informationen, Praktiken, Einstellungen, Kontrollen und Arbeitsabläufe zu verketten, die notwendig sind, um ein bestimmtes organisatorisches oder Compliance-Ziel zu erreichen oder zu übertreffen

Grundlinien haben Ähnlichkeiten mit den beiden erstgenannten Arten von Leitlinien, was ihre Rolle beim Erreichen und Aufrechterhalten der Compliance betrifft, jedoch aus einem anderen Blickwinkel. Leitlinien liefern Ideen für bewährte Praktiken, und Rahmenwerke strukturieren sie und formatieren sie so, dass ein bestimmtes Ziel erreicht wird, aber Grundlinien werden nicht auf dieselbe Weise umgesetzt. Sie fungieren als Barometer, mit dem Organisationen ihren Erfolg bei der Erreichung ihrer Compliance- oder Organisationsziele messen können.

Laienhaft ausgedrückt, sind Leitlinien wie Zutaten. Rahmen ergeben sich aus der Kombination von Elementen, um eine bestimmte Art von Gericht zu schaffen. Schließlich dienen die Grundlinien als Richter, um festzustellen, ob das Gericht entsprechend den verwendeten Zutaten und dem befolgten Rezept richtig zubereitet wurde. Und voilà, bon appétit.

Jetzt, da wir die Unterschiede verstehen, können wir mit Frameworks und Grundlinien weitermachen, denn wir wollen unsere Sicherheitsbedürfnisse verstehen und sie so genau wie möglich erfüllen.

In der Sicherheitsplanung häufig verwendete Frameworks

Das National Institute for Standards and Technology (NIST) SP 800-53, Rev. 5: Sicherheit- und Datenschutzkontrollen für Informationssysteme und Organisationen, bietet einen Katalog von Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen zum Schutz von organisatorischen Abläufen und Vermögenswerten ... vor einer Vielzahl von Bedrohungen und Risiken.

NISTIR 8011, Vol. 4: Der Schwerpunkt von Automatisierung der Bewertung von Sicherheitskontrollen liegt auf der Automatisierung der Bewertung von Sicherheitskontrollen innerhalb jeder einzelnen Informationssicherheitsfunktion, während gleichzeitig das Management von Risiken, die durch Fehler in der Software im Netzwerk entstehen, behandelt wird.

ISO/IEC 27001: Information Security Management Systems (ISMS) ist eine der bekanntesten Normen zur Definition der Anforderungen, die ein ISMS erfüllen muss. Der Rahmen bietet eine ganzheitliche Anleitung für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems.

Cyber Essentials: Eine britische Initiative, die Ihnen zeigt, wie Sie Ihr Unternehmen - unabhängig von seiner Größe - gegen eine ganze Reihe der häufigsten Cyberangriffe schützen können. Es bietet mehrere Stufen an, darunter auch eine praktische technische Überprüfung zur Feststellung der Compliance.

MITRE ATT&CK: Hierbei handelt es sich um eine globale Wissensbasis über die von Cyber-Angreifer*innen verwendeten Taktiken, die auf Beobachtungen realer Techniken beruht. Sie dient als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden und wird in verschiedenen Branchen, Gemeinschaften und Endpoint-Sicherheitslösungen eingesetzt.

Control Objectives for Information and related Technology (COBIT) 2019: Ein von ISACA entwickeltes Rahmenwerk, das sich auf allgemeine Prozesse für die IT-Verwaltung konzentriert und diese mit geschäftlichen und IT-bezogenen Zielen verknüpft. Dazu gehört eine Messkomponente, die die Verantwortlichkeit des Teams sicherstellt und gleichzeitig eine flexible Verknüpfung mit anderen Rahmenwerken wie ISO 27001, ITIL und gängigen Projektverwaltungssystemen ermöglicht.

Payment Card Industry Data Security Standard (PCI-DSS): Der De-facto-Standard für Informationssicherheit, den Unternehmen verwenden und der die technischen und betrieblichen Anforderungen für den Umgang mit Kreditkartenzahlungsdaten regelt und der von den großen Kartenausstellern weltweit durchgesetzt wird.

Cybersecurity Maturity Model Certification (CMMC) 2.0: Basierend auf den Sicherheitsanforderungen mehrerer NIST-Sonderveröffentlichungen bietet das mehrstufige Modell Zertifizierungsstufen für Organisationen, die kumulativ die CMMC-Stufen und die damit verbundenen Verfahrensweisen in allen Bereichen erfüllen.

OWASP Risikobewertung: Dieses Framework von OWASP besteht aus Sicherheitstests, Risikobewertungs- und Scanning-Tools und soll die Unsicherheiten beseitigen, die sich aus der Kompatibilität und Komplexität der Einrichtungsprozesse in der Umgebung ergeben, um eine einfache Möglichkeit zu bieten, die Codequalität und Schwachstellen ohne zusätzliche Einrichtung zu analysieren und zu überprüfen.

macOS Sicherheits-Compliance-Projekt: Das gemeinsame Projekt von Bundesmitarbeitern für IT-Sicherheit des NIST, der National Aeronautics and Space Administration (NASA), der Defense Information Systems Agency (DISA) und des Los Alamos National Laboratory (LANL) ist ein Open-Source-Projekt, das einen programmatischen Ansatz zur Erstellung von Sicherheitsrichtlinien bietet, einschließlich Konfigurationseinstellungen, die eingesetzt werden können, um die Einhaltung bestimmter gesetzlicher Vorgaben zu erreichen.

Die Rolle von Baselines in der Cybersicherheit

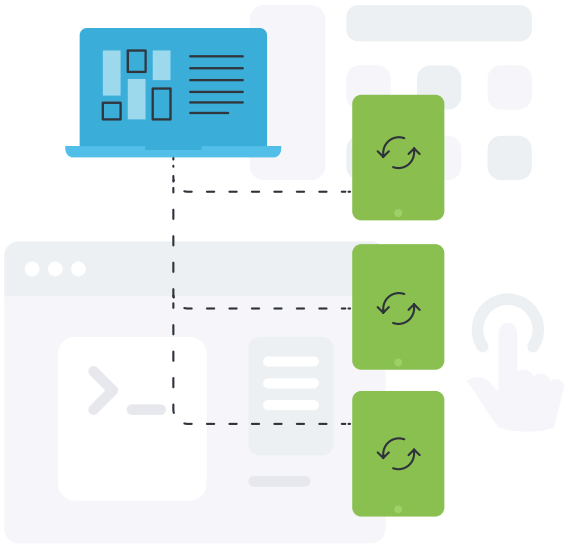
Security Technical Implementation Guides (STIGs) der Defense Information Systems Agency (DISA): Als Konfigurationsstandard, der vom US-Verteidigungsministerium (DoD) verwaltet wird, enthalten die STIGs spezifische Anforderungen für die Absicherung von Computersystemen - von logischen Designs über Protokolle, die auf Hardware-Appliances laufen, bis hin zu der Software, die darauf ausgeführt wird, zielen diese Leitfäden darauf ab, „die Sicherheit für Software, Hardware, physische und logische Architekturen zu verbessern, um Schwachstellen weiter zu reduzieren."

Federal Information Processing Standards (FIPS) 200: Diese Standards wurden ebenfalls vom NIST für die USA entwickelt und gelten für nicht-militärische Computergeräte und -systeme, die von der amerikanischen Regierung und Auftragnehmern verwendet werden. Während die FIPS-Standards eine Reihe von Sicherheitsgrundlagen abdecken, bietet FIPS 200 Standards, die sicherstellen, dass Daten, die von oder im Namen von Bundesbehörden verwendet werden, die Mindestanforderungen an die Informationssicherheit für jede Kategorie in den Zielen erfüllen, wobei das angemessene Niveau der Informationssicherheit entsprechend einer Reihe von Risikostufen gewährleistet wird, während die Auswirkungsstufen für die **Sicherheitsziele auf der Grundlage der CIA -Triade klassifiziert werden.**

NIST SP 800-39: Breit angelegte Leitlinien, die bei der Integration in eine umfassende Enterprise Risk Management (ERM)-Lösung nützlich sind. Das Dokument enthält spezifische Einzelheiten zur Bewertung, Reaktion und laufenden Überwachung von Risiken in Verbindung mit anderen Standards, Leitlinien und Frameworks.

Zentrum für Internet-Sicherheit (CIS): Die CIS-Benchmarks sind präskriptive Konfigurationsempfehlungen für mehr als 25 Produktfamilien von Anbieter*innen. Alle Benchmarks, die im Rahmen einer konsensbasierten Anstrengung globaler Cybersicherheitsexpert*innen entwickelt wurden, bieten sichere Konfigurationsleitfäden, die von Regierungen und Unternehmen weltweit akzeptiert und verwendet werden - und sogar als grundlegende Basis in einige Endpoint-Sicherheitslösungen integriert sind.

Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs): Diese CPGs wurden in Zusammenarbeit mit der CISA, dem NIST und der behördenübergreifenden Gemeinschaft entwickelt und dienen als breit angelegte Basisziele für die Cybersicherheitsleistung, die in allen Sektoren kritischer Infrastrukturen einheitlich sind... Sie helfen insbesondere kleinen und mittleren Organisationen, ihre Cybersicherheitsbemühungen in Gang zu bringen, und dienen gleichzeitig als Maßstab für die Messung und Verbesserung der Cybersicherheits -Reife.



Risikobewertung + kontinuierliche Überwachung + Sicherheitsrichtlinien = Compliance verwaltet.

> *„Erkenne dich selbst und du wirst alle Schlachten gewinnen“* **- Sun Tzu**

Jede dieser Komponenten für sich genommen kann Organisationen nur in gewissem Umfang dienen, aber wenn man sie zusammenfügt, ist man nicht nur dazu in der Lage:

- Bestimmen Sie Ihre Verbindlichkeiten
- Kenntnis des Gesundheitszustands der Endpoints
- Minimierung der Angriffsfläche durch Härtung der Einstellungen
- Erreichen Sie Ihre Compliance-Ziele

Sie können aber auch die Compliance aufrechterhalten, indem Sie Grundlinien festlegen und diese dann durch proaktive Überwachung und die erneute Auswertung umfangreicher Telemetriedaten überprüfen, um den Kreislauf zur kontinuierlichen Verbesserung der Sicherheitslage Ihrer Geräte und Ihrer gesamten Infrastruktur zu schließen.

Wie bereits erwähnt, handelt es sich um einen iterativen Prozess - nicht um einen statischen. Die oben erwähnte Schleife schließt sich nicht, sobald sie erreicht ist. Dennoch wird der Zyklus fortgesetzt und berührt und informiert jede Phase, jede Sicherheitskontrolle, jeden Prozess, jeden Arbeitsablauf, jede Anforderung, jede Richtlinie und jede Einstellung, die für jedes Gerät, jeden Endbenutzer/jede Endbenutzerin und jeden sensiblen Teil der Daten in Ihrem Unternehmen konfiguriert wird.

Unabhängig davon, ob Ihr Unternehmen in einer regulierten Branche tätig ist oder ob es sich um ein Unternehmen beliebiger Größe handelt, das zwar nicht reguliert ist, aber dennoch seine Cybersicherheitsstrategie an Unternehmensrichtlinien und Verwaltungskontrollen - wie z. B. Acceptable Use Policies (AUPs) - ausrichten möchte, betrachten Sie die einzelnen Kernkomponenten als Rädchen im Getriebe, die sich zusammenfügen, um ein besseres Verständnis für Ihre Sicherheitsanforderungen und die zur Schließung der Lücken erforderlichen Informationen zu erhalten.

Sie denken jetzt vielleicht: „Ich bin MacAdmin. Ich weiß, welche Risiken in meinem Unternehmen bestehen, und ich ertrinke in den Gesundheitsdaten der Geräte. Darüber hinaus verdeutlicht dieser Leitfaden die Diskrepanzen zwischen dem derzeitigen Stand und dem, was wir erreichen müssen, um die Compliance einzuhalten. Was nun?! Wie kommen wir von hier nach dort?“

Jamf eingeben

Wir helfen Unternehmen dabei, mit Apple erfolgreich zu sein.

Diese Worte sind mehr als nur eine einprägsame Phrase, sie stehen für das Leitbild von Jamf. Und was noch wichtiger ist: Es ist einfach das, was wir tun. Jamf ist nicht der Goldstandard für Apple am Arbeitsplatz, nur weil wir das sagen. Jamf verdankt seinen guten Ruf den erstklassigen Lösungen, die wir entwickeln und mit denen unzählige Unternehmen in allen Branchen weltweit Millionen von Geräten erfolgreich verwalten und schützen.

Es ist die Unterstützung, die wir anbieten, um sicherzustellen, dass Sie Ihr Potenzial mit Apple Produkten bei der Arbeit voll ausschöpfen können. Sie fragen sich, wie wir Ihnen die Werkzeuge für ein umfassendes und ganzheitliche Verwaltung Ihrer Apple Flotte zur Verfügung stellen und gleichzeitig Ihre individuellen organisatorischen Anforderungen und Compliance-Ziele erkennen, verstehen und erfüllen können?

Ersparen Sie sich das Rätselraten bei der Endpointvalidierung.

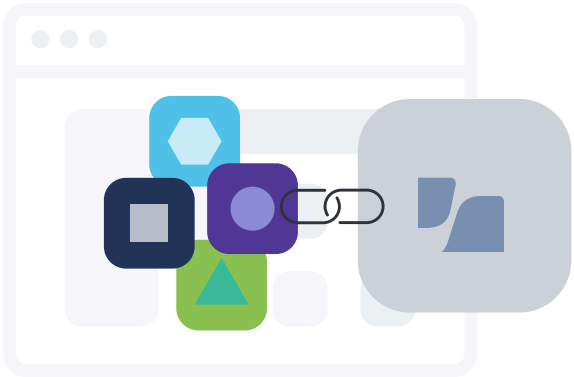
Ein wesentlicher Teil des Verständnisses Ihrer Sicherheitsanforderungen besteht darin, den Status der in Ihrem Unternehmen verwendeten Endpoints zu kennen. Ohne die umfangreichen Telemetriedaten, mit denen der Gesundheitszustand der einzelnen Geräte überprüft werden kann, können Administratoren nur mit Vermutungen arbeiten, die im besten Fall zu Vermutungen und im schlimmsten Fall zu Fehlkalkulationen führen können, die katastrophale Folgen haben können.

Als Administrator*innen **wollen Sie es nicht nur wissen, sondern Sie müssen es wissen.** Und wenn es um die Einhaltung von Compliance geht - sei es bei der Durchsetzung von Vorschriften oder bei der Anpassung an Unternehmensrichtlinien - müssen Sie auch jederzeit den Gesundheitszustand der Endpoints überprüfen, um sicherzustellen, dass die Anforderungen des Unternehmens bei jedem Schritt erfüllt werden.

Social Engineering ist ein wichtiger Angriffsvektor, der von Bedrohungsakteur*innen genutzt wird, um Ihr Risiko auszunutzen. Genauer gesagt, Social Engineering nutzt das bestehende Risiko eines Unternehmens aus und erhöht das Risiko, indem es Anmeldedaten kompromittiert oder bösartigen Code weitergibt, wenn infizierte Geräte eine Verbindung zu Unternehmensressourcen herstellen.

Technologien wie **Zero Trust Network Access** (ZTNA) sorgen für den Schutz Ihrer Geräte, indem sie den Zustand der Endpoints anhand einer Reihe von Anforderungen überprüfen, um sicherzustellen, dass die Geräte ein Mindestmaß an Sicherheit erfüllen, bevor der Zugriff auf angeforderte Ressourcen gewährt wird. Gemäß dem Credo „Niemals vertrauen, immer prüfen“ verifiziert eine ZTNA-Lösung wie **Jamf Connect**, dass der Zugriff von einem registrierten und vertrauenswürdigen Gerät ausgeht, wodurch das Identitäts- und Zugriffsverwaltung zu einem Eckpfeiler Ihrer Sicherheitsstrategie wird.

Endpoint-Sicherheitslösungen wie **Jamf Protect** fügen Ihren macOS, iOS, iPadOS, Android und Windows Geräten ein Sicherheitsnetz hinzu, um sicherzustellen, dass sie (und die Benutzer*innen, die sich auf sie verlassen, um produktiv zu bleiben) gegen mutmaßliche Bedrohungen wie die Verhinderung von Malware und mehr geschützt sind. Dies geschieht durch die Analyse von Bedrohungen auf dem Gerät und im Netzwerk, um eine schnellere Erkennung, eine schnellere Reaktion auf Zwischenfälle und effektive, automatisierte **Workflows zur Bedrohungsabwehr und -beseitigung zu ermöglichen, die die Sicherheit, den Datenschutz und die Leistung nicht beeinträchtigen.**



Verbreiten Sie Liebe und Vertrauen in Ihrer Infrastruktur.

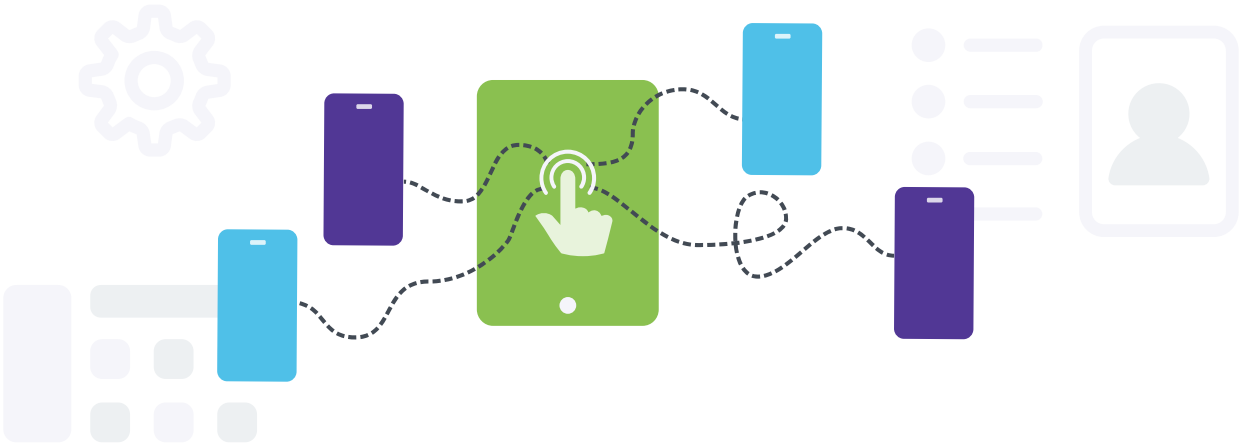
Ihre Anforderungen beginnen nicht erst, wenn ein Gerät zum ersten Mal eine Verbindung zu den Unternehmensressourcen herstellt - sie beginnen schon, bevor das Gerät ausgepackt wird. Lassen Sie uns das erklären.

Die Zero-Touch-Bereitstellung bezieht sich auf einen Prozess, bei dem die **Geräte in dem Moment einsatzbereit sind, in dem der Endbenutzer/die Endbenutzerin sein/ihr Gerät** zum ersten Mal einschaltet. Dieser Arbeitsablauf integriert automatisch und sicher den Apple Business Manager oder Apple School Manager mit Jamf.

Unabhängig davon, ob es sich um firmeneigene Geräte oder persönliche Geräte von Endbenutzer*innen handelt, unterstützt **Jamf Pro** verschiedene Eigentumsmodelle, wie Bring your own device (BYOD) oder vom Benutzer/von der Benutzerin registrierte Geräte, und gewährleistet so die Sicherheit bei gleichzeitiger Wahrung der Privatsphäre der Benutzer*innen. Apropos Sicherheit: Unsere MDM-Lösung bietet Administrator*innen **taggleiche Unterstützung für alle Apple Funktionen, einschließlich Sicherheits- und Datenschutzverbesserungen**, sodass Sie die Funktionen unterstützen und verwalten können, die Benutzer*innen helfen, intelligenter und nicht härter zu arbeiten, ohne Kompromisse oder Ausnahmen bei der Endpoint-Sicherheit einzugehen.

Die Appverwaltung ist ein wichtiger Bestandteil Ihrer Sicherheitsanforderungen. Die Bereitstellung von Aktualisierungen für Betriebssysteme und Apps ist eine Grundvoraussetzung für den Erfolg eines jeden Sicherheitsplans. Denn was nützt es Ihnen, Ihre Sicherheitsbedürfnisse zu verstehen, wenn Sie nichts tun können, um Probleme zu beheben, wenn sie auftreten? Jamf Pro glänzt einmal mehr dadurch, dass es **MacAdmins dabei hilft, die Verwaltung des App-Lebenszyklus** mit Massenverwaltungsbefehlen zu vereinfachen, um Geräte mit Aktualisierungen des Betriebssystems auf dem neuesten Stand zu halten. Und vergessen Sie nicht die Apps! Der **Self-Service-App-Katalog** von Jamf stellt zusammen mit der Leistungsfähigkeit der App-Installer sicher, dass die von Ihren Endbenutzer*innen benötigten Apps leicht zugänglich sind, immer verwaltet werden, automatisch auf die neuesten Versionen aktualisiert werden und sich in ihrem sichersten Zustand befinden.

Die Rationalisierung der Identitäts- und Zugriffsbereitstellung ist ein zentraler Bestandteil einer umfassenden Sicherheitsstrategie. Die Durchsetzung eines Trusted Access, der sicherstellt, dass nur vertrauenswürdige Benutzer jederzeit und überall auf Geräte und Ressourcen zugreifen können, macht den Unterschied bei der Verwaltung von Geräten aus, insbesondere in verteilten Arbeitsgruppen. So können sich die Benutzer*innen auf einfache Weise bei ihren Geräten authentifizieren - von einem nahtlosen Onboarding-Erlebnis über eine Zero-Touch-Bereitstellung bis hin zur täglichen Arbeit und dem Zugriff auf Unternehmensressourcen. ZTNA und die Zugangskontrolle mit **Jamf Connect** verstärken das Paradigma, dass **effektive, anpassungsfähige und flexible Sicherheit nicht optional ist.**



Drei wesentliche Sicherheitselemente - eine vertrauenswürdige Plattform

> *„Gelegenheiten vermehren sich, wenn sie ergriffen werden.“* **- Sun Tzu**

Trusted Access ist ein ganzheitlicher Sicherheitsansatz , der eine umfassende Lösung bietet, die die Verwaltungs- und Sicherheitsanforderungen jeder Organisation in allen Branchen unterstützt.

Jedes Element von Trusted Access - **Geräteverwaltung**, **Endpoint-Schutz** sowie **Transparenz und Compliance** - ist für eine effektive, umfassende Sicherheitsstrategie entscheidend. Es handelt sich um eine Lösung, die fortschrittliche Zugriffskontrollen und sichere Konfigurationen für Geräte, Benutzer*innen und Daten bietet und gleichzeitig Telemetriedaten nutzt, um sich an alle Änderungen der Sicherheitslage Ihrer Geräte oder Ihres Unternehmens anzupassen, um die Sicherheit zu wahren, den Datenschutz zu schützen und die Compliance zu gewährleisten.

Flexibilität und Sicherheit für Ihre gesamte Apple Flotte, jederzeit und überall, ohne die Komplexität.

Setzen Sie sich mit uns in Verbindung, um zu erfahren, wie Jamf Sie bei der Bewertung Ihrer Sicherheitsanforderungen mit unseren Best-in-Class-Lösungen unterstützen kann.

Los geht's

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

jamf

www.jamf.com/de/

© 2024 Jamf, LLC. Alle Rechte vorbehalten.