jamf

Beveiligings-frameworks begrijpen

Cyberbeveiligingsplannen om risico's te beperken en de onderneming te beschermen tegen bedreigingen minimaliseren potentiële aanvalsvectoren. De impact van een holistische beveiligingsstrategie varieert volledig van organisatie tot organisatie, omdat er rekening wordt gehouden met behoeften die uniek zijn voor elke organisatie. Wat direct verband houdt met de behoeften is de rol die compliance van de regelgeving speelt. En dan hebben we het nog niet eens over de talloze mogelijkheden die slechte actoren in het moderne bedreigingslandschap hebben om de beveiliging van organisaties aan te tasten.

Met al deze variabelen in het spel zou je denken dat het opstellen van een cyberbeveiligingsplan veel moeilijker is dan het lijkt, maar dat hoeft niet zo te zijn.

En dan hebben we het nog niet eens over de rol die ze spelen bij het ontwikkelen van samenhangende strategieën voor het minimaliseren van risicofactoren, het handhaven van compliancedoelstellingen en nog veel meer.

Met betrekking tot de cyberbeveiligingslevenscyclus weerspiegelen de volledige implementatie en het doorlopende beheer van cyberbeveiligingscontroles en -oplossingen direct het succesvolle beheer van informatiebeveiligingsrisico's binnen je organisatie — of het falen daarvan.

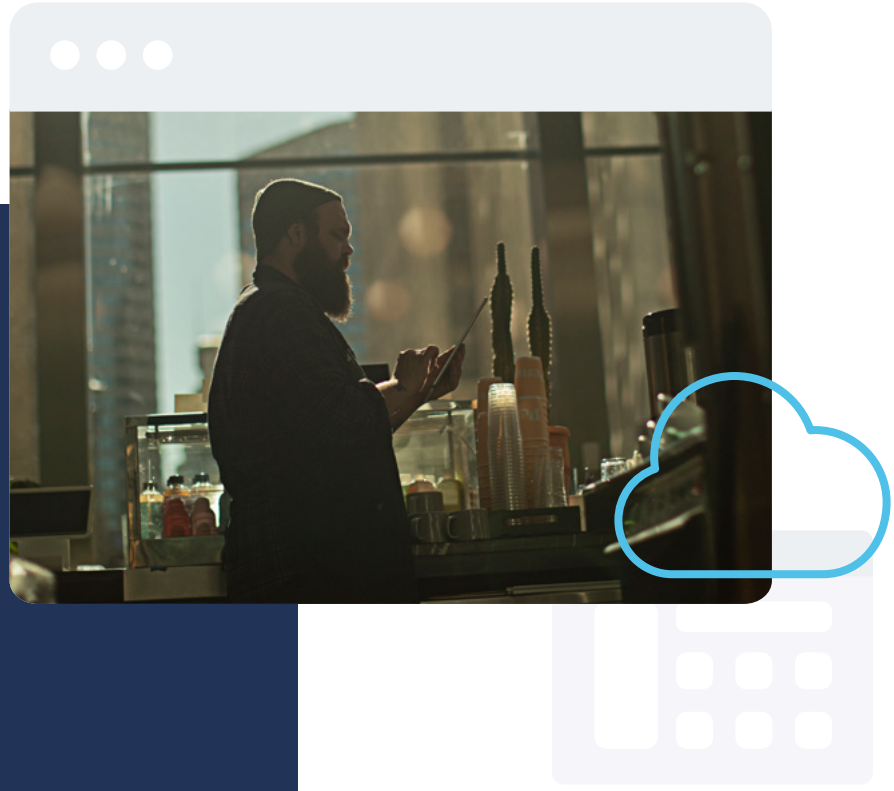
Factoren die van invloed zijn op het succes van cyberbeveiligingsplannen zijn:

- de grootte van je organisatie
- budgettaire beperkingen
- wettelijke vereisten (indien van toepassing)
- eigen behoeften voor de continuïteit van de bedrijfsvoering
- uitgebreide en nauwkeurige risicobeoordelingen
- kennis en vaardigheden van IT- en beveiligingsteams

Hoewel de bovenstaande lijst niet uitputtend is, benadrukt hij de belangrijkste punten die cruciaal zijn voor het succes van elk beveiligingsplan. Zelfs als ze gewapend zijn met deze informatie, kunnen organisaties het moeilijk vinden om aan de slag te gaan, simpelweg omdat er **andere variabelen kunnen zijn waar ze zich niet bewust van zijn** of omdat beperkingen in een van de bovenstaande factoren kunnen leiden tot uitdagingen bij het proberen om de juiste combinatie van hardware, software, configuraties, beleidsregels en workflows in te stellen om te voldoen aan de unieke cyberbeveiligingsbehoeften van je organisatie.

Frameworks pakken deze en vele andere valkuilen aan die mogelijk aanwezig zijn in informatiebeveiligingsstrategieën door organisaties een duidelijke, beknopte routekaart te bieden die ze kunnen volgen bij het opstellen of beheren van hun bestaande cyberbeveiligingsplannen.

WAT ZIJN FRAMEWORKS?



We hebben het woord 'stappenplan' gebruikt om de frameworks hierboven te beschrijven. Een andere, technisch meer accurate uitdrukking zou 'blueprint' zijn. Net zoals een aannemer een blueprint gebruikt om een structureel gezond gebouw te bouwen, kunnen (en moeten) IT- en beveiligingsteams een van de vele verschillende soorten raamwerken gebruiken om een beveiligingsplan op te stellen dat gericht is op:

- identificeren
- beschermen
- detecteren
- antwoorden
- herstellen

De geïmplementeerde kaders moeten samenwerken om de risico's van cyberbeveiliging te beperken door middel van beknopte, georganiseerde en door de sector goedgekeurde beste praktijken en methoden.

SOORTEN FRAMEWORKS

Er zijn verschillende frameworks. Ze richten zich elk op een bepaald onderdeel van informatietechnologie of informatiebeveiliging en versterken dit. Sommige bieden algemene richtlijnen voor het beschermen van je infrastructuur tegen huidige en zich ontwikkelende bedreigingen, en andere geven informatie over het verbeteren van processen die de efficiëntie van IT-beheerservices verhogen. Anderen richten zich daarentegen uitsluitend op het versterken van je beveiligingshouding binnen specifieke beveiligingsscenario's, zoals gereguleerde omgevingen, zoals de gezondheidszorg, de financiële sector of het onderwijs.

GEMEENSCHAPPELIJKE FRAMEWROKS EN REGELGEVING VOOR CYBERBEVEILIGING

FRAMEWORKS

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1: NIST valt onder de jurisdictie van het Amerikaanse ministerie van Handel en heeft als missie het bevorderen van het industriële concurrentievermogen, welke programma's zich uitstrekken tot verschillende laboratoria, waaronder informatietechnologie en beveiliging. Het CSF vertegenwoordigt een voortdurende samenwerking tussen het bedrijfsleven, de academische wereld en de overheid om kritieke cyberbeveiligingsinfrastructuren te verbeteren waarvan de exploitatie financiële en reputatierisico's met zich meebrengt.

NIST Special Publication (SP) 800-53, Rev. 5: Pakt beveiligings- en privacyrisico's aan door een catalogus met beveiligings- en privacycontroles voor informatiesystemen en organisaties te bieden tegen een uiteenlopende reeks bedreigingen en risico's, inclusief maar niet beperkt tot misconfiguratie, slechte actoren en menselijke fouten. De controles zijn flexibel en aanpasbaar en helpen organisaties om risico's te beperken en tegelijkertijd de functionaliteit en zekerheid van computersystemen te verbeteren.

ISO/IEC 27001: Deze norm definieert eisen waaraan beheersystemen voor informatiebeveiliging (ISMS) moeten voldoen en biedt richtlijnen voor het opzetten, implementeren, onderhouden en continu verbeteren van een beheersysteem voor informatiebeveiliging. Het respecteert best practices en principes binnen een internationaal geaccepteerde standaard die van toepassing is op bedrijven van alle groottes en sectoren.

MITRE ATT&CK: Dit is een wereldwijde kennisbank van tactieken die worden gebruikt door cyberaanvallers, gebaseerd op waarnemingen van technieken uit de echte wereld. Het is een basis voor het ontwikkelen van specifieke bedreigingsmodellen en methodologieën voor verschillende sectoren, gemeenschappen en eindpuntbeveiligingsoplossingen.

FRAMEWORKS

System and Organization Controls (SOC) van het American Institute of Certified Public Accounts (AICPA): Een reeks rapporten die drie soorten rapporten omvat, getiteld: SOC 1, SOC 2 en SOC 3, en gedetailleerde informatie en zekerheid verschaft over de controles bij een serviceorganisatie die relevant zijn voor de beveiliging, beschikbaarheid en verwerkingsintegriteit van de systemen die worden gebruikt voor de verwerking van gevoelige gegevens, terwijl een gevalideerde zekerheid wordt verschaft over de controles door de gebruikers van die diensten.

Center for Internet Security (CIS): De CIS Benchmarks zijn normatieve configuratieaanbevelingen voor meer dan 25 productfamilies van leveranciers. Elke benchmark biedt veilige configuratiegidsen die zijn ontwikkeld als onderdeel van een op consensus gebaseerde inspanning van wereldwijde deskundigen op het gebied van cyberbeveiliging en die worden geaccepteerd en gebruikt door overheden en industrieën over de hele wereld en die de basis vormen van sommige oplossingen voor de beveiliging van eindpunten.

macOS Security Compliance Project (mSCP): Samen met de federale operationele IT-beveiligingsmedewerkers van NIST, National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA) en Los Alamos National Laboratory (LANL) is dit project een open-source-inspanning om een programmatische aanpak te bieden voor het genereren van beveiligingsrichtlijnen, inclusief configuratie-instellingen die worden ingezet om compliance van specifieke regelgevingsdoelen te bereiken, specifiek voor het beveiligen van en compliance van Apple macOS.

VOORSCHRIFTEN

Healthcare Insurance Portability and Accountability Act (HIPAA): Moderniseert de informatiestroom in de gezondheidszorg en bevat vereisten voor het omgaan met beschermde gezondheidsinformatie (PHI), waaronder beperkingen op de openbaarmaking van gezondheidsgegevens van patiënten en de gevolgen van het overtreden van de wet.

Sarbanes-Oxley Act van 2002 (SOX): Deze federale wet verplicht organisaties in de financiële sector tot het bijhouden en rapporteren van financiële gegevens.

Richtlijn over de beveiliging van netwerk- en informatiesystemen (NIS): Een EU-mandaat van het Agentschap voor Cyberbeveiliging van de Europese Unie (ENISA) verplicht lidstaten om regelgeving op te nemen in hun respectieve nationale wetten om het niveau van bescherming van cyberbeveiliging te verhogen, dat zich uitstrekt van het melden van beveiligingsincidenten tot de manier waarop responsteams ermee omgaan.

Algemene Verordening Gegevensbescherming (AVG): Deze privacygerichte beveiligingswet is ontwikkeld voor Europa, maar heeft invloed op alle organisaties die gegevens van EU-burgers verwerken. De compliancerichtlijnen hebben betrekking op alle aspecten van de privacy van gebruikers, waaronder procedures voor het verwerken van cookies, ePrivacy en het "recht om vergeten te worden" van gebruikers.

Family Educational Rights and Privacy Act (FERPA): Deze Amerikaanse federale wet beschermt de privacy van studenten en de gegevens in onderwijsdossiers, inclusief toegang tot deze gegevens en het recht om eventuele onjuiste gegevens te wijzigen. Voor minderjarigen geldt dit recht ook voor de ouder of voogd, maar wanneer de student meerderjarig wordt (18 jaar in de VS) of naar een instelling voor hoger onderwijs gaat, gaan deze rechten alleen over op de ouder of voogd.

ZO GEBRUIK JE FRAMEWORKS ALS ONDERDEEL VAN EEN UITGE-BREIDE BEVEILI-GINGSSTRATEGIE

Het implementeren van kaders om je beveiliging te versterken door sleutelfactoren aan te pakken op basis van best practices en gedegen methodologieën hoeft geen zware klus te zijn. Dat zou kunnen, maar als je het goed aanpakt, kan het deel uitmaken van je beveiligingsplan en naadloos integreren met je beveiligingstools om compliance af te dwingen via veilige processen en workflows.

Er is de 'ouderwetse' methode om frameworks op te nemen in je bestaande beheerstrategie, waarbij je handmatig een recente beoordeling van je beveiligingsstatus vergelijkt met een lijst van een van de hierboven genoemde frameworks, waarbij je bijvoorbeeld punt voor punt de lijst afloopt om vast te stellen welke configuraties, instellingen, protocollen, processen, workflows en beleidsregels niet voldoen aan de compliancevereisten. En dat is nog maar het eerste deel van het handmatige proces. Het tweede deel bestaat uit het handmatig corrigeren van alle onderdelen die buiten dhet bereik vallen om ze aan de eisen te laten voldoen.

Omdat beveiliging voortdurend verandert, is dit ook geen 'one-and-done' proces. Het moet regelmatig worden uitgevoerd om te controleren of endpoints beveiligd zijn en om ervoor te zorgen dat ze compliant blijven.

Uitdagingen die de frequentie, nauwkeurigheid en het succes van het handmatig aanpassen van raamwerken in je cyberbeveiligingsplan aanzienlijk beïnvloeden, zijn de volgende:

- aantal en typen apparaten in je vloot
- grootte en vaardigheden van je IT- en beveiligingsteams
- middelen , zoals tijd en geld, die worden toegewezen aan het uitvoeren van dit proces
- mate van ondersteuning door leiderschap
- voorschriften voor bedrijfscontinuïteit
- gevolgen voor gebruikersproductiviteit, uitvaltijd en blokkades
- bestaande beveiligingstools en hun mogelijkheden

Nu we het handmatige proces uit de weg hebben, gaan we over op wat beheerders echt willen: een geautomatiseerde manier om frameworks in hun cyberbeveiligingsplan te implementeren. Eén die geen extra werk oplevert voor de toch al overbelaste IT- en beveiligingsteams, maar juist helpt:

- Los beveiligingsproblemen snel en efficiënt op
- Integreer naadloos met best-of-breed beheertools
- Voeg geavanceerde workflows en op beleid gebaseerd beheer toe om risicobeperkingen te automatiseren
- Gebruik teams van alle groottes door beveiligingstools te gebruiken om het zware werk uit te voeren
- Vermijd administratieve overhead, zodat de tijd beter aan andere taken kan worden besteed
- Bewaakeindpunten voortdurend, zodat je in realtime inzicht hebt in de gezondheid van apparaten
- Met cloud-gebaseerde oplossingen kunnen apparaten altijd en overal worden gemitigeerd

  Automatiseer het lopende proces door dynamische aanpassing aan veranderingen in de beveiligingsstatus om compliance van frameworks en veranderende beveiligingsbehoeften af te dwingen

Eén manier om de implementatie van beveiligingsframeworks te automatiseren is door eindpuntbeveiligingsoplossingen te gebruiken die de frameworks die je organisatie nodig heeft al in de tools hebben opgenomen. Het bovengenoemde MITRE ATT&CK framework kan bijvoorbeeld als basiscomponent worden gevonden in bepaalde eindpuntbeveiligingsoplossingen. Door dit te doen, worden gedragsanalytische gegevens gekoppeld aan bekende bedreigingen in de MITRE ATT&CK-database voor vereenvoudigde detectie, en ingebouwde risicobeperkende workflows herstellen risico's als onderdeel van het doorlopende bewakingsproces.

Een andere, meer holistische manier om compliance te automatiseren via beveiligingsframeworks is door gebruik te maken van je Mobile Device Management (MDM)-oplossing en het mSCP-framework om de bestanden te genereren die nodig zijn om compliance te bereiken en deze te uploaden naar je MDM-oplossing om compliance te automatiseren en af te dwingen.

VOORBEELD

Door mSCP te gebruiken om een aangepaste baseline te bouwen met het NIST SP 800-53r5 framework als basis om HIPAA-compliance te bereiken met endpoints die zijn ingeschreven in je MDM, kan een organisatie een baseline bouwen die voldoet aan de HIPAA-vereisten. Hun volgende stap is om mSCP te gebruiken om aangepaste bestanden te genereren:

- **Configuratieprofielen:** Biedt configuratie van beheerde instellingen aangepast aan je organisatorische behoeften.
- **Compliancescripts:** Twee scripts - één om beheerde apparaten te controleren op beveiligingsbehoeften en het tweede om de nodige herstelwerkzaamheden uit te voeren om het gewenste niveau van compliance te bereiken.
- **PLIST-bestanden:** Deze worden gebruikt om de conformiteit te controleren en auditresultaten vast te leggen.
- **Spreadsheet documenten:** Handig om te overhandigen aan auditors en externe onderzoekers bij het bepalen van complianceniveaus.
- **Rapportdocumenten:** Rapporten in HTML- en PDF-formaat die een overzicht geven van elke instelling die wordt gecontroleerd als onderdeel van het voldoen aan compliance, inclusief informatie over wat wordt gecontroleerd, wat conforme instellingen zouden moeten zijn en hoe deze kunnen worden hersteld.

Met deze bestanden in de hand kunnen beheerders alle aangepaste configuratieprofielen uploaden (die nog niet bestaan binnen MDM) om uit te rollen in hun vloot. Het uploaden van de compliancescripts is echter waar de spreekwoordelijke magie gebeurt. Als het controlescript zo is geconfigureerd dat het volgens jouw tijdschema wordt uitgevoerd, bijvoorbeeld eenmaal per dag, wordt het script dagelijks op elk beheerd apparaat uitgevoerd en wordt de apparaatrecord in de MDM bijgewerkt met nieuwe voorrraadgegevens. Dit automatiseert het verzamelen van telemetriegegevens om te weten of het apparaat voldoet aan de HIPAA-richtlijnen. Vervolgens wordt het saneringsscript geüpload en ingesteld om te worden uitgevoerd als onderdeel van een beleid. Door dit te doen, kunnen beheerders de omvang van de sanering beperken zodat deze automatisch plaatsvindt op alleen de apparaten die niet aan de regels voldoen. Zodra het saneringsscript is voltooid, zal het een inventarisatie van het/de apparaat(en) starten om de apparaatrecords bij te werken en hun conformiteitsstatus binnen MDM weer te geven.

Het automatiseren van compliance door frameworks te integreren via je MDM-oplossing zorgt voor de veilige configuratie van apparaten om compliancedoelen te bereiken, terwijl cloudgebaseerde beheertools worden ingezet om de beveiliging en privacy van je eindpunten af te dwingen. Als een apparaat buiten het bereik valt, identificeren de geautomatiseerde scripts welke instelling(en) werden beïnvloed en herstellen ze het probleem/de problemen - op elk moment, op elke locatie en via elke netwerkverbinding - zonder dat IT- of beveiligingsteams het apparaat fysiek hoeven te hanteren. Door je MDM- en eindpuntbeveiligingsoplossingen te integreren via een beveiligde API-verbinding kun je constante zichtbaarheid en bewaking delen. Het ondersteunt het maken van geavanceerde workflows die een snellere respons op incidenten bieden, inclusief Security Orchestration, Automation and Response-achtige (SOAR) technologie, om de coördinatie van uitvoerings- en hersteltaken te automatiseren.

WAT BEVEILIGINGSFRAMEWORKS WEL EN NIET KUNNEN DOEN

Frameworks zijn uitstekend om een groot aantal problemen aan te pakken. We hebben besproken wat frameworks zijn (en niet zijn.) Vervolgens nemen we even de tijd om te bespreken wat ze wel en niet kunnen doen.

Kunnen

- Compliancevereisten structureren in georganiseerde sets van categorieën
- Mitigatiegegevens formatteren met ondersteuning voor best practices en methodologieën uit de sector
- Alseen blueprint fungeren voor organisaties om te volgen op hun compliancepad
- Een solide basis bieden voor het opzetten van een uitgebreid cyberbeveiligingsprogramma

Niet kunnen

- Organisaties beschermen tegen risico's of aansprakelijkheden die voortvloeien uit gemitigeerde of niet-mitigeerde risico's
- >Vrijwillig zijn, wat betekent dat er geen mandaat is om het geheel of gedeeltelijk te implementeren
- Expliciet voorschrijven dat men zich aan de oplossing moet houden. Veel op compliance gebaseerde frameworks, zoals HIPAA, zijn niet-prescriptief, wat betekent dat ze niet expliciet zijn in hun vereisten over hoe je compliance het best implementeert
- Zelf zorgen voor bescherming. Ze bieden alleen richtlijnen over hoe een uitgebreid beveiligingsplan eruit moet zien
- De tijdsduur tussen updates beperken. Hierdoor kan bepaalde informatie in het beste geval achterhaald zijn en in het slechtste geval volledig onrealistisch als je kijkt naar de moderne bedreigingslandschappen.
- Worden opgenomen naast beveiligingscontroles, aangezien ze ontoereikend zijn voor beveiliging of compliance buiten een defense-in-depth plan
- Voor een consistente staat van compliance zorgen. Er bestaan geen kant-en-klare oplossingen op het gebied van beveiliging en dat geldt ook voor frameworks. Dat je organisatie nu compliant is, betekent niet dat compliance morgen gegarandeerd is.

DE WAARDE VAN APPLE'S EIGEN BEVEILIGINGS-FRAMEWORKS

Voor sommigen is het niet bekend dat Apple een unieke set beveiligingsframeworks ontwikkelt — Apple Platform Security — die elk besturingssysteem ondersteunt en samenwerkt met andere privacygerichte frameworks om de hele Apple productlijn te beschermen.

Ze gaan van hardware tot software, inclusief de manier waarop fysieke en gegevensbeveiliging wordt verwerkt, behandeld, opgeslagen, verzonden en gebruikt door gebruikers op Apple apparaten. En wat privacy betreft, heeft Apple het App Tracking Transparency framework ontwikkeld, dat controleert hoe apps gegevens over eindgebruikers verzamelen en delen om te beperken wat is toegestaan en te beperken wat niet is toegestaan om het recht op privacy van hun gebruikers te beschermen.

Apple heeft het voortouw genomen op het gebied van beveiliging en privacy door deze frameworks te ontwerpen, in te bouwen als onderdeel van hun OS-versies en regelmatig bij te werken om gelijke tred te houden met veranderende bedreigingen die anders de informatiebeveiliging en de privacy van gebruikers in gevaar zouden brengen.

WAAR KOMT JAMF IN BEELD?

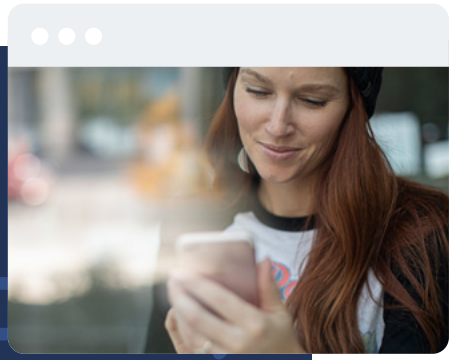
Je weet hoe belangrijk Apple beveiliging en privacy vindt. Maar wist je dat Jamf oplossingen een soort IT- en beveiligingsteam zijn voor jouw IT- en beveiligingsteams?

Nou, dat zijn we. Met onze lange geschiedenis in het ondersteunen van Apple in het bedrijfsleven, biedt Jamf de oplossingen die organisaties helpen succesvol te zijn met Apple. Of het nu op het werk, op school of tijdens het spelen is, Jamf verbetert de native frameworks die door Apple zijn ontwikkeld door inzicht te bieden in deze frameworks, waardoor beveiligingsprofessionals antwoord krijgen op de vragen die ze zouden moeten stellen over hun Apple producten:

- Hoe zijn ze geconfigureerd?
- Wanneer worden ze gebruikt?
- Waarom is deze bron gebruikt?
- Wie heeft er toegang toe?
- Worden apparaten veilig gebruikt?
- Wat kan ze verder beveiligen?
- Hoe kan compiance worden gemeten?
- Wat is er nodig om compliance af te dwingen?

Maar dat is nog niet alles.

JAMF HELPT JE DE THEORIE IN PRAKTIJK TE BRENGEN



Frameworks alleen versterken de beveiliging niet. Uitgebreide telemetriegegevens kunnen inzicht geven in de gezondheid van eindpunten om de compliancestatus te bepalen, maar die gegevens moeten bruikbaar zijn om risico's te beperken en compliance af te dwingen.

Onze MDM-oplossing Jamf Pro is niet alleen de gouden standaard voor het beheer van Apple apparaten omdat wij dat zeggen, maar ook omdat miljoenen beheerde apparaten wereldwijd en in alle sectoren dat zeggen. Jamf helpt organisaties van elke omvang om de baseline van het framework te gebruiken en, in combinatie met hun risicobeoordelingsgegevens om de behoeften op het gebied van gegevensbeveiliging en compliance te bepalen. Deze gegevens worden vervolgens in Jamf Pro opgenomen om apparaatconfiguraties te beheren, het aanvalsoppervlak te minimaliseren door apparaten te harden en beleidsregels in te zetten om hen te helpen niet alleen compliance te bereiken, maar deze ook af te dwingen.

Door een combinatie van geautomatiseerde workflows die worden aangestuurd door Jamf Protect, de beste eindpuntbeveiligingsoplossing die speciaal is gebouwd voor Apple, kunnen IT- en beveiligingsteams snel werk maken van beveiliging en compliance.

Eindpuntbeveiliging met Jamf bevat ondersteuning voor CIS Baselines, wat betekent — of je organisatie nu net begint met het nemen van een duik in de wateren van beveiliging en compliance of je team bestaat uit ervaren professionals — Jamf helpt organisaties om hun infrastructuur snel en vanaf de basis te beveiligen. Stel dat je klaar bent om compliance en beveiliging een stap verder te brengen. In dat geval kun je werken met aanvullende beveiligingsframeworks, zoals MITRE ATT&CK of voldoen aan complexere compliance-vereisten met ondersteuning voor onder andere NIST- en mSCP-frameworks.

Jamf oplossingen op Apple apparaten zorgen ervoor dat IT- en beveiligingsteams zich kunnen richten op het ondersteunen van bedrijfsinitiatieven en het bieden van eersteklas ondersteuning, terwijl ze er tegelijkertijd voor zorgen dat de veranderende beveiligings- en compliancebehoeften van de organisatie worden begrepen, aangepakt en efficiënt en effectief worden verholpen.

Kijk zelf hoe het werkt met een gratis proefversie of neem contact op met je favoriete reseller.

Aan de slag