Apple apparaat beveiliging

VOOR BEGINNERS

jamf

Een goed geplande cyberaanval of het per ongeluk downloaden van malware kan het verschil betekenen tussen een productieve dag en het stilleggen van alle werkzaamheden. Nu hackers steeds geraffineerder worden, moeten organisaties die zich zorgen maken over hun resultaten en de beveiliging van de gegevens van hun gebruikers, zoals klanten, werknemers of leerlingen, bovenop de beveiliging blijven zitten.

Bezorgdheid over de beveiliging van Apple is, net als alle andere zorgen over IT-beveiliging, heel reëel en vormt een kritieke bedreiging voor de resources van de organisatie en de veiligheid van belanghebbenden.

Apple maakt ongelooflijk veilige besturingssystemen; het lijdt geen twijfel dat de focus op de beveiligings- en privacybescherming die in de hardware en software is ingebakken een belangrijke rol heeft gespeeld bij de stijging in populariteit en massale adoptie binnen bedrijven, onderwijsinstellingen en andere industriële organisaties. En omdat Apple het favoriete platform blijft voor persoonlijke en professionele hardware, is het een aantrekkelijker doelwit geworden voor aanvallers. Dit betekent dat beheerders snel moeten reageren op beveiligingsincidenten zodra deze zich voordoen en niet moeten wachten tot een probleem zich voordoet. In plaats daarvan kunnen Mac-beheerders en beveiligingsteams (en de belanghebbenden die zij ondersteunen) zich beter proactief hiertegen wapenen voordat bedreigingen kunnen uitgroeien tot iets veel ergers. Ze kunnen gebruikmaken van oplossingen die op maat zijn gemaakt of speciaal zijn gebouwd voor Apple om op Apple gerichte bedreigingen effectief te beschermen.

Deze gids is bedoeld voor beheerders en managers die serieus werk willen maken van de organisatorische beveiliging van hun Apple apparaten en biedt basisinformatie voor nieuwkomers of zelfs een eenvoudige opfrisser voor Apple beheerveteranen.

Inleiding tot Apple beveiliging

Verschillende factoren werken samen om de beveiliging van de hardware en gegevens van je organisatie te garanderen:

1. **Apple ingebouwde beveiliging:** beveiligingssystemen die al op zijn ingebouwd in macOS, iOS, iPadOS en tvOS
2. **Aangemelde apparaten:** apparaten aanmelden en inzetten met veilig, gecentraliseerd beheer en overzicht
3. **Apparaten beveiligen:** je fysieke apparaten beschermen en je gebruikers beschermen tegen bedreigingen
4. **Gegevensversleuteling:** gegevens in rust en in transit, op het apparaat en in het netwerk te allen tijde beveiligen
5. **Controle op compliance:** apparaten monitoren om de gezondheidsstatus te bepalen en basisregels af te dwingen
6. **Applicatiebeveiliging en patching:** up-to-date blijven met besturingssysteem-, app- en softwarepatches

1

EERSTE BOUWSTEEN:

Apple native beveiliging

Apple apparaten zijn de best beveiligde out-of-the-box hardwareopties op de markt en speciaal ontwikkelde beheer- en beveiligingsoplossingen breiden de kracht van Apple uit.

De beveiligingsfuncties die al zijn ingebouwd in macOS (het besturingssysteem voor Mac), iOS (het besturingssysteem voor iPad en iPhone) en tvOS (het besturingssysteem voor Apple TV) zijn uitgebreid en hebben verschillende voordelen:

- **de besturingssystemen van Apple zijn gebaseerd op de UNIX-onderbouw. Dit zorgt voor een rijke basis voor computergebruik van een volwassen, goed onderzocht platform met diepgewortelde ontwikkeling voor rotsvaste stabiliteit.**
- **Sterk OS-beveiligingsraamwerk:**
  - Notarisatie
  - Gatekeeper
  - Xprotect
  - Malwareverwijderingstool (MRT)
  - Transparantie, toestemming en controle (TCC)
  - Snelle beveiligingsmaatregelen
  - Isolatiemodus
- **Fysieke apparaatbeveiliging in de vorm van vergrendeling en het traceren van zoekgeraakte apparaten met de Zoek mijn-service**
- **Het vermogen om beveiligingscontroles te implementeren en te configureren met behulp van configuratieopties via mobielapparaatbeheer (MDM)**
  - Veilige registratiemodi zijn ingebouwd in Apple apparaten, zoals geautomatiseerde apparaatinschrijving en inschrijving op initiatief van de gebruiker voor apparaten in bedrijfseigendom en/of persoonlijk eigendom om te voldoen aan alle behoeften op het gebied van eigendomsmodellen (zoals BYOD, CYOD en COPE) zonder riskante inschrijvings-URL's of verdachte e-mailuitnodigingen
  - Naadloze integratie met Apple Business Manager of Apple School Manager voor centraal beheer van alle institutionele hardware, inclusief supervisie van apparaten over-the-air en veilige hand-off naar je MDM-oplossing voor apparaatbeheerfuncties, zoals beheerde app-implementatie, veilige apparaatprovisioning en zero-touch onboarding-workflows

Een speciaal ontwikkelde MDM-oplossing kan deze bestaande beveiligingsconfiguraties overnemen, ze afstemmen op je unieke organisatorische behoeften, met inbegrip van benchmarks voor de sector, en ze implementeren (en afdwingen) in je volledige Apple vloot, ongeacht de grootte. Je kunt dus veilig en efficiënt één Mac installeren, net zo gemakkelijk als duizenden Macs. Je krijgt ook uitgebreidere beveiligingscontroles met een MDM-tool waarmee je eenvoudig beheertaken kunt uitvoeren op alle apparaten die je selecteert. Je kunt bijvoorbeeld korte metten maken met terugkerende taken door apparaten die zoek zijn geraakt of uit de voorraad van je faciliteit moeten worden verwijderd, op afstand te vergrendelen en te wissen. Kom meer te weten met ons e-book Apple apparaatbeheer voor beginners.

Details beveiligingsfuncties

Native beveiligingsfuncties voor macOS, iOS, iPadOS en tvOS

macOS	iOS en iPadOS	tvOS
Software-updates	Software-updates	Software-updates
Bescherming van de systeemintegriteit (SIP)	Veilig systeem	App Store
Gatekeeper	App Store	Airplay-instellingen en wachtwoorden
App Store	Biometrische identificatie	Appbeperkingen
FileVault-versleuteling	Hardwareversleuteling	Schermbeveiliging
Supervisie	Supervisie	Supervisie
XProtect en Malware Removal Tool (MRT)	App Sandboxing	
Zoek mijn	Zoek mijn	
Privacy-instellingen	Privacy-instellingen	
Notarisatie en quarantaine van bestanden	Secure Enclave en biometrische identificatie	
API voor eindpuntbeveiliging	Notarisatie	
App Sandboxing		
Secure Enclave en biometrische identificatie		

2

BOUWSTEEN TWEE:

veilig ingeschreven apparaten en implementaties

Zoals bij alle bouwstenen is een solide basis de sleutel tot succes. Dit informeert elke volgende bouwsteen en zet de overkoepelende toon voor het beheer en de beveiliging met betrekking tot de levenscycli van hardware en applicaties.

De eerste stap om op een gestandaardiseerde en efficiënte manier apparaten correct te provisioneren en veilig in te zetten in je hele machinepark is het gebruik van Automated Device Enrollment, dat deel uitmaakt van de gratis diensten die Apple aanbiedt via Apple Business Manager en Apple School Manager.

Met Automated Device Enrollment kun je Apple op de hoogte stellen van alle apparaten die je organisatie bezit, evenals andere eigendomsmodellen die hieronder worden besproken, en ze toewijzen voor beheer door het MDM van je organisatie. Wanneer een apparaat dat in dit programma is geregistreerd, wordt ingeschakeld, wordt het ingeschakeld:

- Automatische aanmelding bij je MDM-instantie
- Schakel Supervisie in, wat een integraal onderdeel is voor strengere beveiligingscontroles
- Sta beheerders toe om configuratieprofielen toe te passen en instellingen te verstevigen
- Zorg ervoor dat kritieke beveiligingsinstellingen en payloads worden geïmplementeerd voordat de gebruiker een apparaat kan gaan gebruik
- Beheer en implementatie van OS-updates en beveiligingspatches stroomlijnen
- Verminder de hoeveelheid workflows voor het beschikbaar stellen van apparaten door de inkoop, configuratie en implementatie van apps te centraliseren, waardoor ook de beveiliging van apps uit gescreende, betrouwbare bronnen wordt gegarandeerd
- Apparaten hoeven minder vaak te worden ingesteld door gebruikers in staat te stellen hun apparaten te onderhouden zonder ondersteuning van IT
- Maak beheer op afstand mogelijk, ongeacht welk ondersteund apparaat wordt gebruikt, waar vandaan en via elke netwerkverbinding

Modellen voor apparaateigendom

Het automatiseren van het beheer en de beveiliging van je apparatenpark is een essentiële functie, vooral naarmate het aantal apparaten toeneemt en het personeelsbestand meer gedecentraliseerd wordt. De toename in de toepassing van en het vertrouwen in het Apple platform en mobiele apparaten op de werkplek is net zo divers geworden als de sectoren en gebruikers die op deze apparaten vertrouwen om productief te blijven.

Sommige organisaties hebben Apple producten omarmd door keuzeprogramma's voor werknemers te implementeren waarin eigen apparaten met macOS, iOS en iPadOS worden toegewezen, terwijl andere organisaties Apple op het werk hebben omarmd door het werknemers toe te staan om persoonlijke apparaten te gebruiken om toegang te krijgen tot zakelijke resources. Door hen in staat te stellen comfortabeler te werken met de hardware en software waarmee ze het meest vertrouwd zijn, besparen organisaties op de kosten van het leveren van apparatuur voor elke betrokkene, vooral wanneer gebruikers al een functioneel apparaat hebben dat ze kennen en waar ze van houden.

Hierdoor verschuift de vraag van "Hoe zorgen we voor apparaten van gebruikers?" naar "Hoe zorgen we ervoor dat bedrijfsmiddelen beveiligd blijven?"

Dit is waar MDM en flexibele modellen voor apparaateigendom van je organisatie samenkomen om de oplossing van meerdere modellen voor apparaateigendom te vormen, zoals:

Bring Your Own Device (BYOD)

Ongetwijfeld het meest voorkomende model, waarbij gebruikers hun eigen apparaten kunnen gebruiken om toegang te krijgen tot bedrijfsmiddelen. Door te eisen dat gebruikers hun apparaten handmatig aanmelden bij MDM van de organisatie voordat ze toegang krijgen tot werkbronnen, is het dubbele voordeel dat gebruikers er zeker van kunnen zijn dat ze de tools krijgen die ze nodig hebben om toegang te krijgen tot de gegevens en services die ze nodig hebben om hun werk uit te voeren; organisaties kunnen gerust zijn in de wetenschap dat de aangemelde apparaten zijn voorzien van de benodigde beveiligingssoftware en -instellingen om bedrijfsgegevens beveiligd te houden tijdens gebruik, in rusttoestand en onderweg.

Choose Your Own Device (CYOD)

Dit is een variatie op BYOD, behalve dat de organisatie of instelling vaak eigenaar is van de apparaten die in dit model worden gebruikt en die moeten worden gebruikt voor het uitvoeren van werkgerelateerde functies of bij het nastreven van leren (in het geval van onderwijs.) Door een keuzeprogramma voor werknemers in te stellen, kunnen belanghebbenden kiezen welk Apple apparaat het beste voldoet aan hun behoeften. Elk apparaat wordt geregistreerd, toegewezen aan een belanghebbende en beheerd door het MDM van de organisatie. De apps, configuratieprofielen, apparaatinstellingen en beveiligingssoftware worden geleverd op basis van een baseline van het beveiligingsbeleid van de organisatie en rekening houdend met de functievereisten van de gebruiker.

Company-Owned Personally Enabled (COPE)

Het COPE-model is een groeiende trend bij grotere organisaties, vooral bij organisaties die volledig op afstand zijn gaan werken of met hybride werkomgevingen. Hierbij kopen organisaties de apparatuur en zijn ze er eigenaar van, terwijl ze deze volledig registreren en beheren binnen het MDM van de organisatie. Net als bij CYOD worden de tools die belanghebbenden nodig hebben om hun taken uit te voeren geïnstalleerd en beheerd op basis van het apparaat en het beveiligingsbeleid van het bedrijf. Maar net als bij BYOD staat de organisatie gebruikers toe en moedigt ze zelfs aan om de apparaten te gebruiken voor persoonlijk gebruik naast professioneel gebruik. Dit zorgt ervoor dat bedrijfsgegevens veilig blijven binnen beheerde apps en configuratieprofielen. Hoewel dit het probleem kan opwerpen van persoonlijke, privégegevens die toegankelijk zijn voor bedrijven via COPE-apparaten, is het belangrijk om rekening te houden met de privacy van de gegevens en de juiste hoeveelheid beheer en privacy te bieden aan deze apparaten door middel van Acceptable Use Policies (AUP's) en gegevensbeheer.

Flexibele inschrijvingsmethoden

Om het beheer van meerdere eigendomsmodellen voor apparaten binnen dezelfde MDM-omgeving te vereenvoudigen, heeft Apple twee verschillende registratiemethoden ontwikkeld die in combinatie met elkaar worden gebruikt om de beveiliging van de organisatie te beheren en af te dwingen zonder de privacy van de gebruiker in gevaar te brengen en vice versa.

Automatische apparaatinschrijving
Dit is de meest gebruikelijke methode die de meeste organisaties met bedrijfsapparatuur verkiezen. Deze methode certificeert dat elke stap in de registratieketen is geverifieerd: van aankoop bij Apple (of een geautoriseerde derde partij) via pre-staging in de MDM tot de registratiefase die begint wanneer het apparaat wordt ingeschakeld: elke stap volgt in een geautomatiseerde procedure van Apple naar MDM naar beheerder voor doorlopend beheer. Omdat deze keten is geverifieerd, wordt Supervisie ingeschakeld op apparaten die zijn aangemeld via Automated Device Enrollment, wat fungeert als een vertrouwde basis waarmee IT volledige controle kan krijgen over het apparaat gedurende de gehele levenscyclus. Supervisie is de basis van vertrouwen, vereist bij het uitvoeren van bepaalde beheertaken op beheerde apparaten.

Door de gebruiker geïnitieerde apparaatinschrijving
Deze aanmeldingsmethode is nieuwer en komt vaker voor wanneer de aangemelde apparaten persoonlijk eigendom zijn als onderdeel van een BYOD-model. Met automatische apparaatinschrijving is de inschrijving afhankelijk van de gebruiker of eigenaar van het apparaat om het apparaat handmatig in te schrijven in de Instellingen-app en te verifiëren met behulp van hun bedrijfsinloggegevens. Na voltooiing van het inschrijvingsproces voor de gebruiker, zorgt de MDM van de organisatie voor beveiligde communicatie in twee richtingen tussen het apparaat van de gebruiker en de beheeroplossing van de organisatie.

Na registratie kunnen apparaten in persoonlijk eigendom worden beheerd via MDM, waarbij beheerders beheerde apps kunnen installeren, configuratieprofielen kunnen implementeren en bepaalde instellingen kunnen wijzigen met behulp van een set configuraties waarmee organisaties apparaatspecifieke vereisten kunnen instellen en beheeracties of vereisten kunnen koppelen aan de gebruiker, niet aan het hele apparaat. Apple heeft de beperking zo ontworpen dat organisaties de nodige stappen kunnen ondernemen om de toegang tot hun gegevens, de interactie met apps, de opslag op het apparaat en de overdracht via netwerken te beveiligen zonder dat dit gevolgen heeft voor de persoonlijke apps, gegevens en privé-informatie op het apparaat. Organisaties kunnen de zichtbaarheid van beheerde apparaten aanpassen door een persoonlijke Apple ID te koppelen aan persoonsgegevens en een beheerde Apple ID aan bedrijfsgegevens.

3

BOUWSTEEN DRIE:

apparaten beveiligen

Apparaten, gegevens en gebruikers beschermen tegen bedreigingen

'Hackers hoeven het maar één keer goed te doen; wij moeten het elke keer goed doen.'

- Chris Triolo, HP

Als we terugkijken naar enkele van de grootste, meest complexe en zelfs dodelijkste datalekken in de recente geschiedenis, vinden we een rode draad. Aanvallen zoals Stuxnet schakelden het Iraanse nucleaire verrijkingsprogramma uit door de laptop van een aannemer te infecteren die updates uitvoerde voor de SCADA-apparatuur. LinkedIn was het doelwit van een ontwikkelaar die misbruik maakte van zijn API om persoonsgegevens van 700 miljoen gebruikers te scrapen en vervolgens de gegevens online te verkopen. Aadhaar - de grootste ID-database, inclusief persoonsgegevens en financiële gegevens, voor meer dan 1,1 miljard Indiase burgers, werd gestolen en verkocht door dreigingsactoren nadat ze toegang hadden gekregen via een onbeveiligde website die aan de database was gekoppeld. In deze en vergelijkbare gevallen werden aanvallen mogelijk gemaakt door slechts één apparaat aan te vallen en in gevaar te brengen.

Een van de meest voorkomende manieren om het beveiligingsraamwerk van een organisatie te omzeilen en toegang te krijgen tot gevoelige gegevens en tegelijkertijd de veiligheid van eindgebruikers in gevaar te brengen, is door een enkel apparaat te compromitteren. Ongeacht de branche waarin je organisatie actief is en of deze gegevens en/of resources levert aan kenniswerkers, leerlingen, leerkrachten, zorgverleners, telewerkers, winkelpersoneel of frequente reizigers — je apparaten kunnen zich op elk moment overal ter wereld bevinden en verbinding maken via een willekeurig aantal niet-vertrouwde netwerken, waardoor het risico op bedreigingen voor zowel het apparaat als het bedrijfsnetwerk exponentieel toeneemt.

Verloren of gestolen apparaten

Een verloren of gestolen iPhone, iPad of Mac is niet alleen een financieel verlies: het is ook een enorm beveiligingsrisico waarvan de gevolgen niet te overzien zijn. De volgende voorbeelden onderstrepen hoe belangrijk het is om de risico's van zoekgeraakte en gestolen apparaten te beperken:

SCENARIO'S UIT DE ECHTE WERELD

Een werknemer op afstand bereidt juridische documenten voor voor een lopende rechtszaak over aansprakelijkheid en werkt vanuit een nabijgelegen cafeetje. Hij laat zijn Mac-laptop van het bedrijf even onbeheerd achter terwijl hij een kopje koffie gaat halen, precies op het moment dat een dief binnenglipt en zijn laptop steelt. Als het apparaat ontgrendeld is, heeft de aanvaller ongehinderd toegang tot gevoelige en mogelijk vertrouwelijke bedrijfsinformatie die een negatieve invloed kan hebben op lopende juridische procedures en de reputatie van het bedrijf.

In een tweede voorbeeld raakt een student die zijn eigen iPhone gebruikt om toegang te krijgen tot lesmaterialen via het onderwijsportaal, zijn apparaat kwijt terwijl hij van lokaal wisselt. Een andere gebruiker vindt de telefoon en krijgt toegang tot de accountgegevens van de student, waardoor hij toegang krijgt tot gevoelige persoonsgegevens, zoals zijn adres, telefoonnummer of studentenkaart. Een onbevoegde gebruiker kan persoonsgegevens zoals deze gebruiken voor identiteitsdiefstal of om misdaden te plegen terwijl hij zich voordoet als het slachtoffer. Het apparaat kan zelfs verder worden aangetast met malware en worden teruggestuurd naar het slachtoffer, waardoor zijn veiligheid en welzijn in gevaar komt door het op afstand volgen en stalken door dreigingsactoren.

Simpel gezegd: apparaten raken zoek en worden gestolen. Ongelukken en momenten van onoplettendheid komen voor. Toch is planning, met de aanname dat het slechts een kwestie is van wanneer en niet of iemand een apparaat kwijtraakt, een belangrijke sleutel om ervoor te zorgen dat de juiste strategieën voor risicobeperking worden toegepast voordat apparaten zoekraken of worden gestolen.

Bijkomende aandachtspunten voor gebruikers- en gegevensbeveiliging zijn dat veel apparaten, vooral apparaten voor leerlingen en patiënten of omgevingen met gedeelde apparaten voor meerdere gebruikers, beveiligd moeten worden tegen misbruik, het per ongeluk ontdekken van andermans gegevens of het openen en bekijken van riskante en ongepaste content.

Afhankelijk van de unieke behoeften van je organisatie kan het verstevigen van beveiligingsinstellingen en het configureren van apparaten zodat ze voldoen aan de vereisten van de organisatie en compliance een aanzienlijke, tijdrovende en arbeidsintensieve onderneming zijn, vooral naarmate het aantal apparaten toeneemt.

Als je apparaten handmatig beveiligt of beperkt, moet je het volgende doen:

Mac

- Wachtwoorden verplichten op alle apparaten
- Zoek mijn Mac inschakelen via Systeemvoorkeuren>iCloud
- Afhankelijk zijn van individuele gebruikers om zich aan te melden bij iCloud of om hun wachtwoord te onthouden (voorwaarde om Zoek mijn in te schakelen)
- Apple op de hoogte stellen van verlies of diefstal van een apparaat en de mogelijkheid bieden om het apparaat te wissen/verwijderen
- Alle voorraad traceren aan de hand van Mac-serienummers of asset tags
- Ouderlijk toezicht op het apparaat inschakelen om ongepaste content en schadelijke websites te blokkeren (met Safari-browser)
- Macs up-to-date houden met alle systeem- en programma-updates om kwetsbaarheden te minimaliseren
- Apparaatinstellingen configureren en verstevigen om misconfiguraties te minimaliseren die gegevens onbeveiligd kunnen achterlaten
- Ondersteunde applicaties implementeren en up-to-date houden
- Eindpuntbeveiliging installeren en configureren om apparaten te bewaken, bedreigingen te identificeren en te herstellen

Telefoon en iPad

- Wachtwoorden verplichten op alle apparaten
- Zoek mijn Mac inschakelen via Systeemvoorkeuren > iCloud
- Afhankelijk zijn van individuele gebruikers om zich aan te melden bij iCloud of om hun wachtwoord te onthouden
- De voorraad in de gaten houden aan de hand van apparaatserienummers of asset tags
- Apple op de hoogte stellen van verlies of diefstal van een apparaat en de mogelijkheid bieden om het apparaat te wissen/verwijderen
- Ouderlijk toezicht inschakelen op een individueel apparaat in en voor elk apparaat een andere account aanmaken
- iOS-apparaten up-to-date houden met alle systeem- en app-updates om kwetsbaarheden te minimaliseren
- Apparaatinstellingen configureren en verstevigen om misconfiguraties te minimaliseren die gegevens onbeveiligd kunnen achterlaten
- Beheerde apps implementeren en up-to-date houden
- Eindpuntbeveiliging installeren om apparaten te bewaken, bedreigingen te identificeren en te herstellen

Apple TV

- Wachtwoorden verplichten op alle Apple TV's
- Beperkingen configureren:
  - Ga in het hoofdmenu naar Instellingen > Algemeen > Restricties
  - Selecteer Beperkingen om het in te schakelen
  - Een viercijferige toegangscode invoeren wanneer daarom wordt gevraagd
  - Voer de vier cijfers nogmaals in om te bevestigen en selecteer vervolgens OK
  - Onthoud de toegangscode
  - Herhaal voor alle Apple TV's

Airplay voor Apple TV beperken :

- Ga in het hoofdmenu naar Instellingen > Selecteer AirPlay
- Schakel AirPlay in of uit

Kies uit:

- Iedereen
- Iedereen op hetzelfde netwerk
- Herhaal voor alle Apple TV's

Een eersteklas MDM-oplossing, zoals Jamf Pro, biedt dezelfde beheertaken om apparaten te beveiligen of te beperken die hierboven zijn beschreven en nog meer:

Mac, iPhone, iPad en Apple TV

- Stel alle beperkingen en beveiligingsfuncties vanaf het eerste gebruik in of schakel ze automatisch in met Supervisie en vertrouwde configuratieprofielen en beleidsregels
- Vergrendel of wis elk verloren of misbruikt apparaat op afstand, ongeacht de fysieke locatie en ongeacht of het apparaat een iCloud-account heeft (geen Apple ID vereist)
- Stel meerdere gebruikers in staat om veilig apparaten te delen door een apparaat te wissen tussen gebruiksmomenten en gebruikers hun inloggegevens en instellingen te laten gebruiken die gekoppeld zijn aan de gebruiker, niet aan het apparaat
- Configureer Apple ID's om toe te wijzen aan het apparaat voor zakelijke taken, terwijl de gebruiker met zijn Apple ID voor consumenten toegang heeft tot persoonlijke apps, gegevens en instellingen die zijn opgeslagen in iCloud
- Houd een voorraad bij van alle apparaten, inclusief de mogelijkheid om ze te groeperen per categorie, niet alleen serienummer of asset tag, om alle benodigde gegevens te verzamelen, zoals gebruikerstoewijzingen, OS-versie of geïnstalleerde apps, om er maar een paar te noemen
- Voer beheertaken uit waarbij opdrachten worden gegeven aan één apparaat of in bulk, zoals beveiligingsupdates implementeren, upgraden naar een nieuwe OS-versie of vergeten toegangscodes op vergrendelde apparaten administratief wissen
- Implemeteer ouderlijk toezicht en blokkeer de toegang tot riskante of ongepaste apps door granulaire beperkingen toe te passen op basis van bepaalde criteria of op alle apparaten tegelijk
- Implementeer beheerde apps die gebruikers nodig hebben om thuis, op kantoor, op school of waar dan ook productief te blijven. Keur apps vooraf apps goed om te hosten binnen de Self Service-app, zodat gebruikers toegang hebben tot de software die ze nodig hebben, precies wanneer ze die nodig hebben
- Integreer oplossingen voor eindpuntbeveiliging met je MDM om ervoor te zorgen dat apparaten voortdurend worden bewaakt en beschermd tegen beveiligingsrisico's, terwijl telemetriegegevens worden gedeeld met de MDM om beheer op basis van beleid mogelijk te maken voor het automatiseren van reacties op incidenten
- Beheer elk facet van apparaatbeheertaken centraal om ervoor te zorgen dat apparaten, gebruikers en gegevens beveiligd blijven tegen cyberbedreigingen met behoud van de privacy van gebruikers

Deze ervaring stroomlijnt niet alleen het werk voor IT-beheerders en -medewerkers, maar ondersteunt ook de eindgebruikers. Het biedt de ervaring waar mensen van houden en die ze van Apple gewend zijn, zonder dat dit ten koste gaat van de organisatie, de compliance en beveiligingseisen in de sector of de privacy van gebruikers ten gunste van strengere beveiligingscontroles.

4

BOUWSTEEN VIER:

Gegevens coderen

De basisprincipes van gegevens in rust en gegevens in doorvoer en hoe beide soorten gegevens veilig te houden.

Of je organisatie nu een school is die informatie over leerlingen beschermt, een gezondheidszorginstelling die de gezondheidsgeschiedenis van patiënten bewaakt of een bedrijf dat zijn intellectuele eigendom wil beschermen, versleuteling is niet langer een optie voor je organisatie: het is een essentiële vereiste voor elk bedrijf dat gevoelige, vertrouwelijke en missiekritische gegevens, of echt gegevens van elk classificatietype veilig wil houden, de beste manier is om alle gegevens op apparaten te versleutelen.

Hieronder volgt een overzicht van de drie gegevensstatussen op een bepaald moment op een apparaat:

Gegevens in rust: lokaal opgeslagen (meestal) op een apparaat dat momenteel niet wordt geopend of gebruikt.

Gegevens in beweging: overgedragen gegevens, zowel ontvangen als verzonden, via een communicatiekanaal, zoals een bekabeld of draadloos netwerk.

Gebruikte gegevens: gegevens die niet permanent worden opgeslagen of via netwerken worden verzonden, maar waar apps of andere processen op dat moment mee werken.

Elk heeft inherente risico's die uniek zijn voor zijn status, wat betekent dat, over het algemeen, een oplossing voor de ene status mogelijk niet volledig compenseert (of helemaal niet werkt) voor een andere status. Hoewel dit de beveiligingsstrategie complexer maakt, hoef je je geen zorgen te maken, want alle effectieve oplossingen zijn gebaseerd op de fundamentele functie van versleuteling.

SCENARIO'S UIT DE ECHTE WERELD

Een nieuwe medewerker op de HR-afdeling van je organisatie ontvangt zijn nieuwe Mac en voltooit snel het installatieproces om aan de slag te gaan. Een van zijn taken is het maken van een noodcontactstructuur **met behulp van spreadsheetsoftware**, met de naam, functietitel, e-mailadres van het bedrijf, persoonlijk adres, persoonlijk contactnummer van elke werknemer en of ze een primaire of alternatieve contactpersoon zijn. Van deze informatie moet **lokaal op de computer een back**-up worden gemaakt, inclusief de persoonlijke contactgegevens van het managementteam en de C-suite-teams, en er moet een duplicaat beschikbaar worden gemaakt voor geautoriseerde belanghebbenden zodat ze deze **veilig kunnen openen vanuit een cloud-opslagplaats.**

In het bovenstaande scenario geven de vetgedrukte gedeelten een specifiek voorbeeld van elke gegevensstatus. Ten eerste is 'spreadsheetsoftware gebruiken' een voorbeeld van gegevens in gebruik, wat aangeeft dat gegevens veilig moeten blijven terwijl er binnen de app mee wordt gewerkt. Dit vereist dat de integriteit van de software wordt gecontroleerd en geverifieerd om er zeker van te zijn dat een bedreigende actor of kwaadaardige code de interne beveiliging niet heeft aangetast. Ten tweede is 'een lokale back-up maken' een voorbeeld van gegevens in rust, wat aangeeft hoe belangrijk het is om versleuteling in te schakelen om te voorkomen dat onbevoegden toegang hebben tot gegevens en deze kunnen lezen. Ten derde is 'veilig toegang krijgen tot een cloudopslagplaats' een voorbeeld van gegevens in beweging, zoals gegevens die worden verzonden en ontvangen via een netwerkverbinding. De netwerkverbindingen die worden gebruikt voor communicatie moeten end-to-end worden versleuteld, zodat alleen de twee verbindingen aan beide uiteinden het bericht succesvol kunnen ontsleutelen en deze gegevens kunnen beschermen tegen onbevoegde ontvangst of afluisteraanvallen.

En hoewel deze derde gegevenstoestand veel lijkt op legacy VPN-services, is het onderdeel dat het onderscheidt van legacy VPN de formulering 'geautoriseerde belanghebbenden', omdat Zero Trust Network Access (ZTNA) versleuteling biedt voor gegevens in beweging. ZTNA integreert ook met je identiteitsprovider (IdP) om ervoor te zorgen dat alleen gebruikers en apparaten die zich succesvol hebben geauthenticeerd en de benodigde toegangsrechten hebben, toegang krijgen tot de gevraagde resources achter extra beschermingslagen, waarbij het principe van de laagste privileges wordt gehandhaafd. In tegenstelling tot bestaande VPN-services die na authenticatie vaak toegang verlenen tot het hele netwerk, maakt ZTNA's implementatie van het beveiligen van verbindingen gebruik van microtunnels om een unieke tunnel te creëren voor elke beschermde app of service. Dit zorgt voor een betere beveiliging door het principe van de minste privileges af te dwingen en tegelijkertijd gezondheidscontroles toe te passen om ervoor te zorgen dat apparaten voldoen aan de minimumvereisten. Dit wordt gecombineerd met de authenticatievereisten van de gebruiker, telkens wanneer een verzoek wordt gedaan en voordat toegang wordt verleend.

De drie gegevensstatussen versleutelen

Gegevens in rust

Volume- of volledige apparaatversleuteling

Het versleutelen van de gegevens die zijn opgeslagen op een mobiel apparaat of in een volume op je computer is om verschillende redenen aan te raden. Het eenvoudig te configureren proces voor het inschakelen van versleuteling bestaat uit proactieve en reactieve maatregelen en biedt maximale veiligheid en beveiliging voor gegevens in rust in permanente opslag. Door algoritmes te gebruiken die aanvallers honderden, of waarschijnlijk duizenden jaren van 24 uur per dag werken met de krachtigste computers zouden kosten om te verslaan, gezien de relatief minimale inspanning die nodig is om versleuteling in te stellen, is het een logische keuze als het gaat om het opnemen van deze beveiligingscontrole als onderdeel van een defense-in-depth strategie - zoals The Alamo, of het spreekwoordelijke "laatste verzet" tussen een bedreigende actor en vertrouwelijke gegevens.

Neem bijvoorbeeld een aantal veelvoorkomende beveiligingsincidenten die effectief worden beperkt door volledige apparaat- of volumeversleuteling in te schakelen:

Verlies of diefstal van een apparaat

Vooral zoekgeraakte apparaten, zoals iPhones, iPads of MacBook laptops, komen vaak voor bij mobiele apparaten. Hoe groter de mobiliteit, hoe groter het risico op verlies of diefstal. Dat gezegd hebbende, zodra een apparaat uit je handen is, hebben actoren van bedreigingen vrij spel om te proberen de gegevens die op het apparaat zijn opgeslagen te bemachtigen.

Natuurlijk zou een complexe toegangscode of een sterk wachtwoord je apparaat moeten beschermen. Afhankelijk van het apparaat kunnen aanvallers echter nog steeds op een andere manier toegang krijgen tot sommige of alle gegevens op het apparaat, behalve als deze versleuteld zijn. Door versleuteling in te schakelen worden de gegevens zodanig vervormd dat ze onleesbaar zijn tenzij de versleutelingssleutel ze ontcijfert. Het maakt niet uit of het apparaat wordt opgestart naar het inlogscherm of dat de SSD op de een of andere manier wordt benaderd en aangesloten op een ander apparaat als een externe schijf. Versleutelde gegevens blijven versleuteld totdat de ontsleutelings- of herstelsleutel wordt gebruikt om ze te ontsleutelen. Elk ander scenario maakt de gegevens onleesbaar en dus onbruikbaar.

Fysieke toegang

Net als bij het gedeelte over verloren of gestolen apparaten hierboven, betekent het verkrijgen van fysieke toegang tot een apparaat niet dat het eerst zoek moet zijn. Denk aan een gedeeld apparaat in een werkruimte, misschien de computer die aan je is toegewezen op je bureau of elke andere computer dat een bedreigende actor kan proberen te gebruiken wanneer niemand kijkt. Als je sessie voorbij is en je uitlogt, je apparaat afsluit of zelfs vergrendelt terwijl je weggaat of het niet gebruikt, zijn en blijven de gegevens in het volume of apparaat versleuteld. Er is een ontcijferings- of herstelsleutel nodig om de gegevens te ontsleutelen en leesbare toegang te krijgen tot de beveiligde gegevens.

Compliance van de regelgeving

Afhankelijk van de branche waartoe je organisatie behoort, kun je onderhevig zijn aan wetten (bekend als voorschriften) die minimumeisen stellen aan de beveiliging van gegevens en de manier waarop deze worden verwerkt, terwijl ze ook beperkingen opleggen over welke functies mogen werken met beschermde gegevenstypen. Specifieke sectoren zijn agressiever gereguleerd dan andere; dit zijn sterk gereguleerde sectoren, zoals de financiële sector en de gezondheidszorg, terwijl andere zich mogelijk alleen richten op bepaalde aspecten van gegevensbeveiliging, zoals onderwijsregelgeving die gericht is op het beschermen van het welzijn van studenten en de persoonsgegevens die met hen is geassocieerd.

Zoals eerder gezegd, zijn regels gebaseerd op wetten en het schenden ervan kan ernstige gevolgen hebben voor de organisatie of instelling als ze zich niet goed houden aan de regels van de bestuursorganen. Vaak is het versleutelen van gegevens een belangrijke beveiligingscontrole die vereist is tijdens verschillende gegevensstatussen, zoals in rust of in beweging, om het risico te minimaliseren dat gereglementeerde informatie in verkeerde handen valt door datalekken, exfiltratie of zelfs blootstelling aan onbevoegde gebruikers.

Gegevensversleuteling en Apple apparaten

- macOS heeft al ingebouwde volumeversleuteling in FileVault. Je hoeft geen extra software toe te voegen om een map, schijf of volume op een Mac te versleutelen.
- Nieuwere Macs, zoals die met Apple Silicon, vertrouwen op de secure enclave. Een speciale hardwarecomponent die zorgt voor het aanmaken en opslaan van versleutelingssleutels en tegelijkertijd algoritmische berekeningen uitvoert.
- Op Intel gebaseerde Macs vertrouwen op een soortgelijk speciaal hardwareonderdeel genaamd de T2 security chip om soortgelijke functies uit te voeren als de secure enclave.
- FileVault is FIPS 140-2 gecertificeerd. Dat betekent dat het versleutelingssysteem van Apple is gecertificeerd door en voldoet aan de hoogste standaarden voor versleuteling door de Amerikaanse federale overheid.
- Je kunt FileVault handmatig of op afstand inschakelen: persoonlijke gebruikers kunnen de optie kiezen op één apparaat, of IT kan de inschakeling automatiseren en afdwingen (met Jamf Pro) op honderden of zelfs duizenden apparaten met één beleid.
- Geef gebruikers toegang tot versleutelde/ontsleutelde volumes door simpelweg te verifiëren in macOS of door hun toegangscode in te voeren op iOS- en iPadOS-apparaten. Gebruikers van ondersteunde apparaten kunnen de TouchID- of FaceID-technologieën van Apple gebruiken om een extra beveiligingslaag toe te voegen aan de gegevensbescherming door middel van biometrie met behulp van hun vingerafdruk of gezichtsherkenningspatronen.

Om FileVault handmatig in te schakelen op macOS:

- Ga naar Systeeminstellingen > Privacy en beveiliging > FileVault
- Selecteer de knop 'Inschakelen...' om volumeversleuteling in te schakelen
- Herhaal dit voor alle apparaten

Om FileVault in te schakelen op alle apparaten van je organisatie, maak je gebruik van je MDM-oplossing voor het automatiseren, implementeren en afdwingen van versleuteling. Je kunt een configuratieprofiel of beleid implementeren dat FileVault inschakelt. IT kan herstelsleutels ophalen als het personeel het volume later moet ontsleutelen.

- Maak een configuratieprofiel door een eenvoudige selectie van opties binnen Jamf Pro
- Implementeer granulair naar zoveel apparaten als je wilt of naar alle op macOS gebaseerde apparaten
- **Er is geen stap drie**

Met Jamf Pro kun je ook de omleiding van herstelsleutels configureren, zelfs als de gebruiker FileVault zelf inschakelt. IT beschikt dan over de sleutel die is opgeslagen in de beheeroplossing, zodat deze eenvoudig kan worden teruggevonden per apparaatrecord.

Hoe zit het met een iPad of iPhone?

Het versleutelen van iOS- en iPadOS-apparaten is nog eenvoudiger. Op iOS-apparaten is versleuteling ingebouwd zodra er een toegangscode is ingesteld. Je kunt dit individueel doen, of je kunt het vereisen van Jamf Pro, net als het instellen van de parameters voor de sterkte van de toegangscode, zoals de minimale lengte en complexiteitsvereisten.

Data in transit

Netwerkverbindingen van begin tot eind versleutelen

Conventionele praktijkvoorbeelden dicteerden het gebruik van een VPN om gegevens te beschermen wanneer ze van het ene apparaat naar een andere service gaan. Deze methode gaat tientallen jaren terug en werd ontwikkeld in een tijd waarin VPN's werden gebruikt om twee ongelijksoortige netwerken veilig te overbruggen via een niet-vertrouwd netwerk, zoals het internet.

Deze beveiligingscontrole nog steeds actief wordt gebruikt door veel persoonlijke en zakelijke gebruikers. Maar de veranderingen in het computerlandschap van de afgelopen jaren, als gevolg van de adoptie van Apple op het werk, de explosieve groei van mobiele apparaten voor persoonlijk en zakelijk gebruik en organisaties die migreren naar volledig externe en hybride werkomgevingen, de beperkingen van VPN-technologie om apparaten, gebruikers en gegevens effectief te beschermen in het moderne bedreigingslandschap aan het licht gebracht.

Deze veranderingen hebben samen een revolutie teweeggebracht in de manier waarop we werken en gamen op computers en mobiele apparaten. Waarom vertrouw je dan nog steeds op legacyprocessen voor je beveiligingsstrategie om gegevens in beweging veilig te houden?

Het korte antwoord is Zero Trust Network Access, kortweg ZTNA. Het lange antwoord is dat deze oplossing is ontwikkeld vanuit de zeer reële behoefte om verschillende soorten apparaten, lokale en gedistribueerde gebruikers en teams te beheren. Ook gegevens die toegankelijk zijn via niet-vertrouwde netwerken en het vertrouwen op cloud-gebaseerde diensten om de infrastructuur uit te breiden terwijl de netwerkperimeter van de organisatie wordt uitgehold. Dit alles terwijl ze worden beveiligd tegen bestaande en nieuwe beveiligingsbedreigingen die worden ingezet door bedreigingsactoren, met een opvallende toename van bedreigingen die gericht zijn op macOS en mobiele apparaten in het algemeen.

Simpel gezegd: netwerkverbindingen beveiligen is niet langer alleen iets voor werknemers die op reis zijn of voor een paar speciale gebruikssituaties om op afstand productief te blijven.

Het gaat ook verder dan alleen het versleutelen van communicatie tussen twee punten en vereist granulaire beveiliging om belanghebbenden te beschermen en toegang tot bedrijfsmiddelen te voorkomen terwijl de introductie van bedreigingen wordt geminimaliseerd. ZTNA doet dit onder andere door:

- Integratie met cloud-gebaseerde IdP's om centraal beheerde gebruikersaccounts uit te breiden met machtigingen die de gebruiker overal volgen.
- Frequente apparaatcontroles zorgen ervoor dat eindpunten voldoen aan de minimumvereisten, zoals het up-to-date zijn met patches, zorgen ervoor dat de beveiligingsintegriteit intact blijft door te controleren op jailbroken of geroote apparaten en dat de eindpuntbeveiliging correct is geïnstalleerd en geconfigureerd.
- Als eindpunten een gezondheidscontrole niet doorstaan of als gecompromitteerd worden beschouwd, maakt ZTNA-integratie met een MDM-oplossing van topklasse, zoals Jamf Pro, beleidsgebaseerd beheer mogelijk door telemetriegegevens veilig te delen om toegang op te schorten. Daarnaast kan ZTNA herstelworkflows uitvoeren om de noodzakelijke taken uit te voeren om het eindpunt in compliance te brengen, waarbij wordt geverifieerd dat alle gedetecteerde problemen zijn opgelost.
- In plaats van impliciet vertrouwen, zoals bij oudere VPN's, werken we volgens de mantra 'vertrouw nooit - controleer altijd' telkens wanneer toegang wordt gevraagd tot een bedrijfsresource. Pas nadat de verificatie succesvol is verlopen, wordt toegang tot de aangevraagde resource verleend.

GEGEVENS VERSLEUTELEN

Wat je nodig hebt voor gegevens in doorvoer

Een beveiligde netwerkverbinding met een VPN-server

Om handmatig verbinding te maken met een VPN:

iOS en iPadOS

- Ga naar Systeeminstellingen> VPN
- Selecteer "VPN-configuratie toevoegen"
- Voer het VPN-serveradres op het apparaat in
- Selecteer het uit je netwerkopties
- Herhaal dit voor elk apparaat

macOS

- Ga naar Systeeminstellingen > Netwerk > VPN & Filters
- Selecteer "VPN-configuratie toevoegen"
- Voer het VPN-serveradres op het apparaat in
- Selecteer het uit je netwerkopties
- Herhaal dit voor elk apparaat

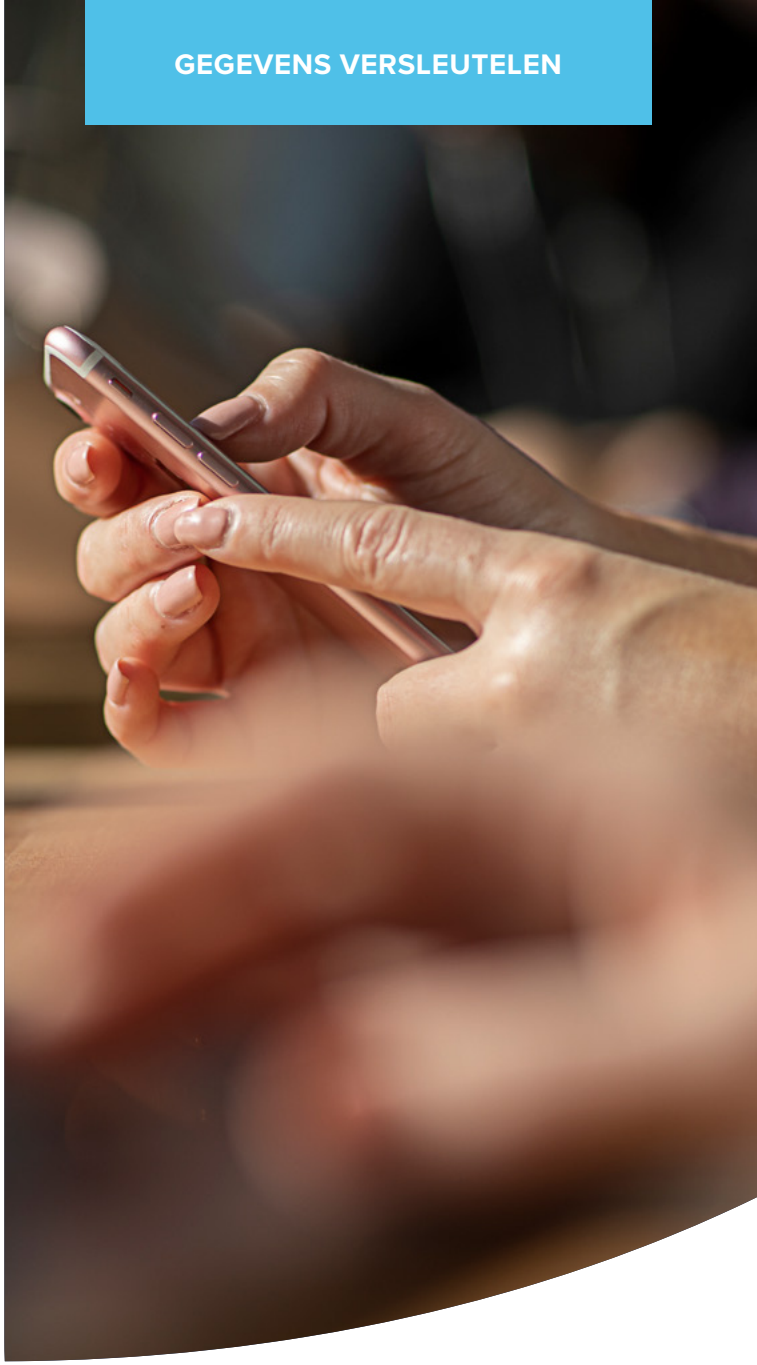
Om meerdere apparaten aan te sluiten op een VPN:

Nadat je een VPN-provider hebt ingesteld

- Maak een configuratieprofiel in een MDM zoals Jamf voor iOS en/of macOS
- Implementeer configuraties op zoveel apparaten als je wilt
- Je raadt het al: er is geen stap drie

'Hoe weet ik zeker dat mijn versleuteling naadloos is?'

Een belangrijke manier om beveiliging en consistente versleuteling te garanderen is door je MDM in de cloud te hosten. Met een gerenommeerd product zoals Jamf Cloud kun je gerust zijn in de wetenschap dat je server veilig is, je gegevens veilig zijn en dat eventuele updates of patches onmiddellijk beschikbaar zijn.



Voordelen van ZTNA ten opzichte van legacy VPN:

- De beveiliging wordt verbeterd door over te stappen van impliciet vertrouwen naar het expliciete Zero Trust- model dat vereist dat gebruikers en apparaten worden geverifieerd voordat toegang tot aangevraagde resources wordt verleend.
- Split-tunneling beveiligt zakelijk verkeer, terwijl persoonlijk verkeer rechtstreeks naar het internet wordt geleid en niet terug naar een centraal netwerk, waardoor overhead wordt verminderd en bandbreedte wordt bespaard. Dit staat gelijk aan betere prestaties en een betere privacybescherming voor eindgebruikers.
- Always-on bescherming betekent dat resources zelfs als de service is uitgeschakeld beschermd zijn: bij het aanvragen van toegang zal het automatisch inschakelen om ervoor te zorgen dat het verkeer elke keer beschermd blijft.
- Een minimale voetafdruk en cloudhosting betekent geen dure supportcontracten, complexe configuraties of hardware die beheerd moet worden.
- Het ondersteunt ook macOS, iOS, iPadOS, Android en Windows, wat de TCO verlaagt en de administratieve last verlicht voor IT-teams die meerdere hardware- en softwaretypes ondersteunen.

In dit gedeelte hebben we de basisprincipes van gegevensversleuteling besproken, de soorten oplossingen die beschikbaar zijn op Apple apparaten en zelfs de stappen uitgelegd om deze beveiligingscontrole in te schakelen op macOS, iOS en iPadOS. We hebben ook besproken hoe moderne ZTNA-technologie verder gaat dan legacy VPN-bescherming door netwerkverbindingen op afstand te blijven beveiligen en tegelijkertijd extra beveiligingslagen in te bouwen om gebruikers en apparaten te verifiëren voordat toegangsverzoeken worden ingewilligd en ervoor te zorgen dat gegevens in rust (eerstgenoemde) en in beweging (laatstgenoemde) veilig blijven. Maar hoe zit het wanneer gegevens worden gebruikt of verwerkt door apps?

Ontgrendel de andere twee gegevensstatussen; gebruikte gegevens hebben geen specifieke beveiligingscontrole om dit risico te beperken. In plaats daarvan ligt de oplossing in de combinatie met lopende beheer- en beveiligingsworkflows.

GEGEVENS VERSLEUTELEN

Wanneer apps gegevens openen en verwerken, gaan de gegevens van het geheugen (RAM) naar de app om te worden verwerkt, waarna ze terug naar het geheugen worden gewisseld voordat ze permanent worden opgeslagen op de opslag van het apparaat. Apps die zijn ontwikkeld door bekende, vertrouwde ontwikkelaars bevatten allemaal beveiligingsmechanismen om ervoor te zorgen dat de interne beveiliging van de app intact blijft. Een van de vele redenen hiervoor is om ervoor te zorgen dat gegevens die binnen een app worden verwerkt niet worden gedeeld met of gelekt naar andere apps, services of processen die op het apparaat worden uitgevoerd. Dit is ontworpen om de integriteit van de gegevens te behouden terwijl de integriteit van de app behouden blijft.

Apps die gecompromitteerd zijn geraakt door misbruik van een kwetsbaarheid, ongeautoriseerde wijzigingen hebben aangebracht in hun interne beveiliging of malafide apps zijn, die op de markt worden gebracht alsof ze één taak uitvoeren maar in werkelijkheid andere clandestiene taken uitvoeren, brengen echter allemaal de beveiliging van gegevens in gevaar tijdens het gebruik.

Vraag je je af wat dan de beste oplossing is? De onderstaande antwoorden omvatten een combinatie van best practices, een defense-in-depth strategie en processen en workflows die gebruik maken van Jamf Pro om gebruikte gegevens zo veilig mogelijk te houden:

- Een beleid voor doorlopend patchbeheer waarbij apps worden aangeschaft bij legitieme bronnen, zoals de Apple App Store, de website van ontwikkelaars of bij een vertrouwde beheerleverancier, zoals App Installers met Jamf.
- Beheerde apps implementeren via de MDM-oplossing van je voorkeur en op beleid gebaseerd beheer implementeren om apps up-to-date te houden.
- Verifiëren van veilige apparaatinstellingen door configuratieprofielen te installeren om de kans op bedreigingen door verkeerde configuraties te minimaliseren.
- De apparaatinstellingen verstevigen om riskant gedrag te beperken dat bedreigingen kan introduceren, zoals het jailbreaken van iOS of iPadOS of het side-loaden van applicaties van onbevoegde of onveilige bronnen.
- Een doorlopend trainingsprogramma voor gebruikers implementeren om belanghebbenden op de hoogte te houden van veelvoorkomende bedreigingen en hoe bepaalde acties, zoals Shadow IT, risico's met zich meebrengen.
- Een Acceptable Use Policy (AUP) ontwikkelen die alle belanghebbenden ondertekenen om hen bewust te maken van de gedragsverwachtingen en de gevolgen van het schenden van het bedrijfsbeleid.

5

BOUWSTEEN VIJF:

toezicht op compliance

Op de hoogte zijn van de status van protocollen en controles op alle apparaten

Een beveiligingssysteem is zo goed als het zwakste punt. Voor de beste dekking moeten beheerders de apparaten van de organisatie in de gaten houden om te controleren of elk apparaat is bijgewerkt, de meest recente patches heeft ontvangen en de juiste configuratieopties heeft ingesteld.

'Besef van onwetendheid is het begin van wijsheid.'

- Socrates

Door continu rijke telemetriegegevens te verzamelen, de details van elk apparaat die inzicht geven in de beveiligingscontroles, instellingen en gezondheidsstatus, kan IT apparaten, gebruikers en gegevens beter beschermen en er tegelijkertijd voor zorgen dat eindpunten die buiten dhet bereik vallen snel worden hersteld en weer aan de eisen voldoen voordat bedreigingen kunnen leiden tot veel ergere gevolgen, zoals een datalek.

Zoals bij de meeste bouwstenen in dit e-book, zijn er meerdere manieren om eindpuntcompliance te monitoren: handmatige en geautomatiseerde methoden. Afhankelijk van de vereisten van je organisatie kan de doeltreffendheid van compliance monitoring worden beïnvloed door factoren zoals de kennisbasis, de gebruikte oplossingen voor apparaat- en beveiligingsbeheer en budgettaire overwegingen, om een paar van de belangrijkste te noemen.

Het handmatig bewaken en beheren van voorraad en compliance betekent:

- Ervoor zorgen dat alle apparaten van je organisatie worden beschermd door apparaten voortdurend te controleren
- Elk apparaat fysiek opsporen voor inventarisbeheer
- Softwareapplicaties op elk apparaat afzonderlijk bijwerken om ervoor te zorgen dat ze up-to-date zijn
- Controleer of beveiligingsinstellingen, zoals versleuteling, consistent zijn geconfigureerd op elk apparaat
- Monitoren en bevestigen dat niemand risico's heeft geïntroduceerd, zoals malware of verdachte apps
- OS en kritieke beveiligingsupdates uitvoeren zodra deze beschikbaar zijn om bekende kwetsbaarheden te verhelpen en bugs in software te repareren
- De inzet van adequaat personeel om gedetecteerde problemen op te lossen, aangetaste apparaten in quarantaine te plaatsen en herstelwerkzaamheden uit te voeren om aangetaste eindpunts weer aan de eisen te laten voldoen

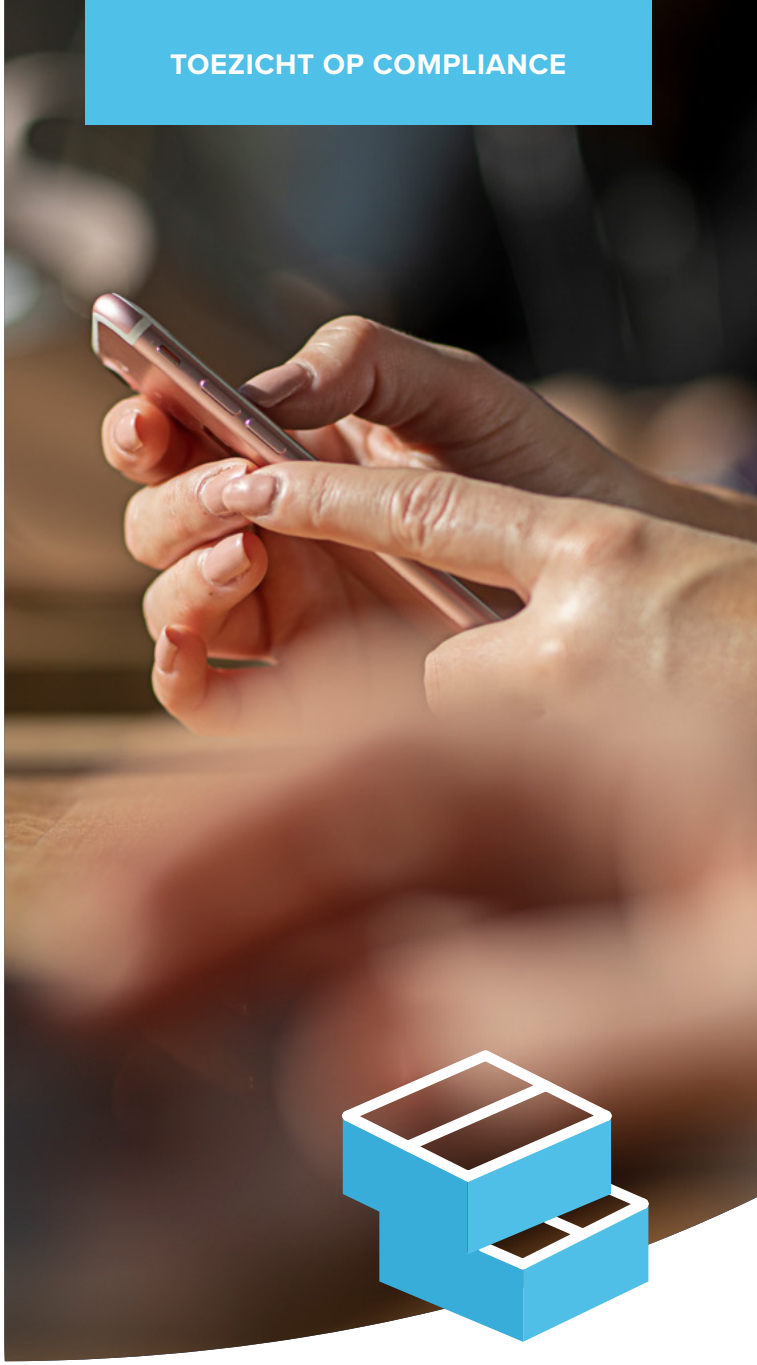
Deze methode vereist voortdurende waakzaamheid en veel tijd voor administratieve overhead in verband met het voltooien van beheertaken. Er is veel buy-in en samenwerking tussen belanghebbenden en managementteams nodig om succesvol te zijn. Het is ook belangrijk om op te merken dat deze methode grotendeels reactief van aard is, wat betekent dat tijdgevoelige kwesties, zoals de responstijden voor incidenten, waarschijnlijk langer zullen zijn, omdat ze optreden nadat problemen zijn gedetecteerd — maar zelden van tevoren.

Als laatste overweging, het aantal en de soorten apparaten die worden ondersteund nemen in omvang toe, de tijd voor IT en Beveiliging om handmatig te reageren op problemen zal ook exponentieel toenemen. Dit geeft bedreigingsactoren meer tijd om bedreigingen in hun aanvalsketen tegen organisaties uit te breiden, waardoor tegelijkertijd het risico op een datalek toeneemt.

Voorraad bijhouden met Jamf betekent:

- actuele, real-time informatie op alle apparaten tegelijk bekijken
- updates en beveiligingsconfiguraties implementeren voor elk apparaat dat niet goed beveiligd is
- Zeg het met ons: **er is geen stap drie**

De mogelijkheid om de voorraadstatus van apparaten in te zien, helpt beheerders om de vinger aan de pols te houden van elk Apple apparaat in hun vloot. Door de huidige status van een apparaat te kennen, kunnen beheerders apparaten en beveiliging efficiënt beheren door te weten welke updates ze waar naartoe moeten sturen en welke beveiligingsfuncties ze respectievelijk moeten configureren. Het maken van slimme groepen, gebaseerd op dynamische criteria, betekent dat beheerders zo gericht of allesomvattend kunnen zijn in updates als ze zelf willen. Of het nu op basis van granulaire machtigingen, specifieke apparaattypes of vrijwel elke andere categorisatiemethode is, Jamf Pro biedt krachtige hulpmiddelen om korte metten te maken met compliance-gerelateerde taken, terwijl je de flexibiliteit behoudt om taken op nul te zetten (of naar alle apparaten in je vloot te sturen) door middel van aanpasbare criteria. Kom er meer over te weten met ons e-book Voorraadbeheer voor beginners.



Compliance van Jamf beheren betekent:

- eindpunten controleren op basis van CIS-benchmarks (Center for Internet Security)
- Stream al je compliancegegevens naar de cloud voor gecentraliseerd beheer
- Toegang tot macOS unified logs en uitgebreide eindpunttelemetrie om bedreigingen snel en efficiënt te identificeren
- Dwing compliance af met behulp van beleidsregels om hersteltaken te automatiseren en eindpunten binnen het bereik te houden
- Monitor op gemeenschappelijke kwetsbaarheden en blootstellingen (CVE) om inzicht te krijgen in de kwetsbaarheden die in je omgeving bestaan
- Voorkom beveiligingsbedreigingen met behulp van uitgebreide analyses die zijn afgestemd op het MITRE &TTACK-raamwerk
- Deel telemetriegegevens veilig tussen beheer- (Jamf Pro) en beveiligingsoplossingen (Jamf Protect) via API om geavanceerde workflows te ontwikkelen om de reactietijd van incidenten automatisch te minimaliseren en geïdentificeerde problemen onmiddellijk op te lossen

IHet is niet genoeg om je apparaten te beveiligen; veel regelgeving verplicht organisaties om te kunnen bewijzen dat apparaten nog steeds veilig zijn en voldoen aan de compliance-eisen. Dit betekent dat organisaties documentatie moeten verschaffen om de complianceniveaus op verschillende momenten in hun tijdlijn te bevestigen. Immers, als je geen bewijs kunt leveren dat het apparaat op een bepaald moment compliant was, dan was het in alle opzichten niet compliant.

De gegevens en rapportage van Jamf bieden organisaties echter de nodige tools om telemetriegegevens van elk eindpunt te verkrijgen en deze gegevens te organiseren aan de hand van kritieke categorisaties, zoals patchniveaus, gedetecteerde kwetsbaarheden en tijdstempels die acties identificeren die tijdens de levenscyclus van het apparaat zijn uitgevoerd. Bovendien kunnen telemetriegegevens dankzij integratie veilig worden gedeeld met tools van derden om gegevens verder uit te breiden via gecentraliseerde dashboards met datavisualisaties en export naar andere formaten voor het delen van compliancerapporten met regelgevende onderzoekers.

6

BOUWSTEEN ZES:

beveiliging en beheer van toepassingen

Patchrapportage, beleidsregels en app-installatieprogramma's om apps up-to-date te houden en de beveiliging eenvoudig af te dwingen.

Beveiliging van toepassingen

Weten dat geïdentificeerde kwetsbaarheden zijn gepatcht, is van vitaal belang voor de beveiliging van het apparaat. Maar weet je waar je apps vandaan komen? En weet je zeker dat ze geen malware of andere kwaadaardige code bevatten? Het antwoord op deze vragen is cruciaal voor je organisatie, want als je je applicatiebronnen niet kunt vertrouwen, loop je het risico dat de beveiliging van je apparaten in gevaar komt, evenals de privacy van eindgebruikers en het blootleggen van gevoelige gegevens.

Apple beschouwt het behoud van veiligheid en privacy als een topprioriteit. Op het gebied van appbeveiliging maken ze apps zo veilig mogelijk om te downloaden en te gebruiken.

Eigenschappen van applicatiebeveiliging en -beheer:

1 **Apps draaien in een sandbox:** elke app draait in zijn eigen unieke ruimte en kan niet communiceren met andere apps. Voordat apps kunnen lezen/schrijven naar/van gedeelde gegevens van anderen, is expliciete goedkeuring nodig van een geverifieerde gebruiker.

2 **Gecentraliseerde en veilige aanschaf van apps:** apps in de App Store van Apple worden doorgelicht om beveiligingsrisico's te beperkena Een deel hiervan wordt bereikt door notariële vastlegging, terwijl het andere deel een veilige, cloud-gebaseerde opslagplaats biedt die door Apple wordt beheerd om apps te hosten die strenge beveiligingsbeoordelingen hebben doorstaan. Het biedt ontwikkelaars ook de mogelijkheid om de nieuwste versie van hun gehoste apps direct in handen van gebruikers te geven, zodat er geen risico's ontstaan door het downloaden van onwettige software uit riskante bronnen.

3 **Notariële vastlegging geeft de integriteit van de beveiliging aan:** door programma's van een notariële akte te voorzien, hebben gebruikers er meer vertrouwen in dat software die is ondertekend met de unieke ID van een ontwikkelaar en naar je Mac is gedownload, door Apple is gecontroleerd op schadelijke onderdelen en problemen met code-signing. Als een app notarieel is vastgelegd, kun je erop vertrouwen dat er niet mee is geknoeid of dat de app is gecompromitteerd.

4 **Gatekeeper blokkeert de uitvoer van verdachte apps:** voordat een macOS-applicatie de eerste keer mag draaien (en na elke volgende update), worden toegewezen notarisatietickets gecontroleerd met Gatekeeper om te bepalen of het ticket geldig is of ingetrokken. Stel dat het eerste het geval is, dan kan de app zonder problemen worden uitgevoerd. Als dit laatste het geval is, wordt de werking van de app beperkt en wordt de gebruiker geïnformeerd dat de app mogelijk is gewijzigd door een onbevoegde partij, waardoor de integriteit van de interne beveiliging wordt aangetast.

5 **Beperkingen op het gebruik van apps:** Op iOS-apparaten is de enige veilige manier om apps te krijgen de App Store. Dat gezegd hebbende, het jailbreaken van iOS- en iPadOS-apparaten introduceert de mogelijkheid om toegang te krijgen tot app stores van derden die vaak worden gebruikt om apps te distribueren die zijn "gekraakt", of waarvan de interne beveiliging is verwijderd, zoals betaalde apps die gratis beschikbaar worden gesteld. Deze apps zijn echter vaak geïnjecteerd met kwaadaardige code door dreigingsactoren om gegevens te stelen of gebruikers te bespioneren. Met een MDM, zoals Jamf Pro, kunnen beheerders waarschuwingen instellen om hen op de hoogte te stellen wanneer jailbroken apparaten worden geïdentificeerd, zodat ze herstelworkflows kunnen uitvoeren om het beveiligingsprobleem op te lossen.

Op macOS kunnen gebruikers (of beheerders met een MDM) kiezen uit twee Gatekeeper-opties:

- Mac App Store
- Mac App Store en geïdentificeerde ontwikkelaars

Door macOS-gebruikers voor hun programma's te beperken tot de Mac App Store, kunnen beheerders de beveiliging van programma's voor het hele apparaat controleren en tegelijkertijd het risico op (schadelijke) bedreigingen door verdachte, riskante en/of gecompromitteerde programma's tot een minimum beperken. Als je echter apps van derden nodig hebt die alleen beschikbaar zijn op de website van de ontwikkelaar, kun je met de tweede optie apps verkrijgen uit zowel de App Store als van geïdentificeerde ontwikkelaars die door Apple zijn doorgelicht en softwarepakketten maken die zijn ondertekend met hun respectieve ontwikkelaars-ID voor een betere beveiliging.

Best practices

Configureer voor macOS het toestaan van de selectie van de Mac App Store en geïdentificeerde ontwikkelaars, vooral als je je eigen programma's maakt of programma's opnieuw verpakt voor implementatie. Vraag ook een developer ID aan bij Apple en onderteken intern ontwikkelde apps door de organisatie zodat Gatekeeper ze zal vertrouwen. Door Jamf Pro als MDM-oplossing te gebruiken, kan de Self Service-appcatalogus worden uitgerold naar alle apparaten, waarbij IT vooraf apps, instellingen, configuraties en nog veel meer goedkeurt voor eindgebruikers, zodat ze toegang hebben tot de tools en diensten die ze nodig hebben en deze kunnen installeren wanneer ze die nodig hebben, zonder dat ze een helpdeskticket nodig hebben, machtigingen hoeven aan te passen of een Apple ID nodig hebben.

Gatekeeper-opties handmatig instellen:

- Navigeer naar: Systeeminstellingen > Privacy en beveiliging > Beveiliging
- Kies uit de twee beschikbare opties
- Herhaal dit voor elk apparaat in je organisatie

Gatekeeper-opties instellen met Jamf Pro:

- stel een configuratieprofiel met je Gatekeeper-instellingen in en implementeer dit op al je apparaten.
- **Dat is alles!**

Applicatie- en beveiligingspatches en updates

Updates van het besturingssysteem, versiebeheer met MDM-commando's, snelle beveiligingsreacties en meer

Organisaties moeten een patchmanagementstrategie implementeren om bugfixes zo snel mogelijk te testen en te integreren om hun hardware, gegevens en gebruikers beschermd te houden. Testen is een vaak over het hoofd geziene noodzaak bij het implementeren van patches, vooral wanneer bugs zichzelf presenteren in de vorm van beveiligingsproblemen die zo snel mogelijk moeten worden aangepakt. Door beide zo snel mogelijk uit te voeren, vermindert IT de impact van beveiligingsrisico's die zich verspreiden, terwijl grotere problemen die voortkomen uit patches die één ding repareren, maar onbedoeld andere, kritischere functies breken, tot een minimum worden beperkt.

In dit hele e-book is de trend van hoe lang administratieve taken die door IT worden uitgevoerd duren, direct gecorreleerd aan het aantal apparaten dat wordt beheerd. Bij het beheren van patches blijft deze regel gelden, op één variabele na: het aantal patches dat moet worden uitgerold kan variëren van weinig tot veel, waardoor de administratieve taken exponentieel toenemen met een onbekende hoeveelheid per apparaat.

Laten we eens kijken naar een aantal opties voor beheerders om patches handmatig en via MDM te beheren:

Opties om patches handmatig te beheren:

- Leer gebruikers om zelf updates uit te voeren zodra ze updatemeldingen op hun apparaten ontvangen.
- Verzamel alle apparaten wanneer er een nieuwe patch wordt uitgebracht en implementeer deze handmatig.
- Herstel apparaten die patches missen als onderdeel van je voortdurende compliancebewakingsprocessen.

Opties voor het beheren van patches via MDM (d.w.z. Jamf Pro):

- Updates en patchmeldingen worden automatisch ontvangen door Jamf, samen met tools om patches uit te rollen naar alle apparaten van je organisatie, zodat je kunt updaten volgens jouw tijdschema - niet dat van iemand anders.
- Met Jamf's Self Service appcatalogus kunnen gebruikers eenvoudig updaten wanneer er een nieuwe patch beschikbaar is door gebruikers te melden dat ze moeten updaten voordat ze een getroffen app kunnen blijven gebruiken.
- Elimineer de afhankelijkheid van eindgebruikers en verlicht de last voor IT door patchdistributie te automatiseren. Stuur patches als beleidsregels naar alle apparaten of richt je op ze met dynamische slimme groepen om ervoor te zorgen dat apparaten up-to-date zijn.

Lees onze whitepaper voor meer informatie over de levenscyclus van apps en het automatiseren en implementeren van apps.

Je beveiliging op een hoger niveau brengen

Als je het nu nog niet geraden hebt, beveiliging is geen 'one-size-fits-all' oplossing. Er zijn lagen voor een allesomvattende strategie die je apparaten, gebruikers en gegevens op holistische wijze zal beschermen en tegelijkertijd ook granulaire beveiligingen zal bieden die samen een digitaal vangnet vormen. Dit wordt defense-in-depth genoemd, wat betekent dat als één laag een bedreiging niet vangt, de volgende laag erboven of eronder is om de bedreiging in te dammen.

Je bent waarschijnlijk al bekend met de gelaagde beveiligingsaanpak en misschien weet je het niet eens. Laten we iets waar je heel vertrouwd mee bent als voorbeeld nemen: je huis.

Met de mix van oude en nieuwe beveiligingen die beschikbaar zijn voor de veiligheid thuis, heb je ongetwijfeld al een aantal (of misschien wel alle) beveiligingen voor je dierbaren en jezelf thuis:

- veiligheidssloten op je deuren
- alarmsysteem thuis
- videocamerabewaking
- beveiligers die op het terrein patrouilleren
- rook- en koolmonoxidedetectoren
- brandblusser
- inboedel- en WA-verzekering

Elk van de bovenstaande oplossingen kan in theorie werken als een op zichzelf staande oplossing voor thuisbeveiliging. Maar op zichzelf biedt het slechts een deel van de totale beveiliging die nodig is, toch? Als je ze echter combineert, passen de verschillende stukjes als een puzzel in elkaar om het volledige plaatje te illustreren en het volledige scala aan problemen aan te pakken. Cyberbeveiliging en het beheer en de beveiliging van je Apple apparaten zijn gebaseerd op vergelijkbare principes, die de kern vormen van het in staat stellen en informeren van gebruikers om goede beveiligingsoplossingen te hebben en te volgen om risico's te minimaliseren en bedreigingen te beperken.

Eén zo'n laag van eindpuntbeveiliging is gewaarschuwd worden voor risico's voor apparaten. Sommige gebruikers kunnen bijvoorbeeld een phishingaanval detecteren en daarom nog niet op een kwaadaardige link klikken; sommige gebruikers zijn misschien iets te goed van vertrouwen en voeren de instructies van de kwaadaardige link uit, waardoor ze mogelijk een risico vormen voor het apparaat, de gebruiker en de gegevens. Hoe kan de getroffen gebruiker weten dat hij op een kwaadaardige link heeft geklikt of een actie heeft uitgevoerd die zijn apparaat of referenties in gevaar heeft gebracht?

Daar is een app voor! Jamf Trust beschermt tegen door de gebruiker geïnitieerde risico's, zoals het bovenstaande voorbeeld van een phishingaanval, door gebruikers op de hoogte te stellen in de vorm van pushmeldingen van Apple wanneer Jamf een bedreiging op hun apparaat detecteert, bijvoorbeeld als die kwaadaardige link waarop eerder werd geklikt kwaadaardige code heeft geleverd in de vorm van malware die op dat moment toetsaanslagen op het apparaat registreert.

De oplossing heeft vastgesteld dat er een bedreiging bestaat en heeft de gebruiker (en ook de beheerder) geïnformeerd. We helpen de gebruiker om zich bewust te zijn van het gevaar en om in de toekomst uit te kijken voor soortgelijke situaties, terwijl IT op het incident kan reageren en het snel kan herstellen door gebruik te maken van een combinatie van Jamf Pro en Jamf Protect om het apparaat in quarantaine van het netwerk te plaatsen, de infectie op te ruimen, de aanwezige kwetsbaarheden te patchen en het apparaat naar de baseline te herstellen. Gebruik tot slot de geleerde lessen voor toekomstige trainingen in beveiligingsbewustzijn voor belanghebbenden.

Apparaat- en gegevensbeveiliging is geen lachertje.

Organisaties hebben de keuze om veel mogelijke aanvallen of gegevensdiefstallen voor te zijn door de sterkst mogelijke beveiliging via Apple te implementeren. Jamf kan dit gemakkelijker, sneller en veel veiliger en efficiënter maken dan handmatige beveiligingsprotocollen.

Niemand houdt van verrassingen op het gebied van cyberbeveiliging en wil al helemaal niet in paniek raken als reactie op een aanval. Ontdek de beste beveiligingsopties voor je organisatie door de productoplossingen van Jamf gratis uit te proberen of neem vandaag nog contact op met een Jamf vertegenwoordiger om te bespreken hoe een op maat gemaakte, allesomvattende oplossing voor Apple beheer en beveiliging eruitziet voor de unieke behoeften van je organisatie.

Je hebt de rest geprobeerd... ga nu voor de beste oplossing!

Probeer Jamf

Of neem contact op met de reseller van Apple apparaten van je voorkeur voor een gratis proefversie.