De kloof overbruggen: macOS-beveiliging

De behoefte aan beveiliging geldt voor elk besturingssysteem en macOS vormt daarop geen uitzondering. Apple heeft veel geïnvesteerd in ingebouwde privacy- en beveiligingsfuncties, maar naarmate het marktaandeel van Apple bij ondernemingen groeit, worden aanvallen op het Mac-platform interessanter voor kwaadwillenden: dat maakt ze een geliefder doelwit voor malware, inbreuken en misbruik van kwetsbaarheden. Meer dan ooit laten bedrijven hun werknemers macOS gebruiken via werknemerskeuzeprogramma's. Daarbij realiseerden zij zich dat net als bij elk ander platform extra beveiliging en zichtbaarheid nodig zijn.

Verschillende beveiligingsleveranciers bieden aanvullende oplossingen om Macs te beschermen, maar veel van deze oplossingen gebruiken een beveiligingsmodel dat specifiek is voor de leverancier en hun Windows-product in plaats van te werken met de moderne frameworks die macOS biedt. Dit maakt het moeilijk om bij te blijven met een steeds veranderend besturingssysteem. De best practice is om het bestaande macOS-beveiligingsmodel uit te breiden, de hiaten op te vullen en de macOS-specifieke mogelijkheden toe te voegen die beveiligingsteams nodig hebben om hun organisatie effectief te beschermen tegen bedreigingen.

In Apple-besturingssystemen vormen privacy en beveiliging de basis voor het platform, met beveiligingen die meteen in de hardware en software zijn ingebouwd. Tegelijkertijd geeft Apple prioriteit aan een intuïtieve ervaring die gebruiksgemak en productiviteit bevordert. Daarom zijn veel functies primair ontworpen voor de individuele gebruiker en niet voor de bredere behoeften van een organisatie, en dat is waar extra zichtbaarheid en beveiligingscontroles waardevol worden.

In ons witboek geven we een overzicht van de huidige staat van macOS-beveiliging en bieden we richtlijnen voor een efficiënte, effectieve en gebruiksvriendelijke manier om de beveiligingsbaseline van Apple te verbeteren.

Je komt meer te weten over:

- details van beschikbare ingebouwde macOS-beveiligingsfuncties
- hoe Jamf deze functies in de onderneming versterkt
- hoe Jamf de detectie van bedreigingen uitbreidt tot meer dan alleen signatures en ingebouwde functies
- aanvullende manieren om het beveiligingsmodel van Apple uit te breiden voor geavanceerde beveiliging van ondernemingen

Applicaties op macOS

Apple heeft veel energie gestoken in het ontwerpen van beveiligingsfuncties om de gebruiker en de apps van derden die ze gebruiken te beschermen. In dit gedeelte zullen we verschillende van deze functies introduceren en bespreken hoe ze strategisch verbeterd en uitgebreid kunnen worden. Ga voor meer inzicht in de beveiligingsfuncties van Apple naar **de uitgebreide platformbeveiligingsgids van Apple**.

Vertrouwen waarmaken met Gatekeeper.

De favoriete en meest vertrouwde manier om apps van derden op Apple-apparaten te installeren is via de App Store. Op die manier kan Apple programma's die niet voldoen aan zijn normen op het gebied van privacy, veiligheid en gebruikerservaring beoordelen en screenen. Apple beperkt echter ook de mogelijkheden van apps in de App Store en veel bedrijfskritische apps zijn niet geschikt voor dit type distributie.

Als distributie via de App Store geen optie is, biedt Apple macOS-ontwikkelaars de mogelijkheid om hun programma's rechtstreeks via gehoste downloads en andere traditionele distributiemethoden te verspreiden. Om deze 'ad hoc'-distributies te ondersteunen, heeft Apple andere controles in het besturingssysteem ingevoerd om het risico van de grootschalige distributie van software over macOS-apparaten te beperken. Gatekeeper is de naam van de functie die centraal staat bij de verificatiecontroles van Apple. Wat in macOS begon als een optie om programma's te laten draaien afhankelijk van hun risicobereidheid, is uitgegroeid tot een uitgebreide en strikte reeks vereisten en beperkingen. De basis acceptatieniveaus om apps toe te laten die zijn gedownload uit de 'App Store' of 'App Store en geïdentificeerde ontwikkelaars' bestaan nog steeds, maar de optie om een problematische of riskante code te draaien blijft gemarginaliseerd.

Merk op dat deze controles alleen gelden voor apps die van het internet zijn gedownload. Apple traceert deze apps door extra metadata aan het gedownloade bestand te koppelen, bekend als het quarantaine-attribuut. Wanneer een programma wordt uitgevoerd, voert Gatekeeper een reeks controles uit, zoals het verifiëren van het quarantaine-attribuut om te bepalen of het kan worden uitgevoerd.Een van deze meest elementaire controles is of de app al dan niet is ondertekend door een rechtmatige ontwikkelaar of is gedistribueerd door de App Store, afhankelijk van de eerder besproken instelling.

Als de app is ondertekend door een ontwikkelaar, wordt het certificaat gecontroleerd aan de hand van een database met ingetrokken signatures om er zeker van te zijn dat de ondertekenaar in het verleden niet in verband is gebracht met malware. Zo kan Apple snel een certificaat intrekken en de grootschalige verspreiding van malware een halt toeroepen.

Vanaf macOS Catalina vereist het slagen voor de Gatekeeper-verificatie ook dat de app door Apple notarieel wordt bekrachtigd. Om door de controle te komen, moet een app worden geüpload naar Apple voor analyse. Bij succesvolle analyse worden notariële gegevens aan de aanvraag gekoppeld om aan te geven dat de aanvraag dit extra inspectieniveau heeft doorstaan.

Het uiteindelijke vertrouwen ligt bij de gebruiker.

In naam van de gebruiksvriendelijkheid laat macOS de eindgebruiker in veel situaties toe om Gatekeeper 'op te heffen'. Een gebruiker kan gewoon met de rechtermuisknop op de app klikken en 'openen' of 'openen met' selecteren. Gatekeeper zal niet botweg weigeren om de app te starten, maar de gebruiker met een nieuwe prompt gewoon waarschuwen dat hij een onbekende of mogelijk kwaadaardige app start. De gebruiker kan de app wel starten. Let wel dat malware die XProtect definitief als zodanig heeft geïdentificeerd niet door een gebruiker mag worden uitgevoerd.

Zodra de app voor de eerste keer is uitgevoerd, wordt de quarantainecomponent bijgewerkt, zodat de acties van de Gatekeeper niet worden herhaald wanneer de app de volgende keer wordt geopend.

⚠ Bedreigingen blokkeren met XProtect en MRT.

De Gatekeeper-suite van technologieën omvat ook de op signatures gebaseerde opsporingsmechanismen van Apple, bekend als XProtect en Malware Removal Tool (MRT). Samen zijn ze in staat om bestanden op het besturingssysteem te scannen, op zoek naar kenmerken binnen bestanden die verband houden met bekende malware. XProtect wordt geactiveerd bij het starten van de app, terwijl MRT periodiek het bestandssysteem scant.

XProtect werkt met een scan-engine voor binaire signatures genaamd Yara. Yara ondersteunt flexibele en krachtige binaire signaturedefinities en een efficiënte executie-engine. Om een app te verifiëren, scant XProtect elke uitvoerbare download bij de eerste uitvoering en na volgende updates. Als er overeenkomende signatures worden gedetecteerd, mag het programma niet worden uitgevoerd. Het bestand met de bekende slechte signature wordt geleverd via onafhankelijke updates voor macOS van Apple. Apple definieert en levert deze signatures naar eigen goeddunken, los van de executie-engine van Yara zelf. Net als Gatekeeper wordt deze scan alleen uitgevoerd als een app het juiste uitgebreide quarantaine-attribuut heeft, dat wordt bijgewerkt na de eerste succesvolle uitvoering van de app.

MRT, daarentegen, wordt op geplande basis uitgevoerd in plaats van tijdens het uitvoeren van een programma en scant het bestandssysteem op specifieke bestandsnamen en artefacten die verband houden met malware uit het verleden en verwijdert deze als ze worden ontdekt. Deze functie is vooral bedoeld om bekende bedreigingen te vinden en te verhelpen die mogelijk al in macOS worden uitgevoerd.

⚙ Gatekeeper uitbreiden naar de onderneming.

Gatekeeper werkt effectief zoals het bedoeld is. Het blokkeert het opstarten van niet-vertrouwde apps en waarschuwt de gebruiker wanneer het een app als verdacht of kwaadaardig identificeert. IT- en beveiligingsbeheerders moeten zicht hebben op pogingen om niet-vertrouwde software uit te voeren op bedrijfsmiddelen. Belangrijker is dat zij zich ervan bewust zijn dat een gebruiker heeft besloten met de rechtermuisknop te klikken en een app te starten, waarmee hij in feite een beveiligingscontrole van het bedrijf omzeilt. Om aan deze behoeften van ondernemingen te voldoen, controleert Jamf for Mac, met zijn eindpuntbeveiligingsoplossing speciaal voor Mac, op aanwijzingen van Gatekeeper-acties en meldt dat de resultaten op een centrale locatie. Zo kunnen IT- en beveiligingsteams hun risico's nauwkeurig beoordelen en weloverwogen beslissingen nemen.

Jamf biedt niet alleen inzicht in de activiteit van Gatekeeper, maar stelt ondernemingen ook in staat het vertrouwensmodel voor ontwikkelaars in eigen hand te nemen door aanvullende ondertekeningsinformatie als niet-vertrouwd in de bedrijfsomgeving te registreren. Met behulp van de nieuwste API voor eindpuntbeveiliging van Apple zal Jamf proactief de uitvoering van elke app op de bedrijfsspecifieke blokkadelijst weigeren. Dit kan worden gedefinieerd op appniveau (app-ID) of op leveranciersniveau (ontwikkelaarsteam-ID)

Bovendien biedt macOS geen signatures of blokkering voor een verscheidenheid aan Grayware (potentieel ongewenste of niet-goedgekeurde software), waaronder veel adware en cryptominer-apps die ongewenst en mogelijk invasief gedrag vertonen. Vaak zijn deze programma's rechtmatig ondertekend door een ontwikkelaar van Apple en stemt de gebruiker er bij de installatie mee in dat zijn gegevens worden verzameld of middelen worden gebruikt — meestal zonder het te beseffen. Daarom bemoeit Apple zich in veel gevallen niet met de werking van deze apps.

In de onderneming is de risicoberekening echter gewoon anders en kan een strengere en gerichtere aanpak gewenst zijn. Daarom dwingt Jamf zijn eigen set beheerde Yara-regels, binaire signatures en niet-vertrouwde ontwikkelaarcertificaten af die worden gebruikt om processen te scannen bij uitvoering, ongeacht of het uitgebreide quarantaine-attribuut aanwezig is of niet. Dit zorgt ervoor dat wanneer nieuwe signatures worden toegevoegd en de onderneming haar beveiligingsbeleid bijwerkt, bestaande apps bij de volgende uitvoering opnieuw worden gescand, niet alleen de eerste keer.

Jamf stelt deze feed van bekende op Mac gerichte malware samen op basis van zijn eigen uitgebreide onderzoek naar macOS-gerichte bedreigingen en gegevens over Mac-bedreigingen van derden. Voor organisaties die nog meer granulaire controle willen over de software die in hun omgeving draait, kunnen ze de lijst van apps die door Jamf zijn geblokkeerd uitbreiden met hun eigen lijst van binaire hashes, TeamID's, enz. Wanneer een app wordt uitgevoerd die overeenkomt met het gedrag of de signature van bekende malware op macOS 10.15 (Catalina) of later, zal Jamf de uitvoering van dat proces voorkomen, het inbreukmakende bestand in quarantaine plaatsen en een waarschuwing registreren dat malware werd voorkomen. Deze operatie vindt plaats buiten de acties van Gatekeeper/XProtect en is ontworpen als een superset van hun functionaliteit. Jamf zal bekende malware identificeren zonder rekening te houden met de quarantaine bit om potentieel onveilige binaries te identificeren en onderhoudt een veel bredere set van malware kennis.

Het vertrouwensmodel van de App Store uitbreiden met Self Service.

In bepaalde situaties kan het gepast zijn om te dicteren welke programma's je gebruikers kunnen installeren door gebruik te maken van een self-service app store die vooraf is gevuld met door IT goedgekeurde ressources.

Jamf Self Service biedt veilige en directe toegang tot ressources door IT in staat te stellen een eigen catalogus met ondernemingsapps te creëren waarmee gebruikers zelf apps kunnen installeren, configuraties kunnen bijwerken en veelvoorkomende problemen kunnen oplossen: zonder dat daarvoor een IT-helpticket nodig is.

Controleer en bewaak het gedrag van apps.

Het gedrag van de app beperken en erkennen met privacycontroles.

In macOS Mojave zijn systeemprivacycontroles geïntroduceerd. Deze controles vereisen dat gebruikers (of ondernemingen) per app toegang verlenen tot specifieke acties en mappen. Als apps eenmaal toegang hebben gekregen tot specifieke acties, zal hen in de toekomst niet meer worden gevraagd wanneer de actie vanuit dezelfde app plaatsvindt. Deze functie zorgt ervoor dat apps expliciet toegang krijgen tot potentieel gevoelige delen van het besturingssysteem (webcam, microfoon, toetsaanslagen, downloads) en zorgt ervoor dat gebruikers langzamer gaan werken en erkennen dat zij apps toegang geven tot privégegevens.

Nietalleen controleren maar het gedrag van apps ook auditen en analyseren.

Hoewel privacycontroles beperken wat apps mogen doen, zullen gebruikers fouten maken en zal er misbruik worden gemaakt van machtigingen. We hebben het er al over gehad hoe Jamf inzicht geeft in de acties van ingebouwde Apple-beveiligingsfuncties en traditionele malware/adware-preventiemogelijkheden om bedrijven op de hoogte en beschermd te houden. Maar bij Jamf geloven we dat een oplossing voor eindpuntbeveiliging daar niet mag stoppen. Jamf levert ook auditing- en monitoringmogelijkheden die traditioneel gereserveerd zijn voor producten voor eindpuntdetectie en respons (EDR), maar met een Apple-first-aanpak en oog voor de normen van privacy en veiligheid die macOS-gebruikers verwachten.

Detectietechniek met Jamf for Mac

De kern van de eindpuntbescherming van Jamf is een agent in de vorm van een lichtgewicht sensor in gebruikersmodus (zonder begeleidende tekst) die gebruikmaakt van een van Apples eigen engines voor het uitvoeren van logica, GameplayKit. Hoewel het gebruik van een game-engine voor het analyseren van beveiligingsgebeurtenissen niet-traditioneel is, stelt het Jamf in staat om nauw geïntegreerd te blijven met het Apple ecosysteem en gegevens op het apparaat te analyseren totdat deze verzameld of gerapporteerd moeten worden. Game-engines zijn ook ontworpen om in realtime een enorm aantal gebeurtenissen te verwerken, waardoor ze perfect zijn voor het analyseren van activiteiten op het moment dat deze op het apparaat plaatsvinden. Zet dit ontwerp eens af tegen de vele beveiligingsoplossingen die eerst op het Windows-platform zijn gericht en vervolgens als bijzaak naar macOS worden geport — of die vereisen dat alle gegevens in de cloud worden verzameld en geanalyseerd.

Een bijkomend voordeel van GameplayKit is dat het, net als Yara, de executie-engine scheidt van de detectiedefinities, waardoor detecties kunnen worden bijgewerkt en uitgebreid zonder dat de kernagent hoeft te worden bijgewerkt. De detectiedefinities zijn ook van Apple zelf. Hiervoor wordt gebruikgemaakt van NSPredicate, een krachtig logisch querymechanisme dat typische querysyntaxis ondersteunt samen met reguliere expressies. Het gegevensmodel van Jamf is speciaal ontworpen om te profiteren van de rijke functies van NSPredicate, inclusief de mogelijkheid om native functies aan te roepen en gegevensmodellen aan elkaar te koppelen. Dit ontsluit mogelijkheden die op andere, meer traditionele manieren rommelig of rekenkundig duur zijn.

Met het gegevensmodel van Jamf en NSPredicate kunnen we bijvoorbeeld:

- Waarschuwen als een bestand zelf is verwijderd, een gebruikelijke techniek om iemands sporen uit te wissen. Deze schijnbaar eenvoudige use case omvat het analyseren van zowel het bestand dat wordt verwijderd als het proces om de verwijdering uit te voeren zonder een dure join operatie of hardcodedetectie.
- Waarschuwen als een niet-ondertekende of verdacht ondertekende binary persisteert als een launch daemon. Hierbij wordt een configuratiebestand geparseerd, een ingesloten binair pad uit de content gehaald en metadata over dat binaire bestand gebruikt in de analyse.
- Waarschuwen als een Microsoft Office-app een onverwacht onderliggend element heeft aangemaakt om Office Macro uitbuiting te identificeren. Dit voorbeeld benadrukt het vermogen om onderliggende/bovenliggende relaties te begrijpen en exploitatie van appfuncties aan het licht te brengen.
- Waarschuwen indien andere 'live-of-the-land'-activiteiten worden gebruikt op manieren die op aanvallen wijzen. Deze klasse van activiteiten vereist toegang tot onderliggend/bovenligggend element en procesgroeprelaties, commandoregel parameters, enz. om misbruik van anderszins onschuldige activiteiten (curl, ssh, python, enz.) aan het licht te brengen
- Volg het USB-gebruik in de hele onderneming en rapporteer metadata over bestanden die naar verwijderbare media worden geschreven.

Om het gemakkelijk te maken om de impact van dit soort detecties te begrijpen, brengt Jamf geïdentificeerde aanvallen in kaart in het MITRE ATT&CK™-framework, indien van toepassing. De dekking omvat nu use cases uit het hele framework, inclusief detectie van technieken in de volgende categorieën:

- persistentie
- initiële toegang
- commando en controle
- defense evasion
- ontdekking
- privilege escalation
- credential access

Verbeterde zichtbaarheid met Mac-native telemetrie

Naarmate organisaties hun macOS-beveiligingsbeleid versterken, wordt dieper inzicht in systeem- en gebruikersactiviteiten belangrijker. Native Apple-frameworks bieden een sterke basis, maar beveiligingsteams hebben vaak rijkere, samenhangende signalen nodig om op schaal afwijkend gedrag te detecteren, incidenten te onderzoeken en compliance te handhaven.

De telemetriemogelijkheid van Jamf berust op de API voor eindpuntbeveiliging van Apple en verzamelt gedetailleerde, macOS-specifieke signalen van elk apparaat. Zo kunnen organisaties systeem-, gebruikers-, applicatie- en netwerkactiviteit nauwkeurig analyseren met behulp van gegevens die de werking van macOS weerspiegelen. Het is een lichte maar krachtige telemetrie die de gebruikerservaring in stand houdt en bestand is tegen knoeien, zodat logboeken en beveiligingsgebeurtenissen betrouwbaar blijven voor onderzoeken en compliance.

Door gebeurtenissen in processen, applicaties, authenticatie, configuratiewijzigingen en gebruikersacties met elkaar in verband te brengen, helpt Jamf-telemetrie beveiligingsteams gedetailleerde tijdlijnen te reconstrueren en gedrag te identificeren dat kan duiden op misbruik of opkomende bedreigingen.

Met Jamf-telemetrie kunnen organisaties:

- Voldoen aan wettelijke en interne compliancevereisten met nauwkeurige, hoogwaardige gebeurtenisgegevens
- Configuratieafwijkingen, schaduw-IT en beleidsafwijkingen detecteren
- Sneller reageren op incidenten door samenhangende gebeurtenissen en aanvalspaden te analyseren
- Proactieve threat hunting ondersteunen met verrijkte, macOS-specifieke inzichten
- Naadloos integreren met SIEM-platforms voor gecentraliseerd overzicht

Deze mogelijkheden vormen een solide basis voor geavanceerde detectie en analyse en bieden daarmee de diepgang en context die nodig zijn om Mac-apparaten op schaal te beheren en te beveiligen. De telemetrie werkt ook naast het macOS Unified Log-systeem, waardoor organisaties zowel verrijkte beveiligingssignalen als gerichte loggegevens kunnen verzamelen voor audits, onderzoeken en compliance.

Eenvoudige verzameling en rapportage van Unified Log

De meeste beveiligingsanalisten en IT-beheerders hebben grote behoefte aan eindpuntlogboeken als onderdeel van een compliance audit of bij het dichten van gaten in andere beveiligingscontroles. Toen macOS overstapte van syslogbestanden naar Unified Logging werd het moeilijker om deze informatie in de hele onderneming te verzamelen, te inventariseren en te inspecteren. De macOS Console-app is geweldig om toegang te bieden tot en inzicht te geven in de Unified Log-infrastructuur op een lokale Mac, maar biedt organisaties niet de mogelijkheid om die gegevens makkelijk te centraliseren.

Met Jamf kunnen clientlogboeken naar een registratiesysteem worden gestreamd zodra ze naar het Unified Log zijn geschreven. Om ervoor te zorgen dat alleen de beoogde gegevens worden verzameld, gebruiken Jamf-beheerders dezelfde predicaatfiltertaal (NSPredicate) als die van het ingebouwde `log stream` opdrachtregelhulpprogramma. Daarmee wordt het opbouwen van registratiesystemen voor Mac-loggegevens een kwestie van eenvoudig configureren, in plaats van het tot vervelens toe per machine verzamelen van die gegevens. Voorbeelden zijn aan- en afmeld-, SSH-, AirDrop- en autorisatiegebeurtenissen. Als gegevens zijn vastgelegd in het Unified Log, kan Jamf die verzamelen.

Afstemmen op de standaarden van Apple.

Ondersteuning op de dag van de release

Voor de uitwisseling met macOS en het verzamelen van de gegevens die nodig zijn voor beveiligingsbeslissingen, maakt Jamf gebruik van native Apple-technologieën. Deze technologieën omvatten opkomende frameworks zoals de API voor eindpuntbescherming van Apple en een protocol voor declaratief apparaatbeheer (een verder ontwikkelde versie van het framework voor apparaatbeheer). Op deze manier minimaliseert Jamf de impact op het apparaat en ontstaan er geen conflicten met wijzigingen in macOS die worden geïntroduceerd in patches of grote OS-releases. Vroeg en vaak patchen is het meest aanbevolen beveiligingsprotocol. Beveiligingstools die zich strikt houden aan ondersteuning op de dag van de release zijn essentieel voor de compliance van dat protocol en een cruciaal onderdeel van een alomvattende defense-in-depth beveiligingsstrategie.

Gebruikerservaring als een functie

Hoewel Jamf voortdurend activiteiten van apps en gebruikers controleert op potentiële bedreigingen, scant het met opzet niet op slapende of Microsoft Windows-gerelateerde malware. Het scannen van bestanden die gewoon op het bestandssysteem staan voor een grote verscheidenheid aan malware signatures draagt vaak in de eerste plaats bij tot een slechte gebruikerservaring. Deze aanpak sluit aan bij Gatekeeper/XProtect in die zin dat bedreigingen worden geïdentificeerd op het moment van potentiële uitvoering, zodat de gebruikerservaring en de gebruikersproductiviteit minimaal worden beïnvloed.

Framework voor declaratief apparaatbeheer

Declaratief apparaatbeheer (DDM), dat werd aangekondigd op WWDC 21, is de verder ontwikkelde versie en update van het protocol voor apparaatbeheer. Met DDM kunnen apparaten proactief beheerinstellingen toepassen, autonoom statuswijzigingen melden en asynchroon communiceren met de MDM-server. Dit is een belangrijke verschuiving van het traditionele opdracht-responsmodel naar een efficiëntere, autonome aanpak.

Privacy

Jamf analyseert gegevens op het apparaat en verzamelt alleen relevante informatie wanneer dat is geconfigureerd, meestal in realtime wanneer een potentieel schadelijke of zeer belangrijke activiteit wordt gedetecteerd. Dit zorgt voor de juiste balans tussen de behoeften van de onderneming en de privacy van de gebruiker, omdat er minder gebruikersgegevens van het apparaat worden gehaald en in de cloud worden opgeslagen. Als kwaadaardige activiteit wordt geïdentificeerd, worden de geïdentificeerde activiteit en de bijbehorende gegevens doorgegeven aan de Jamf-cloudconsole of een geconfigureerd Security Information and Event Management (SIEM)-systeem. Alle specifiek gevraagde gegevens daarbuiten worden ook naar Jamf of het SIEM gestuurd. Door alle overbodige gegevens eruit te filteren, krijgt een beveiligingsanalist die belast is met het monitoren en onderzoeken van incidenten een hoogwaardige verzameling toepasbare gegevens gepresenteerd.

Andere uitbreidingen van het Apple beveiligingsmodel

Beste praktijk: macOS harden

Hoewel Apple enkele van de meest veilige en betrouwbare besturingssystemen levert en ondersteunt, vraagt men zich vaak af welke extra stappen kunnen worden genomen om macOS nog beter geschikt te maken voor je bedrijfsomgeving.

De beste eerste stap is om gebruik te maken van het MDM-framework (Mobile Device Management) van Apple voor geautomatiseerd beheer op schaal. MDM zal je niet alleen helpen je organisatie beter te beschermen, maar zal ook een groot deel van de last van het beheer en de beveiliging van je vloot van IT wegnemen.

Het MDM-framework, dat met OS X 10.7 ("Lion") werd geïntroduceerd, ontsluit een ongelooflijk aantal workflows om de functionaliteit van apparaten af te stemmen op de specifieke behoeften van de organisatie. Configuratieprofielen en beheersopdrachten zijn de twee meest voorkomende manieren om een MDM te gebruiken om ervoor te zorgen dat teams veilig zijn, waar ze ook werken.

Breng beveiliging met MDM naar een hoger niveau door het te combineren met de kracht van Apple Business Manager, een gratis oplossing van Apple voor bedrijven waarmee de aanschaf en het beheer van hardware en meer kan worden geautomatiseerd.

Begin met Apple...

In de loop der jaren heeft Apple een reputatie opgebouwd als een bedrijf dat beveiliging hoog in het vaandel heeft staan en dat is te zien in macOS. Native functionaliteit zoals FileVault 2-versleuteling, verificatie op basis van twee factoren, vergrendeling/wissen op afstand en de mogelijkheid om wachtwoordnormen af te dwingen zijn beschikbaar bij elke nieuwe Mac die aan de omgeving van een organisatie wordt toegevoegd.

Moderne beheer- en beveiligingsplatforms, zoals Jamf, maken gebruik van de nieuwste technologieën van Apple om deze functies een stap verder te brengen en helpen bij het aanpassen van de implementatie, de handhaving en de rapportage van waardevolle beveiligingstools als encryptie.

...Verbeter met Jamf.

Hoewel MDM een geweldige hoeksteen vormt voor elke organisatie, vragen velen zich af wat zij nog meer kunnen doen om hun beveiligingspositie verder te verbeteren en de privacy van werknemers te versterken. Dat is waar Jamf voor kan zorgen.

Het is geen geheim dat apparaatbeheer op een bepaalde schaal een groot beslag legt op de ressources van het team. Meer mensen betekent meer hardware, en meer hardware betekent meer IT-overhead.

Althans, dat was zo voor het ontstaan van platforms als Jamf.

Met gepatenteerde technologie als blauwdrukken en slimme groepen om te helpen bij de organisatie van bedrijfsapparaten en om automatisch beheerfuncties uit te voeren, hebben IT-teams minder tijd nodig voor apparaatbeheer en houden ze meer tijd over voor andere dagelijkse IT-taken. Slimme groepen houden een oogje in het zeil en voegen in realtime apparaten toe aan en verwijderen uit een vooraf gedefinieerde groep naarmate de status van het apparaat verandert.

Modern identiteitsbeheer op macOS

De kern van moderne beveiliging is identiteit — veilige en aangepaste toegang voor eindgebruikers. Verouderde IT vertrouwt op lokale directory services die fungeren als een gecentraliseerde registratie van werknemersinformatie, zoals naam en afdeling. Naarmate de beveiligings- en inzetbehoeften evolueren, moeten bedrijven een nieuwe benadering van identiteits- en toegangsbeheer aannemen als onderdeel van hun ondernemingsstrategie. Met een complete cloudgebaseerde identity stack harmoniseren bedrijven identiteit in hardware en software om functionaliteit en geavanceerde workflows te ontsluiten en uiteindelijk het bedrijf te transformeren.

Cloud-SSO bouwt verder op informatie van directory-services en zorgt ervoor dat eindgebruikers veilige inloggegevens invoeren om bedrijfsmiddelen te gebruiken.

Jamf breidt deze gangbare vormen van identiteitsbeheer uit.

Jamf harmoniseert identiteit in alle bedrijfsapps en de Mac van de gebruiker, met naadloze authenticatieworkflows. Eindgebruikers hebben voordeel van één cloud-identiteit om eenvoudig en snel toegang tot ressources te krijgen die nodig zijn om productief te zijn.

Met Jamf hebben organisaties:

- gestroomlijnde inrichting en authenticatie out of the box voor volledige ondersteuning van medewerkers op afstand en op locatie
- geautomatiseerde synchronisatie van gebruikersidentiteiten en apparaatreferenties
- IT met volledige mogelijkheden voor identiteitsbeheer voor al hun diensten en apparaten
- een Zero Trust Network Access (ZTNA) oplossing ter vervanging van legacy VPN's (virtuele particuliere netwerken) en voldoet aan de behoeften van de moderne, hybride onderneming

reageren op en herstellen van bedreigingen op Mac

Jamf biedt dashboards die organisaties op de hoogte houden van de staat van hun Macs en markeert hardware die aandacht nodig heeft. Met de gepatenteerde slimme groep-functionaliteit kunnen IT-beheerders zich richten op apparaten die moeten worden bijgewerkt of gepatcht om hun beveiliging te verbeteren. Dit gebeurt allemaal op afstand en kan worden geautomatiseerd, dus IT hoeft het apparaat nooit fysiek aan te raken.

Wanneer Jamf Protect wordt gekoppeld aan Jamf Pro, gaat het herstel van bedreigingen nog een stap verder. Met behulp van deze technologie voor slimme groepen kunnen alle MDM- en Jamf-opdrachten worden georkestreerd in reactie op een op activiteiten gebaseerde waarschuwing. Dit omvat automatische netwerkisolatie, mislukte voorwaardelijke toegang, gebruikersmeldingen of een aantal andere gerichte vormen van herstel en respons.

Beveiliging die verder gaat dan apparaatbeheer

Lees ons rapport over de staat van Apple-beveiliging in de onderneming, waarvoor 1.500 IT- en InfoSec-professionals werden ondervraagd. Het omvat het huidige gebruik en de huidige aanpak van apparaten, uitdagingen voor de beveiliging van apparaten en de toekomstige staat van de beveiliging van eindpunten.

Jamf for Mac

Moderne organisaties hebben behoefte aan een uniforme aanpak voor het op schaal beheren en beveiligen van macOS-apparaten. Jamf for Mac ondersteunt dit door de ingebouwde bescherming van Apple te integreren met geavanceerde mogelijkheden als identiteits- en rechtenbeheer, controle op verwisselbare opslag en preventie van bedreigingen. Dit zorgt voor een gelaagde, op Apple afgestemde beveiliging die apparaten in realtime beschermt zonder de vertrouwde macOS-ervaring die gebruikers verwachten te verstoren.

Met Jamf for Mac krijgen organisaties een beter inzicht in de apparaatactiviteit, een betere afstemming op basisrichtlijnen voor compliance en de mogelijkheid om het principe van minimale privileges af te dwingen, verwisselbare media te controleren en webgebaseerde bedreigingen te voorkomen. Deze mogelijkheden helpen de risico's in de hele Mac-vloot te beperken, terwijl de productiviteit van de gebruiker en de naadloze Apple-ervaring behouden blijven.

Door beheer, identiteit en eindpuntbeveiliging samen te brengen in één op Apple gerichte oplossing, stelt Jamf for Mac organisaties in staat om macOS-apparaten holistisch te beschermen en met vertrouwen te werken terwijl hun Mac-implementaties blijven groeien.

jamf

Ga aan de slag
of neem contact op met je favoriete reseller om gratis Jamf te proberen.

www.jamf.com/nl