jamf

WITBOEK

De hiaten opvullen: macOS beveiliging

Ondanks ingebouwde privacy en beveiliging is geen enkel besturingssysteem perfect.

De behoefte aan beveiliging geldt voor elk besturingssysteem en macOS vormt daarop geen uitzondering. Apple heeft veel geïnvesteerd in ingebouwde privacy- en beveiligingsfuncties, maar de waarde van aanvallen op het Mac-platform neemt toe naarmate het marktaandeel van ondernemingen groeit, waardoor ze een geliefder doelwit worden voor malware, inbreuken en het ontdekken 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 waarde toe te voegen die beveiligingsteams nodig hebben om hun organisatie doeltreffend tegen bedreigingen te beschermen.

En hoewel de besturingssystemen van Apple zowel de gebruiker als zijn privacy beschermen, hebben gebruiksgemak en productiviteit altijd de hoogste prioriteit gehad. De Apple ervaring is sterk gericht op de gebruiker en niet op het bedrijf waarin hij werkt. Hetzelfde geldt voor veel van de beveiligings- en privacyfuncties in macOS.

In ons witboek geven we een overzicht van de huidige staat van macOS-beveiliging en geven we richtlijnen over hoe de beveiligingsbaseline van Apple op een efficiënte, effectieve en gebruiksvriendelijke manier kan worden verbeterd.

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. Apple's uitgebreide gids voor platformbeveiliging is te vinden op: **support.apple.com/guide/security**.

Verifieer het vertrouwen met Gatekeeper.

Apple's favoriete en meest vertrouwde manier om apps van derden 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. Op die manier 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. In plaats van botweg te weigeren om de app te starten, zal een nieuwe prompt de gebruiker gewoon waarschuwen dat hij een onbekende of mogelijk kwaadaardige app start, maar Gatekeeper zal hem toestaan dit te doen. Het is belangrijk op te merken dat malware die XProtect definitief 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.

Blokkeer bedreigingen 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 Protect — een eindpuntbeveiligingsoplossing speciaal gebouwd voor Mac — op aanwijzingen van Gatekeeper acties en rapporteert de resultaten naar een centrale locatie, zodat IT- en beveiligingsteams hun risico's nauwkeurig kunnen beoordelen en weloverwogen beslissingen kunnen nemen.

Jamf Protect 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 Protect 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 Protect 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 al dan niet aanwezig is. 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 Jamf's 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 Protect worden 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 Protect 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 Protect 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 ondernemingsapp-catalogus te creëren waar 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.

Beperk en erken het gedrag van de app 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.

Ga verder dan controles en analyseer het gedrag van apps.

Hoewel privacycontroles beperken wat apps mogen doen, zullen gebruikers fouten maken en zal er misbruik worden gemaakt van machtigingen. We hebben al besproken hoe Jamf Protect 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 Protect levert ook auditing- en monitoringmogelijkheden die traditioneel gereserveerd zijn voor Endpoint Detection and Response (EDR) producten — maar met een Apple-first-aanpak en oog voor de normen van privacy en veiligheid die macOS gebruikers verwachten.

Opsporingstechniek met Jamf Protect

De kern van de Jamf Protect-agent is een lichtgewicht sensor in gebruikersmodus (zonder begeleidende tekst) die gebruik maakt 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 een enorm aantal gebeurtenissen in realtime te verwerken, waardoor ze perfect zijn voor het analyseren van activiteiten terwijl ze 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 eigen aan Apple, met behulp van NSPredicate, een krachtig logisch querymechanisme dat typische querysyntaxis ondersteunt samen met reguliere expressies. Het gegevensmodel van Jamf Protect 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. Bijvoorbeeld, met het gegevensmodel van Jamf Protect en NSPredicate kunnen we:

- 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 Protect 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

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 biedt geweldige toegang en zichtbaarheid in de Unified Log-infrastructuur op een lokale Mac, maar het stelt een organisatie niet in staat om eenvoudig die gegevens te centraliseren.

Met Jamf Protect kunnen clientlogs worden gestreamd naar een registratiesysteem zodra ze naar het Unified Log zijn geschreven. Om ervoor te zorgen dat alleen gerichte gegevens worden verzameld, gebruiken Jamf Protect-beheerders dezelfde predicaat filtertaal (NSPredicate) van de ingebouwde `log stream` commandoregelhulpprogramma. Daarmee wordt het bouwen registratiesystemen voor Mac-loggegevens een eenvoudige configuratie in plaats van een vervelende verzameling op een per machine. Voorbeelden zijn het aanmelden en afmelden, SSH, AirDrop en machtigingsgebeurtenissen. Als de gegevens gelogd zijn op het Unified Log, kan Jamf Protect ze verzamelen.

Afstemmen op de standaarden van Apple.

Ondersteuning op de dag van de release

Voor de interface met macOS en het verzamelen van de gegevens die nodig zijn voor beveiligingsbeslissingen, maakt Jamf Protect gebruik van native Apple technologieën. Deze technologieën omvatten opkomende frameworks zoals Apple's Endpoint Security API en het OpenBSM Audit framework voorafgaand. Door deze mechanismen te gebruiken, minimaliseert Jamf Protect de impact op het apparaat en loopt het niet in de pas 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 naleving van dat protocol en een cruciaal onderdeel van een alomvattende defense-in-depth beveiligingsstrategie.

Gebruikerservaring als functie

Terwijl Jamf Protect voortdurend apps en gebruikersactiviteiten 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.

Privacy

Jamf Protect analyseert gegevens op het apparaat en verzamelt alleen relevante informatie wanneer dat is geconfigureerd, meestal wanneer een potentieel schadelijke of zeer interessante activiteit in realtime wordt gedetecteerd. Dit brengt de behoeften van de onderneming in evenwicht met de privacy van de gebruiker, aangezien minder gebruikersgegevens van het apparaat worden gehaald en in de cloud worden opgeslagen. Als een kwaadaardige activiteit wordt geïdentificeerd, worden de geïdentificeerde activiteit en de bijbehorende gegevens doorgegeven aan de Jamf Protect cloud-console of geconfigureerde Security Information and Event Management (SIEM) systemen. Alle specifiek gevraagde gegevens daarbuiten worden ook naar Jamf Protect of de 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. Inheemse 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 beheerplatforms - zoals Jamf Pro, maken gebruik van MDM om deze functies een stap verder te brengen en helpen bij het aanpassen van de implementatie, handhaving en rapportage van waardevolle beveiligingstools zoals 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.

Tenminste, dat was zo vóór vlootbeheerplatforms zoals Jamf Pro.

Met gepatenteerde technologie zoals slimme groepen om bedrijfsapparaten te helpen organiseren en automatisch beheerfuncties uit te voeren, kunnen IT-teams minder tijd besteden aan apparaatbeheer en hebben ze meer vrije tijd 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 verenigen bedrijven identiteit in hardware en software om functionaliteit en geavanceerde workflows te ontsluiten en uiteindelijk het bedrijf te transformeren.

Voortbouwend op informatie van directory services zorgt cloud SSO ervoor dat eindgebruikers veilige inloggegevens invoeren om bedrijfsmiddelen te gebruiken.

Jamf Connect breidt deze gangbare vormen van identiteitsbeheer uit.

Jamf Connect verenigt 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 Connect 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 Pro 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, zodat IT het apparaat nooit fysiek hoeft aan te raken.

Wanneer Jamf Protect wordt gekoppeld aan Jamf Pro, gaat het herstel van bedreigingen nog een stap verder. Met behulp van deze slimme groep-technologie kunnen alle MDM- en Jamf Pro-opdrachten worden georkestreerd in reactie op een op activiteiten gebaseerde waarschuwing van Jamf Protect. Dit omvat automatische netwerkisolatie, mislukte voorwaardelijke toegang, gebruikersmeldingen of een aantal andere gerichte vormen van herstel en respons. Samen met Jamf Pro en Jamf Connect kunnen aanvallen op een gebruiker of apparaat resulteren in opschorting van aanmeldgegevens, wijziging van toegang en allerlei andere herstelmaatregelen rond identiteit.

Beveiliging die verder gaat dan apparaatbeheer

Lees ons rapport over de staat van Apple beveiliging in de onderneming, waarin 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.

Trusted Access

Trusted Access is Jamf's oplossing voor beveiliging voorbij het beheer. Trusted Access is een unieke workflow die apparaatbeheer, gebruikersidentiteit en eindpuntbeveiliging samenbrengt om organisaties te helpen een werkervaring te creëren waar gebruikers van houden en een veilige werkplek die organisaties vertrouwen.

Door Jamf Protect met Jamf Pro en Jamf Connect te gebruiken, kunnen beheerders ervoor zorgen dat alleen vertrouwde gebruikers toegang krijgen tot bedrijfsapps op vertrouwde en conforme apparaten. Als er een probleem is met een geïnfecteerd apparaat, kan het snel worden hersteld en weer in gebruik worden genomen met Jamf Pro.

Trusted Access met Jamf verhoogt de beveiliging van je moderne werkplek drastisch en stroomlijnt tegelijkertijd het werk voor je gebruikers — ongeacht waar het werk plaatsvindt.

Beheer en beveilig Apple voor ongekende voordelen.

Met de juiste tools kunnen IT- en informatiebeveiligingsteams met vertrouwen een Mac-initiatief uitrollen, identiteit en toegang verifiëren en authenticeren, en gebruikers volledig voorzien van de ressources en toegang die zij nodig hebben — en dat alles met het oog op beveiliging en privacy.

Profiteer vandaag nog van de bedrijfsoplossingen van Jamf en geniet van de zichtbaarheid en het herstel die jouw moderne organisatie nodig heeft.

Aan de slag

Of neem contact op met je favoriete reseller om Jamf gratis te proberen.

jamf

www.jamf.com/nl/