jamf

Mobile Threat Defense

voor beginners

Het is een feit: Apple bouwt een van de sterkste kant-en-klare beveiligde platforms op de markt. Het is echter een groeiend platformdoelwit voor vastberaden aanvallers en daarom moeten organisaties worden uitgerust om te reageren op en zich te weren tegen de bedreigingen van vandaag en morgen.

Veelvoorkomende aanvalscampagnes, waaronder phishing, malware en kwetsbare apps, worden gebruikt om apparaten te misbruiken en toegang te krijgen tot bedrijfsresources en gevoelige gegevens, zoals:

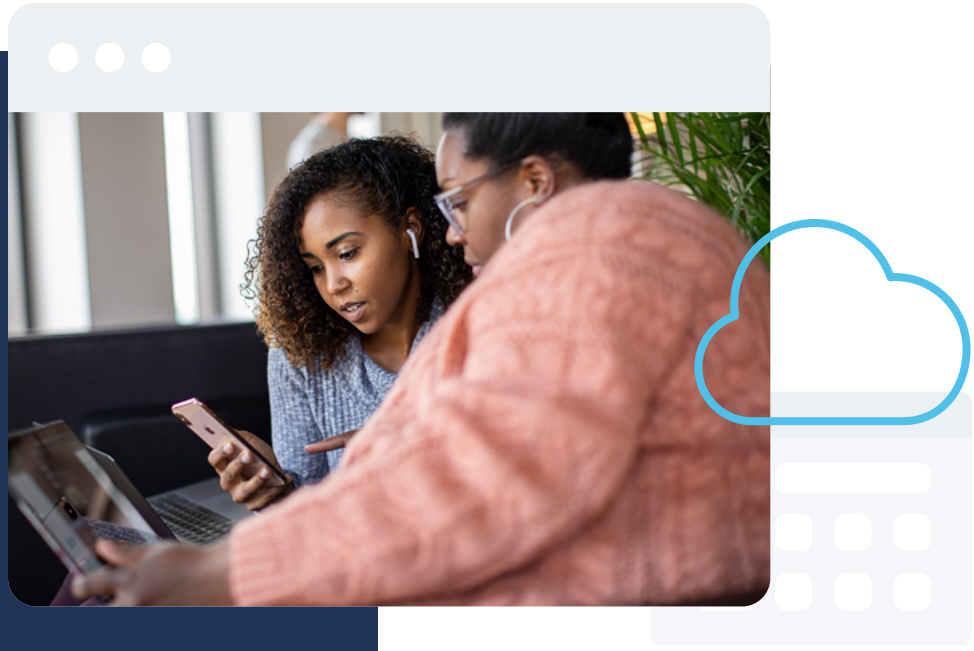
- Exfiltratie van vertrouwelijke informatie
- Toegang krijgen tot bedrijfsservices
- Privacygegevens van gebruikers verzamelen
- Netwerkcommunicatie onderscheppen

Jamf beveiligt je mobiele eindpunten tegen compromittering door detectie van bedreigingen en preventie van zero-day phishing en malware-aanvallen. Dit is een van de belangrijkste punten van zorg voor alle organisaties, vooral voor organisaties die externe of hybride omgevingen hebben geïmplementeerd, gezien de toename van het aantal gerichte incidenten tegen mobiele apparaten door actoren van bedreigingen.

IN DEZE GIDS BESPREKEN WE HET VOLGENDE:

1. Uitgebreide detectie en preventie van bedreigingen
2. Sterke beveiligingen voor elk gebruik
3. Realtime rapportage mogelijkheden
4. Beleidscontroles en voorwaardelijke toegang
5. Uniform operationeel beheer

APPLE IS EEN GROEIEND PLATFORMDOELWIT VOOR VASTBERADEN AANVALLERS...

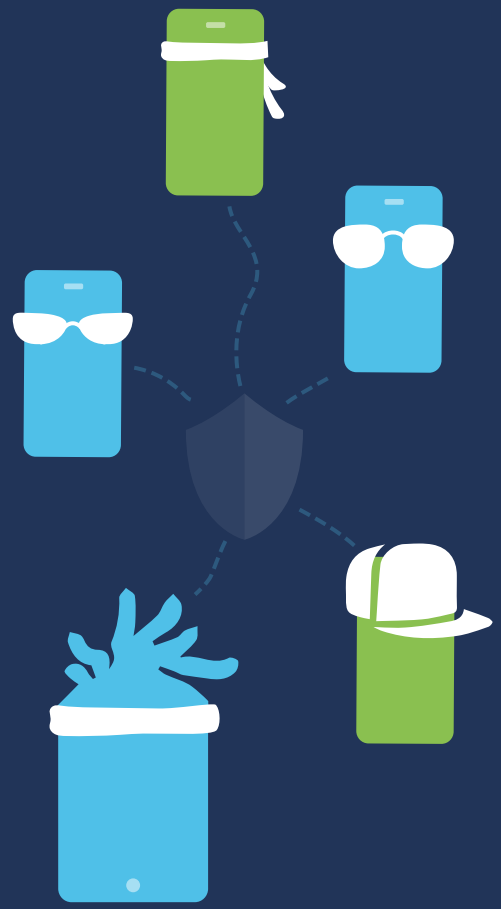


...EN ZE DISCRIMINEREN NIET.

Jamf Protect: de speciaal gebouwde oplossing om mobiele apparaten en je gebruikers te beschermen tegen kwaadaardige bedreigingen met behoud van een lage overhead en een kleine netwerkvoetafdruk met minimale impact op de prestaties van het apparaat en de ervaring van de eindgebruiker.

Organisaties die macOS-apparaten inzetten voor hun gebruikers vertrouwen op Jamf Protect voor eindpuntbescherming om hun vloot te beschermen tegen beveiligingsrisico's, malware te voorkomen en inzicht te geven in de gezondheid van apparaten. Maar hoe zit het met mobiele apparaten, zoals iOS-, iPadOS- en Android-apparaten? Wat voor soort eindpuntbeveiliging is er beschikbaar voor mobiele apparaten die niet alleen voldoet aan hun unieke behoeften, maar ook kan worden geïntegreerd met **Jamf Pro** voor een uitgebreide beheeroplossing?

ZIT JOUW DIGITALE DEUR DICHT?



Voorkom inbraken via de achterdeur: net zoals je je kostbare spullen in je huis beveiligt, moet je gevoelige assets beschermen door de kern te beschermen. In deze gids wordt de kern gevormd door mobiele apparaten. Zij zijn immers het kanaal waar aanvallers zich op richten om toegang te krijgen tot gevoelige gegevens.

41% van de organisaties heeft te maken gehad met een malware-incident op externe apparaten, wat niet alleen opzienbarend veel is, maar ook een aanzienlijke stijging ten opzichte van het voorgaande jaar, volgens het Cloud Security Report 2021. **Lees ons Security 360-rapport voor meer informatie over de beveiligingstrends en -risico's van dit jaar.**

Voor degenen die niet zeker weten wat er achter de piek in incidenten zit, is het antwoord zowel eenvoudig als complex. Door de erosie van de netwerkperimeter als gevolg van een verschuiving naar externe of hybride werkomgevingen, maken gebruikers meer gebruik van mobiele apparaten om productief te blijven terwijl ze niet op kantoor werken. Dat is het eenvoudige gedeelte. Het complexe deel is hoe organisaties hun infrastructuur transformeren om apparaten te beschermen en gegevens te beveiligen.

Jamf minimaliseert de complexiteit en gebruikt een cloud-gebaseerde aanpak, waarbij krachtige, geavanceerde beveiligingstechnologieën worden gecombineerd met extreme flexibiliteit en schaalbaarheid. Inclusief realtime bewaking, detectie en rapportagemogelijkheden, waarmee IT- en beveiligingsteams de gezondheid van hun hele vloot kunnen bewaken.

NETWERK BESCHERMING

Onder de vele beveiligingsrisico's waar moderne bedrijven mee te maken hebben, is phishing slechts één van deze bedreigingen, maar het blijft aantoonbaar de grootste omdat het gericht is op de zwakste schakel in de beveiligingsketen: de gebruiker. De trieste waarheid is dat, zelfs met goedbedoelende en getrainde gebruikers, de foutmarge nog steeds te hoog is, wat betekent dat de succespercentages van compromittering hoog zijn, waardoor aanvallers ze zullen blijven gebruiken in hun aanvalsketen.

Met in-network bescherming kun je zero-day bedreigingen, zoals phishing-websites, actief en in realtime blokkeren. Hierdoor worden apparaten beschermd tegen de effecten van deze campagnes voordat ze een exploitatieve aanval uitvoeren. Door te voorkomen dat het apparaat toegang krijgt tot deze schadelijke domeinen in alle communicatietypes: (bekabeld, wifi of mobiel) kunnen organisaties hun gebruikers en eindpunten beveiligen.

UITBREIDING VAN MOGELIJKHEDEN

Gebouwd met uitbreiding van functionaliteit in het achterhoofd door integratie met het API-framework van een leverancier, heeft Jamf Protect meer Unified Endpoint Management (UEM) en Security Information en Event Management (SIEM) partnerschappen dan andere beveiligingsoplossingen. Dit betekent voor IT en beveiliging dat ze de bestaande investeringen in apparaten, apps en services voor beveiliging en apparaatbeheer kunnen maximaliseren om te profiteren van inzichten in bedreigingen, herstelworkflows en automatisering.

Een uitstekend voorbeeld van integratie is het gebruik van de Jamf risk API naast de functies van Jamf Protect om ongeëvenaarde communicatie mogelijk te maken. Op deze manier worden gegevens in realtime tussen beide systemen gedeeld, waardoor rapportage op maat en herstel van de gezondheid van de mobiele apparaten van je organisatie mogelijk is.

ADAPTIEVE TOEGANG

Jamf Protect werkt onvermoeibaar om de talloze aanvallen met cyberbeveiligingsbedreigingen tegen te gaan die geen tekenen van vertraging vertonen en het mobiele beveiligingslandschap blijven teisteren.

Een van de belangrijkste redenen waarom toegangsgerelateerde bedreigingen zo effectief zijn, is dat als een apparaat gecompromitteerd is en er geen indicatoren zijn die zichtbaar zijn voor de gebruiker (het apparaat blijft schijnbaar normaal werken), de gebruiker nog steeds toegang heeft tot een bron. Het apparaat zal het verzoek verwerken en toegang verlenen, waardoor de bron wordt gecompromitteerd.

Jamf bestrijdt dit tegelijkertijd en verhoogt je beveiligingshouding door alleen beveiligde verbindingen en vertrouwde apparaten toegang te geven tot organisatorische resources. Hoe gebeurt dit?

Door telemetriegegevens en contextuele inputs die uniek zijn voor elk apparaat continu te controleren op afwijkingen.

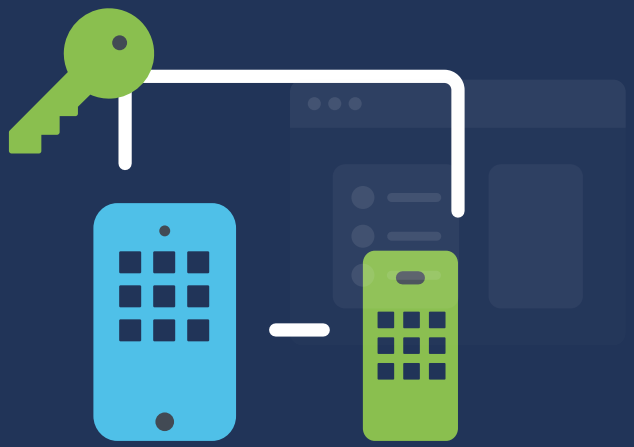
Als wordt vastgesteld dat het eindpunt een hoog risico loopt of gecompromitteerd is, voorkomt Jamf Protect toegang tot resource(s) door het afdwingen van aangepast beleid.

GEAVANCEERDE MACHINE LEARNING

Nadat we hebben gelezen wat Jamf kan doen om je bedrijf en je mobiele apparaten te beschermen, duiken we wat dieper in de basis van de software om je een beter beeld te geven van hoe de software apparaten beschermt tegen bedreigingen. Geen functies op zich, maar eerder een aantal van de ingebouwde defensieve kerntechnologieën die de bovengenoemde functies aansturen.

Even voorstellen: MI:RIAM. Geen vervanging voor Siri, maar eerder een geavanceerde intelligentie-engine die in realtime werkt om het breedste scala aan bekende en zero-day bedreigingen te identificeren. Door gebruik te maken van de grootste verzameling bedreigingsgegevens verzamelt MI:RIAM informatie van 425 miljoen sensoren wereldwijd als input voor zijn algoritmen, waarbij geavanceerde datawetenschap wordt gebruikt om realtime inzicht te bieden in de nieuwste bedreigingsinformatie en actieve risico's.

ALLE APPARATEN WELKOM



Heb je alleen iOS- en iPadOS-apparaten in je vloot? Dat is perfect. Jamf Protect heeft precies het type beveiligingsbescherming dat nodig is om je Apple apparaten en gebruikers te beschermen tegen huidige en opkomende bedreigingen.

Heb je ook andere apparaten in je mobiele apparatenvloot? Dat is ook geweldig! Jamf beveiligt Android- en Windows-besturingssystemen en werkt net zo hard om al je mobiele apparaten te beveiligen. Jamf maakt het voor organisaties mogelijk om meerdere eigendomsmodellen te ondersteunen, zoals bedrijfs- of BYOD-programma's, zonder in te leveren op beveiliging.

Als gebruiker wil je weten dat je beschermd bent. Als lid van je IT- of beveiligingsteam wil je weten op welke manieren je gebruikers worden beschermd. Maar als het op kwaadwillende actoren aankomt, geldt: hoe minder ze weten, hoe beter het is om de beveiliging van je netwerk op peil te houden en, uiteindelijk, informatie veilig te houden. En er zijn verschillende soorten informatie die je koste wat het kost veilig wilt houden om de integriteit ervan te behouden en IT- en beveiligingsteams op de hoogte te houden van de meest recente gezondheidsgegevens van bedrijfseindpunten.

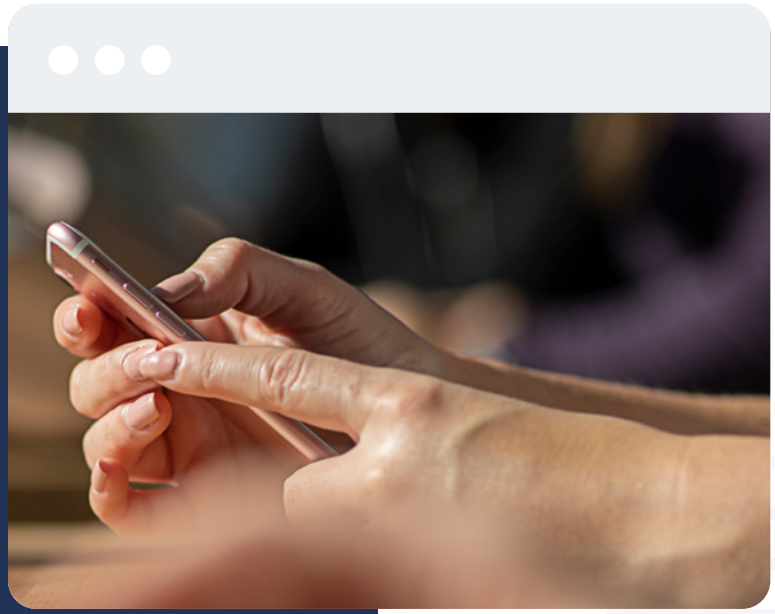
PRIVACY VAN GEBRUIKERS

Persoonlijk identificeerbare gegevens (PII), waaronder persoonlijke gezondheidsinformatie (PHI), behoren tot de belangrijkste gegevenstypen die bedreigingsactoren proberen te bemachtigen. Het is een cyclisch effect: hoe meer ze verzamelen, hoe meer ze de aanval zullen voortzetten en hoe meer ze een middel vinden om hun criminele activiteiten te beëindigen.

Gelukkig beschermt Jamf de online privacy door middel van versleutelde communicatie en bescherming tegen phishingaanvallen. Dit geldt niet alleen voor de persoonlijke gegevens van je gebruikers, maar ook voor gevoelige informatie die nodig kan zijn om aan de regelgeving te voldoen. De geavanceerde privacyfuncties en beleidscontroles voorkomen toegang tot bedrijfsresources en -gegevens door riskante gebruikers of apparaten.

REALTIME INZICHTEN

IT- en beveiligingsteams kunnen gedetailleerde rapporten verkrijgen met betrekking tot de gezondheid van eindpunten door gebruik te maken van de standaard rapportagefuncties die worden meegeleverd of details aanpassen door ze af te stemmen op de specifieke behoeften van je organisatie. Het op maat maken van rapportagefuncties brengt Jamf Protect een stap verder, door beheerders realtime gegevens te verstrekken binnen de console, of deze te exporteren naar een SIEM-partner via de ingebouwde integratiefunctie om gegevens te visualiseren op dashboards. Jamf Protect kan ook gebruikmaken van de API om te integreren met een geïntegreerde beheeroplossing, zoals het koppelen met Jamf Pro, om gegevens te streamen tussen de software, waardoor geautomatiseerd apparaatbeheer en herstel van gedetecteerde eindpuntproblemen mogelijk wordt.



Er is zoveel dat je kunt doen voor je organisatie en je gebruikers om gegevens, apparaten en mensen te beschermen. Er was te veel om in dit e-book te behandelen. Dit is je volgende stap:

Kom meer te weten door het gratis uit te proberen. Je kunt ook samenwerken met de reseller van je voorkeur om te zien wat er mogelijk is met Jamf.

Proefversie aanvragen

We staan te popelen om aan de slag te gaan.