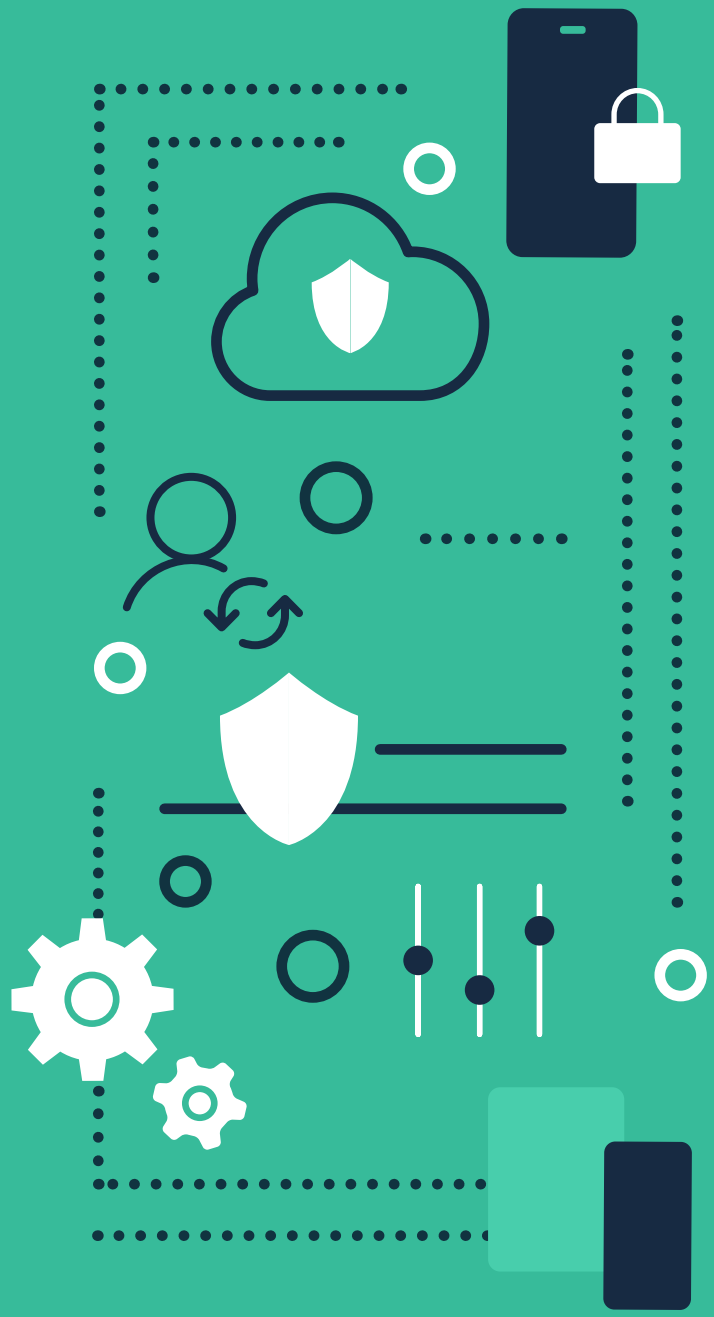


jamf

Mac-eindpunt-bescherming

voor beginners

Native beveiliging is niet het eind(punt)

Er is geen twijfel mogelijk: de Mac is het veiligste apparaat op de markt. Wat al tientallen jaren een waarheid is, geldt nog steeds. Nu organisaties nadenken over de samenstelling van hun vloot, zijn beveiligingsoplossingen voor de bescherming van gegevens, apparaten en gebruikers van cruciaal belang.

Onachtzaamheid kan leiden tot schadelijke of dure inbreuken. Met een oplossing voor eindpuntbescherming die is gemaakt voor Mac, kunnen IT- en beveiligingsteams niet alleen bescherming bieden tegen bekende bedreigingen, maar zich ook blijven aanpassen en anticiperen op toekomstige beveiligingsbehoeften van je organisatie.

Of je nu een onderneming bent met een Apple vloot of een klein bedrijf dat een handvol Macs beheert, Jamf breidt de bescherming van eindpunten verder uit dan wat Apple als native functionaliteit aanbiedt om samen je macOS-apparaten, de gegevens van de organisatie en de eindgebruikers te beschermen.

IN DEZE HANDLEIDING BESPREKEN WE HET VOLGENDE:

- wat Mac-eindpuntbescherming inhoudt
- waarom voor meerdere besturings-systemen ontworpen eindpunt-bescherming onvoldoende is voor Mac

EINDPUNTBESCHERMING OP MAC:

breid het beveiligingsvoordeel van Apple uit en bereid je voor op het onbekende.

Nu het aantal Macs in ondernemingen, kleine bedrijven, scholen en gezondheidszorgorganisaties blijft toenemen, wordt het steeds belangrijker ervoor te zorgen dat apparaten en gegevens worden gebruikt voor legitieme doeleinden, op de juiste wijze en door bevoegde gebruikers.

Om dit te bereiken werken veel bewegende delen — identiteitsbeheer, patching, antivirus (AV), configuratie, eindpuntdetectie en -respons — samen om de behoeften van je IT- en beveiligingsteam te ondersteunen.

Kom meer te weten over het beheer van bedrijfsmiddelen, gegevens en gebruikers met ons e-book Identity Management for Beginners.

IDENTITEITS- EN TOEGANGSBEHEER

Beveiligingsmaatregelen die via identiteitsbeheer worden geïmplementeerd, hebben gevolgen voor zowel eindgebruikers als IT gedurende de hele levenscyclus van de werknemer, ongeacht of deze ter plaatse of op afstand werkt. Zero Trust Network Access (ZTNA)-oplossingen, virtuele particuliere netwerken (VPN's) en SaaS-toepassingen verbinden werknemers met bedrijfsbronnen en bieden allemaal mogelijkheden om je eindpuntbescherming te versterken.

Nu werknemers steeds mobieler worden en op verschillende locaties en op verschillende apparaten werken, moeten organisaties die apparaten en hun bedrijfsgegevens kunnen beheren en beveiligen zonder die apparaten aan lokale Active Directory te hoeven koppelen. Jamf Connect ondersteunt gebruikers vanaf hun eerste tot en met hun laatste werkdag. Met Jamf Connect kan een gebruiker zijn Mac uitpakken, inschakelen en toegang tot al zijn bedrijfsapps krijgen door zich met één set cloudidentiteitsgegevens aan te melden. Met Jamf Connect kunnen organisaties identiteit en toegang bewaken met minimale impact op de eindgebruikerservaring en genieten van consistente prioritering van apparaat- en gegevensbeveiliging.

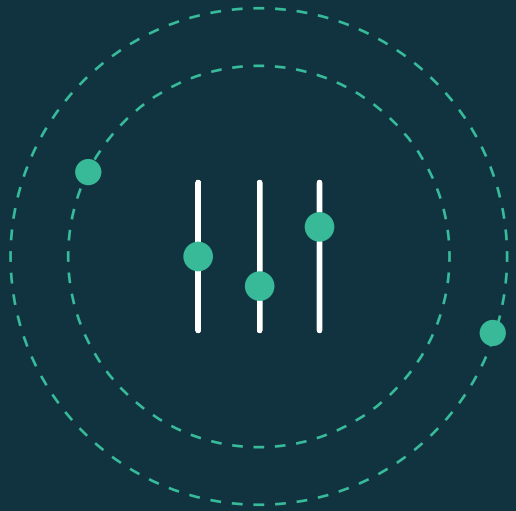
APPBEHEER

Geautomatiseerd appbeheer vereenvoudigt het werk en ondersteunt efficiënte, beveiligde gebruikers.

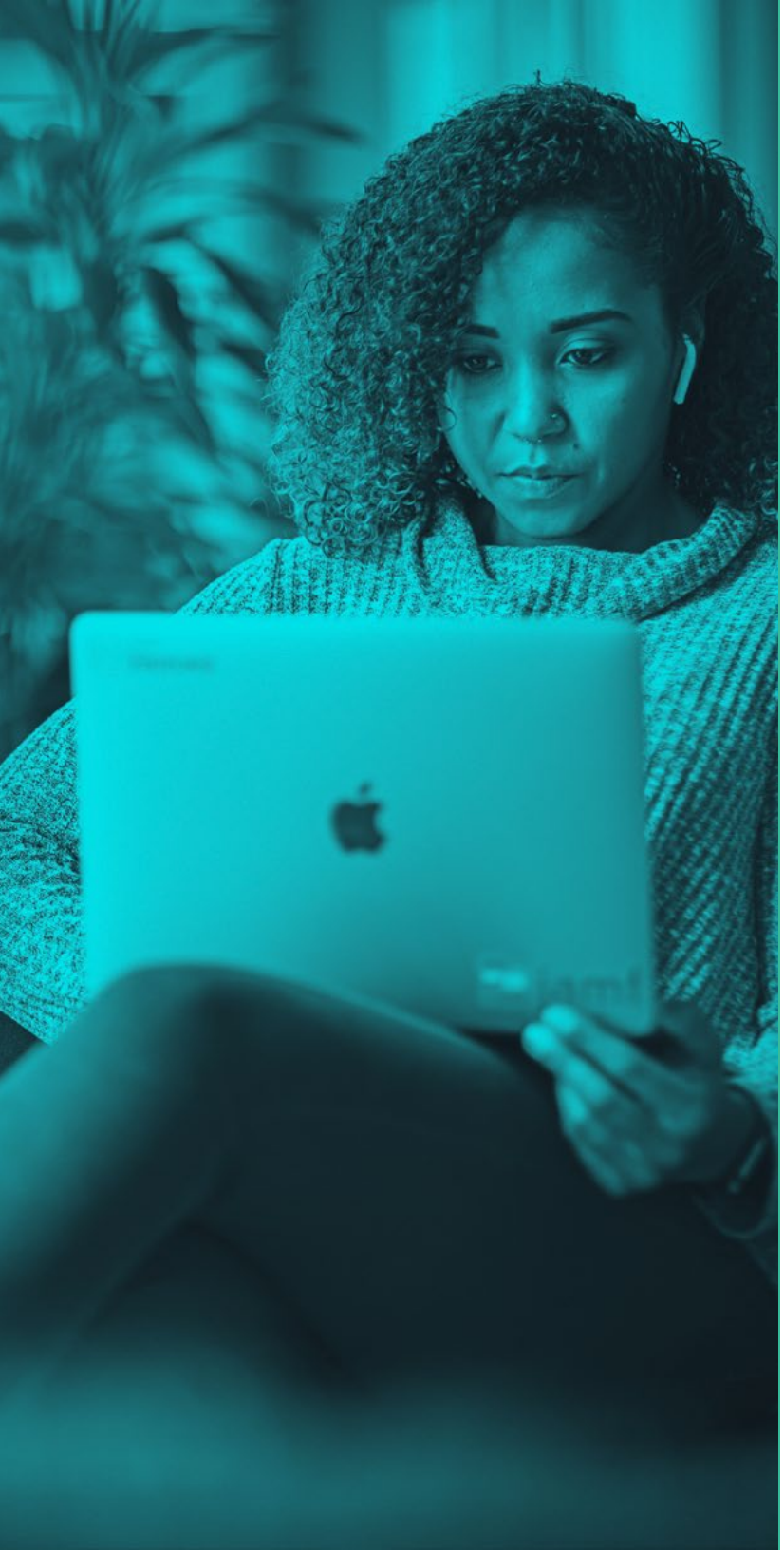
Door ervoor te zorgen dat gebruikers de juiste apps krijgen via beveiligde middelen, zoals Jamf Self Service of de Mac App Store:

- Apps kunnen worden ingezet bij de juiste gebruikers en apparaten
- Aangepaste titels en apps zijn beschikbaar voor gebruikers wanneer ze die nodig hebben
- IT kan updates doorvoeren en eisen stellen die de organisatie en de gebruikers beveiligen

Integreer Jamf Pro met Apple Business Manager om licenties voor apps en software van je organisatie toe te wijzen en te beheren. Bovendien kan Jamf Pro helpen met patching en software-updates. Zo kun je ook eventuele kwetsbare softwareversies bijwerken en beheren en zicht houden op de status van je gehele Mac-vloot. Beveiligingspatches moeten regelmatig en eenvoudig worden uitgevoerd om ervoor te zorgen dat alle bekende kwetsbaarheden van de app worden verholpen. Met Jamf stroomlijn je het werk dat nodig is om applicaties op macOS te onderhouden of bij te werken en biedt je extra zichtbaarheid voor compliance en compatibiliteit, terwijl je een hoogwaardige eindgebruikerservaring levert. Dit betekent ook dat je de nieuwste versie van macOS moet gebruiken zodra die uitkomt, om te voorkomen dat er gaten in de beveiliging vallen door vertragingen bij de upgrade.



Beveiligings- en beheertools mogen geen reden zijn om updates of upgrades van het besturingssysteem uit te stellen. Met Jamf word je niet tegengehouden door de oplossing, maar word je zonder vertraging ondersteund op nieuwe macOS-versies op de dag dat ze uitkomen. Jij bepaalt wanneer je je apparaten wilt upgraden, wij niet.



ANTIVIRUS (AV)

AV kan voelen als een nieuwe behoefte voor Mac, maar er is een nieuwe realiteit. Mac en macOS krijgen meer aandacht naarmate de aanwezigheid ervan in het bedrijfsleven toeneemt.

AV is een basisvereiste voor de meeste organisatorische apparaten om basisbeveiliging te bieden. Apple heeft met XProtect, Gatekeeper en MRT een basis AV-mechanisme in macOS ingebouwd. Deze instrumenten worden echter sporadisch bijgewerkt en organisaties hebben geen zicht op hun acties. Jamf Protect voegt geavanceerde AV-mogelijkheden toe om Mac-malware te voorkomen en in quarantaine te plaatsen en gaat veel verder dan wat Windows-gerichte oplossingen op macOS kunnen bieden.

Organisaties moeten niet wachten tot problemen met malware, adware of andere ongewenste software ontstaan. Zij moeten AV implementeren die effectief Mac-specifieke aanvallen identificeert en verhelpt zonder kostbare middelen te besteden aan het zoeken naar bedreigingen voor Windows op een Mac. Effectieve, efficiënte en uitgebreide Mac AV-mogelijkheden zijn essentieel voor zowel de beveiliging als de apparaatervaring. Tegelijkertijd zal elke AV-oplossing die je eindgebruiker belemmert in zijn mogelijkheden om productief te zijn, alleen maar leiden tot ergernis bij alle betrokkenen. Jamf Protect is ontworpen om macOS tegen malware te beschermen zonder de ervaring te veranderen die eindgebruikers van de Mac verwachten.

Mac AV is niet langer een 'leuk om te hebben', maar een 'noodzakelijk om te hebben'. Je hebt niet alleen AV nodig, je hebt ook voor Mac gemaakte AV nodig, zonder de beperkingen van AV die voor systeemoverschrijdend gebruik is ontworpen.

CONFIGURATIE

De out-of-box beveiliging voor Mac is geweldig — het is de beste die er is — maar met de moderne en steeds veranderende bedreigingen in het cyberbeveiligingslandschap is het niet genoeg. Je moet je beveiliging evalueren en verder ontwikkelen om je apparaten en gegevens te beschermen. En als het verharden van je beveiliging gemakkelijk is, waarom doe je het dan niet?

Er is een aanzienlijke hoeveelheid kennis beschikbaar en binnen de beveiligingsgemeenschap bestaan hiervoor al scripts.

Met Jamf is het eenvoudig om deze te implementeren en uit te voeren en te controleren op gebruikers die deze normen proberen te wijzigen. Jamf neemt de obstakels weg die je er misschien van weerhouden hebben om een basisbeveiliging op je apparaten in te stellen.

FileVault, het inschakelen van firewall en wachtwoordvereisten, het instellen van schermbeveiliging en vergrendelingsvereisten spelen allemaal een rol bij het bepalen van je beveiligingseisen en benchmarks.

Weet je niet waar je moet beginnen? Het Center for Information Security biedt benchmarks voor de sector en Jamf is CIS-gecertificeerd. Met Jamf ben je dus al op weg en we hebben middelen om je te helpen.

Meer informatie over CIS-beveiligingsbenchmarks en Jamf met onze macOS-beveiligingschecklist.

MAC-GERICHTE DETECTIE EN RESPONS

Er bestaan al geruime tijd traditionele EDR-tools (Endpoint Detection and Response) voor Mac, maar de meeste daarvan zijn niet ontworpen om aanvallen die specifiek op Mac zijn gericht effectief te detecteren. In plaats daarvan proberen ze Windows modellen te forceren op Macs. Met Jamf Protect's focus op Mac en macOS, minimaliseert Jamf valse positieven terwijl het de detectiepercentages op Mac maximaliseert.

Wanneer je Jamf Protect koppelt aan Jamf Pro, krijg je minimaal ingrijpende herstelmogelijkheden die veel verder gaan dan de gemiddelde EDR-mogelijkheden. Met Jamf kunnen IT- en beveiligingsteams een naadloos incidentbestrijdingsplan opzetten waarmee je teams kunnen samenwerken.

JAMF IS EINDPUNT-BEVEILIGING.

Mac-eindpuntbescherming met Jamf Protect ondersteunt eindpuntcompliance, voorziet in antivirusbehoeften door het voorkomen van macOS malware, controleert en beveiligt Mac applicaties binnen de organisatie, en detecteert en elimineert Mac-specifieke bedreigingen met minimale impact op de eindgebruiker ervaring.

En in combinatie met Jamf Pro ontsluit Jamf uitgebreide mogelijkheden voor automatisering, onderzoek en herstel om grote en kleine beveiligingsrisico's op eindpunten te beperken.

Vraag een gratis proefversie aan >

of neem contact op met je Apple reseller als je je beveiliging wilt versterken.

Meer informatie over de mogelijkheden voor eindpunt-beschermingvan Jamf.