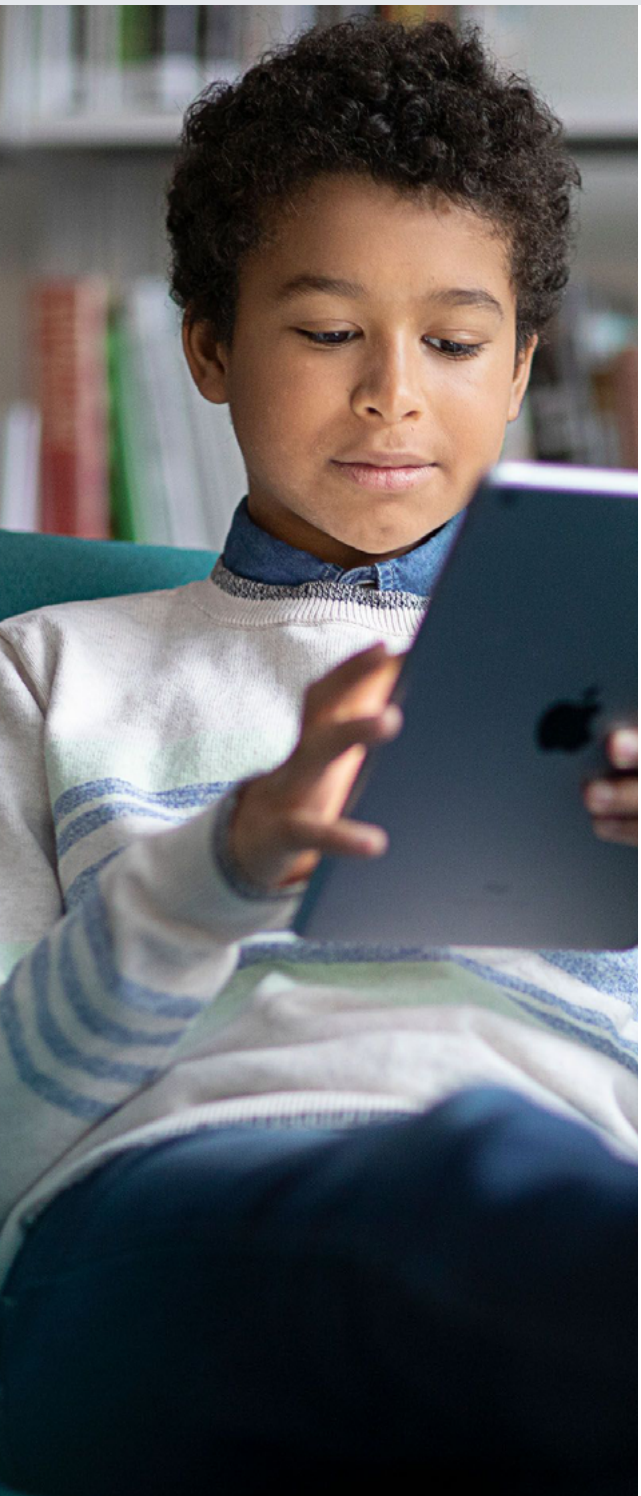
JAMF SAFE INTERNET

Overal waar geleerd wordt veilige, privéverbindingen



Jamf Safe Internet op basis van de engine voor contentfiltering en bescherming tegen netwerkbedreigingen van Jamf is ontwikkeld om scholen te helpen hun leerlingen, personeel en netwerken te beschermen tegen schadelijke content.

Leerlingen brengen bijna twee keer zoveel tijd online door als voorheen. Dat betekent dat er een groeiende behoefte is aan digitale veiligheid om cyberaanvallen uit te sluiten en te voorkomen dat leerlingen toegang krijgen tot onveilige content. Jamf Safe Internet is speciaal ontwikkeld voor onderwijs, contentfiltering en beveiliging met beveiligingstools van Jamf. De oplossing combineert de beste preventie van netwerkbedreigingen en een zeer uitgebreide database voor contentfiltering om onveilige content en kwaadaardige aanvallen zoals malware of phishing te blokkeren, en is geïntegreerd met ons paradepaardje voor het beheer van mobiele apparaten voor het onderwijs: Jamf School.

Cyberbeveiliging die altijd aan staat

In het onderwijs is het essentieel dat netwerken tegen cyberaanvallen worden beschermd, om de continuïteit van het onderwijs te waarborgen, gegevens van personeel en leerlingen te beschermen en andere potentiële risico's die met deze aanvallen gepaard gaan, te elimineren.

Jamf Safe Internet maakt gebruik van tools voor machine learning om phishing, malware, cryptojacking en andere vormen van cyberaanvallen te identificeren en te bestrijden, zodat instellingen en hun netwerken veilig blijven.

Beperkingen afdwingen

Gebruik Jamf Safe Internet om de beperkte modus van YouTube te implementeren en Google SafeSearch af te dwingen. Verberg expliciete content van YouTube's zoekopdracht, opmerkingen en ingesloten YouTube-video's en Google-zoekresultaten.

On-Device Content Filtering (Content filteren op het apparaat (ODCF))

Zorg ervoor dat eindgebruikers de domeinregels niet kunnen omzeilen door sites te bezoeken via IP-adressen. ODCF inspecteert verkeer eerst in een beperkende sandbox en verwijdert gevoelige gegevens wanneer dat de sandbox weer verlaat, en dat levert een krachtige en toch privacybeschermende ervaring voor Apple-gebruikers. *(Exclusief voor Apple)*

Database voor contentfilters

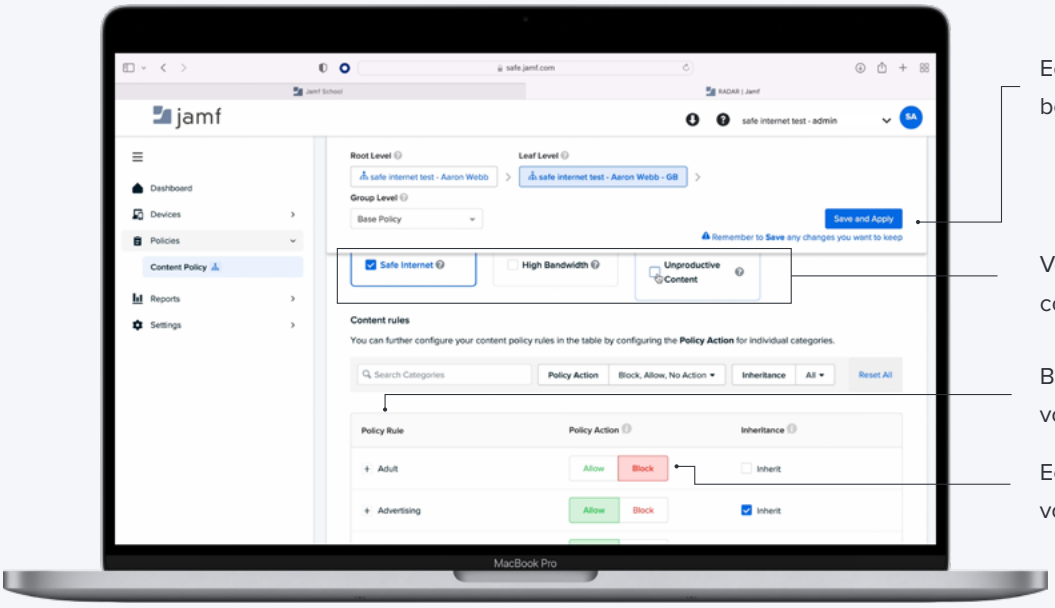
Uitgebreide contentfiltering geoptimaliseerd voor het onderwijs en geïntegreerd met MDM voor eenvoudige, krachtige bescherming van gebruikers. Met behulp van ligchtgewicht, hoogwaardige domeinnaamsysteem (DNS)-technologie stelt Jamf Safe Internet beheerders in staat om de contentfilterresultaten te creëren en aan te passen die passen bij hun schoolbehoeften, zonder inbreuk te maken op de privacy.

Geoptimaliseerd voor het onderwijs

Een console met workflows die specifiek zijn voor de onderwijsbeheerder en een naadloze integratie met Jamf School voor een eenvoudige en intuïtieve implementatie en doorlopende synchronisatie vanaf het platform waar jij het liefst mee werkt. En Jamf Safe Internet integreert ook out of the box met **Jamf Pro** en **Chromebook-** en **Windows-apparaten**.

Aangepaste contentcontroles

Bepaal het beveiligings- en filterbeleid dat past bij jouw behoeften. Of kies gewoon voorinstellingen van Safe Internet en ga aan de slag!



Eenvoudig updates van jouw beleid opslaan en toepassen

Voorgedefinieerde regels om je contentfilterbeleid op te starten

Brede reeks blokcategorieën om de volgende soort inhoud te voorkomen:

Eenvoudige click-to-toggle-functie voor toestaan/blokkeren

Zie hoe Jamf Safe Internet er samen met jouw MDM-platform voor zorgt dat beveiliging en digitale veiligheid centraal in de educatieve ervaring blijven staan.

jamf

www.jamf.com/nl

Ga naar jamf.com/nl voor meer informatie over hoe Jamf Safe internet **leerlingen en gebruikers beschermt.**