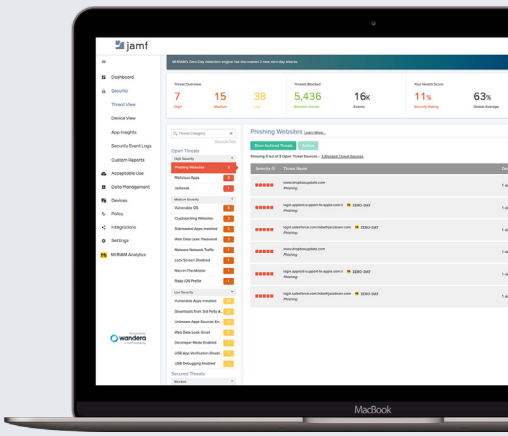
jamf

JAMF THREAT DEFENSE

# Bescherm je devices, applicaties en gebruikers tegen computercriminaliteit

Jamf Threat Defense zorgt voor beveiliging vanuit de cloud die werkt op het device en in het netwerk




## Krachtige eindpuntbeveiliging

Threat Defense detecteert en herstelt het breedste scala van eindpuntbedreigingen, waaronder kwetsbaarheden van devices, malware en riskante apps. Uitgebreide risicobeoordelingen worden continu uitgevoerd om bedreigingen te identificeren, waardoor beveiligingsbeleidsregels kunnen worden afgedwongen in realtime.

## Netwerkbescherming voor gebruikers en data

Stop aanvallen voordat ze beginnen met in-netwerkverdediging. Contentbeveiliging blokkeert kwaadaardige sites, waaronder nooit eerder geziene zero-day phishing-sites ontworpen om zakelijke gegevens vast te leggen. Bovendien voorkomt Threat Defense command-and-control en het ophalen van gegevens door de connectiviteit met riskante sites te blokkeren. Verbindingen worden automatisch beveiligd wanneer person-in-the-middle aanvallen worden gedetecteerd.

## Adaptieve toegang tot je applicaties

Verhoog je beveiligingsniveau door alleen veilige en vertrouwde devices toegang te geven tot zakelijke toepassingen. Threat Defense bewaakt continu een breed scala van telemetrische en contextuele gegevens die kunnen worden gebruikt om toegang tot de applicaties te voorkomen wanneer een eindpunt wordt gecompromitteerd of er een hoog risico hiervoor geldt. Adaptief toegangsbeleid kan lokaal worden afgedwongen via Zero Trust Network Access of de beheeroplossing van Jamf Pro.

jamf

## Uitgebreide detectie en preventie van bedreigingen

### Zero-day netwerkbescherming

Threat Defense identificeert en blokkeert zelfs de meest doordachte aanvallen op het netwerk, met inbegrip van voorheen onbekende, gloednieuwe (zero-day) phishingaanvallen, overname van je systeem (control-and-command) en cryptojacking. De service werkt met elke app, met inbegrip van webbrowsers, e-mailprogramma's, sociale media en sms.

### Realtime risicobeoordeling

Threat Defense evalueert voortdurend de risico's voor je eindpunten – van kwetsbare besturingssystemen tot kwaadaardige profielen. Organisaties kunnen zo snel niet-conforme devices identificeren en echt zero-trust toegangsbeleid handhaven.

### Gedetailleerde app-informatie

Threat Defense zorgt voor uitgebreide details over apps, die bruikbaar zijn voor app-screening en veiligheidsonderzoeken. Elke app krijgt een risicoscore, samen met een gedetailleerd rapport met de rechten en ingebedde URL's die een bedreiging vormen voor de gebruiker en gegevens van de organisatie.

### Dynamische dataversleuteling

Threat Defense biedt realtime versleuteling. Mocht je Wi-Fi-infrastructuur gecompromitteerd zijn, dan blijven gevoelige gegevens geheim. Deze service werkt stil op de achtergrond, zonder actie van de gebruiker.

## Toonaangevende beveiligingsfuncties en -mogelijkheden

### Eindpuntbeveiliging die altijd aan staat

Threat Defense beschermt mobiele medewerkers en devices met een eindpunt-app die kwaadaardige software, kwetsbare configuraties en risicovolle verbindingen identificeert voordat een inbreuk kan plaatsvinden.

### Realtime rapportage en beleidscontroles

Met de unified policy-engine kunnen beheerders snel een beveiligingsbeleid configureren. Er wordt onmiddellijk gehandhaafd, zodat het beleid gaandeweg kan worden afgestemd en aangepast. Gedetailleerde rapporten kunnen worden bekeken in het Threat Defense portaal, of worden geëxporteerd naar externe tools met gebruiksvriendelijke integraties.

### Conditional Access-beleid

Voorkom toegang tot zakelijke applicaties wanneer de ingestelde waarden van je risicodrempels worden overschreden. Het beleid voor voorwaardelijke toegang kan native worden gehandhaafd binnen het netwerk van Threat Defense, of door integratie met Jamf of een identiteitsprovider.

### Verenigde acties en beheer

Threat Defense integreert direct met de beheerinfrastructuur, zodat de service snel kan worden geïmplementeerd op beheerde devices. De integratie vereenvoudigt ook het monitoren van gebeurtenissen en het opsporen van bedreigingen voor ThreatOps door menselijk leesbare namen aan rapportages toe te voegen.

## Jamf Threat Defense werkt naadloos met je bestaande IT-diensten en -technologieën.

Met vergaande integraties met Microsoft, Google, Cisco en meer vergroot je de waarde van je bestaande tech-stack.

jamf

www.jamf.com



Bezoek jamf.com voor meer informatie over hoe Threat Defense gebruikers, mobiele devices en gegevens van je organisatie kan beschermen.