# Dutch IT Awards - Security Innovator of the Year

In een tijdperk waarin mobiele apparaten een onmisbaar hulpmiddel zijn geworden voor moderne werknemers, is het cruciaal om de beveiliging van deze apparaten te waarborgen om waardevolle gegevens te beschermen. Het is algemeen bekend dat de dreigingen van geavanceerde mobiele aanvallen blijven toenemen. Daarom introduceren we met trots Jamf Executive Threat Protection (JETP), een geavanceerde detectie- en reactietool die speciaal is ontworpen voor mobiele apparaten.

Deze oplossing biedt organisaties een efficiënte, externe methode om toezicht te houden op apparaten en te reageren op geavanceerde aanvallen, waardoor de onderzoekstijd aanzienlijk wordt verkort van weken tot minuten.

## Wat maakt JETP zo uniek?

**Bescherming van hoogwaardige doelen**

Terwijl Apple vanaf iOS 16 extreme bescherming biedt voor gebruikers die het doelwit kunnen zijn van geavanceerde digitale bedreigingen, gaat JETP verder. Het identificeert deze geavanceerde digitale bedreigingen en breidt de zichtbaarheid uit naar aanvallen die gericht zijn op gebruikers met een hoge waarde, zoals overheidsfunctionarissen, journalisten en werknemers op hoog niveau.

**Efficiënte detectie en respons**

De eindgebruiker-app verzamelt systeemlogboeken en apparaatinformatie, die wordt geanalyseerd om mogelijke compromittering te identificeren. Hierdoor kunnen gebruikers en organisaties er zeker van zijn dat de integriteit en beveiliging van hun apparaten intact blijven en dat ze onmiddellijk kunnen reageren zodra een potentiële bedreiging wordt gedetecteerd. JETP biedt organisaties ook een ingebouwde toolset voor herstel om geïnfecteerde apparaten snel te herstellen en de integriteit van apparaten met vertrouwen te herstellen.

**Krachtige functies**

JETP is speciaal ontworpen voor gebruik in sectoren zoals overheidsinstellingen, media en entertainment, streng gereguleerde sectoren, olie en gas en energie. Het biedt krachtige functies, waaronder selectieve gegevensverzameling voor mobiel cyberonderzoek, geavanceerde mogelijkheden om bedreigingen op apparaatniveau op te sporen en een uitgebreid analysekader voor het detecteren van mobiele Indicators of Compromise (IOC). Bovendien maakt het automatisch een tijdlijn van verdachte gebeurtenissen, wat cruciale inzichten oplevert in de aard en timing van apparaatcompromitteringen.

JETP wordt ondersteund door Jamf Threat Labs, hooggekwalificeerde professionals op het gebied van cyberbeveiliging, datawetenschap en bedreigingsonderzoek. Deze experts analyseren beveiligingsgegevens van Jamf's uitgebreide klantenbestand om anomalieën en potentiële apparaatcompromitteringen te identificeren en maken deze bruikbare inzichten beschikbaar via Jamf's beveiligingsproducten.

'Mobiele apparaten zijn essentiële hulpmiddelen geworden voor moderne werknemers, die productiviteit en connectiviteit onderweg mogelijk maken. Maar met de opkomst van geavanceerde mobiele aanvallen is het belangrijker dan ooit om de beveiliging van deze apparaten te garanderen om waardevolle gegevens te beschermen,' aldus Dean Hager, voormalig CEO van Jamf. 'Jamf Executive Threat Protection biedt een unieke oplossing die verder gaat dan eindpuntbeveiliging en geavanceerde detectie- en responsmogelijkheden biedt. Dit stelt organisaties in staat om voorop te blijven lopen bij gerichte aanvallen en hun meest risicovolle werknemers te beschermen.'

Meer informatie over [Jamf Executive Threat Protection](https://www.jamf.com/solutions/endpoint-protection/#executive-threat-protection) is beschikbaar op onze website.

Wij zijn van mening dat Jamf Executive Threat Protection een uitzonderlijk innovatief product is dat erkenning verdient in de categorie 'Security Innovator of the Year'. Het biedt niet alleen geavanceerde bescherming voor mobiele apparaten, maar verandert ook de manier waarop we denken over cyberbeveiliging in een wereld waarin mobiele technologie een integraal onderdeel van ons dagelijks leven is geworden.