wandera
a Jamf company

Threat Defense

Bescherm uw devices, gebruikers en applicaties tegen cyberbedreigingen met een cloudgebaseerde beveiliging die actief is 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 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 uw applicaties

Verhoog uw 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 een hoog risico is. Adaptief toegangsbeleid kan lokaal worden afgedwongen via Zero Trust Network Access of de beheeroplossing van Jamf Pro.

Uitgebreide detectie en preventie van bedreigingen

Threat Defense identificeert en stopt het breedste scala van cyberbedreigingen

Realtime netwerkbeveiliging

Threat Defense detecteert dynamisch en blokkeert pogingen om de gegevens van de gebruiker te stelen om ervoor te zorgen dat zelfs niet eerder geziene phishing-aanvallen mislukken. Een breed scala aan factoren wordt gescand zoals merkimitaties, verdachte punycodering en subdomeinentropie. De in-netwerkbeveiliging houdt aanvallen tegen die via e-mail, sociale media en sms worden verstuurd.

Detectie van riskante configuraties

Dankzij diepgaande inzichten krijgen organisaties inzicht in eindpuntrisico's zoals geëscaleerde privileges of verouderde besturingssystemen. Dankzij gedetailleerde controles kunnen beveiligingsbeleidslijnen worden afgedwongen via herstelacties, zoals eindgebruikerswaarschuwingen, het blokkeren van kwaadaardige verbindingen of het beperken van de toegang tot bedrijfsbronnen.

Gedetailleerd inzicht in apps

Begrijp in één oogopslag het risico dat apps vormen, waarbij bekende kwetsbaarheden worden gemarkeerd samen met de app-risicoscore van MI:RIAM en aanbevolen herstelacties. Bekijk gedetailleerde forensische gegevens om inzicht te krijgen in de vereiste machtigingen, de URL waarmee wordt gecommuniceerd of de libraries van derden die door specifieke versies van een app worden gebruikt.

Preventie van onderschepping van communicatie

Openbare wifi-verbindingen zijn ideaal voor kwaadwillenden om aanvallen uit te voeren. Threat Defense beschermt met Failsafe Encryption devices die met wifi zijn verbonden. Wanneer een aanval wordt gedetecteerd, versleutelt Threat Defense automatisch het verkeer van de gebruiker, zodat deze veilig kan blijven werken zonder dat zijn verbinding wordt onderbroken.

Toonaangevende beveiligingsfuncties en mogelijkheden

Robuuste bescherming voor elk gebruik en compatibel met elk willekeurig systeem

Eindpuntbeveiliging die altijd aan staat

Bescherm gebruikers en devices tegen cyberbedreigingen, waar ze ook zijn. De eindpuntsapp van Wandera identificeert kwaadaardige software, kwetsbare configuraties en riskante verbindingen voordat een inbreuk kan plaatsvinden. De herstelacties en waarschuwingen worden automatisch geactiveerd om mogelijke bedreigingen te beperken.

Realtime rapportage en beleidscontroles

Met de unified policy-engine kunnen beheerders snel een beveiligingsbeleid configureren. Er wordt onmiddellijk gehandhaafd, zodat het beleid direct kan worden afgestemd en aangepast. Gedetailleerde inzichten kunnen worden bekeken in het Threat Defense-portaal of in een SIEM/SOAR-dashboard via out of the box-integraties of een reeks API's en datastreams.

Conditional Access-beleid

Voorkom met Conditional Access dat bedrijfstoepassingen door risicovolle gebruikers of devices worden geopend. De rechten van beheerde zakelijke devices en onbeheerde BYO-devices worden ingetrokken totdat ze als veilig worden beoordeeld. De beleidsregels kunnen worden afgedwongen binnen het Threat Defense-netwerk of door integratie met Jamf of IdP.

Verenigde acties en beheer

Door Threat Defense te integreren met een beheeroplossing zoals Jamf of IdP kan informatie over organisatorische gebruikersgroepen worden gesynchroniseerd. Zo kan Threat Defense snel op devices worden ingezet en worden gebruikersrechten eenvoudig toegewezen. De integratie vereenvoudigt ook het monitoren van gebeurtenissen en het opsporen van bedreigingen voor ThreatOps door menselijk leesbare namen aan rapportages toe te voegen.

Aangedreven door MI:RIAM

MI:RIAM is een geavanceerde threat intelligence engine, die in realtime het breedste scala van bekende en zero-day bedreigingen identificeert. MI:RIAM is gebaseerd op de grootste set van bedreigingen, en verzamelt informatie van 425 miljoen sensoren over de hele wereld als input voor zijn algoritmen. MI:RIAM maakt gebruik van geavanceerde datawetenschappen om beveiligingsleiders realtime inzicht te geven in de nieuwste informatie over bedreigingen en actieve bedrijfsrisico's.

Om meer te lezen over hoe Threat Defense gebruikers, mobiele devices en organisatiegegevens kan beschermen tegen kwaadwillige bedoelingen, gaat u naar jamf.com

wandera
a Jamf company