wandera
a Jamf company

# Threat Defense

**Protégez vos appareils, vos utilisateurs et vos applications contre les cybermenaces grâce à une sécurité Cloud qui fonctionne sur l'appareil et sur le réseau.**

## Sécurisation puissante des terminaux

Threat Defense détecte et traite le plus large éventail de menaces pour les terminaux, notamment les vulnérabilités des appareils, les logiciels malveillants et les applications à risque. Des évaluations complètes des risques sont effectuées en permanence pour identifier les menaces, ce qui permet d'appliquer les politiques de sécurité en temps réel.

## Les défenses du réseau protègent les utilisateurs et les données

Arrêtez les attaques avant qu'elles ne commencent avec des défenses au sein du réseau. La protection du contenu bloque les sites malveillants, y compris les nouveaux sites de phishing zero day conçus pour capter les informations d'identification de l'entreprise. De plus, Threat Defense empêche l'exfiltration des commandes et des données en bloquant la connectivité avec les sites à risque. Les connexions sont sécurisées automatiquement lorsque une attaque de l'homme du milieu est détectée.

## Accès adapté à vos applications

Renforcez votre position en matière de sécurité en autorisant uniquement les appareils sécurisés et fiables à accéder aux données des applications d'entreprise. Threat Defense surveille en permanence un large éventail de données télémétriques et contextuelles qui peuvent être utilisées pour empêcher l'accès aux applications lorsqu'un terminal est compromis ou à haut risque. Des politiques d'accès adaptatives peuvent être appliquées nativement par la solution Zero Trust Network Access ou par la solution de gestion Jamf Pro.

# Détection et prévention complètes des menaces

Threat Defense identifie et arrête le plus large éventail de cybermenaces.

### Protection du réseau en temps réel

Threat Defense détecte et bloque dynamiquement les tentatives de vol des informations d'identification de l'utilisateur afin de garantir l'échec des attaques de phishing, même celles qui n'ont jamais été vues auparavant. Un large éventail de facteurs est analysé, tels que l'imitation de marques, les punycodes suspects et l'entropie des sous-domaines. La protection au sein du réseau bloque les attaques envoyées par e-mail, réseau social et SMS.

### Détection de configuration risquée

Des évaluations détaillées des positions offrent aux organisations une visibilité sur les risques liés aux terminaux, de l'escalade des privilèges aux systèmes d'exploitation obsolètes. Les contrôles granulaires permettent d'appliquer les règles de sécurité par le biais d'actions correctives, telles que l'envoi de messages à l'utilisateur final, le blocage des connexions malveillantes ou la restriction de l'accès aux ressources de l'entreprise.

### Aperçu détaillé de l'application

Comprenez le risque que posent les applications rapidement. Les vulnérabilités connues sont mises en évidence, de même que le score de risque de l'application MI:RIAM et les mesures correctives recommandées. Il est possible d'examiner des données détaillées pour comprendre les autorisations requises, les URL communiquées ou les bibliothèques tierces utilisées par des versions spécifiques d'une application.

### Prévention de l'interception des communications

Les connexions Wi-Fi publiques constituent une plateforme idéale pour les acteurs malveillants qui souhaitent lancer des attaques, c'est pourquoi Threat Defense protège les appareils connectés au Wi-Fi grâce à Failsafe Encryption. Lorsqu'une attaque est détectée, Threat Defense chiffre automatiquement le trafic de l'utilisateur, ce qui lui permet de continuer à travailler en toute sécurité sans interrompre sa connexion.

# Excellentes fonctionnalités et capacités de sécurité

Une protection forte pour chaque type d'utilisation, et compatible avec tous les systèmes

### Défense des terminaux toujours active

Protégez les utilisateurs et les appareils contre les cybermenaces, où qu'ils soient. L'application Wandera identifie les logiciels malveillants, les configurations vulnérables et les connexions à risque avant qu'une violation de sécurité ne puisse avoir lieu. Des mesures correctives et des alertes sont déclenchées automatiquement pour atténuer les menaces potentielles.

### Rapports et contrôles des règles en temps réel

Le moteur de règles unifié permet aux administrateurs de configurer rapidement une règle de sécurité. L'application est immédiate, ce qui permet d'ajuster et de personnaliser instantanément les règles. Des informations détaillées sont disponibles dans le portail Threat Defense ou dans un tableau de bord SIEM/SOAR grâce à des intégrations prêtes à l'emploi ou à une suite d'API et de flux de données.

### Règles d'accès conditionnel

Empêchez les utilisateurs ou les appareils à risque d'accéder aux applications professionnelles avec l'accès conditionnel. Les autorisations des appareils professionnels gérés ou personnels non gérés sont révoquées jusqu'à ce que les appareils soient évalués et marqués comme sûrs. Les règles peuvent être appliquées nativement dans le réseau Threat Defense ou via l'intégration avec Jamf ou un IdP.

### Exploitation et gestion unifiées

L'intégration de Threat Defense à une solution de gestion comme Jamf ou un IdP permet de synchroniser les informations sur les groupes d'utilisateurs d'une organisation. Cela permet de déployer rapidement Threat Defense sur les appareils et facilite l'attribution des autorisations aux utilisateurs. L'intégration simplifie également la surveillance des événements et la recherche des menaces par les professionnels du ThreatOps, en ajoutant des noms lisibles aux rapports.

## Alimenté par MI:RIAM

MI:RIAM est un moteur de renseignement avancé sur les menaces ; il travaille en temps réel pour identifier le plus large éventail de menaces connues et de type zero day. Bâti sur le plus grand ensemble de données sur les menaces, MI:RIAM collecte des informations provenant de 425 millions de capteurs dans le monde entier pour alimenter ses algorithmes. MI:RIAM utilise une science des données avancée pour fournir aux responsables de la sécurité un aperçu en temps réel des dernières informations sur les menaces et les risques pour l'entreprise.

Rendez-vous sur jamf.com pour en savoir plus sur la manière dont Threat Defense peut protéger les utilisateurs, les appareils mobiles et les données de l'entreprise contre les actions malveillantes.

wandera
a Jamf company