MTD – Mobile Threat Defense : La solution pour la sécurité mobile

Principaux avantages de MTD

Garantir une protection permanente

MTD utilise des algorithmes d'apprentissage automatique (Machine Learning) optimisés pour une exécution en continu sur vos périphériques. Les menaces connues et de type « Zero Day » sont ainsi détectées et corrigées, même lorsque vos périphériques sont hors ligne.

Améliorer la visibilité sur les menaces

Obtenez une visibilité immédiate et permanente sur les menaces susceptibles d'affecter l'ensemble de vos périphériques mobiles, ainsi que des analyses détaillées sur les applications à risque.

Assurer une adoption à 100 % par les utilisateurs

L'activation de MTD sur les périphériques mobiles recensés dans Ivanti UEM s'effectue sans interaction de l'utilisateur ni déploiement d'application.

Protéger vos périphériques des menaces mobiles

Dans l'Everywhere Workplace, les périphériques mobiles constituent des ressources essentielles pour l'entreprise. Les collaborateurs les utilisent pour accéder à tout, ou presque. Et comme les mesures de sécurité mobiles mises en place par ces utilisateurs sont médiocres, voire inexistantes, les pirates en profitent.

Avec Ivanti Mobile Threat Defense (MTD), vous protégez aussi bien les périphériques Android et iOS de l'entreprise que ceux qui appartiennent aux collaborateurs. Vous pouvez surveiller et gérer les périphériques, et les protéger contre les attaques survenant au niveau du périphérique, du réseau ou des applications. La solution permet aussi de prévenir les attaques par hameçonnage mobile.

De par son fonctionnement, Ivanti MTD se distingue des autres solutions. En effet, il envoie en mode push une action de conformité locale qui détecte les menaces mobiles connues et celles de type « Zero Day » et y remédie même si vos périphériques mobiles sont déconnectés du réseau Wi-Fi ou cellulaire. De plus, l'activation de MTD sur les périphériques mobiles recensés dans Ivanti UEM s'effectue sans aucune intervention de l'utilisateur. L'entreprise peut ainsi obtenir un taux d'adoption utilisateurs de 100 % et s'assurer que tous les périphériques sont protégés contre les menaces mobiles.

Fonctionnalités de MTD

Détection des menaces et application de la remédiation depuis le périphérique

La protection par Apprentissage automatique installée sur le périphérique est capable de contrer les attaques au niveau du périphérique, du réseau ou des applications, ainsi que les attaques par hameçonnage. Le périphérique mobile reste protégé même lorsqu'il est déconnecté du réseau.

Antihameçonnage multivecteur

Pour une efficacité optimale, l'Apprentissage automatique et la recherche d'URL d'hameçonnage peuvent être élargis au Cloud de façon à étendre le périmètre des recherches. Non seulement, les fonctions d'antihameçonnage de la solution détectent les attaques par hameçonnage pour tous les vecteurs d'infection mobile (e-mail, messages texte et SMS, messages instantanés, réseaux sociaux, etc.) mais elles permettent aussi d'y remédier.

Approche proactive en matière de remédiation

Des actions de conformité basées sur des stratégies déclenchent des alertes en cas de comportement dangereux, bloquent proactivement les attaques, isolent les périphériques infectés de votre réseau, et suppriment les applications malveillantes et leur contenu afin de réduire la durée d'exposition aux codes d'exploitation et de bloquer les attaques de type « Zero Day ».

Rapports détaillés

Grâce aux tableaux de bord et aux rapports, vous bénéficiez d'une plus grande visibilité sur les risques encourus par vos périphériques, OS, réseaux et applications. Vous disposez ainsi d'informations exploitables qui vous permettent de réagir rapidement et efficacement face aux différents vecteurs de menace.

Intégration UEM

L'activation de MTD sur les périphériques mobiles recensés dans Ivanti UEM s'effectue sans intervention de l'utilisateur ni déploiement d'application. L'entreprise obtient ainsi un taux d'adoption utilisateurs de 100 %. De plus, elle peut définir et appliquer des stratégies de mise en conformité pour s'assurer que les utilisateurs ne peuvent ni désactiver ni supprimer MTD de leur périphérique.

Exemples en situation réelle

MTD vous protège des attaques intervenant au niveau du périphérique, du réseau et des applications, ainsi que des attaques par hameçonnage.

Attaques par code d'exploitation au niveau du périphérique

Suite à l'envoi de plusieurs MMS à des utilisateurs ciblés, un code d'exploitation « zero click » a été déclenché, sans aucune interaction utilisateur. Il a provoqué une exécution de code à distance permettant d'élever les privilèges d'un cyberattaquant qui a pu ainsi se déplacer latéralement sur le réseau.

Attaques réseau

Une entreprise a été ciblée par une attaque MITM (Man-In-The-Middle) via son réseau WIFI. Cette attaque a été lancée depuis un café situé à proximité des locaux. Les utilisateurs du réseau étaient redirigés vers une page de harponnage, depuis laquelle des données d'entreprise ont été dérobées.

Applis malveillantes

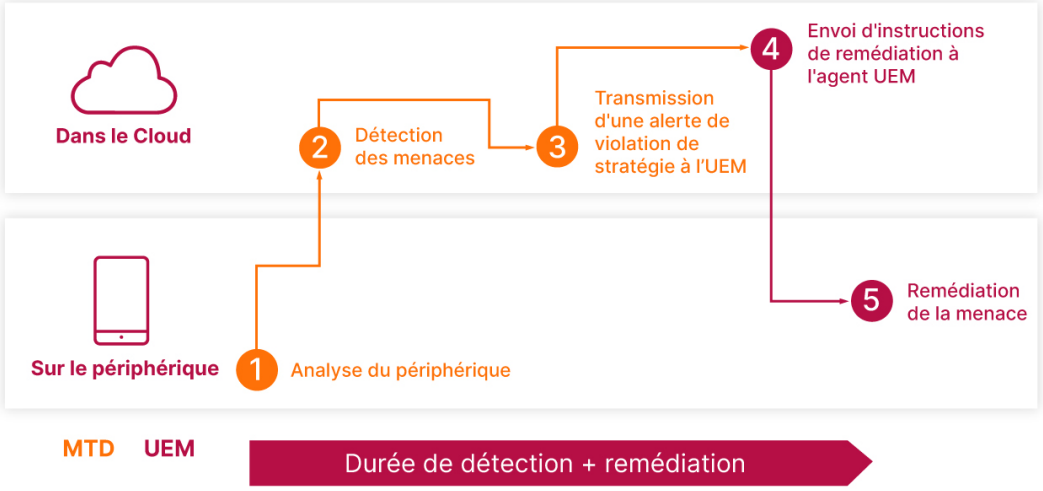
Des utilisateurs peu méfiants ont installé une appli depuis un App Store tiers. Suite à une utilisation abusive des permissions, cette appli a exécuté un code d'exploitation sur leur périphérique, fait fuiter des données et servi d'arme pour s'infiltrer dans les réseaux internes par mouvement latéral, en vue de rechercher des données encore plus sensibles.

Attaques par hameçonnage

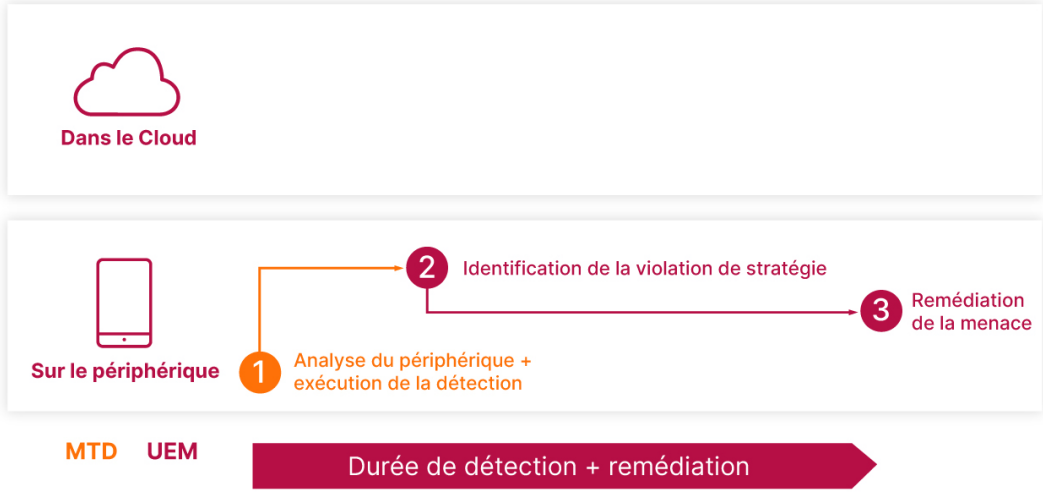
Par une technique d'ingénierie sociale, un cyberattaquant a manipulé un utilisateur peu méfiant pour qu'il clique sur un lien et communique ses identifiants au réseau d'entreprise. Le pirate a ainsi pu se connecter sous le nom de cet utilisateur et accéder à des ressources de l'entreprise.

Détection des menaces et remédiation

Autres solutions de protection contre les menaces



Solution Ivanti MTD



À propos d'Ivanti

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et aux applications du département IT sur différents réseaux, afin de rester productifs en travaillant de partout. La plateforme d'automatisation Ivanti Neurons connecte les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service aux utilisateurs. Plus de 40 000 clients, dont 96 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs biens IT, du Cloud à la périphérie, ainsi que pour fournir une expérience utilisateur d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Pour en savoir plus, visitez le site www.ivanti.fr/.

ivanti

www.ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr