Mobile Threat Defense: La solución para la seguridad móvil

Claves del MTD

Garantizar protección en todo momento

MTD utiliza algoritmos de aprendizaje automático optimizados que se ejecutan de forma permanenteen el dispositivo, lo que permite detectar y corregir las amenazas conocidas y de “día cero”, incluso cuando el dispositivo está desconectado.

Mejorar la visibilidad de las amenazas

Obtenga visibilidad inmediata y permanente de las amenazas maliciosas en todos los dispositivos móviles y análisis detallados de las aplicaciones de riesgo.

Alcanzar un 100 % de adopción por parte de los usuarios

Para activar el MTD en los dispositivos móviles inscritos en Ivanti UEM, no se requiere ninguna interacción con el usuario ni es necesario desplegar una nueva aplicación.

Protección contra las amenazas móviles

En el actual Everywhere Workplace, los dispositivos móviles son un recurso esencial para la empresa. Los empleados los utilizan para acceder a prácticamente todo. Y,dado que la mayoría de los usuarios tienen medidas de seguridad móvil insuficientes, o incluso inexistentes, los piratas informáticos se benefician de ello.

Ivanti Mobile Threat Defense (MTD) permite proteger los dispositivos Android e iOS, tanto corporativos como de los empleados, de las posibles amenazas más sofisticadas. Esto permite a las empresas supervisar, gestionar y proteger los dispositivos contra los ataques que se producen en los niveles de dispositivo, red y aplicación, así como prevenir los ataques de suplantación de identidad móvil.

A diferencia de otras soluciones, Ivanti MTD impulsa una acción de cumplimiento local que detecta y remedia en el dispositivo tanto las amenazas móviles conocidas como las de “día cero”, incluso si no está conectado a una red wifi o móvil. Por otro lado, no se requiere ninguna interacción del usuario para activar MTD en los dispositivos móviles inscritos en Ivanti UEM. Esto ayuda a las empresas a lograr una plena adopciónpor parte de los usuarios, garantizando así que estén protegidos de las amenazas móviles.

Funciones del MTD

Detección y reparación en el dispositivo

La protección basada en el aprendizaje automático en el terminal contra los ataques a nivel de dispositivo, de red, de aplicación y de suplantación de identidad, mantiene la seguridad de los dispositivos móviles incluso cuando no están conectados a la red.

Protección multivectorial contra la suplantación de identidad

El aprendizaje automático de MTD y la búsqueda de URLs de suplantación de identidad pueden ampliarse eincluir la detección en la nube, mejorandoasí su eficacia. La capacidad de la solución para luchar contra la suplantación de identidad, permite detectar y remediar los ataques de suplantación de identidad en todos los vectores de amenazas móviles, incluidos el correo electrónico, los mensajes de texto y SMS, los mensajes instantáneos y las redes sociales, entre otros.

Enfoque proactivo de reparación

Las acciones de cumplimiento basadas en políticas ofrecen alertas de comportamientos de riesgo, cierran proactivamente los ataques en el dispositivo, aíslan los dispositivos comprometidos de su red y eliminan las aplicaciones maliciosas y su contenido, limitando el tiempo de exposición a una posible explotación y detener los ataques de “día cero”.

Informes detallados

Los paneles e informes le ayudan a obtener visibilidad y conocimiento de los riesgos de los dispositivos, el sistema operativo, la red y las aplicaciones, y proveende información procesable para que pueda responder con rapidez y eficacia a los vectores de amenaza.

Integración de UEM

Para activar el MTD en los dispositivos móviles inscritos en Ivanti UEM, no se requiere ninguna interacción con el usuario ni es necesario desplegar una nueva aplicación, lo que ayuda a impulsar la adopción por parte del 100 % de los usuarios. Además, se pueden crear y aplicar políticas de cumplimiento para evitar que los usuarios desactiven MTD o lo eliminen de su dispositivo.

Ejemplos prácticos

MTD protege contra los ataques a nivel de dispositivo, de red, de aplicación y de suplantación de identidad.

Explotación de dispositivos

Tras el envío de mensajes MMS a los usuarios objetivo, se activó un exploit encadenado de cero clics sin ninguna interacción del usuario, lanzando una ejecución remota de código que elevaba los privilegios del actor malicioso y permitía el movimiento lateral en la red.

Ataques a la red

En una cafetería cercana a su oficina, un ataque de intermediario vía wifi contra una empresa redireccionó a los usuarios a una página de suplantación de identidad desde la que se extrajeron los datos corporativos.

Aplicaciones maliciosas

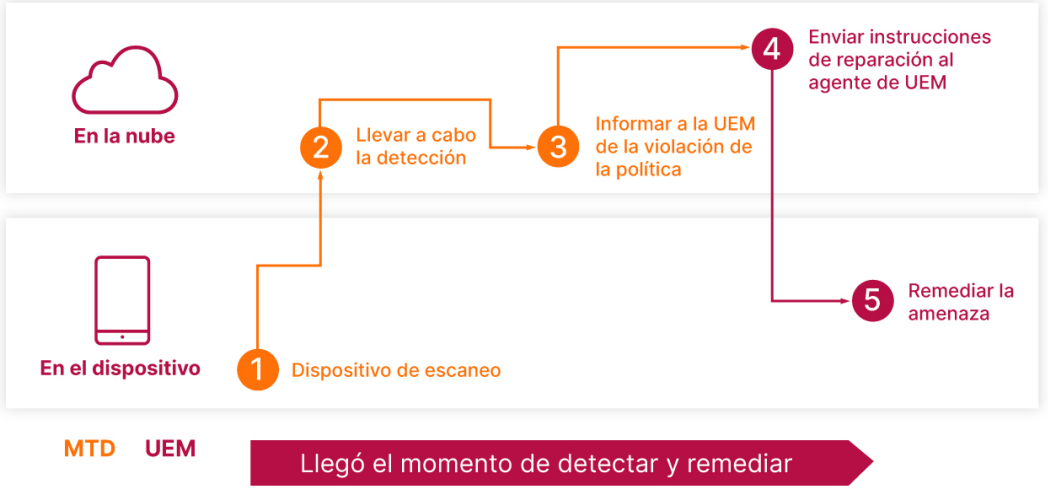
Los usuarios, ajenos a esto, instalaron una aplicación de una tienda de aplicaciones de terceros. La aplicación abusaba de los permisos, ejecutaba un dispositivo de explotación, filtraba datos y se utilizaba como herramienta para penetrar en las redes internas a través del movimiento lateral en busca de más datos sensibles.

Ataques de suplantación de identidad

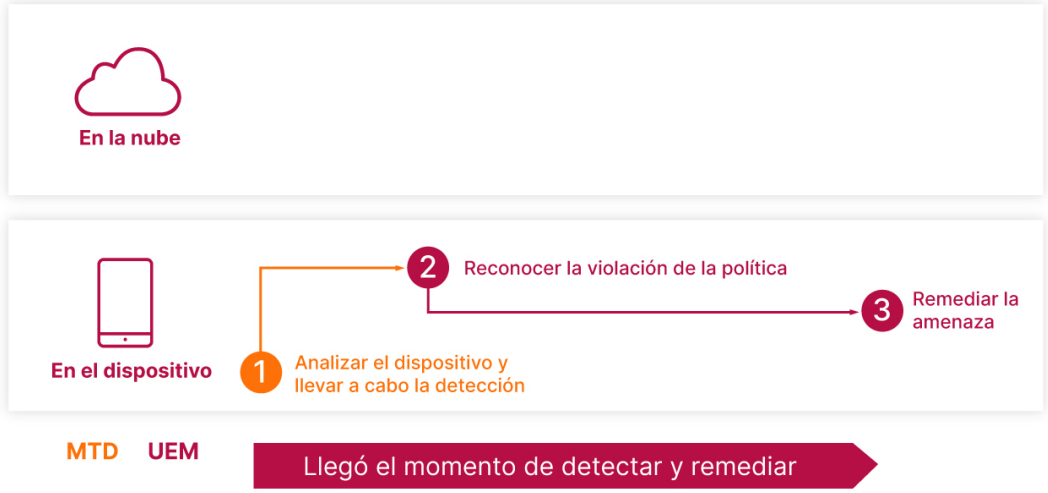
Aprovechando la ingeniería social, un actor malicioso engañó a un usuario ingenuo para que hiciera clic en un enlace y desvelarasus credenciales de acceso a la empresa. Así, el atacante pudo iniciar sesión como si fuera el usuario y acceder a los recursos corporativos.

Detección y reparación

Otras soluciones de protección y defensa contra amenazas



Solución Ivanti MTD



Sobre Ivanti

Ivanti hace posible el Everywhere Workplace. En el teletrabajo, los empleados utilizan un sinfín de dispositivos para acceder a las redes y aplicaciones de TI, y a los datos a través de diferentes redes para mantener su productividad mientras trabajan desde cualquier lugar. La plataforma de automatización delvanti conecta las soluciones líderes del sector de gestión unificada de dispositivos, seguridad de confianza cero y gestión de servicios empresariales, proporcionando un panel único para que las empresas puedan autocurar y autoproteger susdispositivos, permitiendo el autoservicio a los usuarios finales. Más de 40.000 clientes, entre los que se encuentran 96 de las 100 empresas de la lista Fortune, han optado por Ivanti para descubrir, gestionar, proteger y dar servicio a sus activos de TI desde la nube hasta el terminal, ofreciendo excelentes experiencias de usuario a los empleados, dondequiera y comoquiera que trabajen. Para más información, visite ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com