¿UEM? ¿MTD? Por qué se necesitan ambos

Protección completa de extremo a extremo contra las amenazas móviles

UEM

Gestión unificada de puntos finales

Permitir que los dispositivos compatibles accedan al correo electrónico, las aplicaciones y los datos corporativos.

Asegurar los datos entre el dispositivo móvil y la red corporativa.

Separar los negocios de todo lo personal mediante contenedores.

Aplicar una política basada en el riesgo.

+

MTD

Mobile Threat Defense

Detección de ataques conocidos y desconocidos en el dispositivo, con aprendizaje automático y desde el día cero.

Evaluación inicial del riesgo del entorno.

Detección en tiempo real de amenazas avanzadas de dispositivos, redes, aplicaciones y suplantación de identidad.

Acciones de resolución y MDM en tiempo real.

Análisis detallado de amenazas con información de contexto, exportación a SIEM o herramientas orientadas a la detección de amenazas.

Ivanti y Zimperium se han asociado para proporcionar una completa solución de seguridad móvil empresarial que ofrece una protección avanzada contra las amenazas en el lugar de trabajo “en cualquier parte”. Esta solución protege contra la suplantación de identidad, y también protege y soluciona los ataques a nivel de dispositivo, red y aplicación.

Conjuntamente, Ivanti y Zimperium permiten a las empresas gestionar y proteger los dispositivos móviles contra la gran variedad de ataques. Zimperium detecta y analiza continuamente las amenazas y proporciona a Ivanti la visibilidad necesaria para aplicar políticas basadas en el riesgo, con el fin de proteger los dispositivos móviles para evitar comprometer la red corporativa y sus activos.

La solución integrada ofrece a los responsables de la seguridad informática una forma de habilitar de manera segura tanto los equipos suministrados por el gobierno (GFE) como los dispositivos propios (BYOD), y alcanzar el equilibrio entre permitir a los empleados móviles ser más productivos con el dispositivo de su elección y, al mismo tiempo, proteger los dispositivos móviles y a la empresa contra las amenazas avanzadas.

Beneficios clave

Diseñado desde la base para dispositivos móviles, el motor de protección contra amenazas móviles z9 de Zimperium utiliza tecnología de aprendizaje automático optimizada para funcionar en el dispositivo sin conexión a Internet. Su enfoque no invasivo para asegurar el dispositivo proporciona protección las 24 horas del día sin afectar la experiencia del usuario ni vulnerar su privacidad. Mobile Threat Defense (MTD) se integra con el cliente Ivanti UEM, lo que permite a los responsables de la administración impulsar la adopción del 100% de los usuarios.

Cumplimiento de la normativa

NIST 800.53

La Publicación Especial 800-53, Revisión 4, proporciona un enfoque más global de la seguridad de la información y de la gestión de riesgos al ofrecer a las empresas la amplitud y profundidad de los controles de seguridad necesarios para reforzar fundamentalmente sus sistemas de información y los entornos en los que operan dichos sistemas, contribuyendo a que los sistemas sean más resistentes frente a los ciberataques y otras amenazas. El motor z9 MTD de Zimperium potencia el MTD y detecta los ataques de acceso público a la red, el código malicioso a las aplicaciones y al sistema operativo, la respuesta a las incidencias en el dispositivo y los análisis de vulnerabilidad de su personal móvil.

NIST 800.124

Publicación especial del NIST 800-124 Rev. 2 La sección 4.2.3 dice: "Los sistemas MTD están diseñados para detectar la presencia de apps maliciosas, ataques basados en la red, configuraciones inadecuadas y vulnerabilidades conocidas en las apps móviles o en el propio SO móvil". Mobile Threat Protection de Zimperium proporciona una monitorización continua, en tiempo real, del dispositivo, el sistema operativo, la red, el fraude y las aplicaciones. Además, el análisis avanzado de aplicaciones z3A de Zimperium realiza una validación de 20 puntos en todas las aplicaciones del entorno y es capaz de detectar interacciones inesperadas entre aplicaciones, aplicaciones que contienen código defectuoso o erróneo, CVEs que no han sido abordados o acceso a PII.

Marco de trabajo MITRE ATT&CK®

Una base de datos de acceso global sobre las tácticas y técnicas de los atacantes, basada en observaciones del mundo real. Para contrarrestar los ataques, el análisis de aplicaciones MTD premium ayuda a detectar y solucionar el marco de ataque.

Cómo se integra Zimperium con Ivanti:

Facilidad de implantación y actualización

El motor z9 de Zimperium ya está integrado en nuestro agente UEM. Esto significa que la solución ya está desplegada en el dispositivo y solo requiere su activación. La configuración se realiza añadiendo nuestro UEM a zConsole y habilitando la activación desde el UEM para empezar a proteger los dispositivos. No se requiere ninguna interacción con el usuario y no es necesario instalar una nueva aplicación.

Proteja su infraestructura corporativa

Cuando el MTD detecta que un dispositivo ha sido amenazado, puede proporcionar una solución rápida para evitar el ataque. En función del ataque y de la configuración, Ivanti puede llevar a cabo un amplio conjunto de acciones de protección, entre las que se incluyen la finalización de la conexión de red, la denegación de IP/dominios específicos y la puesta en marcha de acciones de cuarentena específicas. Además, el servidor Ivanti puede aplicar políticas de cumplimiento basadas en el riesgo para solucionarlas en función de la gravedad de la amenaza. Las políticas pueden desactivar temporalmente las conexiones del dispositivo móvil a los servicios corporativos (correo electrónico u otras aplicaciones, wifi y VPN) o incluso eliminar las aplicaciones corporativas del dispositivo. Estas acciones detienen la propagación de la infección y evitan el riesgo para los datos corporativos.

Alerta e información

Ivanti ofrece un extenso análisis forense de las amenazas móviles junto con notificaciones al usuario final y alertas al administrador configurables por tipo de ataque para adaptarse a las necesidades de cualquier empresa. Las políticas de recopilación de datos sobre la privacidad se suministran para cumplir también con la normativa regional.

Capacidades	UEM	MTD	MTD Premium
Soporte para dispositivos iOS y Android.	✓	✓	✓
Proporcionar una postura inicial de riesgo de seguridad para el sistema operativo/dispositivo, la red, las aplicaciones y el fraude.	✓	✓	✓
Detectar si el dispositivo tiene activada la seguridad física adecuada (código pin, encriptación a nivel de dispositivo).	✓ Basic	✓	✓
Detectar si el dispositivo está dañado por el usuario (utilizando valores hash conocidos y la ubicación del archivo).		✓	✓
Proporcionar información sobre las herramientas y técnicas de compromiso o ataque a un dispositivo.		✓	✓
Detecta explotaciones del SO/Kernel y USB, cambios de perfil/configuración, manipulación del sistema.		✓	✓
Detectar ataques de aumento de privilegios.		✓	✓
Detectar ataques a la red (ataque de intermediario, redes wifi y móviles fraudulentas).		✓	✓
Detectar el robo de SSL, el SSL falso y los intentos de interceptar el tráfico SSL.		✓	✓
Detectar a los ataques que realizan exploraciones de reconocimiento.		✓	✓
Detectar la suplantación de identidad, el “smishing”, la suplantación de URL, la “tiny URL”, etc.		✓	✓
Entrega y retirada de aplicaciones corporativas.	✓		
Compartir documentos corporativos de forma segura.	✓		
Aplicaciones seguras de línea de negocio.	✓		

Capacidades	UEM	MTD	MTD Premium
Detectar aplicaciones maliciosas, programas maliciosos conocidos y desconocidos, amenazas dinámicas mediante descarga y ejecución.		✓	✓
Revoque el acceso a los dispositivos móviles no conformes.	✓		
Proporcionar un análisis exhaustivo de las amenazas móviles.		✓	✓
Aplique una política basada en el riesgo que incluya el bloqueo o el bloqueo selectivo de los dispositivos amenazados.	✓	✓	✓
Proporcionar una solución instantánea en cuanto se detecta una amenaza.		✓	✓
Analizar las aplicaciones desarrolladas internamente para detectar problemas o riesgos de privacidad y seguridad.			✓
Recibir información sobre privacidad y seguridad de las aplicaciones instaladas en el dispositivo.			✓
Detección de amenazas	**UEM**	**MTD**	**MTD Premium**
Amenazas críticas y elevadas relacionadas con la red			
Dispositivo Android: posible intento de manipulación		✓	✓
Proceso anómalo		✓	✓
Opciones de desarrollo		✓	✓
Encriptación de dispositivos	✓	✓	✓
PIN del dispositivo	✓	✓	✓

Detección de amenazas	UEM	MTD	MTD Premium
Amenazas críticas y elevadas relacionadas con la red			
Las detecciones de fugas/root en dispositivos con acceso a la red MDM son sencillas y pueden evitarse fácilmente. Además, MDM no proporciona ninguna visibilidad de tipo forense sobre las herramientas y técnicas utilizadas en el ataque.	✓	✓	✓
Aumento de privilegios		✓	✓
El sistema de archivos ha cambiado		✓	✓
Aplicaciones con carga lateral		✓	✓
Sistema operativo Linux desactivado		✓	✓
Manipulación del sistema. Se trata de un compromiso avanzado del dispositivo que puede utilizar o no el paso adicional de la fuga de datos (jailbreaking) o el rooting del dispositivo.		✓	✓
Aplicación de iOS sospechosa		✓	✓
Aplicación de Android sospechosa		✓	✓
Perfil no fiable		✓	✓
Modo de depuración USB activado		✓	✓
Versión de Android vulnerable		✓	✓
Versión de iOS vulnerable		✓	✓

Detección y prevención del fraude			
Detección y bloqueo continuo de URLs de phishing.		✓	✓
Detección de suplantación de identidad en el dispositivo.		✓	✓
Inspección mejorada de URLs de suplantación de identidad en el servidor externo.		✓	✓
Detección de suplantación de identidad siempre activa y bloqueo de las URL de estafa procedentes de todas las aplicaciones y de todo el tráfico de Internet en el dispositivo, incluidas las acciones de reparación local.		✓	✓
Amenazas críticas y elevadas relacionadas con la red			
MiTM		✓	✓
MiTM - ARP		✓	✓
MiTM – ICMP REDIRCT		✓	✓
MiTM – Banda SSL		✓	✓
MiTM – banda de SSL falsa		✓	✓
Descenso de SSL/TLS		✓	✓

Sobre Ivanti

Con Ivanti, trabajar desde “cualquier parte” es posible. 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 varias redes para seguir siendo productivos mientras trabajan desde cualquier lugar. La plataforma de automatización Ivanti conecta las soluciones líderes del sector de gestión unificada de puntos finales, seguridad de confianza cero y gestión de servicios empresariales, proporcionando un panel único para que las empresas puedan autocurar y autoproteger los dispositivos, y autoservir a los usuarios finales. Más de 40.000 clientes, entre los que se encuentran 78 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 extremo, y ofrecer excelentes experiencias de usuario final a los empleados, dondequiera y comoquiera que trabajen. Para más información, visite ivanti.com

ivanti

ivanti.lat
+57 315 5718981
contact-latam@ivanti.com

ivanti.es
+34 91 049 66 76
contact@ivanti.es