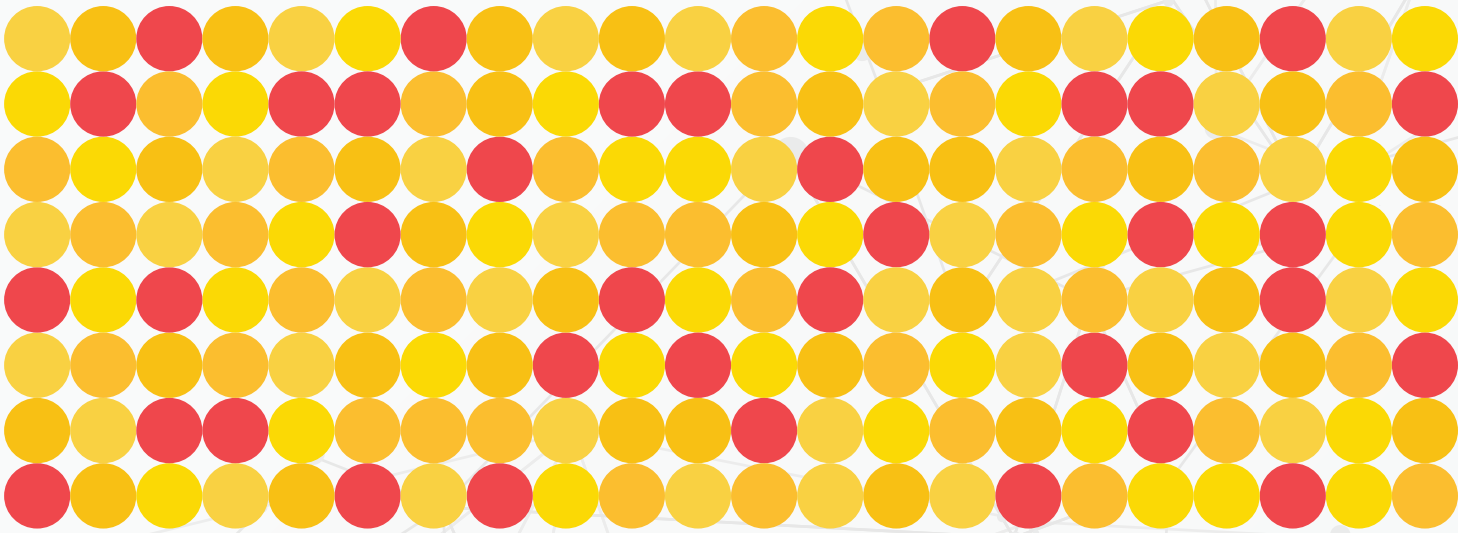
ManageEngine

# AMENAZAS EN AUMENTO:

## ¿Su red es lo suficientemente segura?



www.manageengine.com/products/oputils



Sharon A Ratna

# Índice

# 1. Usted no puede protegerse de lo que no ve

"Usted no puede protegerse de lo que no ve". Esta es una jerga de TI común que más o menos resume la causa de varios ataques de red —un componente o aplicación de TI no monitoreado o un dispositivo de usuario conectado que tiene malware. Las infraestructuras de TI modernas están bajo un constante ataque de varias entidades maliciosas que intentan acceder, manipular e interrumpir la red de la organización. Incluso con medidas de seguridad rigurosas implementadas para proteger la capacidad de uso, disponibilidad e integridad de las redes, la mayoría de estas son aún vulnerables a ataques que se filtran entre las brechas de seguridad.

Ya que la visibilidad es un aspecto crucial para identificar y superar estos ataques, gestionar la TI invisible, los dispositivos de IoT y las políticas de BYOD se hace una pesadilla para los administradores de redes que trabajan en un entorno de amenazas desafiante. Estos activos, que con frecuencia se conectan a la red con motivos genuinos, podrían tratarse de dispositivos maliciosos.

## Lo que sus esfuerzos de seguridad informática no abordan

En resumen, los dispositivos maliciosos son dispositivos que se conectan a su red bajo el pretexto de ser confiables mientras realizan ataques a la red, permitiendo el robo de los datos o la explotación de recursos, e incluso más.

Ya que los entornos de TI escalan más allá de sus funciones gestionables a redes y subredes distribuidas, emergen varias áreas grises en su infraestructura. La mayoría de las estrategias de seguridad informática se enfocan en obtener visibilidad de estas áreas y proteger el aspecto de procesamiento cibernético o de datos en la red. Mientras que las estrategias como implementar firewalls permiten a las organizaciones proteger el software y transportar capas del modelo de red OSI, con frecuencia no permiten la visibilidad en las capas de hardware.

Es en estas capas donde los dispositivos maliciosos funcionan. Escondidos de los analizadores de seguridad en la capa de software, los dispositivos maliciosos pueden pasar desapercibidos ante varias medidas de seguridad informática.

Las organizaciones que no abordan las capas de hardware mientras establecen sus medidas de seguridad de la red exponen sus infraestructuras de TI a la amenaza de ataques maliciosos.

## 2. Volverse maliciosos: Cómo sus empleados se vuelven perpetradores de ataques maliciosos

Con la democratización de la TI, la adquisición, instalación, ejecución y gestión de varios componentes y aplicaciones de TI ya no están bajo la supervisión directa del equipo central de TI de una organización. No obtener el equilibrio perfecto entre ser lo suficientemente flexible para una buena experiencia de los empleados y ser lo suficientemente rígido para evitar ataques de red puede conllevar graves problemas de seguridad en la red. ¡Es tiempo de analizar si sus flexibles políticas de TI están haciendo que sus empleados sean los perpetradores de ataques maliciosos!

### El chico de TI "ignorante"

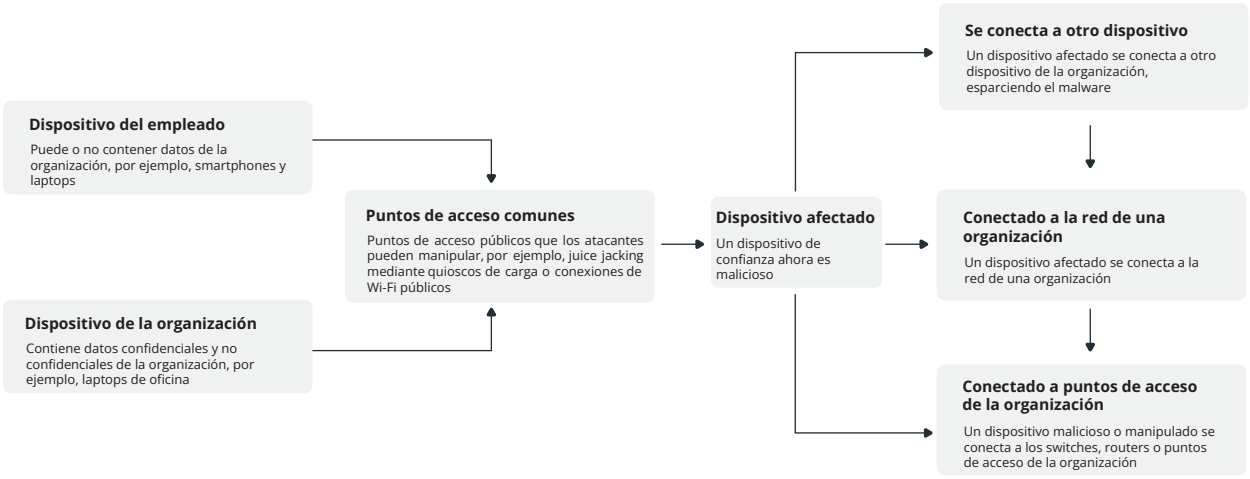
Las políticas de BYOD permiten a las organizaciones ofrecer una experiencia de red más flexible a sus empleados. Esto significa que los empleados van a conectar sus propios dispositivos a los puntos de acceso de su red y consumir los recursos de red de su organización, como el ancho de banda y las direcciones IP. Y no solo eso, pues los empleados también van a acceder y procesar los datos de la organización con estos dispositivos.

Sin embargo, estos dispositivos no tienen configuraciones de seguridad estrictas como los dispositivos dados por la organización. Los atacantes no solo explotan las vulnerabilidades de los dispositivos, sino que también aprovechan las acciones en la red de empleados ignorantes para realizar ataques maliciosos. Sus empleados se pueden convertir en perpetradores de ataques maliciosos bajo algunas de las siguientes instancias:

- **Puntos de acceso públicos:** Conectar el dispositivo de un usuario o de oficina a Wi-Fi o puntos de acceso Wi-Fi públicos permite a los atacantes manipular el dispositivo. Cuando se conecta a un dispositivo o punto de acceso de la organización, este dispositivo del usuario puede fácilmente perpetrar ataques maliciosos en la organización.

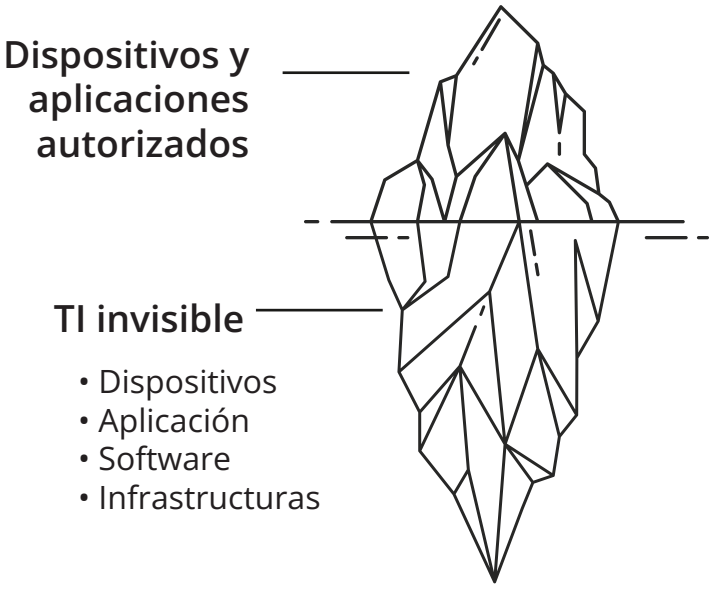
- **Quioscos de carga:** Conectar el dispositivo de un usuario o de oficina a Wi-Fi o puntos de acceso Wi-Fi públicos permite a los atacantes manipular el dispositivo. Cuando se conecta a un dispositivo o punto de acceso de la organización, este dispositivo del usuario puede fácilmente perpetrar ataques maliciosos en la organización.

- **Puntos de acceso en la organización no monitoreados:** Estos puntos de acceso ofrecen un pase gratuito para que los atacantes realicen sus ataques maliciosos en la organización con solo estar lo suficientemente cerca físicamente.




## Acecho desde las sombras

La TI invisible se ha vuelto de alguna manera inevitable con la democratización de la TI. Algunas razones frecuentes para el uso de la TI invisible incluyen el aumento de la eficiencia —al haber una necesidad inmediata, pues la aprobación toma mucho— o la falta de conocimiento sobre lo que se debe o no instalar. Es importante para los equipos de TI de las organizaciones conocer todos los activos y aplicaciones que se ejecutan en sus redes, ya sea el punto de acceso Wi-Fi en el smartphone de un empleado o el nuevo servidor del equipo financiero que requiere un arreglo rápido.




**¡Usted no puede proteger lo que no sabía que tenía!** La gestión del inventario y los activos es crucial para garantizar que no hay ningún dispositivo malicioso funcionando en su red. No obstante, la TI invisible hace de esto una tarea ardua para muchas organizaciones.

## Amenazas internas

Mientras que es verdad que la mayoría de sus empleados no interrumpen su red, los procesos corporativos y las funcionalidades intencionalmente, **¡usted nunca puede ser demasiado precavido!**

Incluso en redes altamente seguras, como las redes con espacio de aire, un infiltrado puede ayudar fácilmente a realizar ataques maliciosos. Un nuevo dispositivo USB para compartir datos o un puerto de switch adicional para extender la conectividad son algunas de las razones frecuentes usadas por los infiltrados maliciosos para realizar o ayudar a realizar ataques maliciosos.

# 3. Ataques maliciosos: ahora los ve, ahora no los ve

Los dispositivos maliciosos frecuentemente no saltan a la vista de su analizador de seguridad de la red. Al manipular la capa de hardware en la red, estos dispositivos pueden pasar desapercibidos ante los firewalls de la capa de software y otro software de seguridad que analice su red. Con la TI invisible aún prevalente en muchas organizaciones, los dispositivos maliciosos pueden pasar desapercibidos incluso por meses antes de que causen varios ataques a la red, resultando en enormes pérdidas financieras y no financieras para la organización.

## Ataques maliciosos comunes que afectan la TI moderna

### Inalámbrico

Con un número masivo de dispositivos que usan Wi-Fi para la conexión a la red, los puntos de acceso maliciosos amenazan la infraestructura de TI inalámbrica.

### Alámbrico

El flujo de comunicaciones y datos críticos de red se da mediante redes alámbricas. Los puertos de switch maliciosos son facilitadores frecuentes de ataques maliciosos aquí.

### En el "medio"

Los ataques man-in-the-middle amenazan la confidencialidad de las comunicacionesde la red establecidas entre distintos componentes de la red.

## Puntos de acceso maliciosos

Los puntos de acceso maliciosos inalámbricos son uno de los más grandes desafíos para una organización cuando intentan minimizar los vectores de ataques maliciosos. Los puntos de acceso maliciosos pueden ser problemáticos de tratar e identificar como una amenaza, ya que:

- Pueden ser puntos de acceso establecidos por empleados para una mejor conectividad a la red. En TI, a estos puntos de acceso se les denomina puntos de acceso blandos.
- Pueden ser de equipos u organizaciones vecinas que están accediendo a sus recursos de red. Ya que los puntos de acceso no requieren una conectividad alámbrica, evitar estos puntos de acceso es desafiante.

- Lo más peligroso de todo es que los puntos de acceso maliciosos establecidos por atacantes de la red pueden comprometer la seguridad e integridad de esta.

Todos estos puntos de acceso deben tratarse como una amenaza a la seguridad de la red, ya que evitan el protocolo de seguridad de la organización.

**Tipos de ataques:** Robo de datos, explotación de tráfico y recursos de red, y facilitadores de ataques posteriores, incluyendo DoS y piratería.

## Switches y routers maliciosos

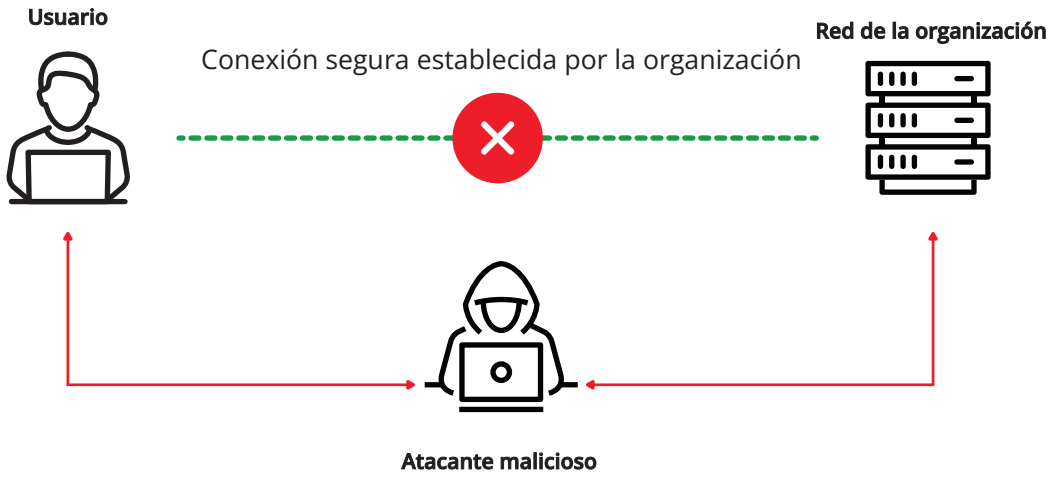
Los switches y routers maliciosos son las contrapartes alámbricas de los puntos de acceso maliciosos. Mientras que cualquier persona lo suficientemente cerca de las instalaciones de la organización puede establecer los puntos de acceso maliciosos, los switches y routers maliciosos requieren un atacante dentro de la organización.

Ellos tienen un gran impacto sobre la seguridad e integridad de la organización. La información crítica de red, como los detalles de MAC IP en las tablas de switches del protocolo de resolución de direcciones (ARP) y las tablas de enrutamiento de los routers puede exponer configuraciones de red internas al atacante. Como los mayores controladores del tráfico de capa 2 y capa 3, es importante garantizar que los routers y switches implementados sean dispositivos de red de confianza y autorizados por la organización.

**Tipos de ataques:** Suplantación de switches, suplantación de ARP y facilitadores de ataques posteriores, incluyendo suplantación de IP y envenenamiento del caché de DNS.

## Ataques man-in-the-middle (MITM)

Mientras que pasan virtualmente desapercibidos ante los analizadores de seguridad, los dispositivos maliciosos son los mayores facilitadores de los ataques MITM. Al actuar en casi todas las capas del modelo OSI de la red al manipular los puntos de acceso, switches, routers y dispositivos de endpoints, los atacantes maliciosos pueden infiltrar las organizaciones para realizar ataques MITM.




Ataque man-in-the-middle

## Algunos de los tipos de ataques más frecuentes incluyen:

- **Detección de paquetes:** Atacantes maliciosos explotan procesadores de datos de red no cifrados, transmisiones de datos y flujos de tráfico usando técnicas de MITM.

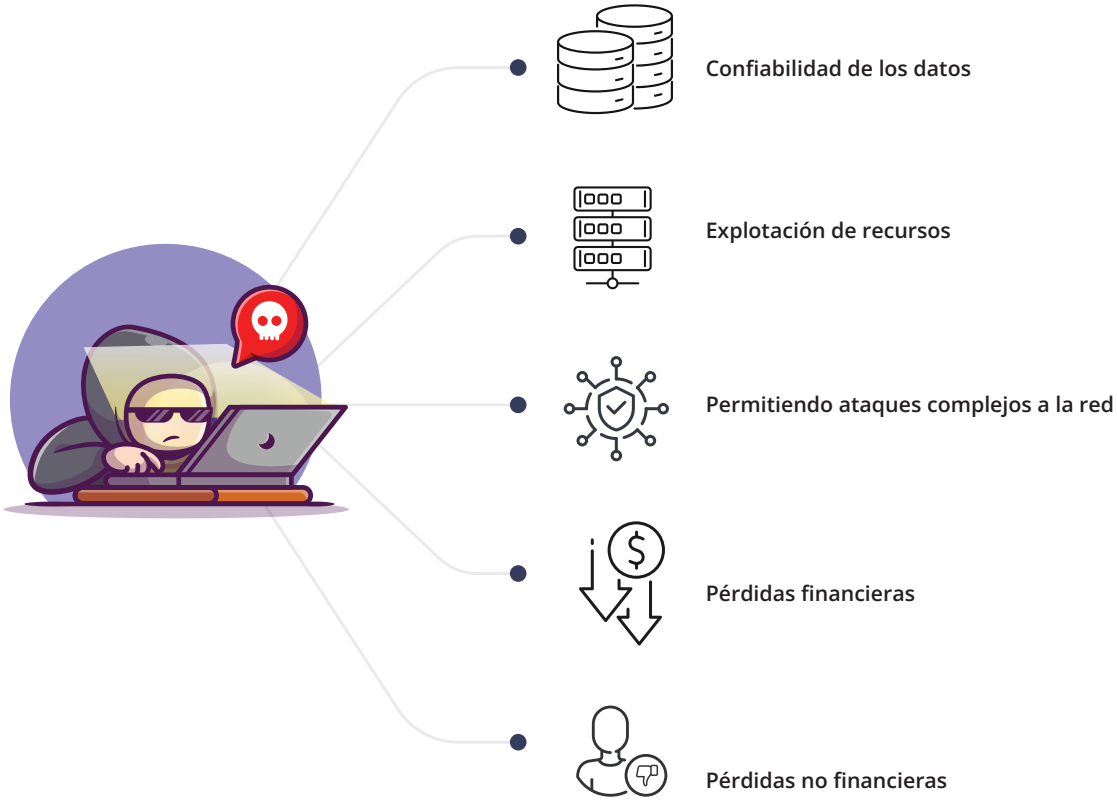
- **Robo de ID de sesiones:** Cuando se realizan transacciones críticas, como acciones de gateway de pagos o registros de contraseña, mediante puntos de acceso maliciosos, los atacantes pueden robar las ID de las sesiones para realizar ataques MITM que pueden resultar en grandes pérdidas financieras.

- **Robo de datos:** Una preocupación principal de las organizaciones, el robo de datos, se ha vuelto inevitable cuando dispositivos maliciosos no detectados realizan ataques MITM. Estas clases de ataques pueden pasar desapercibidos incluso durante años sin estrategias de seguridad efectivas.

## 4. El impacto de los ataques maliciosos: ¿desea arriesgar la TI?

La seguridad de la red está en el centro de la garantía de una experiencia de red ininterrumpida, fiable y de confianza para los empleados de su organización. Superar y evitar dispositivos maliciosos requiere políticas de seguridad estrictas en las capas de hardware y de software de su entorno de TI. Mientras que esto obliga a una menor flexibilidad y prácticas de seguridad de TI más estrictas, el sacrificio es insignificante en comparación con la alternativa —más flexibilidad, menos seguridad.

El impacto de los dispositivos maliciosos puede ser devastador para organizaciones de todas las escalas y complejidades.




- **Confidencialidad de los datos:** Las violaciones de cumplimiento; el robo, pérdida y manipulación de datos; y la interceptación mediante dispositivos maliciosos pueden comprometer críticamente la confidencialidad de una organización.

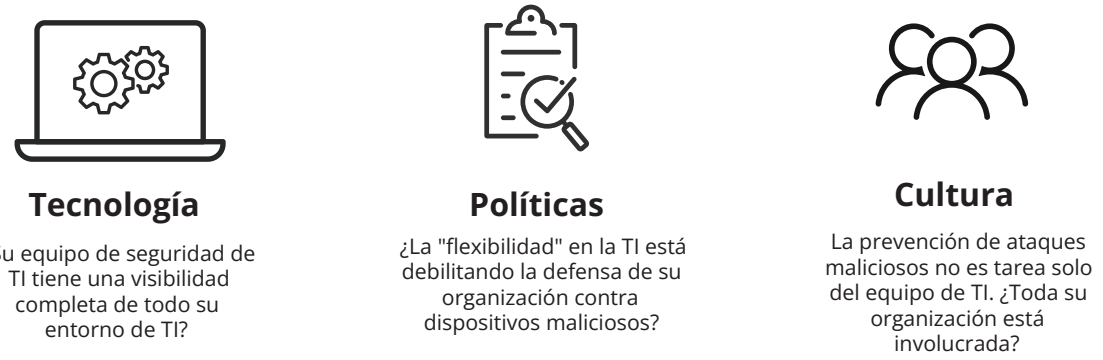
- **Facilitadores de ataques complejos:** Varios ataques avanzados y modernos contra las redes frecuentemente se realizan con base en una intrusión o ataque malicioso primario, como un ataque MITM. Esto hace que la causa o raíz de estos ataques pasen desapercibidos hasta que haya un incidente mayor en la red.

- **Pérdidas financieras:** La explotación de recursos, inactividad de la red y otras consecuencias de los ataques maliciosos resultan en costosas pérdidas financieras para las organizaciones. Las multas regulatorias estatutarias y de cumplimiento pueden también reducir el presupuesto de operaciones de TI en una organización.

- **Pérdidas no financieras:** Como muchos ataques a la seguridad informática, los ataques maliciosos resultan también en pérdidas no financieras. Desde una grave pérdida de la reputación y valor de la marca a pérdida de los esfuerzos de los empleados, los ataques maliciosos suponen varias consecuencias inadecuadas.

## 5. Enfrente los ataques maliciosos: cambios para una TI "a prueba de ataques maliciosos"

Por tanto ¿cómo las organizaciones enfrentan los ataques maliciosos? Para la mayoría de las organizaciones, esto es aún una tarea desafiante. Como toda otra estrategia para la mitigación de amenazas de TI, enfrentar la amenaza de los dispositivos maliciosos requiere que las organizaciones estén actualizadas sobre las últimas mejores prácticas y recomendaciones de seguridad. Sin embargo, no se limita a cuán bien su equipo de seguridad de TI lo está haciendo. También requiere cambios a nivel tecnológico, corporativo y de cultura organizacional.




- **Cambios a nivel tecnológico:** Un paso crucial para evitar ataques maliciosos es hacer de la detección y prevención de dispositivos maliciosos una parte integral de sus estrategias de seguridad de la red. Los administradores de redes deben monitorear continuamente los endpoints de su red en busca de nuevos dispositivos que se conectan a su red. Yendo un paso más allá, las prácticas de detección de dispositivos maliciosos implementadas deben existir al tiempo con estrategias de detección y prevención de intrusiones en los firewalls para garantizar una prevención efectiva de dispositivos maliciosos.

- **Cambios de políticas:** Mientras que es importante suministrar una experiencia de red eficiente a los empleados, una TI no monitoreada y flexible allana el camino para la TI invisible. Con el fin de evitar áreas grises en la infraestructura de TI, las organizaciones necesitan afinar sus políticas de adquisición, implementación y solicitud de TI, junto con las políticas de BYOD.

- **Cultura organizacional:** Es importante educar a los empleados sobre posibles puntos de entrada, amenazas y el impacto de los dispositivos maliciosos con el fin de evitar el caso del "chico de TI ignorante". Los empleados y equipos deben tener niveles adecuados de responsabilidad por las acciones de implementación de TI que supervisan o realizan. Los nuevos empleados deben conocer bien las políticas de BYOD y otros protocolos de seguridad de TI. Se debe establecer una distinción clara entre el uso y la accesibilidad a la red de dispositivos de confianza dados por la organización y dispositivos externos de usuarios.

## 6.Una mirada a OpUtils, la solución de confianza para la mitigación de ataques maliciosos para los administradores en todo el mundo

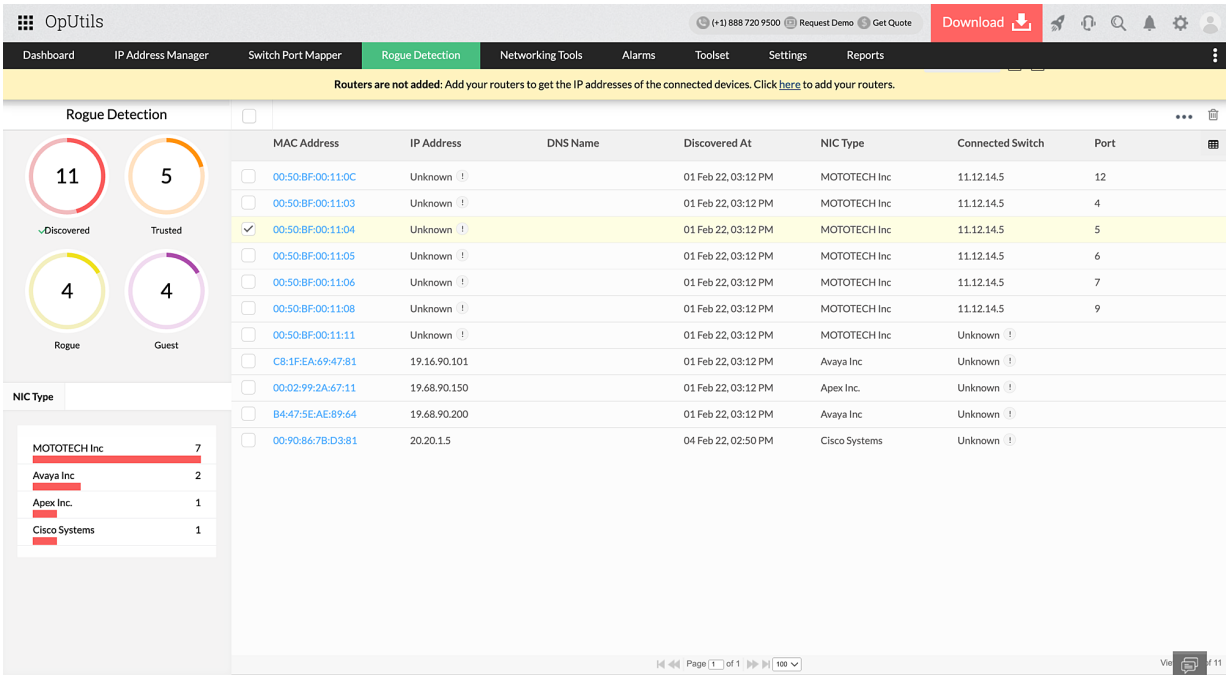
**ManageEngine OpUtils** es un software integral para la detección y prevención de dispositivos maliciosos que ofrece un método holístico para salvaguardar su red de ataques maliciosos. Su módulo de detección de dispositivos maliciosos está integrado estrechamente con los módulos de gestión de direcciones IP y de mapeo de puertos de switch en OpUtils, lo que permite que los administradores de redes obtengan una visibilidad completa de su espacio de direcciones y conectividad de la red.

## Funciones destacadas de la herramienta de mitigación de ataques maliciosos en OpUtils

¡La primera línea de defensa contra los ataques maliciosos nunca ha sido más fácil de establecer!

## Detección de dispositivos maliciosos

El módulo de detección de dispositivos maliciosos en OpUtils puede ajustarse en minutos en redes de todas las escalas y complejidades. OpUtils analiza continuamente endpoints críticos de la red, como routers, puertos de switch y tablas de ARP, y los registra para identificar nuevos dispositivos que se conectan a la red. Su análisis holístico continuo usa varios protocolos de red para garantizar que ningún nuevo dispositivo pase desapercibido.




# Inspección de dispositivos maliciosos

Una vez detectados, OpUtils enumera los dispositivos de red recientemente identificados bajo su módulo de detección de dispositivos maliciosos. Al usar este módulo, los administradores de redes pueden examinar varios aspectos de red en el dispositivo, incluyendo sus detalles de espacio de direcciones y switches mediante los cuales se ha comunicado el dispositivo.

Los administradores de redes pueden inspeccionar la lista blanca o marcar dispositivos autorizados como "confiables" y otros dispositivos no maliciosos de usuarios como "invitados" al configurar un periodo de validez. Los dispositivos sospechosos pueden colocarse en una lista negra o marcarse como "maliciosos" y, tras la inspección, los administradores de redes pueden dar los pasos necesarios para mitigar el acceso malicioso.

# Mitigación de dispositivos maliciosos

El primer paso para enfrentar el acceso malicioso identificado y mitigar el impacto de ataques maliciosos es bloquear el acceso del dispositivo malicioso a su red. OpUtils lo ayuda a hacer esto al escanear y mostrar el puerto de switch que permite la comunicación de los dispositivos maliciosos con su red. Usted puede bloquear instantáneamente estos puertos de switch desde la consola de OpUtils e impedir que los dispositivos maliciosos generen caos en su red.

## Sobre el autor

**Sharon A Ratna**

Product Marketer

Sharon A Ratna es una analista de mercadeo de productos para la suite ITOM de ManageEngine que ha ayudado a equipos de TI en Fortune 100 a nivel mundial por más de 20 años. Ella investiga y escribe sobre tecnologías que desarrollan, mejoran y simplifican las funciones y nuevas oportunidades de la solución actual en el dominio de ITOM. Con un entendimiento excepcional de las tendencias de mercadeo y los puntos críticos para los consumidores, ella trabaja con los equipos de gestión, desarrollo y soporte de productos para afinar y ejecutar estrategias de mercadeo interesantes. Una contadora de historias apasionada, en sus tiempos libres disfruta de leer libros y viajar.

# Glosario

| Término | Definición |
|---|---|
| **IoT** | Internet de las cosas |
| **BYOD** | Una política de traiga su propio dispositivo (BYOD) permite a los usuarios traer y conectar sus propios dispositivos a la red de la organización. |
| **TI invisible** | Cuando componentes de TI, como dispositivos y aplicaciones, se ejecutan sin la autorización del equipo de TI de la organización. |
| **TI encubierta** | Un término usado intercambiablemente con TI invisible. |
| **Modelo OSI** | El modelo de intercomunicación de sistemas abiertos (OSI) explica las siete capas que permiten la comunicación en la red. |
| **Red con espacio de aire** | Una red desconectada de otras partes de la red de la organización y que sigue medidas de seguridad estrictas. Estas redes altamente protegidas evitan la comunicación alámbrica e inalámbrica fuera de la red |
| **DoS** | Un ataque de denegación del servicio (DoS) se enfoca en un recurso crítico particular de la red, como un servidor, y sobrecarga su capacidad, especialmente el tráfico del servidor, lo que lo hace inalcanzable a otros dispositivos genuinos que intentan acceder al dispositivo crítico. |
| **DDoS** | Una variación del DoS, los ataques de denegación distribuida del servicio (DDoS) se enfocan en varios recursos críticos al mismo tiempo, causando interrupciones e inaccesibilidad en toda la red. |
| **Ataque man-in-the-middle** | Un tipo de ataque a la red en el que el atacante se posiciona en la línea de comunicación o en el medio de una transacción entre dos entidades de red, como un usuario y otro usuario, o un usuario y una aplicación. |