ForeScout

ForeScout

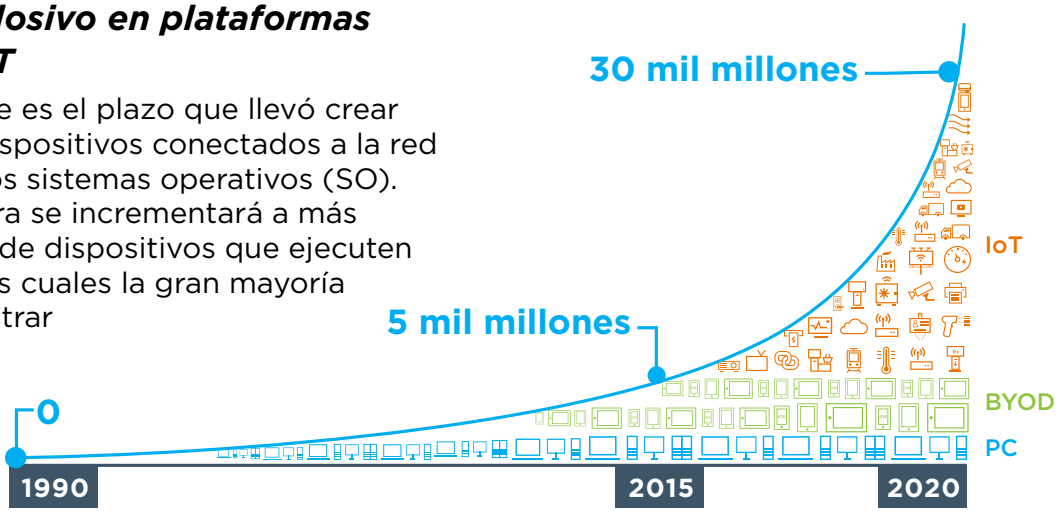
Transformación de la seguridad a través de la visibilidad

VEA

Desafío:

Crecimiento explosivo en plataformas y dispositivos IoT

Veinticinco años. Ese es el plazo que llevó crear 5000 millones de dispositivos conectados a la red que ejecuten algunos sistemas operativos (SO). Hacia 2020, esta cifra se incrementará a más de 30.000 millones de dispositivos que ejecuten cientos de SO, de los cuales la gran mayoría no se podrá administrar con métodos de seguridad basados en agente. Sin un enfoque radicalmente nuevo, los puntos ciegos de la red serán la norma, y el servicio de ataque continuará expandiéndose.



ABI Research, 2017

El crecimiento desmedido de la Internet de las cosas (IoT), y movilidad y SO nuevos crean una explosión de dispositivos sin administrar.

Solución:

Control y visibilidad sin agentes

ForeScout ha sido pionero en tener un enfoque sin agente hacia la seguridad, que proporciona detección, clasificación, evaluación y supervisión en tiempo real de dispositivos, lo que le permite ver qué tiene en la red, desde el campus hasta la nube, y administrarlo con seguridad.

Cómo lo hacemos:

Las empresas de la actualidad no ejecutan redes estándares, según un modelo. Son dinámicas y están en constante cambio. En ForeScout, ofrecemos **seguridad heterogénea** que proporciona visibilidad en toda la red: desde dispositivos dentro del campus hasta cargas de trabajo en el centro de datos y entornos de nube pública y privada. Nuestro enfoque **sumamente flexible** e **independiente de proveedores** admite redes Cisco, Aruba, Juniper y demás en redes con cable e inalámbricas que ejecutan 802.1X, normas que no son 802.1X o ambos.

La seguridad comienza con saber qué hay en su red. **Detectamos** su infraestructura, los sistemas físicos y virtuales, los extremos administrados y no administrados, los dispositivos IoT y no autorizados, todo ello sin necesitar agentes de software ni conocimientos previos sobre los dispositivos. A continuación, nuestra solución **evalúa** la higiene de los dispositivos y **continuamente supervisa** la postura de seguridad.

Nuestras capacidades de **recopilación de datos adaptable admiten su opción de conjuntos de datos** y utilizan técnicas avanzadas activas y pasivas enumeradas a la derecha para brindar visibilidad en profundidad. Nuestra solución evalúa rápidamente dispositivos y aplicaciones, lo que permite determinar el usuario, el propietario, el sistema operativo y la configuración del dispositivo, el software, los servicios, el estado de los parches y la presencia de agentes de seguridad. Este conocimiento le permite impulsar políticas precisas de control de acceso, implementación y corrección.

Cómo ForeScout lo ayuda a ver más

1. Sondeo de conmutadores, concentradores VPN, puntos de acceso y controladores para obtener una lista de los dispositivos conectados
2. Recepción de capturas de SNMP de conmutadores y controladores
3. Supervisión de solicitudes 802.1X para el servidor RADIUS integrado o externo
4. Supervisión de solicitudes DHCP para detectar cuándo un host nuevo solicita una dirección IP
5. Supervisión opcional de un puerto de Analizador de puerto de conmutador de la red para ver el tráfico de red, como el tráfico HTTP y los carteles
6. Ejecución de un análisis del asignador de redes (Nmap)
7. Uso de credenciales para ejecutar un análisis en el dispositivo
8. Recepción de datos de NetFlow
9. Importación de datos externos de clasificación de direcciones del control de acceso de soportes o solicitud de datos LDAP
10. Supervisión de máquinas virtuales en la nube pública o privada
11. Clasificación de dispositivos mediante la alimentación a través de Ethernet con SNMP
12. Uso de agente opcional

Resuelva sus casos de uso más desafiantes

Internet de las cosas:

Detecte dispositivos IoT en el instante en que se conectan a su red sin necesidad de agentes. Clasifique dispositivos, usuarios, aplicaciones y sistemas operativos, establezca un perfil para ellos y asigne dispositivos automáticamente a segmentos seguros de Red de área local virtual (VLAN), y supervise el comportamiento.

Control de acceso a la red:

Obtenga visibilidad en tiempo real de dispositivos, usuarios, aplicaciones y sistemas operativos a medida que acceden a la red. Notifique a los usuarios y al personal de TI de los problemas y aplique automáticamente los controles de acceso adecuados, como restringir o bloquear dispositivos, ponerlos en cuarentena o reasignarlos a segmentos VLAN.

Red de invitados:

Automatice la inscripción de visitantes, contratistas y socios, e implemente el cumplimiento de políticas mediante opciones de incorporación adecuadas. Comparta detalles sobre la postura de seguridad de dispositivos e instrumente acciones de implementación con herramientas de Administración de dispositivos móviles de la empresa y Protección de extremos.

Seguridad BYOD:

Proporcione visibilidad sin agente de equipos portátiles ligeros, tabletas y smartphones de empleados a medida que se conectan a la red. Implemente controles de acceso y políticas de cumplimiento de extremos, a la vez que elimina el trabajo manual asociado con la apertura y el cierre de los puertos de red.

Cumplimiento regulatorio y de extremos:

Supervise dispositivos a medida que se conectan a la red y se desconectan de ella, y notifique a los usuarios de infracciones de políticas, como software de seguridad, sistemas operativos y opciones de configuración desactualizados o de baja calidad. Redirija automáticamente a los usuarios a portales de autocorrección.

Informática en la nube segura:

Extienda la visibilidad y el control de dispositivos y de máquinas virtuales desde el campus hasta sus entornos de nube pública y privada. Obtenga un panorama único y sencillo en entornos físicos y virtuales, a la vez que aprovecha procesos y habilidades existentes del equipo de operaciones de seguridad.

CONTROLE

Desafío:

Demasiadas alertas de seguridad, implementación insuficiente

La mayoría de las herramientas de seguridad son excelentes para enviar alertas, pero incapaces de implementar medidas. En consecuencia, el volumen de alertas que se deben evaluar y resolver de manera manual resulta un agobio para los equipos de seguridad. Algunas alertas generan falsos positivos y se omiten; otras, simplemente pasan debido a limitaciones de recursos.

> **"Hacia el 2020 y con un 5 % actual como punto de partida, por lo menos el 25 % de las organizaciones utilizará un mecanismo de detección, visibilidad y control en tiempo real para proteger IoT".**
>
> —Gartner, *La detección, la visibilidad y el control en tiempo real son fundamentales para la seguridad de IoT*, Saniye Burcu Alaybeyi y Lawrence Orans, 3 de noviembre de 2016

Solución:

Segmentación e implementación basadas en políticas

ForeScout automatiza la implementación y el control de acceso de dispositivos, usuarios y aplicaciones basado en políticas, lo que le permite limitar el acceso a los recursos adecuados, automatizar la incorporación de invitados, encontrar y reparar brechas de seguridad de extremos, y ayudar a mantener y mejorar el cumplimiento de normativas del sector.

Cómo lo hacemos:

ForeScout le permite **automatizar** una amplia variedad de acciones activas o pasivas e **implementar controles luego de la conexión**, según las políticas y la gravedad de la situación. Para lograr esto, utilizamos un motor de políticas que comprueba **continuamente** dispositivos en función de un conjunto de políticas que establece e implementa el comportamiento de los dispositivos en la red. A diferencia de los productos de otros proveedores que periódicamente comprueban y consultan dispositivos, nuestro motor de políticas puede supervisar el comportamiento en **tiempo real** para más de un millón de dispositivos en una sola implementación.

Las políticas se desencadenan según eventos que tienen lugar en un dispositivo específico. Estos pueden ser eventos de admisión de la red (por la conexión a un puerto de conmutador o un cambio de dirección IP), eventos de autenticación (recibidos por servidores RADIUS o detectados por el tráfico de la red), **cambios en el comportamiento del usuario o dispositivo** (que se desactive el software antivirus, se agreguen periféricos prohibidos o se abran o cierren puertos) y **comportamiento del tráfico** específico, como la manera en que el dispositivo se comunica y qué protocolo utiliza.

Notifique

- Envíe correos electrónicos a usuarios y administradores
- Envíe notificaciones en pantalla
- Redirija a páginas web
- Solicite respuestas de usuario final
- Envíe mensajes de Syslog/CEF
- Abra solicitudes de la mesa de ayuda
- Comparta contexto con sistemas de TI

Cumpla

- Pase a la red de invitados
- Cambie el rol de usuario inalámbrico
- Asigne a VLAN de autocorrección
- Restrinja dispositivos no autorizados
- Inicie aplicaciones y procesos
- Actualice agentes antivirus y de seguridad
- Aplique parches y actualizaciones de SO

Restrinja

- Ponga en cuarentena dispositivos
- Apague puertos de conmutador
- Bloquee acceso inalámbrico o a VPN
- Utilice listas de acceso (ACL) para restringir el acceso
- Finalice las aplicaciones no autorizadas
- Deshabilite periféricos y NIC
- Desencadene sistemas de corrección

ForeScout puede implementar el nivel adecuado de control, desde moderado hasta estricto, según sus políticas de seguridad.

INSTRUMENTE

Desafío:
Seguridad fragmentada

Las grandes empresas tienen docenas de sistemas de seguridad desconectados e inconexos. Este enfoque por silos evita una respuesta de seguridad coordinada en toda la empresa, lo que le proporciona a los atacantes más tiempo de explotar las vulnerabilidades del sistema.

Solución:
Automatización de la seguridad

ForeScout instrumenta operaciones de intercambio de información e implementación de la seguridad basada en políticas con productos líderes de administración de seguridad y TI para automatizar flujos de trabajo de seguridad y acelerar la respuesta ante amenazas sin intervención humana.

> **"Cuando es de noche tarde o cuando el personal duerme, ForeScout trabaja con nuestras otras soluciones de seguridad para tomar medidas inmediatas contra las amenazas. No se le puede poner un precio a ese tipo de automatización".**
>
> —Michael Roling, Director de Seguridad de la información del estado de Misuri

Cómo lo hacemos:

Con visibilidad y control como capacidades fundacionales, ForeScout puede **desglosar silos de seguridad** y aprovechar sus inversiones existentes en seguridad. Los módulos de ForeScout permiten un constante intercambio de higiene de dispositivos, amenazas, comportamiento y datos de cumplimiento para que su análisis y sus herramientas existentes de seguridad sean más inteligentes y más sensibles al contexto. Su infraestructura de seguridad obtiene una funcionalidad de control crítica, lo que le permite **automatizar una implementación de políticas manual**, **acelerar la respuesta** y **mejorar su postura de seguridad** significativamente. Estos son algunos ejemplos de cómo ForeScout le permite organizar en capa sus herramientas sobre las nuestras para lograr una instrumentación de la seguridad en todo el sistema:

Detección avanzada de amenazas (ATD): Luego de detectar malware e indicadores de compromiso (IOC), los productos líderes de ATD notifican de manera instantánea a la plataforma ForeScout. A continuación, basándose en políticas, la solución de ForeScout aísla los dispositivos infectados y toma medidas de corrección. También analiza los dispositivos existentes y los nuevos en busca de IOC e inicia la mitigación.

Administración de eventos e información de seguridad (SIEM): La plataforma ForeScout detecta dispositivos y establece sus perfiles a medida que se conectan a la red, y comparte detalles de ellos con la SIEM, lo cual la vuelve más inteligente. La SIEM responde con una evaluación de dispositivos basada en los eventos y los registros recopilados. ForeScout convierte esta información en acción y, entonces, permite o deniega dispositivos, o los coloca en cuarentena, según sus políticas de seguridad.

Segmentación dinámica de la red: La profunda integración con productos de proveedores líderes de firewall, conmutadores y enrutadores le permite a nuestro motor de políticas aplicar automáticamente VLAN o listas de control de acceso (ACL) para colocar o reasignar dispositivos y usuarios a segmentos adecuados de la red. Segmentar invitados, contratistas, empleados específicos y dispositivos IoT ayuda a proteger contra ataques pivote, laterales, de personal interno y DDoS.

Para obtener una lista completa de las capacidades de instrumentación, visite **forescout.com/modules**. Estos son algunos de los socios con los que trabajamos:

amazon web services · Check Point Software Technologies Ltd · CyberArk · FireEye · IBM · McAfee · MobileIron · paloalto networks · Qualys · Rapid7 · servicenow · splunk> · Symantec · tenable · vmware

“Lo que ForeScout logró en tecnología de Control de acceso a la red (NAC) es claramente una transformación”.

—Mejor tecnología de seguridad de redes de 2016, Frost & Sullivan

“ForeScout le brinda a JPMorgan Chase visibilidad y control mejorados en los cientos de miles de dispositivos conectados a nuestra red corporativa”.

—Rohan Amin, Director global de Seguridad de la información de JPMorgan Chase & Co.

Instantánea de la empresa

Sector: Ciberseguridad/seguridad de IoT

Clientes: 2000 empresas y organismos gubernamentales en todo el mundo, en más de 60 países*

Mercados: Servicios financieros, gobierno y defensa, cuidado de la salud, fabricación, educación, venta minorista e infraestructura crítica.

Fundada: 2000

Director ejecutivo: Michael DeCesare

Premios y reconocimientos en 2016:

- JPMorgan Chase Hall of Fame, Premio a la innovación por Tecnología de seguridad transformadora
- Guía de Mercado de seguridad de IoT de Gartner
- Guía de Mercado NAC de Gartner
- Principales 100 empresas de nube de Forbes
- Technology Fast 500™ de Deloitte
- Nanalyze: 9 novedosas empresas incipientes de ciberseguridad
- Empresa de seguridad líder de CRN (Computer Reseller News)
- Empresas de más rápido crecimiento de Inc. 5000
- Mejor solución NAC de SC Magazine Europe

Marcos de trabajo de seguridad y mandatos de cumplimiento:

Los organismos y marcos de trabajo líderes dedicados a los estándares de seguridad comparten un principio fundacional: la seguridad comienza con la visibilidad. ForeScout respalda los esfuerzos de cumplimiento de empresas y organismos gubernamentales mediante estos mandatos:

- Centro para CSC (controles de seguridad críticos) de seguridad de Internet
- Mitigación y diagnóstico continuos (CDM, por sus siglas en inglés)
- Ley Federal de Gestión de Seguridad de la Información (FISMA)
- Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)
- Ley de Tecnologías de Información Médica para Salud Clínica y Económica (HITECH)
- Organización Internacional de Normalización y Comisión Electrotécnica Internacional (ISO/CEI 27001)
- Marco de Trabajo NIST (Instituto Nacional de Normas y Tecnología) para la Gestión de Riesgos
- PCI-DSS (Normas de Seguridad de Datos para la Industria de Tarjetas de Pago)
- SCAP (Protocolo de Automatización de Contenidos de Seguridad)
- SOX (Ley Sarbanes-Oxley)

ForeScout®

Oficinas internacionales:
San José, CA (casa central)
Dallas
Londres
Nueva York
Sídney
Tel Aviv
Washington, D.C.

** Hasta el 31 de diciembre de 2016*