FORESCOUT

Visibilidad total: La llave maestra a Zero Trust

Forescout ofrece la plataforma de visibilidad de dispositivos para una seguridad Zero Trust.

> "La visibilidad es la clave para defender un activo valioso. No puede proteger lo invisible. Cuanta más visibilidad se tenga de la red en todo el ecosistema de la empresa, mayores serán las posibilidades de detectar rápidamente cualquier indicio de violación de seguridad y de detenerla[3]."

No confiamos en nada

El modelo Zero Trust (literalmente, Confianza Cero) de seguridad de la información se ha convertido en una parte integrante tanto de las estrategias de los equipos de seguridad de las empresas como de las hojas de ruta de los desarrolladores de soluciones de seguridad, y por una buena razón. Las arquitecturas de seguridad basadas en la protección del perímetro que disfrutan sistemáticamente de altos niveles de confianza en la red interna siguen fallando de forma estrepitosa y generando enormes costes. Un análisis reciente de Online Trust Alliance descubrió que en 2017 las empresas denunciaron casi el doble de ciberincidentes. De hecho, en los primeros tres trimestres de 2017, las fugas de datos comprometieron más de 7000 millones de registros, lo que multiplica por cuatro la cifra de 2016[1]. El Ponemon Institute pone precio a este destrozo financiero, y estima que el coste de cada registro robado es de 141 dólares, y el coste medio total de una fuga de datos de 3,62 millones de dólares[2].

Los múltiples fallos de la seguridad perimetral

Los entornos empresariales actuales dependen en gran medida de servicios e infraestructura basada en la nube, que en la práctica elimina el perímetro de red. Las cargas de trabajo, los datos y la propia plantilla son ahora móviles, y necesitan una seguridad ágil. Además, los usuarios exigen más opciones de acceso a más cuentas, datos y recursos. Simultáneamente, el volumen y la diversidad de dispositivos que se conectan a recursos de red desborda a la administración de endpoints tradicional. Muchos dispositivos no ejecutan o no pueden ejecutar agentes de administración corporativos (dispositivos de visitantes, sistemas BYOD, dispositivos IoT y tecnologías operativas), por lo que los equipos de seguridad pueden carecer de visibilidad sobre muchos dispositivos de sus redes, y ser incapaces de identificar a sus usuarios, evaluar su estado de seguridad o controlar sus actividades.

Estos fallos sistémicos de la seguridad perimetral llevaron a los analistas de Forrester Research a desarrollar Zero Trust como alternativa. Presentada en 2010, Zero Trust es un modelo conceptual y arquitectónico sobre cómo deben rediseñar los equipos de seguridad las redes en microperímetros seguros, fortalecer la seguridad de los datos utilizando técnicas de ofuscación, limitar los riesgos asociados al acceso con privilegios excesivos de usuarios y mejorar enormemente la detección y respuesta de seguridad con análisis y automatización.

Zero Trust: De modelo conceptual a marco general

En las primeras iteraciones, el modelo Zero Trust se centraba estrictamente en los conceptos de segmentación preventiva y control de acceso de mínimo privilegio, con muy pocas instrucciones específicas sobre cómo podrían aprovecharse los controles de seguridad existentes en implementaciones prácticas. Con el tiempo, el modelo básico ha evolucionado y madurado a lo que Forrester llama el ecosistema Zero Trust eXtended (ZTX). Se trata de un marco general que asocia las tecnologías de seguridad relevantes a las siete dimensiones principales de un entorno empresarial típico al que pertenecen los principios de Zero Trust: redes, datos, personas, cargas de trabajo, dispositivos, visibilidad y análisis, y automatización y orquestación.

El marco ZTX ayuda a los equipos de seguridad a comprender lo que hace la tecnología para:

- Permitir los principios de aislamiento, segmentación y seguridad de red.
- Permitir la categorización, aislamiento, cifrado y control de los datos.
- Proteger a los usuarios (humanos) de la red y los recursos de infraestructura, al tiempo que se protegen los recursos de sus usuarios.
- Proteger las pilas de aplicaciones de las cargas de trabajo en las nubes públicas y privadas.
- Automatizar y coordinar los controles y procesos del modelo Zero Trust en entornos heterogéneos.
- Proporcionar visibilidad y análisis para iluminar y proteger cada rincón del entorno de red ampliado.

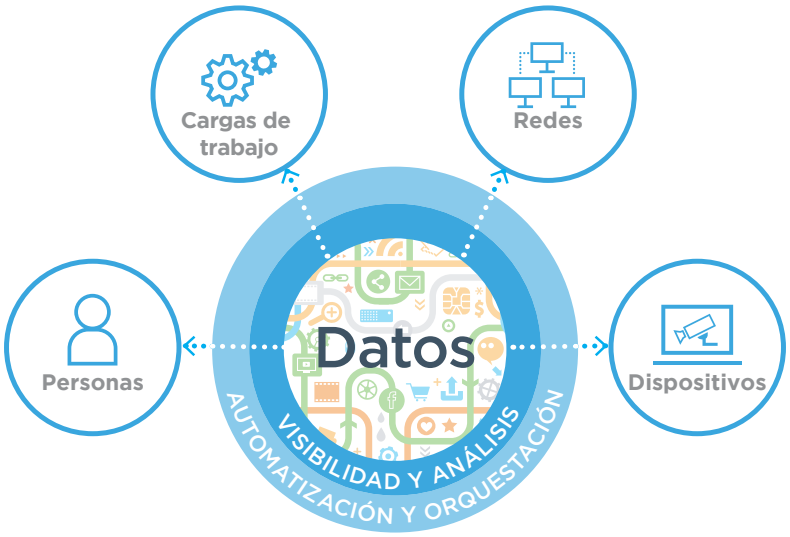

Figura 1: Las siete dimensiones del marco del ecosistema Zero Trust eXtended de Forrester Research

Si la visibilidad es la estrategia, Forescout es la plataforma

Un ejemplo de una estrategia Zero Trust es el objetivo de detectar y clasificar el 100 % de los dispositivos que se conectan a la red (no solo los que tienen agentes de endpoints instalados y operativos) y aplicar de manera estricta la directiva de acceso de mínimo privilegio basada en un análisis granular del dispositivo, la identidad del usuario y las autorizaciones, la pila de software, el cumplimiento de la configuración y el estado de seguridad. Para aplicar una directiva de acceso restrictiva, es necesario ver, evaluar y controlar todo lo que hay en la red.

Forrester hace mucho hincapié en el tema de la visibilidad en Zero Trust. Según el analista de Forrester Chase Cunningham:

para hacer realidad una estrategia semejante se necesita una solución de Device Visibility and Control completa, capaz de ver y controlar hosts que no pueden ver los sistemas de administración de endpoints convencionales: dispositivos de visitantes y propiedad de los empleados (BYOD, Bring Your Own Device), endpoints corporativos con agentes desactivados, dispositivos no autorizados, dispositivos IoT, conmutadores y enrutadores de red, sistemas de plantas de producción y otros sistemas OT.

La plataforma Forescout: Consiga visibilidad de dispositivos y control de riesgos

Forescout ejemplifica la evolución de las tecnologías de red líderes en plataformas Zero Trust. La plataforma Forescout es una solución de seguridad sin agente que identifica y evalúa de forma dinámica los endpoints de red en el momento en que se conectan a su red ampliada, heterogénea y multinube. Determina rápidamente el usuario, propietario y sistema operativo, así como la configuración de dispositivos, software, servicios, estado de los parches y presencia de agentes de seguridad. A continuación, ofrece corrección, control y supervisión continua de estos dispositivos.

Forescout ejerce estas funciones en los dispositivos corporativos, los dispositivos de visitantes no gestionados, los servidores físicos y virtuales, la infraestructura de red, los sistemas de control y operaciones industriales, y los dispositivos IoT, sin necesidad de agentes de software ni de un conocimiento previo de los dispositivos. Se despliega rápidamente en su entorno actual y rara vez requiere cambios en la infraestructura, ampliaciones o reconfiguraciones de endpoints. Esencialmente, funciona sin problemas en entornos físicos y de nubes virtuales e híbridas.

La plataforma Forescout proporciona descubrimiento y clasificación totales de todos los dispositivos conectados mediante IP, así como evaluación constante del riesgo y del estado sin agente, a fin de determinar el conocimiento situacional en tiempo real de cada dispositivo conectado. A continuación, aplica esta información para automatizar los controles basados en directivas y organizar acciones en los dispositivos. Estas funciones sirven de base para la seguridad Zero Trust.

Forrester nombró a Forescout como plataforma Zero Trust dentro de su ecosistema de proveedores Zero Trust eXtended. Según la empresa de analistas, Forescout ofrece funciones líderes del mercado en cinco categorías de componentes de Zero Trust[4].

Visibilidad, análisis y control de dispositivos de Zero Trust

Detección sin agente de cualquier dispositivo: la plataforma Forescout emplea una combinación de métodos activos y pasivos sin agentes para detectar todos los dispositivos de la red ampliada y heterogénea de una organización —desde el campus y el centro de datos hasta la nube y las redes de tecnologías operativas. Detecta PC y portátiles, servidores físicos y virtuales, dispositivos móviles e IoT, instancias de nube y sistemas de tecnología operativa sin necesidad de equipos de red específicos del proveedor, actualizaciones de la infraestructura existente ni reconfiguración de los conmutadores y puertos de conmutador, con o sin autenticación 802.1X.

Figura 2: Forescout proporciona una plataforma de Device Visibility and Control para los entornos empresariales ampliados.

De detección de dispositivos a inteligencia sobre activos: los variados métodos de detección y creación de perfiles de Forescout generan y actualizan continuamente una gran cantidad de información sobre la identidad, el estado y el comportamiento de los dispositivos. La capa de abstracción adaptable de la plataforma ingiere miles de millones de paquetes de datos sin procesar en una amplia variedad de sistemas de red heterogéneos. Correlaciona y consolida estos datos, creando una vista unificada de toda la población de dispositivos con gran nivel de detalle sobre cada uno de ellos. La capa de abstracción se adapta y evoluciona con el entorno de IT, enriqueciendo continuamente la vista de dispositivos a medida que hay disponibles otras fuentes de datos.

Sus datos ofrecen una vista muy detallada de todos los activos del entorno, haciendo posible la toma de una amplia variedad de acciones informadas, y sirviendo de base para los controles de mitigación de riesgos. Además, la plataforma Forescout permite la supervisión y visualización de las comunicaciones entre fuentes de dispositivos y datos, así como interdependencias entre sistemas. Esto es particularmente importante para la asignación de la segmentación, la planificación y la creación de directivas.

La plataforma Forescout permite la supervisión y visualización de las comunicaciones entre fuentes de dispositivos y datos, así como interdependencias entre sistemas. Esto es particularmente importante para la asignación de la segmentación, la planificación y la creación de directivas.

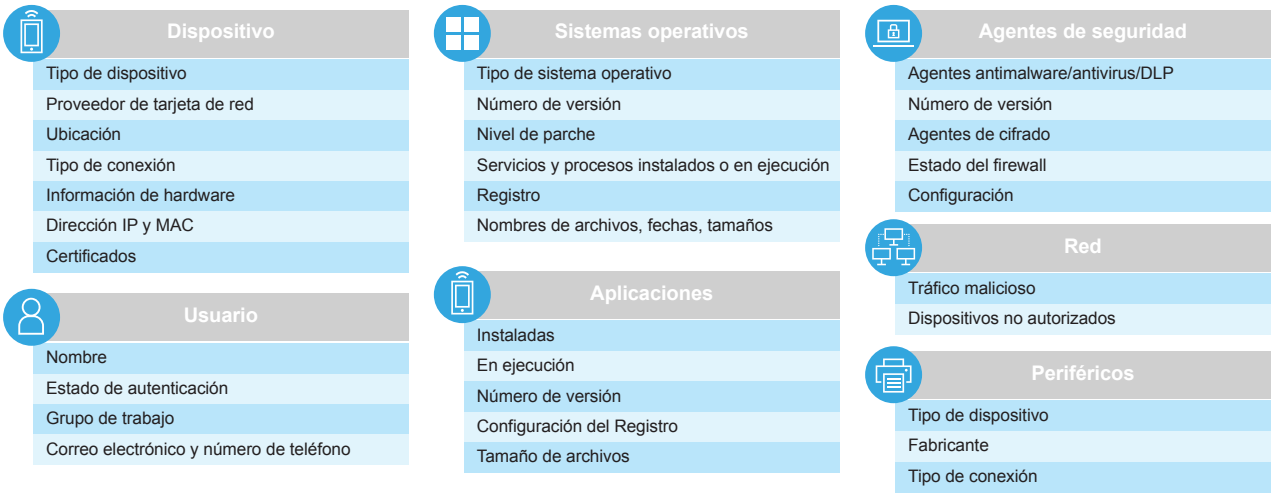

Figura 3: el proceso de clasificación de Forescout extrae datos detallados de todos los dispositivos conectados mediante IP.

Device Visibility and Control basada en directivas permanente: el motor de directivas en tiempo real de la plataforma utiliza esta inteligencia sobre los activos para evaluar permanentemente los dispositivos en relación con las directivas que aplican el comportamiento esperado. Activa directivas en tiempo real basadas en la admisión en la red de un dispositivo, la autenticación u otros atributos personalizables. Por ejemplo, Forescout puede identificar un nuevo dispositivo IoT con acceso a Internet entrante y asignarlo automáticamente a un segmento de red restringido. Puede detectar cambios en el estado de seguridad de un dispositivo, como agentes antivirus o software de cifrado que hayan sido desactivados o que hayan dejado de funcionar. La plataforma reevalúa los dispositivos cuando están en la red cada vez que entran y salen. Comparte contexto de los dispositivos en tiempo real e inicia acciones de evaluación del nivel de seguridad, como volver a analizar los dispositivos en busca de vulnerabilidades e indicadores de riesgo, en colaboración con sistemas de terceros.

Forescout puede ejecutar acciones de control directamente en el dispositivo o a través de la infraestructura de red (véase más adelante). Controles basados en el host que incluyen iniciar y detener aplicaciones, actualizar agentes de seguridad antivirus, desactivar dispositivos periféricos y solicitar confirmación del usuario final. El motor de directivas aplica estas directivas de manera automática con independencia de la ubicación de un dispositivo. Cuando sea necesario, la plataforma puede automatizar las acciones correctivas, como la aplicación de parches a los dispositivos o la reinstalación de la evaluación de vulnerabilidades, la protección de los endpoints, el cifrado u otro software de seguridad a través de la coordinación con herramientas de terceros (se aborda con más detalle más adelante).

Inteligencia sobre dispositivos personalizable para operaciones de seguridad y respuesta a incidentes: los equipos de operaciones de seguridad carecen de una vista completa de los dispositivos conectados y de su contexto de clasificación, conexión y cumplimiento. Esto dificulta la respuesta a incidentes y los informes de cumplimiento. Además de la consola, la plataforma de Forescout incluye ahora un panel web personalizable que ofrece una visión consolidada de todos sus dispositivos y su estado de cumplimiento en toda la empresa. El panel funciona en coordinación con Forescout eyeManage y proporciona información de los distintos tipos de dispositivos conectados a su red heterogénea.

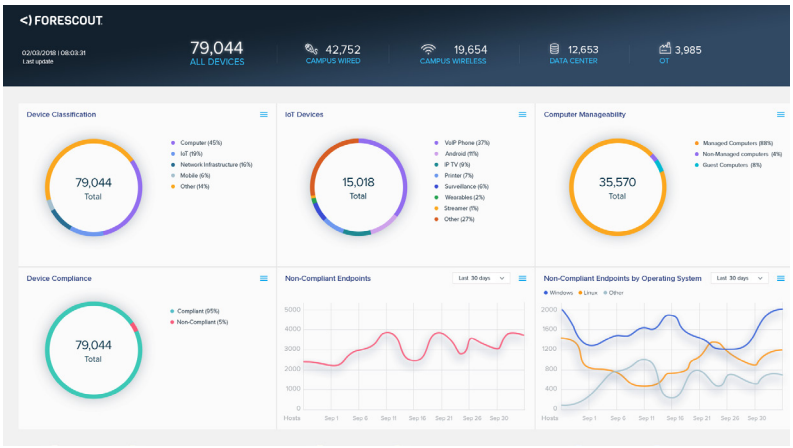

Figura 4: visión consolidada de todos los dispositivos para centros de operaciones de seguridad.

Funciones de red de Zero Trust

Un agente de acceso Zero Trust: la plataforma Forescout aplica las acciones de control de dispositivos a través de la infraestructura de red, ofreciendo un servicio de intermediación centralizado y un punto de decisión para el aprovisionamiento de acceso a la red basado en su vista integrada de la identidad, función, autenticación y estado de los dispositivos de los usuarios. Se integra de forma nativa con productos de más de 30 proveedores de conmutadores y tecnología inalámbrica, y ofrece integración directa con enrutadores que ejecutan el sistema operativo Linux. En función del proveedor, se utilizan distintos métodos de forma individual o en combinación, incluido SNMP, CLI y NETCONF. Gracias a que trabaja en un conmutador de red, esta tecnología puede cambiar la asignación de VLAN, añadir un ACL o desactivar un puerto de conmutador. En una controladora inalámbrica, puede incluir en la lista negra una dirección MAC o cambiar la función de un usuario. Además, nuestra tecnología puede restringir los usuarios VPN remotos.

Una distinción fundamental para la implementación de Zero Trust en el mundo real es que la plataforma Forescout sin agentes puede detectar, evaluar y proporcionar acceso a cualquier dispositivo conectado mediante IP heredado. Forescout ve y controla todos los dispositivos conectados mediante IP y se integra con toda la infraestructura de IT y OT sin excepciones.

Una distinción fundamental para la implementación de Zero Trust en el mundo real es que la plataforma Forescout sin agentes puede detectar, evaluar y proporcionar acceso a cualquier dispositivo conectado mediante IP heredado.

Con la adquisición de SecurityMatters, Forescout amplía además su conocimiento situacional basado en la red más allá de la tecnología de la información (IT), y llega hasta la tecnología operativa (OT) y los entornos de sistemas de control industrial (ICS). Las funciones combinadas incluyen ahora inspección/captura profunda de paquetes de más de 100 protocolos de IT/OT, asignación de red, análisis de flujo, supervisión de directivas y comportamientos, análisis forense de la red, evaluación de amenazas y clasificación de riesgos.

Segmentación dinámica de la red: Forescout también trabaja con firewalls de próxima generación, lo que ofrece puntos de decisión y aplicación para la segmentación dinámica basada en directivas. Los firewalls de próxima generación ofrecen control de red basado en el dispositivo del usuario, aplicación y clasificación del tráfico. Aprovechan el contexto de usuarios y dispositivos de una amplia variedad de fuentes, incluida la plataforma Forescout, a fin de aplicar directivas de acceso granulares con control preciso y flexible de los recursos. De este modo, las organizaciones de IT pueden implementar una segmentación dinámica de la red y crear en sus firewalls de próxima generación directivas de seguridad basadas en la información de contexto de los endpoints de Forescout.

Funciones de automatización y coordinación de Zero Trust

La plataforma Forescout coordina la administración de la seguridad en toda la infraestructura para hacer que productos de seguridad antes inconexos, trabajen como uno. Este conjunto exclusivo de tecnologías de interoperabilidad de redes, seguridad y administración se extiende y amplifica a través de la integración API mediante los productos Forescout eyeExtend a más de 70 productos de administración de IT y de seguridad de terceros*, lo que permite al sistema combinado acelerar la respuesta, conseguir mayores eficacias operativas y ofrecer una seguridad extraordinaria.

Forescout facilita la automatización y coordinación de la seguridad de tres formas:

- **Intercambio de información contextual en tiempo real:** Forescout supervisa continuamente y comparte de forma dinámica información detallada sobre la identidad, la configuración y la seguridad de los dispositivos endpoints con otros sistemas de seguridad y administración de su propiedad y que utilice. Este intercambio de datos bidireccional se añade a las propiedades generales que pueden aplicarse a los motores de reglas y a otras herramientas, lo mejora las directivas y las acciones.
- **Automatización de flujos de trabajo:** Forescout permite a los sistemas compartir decisiones basadas en directivas que anteriormente requerían análisis y aplicación manual en todos los sistemas. La automatización de estos flujos y procesos de trabajo se traduce en una respuesta coordinada e instantánea.
- **Automatización de las acciones de respuesta:** muchos productos de seguridad, como sistemas de detección de amenazas avanzada, administración de información y eventos de seguridad y herramientas de evaluación de vulnerabilidades pueden informar al personal de IT sobre problemas de seguridad. Forescout aplica al instante esta información de seguridad para activar una respuesta automatizada y hacer valer su amplia variedad de controles basados en directivas, como el aislamiento del dispositivo y la corrección del endpoint para eliminar las amenazas.

Funciones de cargas de trabajo de Zero Trust

La plataforma Forescout detecta, clasifica y crea un perfil de los servidores físicos y virtuales de los entornos de centros de datos/nube híbridos, aprovechando los distintos componentes de la infraestructura y las propias cargas de trabajo. Además, controla y supervisa las cargas de trabajo a medida que aumentan y disminuyen en el entorno de centro de datos/nube híbrido, evitando así lagunas de visibilidad. Forescout recopila propiedades de hipervisor o nube de nivel inferior hasta las aplicaciones instaladas/en ejecución en las cargas de trabajo y, a continuación, puede utilizar este contexto para garantizar que solo los usuarios y dispositivos autorizados disponen de acceso a cargas de trabajo específicas como respaldo a las directivas Zero Trust.

Funciones de usuario de Zero Trust

La plataforma Forescout se integra con sistemas de directorios e identidades para obtener la información de usuarios disponible, incluida la función y las autorizaciones de acceso a los recursos. Correlaciona esta información con los datos descubiertos en la configuración, el nivel de seguridad y de cumplimiento de los dispositivos, lo que permite tomar decisiones de acceso a los recursos basadas tanto en información de los dispositivos como de los usuarios. El comportamiento de los usuarios se supervisa de manera continua, y la integración con sistemas de acceso privilegiados detecta las cuentas de usuarios con permisos no conformes.

Funciones de datos de Zero Trust

Forescout es capaz de ofrecer seguridad a los datos en todos los dispositivos conectados mediante IP, lo que proporciona visibilidad de la presencia y estado operativo de cifrado, ofuscación y otro software de seguridad de la información que exija una directiva. Si faltan esas aplicaciones o están inactivas, Forescout puede tomar medidas basadas en directivas, como alertar al usuario, notificar a un administrador o poner en cuarentena el dispositivo hasta que haya sido corregido.

Para que tenga éxito Zero Trust, empiece por disponer de visibilidad total de los dispositivos

Forescout le ofrece muchas maneras de conocer mejor la plataforma Forescout:

- **Haga la prueba:** experimente el antes y el después de la plataforma Forescout con una prueba práctica que le mostrará seis convincentes casos de uso.
- **Solicite una demo:** visite la página de demos de Forescout para solicitar una demostración personal y acceder a toda una serie de demostraciones y vídeos complementarios bajo demanda.
- **Utilice la herramienta de cálculo de rentabilidad/valor de negocio de Forescout (en inglés):** cuantifique el valor de negocio que la plataforma Forescout puede ofrecer a su organización (según el modelo de IDC para calcular el valor de negocio) en solo 10 minutos.
- **Póngase en contacto con Forescout Consulting Services:** ¿Se encuentra en el proceso de diseñar su entorno para el modelo Zero Trust? Los asesores de Forescout cuentan con la formación, experiencia y certificación adecuadas para la implementación de productos, el desarrollo de procesos y la integración de sistemas, así como las mejores prácticas del acceso a la red y el cumplimiento de endpoints.

*A 31 de diciembre de 2018

***Notas**

1 "Cyber Incident and Breach Trends Report" (Informes sobre ciberincidentes y tendencias de fugas de datos), Online Trust Alliance, enero de 2018

2 "Cost of Data Breach Study" (Estudio sobre el coste de una fuga de datos), Ponemon Institute, junio de 2017

3 "The Zero Trust eXtended (ZTX) Ecosystem" (El ecosistema Zero Trust eXtended (ZTX), Forrester Research, enero de 2018

4 "The Zero Trust eXtended Ecosystem Road Map: The Zero Trust Security Playbook" (La hoja de ruta del ecosistema Zero Trust eXtended: manual sobre la seguridad Zero Trust), Forester Research, 11 de julio de 2019

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591

Más información en Forescout.com

© 2019 Forescout Technologies, Inc. Reservados todos los derechos. Forescout Technologies, Inc. es una empresa de Delaware. Encontrará la lista de nuestras marcas comerciales y patentes en www.forescout.com/company/legal/intellectual-property-patents-trademarks. Los demás nombres de marcas, productos o servicios pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios. Version 07_19