Seguridad escalable, flexible y automatizada para la implementación del IoT

Proteja datos, activos e infraestructura crítica con visibilidad, detección y corrección de amenazas en tiempo real

Desafío

El volumen y la variedad de dispositivos IoT hacen de la seguridad un desafío significativo. La mayoría de puntos de conexión IoT tienen huellas limitadas para la ejecución de funciones de seguridad, el personal de seguridad es escaso y las vulnerabilidades de día cero son cada vez mayores. Las soluciones tradicionales de seguridad perimetral no son suficientes.

Solución

La plataforma Software-Defined Secure Network de Juniper le permite usar toda su red existente como una plataforma unificada de ciberseguridad que utiliza los datos estadísticos, el aprendizaje automático y la automatización para mejorar su postura de seguridad y protegerse del crecimiento explosivo de los riesgos del IoT.

Ventajas

- Visibilidad completa de dispositivos, redes y aplicaciones del IoT
- Detección inteligente de amenazas conocidas y desconocidas con datos estadísticos de comportamiento y aprendizaje automático
- Corrección en tiempo real y control a través de la aplicación automatizada de políticas
- Cumplimiento con los requisitos de cumplimiento de las normativas NERC CIP, HIPPA y GDPR
- Protección escalable, flexible y automatizada en cualquier momento y lugar

En 2018, el Internet de las cosas (IoT) experimentará un importante punto de inflexión, ya que muchas empresas pasarán sus implementaciones de IoT de un punto de experimentación temprana a una escala empresarial.[1]

Este es un hito fundamental, que marca la entrada del IoT en el dominio de lo tradicional. Gartner, Inc. proyecta que para 2020, 20 400 millones de cosas conectadas estarán en uso en todo el mundo.[2] Asimismo, IHS Markit predice que el número de dispositivos IoT conectados se elevará a 125 000 millones para 2030.[3]

A medida que la escala de los puntos de conexión del IoT crece, la superficie de ataque crece a la par, lo que da a los ciberdelincuentes mayores oportunidades de realizar nuevas "hazañas". No es de extrañar que la seguridad sea la principal preocupación de las empresas que consideran adoptar el IoT.

El desafío

En los primeros días del IoT, la seguridad era meramente una idea. Los usuarios de hoy en día están pagando el precio de esa falta de previsión. AT&T informó que, en los últimos tres años, el número de atacantes que se dedica a escanear dispositivos IoT en busca de vulnerabilidades ha aumentado en un 3198 %.[4] En 2016, aproximadamente 100 000 dispositivos IoT fueron infectados por el malware Mirai, lo que los convirtió en botnets que lanzaron una gran cantidad (1,2 Tbps) de ataques distribuidos por denegación de servicio (DDoS) contra el sistema de nombres de dominio (DNS) del proveedor de servicio Dyn. Estos ataques provocaron una interrupción que duró más de dos horas y que afectó a importantes proveedores de servicios Web como Twitter, Spotify y Github.

Se calcula que, para las empresas con ingresos anuales de USD 2000 millones o más, el costo potencial de una violación del IoT representa más de USD 20 millones.[5] Además de pérdidas financieras, las violaciones del IoT también pueden causar daños físicos e incluso amenazar la seguridad de las personas. En 2015, Chrysler retiró del mercado 1,4 millones de vehículos después de que unos hackers demostraran que podían secuestrar de manera remota los sistemas digitales de un Jeep. Ese mismo año, un malware de IoT ruso dirigido a la red eléctrica ucraniana, dejó sin energía eléctrica a 230 000 personas.[6]

[1] https://go.forrester.com/blogs/predictions-2018-iot-will-move-from-experimentation-to-business-scale/
[2] https://www.gartner.com/newsroom/id/3598917
[3] https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
[4] https://www.business.att.com/cybersecurity/archives/v4/emerging-vulnerabilities/
[5] https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security
[6] https://www.forbes.com/sites/thomasbrewster/2015/07/24/chrysler-recall-exploit/

Gráfico 1: El Internet de las Cosas

Desafíos de seguridad únicos del IoT

En comparación con los dispositivos conectados tradicionales, como computadoras portátiles, teléfonos móviles y tablets, los dispositivos conectados al IoT tienen sus propios problemas de seguridad. Por ejemplo:

- Muchos dispositivos IoT son pequeños, de baja potencia y de bajo costo, con limitaciones de cálculo y de memoria para procesar funciones de seguridad. Esta es la razón por la que la propia red es tan importante para mitigar las amenazas del IoT.
- Los equipos de operaciones de seguridad deben ir a la par con el crecimiento exponencial de los dispositivos IoT. Por lo tanto, la seguridad de la automatización es fundamental para la implementación del IoT a gran escala.
- La variedad de dispositivos IoT (tipos, sistemas operativos, fabricantes, etc.) representa una gran cantidad de vulnerabilidades de día cero desconocidas que los hackers pueden aprovechar. Las empresas deben utilizar los datos estadísticos de seguridad y el aprendizaje automático para detectar amenazas desconocidas y defenderse contra estos ataques al IoT.
- La tradicional seguridad perimetral asume que todo lo que está fuera del firewall no es confiable, mientras que todo lo que está dentro de este sí lo es. Este enfoque no considera escenarios de IoT en los que los dispositivos internos se ven afectados. Se requiere una nueva perspectiva.

La solución de seguridad de IoT de Juniper Networks

La solución de seguridad de IoT de Juniper incluye los siguientes componentes.

- Puertas de enlace de servicios serie SRX de **Juniper Networks® y firewalls de contenedor y virtuales vSRX/cSRX:** puertas de enlace de servicios virtuales vSRX y físicas serie SRX de Juniper Networks que proporcionan protección de nivel de firewall de última generación (NGFW) con sensibilización de aplicación integrada, prevención de intrusiones y controles de usuario basados en roles, así como la mejor administración unificada de amenazas (UTM) para proteger los activos de la empresa. Los firewalls vSRX y de la serie SRX pueden administrarse de forma centralizada a través de la aplicación de administración Security Director de Juniper Networks Junos Space®.

  El firewall de contenedor cSRX funciona sin sobrecarga de sistema operativo invitado, tiene un tamaño considerablemente menor, y es más fácil de migrar o descargar. Utiliza menos memoria, y su tiempo de aceleración se mide en subsegundos, lo que en suma conduce a una mayor densidad a un menor costo, lo cual es perfecto para diversos casos de uso del IoT.

  Para obtener más información acerca de los firewalls de última generación serie SRX, visite www.juniper.net/us/en/products-services/security/srx-series/.

- **Security Director de Junos Space:** la aplicación de administración escalable e intuitiva Security Director de Juniper permite a los usuarios empresariales tomar decisiones precisas y lograr una visibilidad completa de las aplicaciones, los usuarios y las amenazas a través de sus firewalls virtuales serie SRX. Gracias a una visión holística, a un sólido conjunto de características de seguridad y a una inteligencia procesable fácil de utilizar como la inteligencia de amenazas recibida de Juniper Sky™ Advanced Threat Prevention y Juniper Sky ATP Appliance (ver a continuación), Security Director le ofrece la posibilidad de crear políticas de seguridad que le permitan tomar medidas correctivas y bloquear las aplicaciones y amenazas de alto riesgo. Al ofrecer un solo panel de vidrio, un asistente de creación de reglas de seguridad inteligente fácil de usar y una función de aplicación de reglas automáticas, Security Director permite crear políticas de seguridad menos complejas más rápidamente.

  Policy Enforcer, un componente de Security Director, es un módulo central de inteligencia que se comunica con los elementos de red de múltiples proveedores y productos de seguridad para consolidar la inteligencia de amenazas desde diferentes fuentes a través de la red, proporcionar datos estadísticos, y reforzar las políticas de seguridad de manera global; desde el borde hasta la nube.

  Para obtener más información acerca de Security Director, visite www.juniper.net/us/en/products-services/security/security-director.

- **Juniper Sky Advanced Threat Prevention:** un servicio basado en la nube integrado con el Security Director de Junos Space y los firewalls serie SRX, Juniper Sky ATP ofrece capacidades de inspección profunda, bloqueo en línea y alertas procesables, y es capaz de adaptarse continuamente a un panorama de amenazas en constante cambio mediante el aprovechamiento de la información en tiempo real desde la nube. La tecnología de identificación de Juniper Sky ATP utiliza una variedad de técnicas sofisticadas para detectar y prevenir ataques cibernéticos rápidamente. Estas incluyen:
  - Algoritmos de aprendizaje automático potentes
  - Análisis dinámico con técnicas para inducir al malware a activarse y autoidentificarse
  - Búsquedas rápidas en la caché para acelerar la identificación del malware anterior

  - Motor antivirus basado en firmas para identificar archivos conocidos
  - Análisis estático para estudiar el código de software e identificar posibles fragmentos peligrosos

  Para obtener más información acerca de Juniper Sky ATP, visite www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/.

- **Juniper Advanced Threat Prevention Appliance:** la solución Juniper ATP Appliance proporciona protección completa en las instalaciones contra un panorama de amenazas sofisticado y en constante cambio.

  Con las herramientas tradicionales de seguridad basadas en firmas, los ataques de día cero suelen pasar inadvertidos. Gracias al aprovechamiento del aprendizaje automático avanzado y al análisis de comportamiento, Juniper ATP Appliance puede identificar amenazas avanzadas existentes y desconocidas en tiempo casi real a través de una detección continua y de varias etapas, así como del análisis del tráfico web, del correo electrónico y de la propagación lateral.

  Juniper ATP Appliance recibe fuentes de varios dispositivos de seguridad, aplica análisis estadístico para identificar rasgos maliciosos avanzados y agrega los eventos en una sola línea de tiempo completa en la que aparecen todas las amenazas de la red. Los equipos de seguridad pueden determinar rápidamente cómo ocurrió el ataque y priorizar con facilidad las alertas críticas.

  Para obtener más información acerca de Juniper ATP Appliance, visite www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/.

- **Juniper Secure Analytics:** Juniper Networks JSA Series Secure Analytics Appliances permite combinar, analizar y gestionar una cantidad inigualable de datos de vigilancia (comportamiento de la red, incidentes de seguridad, perfiles de vulnerabilidad e información de amenazas), lo que permite a las empresas automatizar el análisis de grandes conjuntos de datos y administrar eficientemente las operaciones empresariales desde una única consola. Como un componente clave de la plataforma SDSN, JSA Series Secure Analytics se integra también con el software de gestión central Security Director, y proporciona información de inteligencia en tiempo real para una rápida corrección de amenazas y la aplicación directa de políticas a través de la red.

  Para obtener más información acerca de la cartera de opciones de JSA Series Secure Analytics, visite www.juniper.net/us/en/products-services/cecurity/secureanalytics/.

Características y ventajas

La solución de seguridad de IoT de Juniper le permite convertir su red en un único dominio de aplicación generalizado, que utiliza a la vez los análisis estadísticos, el aprendizaje automático y la automatización para ofrecer una visibilidad, detección y corrección de amenazas en tiempo real.

- **Visibilidad completa de dispositivos, redes y aplicaciones del IoT:** si no puede ver la amenaza, no podrá defenderse de ella. Esta es la razón por la que la visibilidad es muy importante.
- **Visibilidad de dispositivos IoT:** cuando un punto de conexión de IoT se conecta a la red, los conmutadores de acceso de Juniper aprovechan los servidores AAA existentes basados en estándares (RADIUS/DHCP/AD/LDAP), así como la integración con el control de acceso a la red (NAC) y los socios de tecnología de seguridad como ForeScout, Aruba ClearPass e Impulse Point, para proporcionar la incorporación y la generación de perfiles de dispositivos. Esto ofrece a los clientes una considerable flexibilidad de implementación, lo que les permite elegir entre opciones alámbricas o inalámbricas, con agente o sin agente, y si desean compatibilidad con el estándar 802.1X. Además, le brinda una visibilidad completa de los dispositivos IoT y del tráfico de red, lo que le permite aplicar políticas de seguridad e implementar la segmentación de la red del IoT.
- **Visibilidad de la red del IoT:** como una solución líder en gestión de eventos e información de seguridad (SIEM), JSA Series Secure Analytics continuamente recopila, agrega, almacena y analiza datos de eventos de Juniper y de dispositivos de red de terceros, lo que ofrece una imagen completa del funcionamiento de la infraestructura de la red en tiempo real y permite identificar comportamientos inusuales. A medida que el número de objetos de red crece, junto con la cantidad de parámetros que se genera, el tradicional modelo de extracción utilizado por SNMP y la CLI (el cual requiere de un procesamiento adicional para realizar sondeos regulares) limita la escalabilidad. Junos Telemetry Interface (JTI), una característica del sistema operativo de Juniper Networks Junos, supera estas limitaciones mediante la adopción de un modelo push que entrega datos de forma asíncrona, lo que elimina la necesidad de realizar sondeos. Una solicitud de datos se envía una sola vez mediante una estación de administración para transmitir actualizaciones periódicas. Como resultado, la JTI es altamente escalable y permite el monitoreo de miles de objetos de red.
- **Visibilidad de aplicaciones del IoT:** Juniper Networks AppSecure, una característica básica de los firewalls de última generación serie SRX , proporciona un potente mecanismo para reconocer instantáneamente incluso las nuevas aplicaciones mediante técnicas que permiten identificar todas las aplicaciones que circulan por la red, independientemente del puerto, del protocolo o del método de cifrado que se utilicen. Gracias a que ofrece visibilidad y control de aplicaciones profundos, AppSecure proporciona el contexto que vincula el uso de aplicaciones al usuario, independientemente de la ubicación y del dispositivo. Con un diseño que permite comprender los comportamientos de las aplicaciones e identificar vulnerabilidades, AppSecure bloquea las amenazas de seguridad transmitidas por las aplicaciones antes de que puedan causar algún daño. Además, Security Director de Junos Space proporciona una forma sencilla e intuitiva de identificar las aplicaciones que utilizan más ancho de banda, que tienen la mayoría de los períodos de sesiones o que están en mayor riesgo.
- **Detección inteligente de amenazas conocidas y desconocidas con análisis de comportamiento y aprendizaje automático:** el volumen de los intercambios de datos y dispositivos IoT puede hacer que la detección de amenazas sea extremadamente difícil.

  Los dispositivos serie SRX incluyen un sistema de prevención de intrusiones (IPS) que proporciona protección completa

contra una amplia gama de vulnerabilidades de seguridad conocidas en aplicaciones, bases de datos y sistemas operativos. Las puertas de enlace de servicios serie SRX buscan constantemente nuevos ataques contra vulnerabilidades recién descubiertas y se aseguran de que la protección de red esté actualizada con los últimos métodos de ataque.

En el caso de las amenazas desconocidas, como los ataques de día cero, la oferta de prevención avanzada de amenazas de Juniper (Juniper Sky ATP basada en la nube y Juniper ATP Appliance para implementación en las instalaciones) proporciona detección de amenazas avanzada a través del aprendizaje automático y el análisis de comportamiento. Los clientes obtienen la capacidad para medir el comportamiento normal de los dispositivos IoT con el objeto de detectar anomalías de comportamiento, activar defensas contra ataques y evitar interrupciones mayores por amenazas de IoT mediante la identificación de amenazas "desconocidas" como ataques conocidos.

- **Control y corrección en tiempo real a través de la aplicación automatizada de políticas:** si examinamos los incidentes de seguridad del pasado, encontramos que la mayoría de sistemas detectaron los ataques y enviaron alertas. Sin embargo, a menudo tardaba horas o, en algunos casos, días reaccionar de forma manual; y para entonces, el daño ya estaba hecho. Con el IoT a gran escala, la automatización de seguridad es necesaria para que los equipos de operaciones puedan ir a la par con el ritmo de crecimiento. Diferentes escenarios requieren diferentes tratamientos; por ejemplo, si una cámara de vigilancia se infecta, puede simplemente desconectarla de la red, mientras que un ataque en, digamos, una línea de fabricación de automóviles requeriría de una interrupción no planificada que podría costar a la empresa USD 22 000 por minuto o USD 1,3 millones por hora[7].

[7] www.businessinsider.com/what-1-minute-of-unplanned-downtime-costs-major-industries-2016-9

La solución SDSN de Juniper le permite definir políticas amplias y flexibles para adaptarse a los diferentes escenarios de IoT y tomar decisiones de aplicación automatizada de políticas coherentes a través de cualquier proveedor, cualquier nube, en cualquier lugar, lo que permite simplificar las operaciones de seguridad generales. Por ejemplo, cuando un dispositivo IoT se infecta con malware e intenta iniciar comunicaciones con un servidor de comando y control (C&C), Juniper Sky ATP o Juniper ATP Appliance detectan este comportamiento anormal y lo comunican de inmediato al componente de aplicación de políticas de Security Director. El componente de aplicación de políticas aplica automáticamente una respuesta predefinida para poner en cuarentena el dispositivo infectado, impide la propagación del malware y soluciona la amenaza; todo en tiempo real.

El flujo de trabajo de remediación se desarrolla de la siguiente manera, y como se muestra en el gráfico 2:

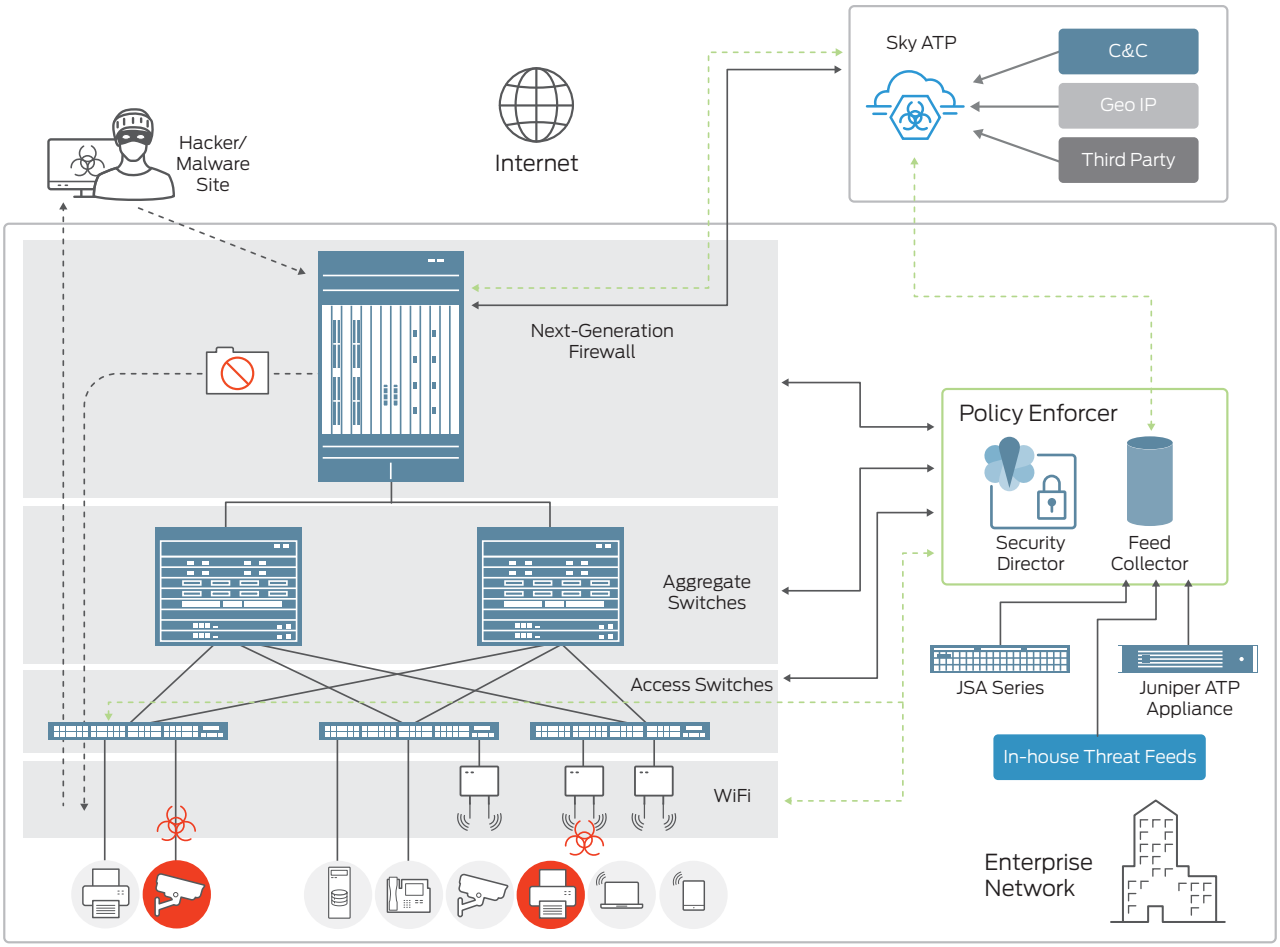

Gráfico 2: Arquitectura de la solución de seguridad de IoT de Juniper

- Un dispositivo IoT infectado conectado a la red intenta descargar un archivo restringido o lanza un ataque contra la infraestructura crítica.
- JSA Series Secure Analytics y ATP Appliance registran el intento de descarga no autorizada y lo comunican al componente de aplicación de políticas del Director de Seguridad de Junos Space.
- El componente de aplicación de políticas aplica una lista de control de acceso/regla de control de acceso de red al puerto de conmutación afectado o al punto de acceso Wi-Fi para poner en cuarentena el host, lo que soluciona rápidamente la amenaza.

- **Cumplimiento de las normativas NERC CIP, HIPPA y GDPR:** con más dispositivos conectados a la red empresarial, mientras cada uno de ellos genera más y más datos, la necesidad de cumplir la normativa es cada vez más crítica.

  Además del tradicional protocolo IP y los protocolos heredados como MODBUS para el sistema Supervisory Control and Data Acquisition/Industrial Control Systems (SCADA/ICS), una serie de nuevos protocolos específicos del IoT como Message Queue Telemetry Transport (MQTT) y el protocolo Constrained Application Protocol (CoAP) también están abriéndose camino hacia el dominio de lo tradicional. Para estar al día con la normativa, las empresas deben ser capaces de identificar las fuentes de comunicación y controlar el tráfico en función de los protocolos IoT utilizados. El IPS de Juniper, disponible en las Puertas de enlace de servicios serie SRX, admite la mayoría de firmas de las aplicaciones de IoT, y permite también a los usuarios finales escribir firmas de aplicaciones personalizadas para satisfacer sus necesidades específicas. Security Director facilita la identificación de las aplicaciones que están en uso y ofrece la posibilidad de modificar las firmas de aplicaciones.

  Los dispositivos de la serie JSA facilitan y automatizan el cumplimiento normativo a través de herramientas potentes de recopilación, correlación y generación de informes. Realiza periódicamente análisis de red y mantiene registros de auditoría detallados con el fin de facilitar el cumplimiento de regulaciones federales o de la industria. La serie JSA está al día con múltiples reglamentaciones y prácticas recomendadas en materia de seguridad, e incluye más de 500 plantillas de informe listas y orientadas al cumplimiento para satisfacer las necesidades específicas de auditoría y generación de informes.

- **Protección escalable, flexible y automatizada en cualquier momento y lugar:** aunque muchos escenarios de IoT enfrentan vulnerabilidades de seguridad similares a las de los entornos de TI tradicionales, el enorme número de dispositivos IoT aumenta considerablemente los requisitos de escalabilidad. Los sensores de IoT pueden crear literalmente millones de sesiones cortas para intercambiar información con aplicaciones de IoT. Además, un gran número de dispositivos IoT estarán ubicados en lugares remotos; algunos incluso podrían estar en constante movimiento. El concepto tradicional de "perímetro" no se aplica en el contexto de IoT. Las amenazas vendrán desde cualquier lugar, por lo que la protección de la seguridad debe aplicarse en todas partes.

  Las líneas SRX4000 y SRX5000 de las puertas de enlace de servicios, ya implementadas en la infraestructura crítica, como las que protegen las extensas redes eléctricas en América del Norte, ofrecen la capacidad de sesión y de muchas conexiones por segundo necesaria para respaldar estas sesiones en implementaciones de IoT a gran escala. Los factores de forma físicos, virtuales y contenerizados flexibles de la serie SRX, grandes y pequeños, permiten colocarlos donde usted quiera, desde un extremo del IoT como un servidor de computación de borde móvil (MEC, Mobile-Edge Computing) o una puerta de enlace de IoT, hasta el interior de un automóvil, o una nube, ya sea pública, privada, híbrida o múltiple. El componente de aplicación de políticas permite aplicar de forma coherente las políticas de seguridad automatizadas, no solo a través de Juniper, sino también de equipos de terceros, lo que le brinda una verdadera protección integral.

Resumen: la seguridad del IoT a gran escala requiere de un cambio de paradigma

Teniendo en cuenta que adoptará tecnologías de IoT en su empresa, con una implementación a gran escala como siguiente paso, deberá abordar la seguridad de forma integral. Las violaciones del IoT suponen grandes pérdidas económicas, daños de reputación y una amenaza para la seguridad de las personas.

Cuando se realiza una implementación a escala, el volumen y la variedad de dispositivos IoT, así como su intercambio de datos, hacen que la seguridad sea un desafío significativo. La mayoría de puntos de conexión del IoT tienen recursos limitados para ejecutar funciones de seguridad, lo que hace que el papel de la red en la mitigación de riesgos sea cada vez más fundamental. Para la mayoría de empresas, el personal de seguridad es un recurso escaso, por lo que, con implementaciones de IoT a escala, mantener sus sistemas seguros será un enorme desafío operativo. Los ciberdelincuentes también seguirán llevando a cabo nuevos ataques, especialmente explosivos, de amenazas de día cero, lo que hace que las soluciones tradiciones de seguridad perimetral sean insuficientes.

El IoT a gran escala requiere de un cambio de paradigma de seguridad. A diferencia de los productos puntuales centrados en acciones individuales, la solución de seguridad de IoT de Juniper, Software-Defined Secure Network, permite emplear toda la red como una plataforma unificada de ciberseguridad que aprovecha los datos estadísticos, el aprendizaje automático y la automatización para mejorar su postura de seguridad defensiva contra la expansión de los riesgos del IoT. La red SDSN de Juniper es escalable, flexible y automatizada, y protege sus datos, activos e infraestructura crítica de IoT en cualquier momento y lugar.

Próximos pasos

Para obtener más información acerca de las soluciones de seguridad de Juniper, visite www.juniper.net/us/en/products-services/security o comuníquese con un representante de Juniper Networks.

Acerca de Juniper Networks

Juniper Networks incorpora la simplicidad a las redes con productos, soluciones y servicios que conectan el mundo. A través de la innovación en ingeniería, eliminamos las dificultades y complejidades de las redes en la era de la nube para resolver los problemas más complejos a los que nuestros clientes y asociados se enfrentan cada día. En Juniper Networks, creemos que la red es un medio para compartir el progreso humano y los conocimientos que cambian el mundo. Nuestro compromiso es imaginar formas innovadoras de ofrecer redes automatizadas, escalables y seguras que permitan moverse a la velocidad de los negocios.

Sede corporativa y de ventas
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 EE. UU.
Teléfono: 888.JUNIPER (888.586.4737)
o +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

Sedes en APAC y EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Ámsterdam, Países Bajos
Teléfono: +31.0.207.125.700
Fax: +31.0.207.125.701

3510636-002-ES-MX Abr 2018