FORESCOUT

Novedades de Forescout 8.1

La transformación digital sigue imparable y las empresas conectan cada vez más dispositivos inteligentes a sus redes para automatizar las operaciones empresariales e incrementar la eficiencia. Ya sean del IoT, IIoT o de OT, estos dispositivos implican un crecimiento y una diversidad sin precedentes de las redes empresariales.

Para facilitar esta transformación, las empresas deben incrementar su capacidad de conectividad e intercambio de información entre redes que eran diferentes. Esto está acelerando la convergencia de la tecnología de la información (TI) y la tecnología operativa (OT), y crea nuevos flujos de datos entre dispositivos de TI conectados a campus, aplicaciones alojadas en la nube y sistemas tecnológicos operativos. Si bien existen ventajas, los riesgos también aumentan, ya que los atacantes pueden desplazarse lateralmente por estas redes que se han interconectado, con el objetivo de acceder a información confidencial o provocar una paralización de la empresa.

> "Para 2021, los departamentos del CIO, CISO o CSO se encargarán del 70 % de la seguridad de TO, en comparación con el 35 % que lo hacen en la actualidad[1]".
> *– Gartner, mayo de 2018*

La convergencia de la TI y la OT plantea nuevas exigencias a los CIO y los CISO que deben encargarse ahora de la protección del ecosistema completo de la empresa. Los equipos de TI ya no son solamente responsables de la administración de los dispositivos, aplicaciones y datos de los usuarios; ahora deben garantizar la ejecución de operaciones empresariales seguras y eficientes. Para afrontar este reto, necesitan visibilidad y control total de los dispositivos.

Forescout 8.1: Visibilidad y control unificados de los dispositivos para la seguridad de TI y OT

Forescout 8.1 es la primera plataforma de visibilidad y control unificados de los dispositivos para las redes de TI y OT convergentes. Esta herramienta permite a las empresas obtener información de contexto de todos los dispositivos en un entorno interconectado, y orquestar medidas para mitigar los riesgos cibernéticos y operativos. Entre sus nuevas funciones se incluyen:

- La visibilidad de los entornos de conmutación industrial Cisco ACI, Microsoft Azure y Belden amplía la cobertura a los centros de datos, las redes de OT y la nube, para ofrecer a las empresas la visión que necesitan de los dominios de TI y OT.
- Las importantes mejoras de la clasificación automática para dispositivos IoT y de OT, la evaluación de vulnerabilidades para sistemas de control industrial (ICS) y la detección de dispositivos no autorizados incrementan la ciberresiliencia de las redes de TI y OT.
- La orquestación para la segmentación con firewalls Fortinet y con Cisco DNA Center, y la respuesta a incidentes con ServiceNow mejoran la capacidad para automatizar los controles y efectuar las operaciones de seguridad de manera eficaz.
- Una capacidad de adaptación inigualable de hasta 2 millones de dispositivos en un solo despliegue que comprende entornos físicos, virtuales, de nube o híbridos.

Escala empresarial

Administración de 2 millones de dispositivos en un solo despliegue que comprende entornos físicos, virtuales, de nube o híbridos.

Descubrimiento de dispositivos

Nueva visibilidad de los entornos de conmutación industrial Microsoft Azure, Cisco ACI y Belden, así como de las capas más bajas de la pila de red de OT.

Clasificación automática

La nueva inspección profunda de paquetes de más de 100 protocolos de TI y OT hace posible la clasificación automática de dispositivos médicos, industriales, de automatización de edificios y del IoT.

Evaluación de riesgos

La nueva evaluación de vulnerabilidades de dispositivos de OT e ICS, y no autorizados, destinada a identificar y detener a los imitadores incrementa la ciberresiliencia.

Automatización del control

Nueva orquestación para segmentación de la red con firewalls Fortinet y Cisco DNA Center, así como respuesta a incidentes con ServiceNow ITSM y Security Operations.

Descubrimiento de dispositivos ampliado

La seguridad empieza por saber qué hay en la red. Esto supone identificar todos los dispositivos en el momento en el que se conectan. En 2019, se espera que haya 900 millones de dispositivos físicos y virtuales más en las redes de las empresas. Una gran mayoría de este crecimiento se debe a los dispositivos IoT y de OT, así como a instancias de la nube pública y privada.

> "Para 2023, el CIO medio será responsable de más del triple de endpoints que gestionaba en 2018[2]".
> *– Gartner, septiembre de 2018*

- Forescout 8.1 sigue ampliando la visibilidad en estas áreas para proporcionar una visión unificada de todos los dispositivos en campus, centros de datos, la nube y redes de OT.
- La visibilidad de varias nubes incluye ahora Microsoft Azure, además de AWS y VMware.
- La integración con Cisco ACI aporta visibilidad de los entornos SDN para centros de datos.
- La integración con los productos de conmutación industrial de Belden ofrece una mayor visibilidad de las redes de OT.
- La supervisión pasiva en las capas más bajas de la pila de red de OT proporciona visibilidad de dispositivos de supervisión, control de procesos e instrumentación.

Excelente clasificación automática

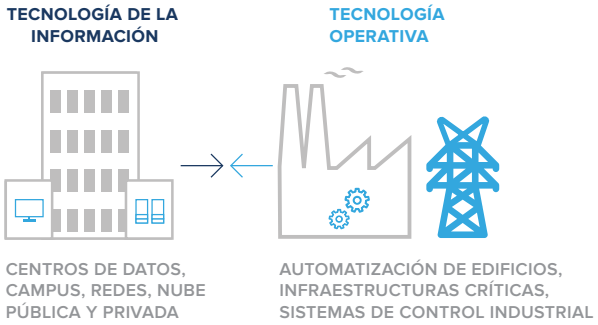
La diversidad de dispositivos IoT y de OT dificulta a las empresas su identificación y catalogación precisas. Sin una clasificación granular, es difícil crear e implementar directivas selectivas para proteger estos dispositivos. Forescout 8.1 incluye amplias mejoras que permiten clasificar automáticamente un mayor número de sus dispositivos y aprovechar este contexto para aplicar directivas con:

- Amplia cobertura para identificar más de 500 versiones de sistemas operativos y más de 5000 proveedores y modelos de dispositivos.
- Clasificación de dispositivos médicos para más de 350 proveedores de tecnología de asistencia sanitaria, incluidos los 20 principales de la lista Global Top 20.
- Nueva inspección profunda de paquetes de más de 100 protocolos de TI y OT para la clasificación automática de miles de dispositivos de automatización industrial de infraestructuras de fabricación, energía, gas y petróleo, servicios públicos, minería y otros sectores críticos.
- Mejor eficacia, velocidad y cobertura de la clasificación gracias a Forescout Device Cloud, con más de 8 millones de dispositivos en entornos de TI, IoT y OT.

Evaluación de riesgos de distintos dominios

Evaluación de vulnerabilidades de OT

Con la creciente conectividad entre redes de TI y de OT, es importante conocer el perfil de riesgo de los dispositivos de los dos dominios. Los dispositivos vulnerables a los dos lados pueden sufrir ataques, y las amenazas atravesarían los dominios y podrían provocar una interrupción de la actividad en la empresa y pérdidas financieras.



- Forescout 8.1 incorpora la evaluación de vulnerabilidades de OT e ICS a las funciones para Windows existentes, y de esta forma ofrece información de los dispositivos de alto riesgo de su red.
- Las frecuentes actualizaciones de Forescout permiten contar con la última información sobre vulnerabilidades y riesgos comunes (CVE) para ICS, con el fin de identificar los dispositivos vulnerables y orquestar las medidas de corrección pertinentes.
- En el caso de los dispositivos industriales y operativos vulnerables que solo se pueden reparar o corregir con parches durante un período de mantenimiento programado, Forescout puede implementar controles de mitigación, como la segmentación de dichos dispositivos en zonas de la red "seguras" hasta que llegue ese momento.

Detección de dispositivos no autorizados

Otra dificultad derivada del incremento de los dispositivos IoT y de OT es la suplantación de dispositivos y la falsificación de direcciones MAC. Los autores de las amenazas que pretenden conseguir acceso a las redes tienen a su disposición una mayor fuente de direcciones MAC, ya que los dispositivos IoT y de OT suelen incluirse en extensas listas blancas para facilitar el acceso a la red. Estos dispositivos tienen con frecuencia pantallas no protegidas que pueden revelar su dirección MAC a cualquiera que pase por ahí. Los falsificadores pueden hacerse pasar fácilmente por dispositivos legítimos, a fin de conseguir acceder a la red y provocar una paralización de la actividad u obtener información confidencial.

Forescout 8.1 incluye una nueva detección de dispositivos no autorizados, pendiente de patente, para identificar y detener a los imitadores que utilizan técnicas de falsificación de direcciones MAC.

- La supervisión continua de la red detecta varios casos de falsificación en redes cableadas e inalámbricas, como conexiones simultáneas, suplantaciones en la misma ubicación y suplantaciones en distinta ubicación.
- Forescout identifica los dispositivos de la víctima y el falsificador, y en función de las directivas, puede bloquear los intentos de suplantación para evitar el acceso malicioso.
- Forescout le permite demostrar su resistencia a la falsificación de direcciones MAC ante los auditores y mejorar el resultado de la auditoría.

Orquestación y automatización del control

Los equipos de seguridad de TI se ven desbordados por una multitud de problemas de seguridad y cumplimiento de normativas que comunican herramientas de seguridad que carecen del suficiente contexto de los dispositivos para efectuar la priorización o de las funciones de automatización para aplicar los controles. Como resultado, los equipos de profesionales especialistas en seguridad pierden el tiempo resolviendo manualmente problemas menores, mientras son incapaces de centrarse en la reducción proactiva de los riesgos o la rápida respuesta a amenazas. Forescout 8.1 le ofrece el contexto de los dispositivos, así como la posibilidad de orquestar acciones y automatizar los controles.

> "Para 2021, el 70 % de las empresas incluirán funciones de automatización, orquestación y respuesta de seguridad, ya sea a través de su SIEM o mediante una plataforma dedicada, a diferencia del 5 % que las incluían en 2018[3]".
> *– Gartner, diciembre de 2018*

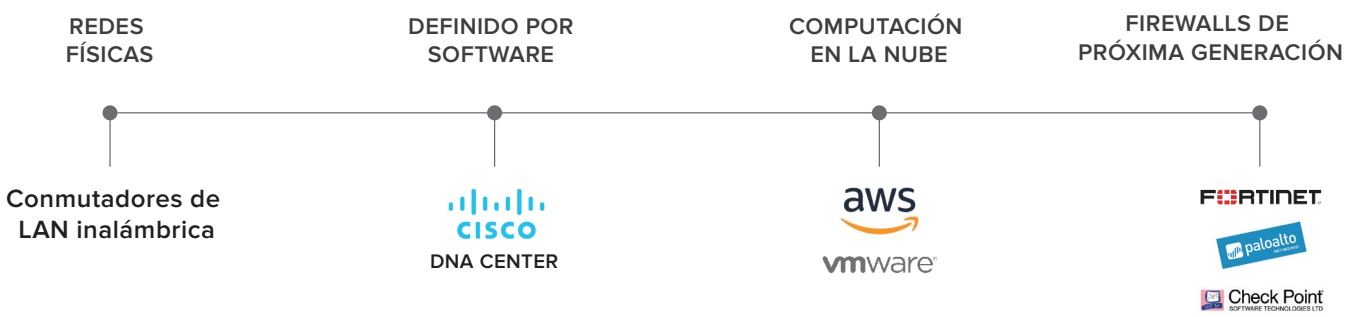
Segmentación de la red

Cuando las empresas definen sus arquitecturas de seguridad de próxima generación para IoT y OT, la segmentación juega un papel fundamental. A diferencia de los dispositivos tradicionales, los del IoT y de OT no se pueden corregir con parches ni proteger con agentes con regularidad. Por lo tanto, la segmentación de estos dispositivos en zonas de seguridad lógicas es esencial para reducir los riesgos.

Forescout 8.1 le permite organizar la segmentación en varias tecnologías, incluidas algunas integraciones nuevas:

- Automatización de los controles de segmentación con firewalls Fortinet, además de la orquestación existente con Palo Alto Networks y Check Point, para proporcionar compatibilidad heterogénea con firewalls de próxima generación.
- Orquestación de controles de segmentación con Cisco DNA Center, además de las integraciones existentes con tecnologías de red definida por software y la nube, como VMware NSX y AWS.

Segmentación de redes de varios dominios



Automatización de repuesta a incidentes

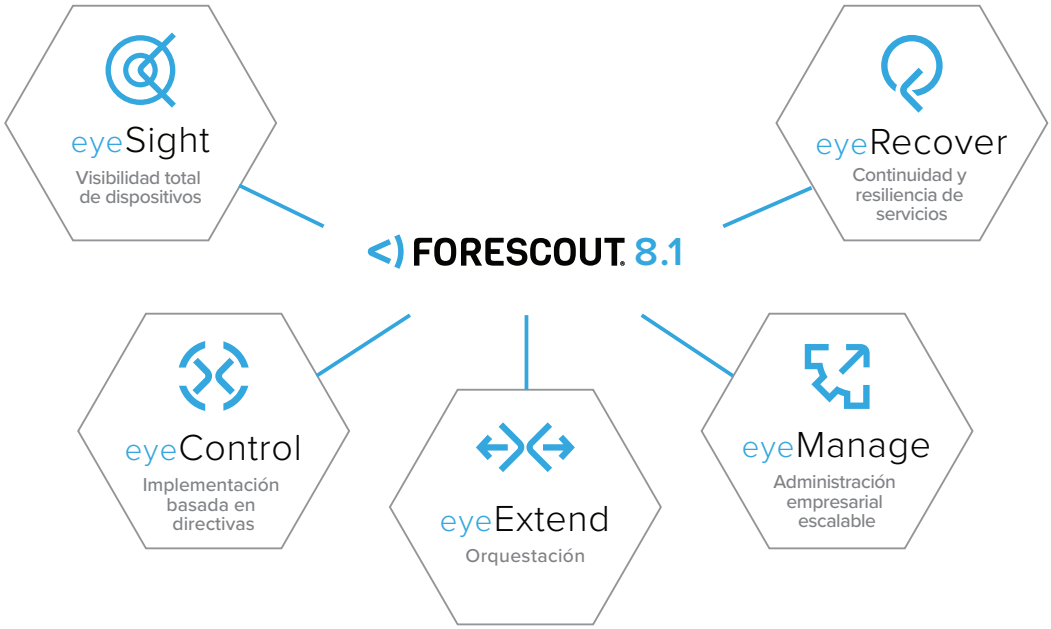
Los equipos de TI y seguridad cada vez se plantean más automatizar la respuesta como medio para afrontar los problemas de bajo riesgo, de manera que sus recursos más especializados puedan centrarse en la mitigación de riesgos y otras áreas del negocio más relevantes. Forescout 8.1 se integra ahora con ServiceNow ITSM y Security Operations para automatizar y acelerar la respuesta a incidentes.

- La nueva orquestación con ServiceNow ITSM automatiza la creación de incidencias de servicio, así como la respuesta basada en directivas para la conformidad de la configuración.
- La nueva orquestación con ServiceNow Security Operations automatiza la creación de incidentes de seguridad y la respuesta a amenazas para dispositivos de alto riesgo o comprometidos.
- La orquestación ampliada con ServiceNow CMDB actualiza Configuration Items (CI), una vez finalizada la reparación del incidente para facilitar un servicio completo y los flujos de administración de la seguridad.

Una plataforma flexible y escalable

Forescout 8.1 proporciona una escala y una flexibilidad de despliegue inigualables para satisfacer los exigentes requisitos de los entornos de grandes empresas:

- Con una sola instalación puede gestionar hasta dos millones de dispositivos físicos o virtuales en su campus, centro de datos, la nube o redes de OT.
- Una suite de productos modulares ofrece flexibilidad para adaptarse en función de cómo cambien las necesidades de su empresa. Empezando por Forescout eyeSight, que aporta visibilidad de los dispositivos, con cada producto que añada disfrutará de eficaces funciones para la automatización de controles, la orquestación de la seguridad, la resiliencia operativa y la seguridad de OT.
- Para tener flexibilidad en la compra, todos los productos de software de Forescout están ahora disponibles como licencia perpetua o bien a través de una suscripción por un período.



1 2018 Strategic Roadmap for Integrated IT Security, Gartner, mayo de 2018
2 Gartner Top Strategic IoT Trends and Technologies Through 2023, septiembre, 2018
3 Gartner, Emerging Technology Analysis: SOAR Solutions, 7 de diciembre de 2018, Eric Ahlm

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Teléfono gratuito (EE. UU.)
1-866-377-8771
Tel. (internacional) +1-408-213-3191
Soporte técnico 1-708-237-6591

Más información en Forescout.com