FORESCOUT

HAWORTH®

Haworth

Este fabricante mundial protege su red de IT y OT con Forescout y rentabiliza extraordinariamente la inversión

SECTOR

Fabricación

ENTORNO

12 000 dispositivos alámbricos e inalámbricos en 20 centros de producción y 55 oficinas en todo el mundo; 6200 empleados.

PROBLEMA

- Falta de visibilidad de todos los dispositivos de la red, incluidos los dispositivos IoT y de OT
- Visibilidad insuficiente del estado de seguridad de las empresas recién adquiridas
- Necesidad de funcionamiento continuo en el entorno de OT
- Equipo de seguridad pequeño con tiempo y recursos limitados

SOLUCIÓN

- Plataforma Forescout
- Forescout Enterprise Manager
- Forescout eyeExtend Module for Palo Alto Networks Next-Generation Firewall

CASOS DE USO

- Visibilidad de dispositivos
- Conformidad de dispositivos
- Control de acceso a la red
- Segmentación de la red
- Respuesta ante incidentes

Descripción

Apostando por la innovación y la productividad, Haworth Inc. diseña y fabrica espacios de trabajo adaptables, lo que incluye pavimentos elevados, paredes móviles, sistemas modulares para oficinas, sillería y dispositivos con tecnología alámbrica e inalámbrica Workware™ para colaborar en tiempo real. Esta empresa internacional con oficinas en Madrid y Barcelona, tiene 6200 empleados, 20 centros de producción y 55 establecimientos comerciales en todo el mundo. Con la reciente adquisición de varias firmas de diseño de estilos de vida, Haworth necesitaba un sistema de control de acceso a la red que solo permitiera acceder a la red corporativa a los dispositivos autorizados que cumplieran las normas de seguridad empresariales.

Para satisfacer esta necesidad y subsanar a la vez otros problemas de seguridad, como la detección y la contención de dispositivos no autorizados, Haworth implantó la plataforma Forescout. Con la visibilidad y el control granulares de la solución de Forescout, el nivel de seguridad de los entornos de IT y de producción mejoró drásticamente. Además, su integración con los firewalls de la empresa permitió automatizar las tareas de seguridad y así liberar considerablemente al equipo de seguridad de la información. La plataforma Forescout también demostró su valía más allá del ámbito de la seguridad y se utiliza en otros departamentos operativos, incluida la administración de redes.

Reto de la empresa

"En estos y otros casos de uso, no solo necesitábamos mayor visibilidad y control, sino también la capacidad de clasificar dispositivos, segmentar las redes por dispositivo y buscar indicadores de riesgo, todo en tiempo real".

— Joseph Cardamone, Analista sénior de seguridad de la información y Responsable de privacidad para Norteamérica, Haworth

Joe Cardamone, Analista sénior de seguridad de la información y Responsable de privacidad para Norteamérica, dirige la estrategia de seguridad de la información en Haworth. Cardamone forma parte de un equipo de tres personas que se esfuerza a diario por proteger tanto el entorno corporativo como el de producción de Haworth en todo el mundo. Este reto se agravó con la reciente adquisición de numerosas empresas de gestión independiente.

Los dispositivos de las nuevas filiales no eran los únicos recursos de los que el equipo requería más visibilidad y control. Por ejemplo, necesitaba un método mejor y más rápido para localizar dispositivos IoT de alto riesgo e impedirles recibir o transmitir comunicaciones no autorizadas. También necesitaba identificar y proteger con facilidad sus propios dispositivos Workware de colaboración digital, que se desplazan constantemente de un lugar a otro y cuyo software y hardware se actualiza con frecuencia.

RESULTADOS

- Rápida creación de valor: 97 % de los endpoints detectados y clasificados en las siete primeras horas
- Visibilidad en tiempo real de todos los dispositivos en el momento en que se conectan a la red
- Protección más fácil de dispositivos de OT y en constante movimiento gracias a la segmentación dinámica de la red
- Control de acceso para las empresas recién adquiridas que se conectan a la red corporativa
- Ahorro de 20 horas a la semana con la automatización de tareas de seguridad
- Ahorro de tiempo adicional al automatizar procesos manuales para buscar y aislar dispositivos de alto riesgo
- Capacidad para maximizar la eficacia del equipo de seguridad de TI de tres personas
- Visibilidad granular que contribuye a la seguridad, los grupos de IT y el equipo de redes
- Detección de un 60 % más de dispositivos de lo previsto

Por qué Forescout

Un "centro neurálgico de información" fácil de desplegar y de utilizar

Cardamone y su equipo realizaron pruebas de concepto de la plataforma Forescout y de una solución de un proveedor que ya tenía presencia importante en la empresa y contaba con el respaldo inicial del equipo de redes de Haworth. Forescout resultó el vencedor indiscutible.

"La plataforma Forescout es un centro neurálgico de información que, a diferencia de nuestra alternativa, es fácil de desplegar y muy fácil de usar", afirma Cardamone. "Desde un panel único, puedo ver todo nuestro entorno con enorme detalle y administrar protección con un solo clic del ratón. La interfaz de usuario es muy intuitiva y la información está tan clara que incluso los miembros nuevos del equipo y otros departamentos ajenos a la seguridad —incluido el de redes— pueden utilizarla y sacarle provecho".

Impacto en el negocio

Rápido despliegue y creación de valor inmediata

La plataforma Forescout tardó menos de un día en desplegarse. "Empezamos la implementación al mediodía y, cuando encendí el ordenador a última hora de la tarde, el 97 % de nuestro entorno ya estaba detectado y clasificado", recuerda. "En siete horas teníamos visibilidad detallada de nuestro entorno en todo el mundo. Es impresionante".

Valor constatado de una visibilidad completa y detallada desde el principio

La visibilidad precisa que nos dio la plataforma Forescout demostró su utilidad inmediatamente tras la implementación. "Creíamos tener unos 7500 dispositivos en nuestras redes, pero la plataforma Forescout detectó más de 12 000 direcciones IP", señala Cardamone. "También descubrimos brechas de seguridad que desconocíamos, como una docena de puntos de acceso inalámbrico instalados en salas de exposición. La nueva visibilidad nos permitió bloquear estos dispositivos y ponernos en contacto con los administradores locales para repararlos".

"Y esto no es más que la punta del iceberg", continúa Cardamone. "La cantidad de información que obtenemos con la plataforma Forescout es increíble. Aunque muchas otras herramientas detectan las direcciones IP de los endpoints, esta solución es con mucho la mejor que he utilizado nunca para buscar, identificar y controlar sistemas de verdad. Para nosotros ha sido tremendamente útil".

"Automatizar una acción para un endpoint es algo frecuente, pero cuando se requiere una intervención manual, basta con pulsar el botón derecho del ratón", prosigue Cardamone. "En una crisis también puedo autorizar a empleados de nivel 1 o 2 a adoptar medidas de nivel 3 sin darles acceso a funciones privilegiadas. La plataforma Forescout ofrece características muy eficaces desde el primer momento, pero también es muy personalizable. Sus posibilidades son ilimitadas".

Visibilidad de la seguridad de los dispositivos de las empresas adquiridas

La plataforma Forescout proporcionó visibilidad de las empresas adquiridas y del estado de seguridad de sus respectivos dispositivos. "Si sus dispositivos llevan mucho tiempo sin instalar parches, lo vemos y podemos solucionarlo", asegura Cardamone. "La plataforma Forescout también comprueba el estado del antivirus, los parches y el sistema operativo de cualquier dispositivo de las filiales que intenta conectarse a la red corporativa, y bloquea los que no cumplen nuestros criterios".

> *"La cantidad de información que obtenemos con la plataforma Forescout es increíble. Aunque muchas otras herramientas detectan las direcciones IP de los endpoints, esta es con mucho la mejor que he utilizado nunca para buscar, identificar y controlar sistemas de verdad. Para nosotros ha sido tremendamente útil".*
>
> **— Joseph Cardamone, Analista sénior de seguridad de la información y Responsable de privacidad para Norteamérica, Haworth**

Segmentación de la red más sencilla pero más personalizable

Utilizando Forescout eyeExtend Module for Palo Alto Networks® Next-Generation Firewall, Cardamone integró rápidamente la plataforma Forescout en los firewalls de la compañía para segmentar la red sobre la marcha en función de la información contextual precisa que proporcionaba en tiempo real la solución de Forescout. "Con la integración entre Forescout y Palo Alto Networks, ya no estamos obligados a segmentar únicamente por identificadores como IP o VLAN", explica Cardamone. "Disponemos de muchas más opciones de las que tendríamos solo con 802.1X, porque podemos basar la segmentación en un perfil de endpoints mucho más profundo y minucioso".

Por ejemplo, en el entorno de fabricación de Haworth, Cardamone utiliza la plataforma Forescout para identificar y clasificar todos los dispositivos IoT de alto riesgo, básicamente los que ha descatalogado el fabricante, como los sistemas operativos Windows® XP o Windows 2000. A continuación, la segmentación dinámica de la red bloquea esos dispositivos para que no reciban ni transmitan información, salvo en circunstancias autorizadas muy específicas.

Enorme ahorro cuantificable con la integración y la automatización

Además, la integración entre Forescout y Palo Alto Networks permitió a Haworth automatizar laboriosos procesos manuales. Tomemos por ejemplo los dispositivos con tecnología Workware de Haworth. Presentes en las oficinas centrales y en las salas de exposición de Haworth del mundo entero e instalados en las VLAN de producción, a estos dispositivos se les solía asignar una dirección IP estática que después podía interaccionar con la red de invitados a través del firewall. Con 130 de estos dispositivos solo en la sede, con los cambios y actualizaciones constantes de hardware y software y con los desplazamientos físicos que modificaban las direcciones IP, era sencillamente imposible que un proceso manual pudiera proporcionar un control adecuado de acceso a la red.

Sin embargo, hoy la plataforma Forescout los detecta, los clasifica y los coloca en un grupo de acceso dinámico sujeto a una directiva de firewall que permite a las direcciones IP de ese grupo interaccionar con la red de invitados en los puertos y las aplicaciones necesarios. "Por lo tanto, aunque el dispositivo se desplace a China o Alemania, Forescout lo encuentra y el firewall sabe qué hacer", afirma. "Lo que antes era una tarea manual constante y casi imposible, ahora es un proceso totalmente automatizado".

"Si sumamos todo el tiempo que hemos ahorrado en los distintos casos de uso desde que instalamos la plataforma Forescout y la integramos con nuestro firewall, calculo unas 20 horas a la semana, o sea, la mitad de la jornada de un empleado a tiempo completo", asegura Cardamone. "Para proteger nuestro entorno, nuestra pequeña plantilla de seguridad puede hacer más, pero con menos trabajo".

Los beneficios de la visibilidad de Forescout trascienden la seguridad

El personal de operaciones de Haworth también se beneficia de la plataforma Forescout. Los técnicos de asistencia la utilizan para localizar dispositivos físicamente. En administración de software se hace uso de ella para buscar aplicaciones no conformes. Hasta el equipo de redes la emplea semanalmente para buscar información sobre puertos y conmutadores. Y siempre estamos proyectando nuevos usos. Por ejemplo, Forescout desempeñará un papel crucial cuando la empresa implemente una directiva de dispositivos BYOD en el futuro.

Más información en
www.forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San José, CA 95134 EE. UU.

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