Guardicore

CASO PRÁCTICO

Openlink Refuerza la Seguridad en la Nube Con Guardicore

El Cliente

Openlink es el líder mundial en soluciones para comercio, tesorería y gestión de riesgos de empresas de energía, productos, corporaciones y servicios financieros. Más de 37.000 usuarios de más de 600 clientes utilizan el software altamente sofisticado de la empresa para actividades como la cobertura de los precios de productos, automatización de la logística, previsión de las necesidades de materias primas y operaciones de derivados.

El Desafío

Asegurar una Infraestructura en la Nube - y la Confianza del Cliente

Al igual que muchos proveedores de software empresarial, Openlink está experimentando una transformación de TI desde la entrega y el soporte local de sus productos hasta una implementación pública en nube. Su plataforma Openlink Cloud, la primera de su tipo en la industria, fue lanzada en mayo de 2017 a través de Microsoft Azure.

"Existían dos motores principales para que nos trasladáramos hacia la nube pública», explica Michael Lamberg, Vicepresidente y Director de Seguridad de la Información de Openlink. "Debido a que nuestro software es intensivo en procesamiento, los clientes típicamente construyen su entorno informático para obtener una capacidad de procesamiento máxima, lo que conlleva un gasto de capital extremadamente alto. Al pasar a la nube pública, podemos escalar automáticamente la aplicación durante los momentos de mayor demanda, de modo que los clientes no están pagando por la capacidad que no están utilizando". En segundo lugar, nuestros clientes suelen mantener varios entornos de pruebas de desarrollo para probar nuevas versiones de nuestro software y complementos (add-ons) de cliente. Al utilizar la nube pública, es mucho más sencillo para nosotros crear un entorno cuando lo necesitan para sus pruebas y eliminarlo cuando terminan, minimizando de esta manera el costo".

Por supuesto, trasladarse hacia la nube trae consigo una gran cantidad de nuevas cuestiones de seguridad. Openlink se responsabiliza de la protección de los datos extremadamente confidenciales y altamente estratégicos de sus clientes, que podrían ser el objetivo de agentes malintencionados. Dado que la ciberseguridad en la nube pública opera bajo un modelo de responsabilidad compartida (donde el proveedor de la nube ofrece un espectro finito de medidas de seguridad sujetas a una auditoría y certificación rigurosa), el cliente de la nube (Openlink en este caso) es el responsable, en última instancia, de proteger sus propios datos y procesos.

openlink

"Las herramientas con las que solíamos contar para analizar cómo funciona una infraestructura han cambiado [con el advenimiento de la nube pública]."

- Michael Lamberg, Vicepresidente y Director de Seguridad de la Información, Openlink

"Los principales proveedores de servicio en la nube han recorrido un largo camino en los últimos 5 años en términos de su capacidad para asegurar grandes infraestructuras", dice Lamberg. "En realidad, están haciendo un trabajo mucho mejor que el de muchas organizaciones que gestionan sus propios centros de datos. Pero todo el mundo opera sobre la base de un modelo de confianza compartida. Azure puede tener el nivel más alto de certificaciones de seguridad a nivel mundial en este momento, pero no nos van a proteger de nuestras propias implementaciones".

Openlink reconoció la necesidad de mejorar la infraestructura de seguridad de Azure con soluciones de terceros para proporcionar el nivel personalizado de mitigación de riesgos que Openlink y sus clientes requieren. Tenemos que ser capaces de demostrar a nuestros clientes que, no sólo Azure está haciendo lo que dicen que están haciendo, sino que también estamos añadiendo una capa de seguridad sobre ellos, reforzando aún más los controles globales de defensa exhaustiva de los datos y entornos alojados en la nube de nuestros clientes".

La Solución

Plataforma de seguridad Guardicore Centra™

Un año antes del lanzamiento de Openlink Cloud, Lamberg fue presentado a Guardicore y vio inmediatamente cómo podía ayudar a aumentar la infraestructura de seguridad en nube de la empresa. La plataforma de seguridad Guardicore Centra™ está diseñada para cubrir puntos ciegos crítico en múltiples infraestructuras, más precisamente, los movimientos laterales de los intrusos que han logrado pasar los firewalls y los sistemas de prevención de intrusiones. Centrada en la detección de anomalías sospechosas en el tráfico este-oeste, la solución de Guardicore confirma y contiene brechas activas antes de que puedan causar daños significativos.

"Un duro despertar que se mueve hacia la nube pública es que todo lo que sabías sobre redes e infraestructura también puede ser desechado", explica Lamberg. "Ya no se aplica desde dos perspectivas: una es que ya no tienes control ni acceso a las capas inferiores de la pila de infraestructura que ha sido virtualizada por Azure. Y la segunda es que las herramientas en las que solíamos confiar para analizar cómo funciona una infraestructura han cambiado. Así que eso es algo que tienes que entender. Todas sus habilidades y experiencia en redes tradicionales no son tan útiles como solían serlo. Ahora todo es nuevo".

En consecuencia, Guardicore se ha convertido en una de las tecnologías de seguridad clave de Openlink, señala Lamberg. "Proporciona la seguridad de que estamos cerrando el entorno adecuadamente mientras validamos que Azure está haciendo su trabajo de una manera muy eficiente y efectiva"."

Los Beneficios

Visibilidad y diagnóstico mejorados

Con el cambio a una infraestructura virtualizada y basada en la nube, el equipo de seguridad de Openlink se vio desafiado por la necesidad de obtener una visibilidad altamente granular de la actividad de las aplicaciones. Una característica clave de la plataforma de seguridad Guardicore Centra es la capacidad de visualizar todas las cargas de trabajo, flujos y procesos dentro de un entorno informático.

"Aunque estamos en la nube pública, no somos multi-tenant", explica Lamberg. "Construimos un ambiente de un solo inquilino para cada uno de nuestros clientes. Como resultado, necesito tener un entendimiento completo de lo que está sucediendo horizontalmente dentro de la infraestructura de cada cliente. Lamberg cita dos escenarios de uso clave que aprovechan Guardicore. El primero es DevTest, que proporciona a los clientes un entorno de pruebas que les permite girar rápida y fácilmente máquinas virtuales para probar la aplicación de Openlink en varias configuraciones antes de pasar a la producción. En caso de alguna anomalía, Guardicore permite al equipo de Lamberg analizar rápida y claramente la situación desde una perspectiva de host, proporcionando visibilidad de todos los procesos de flujo. "Es posible que no sea necesariamente una cuestión de seguridad", dice Lamberg. "Puede tratarse de un fallo de diseño o configuración o quizás el cliente cargó accidentalmente algún malware y de repente veo una conexión de comando y control que intentaba apagarse. Guardicore me da la capacidad de aislar inmediatamente esta anomalía y visualizarla con una claridad sin precedentes".

El segundo escenario de uso que involucra a Guardicore es la gestión de Openlink del entorno de producción soportado por los clientes. "Aunque nuestra aplicación es compleja, es extremadamente determinista", afirma Lamberg. "Por lo tanto, conozco todos los flujos y procesos que se supone que se ejecutan en cada uno de nuestros servidores que dan soporte al cliente. Esto permite generar una línea de referencia de su entorno. En caso de que Guardicore note un proceso o flujo fuera de la línea de referencia, se me avisa inmediatamente".

Esta capacidad de "clasificación y diagnóstico" veloz de problemas es un beneficio central de Guardicore, señala Lamberg. La aparición de un proceso o flujo desconocido - que sería extremadamente difícil, si no imposible, de aislar sin una herramienta como Guardicore - podría simplemente indicar un problema con el software o algo mucho peor. "Es muy poco probable que alguien pueda entrar en nuestro entorno, pero necesito garantías de que disponemos de un mecanismo proactivo para hacer frente a este tipo de situaciones. Guardicore me lo proporciona".

Guardicore también llamó la atención de Lamberg con sus capacidades de microsegmentación, que permiten a los operadores de seguridad establecer políticas de seguridad alrededor de aplicaciones y procesos individuales o en grupos. "Los ataques típicamente ocurren de manera lateral en estos días", señala. "Se afianzan en una máquina y saltan lateralmente a otras. Tener los controles apropiados en todas tus máquinas, y ser capaz de monitorear la interacción de esas máquinas, es la única manera en la que te vas a adelantar a ese problema". Si Openlink decidiera implementar la microsegmentación en el futuro, Lamberg cree que las capacidades de Guardicore podrían poner a la empresa en una mejor posición para hacerlo con éxito

"Guardicore me da la habilidad de aislar inmediatamente el flujo del proceso o anomalías basadas en una conexión y visualizarlas con una claridad sin precedentes."

- Michael Lamberg,
Vicepresidente y Director de Seguridad de la Información, Openlink

"Guardicore ha sido un socio estupendo."

- Michael Lamberg, Vicepresidente y Director de Seguridad de la Información, Openlink

Socios en la Protección

Mientras que actualmente Openlink se está beneficiando de la tecnología de Guardicore, Lamberg también puede ver el valor de la relación de trabajo continua con las personas que están detrás de la solución. "Sólo hago negocios con empresas que están dispuestas a asociarse", afirma. "No sólo adquiero productos de consumo. Y Guardicore ha sido un gran socio. Ellos escuchan nuestros comentarios y lo que necesitamos, y continuamente han refinado la solución basada en eso".

Debido a que las nubes públicas son dinámicas por naturaleza, Openlink cuenta con Guardicore para ayudar a asegurar que la empresa esté optimizando sus entornos a medida que evoluciona la infraestructura de la nube. "Ellos entienden que para resolver problemas, van a tener que trabajar muy de cerca con el proveedor de la nube también. La comunicación constante de Guardicore con Azure asegura que se mantengan al tanto de cualquier cambio que pueda afectar el funcionamiento de su producto".

Como resultado, Guardicore - la empresa y la solución - se han convertido en parte integral de la misión de Openlink de salvaguardar los activos críticos de sus clientes en la nube pública. Nunca quiero meterme en una situación en la que llame a un proveedor para hablar de un problema y me digan: 'Bueno, es un problema de Microsoft, contacta a Azure'". "Nunca he oído eso de Guardicore. Reconocen que los esfuerzos de responsabilidad compartida son necesarios para salvaguardar los activos más importantes de nuestros clientes".

Acerca de Guardicore

Guardicore es innovador en la seguridad de centros de datos y nubes que protege los activos centrales de su organización utilizando controles de microsegmentación flexibles, de implementación rápida y fáciles de entender. Nuestras soluciones ofrecen una forma más sencilla y rápida de garantizar una seguridad persistente y consistente, para cualquier aplicación y en cualquier entorno de TI.

www.Guardicore.com

Guardicore