HISTORIA DE CLIENTE DE AKAMAI

Una empresa de fabricación que cotiza en bolsa estandariza los controles de seguridad y ahorra tiempo gracias a Akamai Guardicore Segmentation

La empresa de fabricación necesitaba una solución global segura

- Visibilidad completa de la red
- Segmentación en todas las infraestructuras de TI
- Respuesta a las amenazas de ransomware

El cliente

Esta empresa de fabricación líder cotiza en la bolsa de Nueva York y ofrece servicios a mercados de todo el mundo.

El desafío

Protección de una empresa global

El equipo de seguridad de TI se encarga de una serie de centros repartidos por todo el mundo. La mayoría de estos centros son instalaciones mixtas que albergan oficinas y plantas de fabricación. Para garantizar una estrategia de defensa sólida, el equipo necesitaba estandarizar los controles de seguridad en toda la organización y proporcionar una protección uniforme en todas las zonas geográficas.

"Queríamos pasar de una red abierta y plana a una arquitectura segmentada de buenas prácticas", explica el arquitecto de infraestructura que dirige el proyecto de segmentación.

Como muchas otras organizaciones, esta empresa de fabricación inicialmente recurrió al uso de firewalls para el proyecto.

Sin embargo, gestionar un gran número de reglas basadas en la infraestructura y actualizaciones y cambios a nivel de estación de trabajo en toda la red pronto se convirtió en una tarea laboriosa, incluso para una única ubicación. Además, aunque la visibilidad mejoró, seguía estando restringida a ciertas zonas, lo que no permitía obtener una panorámica completa y centralizada de la actividad de red y las dependencias entre los activos.

Detención del movimiento lateral no autorizado

Aunque los firewalls ofrecían algunos controles de segmentación rudimentarios, no abordaban una cuestión fundamental para el equipo de seguridad: las comunicaciones punto a punto no gestionadas. Por ello, era indispensable ampliar la protección y la visibilidad a esa área específica. De no haber buscado una solución, la organización habría sido vulnerable a ataques "pass-the-hash", ransomware y otras amenazas que utilizan el movimiento lateral entre terminales para propagarse.

Manufacturing Company

Ubicación
Estados Unidos

Sector
Fabricación

Solución
Akamai Guardicore Segmentation

Resultados clave

- Mitigación de la propagación del malware mediante el movimiento lateral
- Visibilidad detallada
- Protección de los terminales mediante segmentación
- Respuesta ante incidentes más sencilla

Akamai

Selección de una solución

Después de implementar varias soluciones de control de firewalls poco manejables, el equipo descubrió Akamai Guardicore Segmentation y comenzó a analizar internamente las ventajas y las posibilidades de la segmentación de última generación.

La empresa solicita una investigación exhaustiva de todas las nuevas soluciones que se vayan a implementar, por lo que el equipo también valoró otras alternativas. Tras un riguroso proceso de evaluación, el equipo finalmente se decantó por Akamai Guardicore Segmentation. "Ninguna de las opciones que consideramos ofrecía una solución tan completa como la de [Akamai], que nos proporcionaba supervisión del tráfico, etiquetado flexible y amplia visibilidad a nivel de aplicación a través de un único agente en un cliente", explica el arquitecto de infraestructura.

> Con un único agente en una máquina, hemos resuelto el problema de los ataques de movimiento lateral en terminales para siempre.
>
> Arquitecto de infraestructura de la empresa de fabricación

Akamai Guardicore Segmentation

Para la primera fase del proyecto, la empresa implementó Akamai Guardicore Segmentation en alrededor de 2000 estaciones de trabajo. Inmediatamente después de poner en funcionamiento la solución, el equipo de seguridad de TI descubrió un nuevo nivel de visibilidad de la red y sus flujos de comunicación.

Nuevas perspectivas y segmentación en acción

"Gracias a los mapas del tráfico de [Akamai], nuestra visibilidad ha mejorado en un 1000 % e incluye las comunicaciones entre ordenadores", observa el arquitecto de infraestructura.

La capacidad de analizar la actividad de un ordenador individual y, al mismo tiempo, comprender la actividad general a nivel de aplicación ha ayudado a la organización a tomar mejores decisiones de seguridad. Por ejemplo, algunos usuarios han instalado aplicaciones para sus impresoras domésticas en los ordenadores portátiles de la empresa. Se descubrió que muchas de estas aplicaciones analizaban la red corporativa de forma continua en busca de dispositivos compatibles. Gracias a la nueva información que aportaba la visibilidad de Akamai, el equipo pudo detener estos análisis.

Akamai Hunt: cómo utilizar Akamai Guardicore Segmentation para detectar amenazas

Esta nueva percepción de la actividad de la red también ha ayudado a la empresa a detener a los agentes maliciosos externos. Por ejemplo, poco después de implementar la plataforma, el servicio Akamai Hunt detectó que un activo se estaba comunicando con un archivo que presentaba características de un conocido malware llamado GoldenSpy. El equipo de Hunt informó al equipo de seguridad de TI de la empresa de la amenaza detectada. El cliente también recibió un análisis del alcance de la infección, los riesgos potenciales (hallazgos que coincidían con la información de MITRE sobre GoldenSpy), un análisis forense (mediante el uso de Insight) y recomendaciones para la investigación y mitigación internas. A continuación, la empresa utilizó los controles de políticas de Akamai para poner en cuarentena el sistema infectado y, de este modo, evitar que el malware se moviera lateralmente a otras máquinas.

Estandarización y ahorro de tiempo

Esta empresa ahora también puede crear y gestionar las políticas de forma centralizada, lo que incluye una política central y global para las estaciones de trabajo y la flexibilidad para crear excepciones puntuales cuando un caso de uso lo requiera. Esto garantiza un cumplimiento uniforme en cualquier ubicación en la que haya un agente de Akamai y reduce el riesgo de demoras y errores de configuración.

Asimismo, el tiempo que transcurre hasta que se aplica una política en la organización también ha mejorado notablemente. Por ejemplo, antes de utilizar la nueva plataforma, introducir un cambio en los controles del firewall era un proceso que podía llevar varios días. Con las nuevas plantillas de políticas de Akamai como guía inicial, el equipo de seguridad de TI puede crear controles de seguridad incluso para los casos de uso más complejos en menos de una hora y aplicarlos a toda la base instalada en cuestión de segundos.

El futuro con Akamai

Aunque el enfoque inicial del proyecto se centraba en estandarizar los controles de seguridad para la segmentación y el acceso de los terminales, existen planes para abordar casos de uso adicionales con Akamai. Las partes interesadas están analizando una ampliación de la protección para incluir los servidores y las aplicaciones críticas, como el sistema ERP de la organización.

Independientemente de lo que puedan incluir los planes de futuro, el fabricante ya considera que el proyecto original ha sido un éxito, ya que ha conseguido reducir drásticamente la superficie de ataque y los riesgos a los que se enfrentaban las estaciones de trabajo de la empresa. Ahora, el equipo confía mucho más en la estrategia de seguridad de la organización para hacer frente a los ataques de movimiento lateral entre diferentes terminales. Tal y como explica el jefe del proyecto: "Ahora, con un solo agente en una máquina, resolvemos el problema de raíz y podemos implementar toda una serie de controles de seguridad en una estación de trabajo sin políticas en tan solo 30 segundos".

> “Gracias a los mapas del tráfico de [Akamai], nuestra visibilidad ha mejorado en un 1000 % e incluye las comunicaciones entre ordenadores.
>
> Arquitecto de infraestructura de la empresa de fabricación

Visite akamai.com/guardicore para obtener más información.

 | Asistencia | | Publicado en 06/23