INFORME SOBRE LA SOLUCIÓN DE AKAMAI

Deloitte refuerza la respuesta a incidentes y la mitigación del ransomware con ayuda de Akamai Guardicore Segmentation

Desafíos del cliente

Las distintas categorías de los productos de seguridad están muy bien definidas y prometen niveles cada vez mayores de protección contra las amenazas más recientes a las redes empresariales. Sin embargo, pocas opciones han sido capaces de ofrecer un método integral, basado en una única solución, para reducir la superficie de ataque mediante la protección contra el movimiento lateral malicioso, ya sea hacia o desde el hardware local, las cargas de trabajo alojadas en la nube, los dispositivos de usuario final o los contenedores. Tradicionalmente, las iniciativas preliminares de segmentación Zero Trust tardaban meses en completarse, e incluso años. Esto se debe a las limitaciones tecnológicas y de experiencia humana a la hora de ejecutar proyectos que permitan detener los ataques si se eluden productos de seguridad concretos como firewalls heredados o herramientas de detección y respuesta de terminales (EDR), entre otros.

Al abordar los proyectos de segmentación, los clientes de grandes empresas suelen enfrentarse a los siguientes desafíos:

- Falta de visibilidad de todos los activos, flujos de red, usuarios y conexiones en los distintos entornos
- Controles de seguridad limitados sobre tecnologías e infraestructuras dispares, como la infraestructura de nube híbrida, los sistemas operativos heredados y los sistemas OT/IoT
- Necesidad de garantizar la continuidad del negocio evitando el tiempo de inactividad, que a menudo viene de la mano de las técnicas de segmentación tradicionales
- Escasez de recursos de seguridad y talento para crear, implementar y gestionar iniciativas que respalden los modelos Zero Trust

Aspectos destacados de la solución

Akamai Guardicore Segmentation es una solución de microsegmentación basada en host que proporciona la forma más sencilla, rápida e intuitiva de aplicar los principios Zero Trust en la red. Utilizando una combinación de sensores basados en agentes, recopiladores de datos basados en la red y registros del flujo de la nube privada virtual para mapear su red, Akamai Guardicore Segmentation le ofrece una única imagen de todos sus activos y su infraestructura, incluidos los sistemas operativos heredados y modernos, la tecnología operativa y los dispositivos de IoT. A partir de ahí, puede crear y aplicar fácilmente políticas que limitarán las comunicaciones no deseadas, reducirán su superficie de ataque y garantizarán la continuidad del negocio.

Principales casos de uso

- **Controles de tráfico de este a oeste**
  Separe entornos, aplicaciones, usuarios e infraestructuras que no necesiten comunicarse.
- **Mitigación de ransomware**
  Implemente plantillas de políticas con inteligencia artificial (IA) y aprendizaje automático (ML) para bloquear las rutas utilizadas en diferentes ataques de ransomware.
- **Acordonamiento de aplicaciones**
  Céntrese en las dependencias específicas de sus aplicaciones esenciales para crear controles de seguridad estrictos.

- **Segmentación basada en el usuario**
  Impida que los usuarios accedan a aplicaciones, entornos y dispositivos que no sean esenciales para su trabajo.
- **Aislamiento de dispositivos infectados**
  Contenga la propagación de una filtración si uno o varios dispositivos se ven comprometidos.
- **Conformidad normativa**
  Téngalo todo en orden para demostrar la conformidad rápidamente al poder entender bien todo el contexto de su red, dispositivos y posibles rutas de ataque.

Ventajas para el cliente

- Resuelva los problemas de visibilidad con un completo panel unificado que muestra la totalidad de sus redes y conexiones, incluidos servidores, terminales, nubes, contenedores, usuarios y mucho más.
- Aplique políticas Zero Trust para mitigar la posibilidad de que se produzca un ataque de ransomware con éxito.
- Reduzca el tiempo de respuesta a los incidentes mediante la inteligencia ante amenazas y las completas funciones de detección de infracciones y engaño como mecanismo de defensa.
- Simplifique los proyectos forenses y de cumplimiento de normativas de la red mediante funciones tanto históricas como en tiempo real.

Experiencia de Deloitte

1. **Asesoramiento**
   Gracias a la experiencia de Deloitte en la ayuda a la toma de decisiones clave en materia de ciberseguridad, análisis de brechas y creación de planes de implementación, los clientes empresariales pueden aplicar las mejores resoluciones posibles durante las filtraciones, así como en la planificación futura.
2. **Servicios profesionales**
   Disfrute de servicios de implementación totalmente gestionados, así como de integraciones personalizadas en sus soluciones actuales de seguridad, gestión de servicios de TI (ITSM) y nube.
3. **Servicios gestionados de respuesta a incidentes**
   Reciba asistencia inmediata de los expertos en respuesta a incidentes de Deloitte para contener la vulneración y ayudar a prevenir futuros incidentes.
4. **Suscripciones de licencias**
   Deloitte ofrece una amplia gama de suscripciones de licencias.

Caso práctico de cliente: Cómo Akamai y Deloitte resuelven los desafíos que plantea el ransomware a los clientes

Los grandes ataques de ransomware han llevado a los clientes a buscar asesoramiento y soluciones capaces de ayudar de inmediato en un momento crítico. Las capacidades combinadas de los equipos de respuesta a incidentes y seguridad de Deloitte, que aprovechan la visibilidad de red, los análisis forenses de infracciones y las medidas posteriores para reducir la superficie de ataque que ofrece Akamai Guardicore Segmentation, han demostrado ser una combinación ganadora para los clientes.

Antecedentes

Una gran organización sufrió un importante ataque de ransomware que anuló sus operaciones empresariales principales. El cliente no sabía cómo afrontar la situación. Había perdido por completo el control de su centro de datos, compuesto por miles de servidores, y la filtración debía contenerse inmediatamente y de forma segura.
El cliente, que confiaba en los consejos de Deloitte, se puso en contacto para saber cómo proceder. Con el equipo de Deloitte ya preparado para ofrecer e implementar Akamai Guardicore Segmentation, el cliente pudo obtener rápidamente visibilidad de la escala del ataque, comprender qué activos y aplicaciones se habían visto afectados y ver cuáles eran todas las dependencias entre aplicaciones.

Solución

Al trazar un mapa del entorno completo y detallado del cliente, que comprendía incluso los procesos individuales, Akamai Guardicore Segmentation reveló todas las posibles rutas que el malware pudo haber seguido desde la infraestructura comprometida. Así, el equipo de Deloitte pudo centrarse en partes concretas de la red y realizar en ellas análisis forenses adicionales. De este modo, una vez que se restauraron las operaciones empresariales y el acceso al centro de datos, se garantizó que no quedara ningún dispositivo en peligro.

Resultado

Con el ataque de ransomware resuelto, el centro de datos volvió a ponerse online y se reanudaron las operaciones empresariales. A continuación, se tomaron medidas para reducir la posibilidad de que se produjera de nuevo un ataque de este tipo. Al igual que muchos clientes empresariales, esta organización utiliza un enfoque de seguridad por capas con varias soluciones líderes para proteger dispositivos, aplicaciones, usuarios y mucho más. Sin embargo, dado que algo tan simple como un correo electrónico de phishing puede ser la puerta de entrada para un atacante, estas soluciones no fueron suficientes para detener el ataque. Con el contexto completo de la red, las dependencias de las aplicaciones y los usuarios que tienen acceso al centro de datos, el cliente pudo implementar controles de microsegmentación precisos para reducir en gran medida las rutas que podrían seguirse en una futura filtración de ransomware.

Una vez probado el valor de la solución y reforzada la confianza en la experiencia de Deloitte, el cliente decidió mantener la solución en marcha para seguir contando con la segmentación Zero Trust, y solicitó a Deloitte que gestionara la tecnología en el día a día.

En resumen

En resumen, los amplios conocimientos técnicos y la experiencia de Deloitte en la ejecución de proyectos Zero Trust para clientes los convierten en el partner ideal para implementar y gestionar Akamai Guardicore Segmentation para los clientes. Las empresas pueden confiar en Deloitte para utilizar esta tecnología en cualquier iniciativa de seguridad que incluya la reducción de la superficie de ataque, los controles de movimiento lateral, la delimitación de aplicaciones o la mitigación de ransomware.

Acerca de Deloitte

Deloitte presta servicios de auditoría, consultoría, asesoramiento fiscal y legal a muchas de las marcas más respetadas del mundo, incluido el 90 % de las organizaciones de la lista Fortune 500® y más de 7000 empresas privadas. Nuestro personal trabaja al unísono para optimizar todos los sectores industriales que impulsan y dan forma al mercado actual. Así se logran resultados cuantificables y duraderos que ayudan a reforzar la confianza pública en nuestros mercados de capitales, inspiran a los clientes a ver los retos como oportunidades para transformarse y prosperar, y lideran el camino hacia una economía más fuerte y una sociedad más sana. Deloitte se enorgullece de formar parte de la mayor red global de servicios profesionales para clientes con necesidades específicas en mercados clave. Nuestra red de firmas, con una trayectoria de más de 175 años de servicio, abarca más de 150 países y territorios. Descubra cómo se conectan las aproximadamente 415 000 personas que trabajan en Deloitte en todo el mundo para lograr un gran impacto positivo, en deloitte.com.

Contacto

Ola Sergatchov
Director de Alianzas Estratégicas Globales, Akamai
osergatc@akamai.com

©2024 Akamai Technologies | Asistencia | Publicado en marzo de 2024.