Akamai

Desmontamos los 7 mitos sobre la microsegmentación

Puede parecer contradictorio pensar en objetivos sencillos a la hora de escalar a lo grande, pero existen muchas ideas erróneas sobre las soluciones de microsegmentación modernas.

¿Cree que sufrirá tiempos de inactividad de la red o dificultades para poner en marcha una implementación definida por software? Piénselo otra vez. Esto es lo importante a la hora de ir al detalle.

Mito n.º 1

Mi solución de EDR es suficiente para detener los ataques de ransomware

Tanto la detección y respuesta de terminales (EDR) como la segmentación abordan los ataques de ransomware, pero en diferentes fases de la intrusión y de diferentes formas. Las soluciones de EDR buscan detectar la presencia de ransomware en ejecución en los dispositivos o terminales que supervisan. Si la EDR detecta ransomware, puede frenar el proceso, poner en cuarentena el dispositivo y, a veces, revertir cualquier cifrado que se haya producido. La EDR y la segmentación son complementarias: en caso de que la EDR no detecte ransomware, las soluciones de segmentación compartimentan la red en depósitos aislados para limitar el movimiento lateral (este-oeste) de un ataque. En el caso del ransomware, los atacantes deben moverse lateralmente para tener éxito. La segmentación garantizará que los ataques que hayan logrado avanzar más allá del terminal encuentren finalmente un obstáculo, lo que limitará la zona afectada por la infección inicial. Obtenga más información sobre las diferencias entre la EDR y la segmentación.

1 hora y 42 minutos

es el tiempo medio que tarda un atacante en empezar a moverse lateralmente dentro de la red tras ganar el acceso inicial

(Informe de protección digital de Microsoft de 2022)

Mito n.º 2

Ya utilizo la segmentación

La segmentación no es un concepto nuevo, simplemente se ha vuelto más sofisticada. Durante décadas, las organizaciones han utilizado un mosaico de redes VLAN, firewalls internos, ACL y grupos de seguridad para segmentar sus entornos. Pero estos métodos heredados no han evolucionado para adaptarse a las exigencias más complejas de las infraestructuras híbrida y multinube modernas, lo que ha generado brechas de seguridad y puntos ciegos debido a la infrasegmentación.

Por ejemplo: los firewalls heredados no asignan ni evalúan las dependencias del flujo de trabajo, lo que dificulta la identificación de segmentaciones para aplicaciones, cargas de trabajo o usuarios. Por lo tanto, las empresas se ven obligadas a implementar políticas de segmentación amplias que son demasiado permisivas y pueden dar lugar de forma fácil *y rápida* a peligrosas configuraciones erróneas que son difíciles y engorrosas de solucionar.

Con la microsegmentación, las organizaciones pueden segmentar y aplicar hasta la capa 7, mucho más de lo que es posible con las herramientas de segmentación tradicionales.

2 mill. USD

de ahorro en costes de actualización de firewalls en un plazo de tres años

(TEI de Forrester)

Mito n.º 3

La microsegmentación es demasiado difícil de poner en práctica

La microsegmentación moderna está lista para saltar al terreno de juego empresarial, ahora más que nunca.

Con Guardicore Segmentation de Akamai, se consigue la máxima eficiencia operativa mediante el uso de una única solución basada en software para la segmentación, la visibilidad, la creación de políticas y la aplicación de reglas en todos los entornos, desde el centro de datos y la nube hasta los activos basados en contenedores. Tras la implementación, Guardicore Segmentation de Akamai crea un mapa visual dinámico de toda la infraestructura de TI que permite a los equipos de seguridad ver la actividad hasta el nivel del proceso individual, tanto en tiempo real como en el historial.

Esta información detallada sobre el comportamiento de las aplicaciones se puede utilizar para crear rápidamente políticas de microsegmentación detalladas a través de una interfaz visual intuitiva. Las reglas de denegación globales, la delimitación de aplicaciones críticas y la capacidad de segmentar inmediatamente grandes entornos se traducen en un plazo de amortización rápido y una reducción del riesgo.

Con los métodos de segmentación heredados, carece de la visibilidad necesaria incluso para saber por dónde empezar.

↑95 %

de aumento en la productividad de SecOps

(TEI de Forrester)

Mito n.º 4

La microsegmentación implica tiempo de inactividad de las aplicaciones y la red

Con los enfoques tradicionales de segmentación, las aplicaciones se mueven a menudo entre subredes o VLAN, lo que genera tiempo de inactividad e interrumpe la continuidad empresarial. Los ingenieros de red y los administradores de firewall tienen que planificar el tiempo de inactividad programado, el control de cambios o los intervalos de mantenimiento, lo que aumenta el tiempo necesario para implementar nuevos servicios o actualizaciones de aplicaciones. Y lo que es peor, estos retrasos pueden dar lugar a un mayor riesgo debido a la exposición y la vulnerabilidad de los activos.

Por otro lado, la segmentación definida por software desvincula la seguridad de la infraestructura subyacente y los sistemas operativos, de modo que la segmentación se puede realizar de forma independiente, sin intervención de la red ni la aplicación. Si se produce un evento, en lugar de aislar completamente los equipos afectados, solo se bloquea el vector de ataque, lo que limita el impacto negativo en la empresa.

La microsegmentación también se puede implementar en modo de alerta para permitir la prueba de políticas en entornos de producción reales, sin riesgo de causar tiempos de inactividad. Conclusión: las soluciones de segmentación modernas no deberían obligar a elegir entre seguridad y agilidad empresarial.

Mito n.º 5

La microsegmentación no cubre mi entorno de IoT y OT

¿Sabía que se pueden aplicar políticas Zero Trust a los dispositivos IoT y OT que no pueden ejecutar software de seguridad basado en host?

Nuestras capacidades de segmentación sin agentes subsanan las brechas de seguridad entre los dispositivos que no pueden ejecutar agentes para eliminar los puntos ciegos de visibilidad, como los terminales aislados. Esta cobertura ampliada es especialmente importante para entornos de atención sanitaria, retail y fabricación que tienen muchos dispositivos IoT conectados a la red (y vulnerables), así como sistemas de OT heredados. La integración de una segmentación sin agentes en su infraestructura de red posibilita la detección automática de nuevos dispositivos, el uso de la huella dactilar y la aplicación de políticas para mitigar el riesgo y acelerar la transición a Zero Trust en toda la empresa.

Mito n.º 6

Un agente de microsegmentación añade demasiada latencia

Una de las principales falsas creencias sobre la microsegmentación es la latencia añadida.

En realidad, el uso de políticas distribuidas de segmentación basada en software, en lugar de puntos de estrangulamiento específicos por los que debe pasar todo el tráfico, evita la aparición de cuellos de botella en la red. El agente Guardicore de Akamai se ha diseñado para que funcione de forma óptima con Linux, Unix, Windows OS y macOS, y no consume demasiados recursos.

Y como el agente no está en la línea, no realiza una inspección profunda de paquetes que pueda aumentar la latencia.

En su lugar, el agente Guardicore de Akamai toma una información mínima del encabezado del paquete a partir de la cual obtener una imagen completa del entorno del cliente. Si lo que busca es velocidad *y* rendimiento, *puede* tener ambos.

Mito n.º 7

La microsegmentación implica contratar empleados a tiempo completo imposibles de encontrar

Los CISO sienten la presión de "hacer más con menos", por lo que las soluciones de seguridad deben aliviar la carga de los defensores en lugar de consumir más recursos internos, ya escasos.

Los métodos de segmentación tradicionales, como la gestión de firewalls y VLAN, conllevan procesos complejos en varios pasos en los que participan muchos equipos, responsables por separado de la conmutación, el enrutamiento, la implementación de firewalls y la creación de políticas de seguridad. La implementación de un cortafuegos heredado puede tardar de 14 a 22 semanas de media. Todo esto se suma a los plazos del proyecto, lo que supone para la organización importantes costes de mano de obra y gastos generales operativos.

Por el contrario, la solución definida por software de Akamai tarda en implementarse una media de dos semanas y requiere la intervención de un solo empleado a tiempo completo. Además, al añadir Akamai Hunt, nuestro servicio gestionado de búsqueda de amenazas, le ahorraremos tiempo y recursos, pues analiza su entorno en busca de posibles ataques emergentes, movimientos laterales y comportamientos de ataque anómalos.

Hoy en día, los expertos en ciberseguridad son difíciles de contratar y aún más difíciles de retener. Es hora de que las defensas funcionen a favor, *y no en contra*, de su organización.

Estadísticas clave

106 %

Retorno de la inversión demostrado de hasta ~106 % en 12 meses

(TEI de Forrester)

Cómo puede ayudar Akamai

Guardicore Segmentation de Akamai es una solución de microsegmentación basada en software que proporciona la forma más sencilla, rápida e intuitiva de aplicar los principios Zero Trust. Le permite evitar el movimiento lateral malicioso en la red mediante políticas de segmentación precisas, imágenes de la actividad dentro de su entorno de TI y alertas de seguridad de la red. Guardicore Segmentation de Akamai funciona en sus centros de datos, entornos multinube y terminales. Se implementa de forma más rápida que los enfoques de segmentación de la infraestructura y le proporciona una visibilidad y un control de su red sin precedentes.

Descubra cómo Guardicore Segmentation de Akamai posibilita una protección detallada, una mayor visibilidad y una aplicación coherente de las políticas de seguridad según las necesidades para mantener protegidos sus datos más confidenciales.