Akamai

WHITE PAPER

Segmentación de la red y microsegmentación en entornos empresariales modernos

Descripción general

La idea de la segmentación en el ámbito de la seguridad no es novedosa. Los firewalls perimetrales, junto con las VLAN y las ACL, son lo que la mayoría de las empresas han utilizado tradicionalmente para segmentar y proteger su infraestructura de TI. Sin embargo, los tiempos cambian. El aumento de la contenedorización, las redes definidas por software, el uso de infraestructuras públicas y multinube, y la expansión de los dispositivos conectados a Internet han creado un nuevo conjunto de problemas de seguridad que abordar, uno que necesita una solución diseñada para un entorno de TI heterogéneo con diversos requisitos de seguridad. Además, los ataques de ransomware y los hackers de estado son ahora un riesgo para cualquier empresa, y los agentes malintencionados son cada vez más sofisticados en un momento en el que obtener visibilidad en su entorno de TI es una labor cada vez más complicada. Las medidas tradicionales de seguridad perimetral, así como los firewalls de nueva generación basados en la inspección profunda de paquetes o la detección basada en firmas, tienen dificultades para lidiar con la cantidad de tráfico que experimenta un centro de datos empresarial en la actualidad. Veamos cómo las técnicas de microsegmentación adecuadas son la mejor tecnología para abordar las deficiencias de otros enfoques alternativos de segmentación de redes.

> Conforme los entornos de nube híbrida se han convertido en la norma, exigen un conjunto específico de requisitos que van más allá de la seguridad perimetral tradicional

Los firewalls heredados no son adecuados para el tráfico este-oeste

Cuando se trata de segmentar los entornos de TI, una empresa puede recurrir primero a los dispositivos de seguridad perimetral heredados. Desafortunadamente, estos dispositivos se crearon para supervisar el tráfico que se mueve de norte a sur, de cliente a servidor. Esto incluye todo tipo de tráfico que llegue al centro de datos desde cualquier fuente externa. Más recientemente, la cantidad de tráfico dentro del centro de datos que se mueve de un servidor a otro, lo que normalmente se conoce como tráfico este-oeste, ha aumentado exponencialmente. Esto se debe en gran medida al crecimiento de la virtualización y la infraestructura convergente, como la informática basada en contenedores, VPC e hipervisor.

Las medidas de seguridad perimetral, como los firewalls tradicionales, no protegen su empresa de los dispositivos infectados ni evitan que los atacantes amplíen su posición mediante el tráfico este-oeste. Dado el aumento del cifrado TLS y la fácil ocultación de tráfico malicioso en puertos abiertos de aplicaciones legítimas, muchos ataques pueden pasar incluso a través de los firewalls. Esto le impide detectar las vulneraciones existentes y resolverlas o desviarlas. También implica que no se puede limitar fácilmente el tiempo de permanencia de los atacantes en la red. Cuanto mayor sea el tiempo de permanencia, más catastrófica será la filtración. El Manual de estrategias del adversario activo 2022 de Sophos desveló que, aunque el tiempo medio de permanencia era de 15 días, las pequeñas empresas y sectores específicos experimentaron tiempos medios de permanencia mucho más largos, de hasta 34 días.[1] Cuanto más tiempo pase desapercibido en su red un atacante, más daño podrá causar.

Sencillamente, no es posible utilizar suficientes firewalls virtualizados para proteger miles de aplicaciones o cargas de trabajo. Incluso si se pudiera crear una solución virtualizada, sería imposible gestionarla o controlarla teniendo en cuenta los entornos dinámicos en constante cambio en los que ahora trabajamos. En lo que respecta a la nube híbrida, por ejemplo, los firewalls tradicionales son aún más difíciles de usar, ya que necesitan trabajar en varios entornos, deben realizar un seguimiento de las cargas de trabajo en distintas nubes y se ha de controlarlos desde un único punto. Para intentar resolver estos problemas, han aparecido varios enfoques de segmentación de red.

Tres enfoques de segmentación que considerar

Al comprender que los firewalls, incluso cuando están virtualizados, no son adecuados para proteger los centros de datos de nube híbrida, las empresas pretenden aplicar la segmentación dentro de la infraestructura este-oeste de tres formas básicas. Como ya hemos comentado, sin una política de segmentación y medidas de seguridad sólidas, cualquier puerto o servidor tiene acceso para comunicarse con cualquier otro. Esto significa que, si un firewall de servidor sufre alguna filtración, un atacante podrá moverse fácilmente por toda la red. La forma más eficaz de limitar la conectividad entre servidores es segmentando la red. Existen tres tipos básicos de segmentación de la red, en los que la microsegmentación es la tecnología que las empresas pueden utilizar para aplicar políticas y controles cada vez más detallados. Los usuarios pueden combinar los tres tipos de políticas de segmentación que se enumeran a continuación, creando políticas más detalladas para aplicaciones críticas o con mayor nivel de riesgo.

Segmentación de entorno

Este enfoque separa los diferentes entornos entre sí. De esta forma, las empresas podrían segmentar su entorno de desarrollo del de producción, por ejemplo. Esta es la primera etapa crucial de cualquier estrategia de segmentación, a la que puede seguir la creación de políticas más detalladas.

Segmentación de aplicaciones

Llevando la segmentación un paso más allá, el "acordonamiento" de las aplicaciones de gran valor toma cada aplicación crítica específica y la mantiene aislada del resto de la red. Las mejores soluciones de microsegmentación permitirán incluso controlar esto a nivel de proceso.

Segmentación de niveles

La forma más estricta de segmentación se encuentra dentro de la propia aplicación. Puede crear una directiva sobre cómo se gestionan las comunicaciones entre niveles dentro del mismo clúster de aplicaciones, controlando el tráfico entre servidores web, servidores de aplicaciones y servidores de bases de datos, por ejemplo. Esto también se puede controlar con la aplicación a nivel de proceso, si se desea.

Método de segmentación de red: segmentación de red mediante VLAN

La mayoría de las empresas comienzan por utilizar VLAN. Estas redes de área local virtuales permiten a las empresas asignar a cada segmento su propia ruta de comunicación, ya sea a través de un firewall o con listas de control de acceso (ACL) en el propio router. Aunque la VLAN es una opción común para la segmentación de red, hay muchos problemas subyacentes. Analicemos la cuestión más a fondo, haciendo un balance de por qué las VLAN son una opción deficiente para satisfacer las necesidades de seguridad actuales.

Es fácil entender por qué muchas empresas eligen las VLAN como método de segmentación. Son compatibles con la arquitectura existente, lo que hace que su coste parezca bajo y su implementación, sencilla. No obstante, se trata de un enfoque de segmentación muy rígido y complejo, su mantenimiento puede resultar costoso y su implementación requiere tiempo de inactividad.

Para empezar a utilizar las VLAN, deberá familiarizarse con los servidores y las dependencias de cada segmento y, a continuación, crear la configuración que desee para el conmutador o los conmutadores de red que está segmentando. Dado que este proceso lo completan los ingenieros de red y a menudo implica varias ubicaciones, puede llevar muchos días y costar una cantidad desproporcionada de tiempo y dinero. El tráfico puede interrumpirse o ralentizarse durante el periodo de configuración.

En una época en la que la agilidad es una ventaja competitiva importante, tal vez incluso una necesidad, los altos costes y la lentitud a la hora de implementar cambios suponen un desastre para sus resultados finales. Según Forbes, la adaptabilidad es clave para sobrevivir: "La disrupción no es nueva, pero su velocidad, su complejidad y su naturaleza global están a una escala que nunca habíamos visto antes. No sobrevivirá el más grande o el más estable financieramente, sino aquel que logre adaptarse al ritmo de cambio exponencialmente acelerado".[2]

Es importante reconocer que las VLAN no se crearon teniendo en cuenta la segmentación. Puesto que se desarrollaron inicialmente para reducir la congestión, utilizarlas para controlar las comunicaciones no es una forma inteligente de aprovechar esta tecnología existente, sino que en muchos aspectos es un uso indebido. Teniendo esto en cuenta, no es sorprendente que la segmentación mediante VLAN tenga limitaciones.

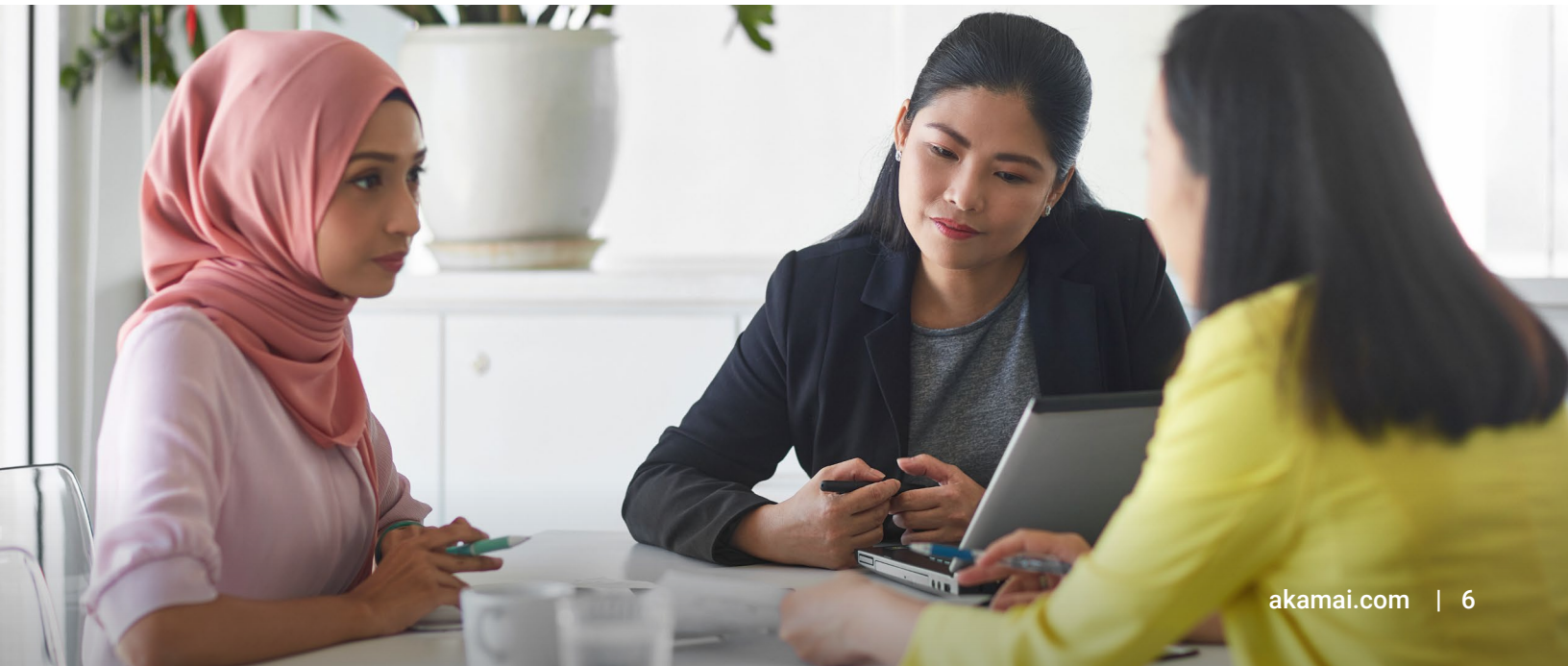
- **Tecnología de nube**: las VLAN y otras políticas tradicionales de segmentación de red no se pueden extender a la nube. Si utiliza firewalls internos segmentados (ISFW) o ACL para controlar qué usuarios pueden acceder a los segmentos de red, es probable que necesite utilizar redes definidas por software (SDN) para la nube. Esto se hace normalmente a través de proveedores de software terceros que utilizan subredes o firewalls virtualizados.
- **Contenedores**: la seguridad sigue siendo una gran preocupación dada la adopción generalizada de contenedores en los entornos de TI. Dado que cada contenedor se ejecuta en el mismo núcleo, un ataque podría poner en riesgo todos los contenedores. El aislamiento es un problema recurrente y no se puede resolver con los métodos habituales de segmentación de la red.
- **Restricciones de protocolo**: el límite para las VLAN es de 4096 segmentos, lo que limita la capacidad de proporcionar una segmentación adecuada en centros de datos de gran tamaño. Los enfoques de segmentación más detallados no tienen esta limitación.

De la segmentación de red a la segmentación de aplicaciones: Introducción de controles de capa 4

Muchos de estos problemas se han atenuado adoptando la segmentación de aplicaciones mediante grupos de seguridad en entornos de nube y firewalls basados en hipervisor para entornos virtualizados locales. La segmentación de aplicaciones tradicional implementa controles de capa 4, lo que permite aislar los niveles de servicio entre sí, de modo que una aplicación tenga un límite seguro. Cada nivel está limitado al acceso que necesita para proporcionar toda su funcionalidad, sin más. Existe una separación clara entre los niveles de una aplicación individual y la amenaza de un posible riesgo se mantiene al mínimo.

Piense en los niveles que puede encontrar en una empresa estándar, desde balanceadores de carga y bases de datos hasta servidores de aplicaciones dentro o fuera de su propia DMZ. Mantener estos niveles separados permite que cada uno tenga sus propias reglas y funciones de seguridad. La segmentación de aplicaciones puede ayudar a las empresas a aplicar los controles adecuados en cada nivel, limitando su información confidencial y sus comunicaciones, al tiempo que permite un amplio acceso de los usuarios cuando sea necesario. Por ejemplo, una empresa puede impedir que determinadas bases de datos se comuniquen con Internet o garantizar que, si un atacante incumple un balanceo de carga simple, no pueda cambiar para acceder a información más confidencial en el nivel de base de datos.

Conforme la solución se vuelve más granular, la segmentación de aplicaciones permite a una empresa segmentar un clúster de aplicaciones completo de otras áreas de la empresa. Como ya se ha comentado, esto reduce el área de la superficie de ataque y la capacidad de los atacantes para realizar movimientos laterales de un nivel a otro.

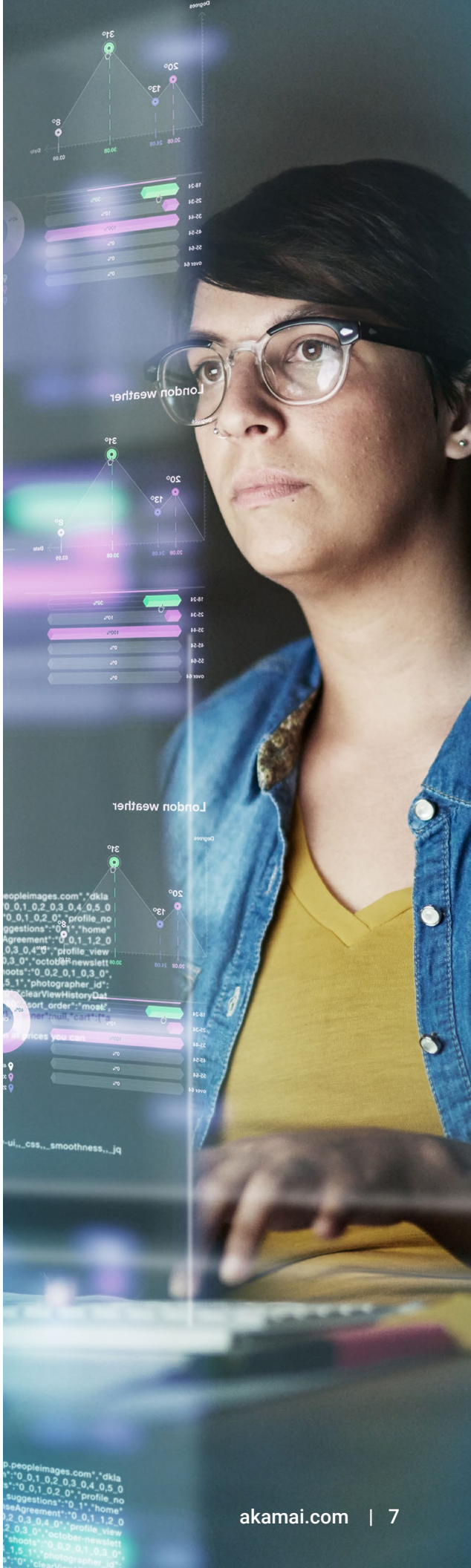


Los límites de los controles de capa 4

La segmentación de aplicaciones tradicional puede carecer de profundidad, lo que tiene un impacto directo en su visibilidad. La capa de red, donde se produce el enrutamiento, mueve los datos entre sistemas, asignando direcciones IP y protocolos que detallan la ruta de los segmentos de datos hasta su destino. La segmentación de aplicaciones a menudo utiliza controles de red de capa 4, centrándose en la forma en que se distribuyen los propios datos. Los segmentos de datos más grandes se dividen en segmentos o bloques más pequeños, listos para volver a agruparse en su destino. El control de flujo permite acelerar o ralentizar este proceso de forma dinámica, cuando los dispositivos que envían o reciben la información lo necesitan.

Con todas las amenazas que existen en la actualidad, los controles de estas capas son esenciales, pero en algunos casos es posible que desee tener la capacidad de establecer políticas a un nivel aún más detallado. Los atacantes han demostrado su capacidad para falsificar direcciones IP y utilizan técnicas de ocultación en puertos permitidos para vulnerar una red. Además, la protección de capa 4 no limita el movimiento lateral dentro de una aplicación o un nivel, lo que podría implicar una superficie de ataque mayor de lo deseado.

Las iniciativas de cumplimiento son uno de los mejores ejemplos de la necesidad de controles más granulares que la capa 4 por sí sola. Las técnicas tradicionales de segmentación de aplicaciones han permitido hasta cierto punto a las empresas cumplir determinadas normativas específicas, como mantener el CDE separado para satisfacer el estándar PCI-DSS o proteger la información médica protegida (PHI) para cumplir con las exigencias de la HIPAA. Sin embargo, si bien las técnicas de capa 4 se han aceptado en el pasado como medios eficaces para mostrar el cumplimiento, en la práctica se ha demostrado que pueden no ser suficiente. Según el Informe de seguridad de pagos 2022 de Verizon, solo el 43 % de las empresas alcanzan el "pleno cumplimiento".[3] Lo que es peor, incluso el 100 % de cumplimiento no equivale a un 100 % de seguridad. Aunque los controles de capa 4 pueden bastar en términos de cumplimiento, no reducen la superficie de ataque lo suficiente como para marcar una diferencia significativa para la seguridad. No hay vuelta de hoja. Los atacantes pueden utilizar un puerto abierto de capa 4 entre dos niveles con un proceso separado (capa 7) y tomar todo lo que quieran.



Segmentación en la oscuridad: La falta de visibilidad en la segmentación de la red y las aplicaciones

Como están descubriendo las empresas, si bien no hay duda de que la segmentación de aplicaciones es un paso en la dirección correcta, no llega lo suficientemente lejos como para resolver todos los problemas inherentes a un enfoque de segmentación general. Otro desafío que aún hay que abordar es la visibilidad. Poder obtener una visión general precisa y en tiempo real de la red es esencial en cada etapa del proceso de segmentación, lo que constituye una limitación de muchos enfoques en este sentido.

Antes de empezar, deberá visualizar las dependencias de las aplicaciones para poder elaborar reglas de directivas precisas. Una vez establecida la segmentación, necesitará pruebas de que la segmentación funciona según lo previsto, no solo para confirmar que su situación de seguridad es sólida, sino también para proporcionar pruebas de cumplimiento normativo cuando sea necesario.

Sin visibilidad histórica y en tiempo real, no hay pruebas para usted ni para terceros interesados y organismos reguladores. La recopilación manual de estas pruebas requiere mucho tiempo y es costosa de gestionar, y siempre existe la posibilidad de que se produzcan fallos y errores de configuración. Una solución de segmentación que no pueda proporcionar este tipo de visibilidad simplemente no da la talla.

Microsegmentación hasta la capa 7: La capa de aplicación

En comparación con lo anterior, la segmentación en la capa de aplicación (capa 7) es muy eficaz para limitar el movimiento lateral, incluso dentro de un clúster de aplicaciones. La capa 7 es donde los servicios de red se integran con el sistema operativo. Los protocolos como HTTP, FTP, TFTP y SMTP son todos protocolos de capa 7. Los últimos avances en tecnología de microsegmentación pueden segmentar en esta capa con mucha más profundidad que otras soluciones, lo que permite a su empresa visualizar y controlar la actividad en la capa 7, además de en la capa 4 tradicional. Esto significa que, en lugar de depender de direcciones IP y puertos, se pueden utilizar procesos y flujos específicos cuando las empresas configuran sus políticas. Esto lleva las ventajas de la segmentación mucho más allá de un nivel específico o incluso un clúster de aplicaciones. También le permite detectar amenazas potenciales con algo tan insignificante como un hash equivocado, incluso cuando el atacante está reflejando un proceso o ruta autorizados.

En lo que respecta a la creación de políticas, la segmentación en la capa 7 permite establecer reglas o excepciones de permisos muy específicas, donde solo se permiten procesos o flujos concretos, y todas las demás comunicaciones se bloquean de forma predeterminada. Esto puede forzar el aislamiento de datos entre sistemas, pero aun así permitir la comunicación para flujos de datos necesarios o críticos para el negocio.

Las mejores soluciones de microsegmentación proporcionan la visibilidad que las empresas necesitan para ganar agilidad

Con agentes en todas las cargas de trabajo (basados en hipervisor o VPC, contenedores, servidores bare metal o incluso sistemas IoT/OT), una solución de microsegmentación integral puede proporcionar a su empresa un mapa visual completo de toda su infraestructura de TI. Las soluciones realmente inteligentes incluyen entornos de centro de datos, nube, multinube y nube híbrida, y dispositivos remotos. Las soluciones tradicionales de segmentación de aplicaciones tienen dificultades para obtener esta visión todo en uno, normalmente porque utilizan una combinación de tecnologías centradas en la red.

Un mapa visual completo de su entorno también debe mostrarle qué políticas de seguridad están en vigor y se aplican en tiempo real. A simple vista, sus ingenieros y profesionales de seguridad deberían ser capaces de detectar posibles deficiencias que subsanar en la cobertura de su política, o qué políticas adicionales deben implementarse o crearse desde cero.

Esta visibilidad también permite a su empresa prepararse con antelación para el nuevo software o las actualizaciones de los sistemas existentes mediante la creación de reglas para segmentar las aplicaciones nuevas o actualizadas con antelación, antes de que estén listas para la implementación. Una vez que las actualizaciones están activas, los equipos de seguridad disponen de la información en tiempo real que necesitan para detectar y resolver cualquier actividad de las aplicaciones fuera de lo habitual, lo que garantiza que ningún riesgo de seguridad pase desapercibido ni se convierta en un ataque activo. Tras esto, su empresa dispone de las herramientas contextuales necesarias para comparar un incidente con los datos históricos y comprender el entorno exacto que posibilitó que se produjera la anomalía. Las políticas se pueden reforzar, la segmentación se puede adaptar y puede detallar el incidente para cumplir las normativas o realizar estudios adicionales.

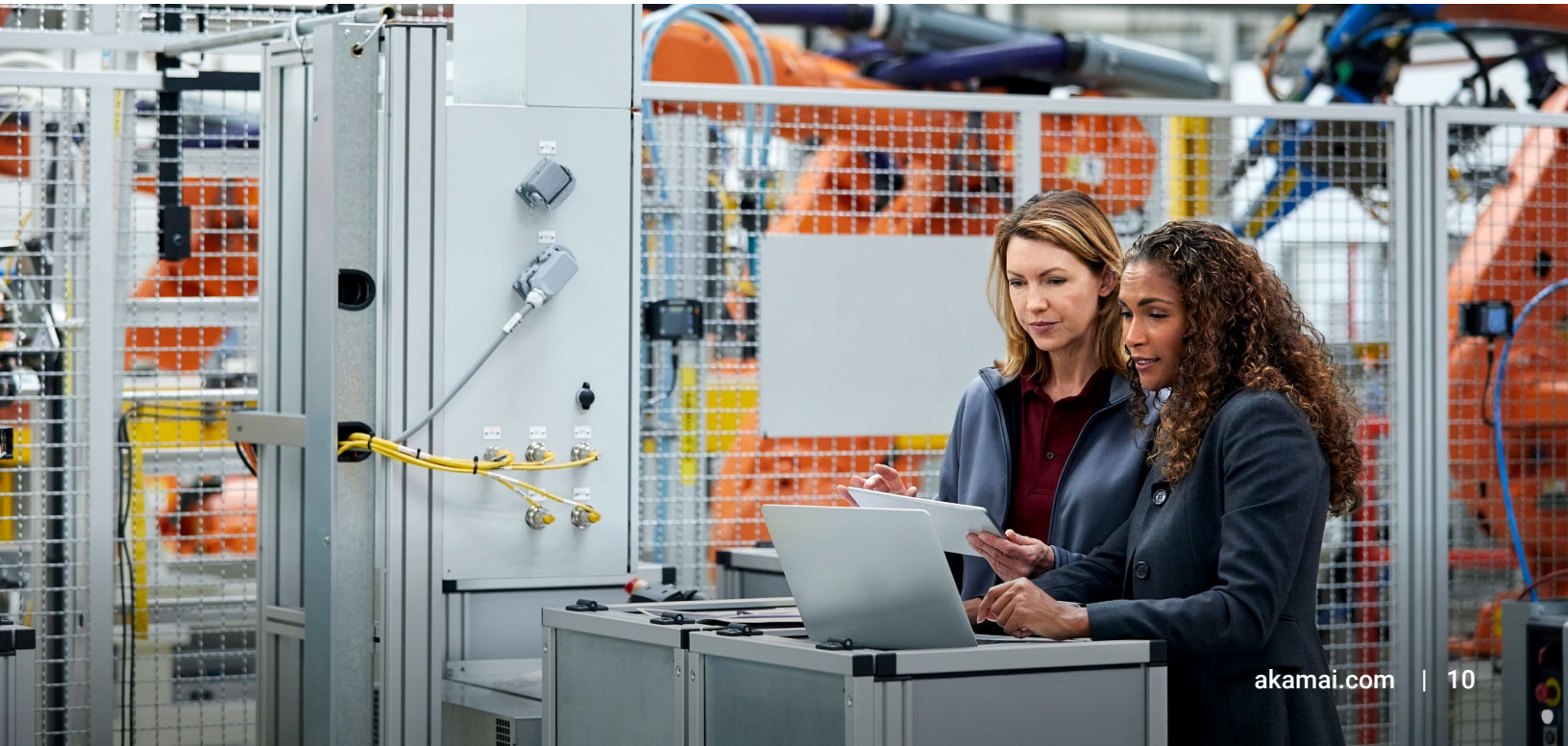
Empleo del modelo Zero Trust

Otra ventaja añadida de la microsegmentación es su capacidad para adoptar el modelo de seguridad Zero Trust. Aunque Forrester acuñó la idea de Zero Trust en 2010, tecnologías como la microsegmentación están ayudando a hacer realidad el concepto, y los investigadores y expertos en seguridad siguen alabando sus beneficios.[4]

La idea es sencilla: no se confía en ningún tráfico o usuario hasta que se demuestre su fiabilidad y se apruebe, ya sea procedente de una fuente externa o interna, cada vez que se produce un intento de conexión. Los tres principios fundamentales de Zero Trust, según Forrester[5], están respaldados por políticas de microsegmentación sólidas y detalladas:

- Hay que comprobar que todas las entidades sean de confianza
- Se implementa una supervisión completa de seguridad
- Se aplica el acceso de privilegios mínimos

Zero Trust se encuentra en el extremo opuesto del espectro de la seguridad exclusivamente perimetral, donde protegerás las entradas de tu castillo con un foso profundo y asumirás que todo lo que se encuentre en su interior tiene autorizado el acceso. Como la mayoría de las empresas ya no tienen una red o un centro de datos contenidos, la idea de un "castillo" es obsoleta, y una estrategia de privilegios mínimos como Zero Trust es la única manera de asegurarse de que puede saber y controlar quién está dentro en cualquier momento.



Prepare su empresa para el futuro con la microsegmentación

La segmentación de red puede ir más allá de la seguridad perimetral, y la segmentación del entorno y de las aplicaciones hasta la capa 4 son pasos importantes para crear su estrategia de segmentación. Sin embargo, a medida que los entornos de TI se vuelven cada vez más complejos, es posible que necesite una solución de segmentación que ofrezca aún más granularidad con la segmentación por niveles y a nivel de proceso en la capa 7 en las fases de aplicación y nivel.

Las empresas modernas han trascendido la infraestructura autónoma. A menudo dependen de tecnologías como SDN en la nube, contenedores o hipervisores bare metal. Asimismo, trabajan en diversas zonas geográficas y centros de datos físicos.

La única forma de protegerse de las amenazas externas e internas es emplear una solución que inspeccione y controle todo el tráfico, tanto este-oeste como norte-sur, y, en el caso de las aplicaciones cruciales o de mayor riesgo, que le ofrezca más visibilidad de la que se puede obtener solo con la capa 4. La microsegmentación hasta la capa 7, ya sea en fase de aplicación o nivel, le permite obtener una visión precisa de todo su entorno de TI y crear y aplicar fácilmente políticas de seguridad granulares conforme al modelo Zero Trust. Una buena solución de microsegmentación no le pedirá que elija entre seguridad y agilidad, así que escoja la opción que le ofrezca la estrategia de seguridad general más sólida en toda su organización.

Visite akamai.com/guardicore para obtener más información.

1 Shier, John. 2022. "Manual de estrategias del adversario activo 2022". Sophos. 7 de junio.

2 Gonda, Rob. 2018. "Adaptability Is Key To Survival In The Age Of Digital Darwinism". Forbes. 24 de mayo.

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. Junio de 2022. "Best Practices For Zero Trust Microsegmentation". Forrester. Abril.

5 David Holmes y Jess Burn. Enero de 2022. "The Definition Of Modern Zero Trust". Forrester. Abril.