Guardicore

Vuelva a plantearse los Firewalls:

Seguridad y Agilidad para le Empresa Moderna

Puntos destacados del Estudio de Investigación del Instituto Ponemon, patrocinado por Guardicore

Firewalls tradicionales: Su momento ya pasó

La necesidad de mayor agilidad en las operaciones IT está llevando al límite a las herramientas de seguridad tradicioanles como los firewalls de red y nueva generación. Los hallazgos obtenidos trás una reciente encuesta/ entrevista de Ponemon nos llevan claramente a pensar que los firewalls tradicionales ya tuvieron su momento y este pasó. Se han convertido en un obstáculo para la necesaria agilidad y flexibilidad, y además esto hace que sean menos efectivos protegiendo aplicaciones y datos, sobre todo en la nube.

Retos Zero Trust, Seguridad en la Nube y prevención de Movimientos Laterales

El estudio de Ponemon sugiere que combinar los firewalls con enfoques modernos de seguridad es un desafio enorme. La tecnología de firewalls perimetrales simplemente no fué pensada para gestionar workloads más precisos y que generan unos requisitos de throughput inmensos, requisitos que son necesarios con la segmentación granular. Las organizaciones que buscan implementar estrategias Zero Trust, que buscan prevenir los movimientos laterales o que quieren asegurar sus aplicaciones en la nube, están viendo las limitaciones de los firewalls tradicionales y están buscando alternativas.

- **El 53%** de los encuestados dicen que sus organizaciones están preparadas para una alternativa o una solución complementaria a su firewall tradicional.
- **El 63%** de los encuestados dicen que los firewalls tradicionales de sus empresas no habilitan políticas de Zero Trust a toda la empresa.
- **Solo el 24%** de los encuestados dicen que sus firewalls pueden defenderse en contra de exfiltración de datos.
- **El 66%** de los encuestados dicen que los firewalls tradicionales de sus empresas no son efectivos para restringir el movimiento lateral.
- **El 64%** de los encuestados dicen que los firewalls tradicionales de sus organizaciones no son efectivos ante ataques de ransomware.

¿Por qué los profesionales de seguridad se preparan para reducir el despliegue de los firewalls?

61%

de los encuestados dicen que sus firewalls tradicionales no pueden contener una brecha en el perímetro de su centro de datos.

52%

más de la mitad de los encuestados dicen que sus firewalls tradicionales no son efectivos al momento de proteger tráfico este-oeste.

60%

de los encuestados dicen que ellos considerarían reducir el despliegue de sus firewalls debido a los altos costos.

Más puntos importantes de la investigación del Reporte de Ponemon

15%

Solo el 15% de los encuestados se siente preparado para defenderse contra movimientos laterales con sus firewalls de legado.

62%

de los encuestados dicen que las políticas de control de acceso de los firewalls de sus organizaciones no están lo suficientemente granuladas.

73%

de los encuestados dicen que sus organizaciones tienen múltiples ambientes en la nube y que su promedio de uso de servicios en la nube promedia el 43% del ambiente IT.

41%

de los encuestados dice que utilizar firewalls tradicionales para segmentación de la red en el centro de datos es muy costoso.

67%

de los encuestados dice que la transformación digital es el evento primario que afecta la postura de seguridad de sus organizaciones.

62%

de los encuestados dicen que las auditorías fallidas son un evento primario que afecta la postura de seguridad de su organización.

¿Por qué más y más profesionales de seguridad están cambiando a soluciones de micro-segmentación?

Reducción de riesgos más efectiva

Habilitando la segmentación rápida de aplicaciones a un nivel muy granular, la segmentación basada en software resulta en una superficie de ataque enormemente reducida.

Velocidad a una postura de seguridad óptima

La segmentación basada en software te hace más seguro, mucho más rápido. Esto también significa que menos recursos – técnicos o humanos – están atados a proyectos de segmentación por períodos más largos.

Costo total dramáticamente más bajo

La segmentación basada en software puede ser lograda con un capital mucho más pequeño en comparación a comprar dispositivos de firewall y equipos adicionales.

OBTÉN EL REPORTE COMPLETO

www.guardicore.com

¿Preguntas?

¿Busca más información o tiene más preguntas? Por favor, póngase en contacto con su representante de ventas local, director de ventas regional o envíenos un correo electrónico a info@guardicore.com.