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 de Legado: Su momento ya pasó

El deseo de mayores velocidades y agilidad en operaciones de IT está empujando los límites de las herramientas de seguridad tradicionales como redes y firewalls de nueva generación. Hallazgos de una entrevista reciente realizada por Ponemon sugiere firmemente que los firewalls tradicionales ya pasaron su momento. Se están convirtiendo en un obstáculo para la agilidad y ahora son menos efectivos en proteger aplicaciones y datos, particularmente en la nube.

Retos con Cero Confianza, Movimiento Lateral y Seguridad en la Nube

El estudio de Ponemon sugiere que los firewalls tradicionales imponen enormes desafíos especialmente para las empresas que buscan desplegar enfoques más modernos a la seguridad. La tecnología de firewalls de perímetro de legado simplemente no fue realizada con la intención de demandas más precisas, restringidas por el ancho de banda que vienen con la segmentación granular. Las organizaciones que buscan implementar seguridad de Cero Confianza, previenen el movimiento lateral o aseguran sus aplicaciones y datos en la nube, están viendo rápidamente las limitaciones de los firewalls tradicionales y están buscando alternativas.

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

¿Por qué los profesionales de seguridad se preparan para reducir la huella de los firewalls?

61%

de los encuestados dicen que sus firewalls tradicionalesno pueden contener una brecha en el perímetro de su centro de datos.

52%

más de la mitad de los encuestados dicen que sus firewalls tradicionalesno son efectivos al momento de proteger tráfico este-oeste.

60%

de los encuestados dicen que ellos considerarían reducir la huella 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 en contra de 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.

© 2020, Guardicore Ltd. All rights reserved. CV0009-USv1