La conectividad centralizada garantizará que las empresas permanezcan seguras

La conectividad centralizada garantizará que las empresas permanezcan seguras. Los riesgos de la computación en la nube y cómo superarlos con una estrategia centralizada.
La computación en la nube ha creado infinitas oportunidades para que las empresas de todo el mundo crezcan y desarrollen servicios, aplicaciones y plataformas; así como la opción de crecer a las tasas que más les convengan.

Si bien ha proporcionado a las empresas un nivel de elección y flexibilidad que no había sido posible antes, la computación en la nube también abre puertas a una serie de problemas de riesgo y seguridad; y estos riesgos potenciales, como el acceso no autorizado al sistema, la complejidad de la gestión de la identidad de la red o la pérdida masiva de datos son difíciles de detectar sin las herramientas y la visibilidad adecuadas.

Para mitigar estos riesgos, los líderes empresariales necesitan mucha más visibilidad para tomar decisiones mejor informadas y educadas que beneficiarán a sus negocios. Con una visibilidad avanzada de dónde se encuentran las amenazas y los riesgos, se pueden construir defensas para mitigar todas las amenazas con confianza. La solución radica en la conectividad centralizada.

Puntos de entrada y salida

Los muchos y variados beneficios de los servicios basados en Internet han visto crecer rápidamente las infraestructuras de las empresas en un período de tiempo muy corto. Si bien esto es excelente para las empresas que desean expandirse

rápidamente, aumentar su flexibilidad y eficiencia tanto para los procesos internos como para los clientes externos, también aumenta el riesgo de amenazas.

A medida que el patrimonio crece, también lo hacen los puntos de entrada a la organización. La expansión demasiado rápida puede introducir puertas interminables que no están selladas de manera efectiva, donde los hackers pueden ingresar sin problemas y sin problemas para acceder a datos valiosos. A diferencia de un centro de datos con una puerta para abrir y cerrar, los servicios multinube y en la nube crean infinitas oportunidades para que los hackers accedan a los datos y, como tal, las empresas se vuelven mucho más vulnerables. Además, a medida que más empresas adopten un enfoque multinube, y con razón, deben ser conscientes de las diversas políticas de seguridad que tiene cada proveedor de la nube, y no adoptar un enfoque informal y poco convincente para cada proveedor de la nube.

Sombras IT

Nadie introduce la TI en la sombra con intenciones maliciosas; en realidad, generalmente se introduce para capacitar a los equipos para que sigan innovando al acceder a herramientas que los hacen más productivos y eficientes.

Sin embargo, crea una cultura aislada que evade completamente al departamento de TI. Con empresas que ahora adoptan culturas más flexibles, y con muchas oficinas ahora repartidas por todo el mundo, una cultura aislada puede ser perjudicial. La falta de visibilidad sobre a qué se accede, comparte y adopta significa que los profesionales que están capacitados para mitigar el riesgo no son conscientes de los riesgos que se están desarrollando.

Esto se está convirtiendo en un problema con investigaciones recientes que revelan que el 80 por ciento de los trabajadores admite usar aplicaciones SaaS en el trabajo sin la aprobación

de TI. No solo es un riesgo de seguridad, sino que también es un problema para los presupuestos; ya que los costos inesperados pueden acumularse sin un conocimiento completo de las tecnologías que utilizan los trabajadores.

Registros de SIEM sin terminar

Muchas empresas han recurrido a las soluciones de gestión de eventos e información de seguridad (SIEM) para proteger las redes de amenazas, tanto internas como externas. Estas soluciones se implementan para llevar a cabo análisis complejos de los datos de la red para identificar cualquier problema de seguridad. Proporciona a las empresas una vista única de todos los datos para identificar cualquier comportamiento y patrones fuera de lo común y permite a los profesionales de TI comprender y prevenir cualquier riesgo de incumplimiento.

Las soluciones SIEM solo pueden proporcionar un análisis claro y correcto si los datos que analiza son de buena calidad. Muchas empresas tienen datos faltantes y registros incompletos, lo que significa que las soluciones SIEM son incapaces de proporcionar un resumen detallado o podrían dar lugar a falsos positivos. Sin datos históricos exhaustivos, es imposible predecir lo que podría suceder en el futuro ya que la imagen no está completamente completa. Como tal, las empresas podrían no ser conscientes de lo que podría suceder en el futuro o, en cambio, buscar falsos positivos que desperdicien tiempo y dinero.

Sin visibilidad central

Hay conocimientos conocidos, incógnitas conocidas e incógnitas desconocidas que las empresas deben estar preparadas para enfrentar todos los días. Sin embargo, sin ninguna visibilidad central, las empresas se encuentran en una posición extremadamente vulnerable para luchar contra todas estas

posibilidades. La demanda de transparencia aumenta de acuerdo con el crecimiento de la empresa, si no más, por lo que las empresas necesitan procesos adecuados para evitar fallas y amenazas de seguridad.

El responsable de estas decisiones y procesos es el Director de Información y Seguridad, que tiene que comprender todo el panorama de riesgos para luego tomar las decisiones correctas para mitigarlo. Sin embargo, sin ninguna visibilidad central, el CSIO es incapaz de tomar decisiones correctas e informadas, ya que están trabajando con datos heredados o incorrectos. En consecuencia, todas las decisiones son erróneas y podrían tener consecuencias perjudiciales para el negocio.

La solución

Todos estos problemas descritos son legítimos y no son infrecuentes para las empresas. Por lo tanto, es imperativo que todas las empresas estén totalmente preparadas para mitigar cualquier riesgo y evitar que cualquier amenaza a la seguridad cause daños irreparables.

Como solución, las empresas deberían considerar centralizar su conectividad para establecer una fuente única, oportuna y precisa de la verdad en toda la empresa. La conexión segura de todas las diferentes entidades en un patrimonio y un ecosistema permitirá a las empresas volverse realmente ágiles, algo que ha perdido su verdadero significado en los últimos tiempos. Para ser realmente ágiles, las empresas deben tener la capacidad de agregar, cambiar y eliminar rápidamente proveedores de la nube, proveedores de conectividad y otros terceros de un tipo similar; poseer el poder de tener el control total y no estar atado a nada ni a nadie.

Sin embargo, Una red centralizada permite a las empresas dar un paso atrás y ver la imagen completa; sin ninguna pieza faltante del rompecabezas que sesgue su vista. Todos los puntos de salida potenciales son monitoreados y solo hay un

punto de salida singular que pasa por una plataforma centralizada que monitorea toda la red.

Las zonas oscuras de IT también se reduce, ya que los equipos de TI ahora están al tanto de todas las diferentes actividades en todo el negocio; incluyendo qué plataformas en la nube se están utilizando y, lo que es más importante, cuáles no. Finalmente, todas las soluciones SIEM pueden funcionar de manera efectiva con registros y políticas consistentes disponibles para trabajar y reducir drásticamente los falsos positivos.

En definitiva, un negocio exitoso solo es verdaderamente exitoso si tiene ojos en todas las áreas. A medida que la adopción de la nube continúa creciendo y aumentando a tales velocidades, es importante que las empresas permanezcan vigilantes en su seguridad. La conectividad centralizada les proporciona mucha más visibilidad y el beneficio de decisiones educadas y más informadas en toda la empresa.

Leer así mismo: 5 formas en que la conectividad de colocación puede transformar su red ; Por qué la conectividad Last Mile, última milla, es importante para su red ; Cómo proteger a su organización de las amenazas de seguridad en medio del aumento de los teletrabajadores