Publicado en Madrid el 18/01/2018

cPacket Networks analiza lo que se avecina para 2018

El fabricante señala tendencias clave como la velocidad, la seguridad y el Big Data en el mercado de las soluciones para redes empresariales

cPacket Networks, proveedor líder en soluciones de última generación de monitoreo de rendimiento de redes (NPM) y analíticas, desvela las predicciones del mercado de soluciones de seguridad y monitoreo de redes empresariales para lo que se avecina en este año 2018.

Actualmente existe una mayor conectividad y cada vez son más las empresas que buscan una transformación digital real de su negocio, convirtiéndose el papel de las redes empresariales en mucho más que crítico. Tendencias como la movilidad de los trabajadores, el aumento del uso del Internet de las Cosas y la proliferación de aplicaciones en la nube demandan más que nunca que las empresas aumenten sus infraestructuras de red para ser capaces de mantenerse al día con los constantes cambios.

Según señala Brendan O'Flaherty, CEO de cPacket Networks, "a medida que aumenta la velocidad de las redes empresariales, los responsables de la gestión de estas redes han de hacer frente a una verdad incómoda: los problemas que afectan a la red se multiplican a una velocidad cada vez mayor". "Si puedes analizar tan solamente un porcentaje del tráfico en una red de 10 Gbps, analizarás un porcentaje aún menor del tráfico de una red de 100 Gbps. A esa velocidad, la fuente del problema tendrá 'más lugares donde esconderse, haciendo que las estrategias de muestreo sean más susceptibles a falsos positivos y falsos negativos", dice O'Flaherty.

"Cuando se inicia una captura y análisis de paquetes después de que ocurra el problema, en la mayoría de los casos, los paquetes capturados pueden no estar asociados al problema y, por lo tanto, es casi imposible realizar un análisis de causa raíz. La solución adecuada es la de un sistema de monitoreo de red continuo que permita mantener un registro de todas las actividades de la red sin que haya impacto en el almacenamiento ni en la propia red", explica.

Respecto a las tendencias en Big Data, O'Flaherty apunta que: "A medida que las empresas observan aumentos cuantitativos en los datos transportados a través de sus redes, se pone de manifiesto la teoría que dice que cualquier conjunto de datos más grande proporcionará más información accionable que un conjunto de datos más pequeño. Pero los profesionales están empezando a reconocer las limitaciones de los macrodatos: primero, porque más datos no equivalen a extraer datos significativos; y segundo, porque puede resultar demasiado costoso a nivel informático encontrar aquellos datos que pueden proporcionar información relamente valiosa".

"El Big Data genera valor a partir del almacenamiento y procesamiento de grandes cantidades de información digital, pero sigue existiendo el reto de que esta información no puede analizarse con precisión con las técnicas o arquitectura tradicionales", apunta, y añade que "según el McKinsey Global Institute se estima que el volumen de datos está creciendo un 40% al año, y que seguirá creciendo 44× entre 2009 y 2020".

Sin embargo, como las empresas se centran en añadir ancho de banda, investigar formas de modernizar sus redes con software y expandir sus capacidades de redes inalámbricas, su principal preocupación es la seguridad de la red.

"Cuando una gran red corporativa se cae, la primera idea es sospechar que se trata de una violación de seguridad. Pero la fuente del problema podría ser un pico o descenso de la energía, o una configuración incorrecta. El problema es que los trabajos de monitoreo del rendimiento de red y monitoreo de seguridad están separados y aislados. Pero, en un apagón, con estos equipos aislados, el resultado final hace que sea que los problemas de red de consecuencias masivas pasen desapercibidos o tarden más en aislarse", dice O'Flaherty, sugiriendo que las empresas deberán comenzar a reconocer que las redes y el personal de seguridad trabaja mucho mejor como un mismo equipo, al igual que el personal de desarrollo y operaciones lo hace con la creación del movimiento DevOps.

Según indica, "los actores maliciosos son cada vez más inteligentes complicando la labor de detectar 'brechas de seguridad' entre los equipos en las organizaciones. El desafío sigue siendo que SecOps y NetOps a menudo son tareas con objetivos diferentes y, frecuentemente, no se comunican como resultado de una estructura corporativa divida en silos".

"Las empresas ganan si ambos equipos trabajan juntos", dice O'Flaherty. "Un equipo de seguridad estrechamente coordinado puede generar ahorros de presupuesto y de tiempo. Por ejemplo, invertir en herramientas y compartir datos de seguridad entre estos equipos eliminará la necesidad de tener que comprar mecanismos preventivos adicionales (y a veces innecesarios)".

Para obtener más información sobre cPacket Networks y sus soluciones de analítica y monitoreo de rendimiento de redes de última generación, visitar www.cpacket.com.

Datos de contacto:
Axicom Spain
671637795

Nota de prensa publicada en: Madrid

Categorías: Telecomunicaciones Hardware E-Commerce Ciberseguridad Recursos humanos