Las cuatro tendencias de redes de 2021 que todo CIO debe conocer

Entramos a 2021 en un lugar muy diferente de donde estábamos a principios de 2020. El papel de las redes y, en general, la función de TI se ha convertido con más frecuencia en el héroe, y a veces en el desprecio, de la continuidad y la resiliencia del negocio en la cara de la pandemia. A medida que los CIO se empapan de los elogios o se resisten, ahora deben mirar al horizonte y definir su enfoque y estrategia en un mundo post pandémico.

Aruba ha identificado cuatro tendencias principales a las que se enfrentan ahora los CIOs que pueden hacer o deshacer el programa de TI de una organización:

- El aumento de la fuerza laboral híbrida y cómo evolucionará durante y después de la pandemia
- El papel cambiante de la seguridad de la red integrada en todo el tejido de la red.
- Pasar de métricas de tiempo de actividad de redes a métricas de satisfacción del usuario, examinando las redes de manera integral como parte de la pila de tecnología de TI más amplia.
- Mantener el rumbo en la implementación de la automatización en las operaciones de redes, a pesar de los desafíos planteados por LAN, WAN y Nube.

La fuerza laboral híbrida está aquí para quedarse

A pesar de los avances recientes en las vacunas para COVID-19, es posible que muchas funciones aún no regresen por completo a la oficina hasta fines de 2021 y, en muchos casos, no regresen en absoluto. Después de hablar con los CIOs de todo el país, lo que está claro es que quedará una cierta cantidad de trabajo remoto después de que desaparezca la pandemia. Esa admisión presagia cambios profundos para los espacios de oficina físicos, la cultura corporativa, la conectividad y las redes.

Lo que muchas organizaciones pensaron que serían configuraciones remotas temporales para “aplanar la curva” de la tasa de infección pandémica, ha evolucionado para formar la fuerza laboral híbrida del futuro, donde los empleados trabajarán desde casa, la oficina o en cualquier otro lugar, donde sea que tengan un conexión segura y confiable.

Para TI, esta crisis ha presentado enormes desafíos, pero hay un lado positivo. Los CEOs y sus juntas directivas han llegado a reconocer el impacto que la TI puede tener en el negocio, incluida la rapidez con la que se pueden implementar los cambios, incluso en circunstancias tan estresantes.

Ahora, los CEOs y sus juntas directivas están pensando en las lecciones aprendidas de la pandemia para hacer que las redes, la seguridad y los programas generales de TI que supervisan sean más flexibles y dinámicos. Como resultado, TI tiene un asiento en la mesa para impulsar formas ambiciosas de transformación digital, incluso acelerando las transiciones planificadas existentes, envalentonadas con la forma en que la fuerza laboral se ha adaptado a lo que se conoce como la “nueva normalidad”.

La seguridad debe verse de forma dinámica: desde endpoints hasta el borde y la nube

Con la maduración de la nube y el crecimiento de las redes de borde con sus innumerables endpoints, todo acelerado por la explosión de IoT, la forma en que se define e implementa la seguridad ahora se está convirtiendo en parte de la arquitectura de la red, y no en un componente integrado en el entorno de TI de la empresa.

Con el auge del trabajo remoto y el entorno de trabajo híbrido, las OSC y los CIOs claman por un enfoque de seguridad conectada. Al observar los principios de diseño de redes del pasado, los expertos en seguridad básicamente comenzaron con una política y luego diseñaron una topología de red que a su vez satisfacía la política, lo que significaba que la topología y la política estaban estrechamente relacionadas. Esa dinámica está cambiando drásticamente. Las soluciones de redes han evolucionado para ofrecer grados significativos de separación, donde la política se programa cuando y donde se necesita, y solo cuando y donde se necesita.

Las soluciones de arquitectura de red Zero Trust seguirán siendo una pieza central de la seguridad efectiva con cargas de trabajo de TI tradicionales que se trasladan desde el borde al entorno de nube o SaaS. El vacío dejado atrás eventualmente será reemplazado por cargas de trabajo específicas de OT / IoT en el borde. Además, con la implementación de 5G, la arquitectura de red debe lidiar con cargas de trabajo de cómputo en el borde de acceso múltiple (MEC), tanto privadas como públicas, lo que requiere enfoques dinámicos de políticas de seguridad que deben evolucionar más allá de los flujos de trabajo centrados en el usuario que Zero Trust está optimizado principalmente para hoy.

La satisfacción del usuario final es el rey

Las métricas clave de TI también están evolucionando. Ya no es suficiente mantener la infraestructura de red en funcionamiento. La métrica del día es la satisfacción del usuario que, desde el punto de vista del CIO, está vinculada a la productividad de los empleados, lo que en última instancia puede afectar la rentabilidad empresarial.

Los equipos de redes y seguridad ahora se centran en las experiencias dinámicas que los usuarios finales desean y esperan con los servicios y aplicaciones que eligen usar para mejorar la productividad. En lugar de preguntar qué tipo de dispositivos se están conectando a la red, también deben concentrarse en mantener la flexibilidad y la agilidad mientras minimizan el riesgo. El objetivo del control de la red va de la mano con la agilidad empresarial. Al aplicar las medidas de seguridad adecuadas, los CIOs pueden facilitar mejor este entorno de TI cada vez más dinámico.

En última instancia, los CIOs quieren información más allá de la propia red y de las aplicaciones de disponibilidad y rendimiento que interesan a los usuarios y líderes empresariales. No están tan interesados en cómo se están desempeñando los aspectos esotéricos de la red, sino más bien, están más preocupados por si un usuario específico tuvo una mala experiencia con Zoom.

Mantener el rumbo de la automatización en las operaciones de red

Vinculado a la comprensión de las necesidades y la experiencia de los usuarios finales está la maduración de la automatización de la red. Pero el progreso de la automatización no es igual en todo el paradigma de las redes. En el centro de datos, que es un entorno más controlado en

comparación con WAN o LAN, la adopción está más avanzada. Los cambios en un centro de datos se llevan a cabo principalmente en una estructura jerárquica natural y, por lo tanto, es más fácil de entender y administrar a través de scripts de automatización.

El borde (tanto LAN como WAN), por otro lado, es un entorno más caótico porque los cambios son provocados por factores que no están totalmente bajo el control de TI, es decir, patrones de comportamiento humanos y de dispositivos que cambian constantemente. Existe una gran necesidad de aprovechar la inteligencia artificial y los modelos de aprendizaje automático para detectar cambios tan pronto como ocurren y responder a los que parecen persistentes, aunque sea por un período corto de tiempo. La madurez de las soluciones implementadas que brindan este componente de aprendizaje de la automatización en el borde mejorará significativamente en 2021. También habrá un progreso significativo en la combinación de estas con APIs y otras herramientas de automatización que brindarán las eficiencias prometidas y los conocimientos que los líderes de TI anhelan.

La pandemia también ha aumentado el interés en la automatización de redes en el borde entre los CIOs y los líderes de TI. Según una encuesta reciente a 2,400 tomadores de decisiones de TI en todo el mundo, el 35% planea aumentar su inversión en redes basadas en inteligencia artificial, ya que buscan infraestructuras más ágiles y automatizadas para entornos de trabajo híbridos.

Haciendo de 2021 un éxito

En 2020, las empresas y la economía fueron rescatadas por una serie de tecnologías de comunicación desarrolladas durante los últimos 40 años, que van desde la seguridad, la conectividad en la nube hasta las aplicaciones administradas y compatibles en la red. Ahora, en 2021, las cuatro tendencias descritas aquí pueden proporcionar a los CIOs y líderes de TI las herramientas para estar mejor equipados para navegar por la imprevisibilidad de hoy y más allá. Permiten a los líderes de TI de arriba hacia abajo posicionar estratégicamente a TI como la función crucial que las empresas necesitan para maniobrar con éxito lo que sea que depare el futuro, desde pandemias hasta cambios acelerados en las tendencias y entornos de la cultura laboral.