ESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Redes de educación superior para el campus digital inteligente

Brinda experiencias excepcionales para los estudiantes, el personal y la TI

Las instituciones de educación superior están bajo una presión constante de respaldar las exigencias de los administradores, los profesores, el personal y los estudiantes. Los programas escolares digitales, la colaboración en el aula y los servicios con reconocimiento del contexto se trasladan hacia la nube. Los campus son ciudades pequeñas fundamentales, y los nuevos dispositivos de la Internet de las cosas (IoT) desbordan en los laboratorios, los edificios y las instalaciones, lo cual obliga a la TI a encontrar formas de asegurar las comunicaciones de redes de TI. Los estudiantes actualmente utilizan más dispositivos en las clases, para el aprendizaje remoto y en residencias estudiantiles, y se solicita a la TI que respalde un aprendizaje personalizado para todos. Finalmente, las solicitudes de seguridad mejorada de los campus llevan a pedidos de detectores de disparos, botones de pánico habilitados por ubicación, cámaras de videovigilancia inalámbricas y sensores de humo.

Edge Services Platform de Aruba provee conectividad segura siempre disponible con una arquitectura que puede extenderse en una gran variedad de aplicaciones de tecnología operativa (TO), TI e IoT. Diseñada en el marco de la seguridad de confianza cero, la plataforma unifica las operaciones cableadas, inalámbricas y WAN y la seguridad donde sea que los usuarios estudien, trabajen o se trasladen. Para mejorar la eficacia operativa, Edge Services Platform utiliza automatización e información manejada por IA para prever problemas y optimizar la red antes de que los usuarios se vean afectados. Los resultados empoderarán a los profesores, el personal y los estudiantes para crear, innovar y colaborar de maneras que nunca antes fueron posibles, con privacidad y seguridad sin precedentes.

La educación superior es comúnmente objeto de las estafas de suplantación de identidad (*phishing*). Los ataques cibernéticos en estas instituciones han dado como resultado la exposición de más de 1.3 millones de identidades. En el último año, alrededor del 56 % de los institutos de estudios superiores y las universidades han visto un incremento en los ataques de *phishing*.

LA CONECTIVIDAD DEBE ESTAR UNIFICADA, AUTOMATIZADA Y SIEMPRE ACTIVA

Los campus funcionan sin parar, y así deben hacerlo las redes que los respaldan. Los estudiantes necesitan acceso a las redes a toda hora. Las clases y los proyectos de investigación avanzan noche y día, y los sistemas de seguridad pública deben estar siempre atentos. Para todas estas aplicaciones, el rendimiento de la red debe ser confiable de manera consistente.

La automatización puede ayudar a disminuir el alto porcentaje de tiempo de inactividad imprevisto de las redes causado por el error humano (Gartner, 2019).

Redes inalámbricas de alto rendimiento

La infraestructura Wi-Fi 6 (802.11.ax) de Aruba está diseñada para respaldar campus de cualquier dimensión con conectividad segura siempre activa. La itinerancia sin inconvenientes posibilita el acceso a la red sobre la marcha, mientras que las capacidades de alta densidad sirven tanto a auditorios para conferencias como a instalaciones deportivas repletas de entusiastas. La administración del aprendizaje y los sistemas de comunicación unificada pueden priorizarse para brindar datos, voz y video sensibles a la latencia y sin demora, pérdida o vibración.

Las actualizaciones sin impacto y la conmutación por error sin impacto garantizan que la red inalámbrica pueda mantenerse al día con las últimas actualizaciones de seguridad, tolerar errores y estar disponible cuando sea necesario. Sin interrupciones por evaluaciones o pruebas en línea, sin pérdidas de datos experimentales y de investigaciones, sin cortes de llamadas.

La infraestructura se beneficia de las herramientas líderes en la industria para autoadaptarse a los entornos y las aplicaciones cambiantes: ClientMatch para optimizar el rendimiento de la itinerancia, AppRF para optimizar el rendimiento de aplicaciones críticas, Adaptive Radio Management para mejorar el rendimiento de radio y AirSlice para administrar la asignación del ancho de banda.

Cita de un cliente: "Nuestra estrategia plurianual para sacar provecho de tecnologías como movilidad, Inteligencia Artificial, IoT, análisis y cadena de bloques depende de la infraestructura del tipo de nuestro Wi-Fi Aruba que sirve como base".

–Radha Krishnan, vicepresidente asociado de Servicios de Información,

Seneca College, Canadá

Switches inteligentes desde el borde hasta el núcleo

Edge Services Platform de Aruba incluye redes cableadas e inalámbricas que funcionan en conjunto para brindar una experiencia de redes consistente y segura. Aruba diseña sus propios semiconductores para que sus switches puedan proveer visibilidad granular alta y sumamente rápida del rendimiento del tejido de conmutación. Power-over-Ethernet (PoE) SmartRate permite que los access points Wi-Fi 6 operen a más de 1 Gbps en el cableado existente, lo cual elimina la necesidad de eliminar y reemplazar plantas cableadas para obtener rendimiento inalámbrico multigigabit.

El sistema operativo AOS-CX de Aruba presenta una base de datos de serie temporal que provee una visibilidad profunda de los datos que recorren el tejido de conmutación. Las intuitivas herramientas de administración definidas por software, los análisis incorporados y la automatización programable ofrecen una información incomparable de la actividad de la red y de los dispositivos, el aislamiento de errores y el rendimiento del sistema. Se pueden habilitar, revertir y cambiar fácilmente las mejoras y las actualizaciones sin producir impacto en la red o la gente que depende de ella.

Cita de un cliente: "Elegimos Aruba porque es líder en esa área... trabajamos en coordinación con el equipo para proporcionar una infraestructura cableada e inalámbrica con el fin de respaldar el aprendizaje en cualquier momento y en cualquier lugar".

–Stephen Castellas, gerente principal, Redes Globales, RMIT, Melbourne

Network Analytics Engine (NAE), incluido con AOS-CX, provee un contexto incorporado para monitorear y solucionar problemas en las redes. EL NAE detecta problemas en tiempo real y analiza las tendencias mediante el uso de bases de datos de serie temporal para que la TI pueda prever problemas futuros de rendimiento y seguridad.

AOS-CX, combinado con los switches de alto rendimiento, brinda la productividad, el desempeño y la información procesable que los administradores de la TI necesitan para manejar cantidades masivas de datos que se generan actualmente en el borde de la red en todos los institutos de estudios superiores y las universidades.

PROTEGE LA RED DE EXTREMO A EXTREMO

A pesar de que las instituciones de educación superior han estado invirtiendo en ciberseguridad, las inquietantes estadísticas de vulneración y los costosos ataques de *ransomware* muestran que se debe hacer aún más para proteger a las personas y la información. Las soluciones de seguridad tradicionales crean un perímetro seguro y detectan ataques y *malware* en función de sus patrones o firmas. Este modelo no es adecuado para los institutos de estudios superiores y las universidades donde no hay perímetro: los estudiantes, el personal y los profesores se trasladan dentro y fuera del campus y necesitan acceso a la red desde cualquier sitio.

El contexto de la seguridad de confianza cero de Aruba segmenta dinámicamente el tráfico de la red. Con administración de políticas, análisis y automatización, se minimizan los riesgos de vulneración de seguridad, y a la vez, se mejoran la detección y las respuestas.

Entérate de lo que hay en la red

Con dispositivos IoT que surgen aparentemente en todos lados, saber qué hay o que debería haber en la red de TI puede resultar un desafío. ClearPass Device Insight potenciado por IA simplifica la identificación y la incorporación de dispositivos mediante el aprendizaje automático para identificar y crear perfiles de tipos de dispositivos de IoT, con el fin de que puedan segmentarse dinámicamente, corregirse o ponerse en cuarentena automáticamente.

Acceso de seguridad de confianza cero

Una vez que se identifican los dispositivos, ClearPass Policy Manager crea perfiles, autentica, autoriza y administra sólidamente el acceso a la red mediante controles de acceso granulares basados en políticas. Los usuarios y los dispositivos tienen acceso restringido únicamente a aquellos recursos de red, TI y aplicaciones para los cuales han sido aprobados. ClearPass también garantiza que los usuarios y los dispositivos cumplan con las regulaciones que rigen la privacidad de los estudiantes y la información identificable personalmente.

Tráfico de estudiantes, de personal y de IoT separados

La segmentación dinámica establece túneles seguros entre dispositivos de TI, IoT y tecnología operativa (TO) de planta y sus aplicaciones asociadas. Esta microsegmentación de confianza cero sin perímetro se aplica a las redes cableadas, inalámbricas y WAN, de manera que, sin importar dónde los usuarios y los dispositivos trabajen o se trasladen, la microsegmentación se mantendrá en efecto. Las políticas se trasladan de extremo a extremo por la red, independientemente de la ubicación del usuario, el dispositivo o el puerto del switch que transporte el tráfico, es decir, el tráfico del aprendizaje de los estudiantes se separa de los registros de los estudiantes, las cámaras de seguridad públicas y el tráfico administrativo.

ACTÚA RÁPIDAMENTE CON LAS INTUITIVAS HERRAMIENTAS DE ADMINISTRACIÓN POTENCIADAS POR IA

Edge Services Platform de Aruba incluye características de aseguración y orquestación para maximizar el tiempo de actividad, optimizar la experiencia de los usuarios y reducir el tiempo para solucionar problemas hasta la causa principal. La aseguración de redes automatizada proporciona información de AIOps desde un panel único, mientras que el monitoreo de la experiencia desde el borde a la nube genera alertas automatizadas basadas en la IA que identifican de manera proactiva los problemas importantes de redes y aplicaciones.

Optimización de la conectividad, la visibilidad y la administración de sitios remotos

La solución SD-Branch de Aruba se beneficia de las capacidades de SD-WAN para brindar conectividad segura a los campus satelitales remotos y las instalaciones de investigación. Al ofrecer el monitoreo de acuerdos de nivel de servicio (SLA) en Internet, conmutación de etiquetas multiprotocolo (MPLS) y enlaces WAN celulares, la solución abarca redes WAN, WLAN, cableadas y la administración de la seguridad.

La implementación es instantánea, y puede realizarla incluso personal no técnico, sin necesidad de visitas del equipo de TI. Se utiliza una aplicación móvil de Aruba para escanear códigos de barras en dispositivos de Aruba y se descargan automáticamente las configuraciones para los gateways administrados en la nube de Aruba Central. No hay una manera más rápida o intuitiva de conectar y habilitar sitios remotos que la solución SD-Branch de Aruba.

Aseguración de AIOps para brindar un rendimiento optimizado Aruba brinda recomendaciones personalizadas mediante el aprendizaje automático basado en IA para mejorar el rendimiento de la red y las aplicaciones en función de una comparación anónima con entornos de pares. Si un cambio puede aumentar el rendimiento un 10 %, se lo recomienda al administrador de la red, quien puede autorizar el cambio de configuraciones.

Aruba User Experience Insight provee a la TI una vista en tiempo real de la experiencia del usuario final y pasos de acción claros para resolver cualquier problema antes de que se emita un ticket de soporte. Estas herramientas poderosas proporcionan una ayuda fundamental para posibilitar que el abrumado personal de TI tome las medidas necesarias y se adelante a los problemas.

SOLUCIONES ÚNICAS QUE BRINDAN EXPERIENCIAS MEJORADAS Y SEGURIDAD A LOS ESTUDIANTES

Los institutos de estudios superiores y las universidades son sitios de enseñanza y de comunidad. La seguridad de los profesores, los estudiantes y el personal solía darse por hecho, pero ya no es el caso. Los actuales desastres naturales, los disturbios civiles y los enfrentamientos con disparos afectan a la seguridad de los campus y constituyen una gran preocupación para los servicios de emergencias. La infraestructura de la red puede ayudar mediante el cálculo de la naturaleza de la amenaza, la identificación de áreas seguras y no seguras y la orientación automática de las personas hacia la seguridad. A pesar de que las redes no pueden evitar que ocurran incidentes, pueden reducir su impacto manteniendo más seguros a profesores, estudiantes, personal, visitantes y servicios de emergencias.

Access points como plataformas de IoT

Estamos acostumbrados a considerar a los access points Wi-Fi en el contexto del acceso seguro a la red inalámbrica, y por muchos años esa fue su función principal. Hoy ya no es así. Los access points Aruba Wi-Fi 6 incluyen radios para señalizaciones, geovallas, rastreo de ubicaciones, monitoreo de sensores, bloqueo de puertas y control de accionadores. Estas capacidades transforman a los access points Aruba en sistemas seguros de comunicación multipropósito que están tanto en rampas de acceso a la red como en plataformas de IoT plenamente desarrolladas.

Cita de un cliente: "Las aplicaciones basadas en Meridian posibilitan que los usuarios naveguen de manera fácil y segura en el campus. Esto beneficia tanto a los estudiantes en sus primeros semestres como a los visitantes. Más importante aún, hemos creado una solución que resalta las rutas de acceso fácil".

–Carsten Hellmich, gerente de proyectos técnicos, Hochschule Hannover

Los dispositivos de seguridad de terceros respaldados por access points incluyen, entre otros, botones de pánico móviles, detectores de disparos, detectores de ocupación, bloqueos electrónicos de puertas y detectores de humo:

- Los botones de pánico móviles se activan para pedir ayuda e identifican la ubicación de la persona en apuros
- Los detectores de disparos identifican el tipo de arma y la velocidad del proyectil, para que los servicios de emergencia puedan llegar preparados
- En caso de un incidente, el sistema de detección de ocupantes activará un mensaje que les preguntará a los ocupantes si están a salvo y luego, generará un modelo del sitio 3D interactivo que indicará a los servicios de emergencia adónde deben ir primero
- El bloqueo electrónico de puertas puede utilizarse para asegurar edificios y residencias estudiantiles, y proveer acceso remoto al personal de emergencias, y
- los sensores de humo pueden utilizarse para hacer que se cumplan las regulaciones que prohíben fumar en baños y dormitorios.

Todo tipo de sistemas de edificios de bajo voltaje (que incluye comodidad, detección de intrusiones, administración de la energía, control de acceso, rastreo de personal y de activos, "hombre caído", botón de llamadas, detección de fugas, seguridad y monitoreo de disparos) puede comunicarse ahora de manera confiable y segura en la infraestructura compartida. Los ahorros que suponen los costos de equipamiento, instalación y mantenimiento para la implementación de las redes de control dedicadas son considerables.

UN SOCIO EN SU TRAYECTO HACIA EL CAMPUS DIGITAL INTELIGENTE

Las experiencias más dinámicas y transformadoras suceden en el borde. La misión de Aruba es aprovechar y asegurar los datos en el borde y, en asociación con nuestros clientes, posibilitar las iniciativas más importantes de digitalización de la educación. Comienza este trayecto y ponte en contacto ahora mismo con tu vendedor local de Aruba.

aruba
a Hewlett Packard Enterprise company

SO_HigherEducationNetworks_SK_051920 a00099194enw