HPE aruba networking

Folleto

Facilitar la adopción de la seguridad de confianza cero

Cómo acelerar tu viaje hacia la confianza cero con conectividad de red impulsada por IA y centrada en la seguridad

Comienza ya >

HPE GreenLake

Índice

Cambio de paradigmas

La innovación es crucial para las organizaciones. En el mundo actual que prioriza lo digital, las grandes experiencias son el sello distintivo de la innovación.

Las grandes experiencias ayudan a las organizaciones a destacarse en un mercado saturado, atraen a trabajadores con talento de todo el mundo y mantienen a las organizaciones prósperas en medio de la incertidumbre, el cambio y la disrupción.

Las grandes experiencias se impulsan mediante la conectividad: conectando a las personas entre sí, a los minoristas con los clientes, a los médicos con los pacientes, a los trabajadores con las aplicaciones, a los dispositivos con la nube y a los datos con los algoritmos.

Esta conectividad nunca descansa. Está siempre en funcionamiento y siempre es accesible, en cualquier lugar.

La conectividad trae consigo la promesa de una mayor personalización, experiencias satisfactorias para usuarios y empleados, ventajas y, en última instancia, crecimiento.

También puede suponer una complejidad para la TI.

Los equipos de redes y seguridad desempeñan un papel cada vez más estratégico a medida que la conectividad y las iniciativas tecnológicas como la inteligencia artificial generativa ascienden en la lista de prioridades principales. Al mismo tiempo, los entornos en lo que operan los equipos de redes y de seguridad se están volviendo más difíciles de navegar. Las medidas de seguridad, privacidad, gobernanza y cumplimiento de la normativa evolucionan constantemente, exigen esfuerzos más coordinados y suponen un reto para los equipos que ya hacen más con menos.

¿Qué es la confianza cero?
Los principios de confianza cero requieren que los usuarios y los dispositivos demuestren su fiabilidad para poder acceder a los recursos que necesitan para hacer su trabajo o cumplir su función. Este concepto de acceso de mínimo privilegio es fundamental para las prácticas de seguridad de confianza cero.

La seguridad de confianza cero también exige la supervisión continua de los usuarios y los dispositivos. La fiabilidad se reevalúa constantemente y si un usuario o dispositivo comienza a actuar de forma sospechosa o incongruente con su rol, su acceso puede verse limitado o revocado. Este control limitado y evaluado dinámicamente puede ayudar a minimizar e incluso impedir la propagación lateral de los ataques.

¿Por qué seguridad de confianza cero?
Los enfoques de seguridad de red centrados principalmente en la protección del perímetro ya no son suficientes, dada la creciente adopción de IoT, la erosión del perímetro corporativo debido al trabajo desde cualquier lugar y las amenazas cada vez más sofisticadas que explotan a los usuarios y dispositivos «de confianza» con fines maliciosos.

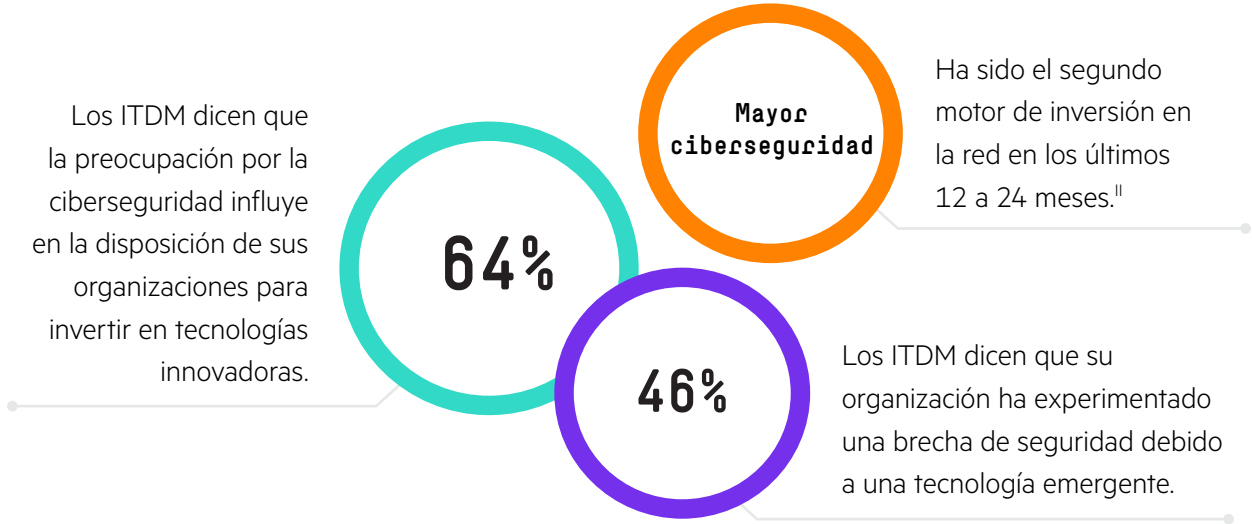
La necesidad de confianza cero

La conectividad es la clave para la innovación y el centro de la conectividad está en la red. Ya sea trabajando en la oficina, comprando en una tienda, iniciando sesión desde una cafetería o conectando una cámara de vigilancia a una aplicación en la nube, la red siempre está ahí.

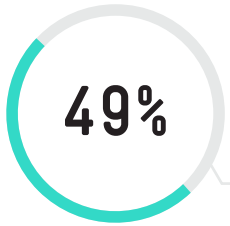
¿Qué más se espera? Amenazas no detectadas.

La expectativa es tan generalizada que ha dado lugar a un nuevo modelo de arquitectura de seguridad: la confianza cero. Los modelos de seguridad de confianza cero suponen que hay un atacante presente en el entorno y, por consiguiente, una red propia no es más segura que una red ajena.[I]

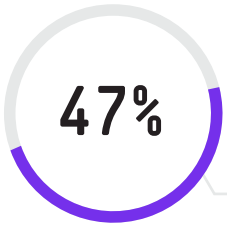
¿Cómo equilibran las organizaciones la necesidad de contar con alto rendimiento y acceso ininterrumpido en toda su red con la necesidad de una seguridad fiable?



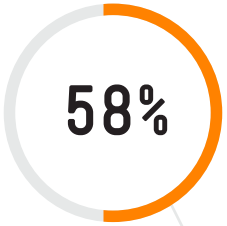
Los desafíos de la confianza cero



de las organizaciones todavía no han implementado seguridad de confianza cero.



calificó a su organización como muy o altamente eficaz en la reducción de amenazas en el panorama de los ataques.



de las organizaciones calificadas como muy eficaces a la hora de hacer frente a un panorama de amenazas en constante cambio han adoptado la seguridad de confianza cero, frente al 50 % de las demás organizaciones.[III]

Si bien la adopción de confianza cero ha crecido en los últimos años, su implementación todavía les resulta difícil a muchas organizaciones. Esto se debe a varios motivos.

1. **Un paradigma, no un producto**. Confianza cero no es un solo producto o solución que se puede comprar en cualquier tienda. Se trata de un conjunto de principios arquitectónicos rectores que deben perfeccionarse constantemente y llevarse a la práctica mediante decisiones políticas y de infraestructura; como tal, no es una iniciativa de «una vez por todas». Avanzar hacia una visión de confianza cero puede llevar tiempo, ya que la mentalidad en materia de seguridad cambia y los procesos se adaptan.

2. **Requisitos entre dominios.** La confianza cero abarca todos los ámbitos tecnológicos de una organización, no solo la conectividad de red, sino también los usuarios, los dispositivos, las aplicaciones y las cargas de trabajo en los campus, las sucursales, los centros de datos, la nube y más allá. La coordinación, el control y la coherencia son críticos, pero difíciles de conseguir dada la diversidad de entornos.
3. **Capacidades fragmentadas.** Las capacidades de control de acceso que admiten las arquitecturas de confianza cero suelen abarcar varias soluciones tecnológicas, que a menudo se combinan de forma inconexa. Con el tiempo, este enfoque de mosaico no solo aumenta la complejidad arquitectónica y operativa, sino que también expone a la organización a lagunas de seguridad, incoherencias en las políticas y su aplicación, y posibles riesgos de ciberseguridad derivados de lagunas involuntarias.[IV]
4. **Colaboración de equipos.** Ofrecer una innovación exitosa que cumpla los requisitos de seguridad de confianza cero a menudo requiere que los equipos de red y seguridad trabajen juntos para perseguir metas y objetivos comunes, proporcionando experiencias superiores, a la vez que se mantiene a la organización a salvo de ataques cada vez más frecuentes y sofisticados. Las herramientas dispares y la falta de controles y datos compartidos pueden crear operaciones aisladas que obstaculizan los esfuerzos por alcanzar resultados de negocio conjuntos.

El nuevo rol de la red

Es fundamental infundir a la innovación los principios de la confianza cero, y la innovación se basa en la conectividad. Esto significa que la red tiene ahora un papel esencial como parte de un ecosistema global de seguridad de confianza cero.

Ha llegado el momento de que los responsables de TI piensen en la red como una solución de seguridad de confianza cero.

Aunque ningún proveedor o solución puede ofrecer por sí solo toda la protección cibernética que necesita una organización, comenzar con una red que proporcione una base integrada para la seguridad de confianza cero puede facilitar la aplicación de los requisitos de seguridad, al tiempo que añade protección en los puntos de entrada digitales críticos. Y, en su doble papel de facilitadora de la conectividad y defensora de la ciberseguridad, la red se convierte naturalmente en un lugar de colaboración y cooperación entre los equipos de red y de seguridad.

Su elección de red es importante cuando se trata de proteger tu organización.

Facilitar el camino para la adopción de confianza cero

Conectividad de red impulsada por IA y centrada en la seguridad

Acelera tu viaje hacia la adopción de confianza cero con conectividad de red impulsada por IA y centradas en la seguridad de HPE Aruba Networking. Creadas con los principios de confianza cero, las soluciones de red impulsadas por IA y centradas en la seguridad de HPE Aruba Networking proporcionan una base común para que los equipos de redes y seguridad impulsen experiencias distintivas y resultados de negocio innovadores sin sacrificar la protección de la ciberseguridad.

Una red impulsada por IA y centrada en la seguridad de HPE Aruba Networking facilita la adopción de la seguridad de confianza cero y respalda el cumplimiento de las normas y reglamentos de ciberseguridad al permitir que los equipos utilicen la red como solución de seguridad. Ahora, la red puede proporcionar visibilidad e información avanzados, gestión de políticas centralizada, protección de datos, defensa frente a amenazas y control de acceso en una única plataforma. Con estas capacidades integradas de seguridad de confianza cero, la propia red se convierte en una línea de defensa crítica que se integra con los elementos del ecosistema de seguridad para mejorar la protección sin la complejidad añadida que suponen múltiples herramientas dispares, o el costoso y perturbador requisito de desinstalación y sustitución de la infraestructura existente.

La conectividad de red impulsada por IA también multiplica el poder humano de una organización, un factor crucial a medida que se amplían los marcos normativos, se ensanchan las brechas de talento y aumentan las amenazas cibernéticas. Con la conectividad de red impulsada por IA y centrada en la seguridad de HPE Aruba Networking, los equipos pueden beneficiarse con la automatización automática que reduce el esfuerzo manual, mejora la visibilidad y la detección de anomalías, y mejora la supervisión y los diagnósticos, todo lo cual garantiza que la organización no se exponga a riesgos innecesarios.

¿Cómo facilita la conectividad de red impulsada por IA y centrada en la seguridad la adopción de la Seguridad de Confianza Cero?

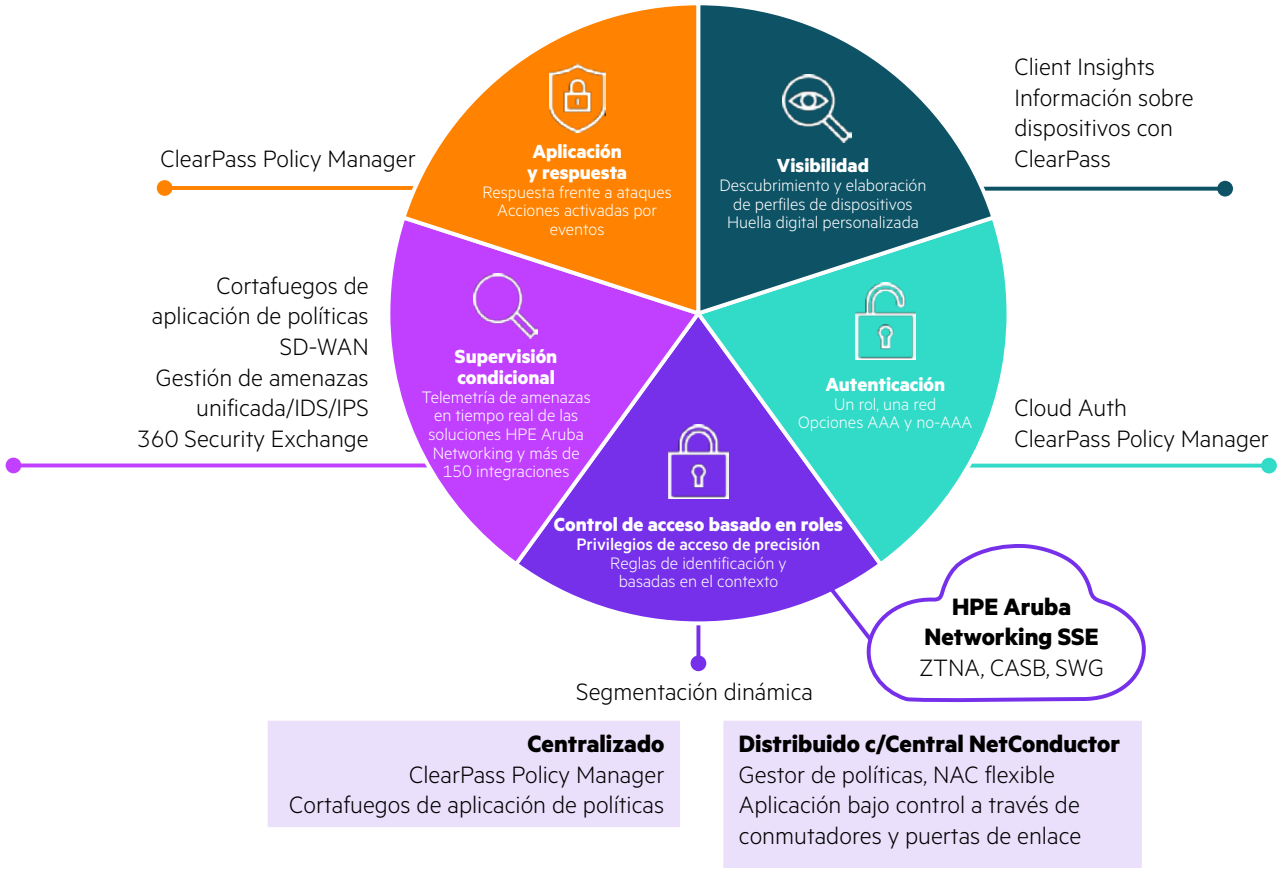
1. Ofrece **visibilidad compartida** para una fuente común de verdad entre equipos y herramientas.
2. Proporciona **gestión de políticas global** para simplificar la definición y la aplicación de políticas.
3. Posibilita la **aplicación desde el extremo hasta la nube** para optimizar el rendimiento y realizar un control coherente.
4. Es **impulsada por IA** para mejorar la eficiencia y la seguridad.

¿Buscas adoptar seguridad de confianza cero? Ten en cuenta sus requisitos básicos.

«Lo ideal sería poder responder a algunas preguntas de cada usuario o dispositivo de su red: ¿Quién eres? ¿Qué se te debe permitir hacer en esta red? ¿Cómo puedo aplicarlo mediante el control de políticas?»

– Jon Green, director de Tecnología y director de Seguridad, HPE Aruba Networking, Hewlett Packard Enterprise[V]

Fundamentos de seguridad de confianza cero con HPE Aruba Networking

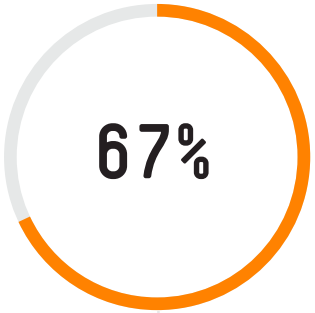


A diferencia de otros enfoques que requieren una colección de soluciones de seguridad inconexas atornilladas a la infraestructura de red, la conectividad de red de HPE Aruba Networking impulsadas por IA y centradas en la seguridad ofrecen soluciones de confianza cero integradas que se planifican, se diseñan y se ponen en funcionamiento como parte natural de una implementación de red. Las soluciones de HPE Aruba Networking también se integran a la perfección con el resto del ecosistema de seguridad para informar y actuar en función de la información procedente de todo el entorno de seguridad, lo que ayuda a mejorar la protección al tiempo que simplifica las operaciones.

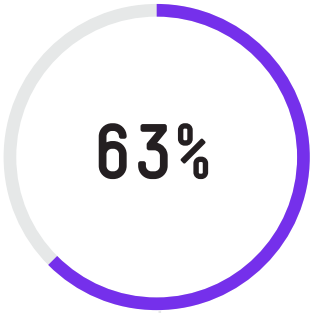
Visibilidad compartida

Operar a partir de una verdad común

La seguridad de confianza cero comienza con la visibilidad de los usuarios conectados y sus dispositivos. Sin embargo, en muchas organizaciones persisten las brechas de seguridad causadas por la falta de visibilidad y control de las actividades de los usuarios y los dispositivos. Gran parte de la brecha está impulsada por el creciente número de dispositivos IoT conectados a las redes empresariales, que representan una expansión significativa de la superficie de ataque de la organización. Para agravar el problema, los dispositivos IoT suelen ser instalados y gestionados por líneas de negocio que no son TI, lo que contribuye a la falta de visibilidad.



Los encuestados afirman que la identificación y autenticación de los dispositivos IoT que acceden a su red es fundamental para la estrategia de seguridad de sus organizaciones.



Los encuestados dicen que los equipos de seguridad carecen de visibilidad y control sobre cada usuario y dispositivo conectado a su infraestructura de TI.[VII]

La conectividad de red impulsada por IA y centradas en la seguridad facilitan a los equipos la implantación de controles de seguridad de confianza cero al ofrecer visibilidad y control compartidos. Tomar decisiones de confianza basadas en una fuente combinada de datos agiliza las operaciones de redes y seguridad, para que los equipos puedan tomar decisiones fundamentadas sobre cómo supervisar y gestionar los riesgos.

Las ventajas de la visibilidad compartida

- Saber con certeza quién y qué está en tu red, y controla continuamente el comportamiento y el estado
- Compartir datos con otros elementos del ecosistema de seguridad, como los SIEM, para ofrecer alertas y perspectivas de toda la infraestructura
- Aprovechar el análisis de tráfico de red integrado y las líneas de base de comportamiento para la detección temprana de ataques, deteniendo o evitando potencialmente su propagación

Soluciones de HPE Aruba Networking

La solución de gestión de red basada en la nube HPE Aruba Networking Central incluye visibilidad y creación de perfiles impulsados por IA con Client Insights. Client Insights analiza la telemetría nativa de la infraestructura procedente de puntos de acceso, conmutadores, puertas de enlace y clientes, sin necesidad de instalar colectores o agentes físicos. Client Insights proporciona perfiles precisos de dispositivos con IA/AA con hasta un 99 % de precisión en clientes conocidos con una tasa <5 % de desconocidos a través de una amplia variedad de puntos finales que se conectan a la red[VIII], entre ellos un conjunto diverso de dispositivos IoT en toda la infraestructura cableada e inalámbrica. Para los entornos no gestionados de forma externa por HPE Aruba Networking Central basado en la nube o con dispositivos de red de terceros, HPE Aruba Networking ClearPass proporciona identificación y creación de perfiles de clientes basada en aprendizaje automático.

Gana hasta un 99 % de precisión en la elaboración de perfiles para dispositivos conectados a la red, incluidos los de IoT

¿Cómo simplifican las políticas basadas en funciones la adopción de marcos de seguridad de confianza cero?
Los roles permiten que las definiciones de políticas se transmitan a través de las redes, independientemente de la ubicación geográfica o del punto de conectividad a la red. Las políticas adecuadas pueden seguir a los usuarios y dispositivos de forma coherente en sus desplazamientos por la empresa, desde el campus a la sucursal, a la oficina en casa y más allá.

Política global

Políticas que siguen al usuario

Una vez que se conoce y se elabora el perfil del usuario o el dispositivo, el siguiente paso en un marco de seguridad de confianza cero es autenticar su identidad cada vez que se conecta y asignarle políticas de control de acceso apropiadas. Sin embargo, definir y gestionar las políticas puede resultar complicado, ya que la dinámica empresarial cambia, los trabajadores se conectan desde cualquier lugar y se añaden dispositivos IoT. Los enfoques que se basan en construcciones específicas de la ubicación o de la red, como las direcciones IP o las subredes, pueden generar complejidad e inflexibilidad en la red y crear riesgos de seguridad asociados a las incoherencias en la definición y la aplicación.

Las capacidades de política global dentro de la conectividad de red impulsada por IA y centrada en la seguridad ayudan a las organizaciones a ampliar su alcance, con políticas de alto nivel definidas y aplicadas en función de la identidad y los roles. Los roles abarcan toda la empresa, lo que elimina el laborioso mantenimiento de los controles de acceso para cada dispositivo de la organización. Las políticas expresadas en términos de intención empresarial simplifican los flujos de trabajo de las políticas al abstraerlas de la complejidad y los cambios de la red física subyacente, de modo que tanto los equipos de red como los de seguridad pueden gestionar por intención.

Ventajas de la política global

- Define la política una vez y aplícala en todas partes, eliminando el laborioso mantenimiento de los controles de acceso y las incoherencias que aumentan el riesgo.
- Supervisa y aplica de forma continua y sin brechas las políticas relativas a usuarios, dispositivos, datos y aplicaciones, independientemente de dónde se encuentren o a qué estén conectados.
- Proporciona a los equipos de red y seguridad una «caja de herramientas compartida» para optimizar el rendimiento de la red y aplicar políticas de seguridad granulares.

Soluciones de HPE Aruba Networking

HPE Aruba Networking ClearPass autentica usuarios y dispositivos a partir de una amplia variedad de fuentes de identidad, como Active Directory. Mediante un rico motor de políticas que permite privilegios de acceso precisos, ClearPass controla qué usuarios y qué dispositivos pueden acceder a qué recursos. Las políticas siguen al usuario y al dispositivo sin fisuras a través de redes cableadas, inalámbricas y de área extensa, incluso en entornos de varios proveedores.

Para las redes gestionadas por HPE Aruba Networking Central, la solución control de acceso a la red (NAC) nativa de la nube Cloud Auth permite la incorporación sin fricciones de usuarios finales y dispositivos cliente, ya sea mediante autenticación basada en la dirección MAC o mediante integraciones con almacenes de identidad en la nube comunes para asignar automáticamente el nivel adecuado de acceso a la red.

Para los usuarios híbridos y remotos, así como para terceros como contratistas y trabajadores temporales, el acceso a la red de confianza cero (ZTNA) HPE Aruba Networking SSE limita el acceso, a través de un agente de confianza, solo a aplicaciones específicas o microsegmentos que han sido aprobados para el usuario, tal como se define a través de una única interfaz de política global. La supervisión continua garantiza que las políticas se adapten automáticamente basándose en cambios de identidad, ubicación y estado del dispositivo, un contexto que facilita la garantía de confianza cero en cada acceso.

Aplicación desde el extremo hasta la nube

Aplicación coherente de políticas para usuarios, aplicaciones, datos y dispositivos

Los marcos de seguridad de confianza cero se basan en la aplicación de políticas para aplicar la confianza y garantizar que los usuarios y dispositivos tengan acceso solo a los recursos que necesitan, siempre que no sean sospechosos de participar en un ataque.

Con la conectividad de red impulsada por IA y centrada en la seguridad de HPE Aruba Networking, las organizaciones pueden implementar la aplicación de confianza cero basada en roles en todos los puntos de control. La conectividad de red impulsada por IA y centrada en la seguridad aplica políticas basadas en roles para todos los usuarios, dispositivos, datos y aplicaciones, sin importar dónde o cómo se conectan o a qué se conectan. La aplicación de políticas en línea dentro de la infraestructura de conmutación evita que el tráfico se desvíe para aplicar las políticas de seguridad, mejorando el rendimiento y la experiencia del usuario y consumiendo menos recursos en el proceso, sin comprometer el acceso ni la protección.

Ventajas de la aplicación desde el extremo hasta la nube

- Aplicar las políticas en todo lugar, como puntos finales, puntos de acceso, conmutadores de acceso, puerta de enlace de SD-WAN, conmutador TOR del centro de datos, en el campus y a través de la nube
- Respaldar la cooperación y colaboración de los equipos de red y seguridad, ya que las políticas ayudan a ofrecer un rendimiento óptimo de la red al tiempo que protegen a la organización
- Reducir la cantidad de soluciones de seguridad externas necesarias a fin de aplicar los controles de acceso requeridos para los marcos de cumplimiento y confianza cero, así como la complejidad asociada

Soluciones de HPE Aruba Networking

La segmentación dinámica de HPE Aruba Networking separa el tráfico de la red en función de la identidad y los permisos de acceso asociados, aplicando el acceso de confianza cero con privilegios mínimos a las aplicaciones y los datos del extremo a la nube. La segmentación dinámica admite múltiples modelos de aplicación —centralizada y distribuida—, lo que permite al departamento de TI utilizar uno o ambos modelos en función de las necesidades del entorno. La aplicación centralizada la proporciona Policy Enforcement Firewall, un cortafuegos de aplicación completa integrado en la infraestructura de red de HPE Aruba Networking. La aplicación distribuida en línea dentro de la infraestructura de puerta de enlace y conmutación la proporciona HPE Aruba Networking Central NetConductor, una solución de pila completa que utiliza tecnología ampliamente adoptada, como EVPN/VXLAN, para producir una superposición de red inteligente adecuada para la rápida implementación de redes empresariales y la escalabilidad masiva para la automatización de redes y seguridad.

Las organizaciones también pueden usar HPE Aruba Networking EdgeConnect SD-WAN para aplicar políticas de seguridad uniformes que abarquen la WAN y la LAN con capacidades globales de cortafuegos de próxima generación (NGFW) integradas, como IDS/IPS, protección ante ataques DDoS y microsegmentación en toda la empresa. Los servicios de NGFW integrados permiten a las organizaciones consolidar la red de sucursales y las funciones de seguridad eliminando los cortafuegos y enrutadores heredados en las sucursales.

Dentro del centro de datos, HPE Aruba Networking Fabric Composer facilita la implementación de la seguridad de confianza cero simplificando y automatizando el proceso de microsegmentación con una interfaz de usuario interactiva y fácil de usar. El conmutador HPE Aruba Networking CX 10000 ofrece microsegmentación distribuida, cortafuegos este-oeste, cifrado y servicios de telemetría en línea, a través de cada puerto, más cerca de las aplicaciones empresariales críticas, eliminando la necesidad de cortafuegos adicionales.

«Las empresas líderes adoptarán arquitecturas de confianza cero, en las que el trabajo de la red no se define en términos de conectar algo a algo, sino más bien como una capa de aplicación de la política de seguridad. Para los usuarios que acceden a aplicaciones, la política de seguridad puede aplicarse en la nube, pero para muchos flujos de tráfico (en particular para los dispositivos IoT y sus servicios asociados), será más eficiente aplicar automáticamente la política de seguridad en dispositivos de acceso como puntos de acceso, conmutadores y enrutadores».

– David Hughes, director de Producto y Tecnología, HPE Aruba Networking, Hewlett Packard Enterprise[IX]

¿Qué es la IA para redes?
La inteligencia artificial (IA) para redes es un nuevo término introducido con el fin abordar de manera específica cómo la inteligencia artificial para las operaciones de TI (AIOps) se aplica a los entornos de wifi, conmutación y WAN.

Operaciones automatizadas con inteligencia artificial

Gestionar y proteger a escala

El panorama empresarial actual es más complejo y difícil que nunca.
En estos días, mantener y proteger una red de confianza cero requiere visibilidad y automatización a tiempo completo. La inteligencia artificial promete multiplicar el potencial humano, por lo tanto, las organizaciones pueden mitigar el riesgo a escala a fin de mejorar la seguridad y liberar a los equipos para que puedan crear ventajas empresariales.

La conectividad de red impulsada por IA y centrada en la seguridad les da a los equipos el poder del aprendizaje automático combinado con una telemetría completa centrada en la red y en el usuario que captura datos de cada usuario, dispositivo y red. Los equipos de seguridad pueden usar estos datos para respaldar la implementación de la seguridad de confianza cero y la supervisión continua a fin de impedir y contener los ataques. Los equipos de redes se benefician con la capacidad de automatizar las tareas mundanas de incorporación, aprovisionamiento y organización de políticas.

Las ventajas de las operaciones automatizadas por IA

- Automatizar la gestión de redes y las tareas de operaciones de seguridad con el fin de reducir el esfuerzo manual necesario para proteger y gestionar la red.
- Mejorar la visibilidad y el control de los usuarios y dispositivos en la red y detectar anomalías para mejorar la detección y prevención de ataques.
- Mejorar la supervisión y el diagnóstico para ofrecer información relevante y práctica que los equipos de red y seguridad puedan utilizar.

Operaciones automatizadas por inteligencia artificial de HPE Aruba Networking

HPE Aruba Networking Central es una consola de gestión de redes y seguridad nativa de la nube para toda la infraestructura de HPE Aruba Networking. Como único punto de visibilidad y control para Aruba ESP (Edge Services Platform), Central ofrece AIOps, automatización de flujos de trabajo y funciones de seguridad avanzadas para unificar operaciones en campus, sucursales, centros de datos y entornos de trabajo remotos.

Central aprovecha la inteligencia artificial y los análisis avanzados para automatizar las actividades comunes de gestión y operaciones de redes y seguridad, con una supervisión inteligente 24x7 de redes, aplicaciones y dispositivos que forman parte del lago de datos. Estas funciones se basan en modelos de aprendizaje automático que se entrenan constantemente con datos de rendimiento de red de una base de clientes variada y global de HPE Aruba Networking. Las capacidades impulsadas por IA de Central incluyen lo siguiente:

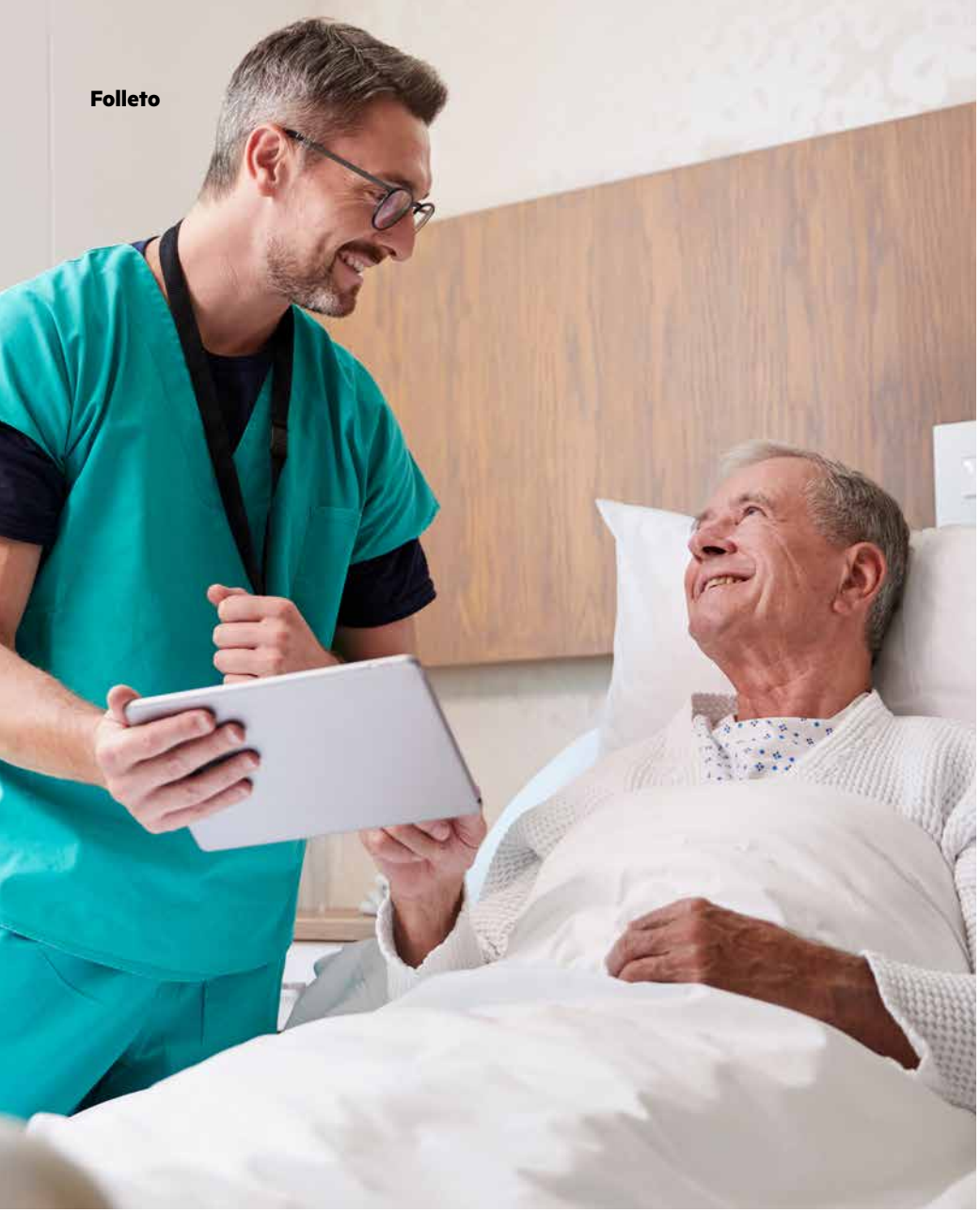
- Detección y diagnóstico automáticos de problemas mediante líneas de base dinámicas, con detección de anomalías integrada para la identificación precisa del problema, la causa raíz y la corrección con una precisión cercana al 95 %.[X]
- Los modelos de aprendizaje automático combinados con inspección profunda de paquetes para identificar y perfilar con precisión a los clientes a través de infraestructuras cableadas e inalámbricas sin colectores físicos ni agentes.
- Recomendaciones de firmware para eliminar la sobrecarga que supone el seguimiento manual de las actualizaciones de firmware y reducir el riesgo de incumplimiento debido a vulnerabilidades de seguridad.

El lago de datos más grande del sector es el motor de las capacidades impulsadas por IA de HPE Aruba Networking Central

2,7
Millones de dispositivos

200
Millones de clientes

+30
Sectores específicos



Bethesda Health Group

Conectividad de red impulsada por IA y centrada en la seguridad en el trabajo

Historia de cliente

Al ofrecer comunidades de jubilados vibrantes y diversas que reflejan de forma única los barrios del Gran St. Louis, así como atención domiciliaria altamente personalizada, Bethesda Health Group se ha forjado una reputación nacional como recurso de confianza para las personas mayores y sus familias durante 135 años. Los 1100 empleados de la organización prestan una atención individualizada, de calidad, innovadora y compasiva en 16 centros.

Para apoyar a sus trabajadores y residentes, cada vez más móviles y conocedores de la tecnología, Bethesda transformó sus operaciones para adoptar una estrategia con un enfoque cloud-first. Aprovecha la conectividad de alto rendimiento para prestar servicios, proporcionar acceso a una serie de aplicaciones y permitir a los residentes mantenerse en contacto con sus equipos asistenciales, familiares y amigos. Con esta transformación llegó también la necesidad de mejorar la ciberseguridad, así como la necesidad de adoptar la confianza cero.

Ya asociado con HPE Aruba Networking para conectividad cableada, inalámbrica y SD-WAN (WAN definida por software), Bethesda decidió optimizar su infraestructura mediante la adopción de la plataforma Secure Access Service Edge (SASE) totalmente en la nube y HPE Aruba Networking Security Service Edge (SSE). Consolida múltiples capacidades de acceso seguro en un único servicio de nube fácil de usar que adapta automáticamente las políticas en función de los cambios en el contexto del usuario, el dispositivo y la aplicación.

Tras desplegar SD-WAN, Bethesda buscaba mejorar la seguridad de acceso y satisfacer los requisitos de auditoría. HPE Aruba Networking ClearPass le permitió a Bethesda modernizar su control de acceso con una solución granular basada en políticas para redes cableadas e inalámbricas, y su escaso personal informático lo encontró intuitivo y fácil de usar.

Bethesda también agradece a HPE Aruba Networking Central el suministro de gestión en la nube basada en inteligencia artificial para unificar aún más su infraestructura cableada e inalámbrica.

«Hemos conseguido una infraestructura de red completa y segura que nos permite gestionar una gran huella cableada, Wi-Fi y SD-WAN con un personal de TI reducido, sin quebrar la banca».

– Michael Keller, director de Informática, Bethesda Health Group[XII]

Leer **la historia completa**

Implementación de la seguridad de confianza cero

Adoptar un modelo de seguridad de confianza cero es un proceso. ¿No sabes por dónde empezar? Considera esta lista de control de capacidades para ayudar a priorizar los próximos pasos:

- ✓ ¿Tienes visibilidad de todos los dispositivos de tu red, aunque no los gestiones?
- ✓ ¿Dispones de métodos coherentes para asignar privilegios a usuarios y dispositivos?
- ✓ ¿Estás aplicando normas de cumplimiento de la seguridad antes de permitir la entrada de un dispositivo en la red?
- ✓ ¿Estás aplicando políticas de seguridad de acceso basadas en funciones de forma coherente en toda la red?
- ✓ ¿Puedes supervisar continuamente el estado de seguridad de un sujeto utilizando todos los datos disponibles?

Para obtener más información sobre la conectividad de red impulsada por IA y centrada en la seguridad de HPE Aruba Networking, visita

arubanetworks.com/products/security/

[I] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Arquitectura de confianza cero. Publicación especial de NIST 800-207. Instituto Nacional de Normas y Tecnología Agosto de 2020.

[II] El dilema de la innovación frente al riesgo. Hewlett Packard Enterprise. 2023.

[III] Estudio global sobre cómo cerrar la brecha de seguridad informática 2023: Solucionar brechas de ciberseguridad del extremo a la nube. Ponemon Institute. Marzo de 2023.

[IV] Estudio global sobre cómo cerrar la brecha de seguridad informática 2023: Solucionar brechas de ciberseguridad del extremo a la nube. Ponemon Institute. Marzo de 2023.

[V] ¿Cuál es el estado de la seguridad de confianza cero? HPE Aruba Networking. Abril de 2023.

[VI] Estudio global sobre cómo cerrar la brecha de seguridad informática 2023: Solucionar brechas de ciberseguridad del extremo a la nube. Ponemon Institute. Marzo de 2023.

[VII] Estudio global sobre cómo cerrar la brecha de seguridad informática 2023: Solucionar brechas de ciberseguridad del extremo a la nube. Ponemon Institute. Marzo de 2023.

[VIII] Infraestructura de red impulsada por IA: La respuesta para la eficiencia de la TI. 2022.

[IX] Hughes, D. Cinco tendencias principales en redes y seguridad para 2024. Enero de 2024.

[X] Redes gestionadas en la nube e impulsadas por IA para redes de sucursales, campus, remotas y centros de datos HPE Aruba Networking Central. 2023.

[XI] Redes gestionadas en la nube e impulsadas por IA para redes de sucursales, campus, remotas y centros de datos HPE Aruba Networking Central. 2023.

[XII] Bethesda Health Group. 2024. https://www.arubanetworks.com/resources/case-studies/bethesda-health-group/

Toma la decisión de compra correcta. Contacta con nuestros especialistas en preventa.

Contáctanos

Visita **ArubaNetworks.com**

Hewlett Packard Enterprise

© Copyright 2024 Hewlett Packard Enterprise Development LP. La información incluida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo aquí indicado debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de las omisiones o errores técnicos o editoriales que puedan existir en este documento.

Todas las marcas de terceros pertenecen a sus respectivos titulares.

BR_EasingZeroTrustSecurityadoption_DT_020124 a00137590ese