



HPE aruba
networking

Visibilidad e información para las redes actuales impulsadas por el IoT

Un enfoque impulsado por IA para proteger los puntos
de conexión de la red con Client Insights

HPE 
GreenLake

A medida que la amplitud y complejidad de los clientes de puntos de conexión en la red siguen creciendo a un ritmo asombroso, muchas organizaciones se esfuerzan por hacer frente a una superficie de ataque en expansión. Con la creciente ubicuidad del Internet de las cosas (IoT) y los nuevos casos de uso generados por las iniciativas de transformación digital, la adopción del IoT ha superado las mejores prácticas críticas de seguridad y cumplimiento en favor de mejores eficiencias operativas y resultados empresariales.

Con este cambio, los equipos de TI y seguridad a menudo desconocen cuándo, dónde y qué tipos de nuevos clientes se conectan a la red. Esta falta de visibilidad les impide aplicar a tiempo medidas de seguridad y cumplimiento. Las mejores prácticas requerirían que cada nuevo cliente sea identificado con precisión, incorporado y asignado a una política, pero a menudo el departamento de TI se ve sorprendido con la guardia baja.

Puntos ciegos en los enfoques actuales

El conjunto de herramientas de visibilidad de red existente se ha centrado en un conjunto bastante reducido de clientes que se identifican fácilmente mediante técnicas básicas de detección y creación de perfiles. Esto incluye la búsqueda de cosas como teléfonos inteligentes populares y ordenadores portátiles con sistemas operativos móviles o de sobremesa comunes. Identificar un teléfono inteligente con Android™ desde un ordenador portátil con Windows ha sido habitual utilizando estas técnicas.

Identificar clientes como dispositivos IoT es particularmente difícil por varias razones, algunas de las cuales incluyen:

- Muchos dispositivos IoT son fabricados por proveedores emergentes y no se pueden comunicar mediante técnicas estándar de detección y creación de perfiles, lo que dificulta la creación de perfiles precisos.
- También es común ver dispositivos IoT contruidos con hardware y software genéricos, como una Raspberry Pi, que cumple diferentes funciones, lo que también dificulta su descifrado.
- Debido a una elaboración de perfiles parcial o imprecisa, los clientes suelen identificarse como clientes Windows o Linux® genéricos y este hecho hace que resulte difícil aplicar políticas precisas.
- La mayoría de las soluciones de visibilidad de red requieren recopiladores o agentes, cuya implementación no siempre resulta factible en ubicaciones a escala.

La importancia del contexto

Con este cambio, se necesita un enfoque de espectro completo para la visibilidad en toda la infraestructura cableada e inalámbrica que no requiera el uso de agentes o el inicio de sesión en los clientes para ver lo que son. Esto significa comprender el comportamiento real de un dispositivo -qué protocolos se utilizan, a qué aplicaciones y URL se accede- y, en definitiva, qué función cumple un cliente en la red. En el caso de muchos de los dispositivos IoT, como los que se pueden encontrar en un hospital o en una fábrica, este contexto enriquecido es la única manera de identificarlos con precisión.

La solución SASE de HPE Aruba Networking: Información sobre clientes impulsada por IA

La solución de gestión de red de HPE Aruba Networking, la nube de HPE Aruba Networking Central, ahora incluye Client Insights impulsada por IA, que ofrece uno de los perfilados y visibilidades más granulares del sector. Client Insights aprovecha la telemetría nativa de la infraestructura procedente de puntos de acceso, conmutadores y puertas de enlace, así como de clientes, sin necesidad de instalar colectores físicos o agentes. Los modelos de clasificación basados en aprendizaje automático se utilizan para crear huellas, identificar y elaborar perfiles precisos de una amplia variedad de clientes en toda la infraestructura con cable e inalámbrica.

La figura 1 muestra cómo Client Insights utiliza aprendizaje automático y crowdsourcing para identificar tipos de clientes.



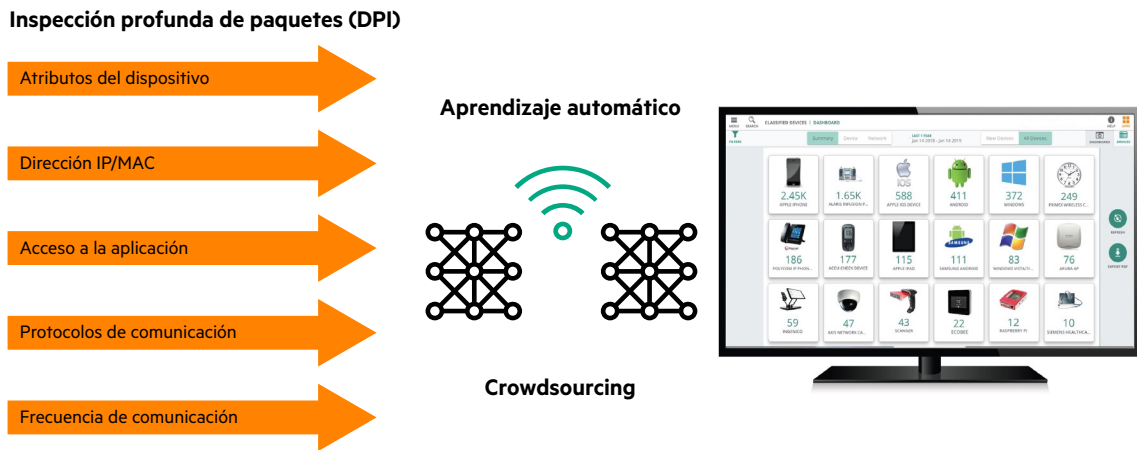


Figura 1. Client Insights utiliza aprendizaje automático avanzado y crowdsourcing para identificar con precisión cualquier tipo de cliente.

Estas capacidades se mejoran aún más con la inspección profunda de paquetes (DPI), que proporciona información adicional sobre el contexto y el comportamiento que ayuda a identificar con precisión esos dispositivos IoT difíciles de detectar. Al aprovechar DPI, Client Insights puede utilizar un conjunto más amplio de atributos del dispositivo para una identificación más precisa. Se analizan los atributos del cliente, que incluyen patrones de comunicación y comportamiento, para crear dinámicamente clústeres de dispositivos similares.

Se utilizan modelos de aprendizaje automático para aprender y actualizar estos atributos constantemente con el fin de actualizar de forma dinámica las huellas digitales y proporcionar recomendaciones de clasificación. La tecnología de crowdsourcing controlado se utiliza para validar las huellas dactilares en varios sitios de clientes antes de añadirlas a la base de datos de clasificación de HPE Aruba Networking. Esto aumenta la precisión y la exhaustividad del motor de clasificación.

La figura 2 muestra cómo Client Insights utiliza la telemetría de los dispositivos de la infraestructura de HPE Aruba Networking para identificar clientes.

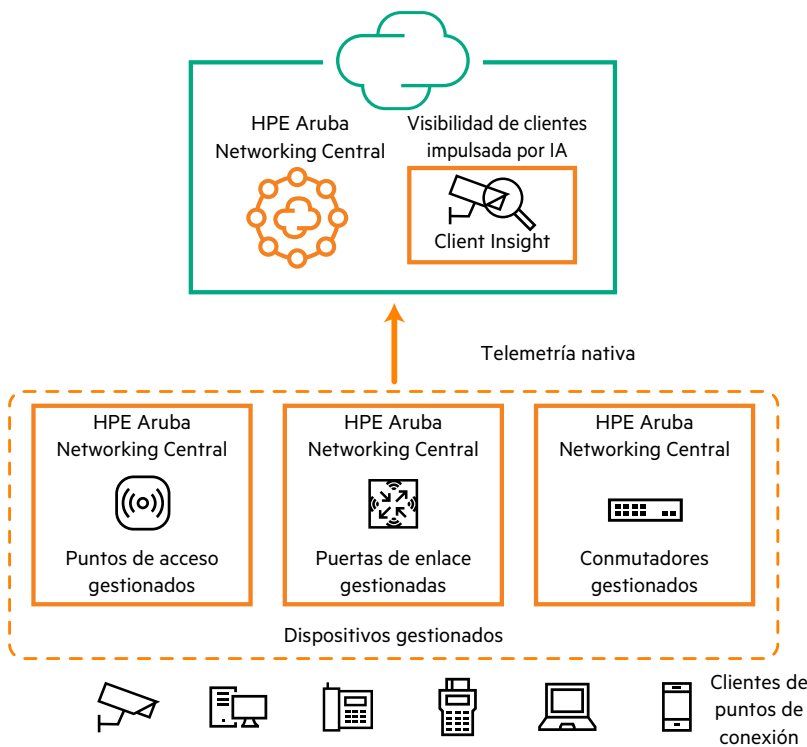


Figura 2. La telemetría nativa de la infraestructura de HPE Aruba Networking se utiliza para identificar con precisión a los clientes conectados mediante una clasificación basada en aprendizaje automático.



La figura 3 muestra el panel de Client Insights con diferentes dispositivos enumerados en diferentes categorías.

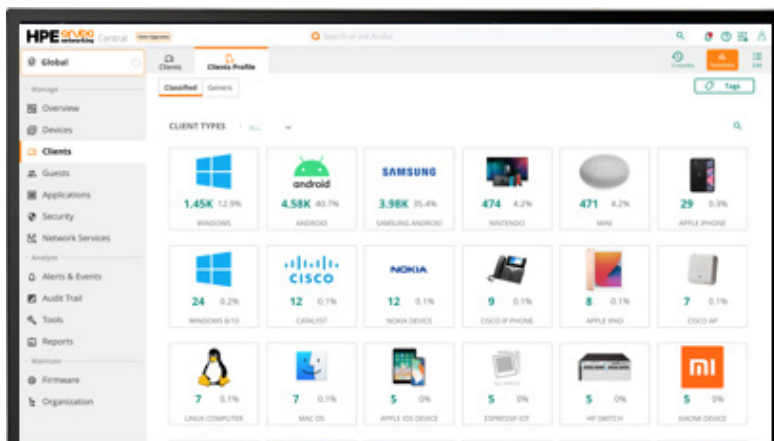


Figura 3. El panel de Client Insights de la nube de HPE Aruba Networking Central muestra todos los dispositivos conectados por categorías.

Para los dispositivos que antes se consideraban genéricos, se utilizan modelos sofisticados de aprendizaje automático para analizar atributos y agrupar clientes similares. A medida que los clientes se agrupan, se pueden etiquetar fácilmente según atributos clave. Una vez etiquetados, los nuevos clientes que se conectan a la red se agregan automáticamente a su clúster específico y se etiquetan en consecuencia.

Para entornos que actualmente no están gestionados por la nube de HPE Aruba Networking Central o para entornos con dispositivos de red de terceros, se puede aprovechar HPE Aruba Networking ClearPass Device Insight para la identificación basada en aprendizaje automático y la creación de perfiles de clientes. HPE Aruba Networking ClearPass Device Insight requiere la instalación de un recopilador físico o virtual y tiene una licencia independiente.

El valor de la aplicación automatizada de políticas

La visibilidad sin un control adecuado puede dejar a las organizaciones expuestas a riesgos de seguridad y cumplimiento. Client Insights permite la supervisión continua de los clientes, que cuando se combina con HPE Aruba Networking ClearPass Policy Manager proporciona un control de acceso de extremo a extremo de bucle cerrado. Esto proporciona visibilidad y una aplicación automatizada de políticas y reduce en gran medida la necesidad de intervención manual en cualquier red cableada o inalámbrica de múltiples proveedores. HPE Aruba Networking ClearPass Device Insight también se integra perfectamente con HPE Aruba Networking ClearPass Policy Manager.

La aplicación automatizada de políticas aborda varios casos de uso diferentes, desde el momento en que los clientes se unen inicialmente a la red, hasta cuando un evento no deseado desencadena la necesidad de eliminar a un cliente por motivos de seguridad o de cumplimiento. Por ejemplo, cuando una cámara de seguridad nueva se conecta por primera vez a la red, puede segmentarse automáticamente como un tipo de cliente desconocido para garantizar que no afecta a infraestructuras o servidores críticos. Si un cliente se ha visto comprometido o actúa de manera sospechosa, puede ponerse en cuarentena total para someterse a pruebas, reparaciones o proceder a su sustitución.

La figura 4 muestra cómo funciona Client Insights con HPE Aruba Networking ClearPass Policy Manager para la segmentación y aplicación automatizadas.



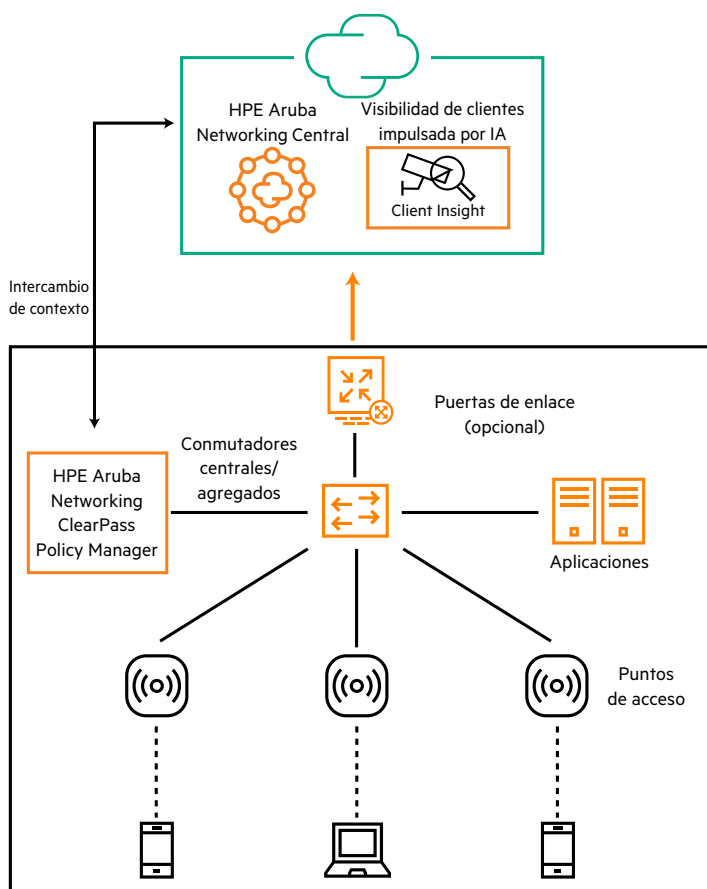


Figura 4. Client Insights se integra con HPE Aruba Networking ClearPass Policy Manager para la segmentación y aplicación automatizadas

La nube de HPE Aruba Networking Central con Client Insights Obtención de beneficios acelerada

La gestión de aplicaciones críticas para la empresa en entornos cada vez más distribuidos genera expectativas de mejora de la disponibilidad, el rendimiento y la seguridad. La nube de HPE Aruba Networking Central ofrece funciones, escalabilidad, gestión y organización modernas que incluyen características avanzadas de IA/aprendizaje automático y seguridad, lo que permite a las organizaciones de TI de todos los tamaños ofrecer experiencias de usuario superiores con una simplicidad sorprendente.

Client Insights aprovecha estas características únicas y la telemetría nativa de la infraestructura de red para reducir el tiempo y el coste de implementación, acelerando la obtención de beneficios. Este enfoque proporciona una detección y supervisión centralizadas e ininterrumpidas de los puntos de conexión de la red a través de implementaciones distribuidas, al tiempo que aumenta tu visibilidad y tu postura de seguridad.





Resumen


Con la adopción acelerada de dispositivos IoT, la cantidad de usuarios en las redes de los clientes continúa creciendo, lo que crea nuevos casos de uso y al mismo tiempo amplía la superficie de ataque. La visibilidad integral es esencial para garantizar que la seguridad y el cumplimiento de las mejores prácticas sigan el ritmo de las eficiencias operativas que conlleva la adopción del IoT.

Identificar y perfilar con precisión a los clientes para aplicar políticas basadas en funciones de alta granularidad y garantizar que cada uno de ellos tenga el nivel adecuado de control de acceso para reducir los niveles generales de riesgo ya no es algo que estaría bien tener, sino una necesidad.

Más información en

HPE.com/es/es/Aruba-Central.html

Visita HPE.com

 **Chat con ventas**