aruba
a Hewlett Packard Enterprise company

ARUBA A SIMPLE VISTA

VISIBILIDAD DE PUNTOS FINALES PARA ENTORNOS CABLEADOS E INALÁMBRICOS

El requisito previo actual para mejorar la seguridad y el cumplimiento

Solía ser muy fácil acercarse a la mesa de un compañero y ver qué tenía conectado a la red, pero eso ya es cosa del pasado. Las políticas de Traiga su propio dispositivo (TSPD) y los dispositivos no gestionados, como las cámaras de vigilancia y otros puntos finales emergentes englobados en el Internet de las cosas (IoT), están consiguiendo que resulte imposible para el departamento de TI mantener una visibilidad completa.

EL DESAFÍO

Para ayudar a identificar los puntos finales conectados, las prácticas heredadas a menudo requerían la implementación de soluciones completas de gestión de puntos finales, agentes, así como la actualización manual de varias bases de datos dedicadas a estos dispositivos. Ninguna de estas opciones entregaba los resultados deseados, puesto que el departamento de TI se veía desbordado por el TSPD, las implementaciones de acceso de invitados y los puntos finales cableados e inalámbricos no autorizados, cuya entrada y salida en muchos casos corría paralela al desplazamiento de los usuarios.

Con los miles de millones de dispositivos IoT que se espera que se conecten a las redes en los próximos tres años, y las infracciones de seguridad debidamente publicitadas que conllevan, existe una fundada demanda entre los profesionales de las TI de obtener visibilidad y funciones de elaboración de informes en tiempo real. Necesitan una solución que ofrezca supervisión y elaboración de perfiles permanentes, en lugar de actualizaciones periódicas, con independencia de la ubicación, la hora y el tipo de punto final.

LA SOLUCIÓN DE VISIBILIDAD INTELIGENTE DE HOY EN DÍA

La familia de productos ClearPass de Aruba ofrece a las organizaciones de redes y seguridad una ventaja única frente a los competidores, ya que la elaboración de informes desasistida en tiempo real puede adquirirse como una aplicación independiente o dentro de una solución de aplicación de políticas completa.

Ambas le permiten identificar continuamente puntos finales y dispositivos en redes cableadas e inalámbricas, con o sin servicios AAA, mediante direcciones IP, tanto dinámicas como estáticas. Las perspectivas completas del panel principal ayudan a ver el número total de puntos finales, y a clasificarlos por categoría, familia y tipo de dispositivo.

VENTAJAS DE ARUBA CLEARPASS

- Detección y categorización automática de puntos finales para fines de seguridad y demandas de auditorías
- Supervisión continua de todos los dispositivos, incluidos los que vienen y van
- La visibilidad desasistida le permite encontrar dispositivos como smartphones de TSPD e IoT
- Uso compartido de atributos contextuales que extiende la visibilidad a una amplia variedad de soluciones de seguridad y servicios de TI
- Eliminación del trabajo que requiere el mantenimiento manual de bases de datos actualizadas
- Mejora del rendimiento y la seguridad de la red al ofrecer comprensión sobre el número, tipo y atributos de los puntos finales presentes

Aruba ClearPass Universal Profiler: una aplicación virtual independiente que puede implementarse y ponerse en funcionamiento en cuestión de minutos. Se ha diseñado para organizaciones que no estén preparadas para una solución de control de acceso a la red (NAC) completa, o para áreas remotas o restringidas donde no se haya implementado un NAC. Está disponible para adaptarse a las necesidades de escalabilidad de cualquier organización.

Aruba ClearPass Policy Manager: una aplicación virtual o un dispositivo físico que incluye elaboración de perfiles completos, aplicación de políticas cableadas e inalámbricas con o sin servicios AAA, acceso de invitados, incorporación de TSPD, funcionalidades de evaluación de puntos finales, elaboración de informes, seguridad de terceros integrada e integración de soluciones orientadas a la experiencia de usuario.

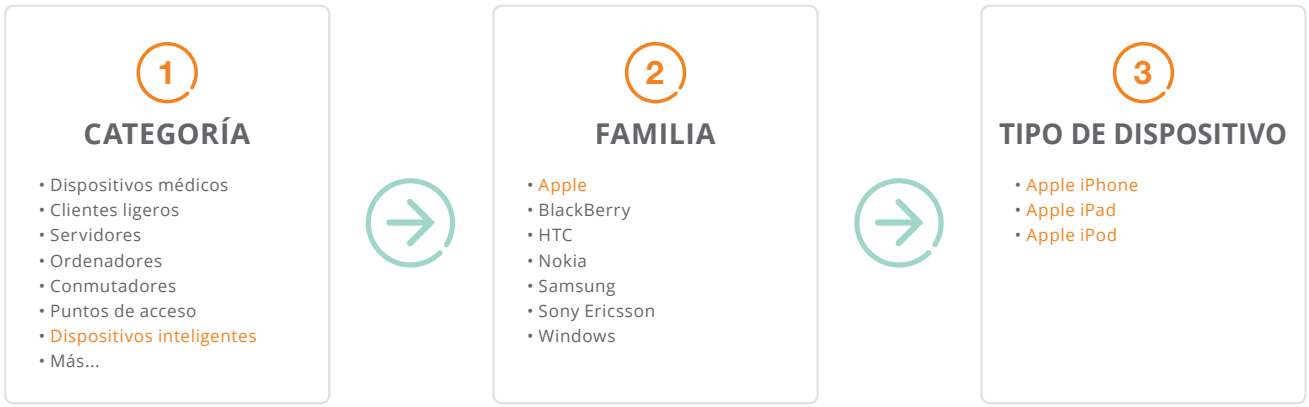

Figura 1: Visibilidad granular por categoría, familia y tipo de dispositivo

La familia ClearPass descubre los puntos finales con una facilidad incomparable, al tiempo que identifica y perfila atributos que determinan su categoría, fabricante, sistema operativo, dirección IP, nombre de host, titular y más. La clasificación de puntos finales automática y personalizable por el departamento de TI garantiza la rápida clasificación de los dispositivos IoT nuevos y desconocidos en las familias de dispositivos que les corresponden. De este modo, se obtiene visibilidad y se facilita la aplicación de políticas de seguridad.

Si se desea flexibilidad adicional, ClearPass proporciona opciones para el descubrimiento dinámico de redes utilizando supervisión de puertos estándar o SPAN. Ello se desmarca de las soluciones de control de acceso a la red (NAC) de las redes de TI heredadas, que pueden requerir que dedique varios costosos puertos 10G a la duplicación en implementaciones de puntos finales de gran envergadura.

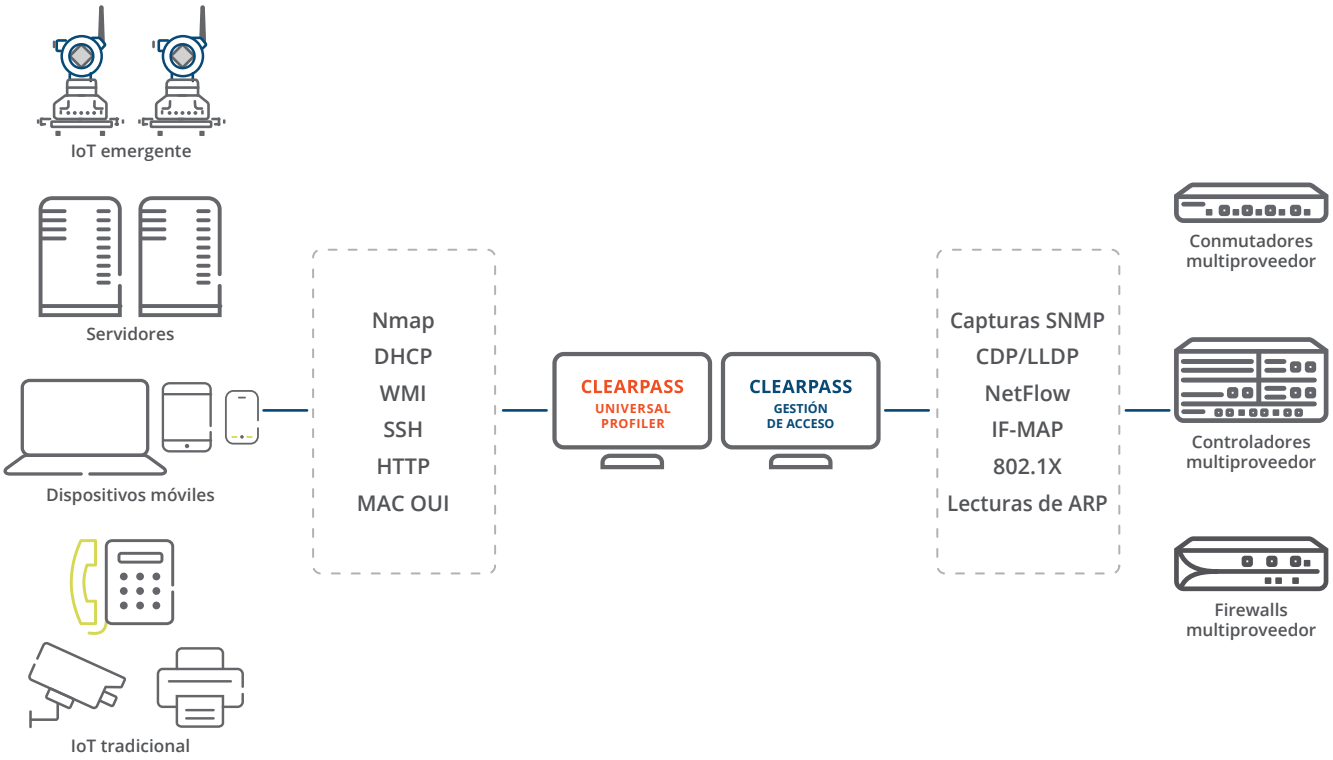

Figura 2: Métodos de identificación granular y elaboración de perfiles

MÉTODOS DE DESCUBRIMIENTO GRANULARES

Varios métodos de elaboración de perfiles ayudan a recopilar atributos granulares de puntos finales por dispositivo que pueden ayudar a identificar posibles problemas de rendimiento y amenazas de seguridad. Este aumento de la visibilidad y del conocimiento contextual puede compartirse por ambas soluciones de ClearPass o utilizarse directamente por ClearPass Policy Manager para ayudar a optimizar las políticas de qué puede conectarse y con qué rapidez puede responder el departamento de TI a las amenazas potenciales.

APROVECHE LA VISIBILIDAD DE LOS PUNTOS FINALES CON SOLUCIONES DE TERCEROS

Las API de ClearPass, la mensajería syslog y la funcionalidad de Extensions facilitan el intercambio de atributos de puntos finales con firewalls, SIEM, paquetes de cumplimiento para puntos finales y otras soluciones para mejorar la gestión de políticas. Estas soluciones pueden ingerir atributos de puntos finales para analizar la coincidencia con patrones de tráfico, en base a sus reglas específicas para cada categoría de dispositivo, así como para optimizar conexiones o resolver problemas con tráfico sospechoso.

MÁS INFORMACIÓN

Para obtener información adicional sobre ClearPass Universal Profiler y ClearPass Policy Manager, así como sobre cómo ofrecen la capacidad exclusiva de identificar todos los puntos finales, ayudar a aplicar políticas y proteger mejor sus redes cableadas e inalámbricas, visite www.arubanetworks.com/clearpass.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com