aruba
a Hewlett Packard Enterprise company

RESUMEN EJECUTIVO

IDENTIFIQUE, CONECTE Y PROTEJA DISPOSITIVOS MÓVILES E IOT EN EL BORDE DE LA RED

INTRODUCCIÓN

El simple número de dispositivos de TI que se conectan a las redes empresariales supone un desafío para el departamento de TI cuando éste pondera las ventajas de los edificios inteligentes frente al riesgo de incorporar grandes cantidades de dispositivos desconocidos en sus entornos, especialmente si no dispone de un conjunto adecuado de herramientas para identificarlos, perfilarlos, autenticarlos y aplicarles políticas.

El anuncio más reciente de Aruba se enfrenta a estos desafíos con un enfoque de 4 pasos para la conectividad de los dispositivos del Internet de las cosas (IoT) en el borde: Identificar qué hay en la red, conectar los dispositivos móviles y del IoT con conmutadores inteligentes, proteger la red con gestión de políticas líder en el sector e innovar con nuestro ecosistema de partners para proporcionar seguridad extremo a extremo.

EL IOT INTRODUCE DESAFÍOS

La explosión del número de dispositivos móviles y el traslado a edificios inteligentes presenta importantes desafíos para los departamentos de TI y los directores de las empresas.

Falta de visibilidad: ¿Realmente sabe qué hay en su red?

La seguridad empieza comprendiendo qué hay en la red: smartphones no gestionados, puntos finales no autorizados, dispositivos IoT. Todos aumentan la superficie de ataque y amenazan la seguridad de la empresa. La capacidad de ver qué hay en la red permite al departamento de TI comprender mejor qué está utilizando su red, y cómo. El departamento de TI debe ser capaz de identificar y elaborar un perfil de cada dispositivo que se conecta a la red, con independencia de su procedencia. Esto se complica a medida que nuestras redes se ven inundadas por dispositivos IoT inalámbricos y cableados desconocidos. Es necesario elaborar un perfil de todos los dispositivos y evaluarlos en el momento de la conexión, asignarles una categoría y concederles o denegarles el acceso en función del tipo de dispositivo, el tipo de titularidad o el sistema operativo.

El entorno cableado es la nueva preocupación.

Para organizaciones del ámbito empresarial e industrial, el número de dispositivos IoT cableados esperado puede ser del 35 % al 50 % o más, en función de la vertical: detectores de movimiento, equipos médicos o controladores de procesos en la fábrica, por mencionar unos pocos. En el pasado, los debates sobre el control de acceso a la red (NAC) se centraban principalmente en cómo proteger la red inalámbrica, porque era sobre ella como se conectaba la mayoría de los dispositivos. Las conexiones seguras por sesión se convirtieron en un requisito, dado que las escuchas inalámbricas y los usuarios desconocidos podían acceder desde cualquier lugar que se encontrara dentro del alcance de un punto de acceso sin un SSID seguro.

La gran atención dirigida a proteger las redes inalámbricas significó que las redes cableadas se dejaron desprotegidas, puesto que los conmutadores se instalaban detrás de puertas cerradas y se creía que no presentaban las mismas vulnerabilidades que el entorno inalámbrico. Lamentablemente, a medida que crecieron las redes cableadas, no se trataron igual todos los conmutadores y se dejaron puertos abiertos, que quedaron accesibles a cualquiera. Los puertos de las salas de conferencias y áreas de impresoras son un ejemplo clásico de cómo se ha aplicado la seguridad de forma aleatoria. Ante la multitud de dispositivos IoT que se conectan ahora por cable, ha llegado la hora de dedicar la misma atención a proteger esta infraestructura.

Las infraestructuras cableadas tradicionales no se optimizaron para el Internet de las cosas (IoT)

En los entornos de conmutación heredados, la plantilla no era móvil y el Internet de las cosas (IoT) no existía siquiera. Los activos residían detrás de un firewall y el departamento de TI tan sólo tenía que asegurarse de la solidez del perímetro. Pero con la aparición del Internet de las cosas (IoT), es necesario que la infraestructura cableada sea tan inteligente como la inalámbrica, y los conmutadores actuales deben disponer de seguridad y gestión de red inteligente integradas para que todos los dispositivos puedan conectarse de forma segura y sin interrupciones.

Proteger la red requiere flujos de trabajo automatizados

Con los miles de dispositivos móviles e IoT desconocidos que se conectan a diario a una red empresarial, resulta imposible asignar y aplicar manualmente políticas a cada uno. Todo el proceso debe automatizarse para reducir el riesgo y la participación directa del departamento de TI. También es necesario elaborar perfiles y comprobar automáticamente los dispositivos estáticos y la propia infraestructura en busca de cambios sospechosos. Si un dispositivo actúa de forma sospechosa, debe ponerse en cuarentena automáticamente hasta que se evalúe la amenaza.

Mantenerse por delante de los piratas es costoso

Parece que se hace pública una infracción masiva de datos prácticamente a diario. La inversión en seguridad requiere grandes cantidades de tiempo y dinero, pero resulta casi imposible mantenerse por delante de los piratas únicamente con la innovación. El ecosistema de partners de Aruba se ha diseñado para reunir a los mejores proveedores de seguridad y ofrecer una solución extremo a extremo.

EL PROYECTO DE ARUBA PARA PROTEGER LA CONECTIVIDAD DE IOT EN EL BORDE

1. Identificar y elaborar perfiles de los dispositivos desconocidos en redes inalámbricas y cableadas de varios proveedores

Puesto que la seguridad de la red empieza por saber qué hay en ella, resulta esencial para las organizaciones poder identificar y elaborar perfiles de todos los dispositivos. La familia de productos ClearPass de Aruba ofrece una ventaja única frente a los competidores, ya que la elaboración de informes desasistida en tiempo real puede adquirirse como una aplicación independiente o como parte de una solución de aplicación de políticas completa.

Ambas soluciones 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.

La nueva Aruba ClearPass Universal Profiler es 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, así como para áreas remotas o restringidas donde no se haya implementado un NAC. Universal Profiler es una forma simple y rentable de identificar y elaborar informes sobre lo que hay en la red.

Aruba ClearPass Policy Manager es 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.

2. Conecte dispositivos IoT con inteligencia automatizada

El traslado a edificios inteligentes significa que las empresas de hoy en día necesitan que la infraestructura cableada también sea más inteligente. Las últimas mejoras en ArubaOS-Switch se han diseñado para alimentar y proteger el borde inteligente, además de optimizarlo para dispositivos móviles e IoT. Estas mejoras permiten un acceso unificado a redes cableadas e inalámbricas basado en roles, que permite identificar y asignar roles a dispositivos IoT conectados y priorizar de este modo las aplicaciones críticas para la empresa, además de proteger la red.

Los conmutadores de capa 3 de Aruba también son capaces de tunelizar tráfico cableado basado en usuarios o puertos a un Mobility Controller, con el fin de aplicar políticas, extender servicios avanzados y cifrar el tráfico para proteger la LAN. Para poder responder a la demanda de rápido crecimiento de los dispositivos IoT y conectados en empresas distribuidas, los rentables conmutadores Aruba 2540 (y otros de este mismo proveedor) admiten aprovisionamiento sin intervención y gestión basada en la nube opcional, a fin de permitir a las empresas simplificar y reducir los costes de implementación y gestión de red.

3. Proteja la red con políticas inteligentes

Una vez que dispone de visibilidad sobre los dispositivos, entra en juego la aplicación de políticas automática. Aruba ClearPass Policy Manager puede ayudarle a ver qué hay en su red, así como a aplicar políticas y flujos de trabajo automatizados a través de infraestructuras cableadas e inalámbricas de varios proveedores. ClearPass entrega definición de perfiles, aplicación de políticas, acceso de invitados, incorporación TSPD y más para poder descargar al departamento de TI de tareas, mejorar la protección ante amenazas y ofrecer una experiencia de usuario sin interrupciones. Y con la nueva filosofía dedicada a proteger la infraestructura cableada, la característica OnConnect aprovecha los protocolos de conmutador existentes, lo que le ayuda a bloquear puertos cableados en lugares vulnerables, como salas de conferencias, teléfonos IP y áreas de impresoras.

4. Acelere la innovación para mejorar la seguridad en el borde

El ecosistema tecnológico de Aruba incluye soluciones de seguridad líderes en el sector que se integran con ClearPass Exchange para garantizar una seguridad extremo a extremo y de borde a núcleo. Nuestras últimas alianzas se centran en la seguridad del Internet de las cosas (IoT):

- Niara utiliza patrones de tráfico conocidos y asociados con los tipos de dispositivos para identificar comportamientos sospechosos. A continuación, pide a ClearPass que retire el dispositivo de la red.
- Attivo permite al departamento de TI crear dispositivos IoT "falsos virtuales", con los que se intentan realizar ataques a la red. Cuando se detecta que el dispositivo virtual está realizando comportamientos no deseados, se pide a ClearPass que elimine los dispositivos de la red.

CONCLUSIÓN

A medida que las organizaciones introducen cada vez más el Internet de las cosas (IoT) en las operaciones convencionales, la incorporación y gestión de dispositivos IoT se vuelve crítica para el éxito. Las empresas necesitan una estrategia para conectar con seguridad los dispositivos móviles e IoT en el borde y extraer el valor y las eficacias asociadas con los edificios inteligentes, al tiempo que mantienen seguros los activos corporativos y la red. El enfoque de 4 pasos de Aruba con respecto a la conectividad de IoT se enfrenta a los desafíos de identificar qué hay en la red, conectar los dispositivos a través de infraestructuras cableadas e inalámbricas inteligentes, proteger la red con una gestión de políticas automatizada y utilizar nuestro ecosistema de partners tanto para mejorar la seguridad extremo a extremo como para estar siempre por delante de los riesgos potenciales.

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com

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