aruba
a Hewlett Packard Enterprise company

DESCRIPCIÓN DE LA SOLUCIÓN

ARUBA CLEARPASS POLICY MANAGER

Acceda a visibilidad y seguridad para entornos cableados e inalámbricos

¿Recuerda cuando el departamento de TI actuaba como un guardián e imponía una combinación de políticas estrictas en un ecosistema totalmente contenido? Esos días quedaron atrás hace ya mucho tiempo. Hoy en día, tanto los dispositivos de TI como los que son propiedad de los usuarios están conectados dentro y fuera de la seguridad del perímetro.

Los equipos portátiles, smartphones, tablets y dispositivos del Internet de las cosas (IoT) están inundando el lugar de trabajo. Identificar qué hay en la red es el primer paso para proteger sus datos. La aplicación de políticas automatizada garantiza que solamente puedan conectarse los usuarios y dispositivos deseados. Además, se requiere protección ante amenazas en tiempo real para satisfacer los requisitos internos y externos de auditoría y cumplimiento.

Y si las expectativas van bien encaminadas, el uso de dispositivos IoT en redes cableadas e inalámbricas está atrayendo la atención del departamento de TI. En el pasado, la mayoría de las organizaciones protegieron sus redes y dispositivos digitales, pero descuidaron los puertos cableados ubicados en las salas de conferencias, detrás de los teléfonos IP y en las áreas de impresoras. Y dado que los dispositivos del IoT pueden carecer de atributos de seguridad y requerir que se acceda a ellos desde recursos de administración externos, el acceso cableado se ha convertido en el nuevo riesgo.

Mientras el departamento de TI lucha por mantener el control, necesita el conjunto adecuado de herramientas para poder programar rápidamente la infraestructura subyacente bajo demanda y controlar el acceso a la red de cualquier dispositivo de IoT y móvil, tanto conocido como desconocido.

La solución de seguridad de acceso de hoy en día debe incluir definición de perfiles, aplicación de políticas, acceso de invitados, incorporación BYOD y más para poder liberar al departamento de TI, fortalecer la protección frente a amenazas y mejorar la experiencia de usuario.

LA MOVILIDAD Y EL IoT ESTÁN CAMBIANDO NUESTRA FORMA DE ENTENDER EL CONTROL DE ACCESO A LA RED

Los límites de los dominios del departamento de TI se extienden más allá de las cuatro paredes de la empresa. Y el objetivo de las organizaciones consiste en proporcionar conectividad en cualquier momento y lugar, sin sacrificar la seguridad. ¿Cómo mantiene el departamento de TI la visibilidad y el control sin afectar a la empresa y la experiencia de usuario? Todo comienza con un plan de 3 pasos.

1. **Identifica** qué dispositivos se están utilizando, su número, de dónde vienen y qué sistemas operativos son compatibles. Esta información proporciona la base sobre la que trabajar. Asimismo, el conocimiento continuo, tanto de los cambios como de los dispositivos que entran y salen, le ofrece la visibilidad que necesita a largo plazo.
2. **Aplicar** políticas precisas que proporcionen un acceso de usuarios y dispositivos adecuado, con independencia del usuario, el tipo de dispositivo o la ubicación. Esto permite obtener una experiencia de usuario previsible. Las organizaciones deben adaptarse a la evolución de los dispositivos actuales y su uso, ya sean smartphones o cámaras de vigilancia.

3. **Proteger** los recursos mediante controles de políticas dinámicos y una solución de amenazas reales que se extienda a sistemas de terceros. Ésta es la última pieza del rompecabezas. Estar preparado para un comportamiento inusual de la red a las 3 de la madrugada requiere un enfoque unificado que bloquee el tráfico y cambie el estado de la conexión de un dispositivo.

Las organizaciones deben elaborar planes para responder a desafíos tanto existentes como imprevistos. No resulta realista confiar en que el departamento de TI y el personal de asistencia intervengan manualmente cada vez que un usuario decida trabajar remotamente o comprar un nuevo smartphone. El control de acceso a la red (NAC) ya no sirve únicamente para realizar evaluaciones de dispositivos conocidos antes de que accedan.

UNA UBICACIÓN PARA VER Y GESTIONARLO TODO

La solución de políticas y servicios AAA (autenticación, autorización y contabilización) de ClearPass, proporciona definición de perfiles de dispositivos integrada, una interfaz administrativa basada en web y una elaboración de informes completa con alertas en tiempo real. Todos los datos contextuales recopilados se aprovechan para garantizar que los usuarios y dispositivos reciben los privilegios de acceso que les corresponden, con independencia del método de acceso o la titularidad del dispositivo.

El motor de definición de perfiles integrado recopila datos en tiempo real que incluyen las categorías de los dispositivos, los proveedores, las versiones de los sistemas operativos y más. Ya no es necesario adivinar cuántos dispositivos están conectados a las redes cableada e inalámbrica. La visibilidad granular proporciona los datos necesarios para pasar las auditorías y determinar de dónde podrían provenir los riesgos para el rendimiento y al seguridad.

El ClearPass Universal Profiler autónomo proporciona la misma visibilidad de definición de perfiles para aquellas organizaciones que no estén preparadas para una aplicación completa de políticas. También puede resultar de utilidad en áreas remotas donde podría no implementarse inicialmente ClearPass.

Una aplicación de políticas basada en plantillas permite al departamento de TI construir políticas orientadas a las redes cableadas e inalámbricas y aprovechar los roles de usuario, tipos de dispositivo, datos MDM/EMM, el estado de los certificados, la ubicación, el día de la semana y más. Las políticas pueden aplicar fácilmente reglas para empleados, alumnos, médicos, invitados, ejecutivos, así como para cada tipo de dispositivo que lleven consigo.

ClearPass OnConnect es una característica integrada que permite a las organizaciones bloquear esos miles de puertos cableados que no utilizan servicios AAA. No se necesita ningún tipo de configuración de dispositivos y basta con introducir una línea de comandos en el conmutador. También se admiten los métodos AAA/802.1X estándares para contextos cableados e inalámbricos.

Ello permite una aplicación de políticas homogénea y un enfoque extremo a extremo que las soluciones divididas en nichos de AAA, NAC y políticas no son capaces de entregar. La capacidad para utilizar en un mismo servicio de políticas varios almacenes de identidades, entre los que se incluyen Microsoft Active Directory, directorios compatibles con LDAP, bases de datos SQL compatibles con ODBC, servidores de tokens y bases de datos internas, diferencia a ClearPass de cualquier solución heredada.

THE POWER OF CLEARPASS EXCHANGE

APROVISIONAMIENTO DE DISPOSITIVOS SIN PARTICIPACIÓN DEL DEPARTAMENTO DE TI

Gestionar la incorporación de dispositivos para implementaciones de Traiga su propio dispositivo (TSPD)

puede suponer una gran carga para el departamento de TI y el personal de asistencia. Además, genera grandes preocupaciones sobre la seguridad.

ClearPass Onboard permite a los usuarios configurar por sí mismos los dispositivos para su uso en redes seguras. Los certificados específicos para dispositivos eliminan incluso la necesidad de que los usuarios tengan que introducir credenciales de inicio de sesión una y otra vez durante el día. Tan sólo la comodidad que ello supone ya representa una ventaja. El aumento de la seguridad que se consigue utilizando certificados es otro valor añadido.

El equipo de TI define quién puede incorporar dispositivos, así como su tipo y el número por persona. Una autoridad de certificados integrada permite que la organización de TI admita dispositivos personales mucho más rápidamente como PKI internos, lo que elimina la necesidad de emplear más recursos de TI posteriores.

El acceso de invitados es así de simple y rápido

Las políticas de TSPD no se limitan a los dispositivos de los empleados. Incluyen a cualquier visitante cuyo dispositivo necesite acceder a la red, ya sea cableada o inalámbrica. El departamento de TI necesita un modelo simple que empuje el dispositivo a un portal de marca propia, automatice el aprovisionamiento de las credenciales de acceso y proporcione características de seguridad que mantengan la separación del tráfico empresarial.

ClearPass Guest facilita que los empleados, recepcionistas, coordinadores de eventos y demás personal ajeno al departamento de TI creen de forma eficaz cuentas de acceso temporal a la red para cualquier cantidad de invitados por día. El MAC Caching también asegura que los invitados puedan conectarse con facilidad a lo largo del día sin tener que introducir una y otra vez sus credenciales en el portal de invitados.

El autorregistro evita a los empleados tener que realizar esta tarea y permite a los invitados crear sus propias credenciales. Las credenciales de inicio de sesión se entregan en chapas impresas, mensajes SMS o correos electrónicos. Las credenciales pueden almacenarse en ClearPass durante periodos predefinidos, así como configurarse para caducar automáticamente tras un número concreto de horas o días.

Cuando el estado del dispositivo determina el acceso

Durante el proceso de autorización, puede ser necesario realizar evaluaciones de estado de determinados dispositivos con el fin de garantizar que cumplen las políticas antivirus, antispyware y de firewall de la empresa. La automatización motiva a los usuarios para realizar un análisis antivirus antes de conectarse a la red empresarial.

ClearPass OnGuard ofrece funcionalidades integradas que realizan comprobaciones de estado basadas en políticas para eliminar vulnerabilidades en una amplia gama de sistemas operativos informáticos y versiones. Con independencia de que se utilicen clientes persistentes o disolubles, ClearPass puede identificar centralmente puntos finales conformes en infraestructuras inalámbricas, cableadas y de VPN.

Algunos ejemplos de comprobaciones de estado avanzadas que proporcionan seguridad adicional:

- Gestión de aplicaciones, servicios y claves de registro punto a punto.
- Determinación de si se permiten dispositivos de almacenamiento USB o instancias de máquinas virtuales.
- Gestión del uso de interfaces de redes con puentes y cifrado de discos.

Obtenga mayor rendimiento de las soluciones de terceros

ClearPass Exchange le permite automatizar la solución de amenazas de seguridad o mejorar un servicio utilizando soluciones de terceros populares, como firewalls, MDM/EMM, MFA, registro de visitantes y herramientas SIEM. Al aprovechar la inteligencia de contexto que contiene ClearPass, las organizaciones pueden asegurarse de proporcionar seguridad y visibilidad a nivel de dispositivos, acceso de red, inspección de tráfico y protección frente a amenazas.

Con una (REST) API de lenguaje común, mensajería syslog y el repositorio integrado ClearPass Extensions, las decisiones y los flujos de trabajo automatizados ayudan a simplificar las tareas y proteger la empresa; ya no será necesario recurrir a complejos lenguajes de secuencias de comandos ni a interminables configuraciones manuales. Y para acelerar la integración, Extensions permite a los partners cargar una extensión para la entrega en tiempo real de nuevos servicios a clientes conjuntos.

Con ClearPass Exchange, las redes pueden actuar automáticamente:

- Los datos MDM/EMM, como el estado de jailbreak de un dispositivo, pueden determinar si se puede conectar a una red.
- Los firewalls pueden aplicar con precisión políticas basadas en usuarios, grupos y atributos de dispositivo

específicos, así como aprovechar ClearPass para solucionar los problemas de un dispositivo que presente un comportamiento incorrecto.
- Las herramientas SIEM pueden configurarse para almacenar los datos de autenticación de todos los dispositivos conectados.
- Se puede pedir a los usuarios que utilicen autenticación con varios factores para demostrar que realmente son ellos los que se conectan a las redes y los recursos.

Los eventos de red también pueden desencadenar que los firewalls, SIEM, y otras herramientas informen a ClearPass para que actúe sobre un dispositivo, iniciando acciones de forma bidireccional. Por ejemplo, si un usuario realiza varias autenticaciones de red incorrectas, ClearPass puede iniciar un mensaje de notificación dirigido directamente al dispositivo o incluirlo en una lista negra que le prohíba el acceso a la red.

Acceda con seguridad a las aplicaciones profesionales desde cualquier lugar

Iniciar sesión en las aplicaciones profesionales durante la jornada debe ser un proceso rápido y sin esfuerzos. ClearPass es compatible con SSO y la funcionalidad ClearPass Auto Sign-On por ese motivo. En lugar de un inicio de sesión único, que requiere que todo el mundo inicie sesión una vez en las aplicaciones, Auto Sign-On utiliza un inicio de sesión de red válido para que los usuarios puedan acceder automáticamente a las aplicaciones móviles de la empresa. Los usuarios solamente tienen que realizar su inicio de sesión de red o disponer de un certificado válido en sus dispositivos.

Donde utilice Single Sign-On, también puede emplear ClearPass como proveedor de identidad (IdP) o proveedor de servicio (SP).

Servicios Bonjour, DLNA y UPnP

Los usuarios pueden compartir proyectores, televisores, impresoras y otros dispositivos multimedia que utilicen LNA/UPnP o Apple AirPlay y AirPrint sobre su infraestructura Wi-Fi de Aruba. ClearPass facilita la búsqueda de estos dispositivos y su uso compartido.

Por ejemplo, un profesor que quiera mostrar una presentación de una tablet en una pantalla solamente verá la que está disponible en su aula. No verá los dispositivos que se encuentren en otras zonas del campus. También puede emplear el portal para seleccionar quién más puede utilizar la pantalla, y evitar así que los alumnos lleguen a controlarla.

Otro ejemplo se encuentra en el sector de la sanidad. Los médicos pueden proyectar fácilmente imágenes PACS digitales desde sus iPad a una pantalla de mayor tamaño en cualquier lugar del hospital. La colaboración con los pacientes acaba de volverse más simple.

UNA BASE CON CAPACIDAD DE ADAPTACIÓN PARA LA SEGURIDAD Y LOS SERVICIOS

Poder proporcionar una experiencia sin interrupciones para los usuarios móviles de hoy en día y la rápida adopción de tecnologías de IoT son dos factores que han generado multitud de nuevos desafíos de TI. Se necesita planificación, herramientas adecuadas y una sólida base para asegurar el acceso en cualquier momento y desde cualquier lugar en los entornos cableados e inalámbricos.

ClearPass resuelve estos desafíos entregando identidad de dispositivos, control de políticas, automatización de los flujos de trabajo y protección automatizada ante amenazas desde una misma solución homogénea. Al capturar y correlacionar datos contextuales en tiempo real, ClearPass le permite definir políticas que funcionan en cualquier entorno: la oficina, el campus o un estadio.

Las últimas mejoras de ClearPass también responden a los desafíos de seguridad de red emergentes que surgen de la adopción del Internet de las cosas (IoT), el fortalecimiento de la autenticación de dispositivos y aplicaciones móviles, y la mayor visibilidad de las incidencias de seguridad. La protección automatizada frente a las amenazas y las características de servicio inteligente garantizan que cada dispositivo reciba los privilegios de acceso a la red correctos, con una interacción directa mínima con el departamento de TI.

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