Patrocinado por: **Aruba, una empresa de Hewlett Packard Enterprise**

Autores:

Robert Ayoub
Matthew Marden

Abril de 2016

El valor empresarial de proteger y autenticar a los usuarios de las redes inalámbricas y cableadas

Puntos destacados del valor empresarial

12 036 dólares

Valor del tiempo del personal de TI ahorrado por cada 1000 dispositivos en redes

Más del doble de dispositivos autenticados

60 %

Porcentaje en que aumentó la rapidez de respuesta a las incidencias relacionadas con el acceso a la red

89 %

Porcentaje en que aumentó la rapidez de incorporación de dispositivos a la red

RESUMEN EJECUTIVO

El Internet de las cosas (IoT) sigue ampliando el número de dispositivos que los empleados e invitados introducen en la red corporativa. Hoy en día, los empleados dependen de una combinación de dispositivos, que abarcan desde portátiles y tabletas a smartphones y dispositivos que se pueden llevar puestos, para trabajar de forma más eficiente y lograr una mayor conciliación laboral y familiar. Los clientes introducen en las redes con cada vez mayor frecuencia sus propias combinaciones de dispositivos conectados, desde teléfonos móviles a cámaras, con la esperanza de obtener conectividad, así como de interactuar con los medios sociales.

Cada dispositivo que se conecta a la red debe observar las políticas de seguridad para garantizar que no introduce malware o se lleva datos sensibles. Los profesionales de la seguridad se ven superados por los posibles incidentes, sumados a los aspectos operativos diarios de la seguridad, que a su vez, se complican todavía más por la variedad y enorme distribución del conjunto de puntos finales conectados que deben gestionar.

Como consecuencia de la necesidad de aplicar políticas homogéneas para todos los dispositivos, empleados, subcontratistas e invitados, muchas organizaciones están recurriendo al control de acceso a la red (NAC). Aunque las primeras implementaciones del NAC presentaban carencias, las soluciones NAC de nueva generación pueden ahorrar tiempo y dinero a las organizaciones al ofrecer una incorporación rápida de dispositivos, una aplicación de políticas homogénea, una seguridad añadida y una mejora de las funcionalidades de respuesta ante incidencias.

IDC ha entrevistado a cinco organizaciones que utilizan Aruba ClearPass como plataforma de gestión de políticas para el control de acceso a la red para comprender el valor y los costes asociados con su uso. Estas organizaciones se enfrentan a desafíos comunes a otras que intentan habilitar el acceso a la red desde cualquier lugar, con cualquier dispositivo, sin dejar de mantener una sólida seguridad de red. Las entrevistas con estas organizaciones muestran que Aruba ClearPass ha mejorado tanto sus procedimientos como la seguridad de acceso a la red de la siguiente manera:

- Autenticando y protegiendo más dispositivos, al tiempo que proporciona mayor visibilidad de todas las autenticaciones correctas y fallidas, así como de los dispositivos (portátiles, smartphones, IoT) de sus redes
- Resolviendo más rápidamente los problemas relacionados con la red. De este modo, ahorra tiempo al personal de TI y mejora la experiencia de usuario
- Incorporando nuevos dispositivos en menos tiempo, lo que mejora la productividad de los empleados y reduce el tiempo dedicado al soporte
- Mejorando la eficacia de las operaciones de TI, lo que libera tiempo que puede dedicarse a otras actividades.

Descripción general de la situación

Descripción general de las tendencias del mercado

El control de acceso a la red (NAC) no es una tecnología nueva. No obstante, el paisaje de TI actual es muy distinto del que había hace 10 años. Aunque la necesidad de supervisar el estado de los dispositivos invitados sigue siendo un desafío clave, existen muchos factores adicionales que impulsan la necesidad de contar con control de acceso a la red hoy en día.

El impacto de las políticas de BYOD y la IoT. El crecimiento exponencial de las políticas de "traiga su dispositivo" (BYOD) y el potencial de la Internet de las cosas (IoT) plantean demandas sin precedentes tanto sobre la red inalámbrica como sobre la cableada. Los administradores no solo deben admitir un volumen mayor de tráfico, sino que ahora deben habilitar a los empleados para acceder a la red corporativa sin comprometer la seguridad de esta ni la de las aplicaciones. Las soluciones de control de acceso a la red permiten la estandarización de la seguridad y la aplicación de políticas de acceso independientes del método, contexto o dispositivo utilizado para ello.

Varios dispositivos por usuario. No sólo los usuarios introducen sus propios dispositivos en la red, sino que han multiplicado su número y diversidad. Deben aplicarse políticas homogéneas con independencia del dispositivo. Asimismo, los nuevos dispositivos presentan vectores de ataque ante los que deben protegerse las organizaciones.

Mayor atención a la experiencia de los clientes y empleados. Las organizaciones reconocen que proporcionar una experiencia inalámbrica sin interrupciones puede mejorar la lealtad de los clientes y multiplicar las oportunidades de generación de ingresos. Los empleados pueden ser más productivos si disponen de una infraestructura inalámbrica fiable cuando se desplazan por las instalaciones.

Las organizaciones siguen siendo responsables de su seguridad. En última instancia, las organizaciones son las principales responsables de proteger sus redes y datos. Por tanto, necesitan mantener homogénea la forma de aplicar la seguridad en toda la infraestructura de red, ya sea cableada o inalámbrica, y con independencia del tipo de dispositivo o el usuario.

Aruba ClearPass

Aruba ClearPass permite a los clientes crear y aplicar políticas que se extienden por toda la red hasta los dispositivos y las aplicaciones. Las organizaciones pueden aplicar un control total sobre sus servicios de movilidad y simplificar el despliegue y la protección de los dispositivos gestionados por el departamento de TI, así como de aquellos introducidos por BYOD o la Internet de las cosas. ClearPass, que opera en un entorno multiproveedor, proporciona la capacidad de incorporar un dispositivo con seguridad, gestionar las reglas aplicables a los dispositivos, admitir usuarios invitados y realizar evaluaciones de estado de los puntos finales, entre otras funcionalidades.

ClearPass Exchange se integra con otros componentes de seguridad, como firewalls y MDM/EMM, para ofrecer soluciones más granulares. ClearPass Exchange permite compartir datos de contexto claves (usuario, dispositivo, hora, ubicación, etc.) para mejorar la infraestructura de seguridad global, al permitir que dispositivos de terceros trabajen conjuntamente para tomar decisiones más precisas sobre políticas.

El valor empresarial de Aruba ClearPass

Demografía de la encuesta

IDC entrevistó a cinco organizaciones que utilizan ClearPass como plataforma de gestión de políticas para el control de acceso a la red. Estas entrevistas se diseñaron para comprender los casos de uso de estas organizaciones, así como para recopilar información cuantitativa y cualitativa sobre el impacto de ClearPass en sus operaciones. Todas estas organizaciones proporcionan acceso de red inalámbrico tanto a los usuarios como a los invitados que acceden a sus redes, y utilizan ClearPass para habilitar la seguridad de red y el acceso basado en roles. Estas organizaciones tienen una media de 4876 empleados, pero cuentan con un número significativamente mayor de dispositivos en sus redes (una media de 14643), además de numerosos dispositivos adicionales que utilizan grupos de alumnos e invitados.

TABLA 1

Demografía de las organizaciones entrevistadas que utilizan Aruba ClearPass

	Media	Medio
Número de empleados	4876	600
Personal de TI	49	27
Usuarios de TI	4849	550
Alumnos (tres escuelas)	52396	41000
Emplazamientos	27	7
Dispositivos móviles en redes	14643	8848
Países	Estados Unidos	
Sectores	Ingeniería, educación, sector público/sin ánimo de lucro	

Fuente: IDC, 2016

Análisis del valor empresarial

Los clientes de Aruba ClearPass indicaron que obtienen valor al mejorar el control, la protección y el acceso a sus redes. El resultado es que estas organizaciones son capaces de minimizar el riesgo de sus redes ante usuarios desconocidos y otras infracciones de seguridad potenciales, al tiempo que extienden la funcionalidad completa de la red a los usuarios conocidos.

Entre tanto, el personal de TI se ha beneficiado entregando un acceso de red seguro de forma oportuna y eficaz. En consecuencia, ClearPass constituye un elemento importante en los entornos de red globales de estas organizaciones, al tiempo que ayuda a maximizar el valor de las inversiones realizadas en sus ecosistemas de seguridad.

Autenticación de dispositivos

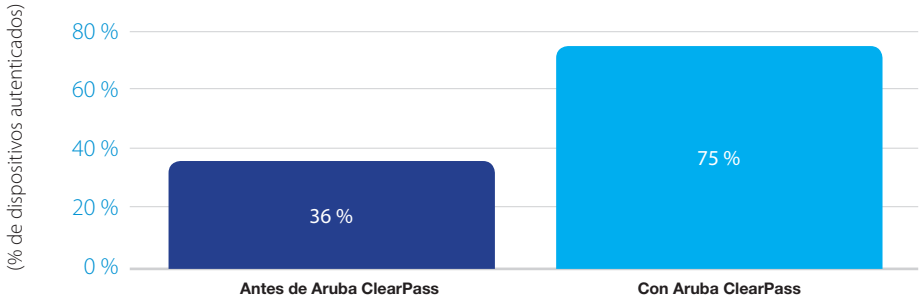
Las organizaciones entrevistadas indicaron que una ventaja central de Aruba ClearPass es que permite autenticar usuarios de forma más homogénea y otorgarles el nivel adecuado de acceso a la red. Varias organizaciones explicaron que habían tenido problemas para lograr niveles homogéneos de acceso a la red y autenticación de dispositivos antes de utilizar ClearPass. De media, las organizaciones entrevistadas habían duplicado el número de dispositivos que podían autenticar correctamente. Ahora autentican una media de tres cuartas partes de los dispositivos que entran en contacto con sus redes (consulte la Figura 1). Ello significa que saben qué dispositivos están conectados a sus redes y, por consiguiente, aplican mejor los privilegios de red. En última instancia, ambas ventajas permiten mejorar su seguridad de red.

Las organizaciones entrevistadas proporcionaron varios ejemplos de cómo ClearPass ha permitido mejorar los flujos de trabajo de autenticación. Un director de TI de Poway USD explicaba: "Cuando llegó ClearPass, constatamos que tenía la capacidad de operar perfectamente con todos los sistemas operativos con los que trabajamos: Windows, Mac OS, iOS, Android. Su compatibilidad con todos fue un factor determinante para seleccionarlo".

- **Un director de TI** de Cypress-Fairbanks ISD comentó cómo ClearPass apoya de forma efectiva sus esfuerzos de autenticación: "ClearPass es capaz de determinar si el usuario es un simple visitante o un empleado con su propio dispositivo que se está autenticando en la red con su ID y contraseña".
- **Mientras tanto,** un director de TI de un organismo público explicó la manera en la que ClearPass ha apoyado a su organización: "Creo que proteger los dispositivos propiedad de los empleados, la conectividad y la autenticación de estos dispositivos en la red interna era algo esencial. Nuestros empleados realizan numerosas operaciones en nuestra red inalámbrica, así que no queríamos que utilizaran continuamente la red para invitados".

FIGURA 1

Porcentaje de dispositivos autenticados, Aruba ClearPass



Fuente: IDC, 2016

Eficiencias de gestión de incidencias

Las organizaciones entrevistadas indicaron que Aruba ClearPass les ofrece una mayor visibilidad de los problemas que afectan a los usuarios cuando intentan acceder a las redes, y ello les permite resolver los problemas en menos tiempo. De media, las organizaciones han reducido el tiempo necesario para resolver este tipo de incidencias en un 60 %, al pasar de casi dos horas a menos de una (consulte la Tabla 1). Por una parte, esto reduce el tiempo que el personal solía dedicar a intentar determinar y aislar la causa del problema, y por otra, significa que los propietarios de los dispositivos se enfrentan a una interrupción del acceso a la red más breve. En total, el personal de TI ha reducido un 65 % el tiempo que debe invertir en responder a este tipo de incidencias y resolverlas gracias a ClearPass. Se proporcionaron varios ejemplos concretos, y entre ellos, los siguientes:

- **Identificación más rápida de problemas.** Un director de TI de un organismo público explicó: "ClearPass nos permite identificar las cosas un poco más rápido cuando nos enfrentamos a problemas de red. No dedico tanto tiempo como antes a distinguir las configuraciones incorrectas de las amenazas".
- **Aislar problemas más rápido.** Un director de TI de NuScale explicó: "Una ventaja clave de ClearPass es su capacidad para aislar lo que está provocando los problemas. Solíamos tener que recurrir a "mostrar todo" y aplicar referencias cruzadas en Active Directory, además de analizar los archivos de registro. . . Yo diría que, antes de implementar Aruba Wireless y Aruba ClearPass, tardábamos muchísimas horas en resolver cada incidencia. Ahora, no tardamos más de 1 hora u hora y media".

TABLA 1

Demografía de las organizaciones entrevistadas que utilizan Aruba ClearPass

	Antes de Aruba ClearPass	Con Aruba ClearPass	Diferencia	% de cambio
Tiempo medio por incidencia, horas	1,8	0,7	1,1	60 %
Total de horas por respuesta a incidencias por año y organización	2852	1010	1842	65 %
Total de horas de impacto por 1000 dispositivos y año	195	69	126	65 %
Valor del tiempo del personal de TI por 1000 dispositivos y año	8289 dólares	2936 dólares	5353 dólares	65 %

Fuente: IDC, 2016

Eficiencias de incorporación de dispositivos

ClearPass Onboard ayuda a los usuarios a realizar un aprovisionamiento automático de sus dispositivos, lo que mejora su experiencia y permite al personal de TI dedicar menos tiempo a los problemas de este ámbito. ClearPass Onboard puede aplicar la política de seguridad flexiblemente sin dejar de automatizar el proceso de incorporación. Gracias a ello, se reduce la probabilidad de que se produzcan errores de incorporación de dispositivos a la red. Esta ventaja resulta especialmente valiosa en los casos en los que los propietarios de los dispositivos necesitan que el departamento de TI los ayude a completar el proceso de incorporación. Las organizaciones entrevistadas indicaron que su personal ha reducido en un 89 % el tiempo que dedica a estas actividades gracias a ClearPass (consulte la Tabla 2). Un director de TI de Cypress-Fairbanks USD comentó: "Con ClearPass, no solo podemos conectar a más usuarios más rápidamente, sino que la resolución de problemas resulta más fácil, lo que mejora enormemente la satisfacción de los usuarios finales. Pueden incorporarse fácilmente, no tienen tantos problemas, y cuando los tienen somos capaces de solucionarlos más rápidamente".

Las eficiencias relacionadas con la incorporación de dispositivos resultan especialmente valiosas para estas organizaciones cuando necesitan introducir muchos dispositivos de usuarios en sus redes en poco tiempo. Por ejemplo, la Universidad Trevecca Nazarene incorpora a cientos de alumnos al principio de cada semestre. Uno de sus directores de TI indicó que ClearPass les está ayudando a ahorrar mucho tiempo, al reducir el número de alumnos que requieren soporte: "Implementamos ClearPass para poder incorporar dispositivos a la red inalámbrica. Con ClearPass, solemos tardar cinco minutos o menos, frente a los más de 15 minutos que hacían falta en el pasado… Cada semestre, teníamos a varios cientos de alumnos que necesitaban ayuda durante el proceso de incorporación de sus dispositivos. Ahora, son tan sólo unos 50 alumnos por semestre los que no lo consiguen".

TABLA 2

KPI relacionados con la incorporación de dispositivos de usuarios, Aruba ClearPass

	Antes de Aruba ClearPass	Con Aruba ClearPass	Diferencia	% de cambio
Tiempo medio de incorporación, horas	2,2	0,5	1,7	78 %
Total de horas para la incorporación de dispositivos por año y organización	1142	122	1020	89 %
Total de horas de impacto por 1000 dispositivos por año	78	8	70	89 %
Valor del tiempo del personal de TI por 1000 dispositivos por año	3318 dólares	353 dólares	2965 dólares	89 %

Fuente: IDC, 2016

Eficiencias del personal de TI

Las eficiencias en la resolución de problemas y la incorporación de dispositivos, combinadas con mejores cifras en términos de mantener la seguridad de la red y gestionar las redes de acceso para invitados, crean un valor significativo para las organizaciones entrevistadas que utilizan Aruba ClearPass (consulte la Tabla 3). IDC utiliza las áreas de seguridad de red, gestión de incidencias, incorporación de dispositivos y gestión de invitados de red, para calcular un ahorro de tiempo de 283 horas por cada 1000 dispositivos al año, lo que a su vez se traduce en 12036 dólares en tiempo del personal de TI. Para organizaciones de TI a las que se les exige que hagan más sin dejar de rendir con la máxima eficiencia, estos ahorros de tiempo pueden reinvertirse en actividades que apoyen mejor las operaciones empresariales. Un director de TI de Poway ISD explicó el impacto al más alto nivel que ha tenido ClearPass en las operaciones de TI de su organización: "ClearPass nos permite hacer cosas que antes no podíamos. Es como añadir funcionalidades con las que no contábamos en el pasado. Es decir, en cuanto descubríamos alguna funcionalidad determinada que nos ofrecía ClearPass, pensábamos la forma de utilizarla para realizar acciones que antes resultaban imposibles".

TABLA 3

Ahorro de tiempo y eficiencias del personal de TI, Aruba ClearPass

Horas por 1000 dispositivos por año	Antes de Aruba ClearPass	Con Aruba ClearPass	Diferencia	% de cambio
Seguridad de red	135	101	34	26 %
Gestión de incidencias	195	69	126	65 %
Incorporación de dispositivos	78	8	70	89 %
Gestión de red de invitados	66	13	53	80 %
Total	474	191	283	60 %
Valor total (por 1000 dispositivos y año)	20 165 dólares	8129 dólares	12 036 dólares	60 %

Fuente: IDC, 2016

Desafíos y oportunidades

Como con cualquier solución de TI, el control de acceso a la red presenta un conjunto exclusivo de ventajas e inconvenientes. Los departamentos de TI de las empresas deben considerar cuidadosamente los desafíos potenciales y sopesarlos frente a las ventajas que se han explicado anteriormente.

- **Evaluación de la rentabilidad de la inversión de una solución.** Implementar una red unificada conlleva costes de tiempo y equipos que afectan tanto al presupuesto operativo como al de capital. Los responsables de decisiones de TI deben realizar un análisis de costes/beneficios detallado antes de emprender una actualización, especialmente si se va a introducir un nuevo proveedor/una nueva solución que implique una curva de aprendizaje. Al evaluar la rentabilidad de la inversión de una solución de acceso a la red unificada, los responsables de decisiones de TI deben considerar el impacto de la automatización de procesos, la seguridad y la conformidad.

- **Las políticas y la integración deben definirse por adelantado.** Con cualquier solución de seguridad, las políticas deben estar claramente definidas y desplegadas en el momento de la implementación. Aruba ClearPass puede facilitar el proceso de incorporación, implementar políticas de forma homogénea a través de la organización, y realizar evaluaciones de puntos finales, pero dichas políticas deben definirse por adelantado. ClearPass aplica políticas, pero no va a proporcionar prevención ni soluciones para todo. Añadir ClearPass puede requerir la integración con soluciones de seguridad de terceros para proporcionar protección de extremo a extremo. No obstante, ClearPass Exchange cuenta con un ecosistema tecnológico muy sólido para garantizar la compatibilidad con la mayoría de los proveedores de equipos de seguridad.

- **Impacto potencial sobre el rendimiento.** Cualquier evaluación del punto final puede llegar a afectar al rendimiento del dispositivo en cuestión. La cuarentena de un dispositivo infectado puede afectar a la experiencia de usuario y requerir una intervención manual para su solución. Las organizaciones deben sopesar una experiencia de usuario potencialmente negativa frente a la protección de la red de la empresa y determinar la mejor forma de gestionar las excepciones.

Resumen y conclusión

Las organizaciones se enfrentan al desafío de encontrar formas eficientes de proporcionar acceso a la red a un número cada vez mayor de usuarios y dispositivos sin comprometer la seguridad ni sobrecargar a sus equipos de TI. Tanto los empleados como otras personas esenciales para el éxito organizativo, incluidos los invitados y alumnos, esperan poder utilizar sus propios dispositivos con un acceso a la red sólido y sin retrasos indebidos. Esto ha llevado a las organizaciones a ver las soluciones de acceso a la red como una forma de garantizar

una incorporación rápida, sin comprometer la seguridad global. La investigación realizada por IDC para este estudio muestra que las organizaciones entrevistadas están obteniendo valor con Aruba ClearPass al mejorar el control, la protección y el acceso a sus redes. Ello les permite reducir el riesgo y reducir al mínimo el tiempo que debe dedicar el departamento de TI a incorporar y prestar soporte a los usuarios en sus redes, incluso cuando extienden toda la funcionalidad de estas a los usuarios conocidos. El resultado es que las organizaciones pueden proporcionar acceso de red para apoyar plenamente a sus empleados y garantizar la experiencia de otros usuarios de una forma rentable y segura.

Anexo

IDC ha utilizado su metodología estándar para este proyecto. Esta metodología consiste en recopilar datos de usuarios actuales de Aruba como base para el modelo. Los cálculos de valor realizados por IDC utilizan una serie de supuestos, que incluyen:

- Los valores de tiempo se multiplican por el salario gravado (salario + 28 % de complementos y gastos generales) para cuantificar la eficiencia y el ahorro de productividad del área de gestión.
- Los valores de los salarios asumidos para este estudio son: 80 000 dólares anuales para el personal de TI y 63 000 dólares anuales para otros empleados (usuarios de servicios de TI).
- La productividad perdida es el producto del tiempo de inactividad multiplicado por el salario gravado.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor internacional de inteligencia de mercado, servicios de asesoramiento y eventos para los mercados de la tecnología de la información, las telecomunicaciones y la tecnología de consumidor. IDC ayuda a los profesionales de TI, ejecutivos empresariales, así como a la comunidad de inversores, a tomar decisiones basadas en hechos en relación con las adquisiciones tecnológicas y la estrategia empresarial. Más de 1100 analistas de IDC ofrecen experiencia global, regional y local sobre oportunidades y tendencias tecnológicas y sectoriales en más de 110 países de todo el mundo. Durante 50 años, IDC ha proporcionado conocimiento estratégico para ayudar a nuestros clientes a alcanzar sus objetivos empresariales. IDC es una filial de IDG, la empresa líder en medios, investigación y eventos sobre tecnología del mundo.

Sede internacional de IDC

5 Speen Street
Framingham, MA 01701
EE. UU.
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

IDC Analyze the Future