aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

CONTROL DE ACCESO A LA RED SEGURO CON CLEARPASS Y CERTIFICACIÓN COMMON CRITERIA

INTRODUCCIÓN

Los ataques cibernéticos son cada vez más inteligentes, específicos y dañinos. Gracias a una superficie susceptible a los ataques en rápida expansión que incluye móviles, TSPD, la nube y el IoT, la probabilidad de éxito de los ataques no deja de aumentar. Ya se trate de una agencia gubernamental que protege una infraestructura o un proveedor de servicios sanitarios preocupado por la información de los pacientes... ninguna organización es inmune al estrés asociado a la prevención de estos ataques.

Mientras que las agencias gubernamentales se han puesto al frente de la definición de los criterios y procesos de certificación de los productos, los equipos de seguridad necesitan saber que los productos que están implementando para proteger sus organizaciones cumplen un conjunto de estándares de seguridad validados.

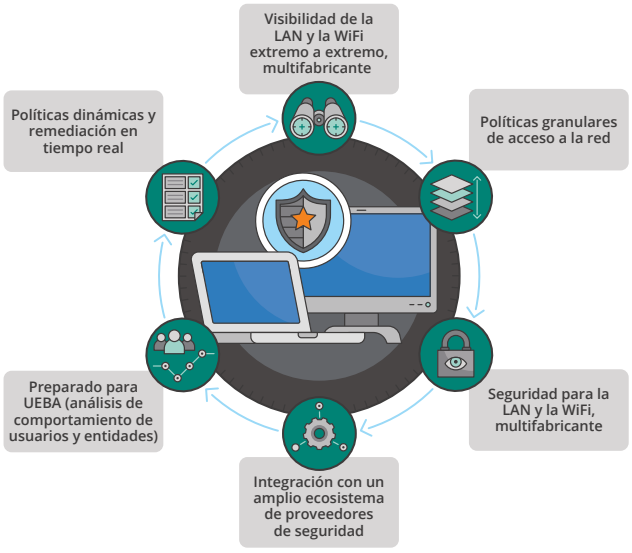
Desde el año 1999, los gobiernos de todo el mundo participan en un programa de validación y puesta a prueba de la norma ISO Common Criteria. Este programa analiza y garantiza que los productos de Tecnología de la Información cumplen una serie de requisitos de calidad elevados y homogéneos, lo que contribuye de manera importante a la fiabilidad de la seguridad de estos productos. En la actualidad, 28 países participan en el consorcio Common Criteria a través de iniciativas como NIAP en EE. UU., la Agence nationale de la sécurité des systèmes d'information (ANSSI) en Francia y el Australian Signals Directorate. Como resultado de ello, la certificación Common Criteria figura entre los requisitos en muchas listas de concursos de ofertas de compras gubernamentales.

La cartera de productos de Aruba, que incluye puntos de acceso inalámbricos, controladores y software de conexión remota (VPN), es pionera en la certificación Common Criteria. Como elemento clave del 360 Secure Fabric de Aruba, con vanguardistas soluciones de seguridad, ClearPass Policy Manager cuenta con las certificaciones FIPS y Common Criteria.

DESCRIPCIÓN GENERAL DE CLEARPASS

La familia ClearPass de productos de seguridad para el control de acceso a la red ofrece elaboración de perfiles, autenticación y autorización uniformes, completas y precisas para usuarios, sistemas y dispositivos que intentan acceder a los recursos de TI. ClearPass se ha diseñado para abordar los retos de seguridad asociados con una organización sin fronteras de TI, por ejemplo:

- **Visibilidad total.** Cuando se puede proporcionar acceso a la red desde casi cualquier lugar, en cualquier momento y con cualquier dispositivo, saber qué se encuentra conectado a la red constituye el primer reto. ClearPass ofrece detección y elaboración de perfiles completas para permitir que, no solo el equipo de seguridad, sino también el departamento de TI al completo, pueda ver quién y qué está conectado. Esto es especialmente importante cuando hay dispositivos tipo IoT conectados a la red.
- **Control proactivo.** Con ClearPass Policy Manager, se autoriza el acceso de usuarios, sistemas y dispositivos presentes en la red solo a aquellos recursos que su función requiere. ClearPass autentica cada entidad y asigna privilegios de acceso basados en políticas que ajustan los permisos en función de la ubicación, el dispositivo empleado, la hora del día, el tipo de usuario y otros factores.
- **Respuesta de bucle cerrado.** Piensa en ClearPass como en el guardián de la red. El mismo motor de políticas que habilita el acceso a la red se puede utilizar para responder a un ataque cibernético. Cuando se recibe una alerta de un ecosistema de seguridad (cortafuegos, sandboxes, respuesta y detección de punto final, SIEM, UEBA, etc.), ClearPass puede adoptar una serie de medidas basadas en políticas: desde una repetición de la autenticación, una restricción del ancho de banda, una cuarentena o un bloqueo.



Leyenda: Aruba ClearPass proporciona un enfoque de bucle cerrado a la respuesta y al control de acceso a la red.

LA VENTAJA CLEARPASS

- **Garantía de la seguridad a través de una certificación Common Criteria exhaustiva.** ClearPass posee la certificación Common Criteria para el NDcPP (Network Device collaborative Protection Profile), que abarca todos los aspectos del control de acceso, como el cifrado, la seguridad física, la validación y el procesado de certificados y el procesado de SSL. Además, el servidor de autenticación ClearPass también ha obtenido una certificación Common Criteria adicional que valida las capacidades centralizadas de autenticación, autorización y registro (Authentication, Authorization and Accounting - AAA) para el protocolo cliente/servidor RADIUS estándar del sector. Este nivel de certificación habilita a ClearPass para funcionar en redes clasificadas y con requisitos sensibles similares en el sector privado.
- **Integración abierta y fluida.** A diferencia de otras soluciones de control de acceso que requieren el compromiso con la infraestructura de un solo proveedor, ClearPass está optimizada para funcionar en cualquier red. Además, ClearPass se integra con más de 120 soluciones de seguridad y TI general para permitirles aprovechar perfiles y contexto de dispositivos que ClearPass genera. Los equipos de seguridad también utilizan ClearPass para actuar bien de forma manual o automática en respuesta a un ataque cibernético.
- **Una red, una vista, una política.** La capacidad de ClearPass para controlar el acceso a los recursos de TI no solo es independiente del proveedor que suministra el equipo, sino también de si el acceso es cableado, inalámbrico o remoto. Las organizaciones diseñan e implementan una política por usuario o dispositivo y ClearPass ejecuta esta política de manera uniforme en toda la topología de red. Esto ofrece ahorros de tiempo y costes que se pueden destinar a otros proyectos de seguridad y TI.
- **Redes optimizadas.** Un beneficio en términos de ROI de ClearPass es una aplicación basada en políticas de uso y acceso a puertos. En lugar de designar puertos para casos de uso específicos (para conectar impresoras, servidores, etc.), las organizaciones pueden utilizar una estrategia de "puertos sin denominación", por la que cada puerto se puede conectar a cualquier dispositivo mientras ClearPass ejecuta los controles de acceso basados en funciones adecuados. Así se simplifica la configuración de switches y se optimiza la utilización de los puertos.
- **Acceso blindado: comprobar y luego confiar.** Algunas soluciones de control de acceso permiten la entrada de cualquier usuario y dispositivo a la red y, a continuación, toman medidas si algo va mal. Este enfoque "NAC permisivo" hace posibles los ataques cibernético ultrarrápidos por los que el malware tarda un segundo en irrumpir en la red y lanzar un ataque más prolongado y dañino. ClearPass adopta el enfoque por el cual ningún usuario ni dispositivo puede acceder a la red sin autenticación positiva y la autorización de políticas correspondiente. Cuando los segundos importan, el control de acceso debe empezar en T cero.
- **Interceptación de ataques.** El axioma es: "no se puede proteger lo que no se ve". Una de las ventajas de la detección y la elaboración de perfiles de ClearPass es la visibilidad total. Pero en un mundo donde cada segundo cuenta en la respuesta a un ataque, tampoco se puede resolver lo que no se puede ver. Al usar ClearPass para establecer respuestas predeterminadas a señales de un ataque cibernético de un ecosistema de seguridad, los equipos de seguridad pueden frenar ataques antes de que causen daños, mientras que siguen investigando y estableciendo el alcance del mismo.

RESUMEN

La certificación Common Criteria es un proceso complejo que requiere que la protección de la seguridad forme parte integrante de la implementación y la arquitectura de un producto. En otro tiempo, Common Criteria era algo que solo exigían las agencias gubernamentales debido al elevado valor de los activos y la información que debían proteger. En la actualidad, todas las organizaciones deben hacer frente a riesgos similares, con consecuencias similares si un ataque cibernético tiene éxito. Para una solución esencial como es el control de acceso a la red, la certificación Common Criteria es clave. Con unas certificaciones Common Criteria mejoradas, ClearPass no solo ofrece una base segura, sino también un elemento esencial sobre el que apoyar la estrategia de seguridad de TI al completo.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com