aruba
a Hewlett Packard Enterprise company

RESUMEN DE SOLUCIÓN

SEGURIDAD DE PUNTOS TERMINALES CON ARUBA CLEARPASS E INTROSPECT

DESAFÍOS DE SEGURIDAD ACTUALES

Los ataques enfocados de la actualidad están diseñados para permanecer "abajo del radar", moviéndose en pequeños pero deliberados pasos durante largos periodos de tiempo — frecuentemente con credenciales legítimas de un usuario, sistema, o dispositivo comprometido.

El protegerse en contra de amenazas cibernéticas ahora requiere una estrategia de seguridad con capas múltiples que incluya la capacidad de detectar y de combatir amenazas que hayan evadido soluciones tradicionales de reglas y basadas en firmas, mientras que utilizan credenciales legítimas de empleados, contratistas, partners, o dispositivos IoT comprometidos. De acuerdo con el Reporte de Investigación de Violaciones de Datos de Verizon de 2016:

- Más del 60% de las violaciones de datos confirmadas involucraron contraseñas débiles, por omisión, o robadas
- 70% de todas las violaciones por mal uso de privilegios o por parte de personas internas tardaron meses o años en ser descubiertas

Normalmente, los equipos de seguridad enfrentan estos tipos de ataques utilizando métodos de investigación manuales, que consumen tiempo, con procesos reactivos y de remediación retrasada que frecuentemente no son efectivos. El objetivo es aprovechar el control de acceso granular y visibilidad – en combinación con la detección de ataques automatizada – para un enfoque de seguridad más proactivo y oportuno:

- Visibilidad de todos los dispositivos conectados y que se estén conectando, alámbricos e inalámbricos, de múltiples proveedores,
- Control para asegurar que solamente dispositivos autenticados o autorizados accedan a la empresa
- Respuesta al Ataque utilizando el propio sistema de corretaje de ClearPass y de partners de intercambio para entregar seguridad a vectores de ataque conocidos y desconocidos

DETECCIÓN DE ATAQUES AUTOMATIZADA Y REMEDIACIÓN ACELERADA

De sensores a sistemas a usuarios, los ataques provenientes desde adentro requieren una nueva estrategia. Afortunadamente, soluciones de seguridad innovadoras utilizando analíticos basados en aprendizaje de máquina y en plataformas de big data ahora pueden proporcionarles a las empresas una nueva dimensión de protección que los productos de seguridad tradicionales no tienen.

BENEFICIOS DE ALTO NIVEL

Ya sea un partner no autorizado o botnets IoT, Aruba ClearPass e IntroSpect entregan un antídoto potente para ataques desde adentro, sin importar en donde se originen.

- Perfilado de precisión y visibilidad en base al contexto de usuarios y dispositivos en tiempo real
- Soporte para cualquier tipo de dispositivo, incluyendo IoT
- Detección de ataques en base al aprendizaje de máquina, el cual no está disponible en sistemas de seguridad tradicionales
- Soporte a decisiones escalable y exhaustivo para investigación y remediación más rápidas
- Cumplimiento automatizado y preciso, independientemente de tiempo, ubicación, o dueño del dispositivo
- Integración transparente interconstruida

Aruba IntroSpect, una solución líder de Analíticos de Comportamiento de Usuarios y Entidades (UEBA por sus siglas en inglés) utiliza aprendizaje de máquina supervisado y no supervisado para establecer automáticamente una línea base de comportamiento de usuarios y dispositivos mientras busca activamente actividad anómala que pueda indicar una amenaza. Cuando IntroSpect se integra con Aruba ClearPass, la solución combinada entrega tres innovaciones clave de seguridad: detección avanzada de ataques, investigación acelerada y cumplimiento proactivo basado en políticas.

Ahora, los usuarios comprometidos o maliciosos, o los sistemas que participen en ataques, o los dispositivos IoT enrolados en un ejército latente de botnets pueden ser descubiertos y remediados antes de que efectúen cualquier daño a la infraestructura, a los activos, o a la reputación de una organización.

ARUBA INTROSPECT Y CLEARPASS PARA PROTECCIÓN DE 360 GRADOS

IntroSpect detecta sistemas o dispositivos de usuarios comprometidos, utilizando modelos de aprendizaje de máquina, supervisados y no supervisados, para ver cambios indicativos en el típico acceso y uso de TI. Cuando estas señales sutiles se agregan y se ponen en contexto en el tiempo, la presencia de un ataque

próximo se confirma y se alerta. Mediante comunicación bidireccional fuertemente integrada, IntroSpect entonces dispara a ClearPass para que efectúe un cambio de autorización para la entidad en cuestión.

DETECTE, RESPONDA, INVESTIGUE, DESPUÉS REMEDIE

CLEARPASS + UEBA = PROTECCIÓN DE 360°

Una vez que la amenaza se encuentre bajo control, un analista podrá entonces acudir al sistema de investigación de incidentes basado en big data de IntroSpect, en donde el historial completo de TI de la entidad bajo escrutinio—hasta el nivel de paquete—está disponible en segundos, para que la toma de decisiones y la remediación se reduzcan de horas y días a minutos.

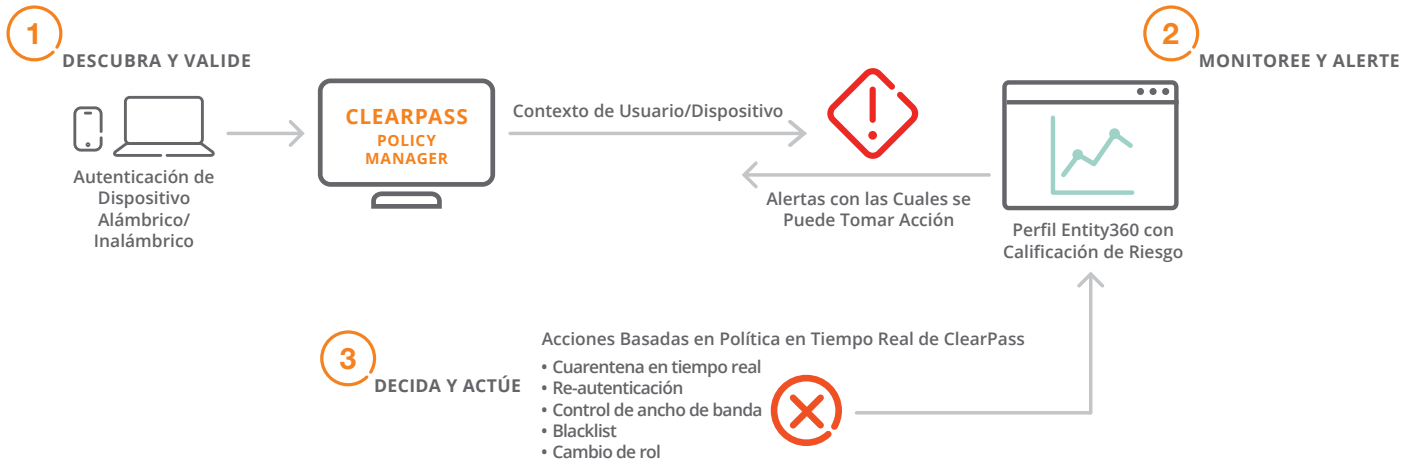

Figura 1: Cuando UEBA de IntroSpect se integra con Aruba ClearPass, la solución combinada entrega tres innovaciones clave de seguridad: detección avanzada de ataques, investigación acelerada y cumplimiento proactivo basado en políticas.

PRIORICE LOS RIESGOS DE SEGURIDAD

¿Laptops comportándose de mala manera? ¿Dispositivos IoT están desbocados? Las amenazas de la actualidad requieren un flujo de trabajo de administración de amenazas inteligente que integre detección, respuesta, investigación en tiempo real y remediación exhaustiva. Para lograr este nivel avanzado de administración de ataques provenientes de fuentes internas, ClearPass le proporciona a IntroSpect información de perfilado de cada dispositivo que ingresa a la red, incluyendo el rol del usuario o dispositivo, tiempo de conexión, ubicación y lo que esa entidad tiene permiso a acceder.

Con visibilidad detallada, IntroSpect entonces puede establecer una línea base y analizar el tráfico de un dispositivo en función a las características esperadas.

Por ejemplo, si IntroSpect detecta que un dispositivo asociado a un "Visitante" está exhibiendo comportamientos anómalos, IntroSpect puede disparar una respuesta de seguridad basada en políticas que ClearPass entonces puede hacer cumplir, la cual puede incluir colocar a una entidad en cuarentena o en una lista negra.

Como parte del flujo de trabajo de investigación de IntroSpect, un analista puede ver fácilmente cambios en la cantidad de datos transferidos, direcciones visitadas, ciclo de trabajo y el horario o ubicación para los cuales se reconoce la anomalía. La capacidad de aprovechar perfilado, reglas de acceso granulares y niveles diferenciados de cumplimiento asegura la remediación apropiada de una entidad comprometida.

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/latam