RESUMEN EJECUTIVO

ARUBA 360 SECURE FABRIC

360º de protección cibernética activa basada en analíticos y acceso seguro

No hace mucho, los equipos de seguridad empresariales podían identificar el perímetro que estaban protegiendo y trabajar con operaciones de TI para obtener control pleno de los recursos que sus empleados podían utilizar y a los cuales podían acceder, desde redes a sistemas a aplicaciones a datos. Hoy, no faltan trastornos de tecnología – movilidad, BYOD, virtualización, la nube, big data e IoT se han apoderado de la empresa y han provocado que el enfoque de seguridad basado en perímetros sea insuficiente. El problema se acrecienta por una era de desagregación de TI y por ataques altamente organizados y enfocados. El asegurar la seguridad de la organización no es tan sólo un asunto de misión crítica; ahora se ha tornado exponencialmente más difícil. Claramente, se necesita un enfoque moderno para enfrentar el rápidamente cambiante panorama de amenazas de hoy.

De acuerdo con Gartner, los Analíticos de Comportamiento de Usuarios y Entidades (User and Entity Behavioral Analysis, UEBA por sus siglas en inglés) es una categoría innovadora de tecnología de seguridad para identificar y mitigar amenazas avanzadas. "Durante al menos los últimos dos años, Gartner ha presenciado el surgimiento de muchos proveedores nuevos con analíticos avanzados en varios segmentos del mercado de seguridad. Un área que ha estimulado mucha innovación es UEBA, la cual habilita analíticos de seguridad de amplio alcance, en forma similar a como SIEM (Security Information and Event Management) habilita el monitoreo de seguridad de amplio alcance. UEBA proporciona analíticos para el comportamiento de usuarios, pero también de otras entidades como puntos terminales, redes y aplicaciones. La correlación de los análisis a través de varias entidades hace que los resultados de los analíticos sean más exactos y la detección de amenazas sea más efectiva, al igual que ocurre con SIEM."[1]

ARUBA 360 SECURE FABRIC

La mayoría de las soluciones de seguridad que se encuentran en el mercado en la actualidad es una numerosa colección de tecnologías diseñadas para los ambientes de ayer, basados en perímetros y en ambientes cerrados y estáticos. Estas tecnologías de seguridad dispares sólo pueden responder a uno de los muchos tipos de amenazas y vulnerabilidades de hoy. Esto requiere que operaciones de TI y de seguridad creen una solución de seguridad remendada que una a firewalls con IPS, con control de acceso, con anti-malware y con analíticos.

Impulsada por las exigencias de movilidad empresarial, BYOD, la nube e IoT, Aruba vio la necesidad de un enfoque de diseño diferente para conectar y asegurar redes. Aruba está ahora cambiando el paradigma con Aruba 360 Secure Fabric, un marco de trabajo de seguridad empresarial que les otorga a los equipos de seguridad y de TI una forma integrada de recuperar la visibilidad y el control. Permite que usted detecte ataques que se estén gestando con inteligencia aprendida por máquina y que responda proactivamente a estos ataques cibernéticos avanzados en cualquier infraestructura – con la escala empresarial para proteger a millones de usuarios y dispositivos y para asegurar grandes cantidades de datos distribuidos.

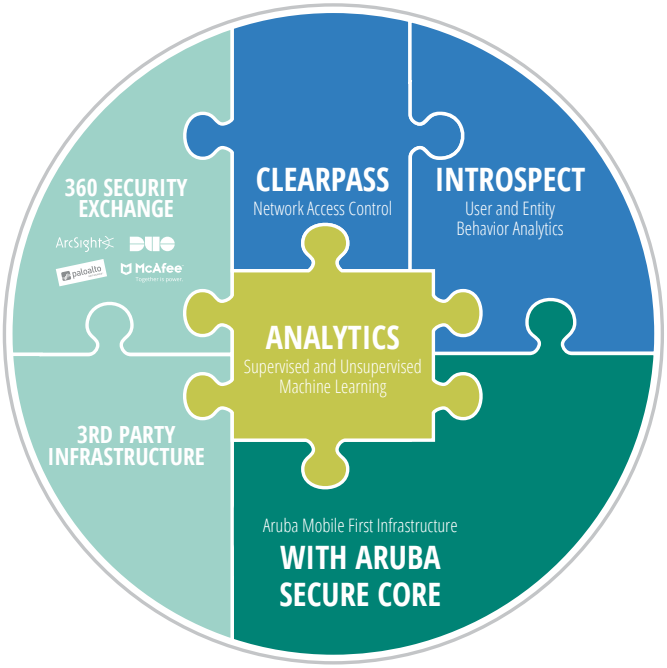

Figura 1: Aruba 360 Secure Fabric proporciona un marco de trabajo de seguridad integrado para que los equipos de TI y de seguridad obtengan nuevamente visibilidad y control de su red, centrado alrededor de analíticos.

Existen 3 elementos de este fabric:

- Software de Seguridad de Aruba: Control de acceso a la red proactivo y administración de políticas y UEBA líder en la industria para cualquier red
- Core Seguro de Aruba: Infraestructura de red preparada para analíticos con seguridad embebida
- Un ecosistema de seguridad mejor en clase

Figura 2: El nuevo imperativo de seguridad

Comenzando con las capacidades de seguridad core embebidas en la base de todos los access points (APs), switches, ruteadores y controladores Wi-Fi de Aruba, Aruba construye sobre esta base, integrando detección de ataques basada en aprendizaje de máquina de IntroSpect con sistemas de control de acceso como Aruba ClearPass en una plataforma abierta para múltiples proveedores. Con Aruba 360 Secure Fabric, los equipos de seguridad ahora pueden desarrollar un trayecto transparente desde el descubrimiento y acceso de usuarios y dispositivos hasta la detección y respuesta a ataques impulsados por analíticos – en base a las políticas establecidas por la organización.

UNA FORMA EXHAUSTIVA DE OBTENER VISIBILIDAD Y CONTROL SOBRE SUS REDES, USUARIOS Y DISPOSITIVOS

La desagregación de TI significa que las organizaciones no tan sólo necesitan una base de red segura, sino también visibilidad y control de los usuarios y dispositivos conectados a la red. ClearPass permite que la empresa cubra el conjunto completo de casos de uso de control de acceso, para dispositivos alámbricos e inalámbricos, visitantes, integración de BYOD y respuesta y rem[illegible] de ataques en [illegible]líticas.

VISIBILIDAD
Conozca lo que se encuentra en su red

CONTROL
Autentique y autorice todas las "cosas"

RESPUESTA
Coordinación de las herramientas de seguridad a través de ClearPass Exchange

Figura 3: ClearPass no tan sólo proporciona visibilidad, sino también extiende el control para dispositivos y usuarios que se conectan a su red.

Yendo un paso más allá, en febrero de 2017, Aruba agregó capacidades de detección de ataques basadas en aprendizaje de máquina, adquiriendo a Niara. Esta adición aprovecha la visibilidad de ClearPass del acceso a la red, así como la capacidad de implementar un rango de acciones manuales o automatizadas en respuesta a un ataque.

La solución de Analíticos de Comportamiento de Usuarios y Entidades (UEBA por sus siglas en inglés) de Aruba IntroSpect, detecta ataques identificando pequeños cambios en comportamiento que frecuentemente son indicativos de ataques que han evadido las defensas de seguridad tradicionales. Los ataques de la actualidad pueden estar compuestos de muchas acciones más pequeñas que ocurren durante largos periodos de tiempo. Estos tipos de ataques también son particularmente difíciles de detectar porque pueden involucrar a usuarios y a hosts comprometidos, en donde los criminales cibernéticos han evadido las defensas perimetrales utilizando credenciales legítimas para acceder a recursos corporativos. Estafas de phishing, ingeniería social y malware son tan sólo unas cuantas de las técnicas populares mediante las cuales estos criminales consiguen las credenciales corporativas de empleados. IntroSpect utiliza inteligencia mediante aprendizaje de máquina y automatiza la detección de estos ataques, proporcionándoles a los equipos de seguridad y de operaciones de red visibilidad anticipada. Los modelos de aprendizaje de máquina, supervisados y no supervisados, procesan grandes cantidades de datos con el objeto de establecer una línea base de la actividad de TI típica para un usuario, dispositivo, o sistema. Las desviaciones de estas líneas base frecuentemente constituyen la primera indicación de que se está gestando un ataque.

Tanto ClearPass como IntroSpect fungen como la solución de software de seguridad de Aruba y se pueden aplicar en forma individual o en conjunto en cualquier red a través de ambientes edge campus, de empresa distribuida, en la nube, o para IoT. El sobreponer las tecnologías Secure Core, ClearPass e IntroSpect de Aruba proporciona protección sin paralelo impulsada por analíticos en contra del panorama cambiante de amenazas de la actualidad.

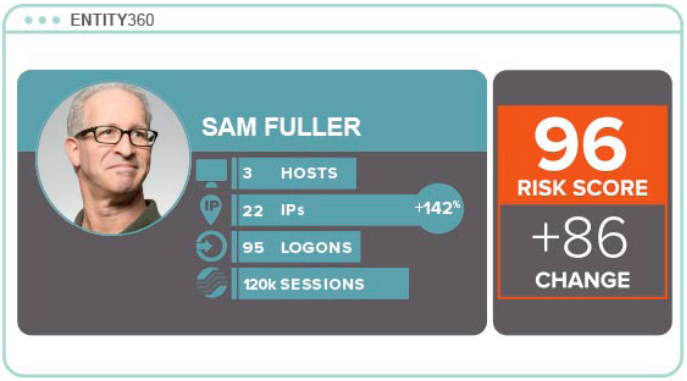

Figura 4: Detecte amenazas antes de que puedan causar daños con UEBA (User and Entity Behavior Analytics) de IntroSpect.

ARUBA SECURE CORE: INFRAESTRUCTURA DE RED SEGURA Y CONFIABLE

Durante más de 15 años, Aruba ha estado en el primer plano en la entrega de redes alámbricas e inalámbricas de alto rendimiento, altamente confiables y seguras – comenzando con access points y controladores inalámbricos y expandiéndose a switching de acceso y core. Como un proveedor de seguridad, Aruba ha introducido consistentemente innovaciones de vanguardia en las áreas de cifrado, seguridad física, acceso remoto y firewalls embebidos para asegurar que el tráfico de usuarios, de sistemas y de dispositivos es confiable. CISOs (Chief Information Security Officers) en todo el mundo han dependido del "arranque rápido" en seguridad que la infraestructura segura de Aruba proporciona.

ARUBA 360 SECURITY EXCHANGE: PROTECCIÓN ABIERTA, PARA MULTI PROVEEDORES

Una ventaja crítica de la solución Aruba 360 Secure Fabric es una integración abierta de múltiples proveedores para las soluciones de seguridad de Aruba, con más de 100 partners inscritos en el programa 360 Security Exchange. Los clientes pueden aprovechar sus inversiones existentes en seguridad integrando transparentemente productos provenientes de Exchange con las soluciones de Aruba. A diferencia de otros proveedores de infraestructura que obligan a sus clientes a actualizaciones costosas y a una sola fuente de productos, Aruba 360 Secure Fabric proporciona los mejores elementos de una solución unificada con la flexibilidad de una arquitectura abierta.

RESUMEN

Al trabajar en conjunto con partners en un ecosistema abierto para múltiples proveedores, Aruba Secure Core en la infraestructura Mobile First de Aruba, en combinación con la visibilidad y control de ClearPass y la detección avanzada de ataques de IntroSpect, Aruba 360 Secure Fabric proporciona 360° de detección y respuesta a ataques desde el edge al core a la nube – eso es lo que significa ser "Aruba Secure".

[1] Gartner Foundational Research Report, Actualizado el 9 de agosto de 2017, The Fast-Evolving State of Security Analytics

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