EL VALOR DE LA PLATAFORMA DE SEGURIDAD DE NUEVA GENERACIÓN: ANÁLISIS DEL MUNDO REAL

Greg Day
Vicepresidente y Director de Seguridad,
EMEA Palo Alto Networks

Resumen Ejecutivo

La combinación de los complejos entornos de TI modernos con un panorama de amenazas que evoluciona rápidamente generó a muchos negocios el problema de controlar los costos y a la vez proteger de forma efectiva los sistemas de los cuales dependen sus operaciones. En muchos casos, los desafíos se generan por la combinación de demasiadas soluciones de seguridad que no comparten el contexto y tiempo y/o experiencia insuficiente. Para abordar estos desafíos, las organizaciones buscan formas de consolidar su infraestructura de seguridad para (1) mejorar su postura de seguridad y (2) reducir su costo total de propiedad.

Presentamos Nuestra Plataforma de Seguridad

La Plataforma de Seguridad de Nueva Generación de Palo Alto Networks® le permite fortalecer su negocio con un motor de software de paso único que proporciona un conocimiento completo del contexto de la aplicación, el contenido en ella, y el usuario. Cuando nuestra plataforma ve por primera vez el tráfico de la red, el software de paso único inmediatamente determina tres elementos cruciales que impulsan su política de seguridad: la identidad de la aplicación, sin importar el puerto; el contenido, ya sea malicioso o no; y la identidad del usuario. Con estos tres elementos como base de su política de seguridad, puede reducir la impronta de las amenazas, prevenir ataques y asignar políticas a los usuarios. Para complementar la arquitectura de paso único y habilitar la consolidación del funcionamiento de seguridad, existe una metodología de políticas basadas en zonas. En lugar de adherirse a límites DMZ de "confianza/desconfianza" estrictos, las Zonas de Seguridad permiten la creación de grupos lógicos de interfaces físicas, VLANs y direcciones IP. Una vez creadas, cada zona es protegida por políticas de firewall de modelos de control positivo que dictan lo que se permitirá o no La Plataforma de Seguridad de Nueva Generación permite a las organizaciones:

- **Reducir la impronta de amenazas.** Clasificar todo el tráfico, en todos los puertos, todo el tiempo. Hoy, las aplicaciones, y el contenido asociado, pueden evitar fácilmente un firewall basado en puertos con una variedad de técnicas. Nuestra plataforma de seguridad aplica de forma nativa múltiples mecanismos de clasificación al flujo del tráfico para identificar aplicaciones, amenazas y malware. Todo el tráfico se clasifica, sin importar el puerto, cifrado (SSL o SSH) o técnicas evasivas empleadas. Las aplicaciones sin identificar, generalmente un pequeño porcentaje del tráfico pero de alto riesgo potencial, se categorizan automáticamente para su gestión sistemática. Con un modelo de control positivo, un diseño único de nuestra plataforma, se pueden establecer políticas basadas en aplicaciones o funciones y bloquear todas las demás (implícita o explícitamente) y, por lo tanto, reducir la impronta de amenazas.
- **Prevenir ataques conocidos y desconocidos.** Una vez que la impronta de amenazas se reduce al permitir aplicaciones específicas y rechazar todas las demás, la prevención de ciberataques coordinada puede aplicarse para bloquear sitios de malware conocidos y prevenir exploits de vulnerabilidades, virus, spyware y búsquedas de DNS maliciosas. Cualquier malware personalizado o conocido se analiza e identifica al ejecutar los archivos y observar directamente su comportamiento malicioso en un entorno sandbox virtualizado. Cuando se descubre un nuevo malware, se genera automáticamente una firma del archivo infeccioso y del tráfico de malware relacionado y se le envía a usted. Las políticas de prevención de amenazas se aplican únicamente a los flujos de aplicaciones específicas, no globalmente a puertos específicos.

- **Vincular políticas con usuarios.** Para mejorar la postura de seguridad y reducir el tiempo de respuesta ante incidentes, es crucial asignar el uso de aplicaciones a usuarios y tipos de dispositivos, y poder aplicar ese contexto a las políticas de seguridad. La integración con un amplio rango de repositorios de usuarios empresariales proporciona la identidad del usuario de Microsoft® Windows®, Mac® OS X®, Linux®, Android™ o iOS y el dispositivo que accede a la aplicación. La visibilidad y el control combinados sobre los usuarios y dispositivos significa que puede habilitar de forma segura el uso de aplicaciones que atraviesan su red, sin importar dónde esté el usuario o el tipo de dispositivo que usa. Establecer el contexto de aplicaciones específicas en uso, el contenido o amenaza que podrían llevar y el usuario o dispositivo asociado lo ayuda a alinear la gestión de las políticas, mejorar su postura de seguridad y acelerar la investigación de incidentes.

Reducir el TCO Con un Enfoque de Plataforma

Actualmente existe un número de herramientas que generan un retorno especulativo de las cifras de inversión basado en diferentes enfoques de la consolidación. Sin embargo, en un esfuerzo por elevar esta discusión de la especulación a la realidad observada, nos comunicamos con clientes existentes de Palo Alto Networks para probar la hipótesis de ahorro de costos de consolidación en base a su experiencia en el mundo real.

Durante mayo y junio de 2016, casi 150 clientes compartieron datos que demostraron reducciones en el gasto operativo y de capital como resultado de consolidar sus tecnologías de ciberseguridad con Palo Alto Networks. En promedio, estos clientes tienen 3,2 suscripciones implementadas con nuestro firewall de nueva generación. Este documento resume los resultados de la encuesta y enumera las razones por las cuales los clientes pueden lograr estos resultados con la plataforma de Palo Alto Networks.

Resultados de la Encuesta: Resumen

CAPEX: Hardware y Soporte

- 65 % de los encuestados informaron una disminución en la cantidad de eventos de seguridad que requieren intervención humana.
- Los clientes informaron que la reducción en el gasto de hardware incluyó, en promedio, un 20 % de ahorro y el porcentaje de organizaciones que ahorró se duplicó entre la primera, segunda y tercera suscripción implementada
- Una tendencia similar se presentó al analizar los costos de soporte. Sobre aquellos informes de reducción de gastos de soporte técnico, el ahorro promedio fue de 19 %.

OPEX: Gestión del Firewall

- Después de adoptar nuestro firewall de nueva generación, los clientes informaron una reducción promedio del 26 % en la cantidad de tiempo requerido para agregar nuevas reglas para gestionar sus firewalls, incluso el tiempo para asegurar que las nuevas reglas no generen conflictos con las existentes.

OPEX: Análisis de Ataques

- 65 % de los encuestados informaron una disminución en la cantidad de eventos de seguridad que requieren intervención humana.
- Los clientes que informaron una reducción en la cantidad de alertas que requieren intervención humana notaron un descenso promedio del 25 %.
- El 60 % de los clientes observó un descenso en el tiempo necesario para completar el análisis de los ataques que requieren intervención humana.
- En promedio, los clientes que informaron una reducción en el tiempo necesario para que un analista investigue un evento para generar una acción técnica para prevenir o bloquear un incidente vieron una reducción del 30 %.
- Los clientes que emplearon nuestros cuatro servicios con el firewall de nueva generación pudieron ahorrar más tiempo, de los cuales un 23 % vio más del 40 % de ahorro de tiempo para analizar los eventos que requieren intervención humana.

Estos resultados demuestran que, al consolidar sus tecnologías de seguridad con la Plataforma de Seguridad de Nueva Generación de Palo Alto Networks, los clientes logran un progreso significativo para reducir el costo total de propiedad de seguridad y a la vez logra mayor efectividad y eficiencia operacional.

¿La consolidación de tecnologías es la única razón por la cual los clientes pudieron lograr estos resultados? Si eso fuera verdad, las aplicaciones UTM podrían ofrecer los mismos resultados. Pero no pueden, porque la consolidación no es el único factor en juego. Específicamente, los clientes lograron estos resultados gracias a una plataforma integrada de forma nativa, no un montón de tecnologías de software vendidas en conjunto, y un foco firme en la prevención de brechas de ciberseguridad, en lugar de aceptar brechas como una realidad inevitable.

4401 Great America Parkway
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte: +1.866.898.9087

www.paloaltonetworks.com