Reducción de costes en herramientas de Seguridad

Problema

Las herramientas de seguridad son totalmente criticas para poder implementar las políticas definidas por el CISO de la organización de cara a defender los activos de información dela empresa. Lamentablemente, el numero de tecnologías de seguridad tiende al numero de vectores de ataque existentes, que no deja de aumentar, por lo que el CISO se acaba enfrentando siempre al dilema de como distribuir su presupuesto, muchas veces exiguo, para poder adquirir herramientas que tienen un elevado CAPEX, y peor aun, un mas aun elevado OPEX, normalmente asociado a actualizaciones de firmas, y que conlleva otro elevadísimo coste de recursos humanos para poder administrar los equipos. Es por ello critico poder reducir el coste de estas herramientas para disponer de presupuesto que hacer este malabarismo con los presupuestos

El principal parámetro por el que suelen dimensionarse estas herramientas es siempre el volumen de trafico que van a tener que tratar, que combinado con la necesaria amplitud en el perímetro de red a securizar, acaba siempre resultando en elevados costes de implementación. Poder reducir el ancho de banda que deberá tratar la herramienta, además de simplificar en la medida de lo posible la arquitectura de despliegue, hará que el proyecto sea mas atractivo económicamente

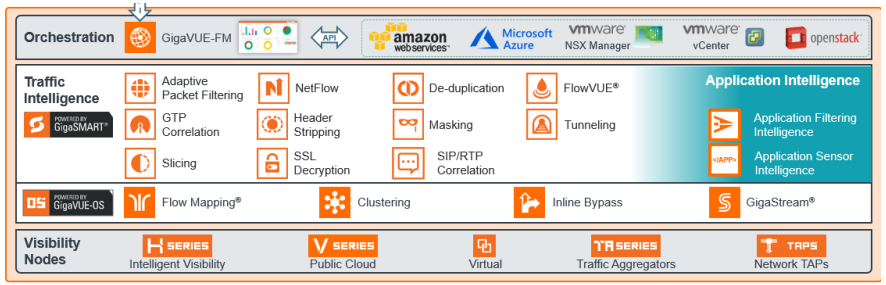
Solución

La combinación de soluciones de toda la suite de Gigamon va a permitir no solo simplificar los despliegues de las herramientas de seguridad, paradójicamente mientras se extiende la seguridad a las sedes remotas y entornos de virtualización, sino que además acaba siempre resultando en un importante ahorro en la propia tool de seguridad que se emplea

Las técnicas de reducción de costes son numerosas, pero enumerando las principales:

- Filtrado de trafico a nivel L2-3-4-7
- Generación de metadatos, que reduce drásticamente el volumen de trafico que se procesara
- Recorte de paquetes, para enviar a la tool solo las cabeceras necesarias para el análisis
- Recorte avanzado de paquetes, por el que se envían solo los primeros paquetes de una sesión, muchas veces suficientes para su análisis
- De duplicación de trafico de cara a enviar solo una vez una copia de todo el trafico que circula por la red
- Descifrado de SSL, para descargar de esa pesada tarea a las herramientas
- Tunelización, por la que se puede extender una herramienta centralizada a una red dispersa gegráficamente

Esquema



Licencia

Flow Mapping
Suite Gigasmart

LINK