

# Visibilidad para tráfico SSL

## Problema

Hoy en día más del 90% del tráfico Web en Internet está cifrado. De hecho, la noticia de que Google no indexará los sitios Web que no estén cifrados ha sido el detonante final para que deje de usarse el protocolo HTTP versus HTTPS: Sin embargo, esto conlleva que las empresas están perdiendo la posibilidad de tener la visibilidad necesaria del tráfico para el puesto de trabajo siendo imposible detectar amenazas en Internet. Por otro lado, los atacantes conscientes de hecho ya solo usan vectores de ataque con cifrado SSL para la mayoría de ataques conocidos, Command&Control, Criptolockers, etc.

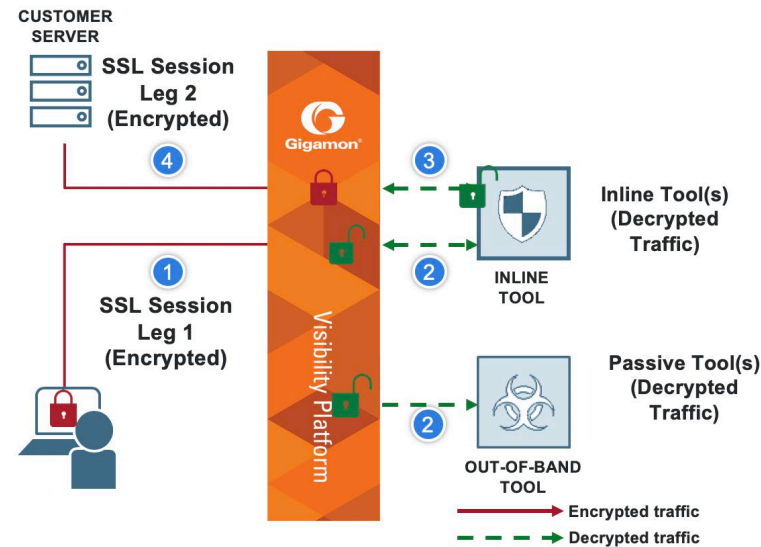
## Solución

Gracias a la solución de descifrado unificado de Gigamon, es posible tener visibilidad del tráfico saliente hacia internet aun cuando este esté cifrado mediante el uso de técnicas de MitM (Man-in-the-Middle).

Gigamon ofrece la posibilidad de descifrar SSL una única vez, para luego permitir que todas las soluciones de seguridad puedan ver el tráfico en claro y una vez securizado dicho tráfico se vuelva a cifrar hasta el destino final. Las características de esta solución comprenden:

- ✓ Solución unificada para herramientas en línea y fuera de línea.
- ✓ Selección de la versión de SSL desde TLS1.0 hasta TLS1.3.
- ✓ Soporte de RSA, DHE, PFS, ECC
- ✓ Protocolos de revocación: CRL y/o OCSP
- ✓ Detección de tráfico asimétrico.
- ✓ Uso de dos certificados, uno conocido y uno inválido para poder replicar el estado del certificado remoto.

## Esquema



Inline SSL  
OOB-SSL  
Flow Mapping  
Load Balancing

[LINK](#)