

Pre-Cryption

Problema

Antes de la adopción de la tecnología de Precryption, las organizaciones enfrentaban una problemática crítica relacionada con la falta de visibilidad en su tráfico de red cifrado. Este problema se extendía más allá de la simple incapacidad de inspeccionar los datos encriptados y tenía ramificaciones significativas en la seguridad y el cumplimiento normativo.

1.Dificultad en la Detección de Amenazas Ocultas: La incapacidad de ver el tráfico cifrado antes y después de la encriptación permitía a las amenazas avanzadas esconderse detrás del cifrado. Esto incluía ataques de malware encriptado, ataques de día cero y otros intentos de explotación que eran difíciles de detectar mediante métodos convencionales.

2.Aumento del Riesgo de Brechas de Seguridad: Con la creciente adopción de cifrado SSL/TLS para proteger la privacidad de los datos, las organizaciones se volvieron más propensas a ataques que aprovechaban el tráfico cifrado. Esto aumentaba el riesgo de brechas de seguridad, pérdida de datos confidenciales y daños a la reputación.

3.Desafíos en el Cumplimiento Normativo: La falta de capacidad para inspeccionar el tráfico cifrado obstaculizaba el cumplimiento de regulaciones de seguridad y privacidad, como el GDPR. Las organizaciones no podían cumplir con los requisitos de inspección y protección de datos en tránsito, lo que las exponía a posibles sanciones y multas.

4.Reducción en la Eficiencia de la Seguridad: La falta de visibilidad también impactaba la eficiencia de las herramientas de seguridad y análisis. Sin la capacidad de analizar el tráfico cifrado de manera efectiva, las herramientas de seguridad no podían operar a su máxima capacidad, lo que afectaba negativamente el rendimiento y la capacidad de respuesta ante amenazas.

Solución

La tecnología Precryption de Gigamon resuelve la problemática crítica de la falta de visibilidad en el tráfico de red cifrado mediante una solución técnica avanzada. Esta solución se caracteriza por su capacidad para capturar y analizar el tráfico en sus estados no encriptados y descriptados, proporcionando así una visibilidad completa y end-to-end. Precryption logra esto de manera eficiente al adquirir datos de tráfico antes de que sean cifrados en el servidor y después de que sean descriptados en el receptor, sin requerir una descriptación adicional en los dispositivos. Esto no solo mejora la detección de amenazas cibernéticas ocultas, sino que también preserva la privacidad de los datos al no requerir el acceso a las claves de cifrado.

Además, Precryption minimiza la sobrecarga al descentralizar la descriptación, lo que significa que no hay una carga adicional en los dispositivos V Series ni una necesidad constante de descriptar todo el tráfico en un solo punto. Esta descentralización reduce la complejidad de la infraestructura y garantiza un cumplimiento más sencillo de las regulaciones de seguridad y privacidad, ya que los datos sensibles pueden permanecer cifrados en la mayoría de los casos.

En resumen, Precryption de Gigamon ofrece una solución técnica avanzada que no solo proporciona visibilidad completa del tráfico cifrado, sino que también aborda los desafíos de rendimiento y cumplimiento al descentralizar la descriptación y preservar la privacidad de los datos sensibles. Esto permite a las organizaciones fortalecer su seguridad, detectar amenazas ocultas y cumplir con las normativas de manera eficiente.

Esquema



Licencias

VBL-BN-SVP

LINK