Gigamon®

Feature Brief

SSL/TLS Decryption

Powered by GigaSMART

Protect yourself against encrypted threats.

48% of SecOps teams cite they do not possess information on what is being encrypted in the network*

80% of enterprise traffic will be encrypted by 2019**

Key Benefits

- ✓ Expose hidden threats, malware, and data exfiltration, with support for modern crypto applications.
- ✓ Enhance security tools by centralizing SSL/TLS decryption and re-encrypt – creating a decryption zone.
- ✓ Scale by decrypting once and delivering traffic to multiple inline and out-of-band tools simultaneously.
- ✓ Increase performance with additional GigaSMART® modules.
- ✓ Help preserve data privacy compliance with policy-based selective decryption using whitelists, blacklists and URL categories.

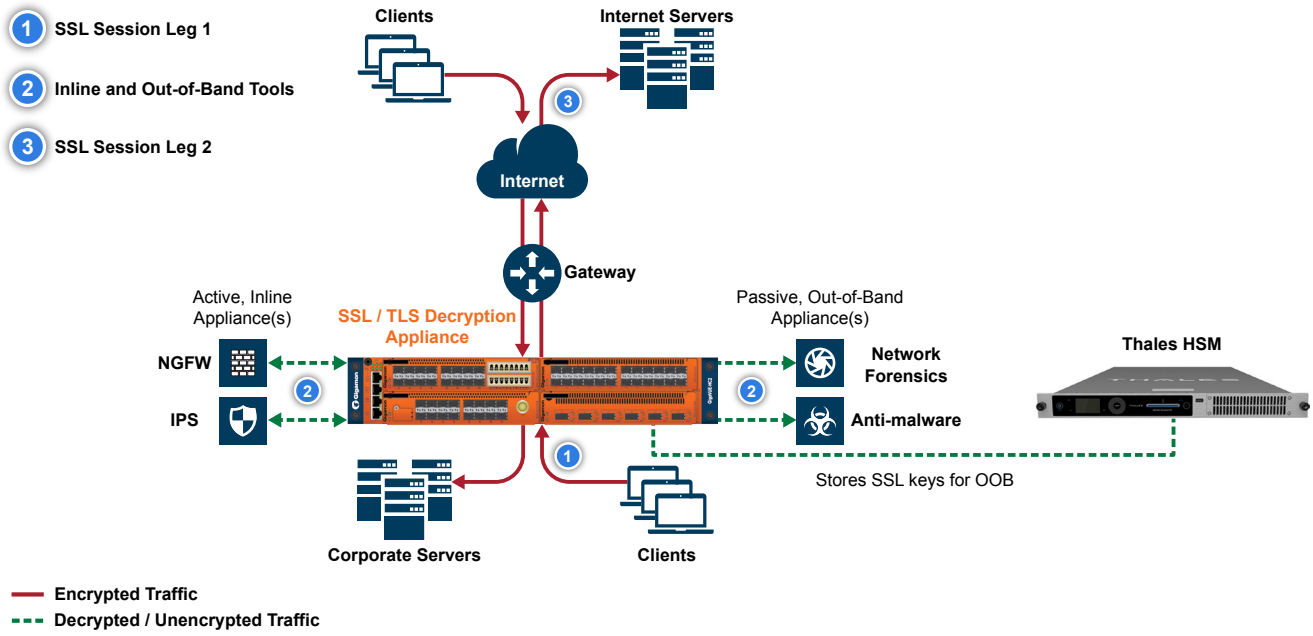
Scalable, Automatic Visibility and Management of SSL/TLS Traffic

Email, e-commerce, voice-over-IP (VoIP), online banking, file storage and countless other applications are secured with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption. The very technology that makes the Internet secure can become a significant threat vector by hiding malware and hindering network visibility.

GigaSMART SSL/TLS Decryption is a licensed application that enables SecOps teams to obtain automatic visibility into SSL traffic regardless of TCP port or application, so that they can monitor application performance, analyze usage patterns and secure their networks against data breaches and hidden malware in encrypted networks.

- **Improve analytics efficiency.** Leverage hardware performance accelerators in GigaSMART modules to decrypt, forward traffic to the appropriate tools and then re-encrypt.
- **Scale as your needs increase.** One instance of SSL/TLS Decryption in a Gigamon visibility node cluster is sufficient for any port in a cluster to take advantage of SSL/TLS decryption. Increase SSL/TLS decryption throughput by adding more GigaSMART modules.
- **Help protect data privacy and compliance.** Selectively decrypt traffic based on your own policies using a variety of parameters to help ensure that sensitive data remains secure.
- **Simplify your auditing process.** Fields within the payload can be masked to hide them from identification and in out-of-band mode decrypted packets can be sliced to remove irrelevant or private payload data so that private data is never stored, read or analyzed.
- **Increase the resiliency of your security and monitoring capability.** With Inline Bypass, in the event of a tool failure, traffic can be redistributed to the remaining healthy tools.
- **Strengthen your organization's security posture.** Validate server certificates against certificate trust stores and check for invalid certificates with Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP).
- **Store your decryption keys centrally.** The GigaSMART out-of-band decryption capability can access SSL decryption keys that your organization has stored centrally in a Hardware Security Module (HSM).

*Source: "Hide and Seek: Cybersecurity and the Cloud," by independent market research company, Vanson Bourne (May 2017).
**Gartner Predicts 2017: Network and Gateway Security



SSL/TLS decryption deployment with GigaSMART technology

Technical Features

Features	Specifications		
Products Supported	GigaVUE-HC1	GigaVUE-HC2	GigaVUE-HC3
Hardware Required	At least 1 GigaSMART module		
Software Required	GigaSMART SSL/TLS Decryption license		
Interfaces Supported	1 and 10Gbps	1, 10 and 40Gbps	10, 40 and 100Gbps
Number of Categories Supported for Selective Decryption (e.g. Finance, Government, Healthcare, Gambling)	83		
Inline SSL Decryption Throughput (per GigaSMART module)	2Gbps	3Gbps	12Gbps
Physical Inline Bypass Options	1 and 10Gbps	1, 10 and 40Gb	40 and 100Gb

Use Cases

Malware Detection
Analyze decrypted traffic for potential threats.

Data Loss Prevention (DLP)
Inspect decrypted traffic for potential data exfiltration and misuse.

Application Performance Monitoring (APM)
Monitor and assess SSL data used by business applications.

On-Premise Monitoring of Cloud Services
Inspect and monitor services running to and from the cloud, including web and Internet-of-Things (IoT) applications.

Enhance Existing Security Tools
Offload processor-intensive decryption functions from security tools such as NGFW and IPS appliances to increase threat inspection effectiveness.

Ordering Information

To order inline or out-of-band SSL/TLS decryption capabilities, please refer to the data sheet specific to your Gigamon visibility node. Depending on your needs, you may want one or several rear or front GigaSMART modules and a license for inline, out-of-band or combined GigaSMART SSL/TLS decryption.

For More Information

For more information about the Gigamon Visibility Platform or to contact your local representative, please visit: **www.gigamon.com**

3220-09 08/18

Gigamon® 3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com