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.

Get automatic visibility into SSL/TLS traffic regardless of TCP port or application, so that you can monitor applications' performance, analyze usage patterns, and secure your network against malware hiding in SSL/TLS sessions.

- **Improve analytics efficiency.** Leverage hardware performance accelerators in GigaSMART modules to decrypt, forward traffic to the appropriate tools, and 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).

---

**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-encryption
- Scale by decrypting once and distributing to multiple inline security tools
- Increase performance with additional GigaSMART® modules
- Help preserve data privacy compliance with policy-based selective decryption

---

*2016 Trustwave Global Security Report
**Gartner Predicts 2017: Network and Gateway Security

© 2017 Gigamon. All rights reserved.
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 in the cloud, including web and Internet-of-Things (IoT) applications.

Next-Gen Firewall/IPS
Offload decryption functions to get the best of your firewall’s IPS and DPI capabilities.

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