DATASHEET

Fidelis Decryption®

A High Performance TLS Visibility Appliance

Use of encryption is widespread. Over 80% of internet traffic is secured over https using TLS[1]. While encryption enables much-needed data privacy and integrity, it also creates blind spots, allowing malware and trojans to bypass security controls and provides an encrypted tunnel to bypass advanced counter threat measures put in place.

The Fidelis TLS decryption appliance provides Man-in-the-Middle (MITM) decryption of TLS traffic to expose application protocol traffic and content to the enterprise security team for threat detection and response. Decrypting traffic increases ROI on existing security investments.

Fidelis Decryption® is the only solution that, when deployed with the award-winning Fidelis Network®, can extract the TLS session metadata as well as the decrypted application protocol and content. This additional visibility extends to the Fidelis Elevate platform, enabling users to quickly detect and respond even to encrypted threats.

Features

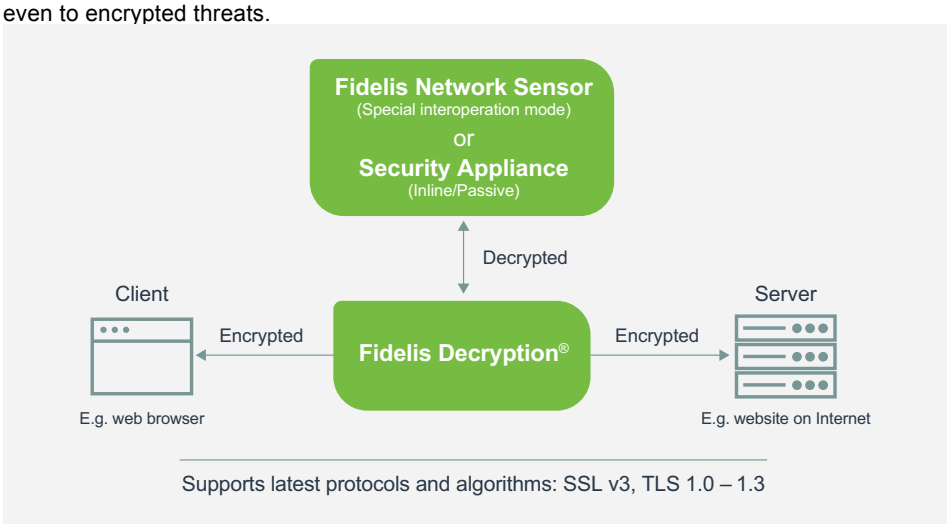
Visibility into Encrypted Traffic

The Fidelis TLS decryption appliance enables application protocol and content analysis for encrypted traffic, thereby removing any blind spots. It:

- Leverages high performance hardware accelerated TLS decryption and re-encryption
- Decrypts inbound and outbound encrypted traffic
- Stores server keys and certificates in disk encrypted using keys stored in FIPs-certified TPM (Trusted Platform Mode)

Comprehensive Protocol and Cipher Support

The Fidelis Decryption appliance has comprehensive protocol and cipher support to ensure full coverage of encrypted traffic.



Key Benefits:

- Removes blind spots by decrypting traffic
- Increases RoI on existing security investments
- Improves performance of existing appliance by offloading decryption
- Comprehensive protocol and cipher support

These include:

- TLS 1.0, 1.1, 1.2 and 1.3
- SSLv3
- AES-GCM, AES-SHA (128/256-bit keys), ChaCha20-Poly1035 cipher suites
- RSA and ECDH public key mechanisms
- Line rate performance

Decryption/re-encryption is performed at line speed. When forwarded to a security appliance, this line-rate facilitates malware and anomaly detection at near real time. The hardware appliance comes in 5 Gbps and 25 Gbps line speeds. And the VM appliance can process up to 1Gbps line speeds to match varying enterprise network needs.

Flexible Deployment Modes

The decryption appliance can be deployed in active inline mode. Once deployed, the decryption appliance can:

- Send decrypted traffic to one or more security appliances in passive or inline mode for investigation (traffic is automatically load balanced when sent to more than one appliance)
- Bypass with expernal packet brokers should a need arise (e.g., in the event of power failure)
- Work seamlessly with a Niagara bypass switch (inline deployment mode)

[1] https://letsencrypt.org/stats/#percent-pageloads

Granular Policy and Security Compliance

A policy-based traffic steering technology provides flexible and granular control over decryption to meet data privacy and compliance requirements.

- URL database for category-based decryption (optional additional subscription required)
- Block traffic by specifying drop (silently discard packets) and reject (actively close connection) rules
- Bypass decryption based on SNI, IP range, or other conditions including expired certificates

Easy Management, Administration, and Maintenance

The simplified management console is the one-stop shop to configure, manage, monitor, and maintain the decryption appliance.

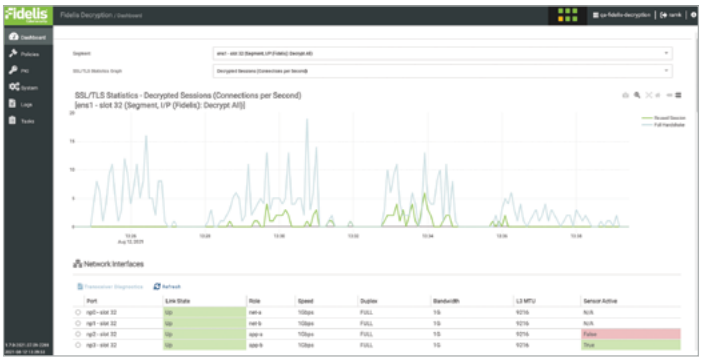
Configure System and Policies: Set up the appliance and chose the mode best fit (inline/passive) for your enterprise. Select policies to determine traffic to be decrypted (e.g. healthcare or financial data are typically not decrypted) or certificates and keys to be employed in the process.

Manage Certificates and Keys: Configure certificate authorities (internal/external), CRLs and SSH intercept keys. Generate self-signed CAs or import external CAs.

Monitor: Dashboard to easily monitor system, appliance, and traffic health.

Maintain: Backup/restore configurations. Restart services reboot appliance. Administer users.

Decryption Appliance Management Console



Appliance Specification — Hardware

	TLS-5G	TLS-25G
Form Factor	10 HPE Proliant DL360 Gen10 Chassis	10 HPE Proliant DL360 Gen10 Chassis
CPU	Dual Silver 4214R 12/24-core 2.4Ghz	Dual Gold 6248R 24/48-core 3Ghz
TPM	TPM 2.0	TPM 2.0
Memory	64GB	128GB
Storage Capacity and Configuration	300GB 2x HDD RAID-1	300GB 2x HDD RAID-1
Network Adapters	4x 1GbE 4x 1/10GbE 2x 1G/10GbE 6x SFP+ (Optical, multi-mode, 1G/10G)	4x 1GbE 4x 1/10/25GbE 2x 1G/10GbE 6x SFP+ (Optical, multi-mode, 10G/25G)
Out of Band Management	3-year ILO-HPE Advanced 24x7 Tech Support and Updates	3-year ILO-HPE Advanced 24x7 Tech Support and Updates
Dimensions	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)
Weight (approx.)	16.27 kg (35.86 lb)	16.27 kg (35.86 lb)
Power Supply	Dual hot-swap 800W High efficiency AC power supplies	Dual hot-swap 800W High efficiency AC power supplies
Operating Temperature	10° to 35°C (50° to 95° F) at sea level	10° to 35°C (50° to 95° F) at sea level
AC Input Requirements	100 – 120 VAC 200 – 240 VAC	100 – 120 VAC 200 – 240 VAC
BTU Rating (max)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)

Appliance Specification — TLS-1G VM

The table below specifies the minimum hardware requirements to achieve 1G decryption speeds with the TLS-1G VM appliance. Please note the peak capacity is based on commonly used cipher suites. Variation in cipher suite may impact peak processing capacity.

	TLS-1G VM
Hypervisor	VMWare ESXi 6.5 or newer
CPU Generation	Haswell equivalent or newer
CPU Cores	8
Memory	16GB
Disk	70GB

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com