

Symantec Technology Integration Partner: Fidelis Cybersecurity

Business Challenge

SSL encrypted traffic is pervasive in organizations around the world, representing 35% of all enterprise network traffic today. With a 20% annual growth rate, SSL encrypted traffic increasingly presents a blind spot in organizations; most current security solutions cannot see or manage this traffic or the threats that hide within. Advanced Persistent Threats (APTs) are increasingly using

SSL-based attacks, with Gartner predicting that 50% of all network attacks will be encrypted by 2017. Security tools such as Next Generation Firewall (NGFW), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Leak Prevention (DLP), security analytics and malware analysis devices are typically blind to SSL traffic or experience significant performance degradation if SSL inspection is enabled. A new approach is clearly needed.

Solution: Symantec SSL Visibility and Fidelis XPS™

Symantec's encrypted traffic management (ETM) solution eliminates the encrypted traffic blind spot and combats the security threats hidden in encrypted traffic while preserving privacy, policy and regulatory compliance. Comprised of the market-leading Symantec SSL Visibility, it enhances existing security solutions by providing visibility into previously hidden traffic and advanced threats without requiring significant upgrades or re-architecting the network security infrastructure.

SSL Visibility is a high-performance purpose-built solution that utilizes comprehensive policy enforcement to inspect, decrypt and manage SSL traffic in real time while ensuring data privacy and regulatory compliance. SSL Visibility's unique "decrypt once, feed many" design empowers multiple security tools, such as Fidelis XPS, with new-found visibility into

encrypted traffic to effectively detect and eliminate advanced threats without hindering device or network performance. The combination of SSL Visibility and the Fidelis XPS solution delivers best-in-class ETM to decrypt SSL traffic, uncover hidden threats, and eliminate these SSL blind spots.

Fidelis XPS provides Advanced Malware Protection, Data Theft Protection, and Network Security Analytics in a single, tightly integrated system for continuous protection across the enterprise. To combat the new threats and attacker techniques emerging every day, Fidelis XPS receives real-time actionable threat intelligence from proprietary research and data gathered from our industry partners. Combined with Symantec SSL Visibility, the Fidelis XPS solution delivers complete visibility, empowering security analysts to safeguard information and stay ahead of the adversary.



Partner: Fidelis Cybersecurity

Partner Product: Fidelis XPS Solution

Symantec Product: SSL Visibility



SSL Visibility is an integral component to an organization's encrypted management strategy, and provides visibility into SSL encrypted traffic without requiring the re-architecting of the network infrastructure. The SSL Visibility gives the Fidelis XPS solution visibility into all SSL traffic and applications to close the security visibility loophole created by encrypted traffic. In addition, it has the ability to selectively decrypt and inspect suspicious or unknown encrypted traffic while not inspecting other SSL traffic due to mandates such as HIPAA, SOX, PCI, Sarbanes-Oxley, and so on.

How it Works

The diagram below demonstrates how the Symantec and Fidelis XPS solutions work together to provide best in class ETM.

SSL Visibility provides decrypted content from SSL flows to the Fidelis XPS appliance. Based on its unique "decrypt once - feed many" design, the appliance can also simultaneously share its decrypted data with other existing security appliances already deployed in enterprise security stacks. This provides these complementary security appliances and applications with the necessary visibility into SSL traffic. This joint solution allows enterprises to easily add SSL visibility and inspection capabilities, along with category-based inspection policies into their existing network security architectures.

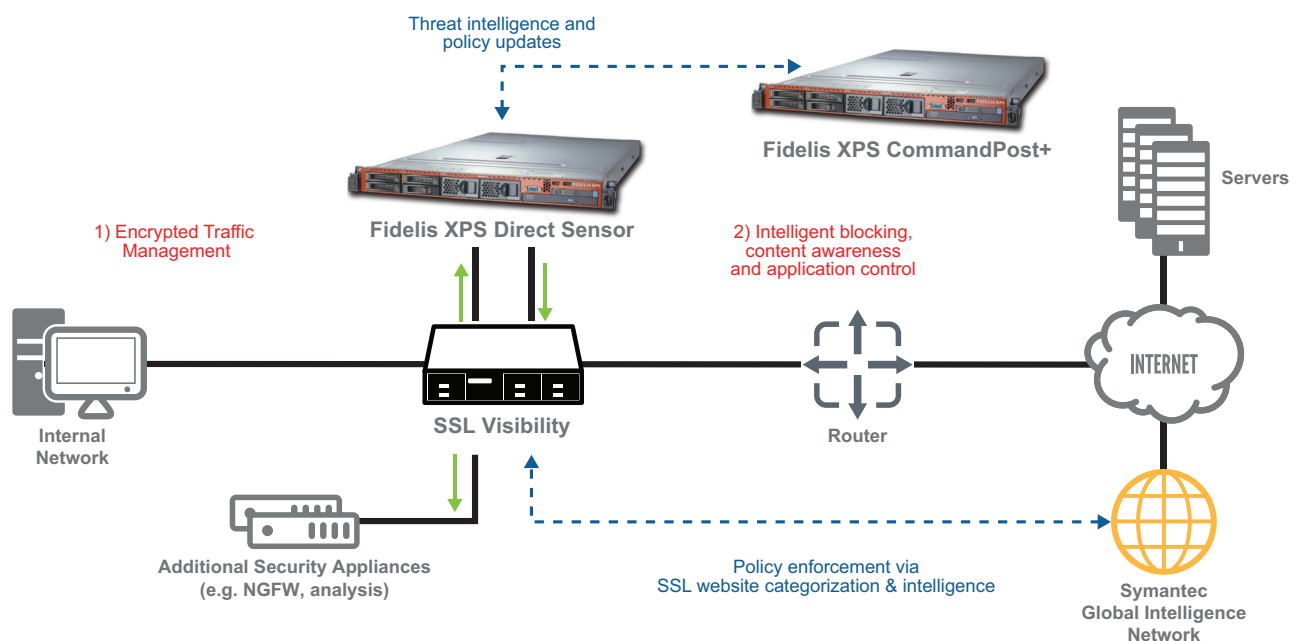
The Fidelis XPS platform uniquely leverages advanced threat research with the powerful correlation of security events and vulnerabilities. This joint solution leverages the capabilities of SSL Visibility to identify and decrypt SSL traffic with Fidelis XPS's ability to detect and eliminate SSL-based and other advanced threats to ensure optimal detection and response in managing threats across your network. To enable the Fidelis XPS solution to inspect decrypted traffic from the SSL Visibility, simply add port 443 to the "HTTP - tcp" service and other ports to the respective services that you want to monitor.

The SSL Visibility provides much needed enterprise visibility into encrypted SSL sessions – both inbound and outbound – and when combined with Fidelis XPS, the joint solution provides the highest level of enhanced visibility into content hidden using SSL/TLS protocols.

Benefits

The combined SSL Visibility and Fidelis XPS solution:

- Provides best in class ETM to detect and eliminate the SSL encrypted traffic blind spots
- Preserves privacy, policy and regulatory compliance
- Combats advanced cyber threats
- Integrates seamlessly with existing infrastructure





About Fidelis Cybersecurity

Fidelis Cybersecurity offers a comprehensive portfolio of products, services and expertise to combat today's sophisticated advanced threats and prevent data breaches. Our commercial enterprise and government customers around the globe can face advanced threats with confidence through use of our Network Defense and Forensics Services, delivered by a team of security professionals with decades of hands-on experience, and our award-winning Fidelis XPS Advanced Threat Defense products, which provide visibility and control over the entire threat lifecycle. To learn more about Fidelis Cybersecurity, please visit www.fidelissecurity.com.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Copyright © 2017 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.
#SYMC_sb_TechPartner_SSLVisibility_Fidelis_Cybersecurity_EN_v1a

