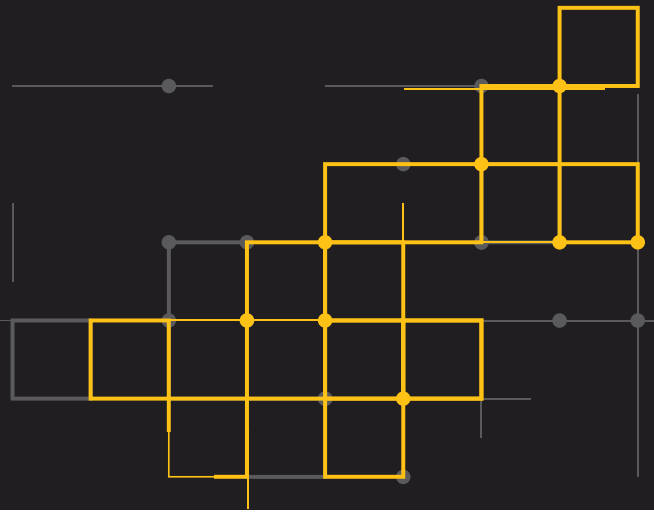# Symantec Technology Partner: ReversingLabs

Business Challenge

SSL encrypted traffic is pervasive in organizations around the world, representing 30-70% 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. At the same time, there is an overall growth in the sheer volume of network traffic with growing potential for malicious or questionable content often obfuscated to avoid traditional AV, behavioral and dynamic analysis solutions that are already unable to keep up with the file flow volume. This further compounds the problem.

Solution: Symantec SSL Visibility and ReversingLabs Network Security Appliance and Automated Static Analysis

Symantec's Encrypted Traffic Management solution eliminates the encrypted traffic blind spot and combats the security threats hidden in encrypted traffic. This provides a perfect complement to ReversingLabs N1000 Network Security Appliance and Automated Static Analysis engine, which can recursively unpack and de-obfuscate all of this network traffic (in/out/across) in near real time with the ability to scale to handle millions of files. Symantec SSL Visibility is able capture and decrypt SSL-encrypted traffic and pass to the ReversingLabs N1000 for processing and integration in downstream remediation workflows including SIEMs, as well as the ReversingLabs A1000 Malware Analysis Platform.

ReversingLabs has pioneered intrusion detection technology that enables deep file analysis of all payloads as well as support for detecting known, unknown, and zero-day vulnerabilities. By sitting before dynamic analysis solutions, ReversingLabs technologies can explore every binary on the network without regard to operating system, pre-execution, thus not tipping off the bad actors. This unique approach enables ReversingLabs to close the gaps left by traditional vendor solutions, as well as complement and enhance the value of the Symantec Encrypted Traffic Management solution.

Symantec SSL Visibility is an integral component to an organization's encrypted management strategy. Coupled with the ReversingLabs solutions to analyze and convict all network traffic, this combination provides a unique and scalable intrusion prevention solution.

Partner: ReversingLabs
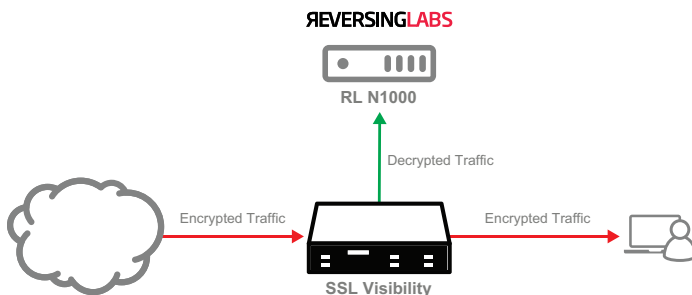**Partner Product:** N1000 Network Security Appliance and Titanium Core Automated Static Analysis
Symantec Product: SSL Visibility

REVERSINGLABS

✓Symantec™

How it Works

The diagram below demonstrates how the Symantec and ReversingLabs solutions work together to provide a unique solution for deep file content of all network traffic.

REVERSINGLABS

RL N1000

Decrypted Traffic

Encrypted Traffic   Encrypted Traffic

SSL Visibility

Symantec SSL Visibility provides decrypted content from SSL flows to the ReversingLabs N1000 Network Security Appliance and TitaniumCore Automated Static Analysis engine that recursively unpacks and de-obfuscates every contained file, identifying over 350 file formats and returning 3000 metadata information fields per file. These results can then be returned to the Symantec SSL Visibility for further processing/routing or other malware analysis solutions including the ReversingLabs A1000 Malware Analysis Platform.

Benefits

The combined SSL Visibility and ReversingLabs Automated Static Analysis:

- Decrypt all SSL/TLS network traffic
- Near real-time static analysis of all internal/external/lateral file traffic
- Complete unpacking of all payloads exposing true intent of contained files
- Expose 0-day threats based on static analysis and code functional similarity
- Roundtrip results to enhance post-processing remediation and learning

About ReversingLabs

ReversingLabs develops core technologies and solutions that drive Continuous Incident Response (CIR). Founded in 2009 and based in Cambridge, MA, ReversingLabs solutions are driven by three core and innovative technologies: Automated Static Analysis, the world's largest curated and private File Reputation Service and Code Functional Similarity Hashing Algorithm that drives malware conviction based on identifying known code segments being reused in new disguises.

ReversingLabs is an In-Q-Tel Portfolio company, originally funded to help close the gaps left by traditional AV, Behavioral and Dynamic Analysis solutions.

For More Information

Learn more about Symantec technology partners on our website.

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