Solution Brief

# Symantec Technology Integration Partner: cPacket

## Business Challenge

Organizations cannot protect against attacks they can't see or understand. While monitoring and analysis tools, such as cPacket Networks' Performance Monitoring Fabric (PMF), provide much needed visibility into the attacks that target organizations, they are still blind to threats hiding in encrypted traffic. Gartner has predicted that 50% of all network attacks will come through encrypted traffic in 2017. What's needed is a way to remove the blind spots and expose what's potentially hidden within all types of SSL/TLS encrypted traffic so organizations can effectively manage their risks and protect their assets.

## Solution: Symantec SSL Visibility Appliance and cPacket Performance Monitoring Fabric

To extend visibility into what's otherwise hidden, organizations can enhance their cPacket PMF deployment with the market-leading Symantec (formerly Blue Coat) SSL Visibility Appliance. The cPacket next-generation Network Performance Monitor (NPM) is enhanced by the capabilities of the SSL Visibility Appliance to provide advanced security, real-time high resolution network visibility, and analytics for all SSL/TLS encrypted traffic across the entire PMF.

**Partner:** cPacket

**Partner Product:** Intelligent Monitoring Fabric, Network Performance Monitor

**Symantec Product:** SSL Visibility

The SSL Visibility Appliance is a high-performance, dedicated solution that eliminates the blind spots created by SSL/TLS traffic to help combat the advanced security threats. It can be easily deployed to enable real-time inspection and management of SSL/TLS without having to upgrade or re-architect security infrastructure. Selectively decrypting traffic, based on policies, enables inspection from suspicious, risky or unknown sources, while leaving known privacy or compliance sensitive encrypted traffic untouched. This helps ensure compliance with the data privacy regulatory requirements of HIPAA, PCI, Sarbanes-Oxley and others.

The product's unique "decrypt once, feed many" design makes the decrypted traffic available to the PMF for real time complete packet inspection at Layers 2 through 7. It provides the highest resolution telemetry and scales at all network speeds.

Providing cPacket visibility into the encrypted traffic, organizations can strengthen their network security profile, as well as identify performance bottlenecks, by detecting and eliminating advanced hidden threats without impacting device or network performance.

# Organizations can benefit from multiple use cases, including:

## 1 Provides complete visibility into SSL/TLS traffic across the IMF

cPacket deployments are able to leverage the SSL Visibility Appliance to gain full visibility into encrypted traffic that would otherwise reduce the traffic analysis capabilities of the cPacket monitoring node, and other tools connected via cPacket's open architecture. Visibility ensures encrypted traffic isn't being used to:

a. Hide an attacker/botnet's command and control (C&C) channel or the use of unconventional ports to send stolen data home or download additional malicious code.
b. Masquerade sensitive data as normal traffic, using conventional ports, such as 443 or 80, to avoid detection by data loss prevention (DLP) systems.
c. Mask phishing and malware attacks to avoid detection by an intrusion detection or prevention system (IDS/IPS).

## 2 Eliminates asymmetric routing of traffic on conflicting interfaces and in high availability environments

Symantec can leverage the cPacket PMF as the convergence point for all network traffic feeds. This simplifies the deployment, as everything enters the SSL Visibility Appliance using a single interface. It also ensures the SSL Visibility Appliance sees both sides of the connection to facilitate proper inspection of the SSL/TLS flow. This is particularly useful in Active-Active High Availability environments, where incoming and outgoing traffic from the same feed traverse different links for redundancy.

## 3 Enables scalable SSL management in high capacity networks

Within high-capacity networks, multiple SSL Visibility Appliances may be needed to handle all the SSL decryption and inspection. The cPacket PMF can optimize and intelligently balance the traffic across multiple SSL Visibility Appliances, in a way that maximizes the bandwidth of each device, regardless of link speed or throughput capacity. This makes it easy to scale your SSL/TLS inspection and decryption infrastructure.

## 4 Ensures comprehensive traffic flow analytics and correlation capture and storage for intelligent forensics

Many organizations leverage packet capture recording devices to support compliance, forensic investigations, incident response, and troubleshooting. While most packet capture solutions record all traffic, limitations in processing speeds often require analysis to be completed after an incident occurs. cPacket PMF eliminates the delay, completing Layer 2 through 7 packet analysis in real time, at full line rate and selectively capturing only the relevant traffic. When the SSL Visibility Appliance is integrated into cPacket's Intelligent Forensic Recording, encrypted blind spots within the storage environment are eliminated.

## 5 Enables threat vector correlation of encrypted traffic

When perimeter threats are identified by security tools, such as next-generation firewalls (NGFWs), IDS/IPSes, and DLPs, organizations often need to obtain additional packet-based intelligence to better understand the nature of the threat. The SSL Visibility Appliance decrypts traffic and sends it for analysis to the cPacket PMF, which does real-time forensic searches and advanced behavioral correlation, base-lining and performance analytics to provide InfoSec teams the threat intelligence they need to understand what is going on in their network.

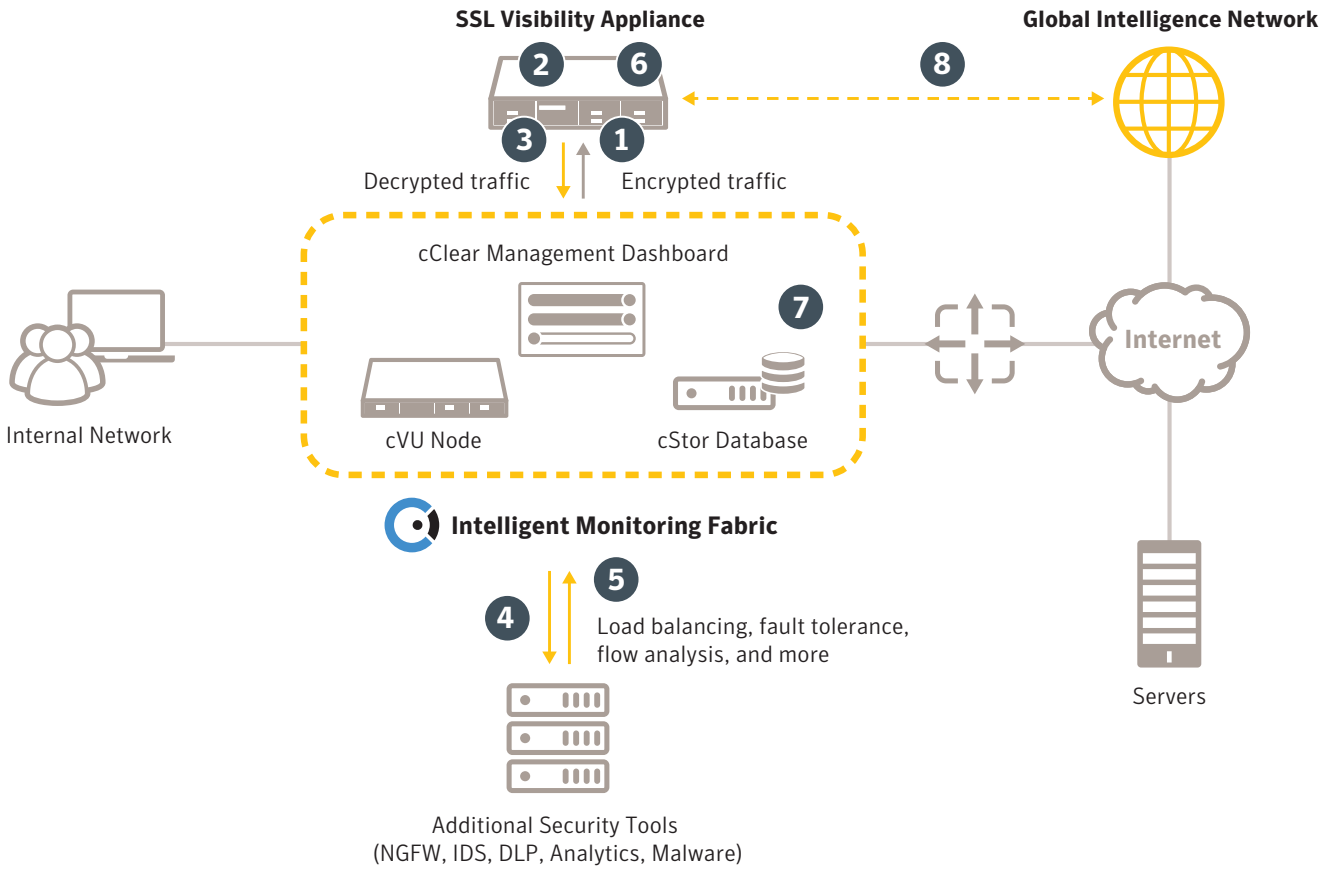
## 6 Network Performance Analytics context and the nature of threats

must be understood and as such data must be analyzed and cor-related from distributed locations with a high level of accuracy and synchronization in order to be useful and effective. cPacket provides the most accurate network telemetry presented in dashboards that allow you to quickly visualize changes or anomalies, or threshold based alert.

## How It Works

This diagram demonstrates how the Symantec and cPacket solutions work together to provide best-in-class encrypted traffic visibility, management, network analysis and forensic storage. The SSL Visibility Appliance enhances the PMF deployment, which consists of a cVu Monitoring Node, cStor Forensic Storage, and cClear Dashboard that can handle 1G/10G/40G network links, to provide a dynamic, flexible cost-effective solution for any network.

1. All SSL/TLS traffic is directed to the SSL Visibility Appliance by the PMF.
2. The SSL Visibility Appliance decrypts traffic, based on established policies.
3. Traffic is sent back to the cVu Monitoring Nodes. The nodes correlate the encrypted/decrypted traffic streams to ensure the decrypted traffic output is performing as expected and performs advanced Layer 2-7 wire speed packet inspection. The nodes also provide detailed network traffic statistics and troubleshooting alerts.
4. This provides connectivity to all other solutions within the security infrastructure that are connected to cPacket's open architecture, such as the NGFW, malware analysis, forensics, compliance, and DLP systems.
5. Traffic from security devices is sent back to cPacket.
6. Traffic is then sent to SSLV where is it re-encrypted.
7. Re-encrypted traffic is sent to its destination via cPacket.
8. The solutions work in concert with the Symantec Global Intelligence Network to determine whether encrypted network traffic should be allowed or prevented from going to and from external networks.



## Benefits

The combined Symantec and cPacket solution provides:

- **Ease of use:** enabling enterprises to easily add SSL visibility and inspection capabilities to their existing network security architectures.
- **Adherence to corporate and regulatory policies:** allowing the selective decryption of traffic, based on policies, to ensure data privacy and regulatory compliance with mandates.
- **Enhanced security:** eliminating SSL/TSL blind spots by ensuring decrypted network traffic is forwarded to all the security solutions connected to the PMF, and enhance their ability to uncover attacks and enforce security and compliance policies
- **Highest level of performance of accuracy and scalability:** both the Symantec SSL Visibility Solution and the cPacket Performance Monitoring fabric provide the highest levels of wire speed performance due to their unique architecture and hardware based approach.

## About cPacket

cPacket Networks offers customers that operate large complex networks an innovative Distributed Monitoring Architecture, which delivers higher operational efficiency and more integrated intelligence than legacy "bottleneck by design" centralized solutions. cPacket's distributed intelligence enables operators to proactively pinpoint imminent issues before they become problems that negatively impact end-users, and also to reduce troubleshooting time-to-resolution by over 80 percent. cPacket's advanced Intelligence overcomes scalability issues by leveraging the company's unique algorithmic chip that performs complete packet inspection "immediately at the wire" on the fly. The company's unique next generation network performance monitoring solution combines: dynamic maps visualization, granular key performance indicators, proactive alerting, interactive search (L2 - L7), and forensic packet-based analysis on-demand for unmatched integrated operational intelligence. Improving operational efficiency and being proactive enables customers to achieve substantial OPEX and CAPEX savings. Based in Silicon Valley, CA, cPacket solutions are relied on by the operators of the world's largest networks.

**Learn more about Symantec Technology Partners on our website.**

### About Symantec

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.

Symantec

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



SYMC_SB_TechPartner_cPacket_EN_v3d