

### Solution Summary and Proof Points

**Blue Coat SSL Visibility Appliance**  
*Inspect. Accelerate. Comply.*



Close the security loophole created by encrypted traffic.

#### WHY

- SSL use growing significantly in organizations worldwide – typically 25 –35% of all enterprise network traffic
- Increasing use of SSL as transport for Advanced Persistent Threats (APTs) – estimate of 80%
- Current security appliances need visibility into this traffic to mitigate threats

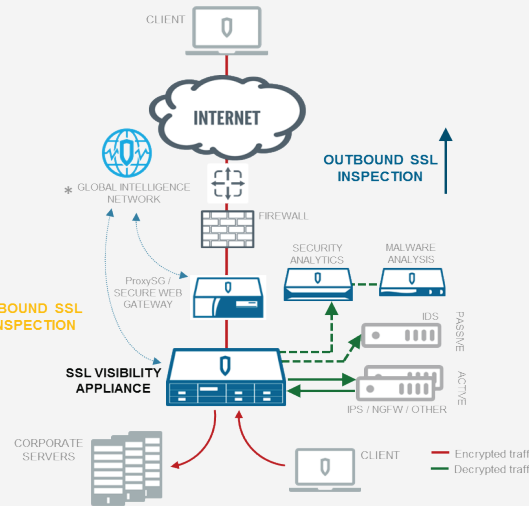
#### HOW

- Identify and inspect SSL traffic in real-time without hindering business critical application performance
- Empower multiple traditional security applications simultaneously such as NGFW, NGIPS, SIEM and DLP with visibility into encrypted traffic (*'Decrypt Once - Feed Many'*)

#### WHAT

- Key attributes:
- Unmatched industry-leading performance
  - Scalable interoperability with multiple security applications like NGFW, NGIPS, DLP, Analytics and Forensics
  - Complements and enables ATP solutions (e.g., Security Analytics, Malware Analysis)

### Comprehensive Encrypted Traffic Management



\*Host and Web categorization through the Global Intelligence Network is a subscription-based service

### Handling Objections

Scenario	Selling Strategies
Customers with malware solutions such as FireEye	<ul style="list-style-type: none"> <li>• Provides a simple method to identify previously hidden traffic and help block potential threats</li> <li>• Exposes advanced and unknown malware that utilizes SSL as a transport (i.e., Gameover, Zeus, SpyEye, ShyLock)</li> <li>• Enhances the customer's installed advanced threat detection and blocking investment</li> </ul>
Customers with forensics solutions such as our Security Analytics Platform or RSA's NetWitness	<ul style="list-style-type: none"> <li>• Provides a simple method to analyze previously hidden traffic and track potential threat behavior</li> <li>• Does not hinder the performance of business critical applications (i.e., VoIP)</li> <li>• Enhances the customer's installed network forensics and analysis investment</li> </ul>
Customers with NGIPS or NGFW	<ul style="list-style-type: none"> <li>• Enhance security by enabling other security appliances such as NGIPS or NGFW to have visibility into all encrypted traffic – including IMAP, FTP, POP and HTTPS</li> <li>• Adheres to the ProxySG's web policies on what to decrypt, or use its own policies when utilizing Blue Coat Host Categorization service</li> </ul>
Objection	Response
We already have SSL traffic management on our NGFW / NGIPS / DLP	<ul style="list-style-type: none"> <li>• While some security appliances and applications provide SSL decryption and encryption as an additional feature, once enabled, it reduces performance significantly as throughput, and even manageability, is sacrificed</li> <li>• As encrypting and decrypting is a very CPU-intensive task, current research states significant performance degradation of appliances, often by up to 80%, which often means effectively doubling the network traffic inspection spend</li> <li>• Offload SSL processing and let complementary applications focus on their security strengths</li> </ul>
Our organization doesn't use SSL encryption	<ul style="list-style-type: none"> <li>• In the current state of business, this may not be true as countless commonly used applications now utilize SSL/TLS encryption as a standard means of communication: Gmail, Google Docs, Facebook, Twitter, Salesforce, Yahoo, LinkedIn and Evernote have all moved – or are in the process of moving – to encryption as a standard for their communication and messaging tools</li> </ul>

### Key Differentiators and Strategies

The SSL Visibility Appliance is an integral component of an organization's Encrypted Traffic Management strategy – enabling acceptable use policies and a comprehensive architecture that protects assets, mitigates risk and addresses regulatory compliance.

#### Unmatched performance

At over **10x the performance** of competitors, supports visibility into up to 4Gbps SSL traffic, 400,000 concurrent SSL flows and up to 11,500 SSL flow setups / tear-downs per sec

#### Enhances Existing Security Investments

Supports a variety of both inline and passive security appliances. This enables decrypting once and then providing data to many analysis, action or logging.

#### Comprehensive, Real-time Threat Intelligence

Global Intelligence Network with timely automatic updates to SSL Visibility Appliances, ProxySG and PacketShaper solutions with world-class malware research



#### Supports an Advanced Threat Protection Lifecycle Defense

An integral component of Blue Coat's comprehensive lifecycle defense with – the SSL Visibility Appliance, ProxySG, Content Analysis, Malware Analysis Appliance and the Security Analytics Platform with ThreatBLADES.

### Market Landscape and Challenges

**Encrypted communication is exploding**

- Business applications are rapidly evolving and using encrypted communications by default. Modern applications such as Yahoo, Gmail, Google Docs, LinkedIn – as well as Cloud-based Software-as-a-Service (SaaS) offerings such as Salesforce.com – increasingly utilize SSL/TLS as their foundation
- Today’s Enterprises use encrypted traffic for 25–35% of their communications. For some industries such as healthcare, the amount of encrypted traffic can approach 70%!
- Search Engine and Social media applications represent 43% of SSL/TLS traffic on the internet
- Market research estimates that encrypted traffic will continue to grow at 20% annually

**Advanced malware is increasingly using encryption to bypass security tools**

- SSL is increasingly used by cybercriminals to circumvent detection and distribute malware, hide commonly used “Command & Control” channels as well as hide data exfiltration
- Recent publicized corporate breaches at global retailers and financial institutions were due to SSL-based attacks, utilizing malicious trojans such as Zeus, Gameover, Cridex, ShyLock and SpyEye

**Current security tools are insufficient**

- While some Next-Generation Firewalls (NGFW) and Intrusion Prevention Systems (NGIPS) offer SSL traffic decryption and inspection options, it is rarely enabled due to drastically reduced performance
- Market research estimates that less than 20% of organizations with a FW, IPS or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic as it reduces the overall performance of the appliance, often by more than 80%

**Organizations are looking for a better solution**

- An evolved ‘defense-in-depth’ approach is needed that will complement and enhance organizations’ existing network and security investments, while not disrupting current architectural models nor hinder business critical application performance

### Customer Needs and Ideal Solution

**What if you had...**

**Market-leading Performance**

- A purpose-built, high performance solution that provides visibility into all encrypted traffic types regardless of the TCP port or application
- Encrypted traffic management at over 10x the performance of competitors

**Investment Protection**

- Complete interoperability with your existing network and security application investments
- Ability to utilize the full potential of your dedicated security products, such as NGFWs, NGIPS, DLP, analytics and more – without re-architecting your network

**Defense in Depth**

- Ability to easily add encrypted traffic visibility and management into your organization’s network
- A policy-based enforcement solution that provides granular control of encrypted traffic
- Ability to share decrypted traffic with multiple active and/or passive devices simultaneously (i.e., “Decrypt Once - Feed Many”)

### Blue Coat Benefits Spotlight

**Comprehensive Encrypted Traffic Management**

**Unmatched Encrypted Traffic Policy Enforcement**

- See and manage **all** encrypted traffic types regardless of the application or TCP port (e.g., HTTPS, SPDY, IMAP, POP, FTP)
- Establish comprehensive policy-based on SSL traffic parameters and web categories
- Connect with and utilize collaborative, global threat intelligence through the Global Intelligence Network comprised of 75 million users in 15,000 enterprises worldwide.

**Integration with Firewall (NGFW), Intrusion Detection (IDS) and Prevention Systems (NGIPS)**

- Complement and optimize existing security application / appliance deployments and offload their SSL processing
- Provide decrypted traffic visibility to multiple active and/or passive devices simultaneously
- Allow these devices to readily detect and block malware hidden within encrypted communications

**Integration with Advanced Threat Protection (ATP) Solutions**

- Enhance ATP solutions from Blue Coat (e.g., Security Analytics, Content Analysis, Malware Analysis, ProxySG) and third-parties (e.g. FireEye, RSA NetWitness) with encrypted traffic visibility

<b>Qualifying Questions</b>	<p><b>Policy and Compliance</b></p> <ul style="list-style-type: none"> <li>Q What is your corporate policy on allowing/denying encrypted traffic?</li> <li>Q What visibility do you currently have into encrypted traffic?</li> <li>Q What processes have you put in place to manage a breach in your organization due to malware hidden within encrypted traffic?</li> <li>Q How do you define the potential consequences of a breach?</li> </ul>	<p><b>Architecture and Investment</b></p> <ul style="list-style-type: none"> <li>Q How are current security solutions utilized to control encrypted traffic?</li> <li>Q What performance issues occur when enabling SSL inspection for your current security devices?</li> <li>Q If you were to look at improving SSL visibility, how important is it that new solutions not require the re-architecting of your network?</li> </ul>	<p><b>Integrated Security</b></p> <ul style="list-style-type: none"> <li>Q How does your organization process your decrypted traffic today?</li> <li>Q What other security applications like forensics, malware analysis or reporting tools do you use to further inspect decrypted traffic?</li> <li>Q How well do your current solutions interoperate with other best-of-breed security solutions (e.g., Sourcefire, HP, PAN)? How important is that to you?</li> </ul>
-----------------------------	--	--	---