7 modern security problems

you can solve with encrypted traffic management

As the use of SSL/TLS encrypted communications grow, so does risk due to hidden threats. In response, enterprises are deploying Next-Gen Firewalls (NGFW), Intrusion Prevention Systems (IPS), Anti-Malware technologies and other solutions—but those measures can't uncover the malware inside encrypted traffic without slowing the network, adding complexity and increasing cost.

Only Blue Coat Encrypted Traffic Management (ETM) solutions cost-effectively boost the capabilities of network security infrastructure while effectively managing your SSL/TLS traffic.

Learn how Blue Coat ETM solutions help resolve challenges in your network security infrastructure:

1. Limited encrypted traffic visibility that enables data loss and exfiltration
2. Incomplete sandboxing that can't analyze all malicious threats
3. Inadequate intrusion protection that won't stop attacks
4. Weak network forensics that can't monitor and capture sophisticated attacks
5. Decentralized SSL decryption that adds complexity and cost
6. SL traffic inspection and decryption that really slows you down
7. Adhering to growing data privacy and compliance demands

1. Limited encrypted traffic visibility that enables data loss & exfiltration

Problems

- SSL/TLS traffic consists of more than HTTPS/Web/Port 443 traffic, as innovative Cloud and Mobile applications, as well as advanced malware, increasingly use different and non-standard ports.
- Data Loss Protection (DLP) and Data Theft Protection security tools are blind to data within SSL/TLS traffic, leading to great risk as well as policy and regulation non-compliance.

Solution

- Blue Coat ETM solutions eliminate the security blind spot by automatically seeing all SSL/TLS traffic regardless of port, application or service—without complex configuration or rule sets.
- Blue Coat ETM solutions intelligently feed devices like DLP technologies with decrypted and unencrypted traffic allowing them do their jobs more effectively to expose critical data movement.

2. Incomplete sandboxing that can't analyze all malicious threats

Problems

- Sandbox or Anti-Malware solutions are blind to encrypted traffic and cannot inspect, isolate, and detonate malware that is hidden within SSL/TLS.
- Your return on investment of sandbox solutions is hampered by SSL/TLS traffic—as these tools are less effective in stopping modern sophisticated Advanced Persistent Threats (APTs).

Solution

- Blue Coat's ETM solutions intelligently identify and control SSL/TLS traffic and feed both decrypted and unencrypted traffic to multiple security devices for total threat analysis and prevention.
- The Blue Coat SSL Visibility Appliance significantly increases the efficiency of Sandbox/Anti-Malware solutions in detecting and isolating APTs, while also preserving and extending their ROI by enhancing them with newfound visibility and analysis of formerly hidden threats.

3. Inadequate intrusion protection that won't stop attacks

Problems

- Most Intrusion Detection and Prevention solutions (IDS/IPS) cannot see and inspect SSL/TLS traffic—making them less effective in securing modern networks.
- As nefarious SSL-based Command and Control (C&C) communications are increasing rapidly, IDS/IPS technologies are blind to their inbound and outbound traffic containing dangerous malware and APTs.

Solution

- Blue Coat ETM solutions enable IDS/IPS to find and eliminate advanced threats hidden within SSL/TLS without hindering performance.
- The Blue Coat SSL Visibility Appliance preserves and extends the ROI of your IDS/IPS solutions by enhancing them with newfound visibility and control of formerly hidden network traffic and potential threats.

4. Weak network forensics that can't monitor & capture sophisticated attacks

Problems

- Network forensics tools cannot see, analyze or respond to threats hidden in SSL/TLS traffic—resulting in serious security blind spots and weak incident response.

Solution

- Blue Coat ETM solutions enable the prompt identification of suspicious network and attacker behavior and the remediation of compromised network assets regardless of whether SSL/TLS is used.
- The Blue Coat SSL Visibility Appliance preserves and extends the ROI of your Security Analytics / Network Forensic solutions by enhancing them with newfound visibility, complete analysis and faster response to formerly hidden network traffic and advanced threats

5. Decentralized SSL decryption that adds complexity and cost

Problems

- Incorporating a new SSL/TLS traffic management tool often requires you to add duplicate security devices or more hardware capacity to meet network performance needs
- This can be quite costly and difficult as it also requires you to re architect your network security infrastructure.

Solution

- The Blue Coat SSL Visibility Appliance scales to manage encrypted traffic on multiple network segments with active and passive devices on each segment, simultaneously.
- Using intelligent enforcement policies, the Blue Coat SSL Visibility Appliance provides inspected, decrypted and unencrypted SSL traffic to existing security appliances such as DLP, NGFW, IPS, malware analysis, network forensics and more.
- Existing security appliances get newfound and much needed visibility into SSL/TLS network traffic—and potential hidden threats-without degrading network performance or the need for significant, costly hardware capacity upgrades.

6. SSL traffic inspection decryption that really slows you down

Problems

- Security devices that may be able to see and inspect SSL traffic like NGFWs and IPS—suffer significant performance degradation up to 80% once SSL is "turned on." *
- Gartner research confirms this fact and indicates that "less than 20% of organizations with a firewall, an IPS or a unified threat management (UTM) appliance decrypt inbound or outbound SSL traffic." *

Solution

- The Blue Coat SSL Visibility Appliance supports up to 9 Gbps of SSL throughput and 800,000 concurrent SSL sessions—to support the most demanding enterprises.
- Blue Coat's "Decrypt Once and Feed Many" design scales to intelligently deliver decrypted and unencrypted traffic to multiple security tools like NGFW and IPS—significantly reducing configuration and operations time.
- The Blue Coat SSL Visibility Appliance preserves and extends the ROI of your NGFW/IPS solutions by enhancing them with newfound visibility and control of formerly hidden traffic and threats.

7. Adhering to growing data privacy and compliance demands

Problems

- Inspecting and decrypting certain types of SSL/TLS traffic violates data privacy and compliance regulations
- Not inspecting and decrypting SSL/TLS introduces risk due to the rise in innovative advanced malware that hides within encrypted traffic
- An "all or none" SSL decryption approach is unrealistic and impractical

Solution

- Blue Coat ETM solutions enable 'selective inspection and decryption based on a comprehensive policy engine–so you can decrypt the unknown and suspicious traffic, while allowing the "good", trusted traffic to pass through in its encrypted state.
- The Blue Coat Host Categorization Service utilizes the unrivaled, collaborative Global Threat Intelligence database for up-to-date threat, traffic and website analysis and categorization–ensuring your network security posture is responsive, using the latest security standards.
- Blue Coat ETM solutions ensure data privacy and compliance and make everyone happy—especially Legal, Compliance and HR teams.

Solve your security problems with Blue Coat ETM

When preparing your ETM strategy, keep in mind that any solution you implement needs to provide complete visibility into SSL/TLS traffic, while complementing and not replacing your existing security infrastructure. This solution must cost-effectively accommodate comprehensive policy enforcement and rapid growth on multiple fronts: corporate growth, increased adoption across the enterprise and, of course, the rapid growth of encrypted traffic. It's why Blue Coat ETM scales simply and efficiently to solve the problems caused by SSL/TLS traffic.

Learn more about the core capabilities and advantages of Blue Coat ETM at **bluecoat.com/uncoverssl**