BLUE COAT AND KASPERSKY LAB

BLUE COAT®

Blue Coat Content Analysis System (CAS), powered by Kaspersky security technologies, is a layered platform that offers you the best protection against known, unknown, and tar geted attacks.

Content Analysis System uses a cutting-edge, layered approach to protecting against known and unknown threats, and includes Kaspersky anti-malware technology as well as Kaspersky whitelisting. The fusion of these products provides the best malware protection against targeted attacks on the market today.

Together, they deliver superior performance and scalability, so you can protect against viruses, Trojans, worms, spyware, and other forms of malicious content.

Key CAS Benefits

The Content Analysis System's best-of-breed strategy allows Blue Coat to partner with visionary security vendors to offer superior protection. Leading network-based malware engines (such as Kaspersky Anti-Virus engine) can provide better protection than many desktop anti-malware solutions. Threat detection engines include checksum signature matching for known threats, behavioral analysis for proactive detection, and emulation mode for deep script and executable analysis.

The system can be configured to analyze both inbound and outbound traffic. The Content Analysis System provides best-in-class malware scanning with performance and security.

- Fewer appliances mean less management and rack space, providing a better ROI.
- Built-in investment protection with 4 & 5 yr. service contracts
- Best-of-breed architecture
- Innovative layered approach to security
- Integration with Blue Coat eco-system
- No tradeoff between security and performance
- They are equally suitable for secure high-speed Internet access and for protect critical data centers.

Kaspersky Whitelist Service

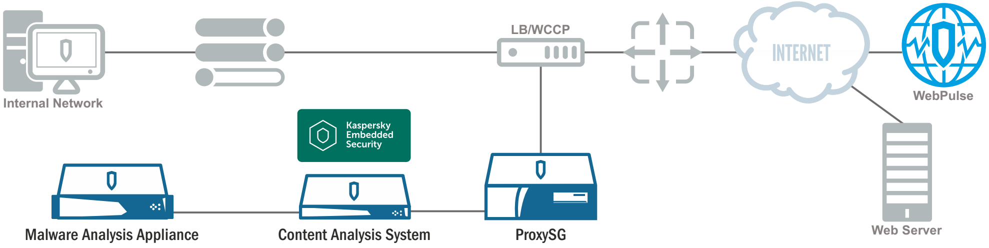
Kaspersky Whitelisting is a technology providing Blue Coat CAS with systematic knowledge of legitimate software. This enables Blue Coat customers to adopt the Whitelist Security Approach, allowing them to boost anti-virus performance and protect the users from targeted attacks. Whitelist database includes:

- Reputations of application files
- Advanced categorization of legitimate software
- Up to 96% of consumer software and 94% of corporate software coverage
- All-around information about the application files gathered by Kaspersky Security Network: Verdict, Software Category, Product name, Application signature, File popularity, etc...

BLUE COAT CONTENT ANALYSIS SYSTEM S400

BLUE COAT CONTENT ANALYSIS SYSTEM S500

Kaspersky® Embedded Security



Blue Coat Content Analysis System bridges the gap between prevention and incident containment.

Kaspersky Embedded Security inside.

Joint Solution Benefits

The joint solution produced by Blue Coat and Kaspersky Lab is fully optimized and provides the following benefits:

- Layered defense against all threats – cloud service + inline threat detection + web application and content controls + integrated data loss prevention + remote user protection
- A patented caching technology and special anti-virus architecture has been developed for high performance and low latency virus scanning
- Enhanced scanning performance and scalability in line with the requirements of large enterprises
- World's fastest response to new malware threats to defend against zero-day attacks with minimum false positives
- Maximum stability is guaranteed by Blue Coat scanning policy enforcement and is reinforced by Kaspersky best-in-class AV technology
- The cutting-edge Blue Coat Content Analysis System and Kaspersky Anti-Virus Engine together provide proven benefits to protect information and maintain productivity

Why Choose Kaspersky Lab?

Blue Coat CAS supports other two well-known anti-malware engines along with Kaspersky. So why should one choose Kaspersky? Here's why.

Kaspersky Lab is a premier developer of advanced and highly effective anti-malware products, ensuring that the users of this joint solution get:

- Comprehensive protection against all known kinds of internet threats
- Frequent (on average hourly) updates of malware signature DBs, ensuring optimum update frequency-to-content ratio
- Industry-leading zero-day protection (i.e., protection against malware that had only just appeared on the Internet), according to independent AV-Comparatives laboratory tests
- Very fast new threats response time – no more than 15 minutes in many cases
- Largest number (> 4000) of packers and archivers supported
- Faster scanning speed – up to 50% increase when compared with older joint Blue Coat / Kaspersky Lab solutions
- New signature databases: smaller DB size; better complex threats / rootkits detection; increased updates frequency
- Lowest false positives rate
- The joint solution keeps your malware inline detection at its best. These, in turn, combine with Blue Coat WebFilter on the ProxySG, for the ultimate Web gateway defense against today's multi-threaded malware attacks.