Blue Coat Content Analysis System (CAS)

AVANTEC
Competence. Security. Trust.

Block Known Threats with Advanced Threat Protection at the Gateway

With the Blue Coat ProxySG appliance and Blue Coat Content Analysis System, you can bridge the gap between real-time blocking of known threats and incident containment through the analysis and mitigation of unknown threats. The net result: your business can move beyond fear and start focusing on possibilities.

With the Blue Coat Advanced Threat Protection Lifecycle you can:

- Block known web threats
- Allow known good files
- Block known bad files
- Analyze unknown threats
- Update the Global Intelligence Network to protect against future attacks

A New Approach for Advanced Threat Protection

A new breed of hackers – including cybercriminals, nation states, hacktivists, and insiders – is perpetrating increasingly sophisticated, targeted, and effective exploits on enterprises. This shift in the threat landscape requires a new defense that combines prevention with more effective attack detection, preparedness and response.

Today, enterprises have a gap between their ongoing operations, where they detect and block known threats, and incident containment, where they analyze and mitigate zero-day threats and advanced or unknown malware. This gap exists because traditional malware analysis technologies cannot operationalize new threat intelligence discovered during incident containment across the security infrastructure.

This silo-style of defense inhibits the ability of the organization to continually fortify its defenses. The new strategic imperative for enterprises demands an integrated approach that can analyze advanced targeted attacks, zero-day threats, and unknown malware and provide that intelligence back to continually strengthen prevention defenses. The advantage for enterprises is immediate inoculation against all new threats.

Blue Coat: Bridging the Incident Containment Gap

The Content Analysis System combined with the Blue Coat Malware Analysis Appliance are critical components of the Blue Coat Advanced Threat Protection (ATP) solution. This combination, together with the ProxySG appliance, offers the most complete ATP solution in the marketplace for blocking known threats and analyzing day-zero and other advanced threats.

As part of ongoing security operations, the ProxySG appliance and Content Analysis System (with malware scanning and whitelisting) can block all known threats, sources and signatures and centrally analyze unknown content. The threat intelligence is shared locally between the ProxySG and the Content Analysis System as well as globally through the Global Intelligence Network to continuously fortify the security infrastructure.

Zero-day threats are automatically escalated and brokered by the Content Analysis System to the Malware Analysis Appliance with dynamic sandboxing techno-logy. This offers a unique hybrid analysis solution inclu-ding the customizable IntelliVM virtualized sandbox to replicate production environments, and a bare metal sandbox emulator for accurate analysis and detection of VM-evasive malware. File filtering by the Content Analysis System mitigates the problem of 'false-positive' identification of malware, and improves sandbox efficiency by reducing the number of files sent for analysis by 37%.

Unlike other sandboxing solutions, information derived from the analysis of malware files is automatically shared with the ProxySG appliances and Content Analysis System, so future instances of the malware will be blocked at the gateway.

The solution is powered by the Blue Coat Global Intelligence Network, which creates a network effect by sharing threat intelligence with 75 million users in 15,000 organizations worldwide. The discovery of new malware, threats or malicious files is shared locally within your infrastructure and out through this global community for faster protection against advanced targeted attacks and zero-day malware.

AVANTEC AG ▪ Badenerstrasse 281 ▪ CH-8003 Zürich ▪ Tel. 044 457 13 13 ▪ Fax 044 457 13 14 ▪ info@avantec.ch ▪ www.avantec.ch

Blue Coat Content Analysis System (CAS)

AVANTEC
Competence. Security. Trust.

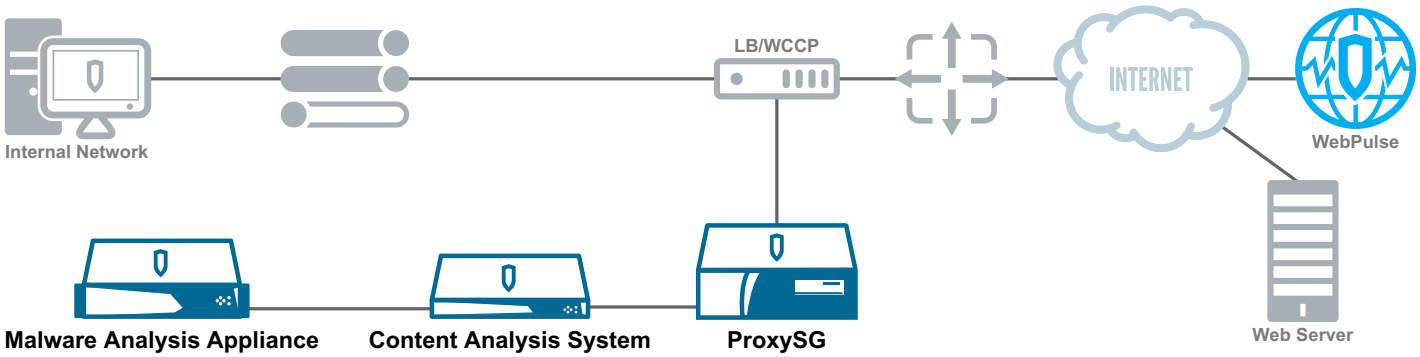
Blue Coat delivers advanced threat protection at the web gateway with the following products:

- **Blue Coat ProxySG Appliances:** The industry-leading web security gateway provides complete control over all your web traffic.
- **Blue Coat Content Analysis System:** This flexible system provides real-time malware scanning with up to two malware signature databases and file whitelisting. It also acts as a broker for Blue Coat and third-party sandboxing engines.
- **Blue Coat Malware Analysis Appliance:** This highly customizable malware analysis solution combines a virtualized environment and a bare-metal emulator to detect unknown malware and zero-day threats in an environment that replicates the systems on your network.
- **Blue Coat Global Intelligence Network:** This collaborative defense provides real-time analysis of content and shares new threat intelligence with customers worldwide to create a network effect that delivers faster, more comprehensive protection.

Summary: Benefits and Advantages

Blue Coat brings together the full range of products, services, and technologies needed to deliver advanced threat protection at the web gateway. The table below summarizes the business advantages of the Blue Coat solution.

Scalable, effective defense against advanced targeted attacks, APTs and zeroday malware	New threat intelligence is shared locally across the security infrastructure and globally across 15,000 customers and their 75 million users to turn unknown threats into known threats and shift protection to the gateway.
Defense in-depth against advanced threats	At the web gateway, combine real-time blocking and malware scanning, with application whitelisting and dynamic malware analysis
More comprehensive detection of zero-day threats	A customizable IntelliVM virtualized sandbox and a bare metal sandbox emulator deliver more accurate analysis and detection of VM-evasive malware.



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

AVANTEC AG • Badenerstrasse 281 • CH-8003 Zürich • Tel. 044 457 13 13 • Fax 044 457 13 14 • info@avantec.ch • www.avantec.ch