

COMPREHENSIVE WEB SECURITY AS A SERVICE

The Web Security Module of the Blue Coat Cloud Service provides market-leading web protection to organizations of all sizes without updating appliances, servers or user desktops. The Web Security Module is an Internet-delivered service that leverages Blue Coat's proven technology and collaborative, cloud-based community of over 70 million users to ensure real-time protection against known and unknown web-borne threats. With extensive web application controls and detailed reporting features, the Web Security Module enables administrators to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.

Reduced cost and complexity

Large and mid-sized enterprises must defend themselves against sophisticated web-borne malware, while reducing IT costs and boosting productivity for an increasingly distributed workforce. The Web Security Module of Blue Coat's Cloud Service allows customers to realize significant cost savings, eliminating the need to purchase, deploy and maintain on-premise hardware or software. Intuitive tools make it easy to create, enforce, and monitor effective web use policy. And because the service leverages a user-based subscription, customers pay only for what they need, and can seamlessly scale their web threat protection as required.

Real-time, dynamic malware protection

The Web Security Module delivers the best malware protection, using a combination of sophisticated, real-time web ecosystem analysis and inline malware scanning, including AV technology from leading vendors. Blue Coat's sophisticated web traffic behavioral analysis system inspects all parts of the web ecosystem to determine suspicious and malicious sites, and also examines malware-prone file types in detail. It even identifies "phone-home" or botnet traffic, enabling IT to quickly find and clean infected assets. By leveraging real-time web ratings and the web activities of millions of users in the WebPulse™ cloud community, the Web Security Module offers comprehensive web threat protection.

Market-leading web content filtering

The Web Security Module includes Blue Coat's comprehensive web filtering capabilities, which enable customers to achieve compliance by consistently enforcing their acceptable use policies. These features also allow IT to accurately filter web traffic by assigning multiple categories to any given URL, based on ratings from the global WebPulse user community.

Because static ratings of known web threats cannot protect against highly agile sources of malware, the service provides dynamic rating algorithms that identify and categorize web content in real time, ensuring the most up-to-date URL filtering. Blue Coat also maintains Blue Coat Labs to augment rating accuracy of web pages or domains.

Granular web application controls

The Web Security Module provides the industry's most effective controls for managing Web 2.0 applications, including the ability to control the use of leading social media applications such as Facebook, MySpace, Twitter, Flickr, YouTube, LinkedIn and more. IT can apply policies based on a wide range of criteria, including user, group, applications, postings, and media transfer controls:

- > Allow access to social media sites such as Facebook, but block specific activities within the site, such as gaming or posting.
- > Enforce SafeSearch and keyword search controls for all major engines, including media search engines.
- > Control whether users can send or receive messages and attachments for all major webmail services, such as Yahoo, MSN, AOL, and more.

IPSec VPN

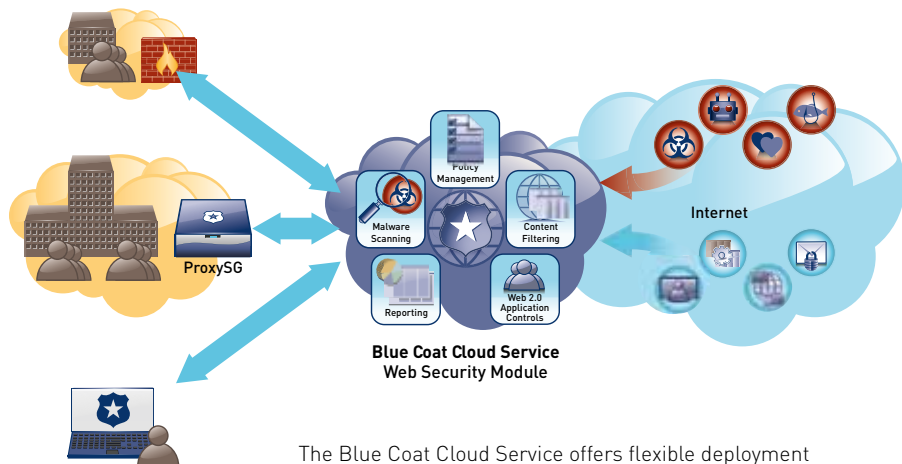
- > Users behind firewall; traffic forwards to service transparently.
- > Authentication agent on AD domain manager

Proxy Chaining

- > Forward from existing ProxySG, Squid or ISA
- > Authentication based on proxy

Desktop Agent

- > Client software forwards to service transparently
- > Authentication based on system credentials



The Blue Coat Cloud Service offers flexible deployment options for any size organization

Powerful, intuitive policy management and reporting

The Blue Coat Cloud Service incorporates industry-leading proxy and policy technologies, which have become the global standard for network security architectures. Administrators can quickly and easily enforce broad-based or detailed policies for network access and use – from small groups to hundreds of thousands of users – all in one simple configuration.

Through seamless integration with customers’ existing authentication systems, Web Security Module administrators can instantly report on web activity by user, group or across the organization. Organizations of any size can leverage the rich, enterprise-level reporting features of the Web Security Module, including dashboards, drill-down, and custom reports.

Flexible deployment options

The Cloud Service was architected to ensure flexibility and instant interoperability with existing network infrastructures. A simple configuration change to firewall, router, or proxy solution allows administrators to instantly protect and enforce Internet use policies for all users connected behind the device. An optional lightweight desktop agent ensures that roaming users are protected regardless of their location.

A web security service for any size business

The Cloud Service is built on a secure, high-performance, multi-tenant architecture. Data center deployment is geographically dispersed, with multi-network vendor locations and extensive redundancy. Individual components of the service are built on highly secure foundations.

As a testament to its reliability, the service infrastructure has been in production for over six years without a major outage, with over 70 million users regularly accessing it.

BENEFITS

Market-leading web threat protection and control

- > Sophisticated web intelligence and inline malware scanning
- > Identify and categorize new web content in real time with >99% accuracy
- > Manage Web 2.0 applications with granular controls

Reduce cost and complexity

- > No upfront costs – pay as you go
- > Integrates seamlessly with existing network infrastructure
- > Less downtime, higher user productivity
- > Service architecture provides infinite scalability

Easy to configure and manage

- > Quickly enforce policies for network access and use
- > Instantly report on web threats and user activity
- > Support cloud-only or hybrid deployment models
- > Transparent AD integration

Built on a robust, scalable infrastructure

- > Deployed globally on a purpose-built, multi-tenant architecture
- > Over 70 million users regularly access the service
- > In production for over six years without a single major outage
- > Backed by a guaranteed 99.999% uptime SLA

Connection Methods

IPSec VPN (Site to Site)

Proxy Chaining

Desktop Connector Agent

- Operating Systems
- Microsoft Windows XP (32-bit) with Service Pack 3 or later
 - Microsoft Windows Vista (32-bit and 64-bit) Service Pack 2 or later
 - Microsoft Windows 7 (32-bit and 64-bit)

- Minimum Hardware Requirements
- Must meet minimum operating system requirements for Microsoft Windows XP/Vista/Win7
 - x86 or x86-64 compatible processor
 - 100 MB of available hard disk space for software installation and logging
 - High-speed Internet connection (Ethernet or Wi-Fi network adapter required)

Supported Authentication Services

Active Directory

- Operating Systems
- Windows 2003 SP2 or later
- Minimum Hardware Requirements
- Must meet minimum hardware requirements for Windows 2003 SP2 and later
 - X86 or x86-64 compatible processor
 - 100MB of available hard disk space for software installation and logging
 - High speed internet connection