BLUE COAT

Security Empowers Business

COMPREHENSIVE WEB SECURITY AS A SERVICE

Blue Coat Cloud Service - Web Security Service

The Web Security Service, part of the Blue Coat Cloud Service, provides proactive web protection to organizations of all sizes without updating appliances, servers or user desktops. As part of the Security and Policy Enforcement Center, the Web Security Service offers proven technology as an internet-delivered service. It works with Blue Coat WebPulse™, the collaborative defense with over 75 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 Service 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 Service allows customers to realize significant cost savings by 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 Service delivers enterprise-grade malware protection using a combination of sophisticated, real-time web ecosystem analysis and inline malware scanning. 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. The Web Security Service is powered by the WebPulse collaborative defense, which provides real-time inputs from 75 million users for unmatched intelligence on global web activity. This intelligence is used to generate proactive malware defenses that identify and block malware before a user is infected.

Accurate and Relevant Web Content Filtering

The Web Security Service 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.

Granular Web Application Controls

The Web Security Service 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.

WEB SECURITY SERVICE

Control whether users can send or receive messages and attachments for all major webmail services, such as Yahoo, MSN, AOL, and more.

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 your existing authentication systems, Web Security Service 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 Service, including dashboards, drill-down, and custom reports.

Enterprise-Grade 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.

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 and operations with granular controls

Reduce cost and complexity

- Flexible cost mode – 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
- Backed by a guaranteed 99.999% uptime SLA
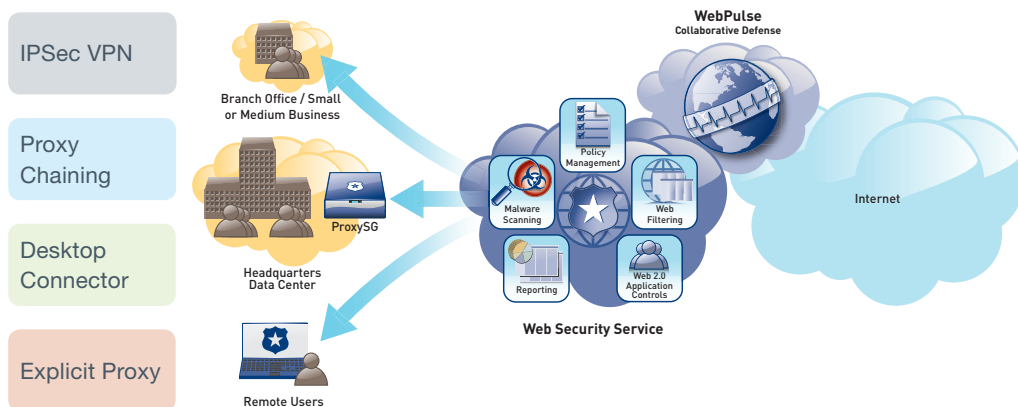
The Blue Coat Cloud Service offers flexible deployment options for any size organization

BLUE COAT

CONNECTION METHODS

IPSec VPN (Site to Site) – most IPSec-capable Juniper, Cisco and Checkpoint firewalls*

Proxy Chaining – from ProxySG, Squid, ISA/TMG devices*

Explicit Proxy

Desktop Connector	Operating Systems	Minimum Hardware Requirements

	• 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)
	• Apple Macintosh
	  › OS X 10.6 (Snow Leopard)
	  › OS X 10.7 (Lion)
		• Must meet minimum hardware requirements for Windows 2003 SP2 and later or Macintosh OS X 10.6 or later
		• X86 or x86-64 compatible processor
		• 100MB of available hard disk space for software installation and logging
		• High speed internet connection

*Refer to the Deployment Guide for details

SUPPORTED AUTHENTICATION SERVICES

Active Directory	Operating Systems	Minimum Hardware Requirements
	• Windows 2003 SP2 or later • Windows 2008 SP2 or later	• 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