BLUE COAT

Security Empowers Business

HOW MOBILITY AND BYOD ARE DRIVING MOBILE APPLICATION CONTROLS

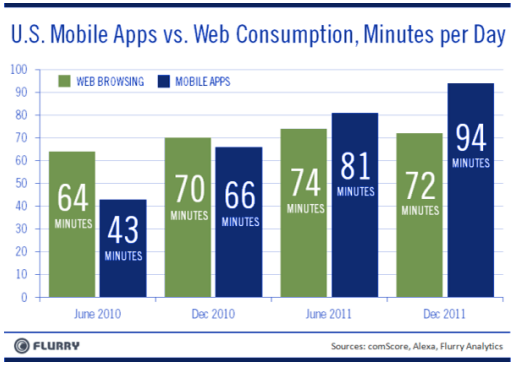
SOLUTION BRIEF

With the prevalence of tablets and smartphones, BYOD (Bring Your Own Device) has become commonplace in the work environment. Employees regularly connect personal devices to the corporate network. Mobile applications are increasingly used to enable the dynamic relationships and information-sharing that businesses use to stay competitive.

The problem is that applications like Facebook, IM, YouTube and others can be a drain on productivity and consume valuable corporate bandwidth. They can also expose your organization's network to malware and increase the probability of information loss. To mitigate these risks and maximize the value of mobile applications, your organization needs the ability to identify, monitor and report on them, and to implement granular controls over their use.

The Rapid Increase in Tablet and Smartphone Use

One study estimates that by 2015 the average U.S. citizen will have seven internet-connected devices. Another found that 40 percent of the devices that employees use to access business resources are personally owned. Given the proliferation of these devices interacting with the corporate network, it is an increasingly important function of the Secure Web Gateway to secure their access, enforce compliance, and protect users from web threats.



How Mobile Applications Bypass Web Controls

While web application controls currently in use offer significant granularity in controlling access to applications like Facebook, LinkedIn, and Webmail, they're not always effective in controlling them as mobile applications on iOS or Android. Many of these applications use alternate websites, servers and services for their functionality, leaving a potential gap in security and compliance for organizations that allow tablets and smartphones on their networks.

Facebook, for example, can be controlled in a web browser through web application controls. But Facebook on iOS or Android may use different websites, servers and services, and require different algorithms and detection mechanisms. For that reason, Blue Coat now offers mobile application controls that recognize and control applications on mobile devices, using the same policy engine, user controls and group controls available in its web application controls.

The Need for Web and Mobile Application Control Keeps Growing

Business use of Web 2.0 applications is growing exponentially. One study found that over 72 percent of companies in Europe and 88 percent in the U.S. will be increasing their social media spend by a median 10 to 25 percent in 2012.

The greatest growth is expected to be in customer service and engagement, as communications and marketing already rely heavily on these applications. Support for employees' personal use of Web 2.0 services is also becoming an imperative as the line between work hours and free time continues to blur.

To stay competitive in this swiftly changing landscape, your organization needs quick and flexible access to information and reliable connectivity between all stakeholders. Web 2.0 applications can help, but they present known risks. To mitigate those risks, and to maximize the value of Web 2.0 services, your organization needs the ability to identify, monitor and report on web-based applications and their mobile implementations – and implement granular controls over both of them.

BLUE COAT

Security Empowers Business

SOLUTION BRIEF

The First Step: Blue Coat WebFilter

Blue Coat WebFilter™ analyzes web pages or URLs and assigns them to one of more than 84 pre-defined categories.

WebFilter provides deep analysis ratings and granular categorization on approximately a billion daily web and application requests by leveraging Blue Coat WebPulse™, a collaborative defense with over 75 million users.

Leveraging dynamic input from this community, WebPulse can identify and categorize the most current and relevant web content in real time. The multi-dimensional URL categorization engine accurately assigns up to four categories to granular controls through the web and mobile application policy engine.

Next: Granular Application Controls

Application policies let you control the way users interact with web and mobile applications. For example: a policy can be used to prevent posting comments, uploading photos, downloading attachments, and other operations in either a web page or a mobile application. Blue Coat's application policy engine provides controls for well over 100 applications and counting. Blue Coat automatically processes new applications and operations through WebPulse, so that policies are automatically updated and enforced. Social networking applications supported by a Blue Coat policy include Facebook and MySpace, email applications like Hotmail and Yahoo Mail, blogging sites like Blogger, media sharing sites like Flickr, and other web-based applications.

Blue Coat allows you to take the information in the WebFilter database, such as Application Name (e.g. Facebook), Application Operations (e.g. Post Message), and Application Category (e.g. Social Networking) to identify applications and operations and create policy for end-users, groups or the entire organization. The application policy engine lets you create granular policies that control web and mobile application usage. This includes the ability, for example, to make Facebook a read-only application, or to prevent the download of potentially malicious webmail attachments – without denying access.

Monitoring and Reporting Are Essential

In addition to policy, monitoring and reporting are essential to measuring the effectiveness of policy and control. Blue Coat Reporter gives you the visibility you need to see into web and mobile application and operation usage on a granular level. Using Blue Coat Reporter, you can generate reports on web application usage and specific operation usage, such as commenting, uploading or downloading. This allows you to see the effects of a web and mobile application policy, in clear and concise reports with drill-down capability, before it's even implemented.

Blue Coat Provides Complete Protection

Blue Coat enables you to fine-tune web and mobile application activity for compliance and data loss prevention. Application policy also enables better management of the way employees use key applications such as webmail and social networking. Granular control of web and mobile applications helps protect the organization and saves valuable network bandwidth for business-critical activity.

Why Granular Controls Matter

Granular controls for web applications and their mobile counterparts give you the ability to control specific website operations – such as posting comments, uploading video or playing games – by user or by group. Granular controls, combined with web filtering and application-based policies, can help you maximize bandwidth, minimize risks, and adhere to corporate and regulatory policy.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000