Web Security Technology Overview

Cisco IronPort **Web Data Security and Data Loss Prevention**

Data security and data loss prevention (DLP) is a serious issue for companies, as the number of incidents – and the cost to those experiencing them – continues to increase. Whether it's a malicious attempt, or an inadvertent mistake, data loss can diminish a company's goodwill and reputation, reduce shareholder value, introduce legal liability, and put individuals and organizations at risk of financial theft.

As a leader in web security, Cisco® understands the complexities of creating a solution to address one of the most significant vectors for data loss: ubiquitous Internet access. Across all key network protocols, an intelligent, high-performance data security and DLP solution for the web and web applications is a must-have for today's organizations. Decision makers should look to vendors like Cisco with deep expertise in security and content scanning and select a best-of-breed solution that includes data security and DLP technologies – including integrating with external DLP solutions to enforce policies.

> "The increased use of Web 2.0 technologies such as blogs, social networking, and consumer-grade instant messaging increases the speed with which information moves outside of the enterprise."
>
> *– Andrew Jaquith, Senior Analyst*
> *Forrester Research*

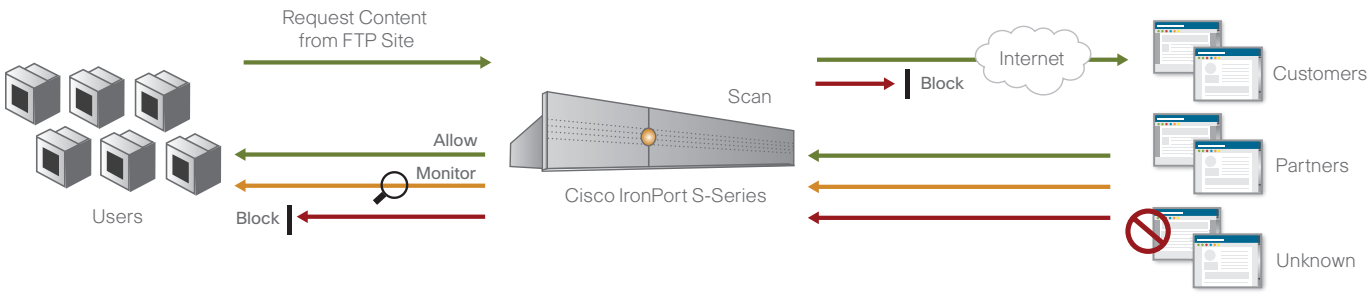
THE CISCO IRONPORT WEB DATA SECURITY SOLUTION

Data-stealing malware presents a real and imminent threat to business today, and is the starting point for any discussion on data security for the web. The Cisco IronPort web security appliance provides the best protection against data-stealing malware, using Cisco IronPort Web Reputation Filters, the Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine and the Layer 4 Traffic Monitor (L4TM). These technologies prevent Trojans and other malicious applications from entering the network, while blocking the "phone home" data connections from existing malware.

The data loss problem extends well beyond malware. Employees can easily use webmail to send a message including proprietary information, post confidential data on social networks and blogs, or transfer financial documents over FTP to a server outside the corporate network. Making sure that sensitive data does not leave the corporate boundary – while allowing users to leverage the full power of the Internet – is an important and challenging issue to solve.

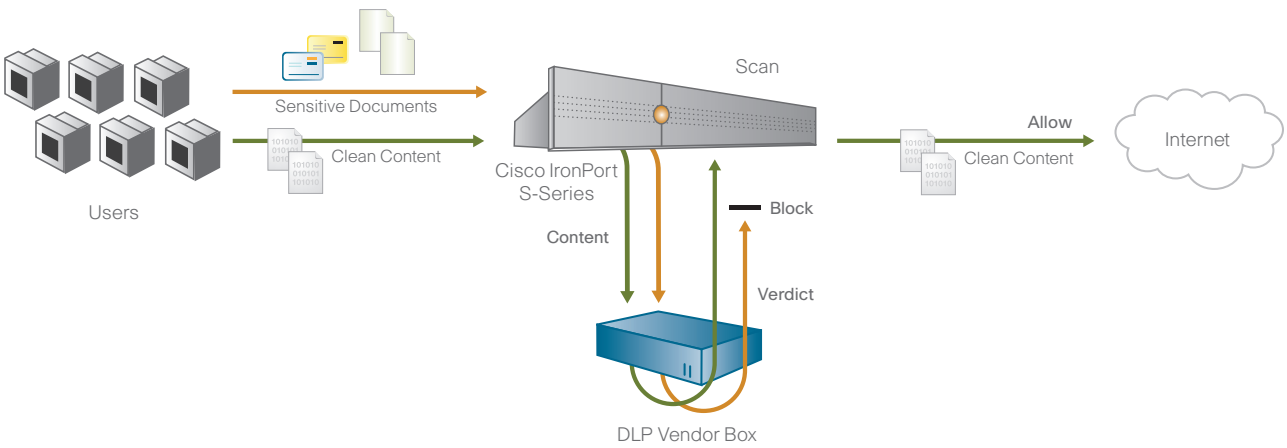
THE CISCO IRONPORT WEB DATA SECURITY SOLUTION (CONTINUED)

Cisco IronPort web security appliances enable organizations to take quick, easy steps to enforce simple, common sense data security policies. For example, preventing engineers from sending design files by webmail, blocking uploads by finance staff of Excel spreadsheets over 100KB, or preventing posts of content to blogs or social networking sites. These simple data security policies can be created for outbound traffic on HTTP, HTTPS and FTP.



Common sense data security policies are easily enabled and enforced with the Cisco IronPort web security appliance.

For enterprises that have already invested in special-purpose DLP systems, Cisco IronPort web security appliances offer the option to interoperate with DLP vendors via ICAP. By directing all outbound HTTP, HTTPS and FTP traffic to the third-party DLP appliance, organizations can allow or block based on the third-party rules and policies. This also enables deep content inspection for regulatory compliance and intellectual property (IP) protection, incident severity definition, case management and performance optimization.



Deep content inspection for HTTP, HTTPS and FTP traffic is enabled through integration with a third-party DLP appliance.

DATA SECURITY POLICY DEFINITIONS

With Cisco IronPort web security appliances, policy definition is intuitive and powerful – offering control over specific users, groups, locations, metadata, web reputation, URL category and applications (webmail, social networks, etc.). This high-performance system makes data security seamless and transparent.

Granular policy creation, using Cisco IronPort Web Security Manager, allows administrators to create and manage data security policies on a per-user and per-group basis – providing tremendous flexibility and control. Additionally, administrators can define groups using network segments, IP addresses, subnet or CIDR ranges. They can also combine multiple network segments or separate groups into a single unit.

DATA SECURITY POLICY DEFINITIONS (CONTINUED)

Comprehensive application, object and protocol filtering enables the configuration of granular controls. Administrators can choose to block or allow confidential data traveling through any application that uses HTTP or FTP. Object filtering (based on "true type") accurately recognizes objects to restrict downloads that present security and/or compliance risks. Cisco IronPort web security appliances also enable warn/continue pages – allowing an organization to educate users on corporate acceptable use and security policies.

Customized and localized notifications automatically alert end-users to policy violations that impact their Internet browsing and data-transfer activity. Administrators can enable system-determined notifications across more than 25 trigger events or choose to redirect to a separate customizable internal policy and notification page. The ability to customize notifications allows administrators to maximize the educational opportunity of blocked web content.

DEPLOYMENT OPTIONS

Sizing Up Your Web Security Solution

The Cisco IronPort web security product line address issues faced by organizations ranging from small businesses to the Global 2000.

Cisco IronPort S660	Suggested for organizations above 10,000 users.
Cisco IronPort S360	Recommended for organizations with 1,000 to 10,000 users.
Cisco IronPort S160	Designed for small businesses and organizations with up to 1,000 users.

SUMMARY

Cisco delivers high-performance, comprehensive data loss prevention for the web – helping organizations both large and small prevent leaks, enforce compliance and protect their brand and reputation. Cisco believes that a holistic solution for monitoring and enforcing data security across all communication channels, including the web, is vital to ensure the integrity of an organization's policies. Leadership within the Internet security market, together with its partnerships with industry-leading DLP vendors, puts Cisco in the unique position to offer a simple, easy-to-deploy solution for this critical functionality.

CONTACT US

How to Get Started

Cisco sales representatives, channel partners and system engineers are ready to help you evaluate how Cisco IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from these industry-leading products, please call 650-989-6530 or visit us on the web at www.ironport.com/leader.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.

435-0252-1 4/09