Solution Overview

# Cisco Web Security Appliance

## Data Loss Prevention Solution Overview

### Comprehensive, Easy-to-Deploy Data Loss Prevention Solution

Organizations in every industry have data—in motion, at rest, and in use—that they must keep safe from exposure. In particular, they must stop confidential customer data and intellectual property from leaving their network. In outbound Internet communications, data can be lost through many channels, such as webmail and FTP transfers. Inaccurately monitoring or controlling these channels leaves the organization with little or no visibility into the extent of its exposure and potential data loss.

Regulatory compliance continues to be the primary driver for enterprises to invest in data protection products. Beyond simply securing their data, organizations must comply with government and industry regulations designed to ensure information privacy. This means that organizations must focus on their regulation-driven needs to identify, locate, and control sensitive data. Most organizations don't know where their sensitive data resides in the network or where it crosses network boundaries. This blindness can lead to the unauthorized disclosure of confidential data, whether intentional or inadvertent.

Digital Guardian, a Cisco partner, offers a complete data loss prevention (DLP) solution. It uses content and context awareness to support complex use cases that involve intellectual property, trade secrets, customer lists, customer credit card information, and other data.

The Cisco® Web Security Appliance (WSA) with Advanced Malware Protection (AMP) is an all-in-one highly secure web gateway that offers broad protection, extensive controls, and investment value. It offers an array of competitive web security deployment options, each of which includes Cisco's market-leading global threat intelligence infrastructure. WSA offers an integrated approach to help disparate security point solutions to work together, to triangulate information for faster identification, and to more effectively mitigate and remediate threats.

Digital Guardian's DLP solution and Cisco WSA come together to provide a comprehensive, easy-to-deploy data loss prevention solution that helps you effectively monitor, control, and prevent sensitive data from leaving the network. The solution enforces policies to ensure protection over Web (HTTP/HTTPS), File Transfer Protocol (FTP), Secure Sockets Layer (SSL), and Web 2.0 applications such as webmail, blogs, and wikis.

## Why Organizations Need a Data Loss Prevention Solution

Many organizations use content-aware pattern-matching methods to protect outbound Internet communications such as email. However, they neither monitor nor control outgoing electronic communications through web and FTP access. Data loss through web and FTP access is considered a relatively minor threat, and it can go undetected or unresolved for days or even longer, creating the risk of confidential information falling into the wrong hands.

Organizations need a DLP solution for many reasons:

- More than 50 countries, including the United States and countries in EU, have enacted data protection laws that require organizations to demonstrate their compliance with government and industry regulations regarding information privacy. These regulations go beyond simply securing data. Failure to comply with them may result in civil and criminal penalties. A comprehensive DLP solution helps organizations comply with these government and industry regulations.
- Data breaches by employees pose a tremendous threat to efforts to prevent confidential data from leaving an organization. Organizations want to have 360-degree monitoring and control of data use across corporate and web emails, external file uploaders, social media, and other applications, including SSL-encrypted sessions. Deploying a comprehensive DLP solution will help them monitor and control the applications that employees access. It also provides historic data for forensic analysis in case of reported violations.

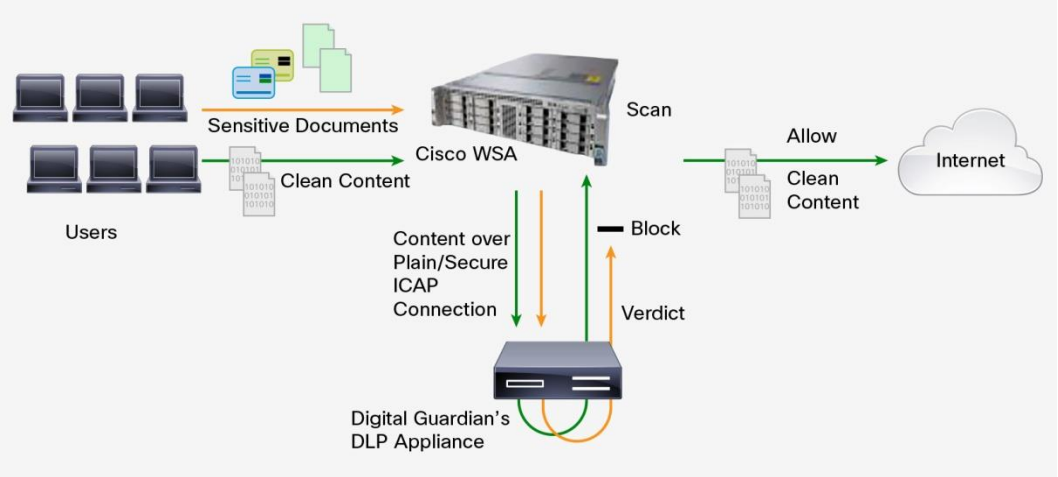
Whether it is intentional or inadvertent, data loss can diminish a company's brand, reduce shareholder value, and damage the company's goodwill and reputation. The exposure of sensitive information can result in fines, bad publicity, loss of strategic customers, loss of competitive intelligence, and legal action. Not only can a comprehensive DLP solution help an organization prevent a potential data loss, but it can also help the organization compete more effectively and protect the business from a financial loss.

## The Digital Guardian and Cisco DLP Solution

The Cisco and Digital Guardian DLP solution is a high-performance, comprehensive security solution for data in motion. The solution monitors and controls traffic sent using HTTP/HTTPS, File Transfer Protocol (FTP), or Secure Sockets Layer (SSL) as well as applications such as webmail, blogs, and wikis. The solution provides content and context awareness, shortens deployment times, and lowers the cost of ownership.

Cisco WSA communicates with Digital Guardian’s Network DLP appliance by means of plain or secure Internet Content Adaptation Protocol (ICAP). By directing all outbound HTTP, HTTPS, and FTP traffic to Digital Guardian's Network DLP appliance, you can allow or block the traffic based on the configured rules and policies. You can also conduct deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization (Figure 1).

**Figure 1.** Deep Content Inspection




## Key Features

- Monitors and inspects HTTP, HTTPS, FTP, and FTPS traffic for data violations
- Applies policies to monitor and block Web 2.0 applications, including wikis, blogs, and other applications
- Protects customers' and partners' sensitive and confidential data
- Monitors and controls webmail communications, including SSL-enabled sessions
- Helps enable deep content inspection to meet regulations such as required by the Health Insurance Portability and Accountability Act of 1996 (HIPPA), the Payment Card Industry Data Security Standard (PCI DSS) and protected health information (PHI)
- Enforces company policies for external communications to prevent accidental data disclosure
- Provides accurate content detection with fingerprint-based inspection
- Delivers full-featured protection with low administration overhead and extreme ease of use
- Shortens the time to deployment and lowers the cost of ownership
- Provides detailed activity logging and reporting for the correlation of all activities
- Provides historic data for forensic analysis in case of reported incidents of violation

## Conclusion

The Cisco WSA and Digital Guardian's data loss prevention solution delivers high-performance, comprehensive data loss prevention. It helps organizations of all sizes prevent leaks, enforce compliance, and protect their brand and reputation. A comprehensive data loss prevention solution for monitoring and enforcing data security across all communication channels is vital to the integrity of an organization's policies. Cisco's leadership within the Internet security market, together with our partnership with Digital Guardian puts us in a unique position to offer a simple, easy-to-deploy solution for this critical functionality. The solution can expand beyond data in motion to all areas of enforcement, including data at rest and data in use, to provide full integrity.

## About Cisco

Headquartered in San Jose, California, Cisco is the largest networking company in the world that designs, manufactures, and sells networking equipment. Cisco's comprehensive portfolio of advanced threat protection solutions reduces complexity and delivers superior visibility, continuous control, and advanced threat protection across the entire attack continuum. Cisco's network security portfolio is built on the concept that security should be embedded everywhere in the network, which goes beyond traditional walls and includes data centers, endpoints, web and email gateways, virtual systems, and mobile devices.

## About Digital Guardian

Digital Guardian is a worldwide leader in data loss prevention solutions. It offers a complete DLP solution that allows companies to effectively discover, monitor, control, and secure sensitive data, whether on the network, in use on desktops or laptops, at rest on end-user devices and network servers, or stored in the cloud. Digital Guardian's DLP solution provides the deepest visibility, the fine-grained control, and the industry's broadest data loss protection coverage to stop sensitive data from getting out of the organization.

## How to Get Started

Cisco sales representatives, channel partners, and system engineers are ready to help you evaluate how Cisco WSA and Digital Guardian's comprehensive data loss protection solution can make your corporate network infrastructure secure from unauthorized disclosure of confidential data. If you believe that your organization could benefit from this industry-leading solution, please call 650-989-6530 or visit us on the web at http://www.cisco.com/go/wsa.

## Cisco Capital

**Financing to Help You Achieve Your Objectives**

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

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.



Printed in USA C22-738537-00 02/17