



SBA

ENTERPRISE

BORDERLESS  
NETWORKS

# Cisco Data Security Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

Revision: H2CY10

# Using this Data Security Deployment Guide

This document is for the reader who:

- Has read the Borderless Networks for Enterprise Organizations Deployment Guides
- Wants to connect Borderless Networks to a Cisco data security solution
- Wants to gain a general understanding of the Cisco data security solution
- Has a level of understanding equivalent to a CCNA® certification
- Wants to protect sensitive intellectual property and customer data within the organization and prevent accidental leakage
- Wants to address data security compliance and regulatory requirements
- Wants to implement data security policies within the organization
- Wants the assurance of a validated solution

This guide introduces the Cisco data security solution. It provides details on how Cisco content security appliances work with RSA Data Loss Prevention (DLP) products to solve end-to-end data security problems. An overview diagram of the solution is illustrated in Figure 1.

This document is divided into the following sections:

**Business Overview**—outlines the business problems faced by enterprise organizations in the area of data security.

**Technology Overview**—provides details on data security system concepts and the important characteristics that the industry looks for when evaluating such solutions.

**Detailed Configuration**—discusses some of the best practices and the steps required to deploy the Cisco data security solution.

## Additional Information

This is a supplement guide to the Smart Business Architecture (SBA) for Enterprise Organizations (2,000 to 10,000 connected users) deployment guides. The SBA for Enterprise Organizations is a reference architecture that delivers an easy-to-use, flexible and scalable network with wired and wireless security.

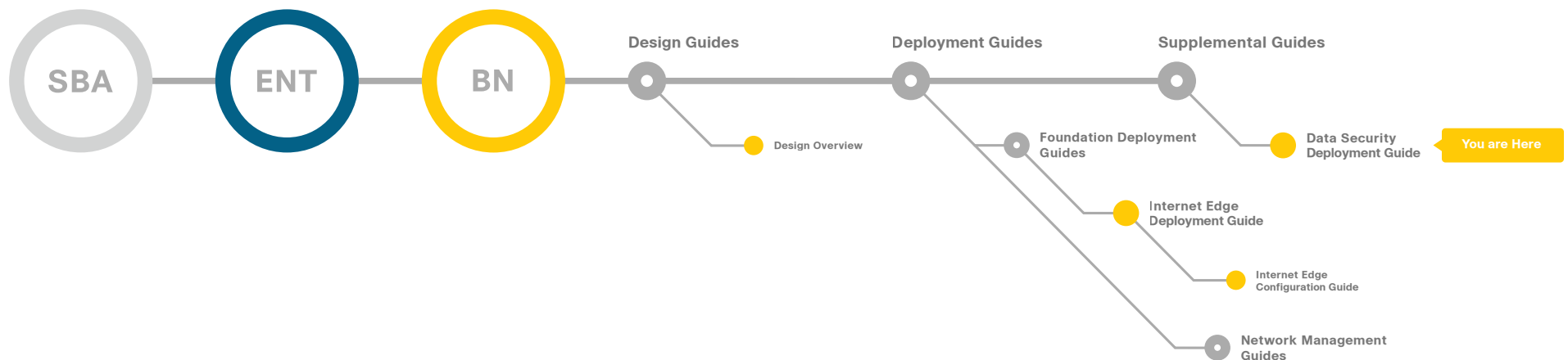
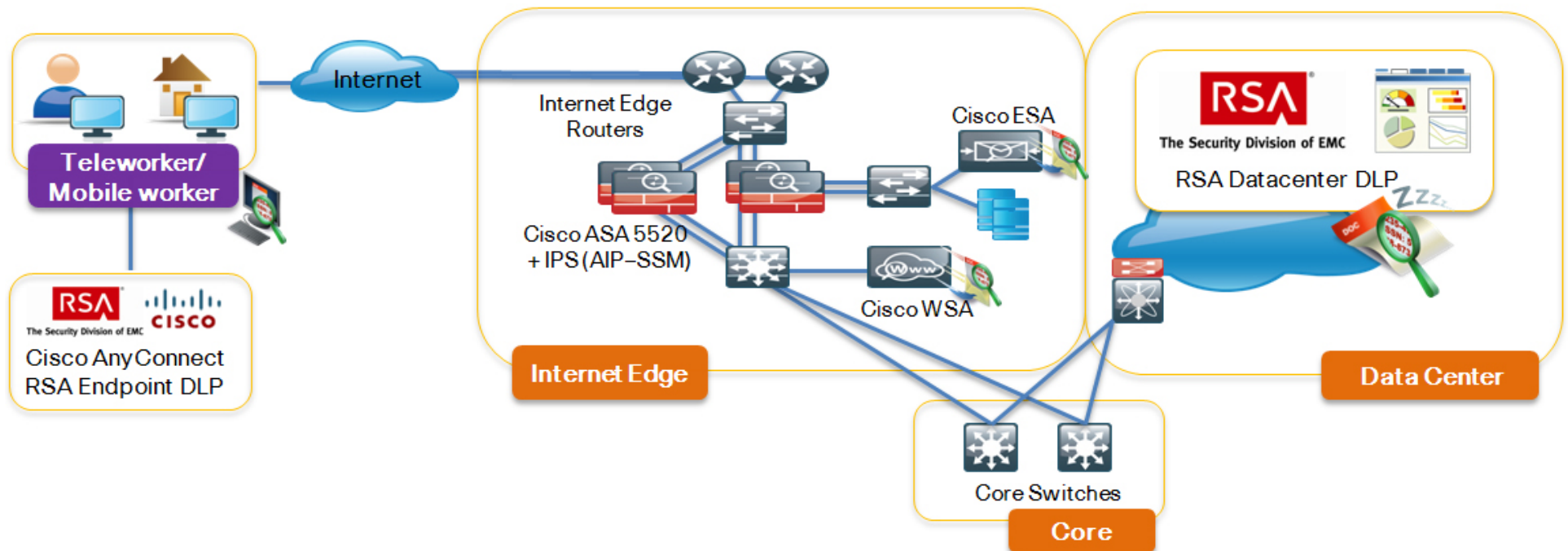


Figure 1. Solution Diagram



## Related Documents

Smart Business Architecture (SBA) for Enterprise Organizations (2000 to 10,000 connected users) deployment guides ([http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns982/landing\\_sBus\\_archit.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns982/landing_sBus_archit.html))

Internet Content Adaptation Protocol (ICAP)  
<http://www.faqs.org/rfcs/rfc3507.html>

Technology partner deployment guides can be found here:  
<http://www.cisco.com/go/securitypartners>



# Table of Contents

Business Overview .....	1
Technology Overview .....	2
Cisco Data Security Configuration Details.....	5
Endpoint Security.....	15
Datacenter Security .....	17
Summary .....	19
Appendix A: SBA for Enterprise Organizations Document System .....	20

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

© 2010 Cisco Systems, Inc. All rights reserved.

# Business Overview

Network borders are rapidly being eroded by the need to enable anyone, anywhere to connect to anything, at any time. Employees, partners, and customers are using mobile devices and applications to connect from homes, hotels, airport Internet kiosks, and local coffee shops, collaborating through mobile platforms, increasing business efficiency, productivity, and flexibility. However, enhanced communication also increases the risk of losing sensitive information, such as intellectual property and customer data, due to innocent or malicious activities.

Recently, multiple data loss incidents affecting large organizations have made headlines, resulting in negative media coverage and public embarrassment. In some cases, penalties and corrective actions have cost millions of dollars. Organizations must take steps to protect their intellectual property and sensitive customer data, and to comply with local, national, and international regulations that govern many different kinds of data.

Intellectual property is one of an organization's most important business assets; businesses lose billions of dollars each year from theft of trade secrets. Intellectual property can be lost through inadvertent disclosure, or through malicious action by an employee or an outsider.

Organizations need to protect customer data, including personally identifiable information (PII), credit card numbers (CCNs), Social Security numbers (SSNs), and other records. Sophisticated criminal enterprises are using botnets and malware to infiltrate organizations in order to steal this information. Breached companies often bear the costs of notifying customers and the public of a data loss incident, and may also have to bear remediation expenses.

International, national, state, and local regulatory requirements are increasing, especially for protection of sensitive information assets. Thousands of data privacy regulations have been created in recent years, and countries and states have enacted data-breach notification laws.

Organizations from different industries and operating in different countries are under mandates to comply with different regulations, such as:

- **Health Care**—EU Directive, PIPEDA, and HIPAA
- **Education**—FERPA, HIPAA, and possibly PCI-DSS
- **Financial**—GLBA, SOX, PCI
- **Retail**—PCI-DSS

To solve these data protection problems and meet regulatory requirements, a comprehensive and well thought out data security solution is essential.

# Technology Overview

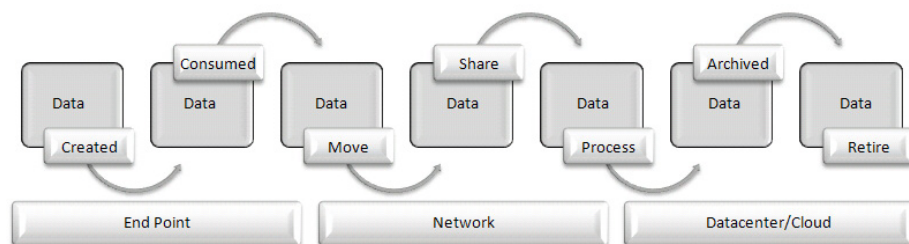
## Data Security

A data security solution identifies data based on its content and/or the context in which it occurs. The identification process occurs at many different locations and in many different ways. For example, data identification can take place when data is created and when endpoint devices such as laptops, mobile phones, and removable media consume it. In addition, identification can occur when data is moved or shared across a network, and when it is stored or archived in the data center or a cloud network. An effective data security system must protect the data throughout its entire lifecycle, as depicted in Figure 2.

A primary goal of data security systems is to protect against theft of intellectual property and confidential customer data. Doing so helps organizations comply with legal and regulatory standards. Data security systems interact with networks, endpoints, and data centers, and consist of multiple components, including DLP, encryption, device control, information rights management, and secure delivery, as depicted in Figure 3.

DLP is an important component of a comprehensive data security solution. DLP provides content-based data discovery, monitoring, and protection of sensitive data at rest, in use, and in motion.

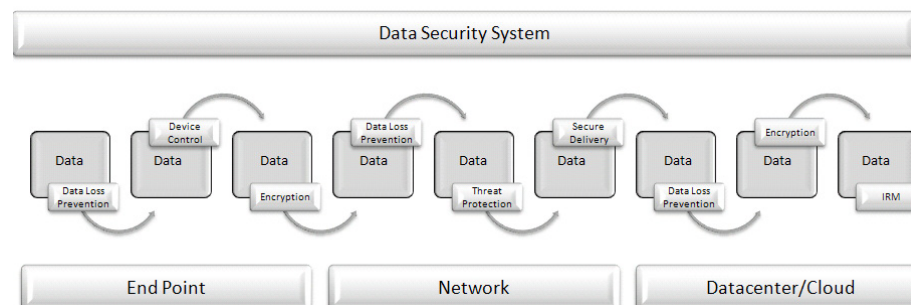
Figure 2. Data Security Lifecycle



Endpoint data security uses device control, encryption, and content-aware DLP techniques to protect data at rest and data in use on mobile devices such as laptops, netbooks and smartphones. On laptops and on removable media, data at rest is protected by full disk encryption or intelligent, policy-based encryption of sensitive data. On smartphones, data at rest

is protected by encryption and by device control features such as device wipes and personal identification number (PIN) locks. Encryption and device control help mitigate the risk of lost or stolen devices. Content-aware DLP can also discover and classify sensitive information on endpoint devices, preventing accidental leakage of information through such means as USB flash drives or uncontrolled printouts.

Figure 3. Data Security System



Network data security focuses on secure data delivery, threat protection, and data loss prevention for data in motion across the network perimeter. Secure data delivery solutions, such as VPNs, protect data integrity and confidentiality for sensitive information over insecure public links. Threat protection solutions like intrusion prevention systems (IPS) protect against threats such as buffer overflows, injection attacks, directory traversals, and other common attacks. DLP data-in-motion solutions use content-aware techniques to ensure that sensitive information does not leave an organization accidentally or by any unauthorized means.

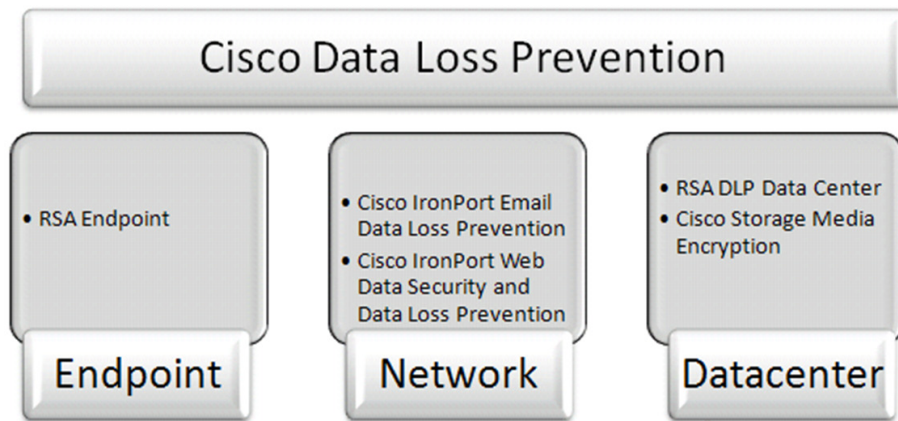
Data center security and cloud data security have many different components, such as database encryption, file-share encryption, storage area network (SAN) data encryption, content-aware data discovery of sensitive data on servers, and information rights management for prevention of unauthorized access. Data center DLP technologies focus on discovery of sensitive information by local or remote agents that crawl databases, document management systems, and other servers, and classify data. Data center security addresses the need to meet data security regulatory requirements, to discover and protect intellectual property, and to provide insight into who has access rights to data.

Data security systems include a central management server for creating and administering data security policies, an incident workflow, a reporting system, and data discovery and enforcement across various points.

## Overview of the Cisco Data Security Solution

Cisco is partnering with leading companies through the Cisco Developer Network (CDN) to deliver a comprehensive data security solution, including an array of technologies to protect data throughout its lifecycle, as shown in Figure 4 below. This solution provides organizations a policy-based approach for monitoring, identifying and preventing leakage of information across the network, endpoints and data center.

Figure 4. Comprehensive Data Security Solution



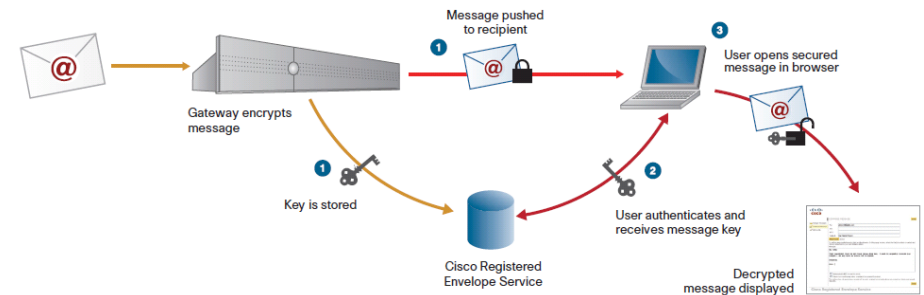
### Network Security

Sensitive data can leave the network perimeter by many different means, such as email, web applications, file transfers, and instant messaging. Enforcing content policies at the network perimeter is an effective defense against accidental data loss. Cisco partners with RSA, a leading DLP solution provider, to provide integrated DLP technology on Cisco IronPort Email and Web Security Appliances.

RSA Email DLP is built into the Cisco IronPort Email Security Appliance to provide content-level scanning of email messages and attachments, and to detect sensitive information before it leaves an organization. It contains an integrated DLP scanning engine with over 100 DLP policy templates, and is activated through a software license. DLP policy in the Email Security Appliance allows messages to be examined for data patterns that are associated with sensitive data that should not be exposed to the outside world. Several actions can be taken when a pattern match occurs, ranging from sending a warning message to blocking the entire message.

DLP policy can also enforce encryption of messages containing sensitive data, using the email encryption feature of the appliance. Email encryption can use either the Cisco Registered Envelope Service (CRES) or a local key server, as shown in Figure 5. CRES provides secure and transparent management of key creation, distribution, and retention.

Figure 5. Cisco Registered Envelope Service in Use



Gateway-to-gateway encryption through Transport Layer Security (TLS) is another way of protecting sensitive information. The Email Security Appliance can securely relay a message over a TLS connection, and the administrator can configure the policy to control whether TLS transport is mandatory, or used only when the other side of the connection supports it, and whether message-level encryption is used as a fallback when TLS is not available.

While the Email Security Appliance protects standard Internet email sent using the Simple Mail Transfer Protocol (SMTP), other increasingly popular alternatives, such as instant messaging and web-based email services, must also be inspected for sensitive data. Cisco IronPort Web Security Appliances can connect to an external DLP system using ICAP. This enables the Web Security Appliance to apply DLP policies to HTTP, HTTPS, and FTP traffic in the same way as the Email Security Appliance does to SMTP traffic, providing consistent enforcement no matter which protocol is being used to send the information.

### Endpoint Security

Endpoint data security includes content aware policy enforcement, mandatory encryption of sensitive data on laptops and smartphones, and protection of sensitive information being copied or transferred to removable media. Cisco partners with endpoint data protection market leaders to provide validated and compatible policy-based encryption and device control solutions for data at rest and data in use on endpoints.

Cisco recommends RSA DLP Endpoint for the protection of information assets on laptops and desktops. RSA DLP Endpoint consists of two modules, Discover and Enforce. The Discover module provides content-based data classification and fingerprinting that provides visibility for sensitive data on laptops and desktops. The enforcement module provides protection for data in use by preventing copying of sensitive data to USB devices and other removable media.

## Data Center Security

DLP for the data center involves discovering, classifying and encrypting sensitive data no matter where it resides in the data center—file systems, databases, email systems, or network-based storage. Cisco recommends RSA DLP Datacenter, which can discover sensitive data and help to enforce policies across file shares, databases, network storage, Microsoft SharePoint sites and other data repositories to reduce the risk and business impact associated with enterprise data loss.

RSA DLP Datacenter offers permanent and temporary agents. Temporary agents scan data, collect policy violations, and self-uninstall to allow organizations to survey their risk landscape. RSA Enterprise Manager can deploy policies across RSA DLP Datacenter, DLP Network and DLP Endpoint.

For data center SAN storage, Cisco MDS 9000 Family Storage Media Encryption (SME) offers a heterogeneous, standards-based encryption solution for data at rest, with comprehensive built-in key-management features.

## Data Security Deployments and Use Cases

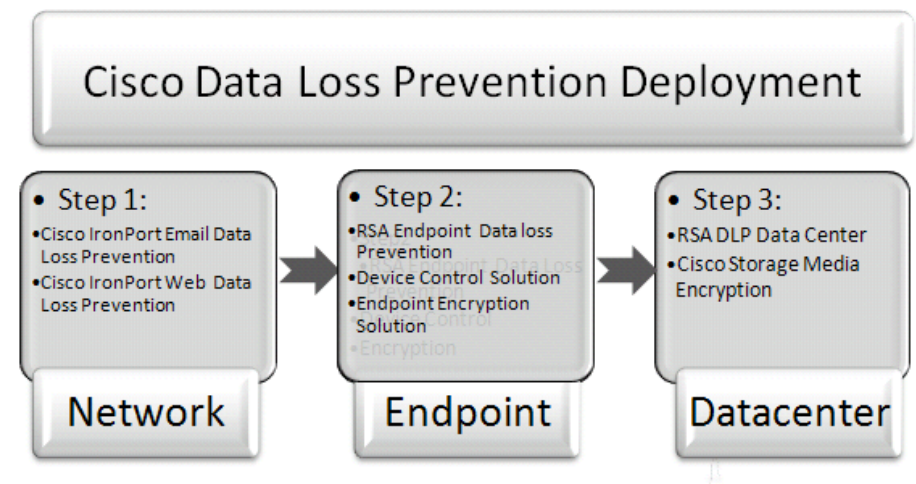
A complete data security system is best deployed in stages, as depicted in Figure 6 below. Cisco recommends implementing DLP in three sequential steps:

1. **Network Deployment** provides broad coverage with ease of management, using the security management features of Cisco IronPort Email Security and Web Security Appliances.
2. **Endpoint Deployment** provides policy-based device control and encryption to prevent sensitive information from leaving through external removable media, printing, copying and other means of data in use.
3. **Data Center Deployment**, the final step, requires understanding the organization's unstructured or structured sensitive data assets, and determining what policies need to be enforced at various points in the data security deployment. RSA DLP Datacenter and Cisco SME address issues of discovering and encrypting sensitive information in the data center.

In addition, after each step is completed, we recommend two additional activities:

- **Tuning**—after organizations identify their sensitive data, they configure DLP to meet their particular requirements. This involves testing to ensure they are detecting violations, frequently by configuring the products in learning or non-block mode to gather information for secondary analysis, before implementing more stringent controls.
- **Optimization**—finally, the data security system should be optimized for easy maintenance and management. In this phase, automatic updates, instant reports for executives, automatic decision making information and detailed violation reports are typically configured.

Figure 6. Cisco Data Loss Prevention Deployment





# Cisco Data Security Configuration Details

## Network Security

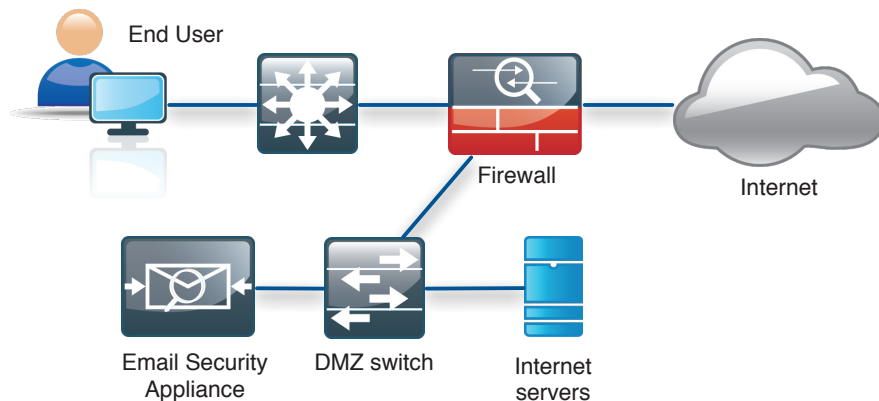
### Process

#### Cisco Email Data Security Configuration

1. Enable DLP
2. Set Up the Basic DLP Policy
3. Testing and Monitoring the Data Security System
4. Monitoring DLP Policies

The Cisco IronPort Email Security Appliance is placed in the DMZ of the Internet edge of the SBA Borderless Networks for Enterprise Organizations architecture. For simplicity, the appliance is connected by a single interface, as shown in Figure 7.

Figure 7. Cisco Email Data Security Architecture



Implementing DLP with Email Security Appliances requires the following high-level procedures, each involving several steps, as listed below:

- Enable DLP
- Set up basic DLP policy
  - a. HIPAA Policy
  - b. GLBA Policy
  - c. PCI-DSS Policy
  - d. Custom Policy
- Connect the DLP policy with outgoing mail policy
- Test and monitor policy violations

### Procedure **Enable DLP**

DLP is a licensed feature on the Cisco IronPort Email Security Appliance. You can activate this feature by providing the license key in the Feature Key tab of the web management interface by selecting **System Administration > Feature Keys** and then clicking "Check for New Keys". Verify that the key is active, as shown in Figure 8.

Figure 8. Activate DLP

Feature Keys for Serial Number: 001E4F20C614-C0YG5G1			
Description	Status	Time Remaining	Expiration Date
RSA Email Data Loss Prevention	Active	89 days	08 Sep 20:23 (GMT)
Bounce Verification	Active	Perpetual	N/A
IronPort Email Encryption	Active	231 days	28 Jan 07:05 (GMT)

Note that the email encryption feature license is also active in the example and is required in order to employ message encryption as an option in the DLP policy. If you have not licensed email encryption, this action will not be available.

To start scanning the outgoing emails for sensitive data you must first enable DLP on the appliance using the following steps in the web management interface:

**Step 1:** Select **Security Services > RSA Email DLP**.

**Step 2:** Click **Enable**. The license agreement page appears.

**Step 3:** Read the agreement, then click **Accept**.

**Step 4 (optional):** Enable Matched Content Logging to allow the logs to include the content that triggers a violation. Note that this option will cause potentially sensitive information (such as credit card numbers) to appear in the security logs. Your organization's policy requirements will determine if this is desirable or not. Also note that this feature requires that the message tracking service is enabled under **Security Services > Message Tracking**.

## Procedure

### Set Up the Basic DLP Policy

The DLP Policy Manager is a single dashboard in the web interface that allows you to manage all email DLP policies. You can access the DLP Policy Manager from the **Mail Policies** Menu. The appliance comes with over 100 predefined policy templates developed by RSA, some of which are shown below. In the following examples, configurations of HIPAA, GLBA, and PCI-DSS policies from predefined RSA templates, as well as one custom policy, are shown.

## HIPAA Policy

**Step 1:** Select **Mail Policies > DLP Policy Manager**.

**Step 2:** Click **Add DLP Policy**.

**Step 3:** Click **Regulatory Compliance** and then click **Add HIPAA**.

Figure 9. Add DLP Policy

Add DLP Policy from Templates	
Display Settings: <a href="#">Expand All Categories</a>   <a href="#">Display Policy Descriptions</a>	
Regulatory Compliance	
Add	Payment Card Industry Data Security Standard (PCI-DSS)
Add	PIPEDA (Personal Information Protection and Electronic Documents Act)
Add	FERPA (Family Educational Rights and Privacy Act) <i>Customization recommended.</i>
Add	GLBA (Gramm-Leach Bliley Act) <i>Customization recommended.</i>
Add	HIPAA (Health Insurance Portability and Accountability Act) <i>Customization recommended.</i>
Add	SOX (Sarbanes-Oxley)
US State Regulatory Compliance	
Acceptable Use	
Privacy Protection	
Intellectual Property Protection	
Company Confidential	
Custom Policy	

In this example, assume the organization's patient ID numbers follow a pattern of three digits, each ranging from 2 to 4, followed by seven digits ranging from 0 to 9. This pattern is matched by a regular expression of the

form `[234]{3}[0-9]{7}`; additionally, the phrase "Patient ID" must appear in the data, in order for the policy to match.

**Step 4:** Enter `[234]{3}[0-9]{7}` in the "Patient Identification Numbers as a regular expression" field.

**Step 5:** Enter "Patient ID" in the "AND match with related words or phrases" field, as shown in Figure 10 below.

The completed form is shown below in Figure 10. If an outgoing email message contains a number that matches both the regular expression and the text "Patient ID", it triggers this DLP policy.

Figure 10. HIPAA DLP Policy

Policy: HIPAA (Health Insurance Portability and Accountability Act)	
DLP Policy Name:	HIPAA (Health Insurance Portability and Accountability Act)
Description:	Identifies documents and transmissions that contain patient-identifiable medical information protected by the Health Insurance Portability and Accountability Act (HIPAA) enacted by the Congress
Content Matching Classifier:	Patient Identification Numbers (customization recommended) OR Patient Identifiers AND HIPAA Dictionaries
	<p>Patient Identification Numbers as a regular expression:</p> <p><code>[234]{3}[0-9]{7}</code></p> <p>Combine multiple number patterns with " " to form a single expression. (Example: 123-CL456789 matches the regular expression <code>[0-9]{3}\-[A-Z]{2}[0-9]{6}</code> See more examples.)</p> <p>AND match with related words or phrases:</p> <p>Patient ID</p> <p>Separate multiple entries with a line break or comma. Sometimes number patterns consistently appear with words or phrases as in "Patient Identification Numbers: 123-CL456789." Including the words "Patient Identification Numbers:" would improve content matching accuracy.</p>
Filter Senders and Recipients:	Restrict this DLP policy by specific recipients and senders.
Filter Attachments:	Restrict this DLP policy to detect specific attachment types.

**Step 6:** Under **Severity Settings > Critical Severity Settings**, select **Quarantine** from the **Action Applied to Messages** drop-down menu. Messages that contain DLP violations will be held in a quarantine area.

**Step 7:** Select **Sender** under **Advanced > DLP Notification**. Optionally, you can choose to encrypt the message, modify its header, deliver it to an alternate host, send a copy (bcc) to another recipient, and send a DLP notification message.

**Step 8:** If you want to define different settings for messages that match the high, medium, or low severity level, uncheck the **Inherit Settings** check box for the appropriate security level. Edit the overall action for the message and the other settings. In this example different settings by severity level remain unconfigured.

**Step 9:** Click **Submit** and then **Commit Changes**. The policy is added to the DLP Policy Manager.

## GLBA Policy

Follow the preceding steps and add a GLBA policy. However, in this example assume the account numbers consist of three digits in the range of 4 to 6, followed by six digits in the range of 0 to 9.

**Step 1:** Select **Mail Policies > DLP Policy Manager**.

**Step 2:** Click **Add DLP Policy**.

**Step 3:** Click **Regulatory Compliance** and then click **Add GLBA**.

**Step 4:** Enter `[456]{3}[0-9]{6}` in the “Custom Account Numbers as a regular expression” field.

**Step 5:** Enter “Account Number” in the “AND match with related words or phrases” field.

An outgoing email that contains a matching account number and key word will now trigger an alert for a GLBA violation.

**Step 6:** Under **Severity Settings > Critical Severity Settings**, select **Quarantine** from the Action Applied to Messages drop-down menu. Messages that contain DLP violations will be held in a quarantine area.

**Step 7:** Select **Sender** under **Advanced > DLP Notification**. Optionally, you can choose to encrypt the message, modify its header, deliver it to an alternate host, send a copy (bcc) to another recipient, and send a DLP notification message.

**Step 8:** If you want to define different settings for messages that match the high, medium, or low severity level, uncheck the **Inherit Settings** check box for the appropriate security level. Edit the overall action for the message and the other settings. In this example different settings by severity level remain unconfigured.

**Step 9:** Click **Submit** and then **Commit Changes**. The policy is added to the DLP Policy Manager.

Figure 11. GLBA DLP Policy

The screenshot shows the configuration page for a DLP policy named "GLBA (Gramm-Leach Bliley Act)". The "Description" field contains text about identifying financial information regulated by the GLBA. The "Content Matching Classifier" is set to "Custom Account Numbers (customization recommended) OR US Drivers Licenses OR Credit Card Number OR US Social Security Number". Under "Custom Account Numbers as a regular expression", the value `[456]{3}[0-9]{6}` is entered. Below this, a note explains that multiple number patterns can be combined with "|" to form a single expression, with an example: `123-CL456789` matches `[0-9]{3}\-[A-Z]{2}[0-9]{6}`. The "AND match with related words or phrases" field contains "Account Number, Account No#, A/C No". At the bottom, there are two expandable sections: "Filter Senders and Recipients" (restricted by specific recipients and senders) and "Filter Attachments" (restricted to detect specific attachment types).

## PCI-DSS Policy

PCI standards mandate that credit card numbers never be transmitted in unencrypted form. Before adding a PCI-DSS Policy, enable the encryption profile in order to take encryption as action within the PCI-DSS policy:

**Step 1:** Click **Security Services** and then **IronPort Email Encryption Services**.

**Step 2:** Make sure the IronPort Email Encryption is enabled and that the proxy server setting is correct for your network. In our example, no proxy server is required, as shown below.

Figure 12. Enabling Email Encryption

The screenshot shows the "Email Encryption Global Settings" page. At the top, a success message states "Settings have been saved." Below this, a table shows the settings: "IronPort Email Encryption" is set to "Enabled", and "Proxy Server (optional)" is set to "Not Configured". An "Edit Settings..." button is located at the bottom right of the settings table.

**Step 3:** Click **Add Encryption Profile** and use `Encryption_Enable` as the profile name.

For example, use CRES for key management and select **Cisco Registered Envelope Service** from the Key Service Type list as shown below.

Figure 13. Adding an Encryption Profile

Encryption Profile Settings	
Profile Name:	<input type="text"/>
Key Server Settings	
Key Service Type:	<b>Cisco Registered Envelope Service</b>
Proxy:	<i>A proxy server is not currently configured.</i>
Cisco Registered Envelope Service URL:	<input type="text" value="https://res.cisco.com"/>
Envelope Settings	
<a href="#">Example Envelope</a>	
Envelope Message Security:	<input checked="" type="radio"/> <b>High Security</b> <i>Recipient must enter a password to open the encrypted message, even if credentials are cached ("Remember Me" selected).</i> <input type="radio"/> <b>Medium Security</b> <i>No password entry required if recipient credentials are cached ("Remember Me" selected).</i>
Logo Link:	<input checked="" type="radio"/> <b>No link</b> <input type="radio"/> <b>Custom link URL:</b> <input type="text" value="http://"/> <i>By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (example: http://www.mycompany.com/).</i>
Read Receipts:	<input checked="" type="checkbox"/> <b>Enable Read Receipts</b>
<a href="#">Advanced</a> <i>Advanced envelope settings.</i>	

To enable the PCI-DSS policy, follow the same steps that you used to add the HIPAA Policy, with the following exception:

In Step 5, in the Critical Severity Settings section, choose the **Quarantine** action as in the previous example, but also select the **Enable encryption on release from quarantine** option. From the **Encryption Rule** drop-down list, select **Only use message encryption if TLS fails** and choose the **Encryption\_Enable** profile from Step 2 in the **Encryption Profile** drop-down list.

Figure 14. Enabling Message Encryption if TLS Fails

Severity Settings	
Critical Severity Settings	
Action Applied to Messages:	<b>Quarantine</b>
<input checked="" type="checkbox"/> <b>Enable encryption on release from quarantine</b>	
Encryption Rule:	<b>Only use message encryption if TLS fails.</b> <i>(See TLS settings at Mail Policies &gt; Destination Controls)</i>
Encryption Profile:	<b>Encryption_Enable</b>
Encrypted Message Subject:	<input type="text" value="\$subject"/>
Policy Quarantine:	<input type="text" value="Policy"/>

## Custom Policy

When using the pre-built PCI-DSS policy or the Credit Card Number Classifier feature, it is important to note that those cover CCNs from American Express, Discover, Diners Club, JCB, MasterCard, and Visa. If you want to add support for specific store credit cards, you must use a custom policy and configure regular expressions to match the CCNs in e-mail.

The following example, illustrated in Figure 15, configures a regular expression to match a CCN that is 16 digits long and begins with the prefix 6035, with each group of four digits separated by a space, so the CCN structure is 6035 0000 0000 0000. In a regular expression, this can be represented as `6035\s\d{4}\s\d{4}\s\d{4}`. Note that here, “\s” represents a space, and “\d” a digit, equivalent to the range [0-9].

**Step 1:** Select **Mail Policies > DLP Policy Manager**.

**Step 2:** Click **Add DLP Policy**.

**Step 3:** Click **Custom Policy** and assign the name `Store_Card`.

**Step 4:** Configure the following three rules:

- Regular Expression: `6035\s\d{4}\s\d{4}\s\d{4}`
- Entity: US Address
- Entity: Proper Name

Figure 15. Creating a Custom DLP Policy

Content Matching Classifier		
Content Matching Classifier Name:	<b>Store_Card</b>	
Classifier Description:	<input type="text"/>	
Proximity:	<input type="text" value="300"/> Characters	
Minimum Total Score:	<input type="text" value="10"/>	
Rules		
<div> <div>All rules match</div> <div>Add Rule</div> </div>		
Regular Expression	<div> <div>Regular Expression Pattern:</div> <input type="text" value="6035\s\d{4}\s\d{4}\s\d{4}"/> <div> Combine multiple number patterns with “ ” to form a single expression.  (Example: 123-CL456789 matches the regular expression [0-9]{3}\-[A-Z]{2}[0-9]{6}  See more examples. </div> </div> <div> <div>Exclude Pattern:</div> <input type="text"/> </div> <div> <input type="text" value="10"/> Weight <input type="text" value="100"/> Max Score </div>	<div> <div></div> </div>

**Step 5:** Under **Severity Settings > Critical Severity Settings**, choose **Quarantine** from the **Action Applied to Messages** list.



**Step 6:** Select **Sender** under **Advanced > DLP Notification**. Optionally, you can choose to encrypt the message, modify its header, deliver it to an alternate host, send a copy to another recipient, or return a system-generated notification message to the sender.

**Step 7:** Click **Submit** and then **Commit Changes**. The policy is added to the DLP Policy Manager. The DLP policies will look like those shown in Figure 16 below.

The order of the policies is important. The appliance evaluates the policies in the order that they are listed in the DLP Policy Manager, reading from top to bottom. If a message matches more than one DLP policy, only the first one found in the list will be applied. **Edit Policy Order** can be used to rearrange the rules, if needed.

Figure 16. Setting the Order of Policies

Active DLP Policies for Outgoing Mail			
Add DLP Policy...			
Order	DLP Policy	Duplicate	Delete
1	HIPAA (Health Insurance Portability and Accountability Act)		
2	GLBA (Gramm-Leach Bliley Act)		
3	Payment Card Industry Data Security Standard (PCI-DSS)		
4	Custom_Policy		
Edit Policy Order...			

Advanced Settings	
US Drivers Licenses:	All Classifiers Enabled
Custom DLP Dictionaries: (for use in Custom Policies only)	None Available

Procedure

Connect the DLP policy with Outgoing Mail Policy

Outgoing mail policy determines which DLP policies are applied to messages leaving the organization. To apply the DLP rules created in the steps above, go to **Mail Policies > Outgoing Mail Policies** and select the current DLP policy rules for the outgoing default policy. Note that if you have not yet set up DLP policies, the current DLP policy rules will appear as “Disabled”. Clicking on that link will allow you to select **Enable DLP** and to enable or disable the individual policies.

Figure 17. Configuring Outgoing DLP Mail Policies

Find Policies						
Email Address:		<input type="radio"/> Recipient <input checked="" type="radio"/> Sender		Find Policies		

Policies						
Add Policy...						
Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	DLP
	Default Policy	Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	Disabled	Disabled	Custom_Policy GLBA (Gramm-Leach Bliley Act) HIPAA (Health Insura... Payment Card Industr...

Key: Default Custom Disabled

## HIPAA Policy Example

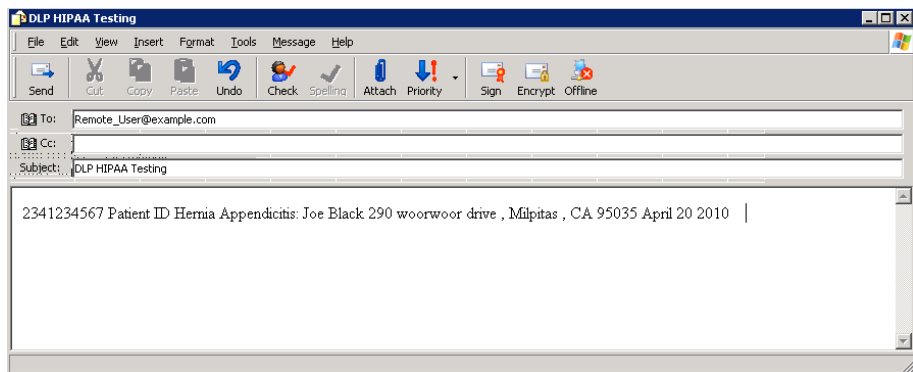
The pre-defined HIPAA policy in the RSA Email DLP engine looks for data in this fashion:

(Drug dictionary OR Disease dictionary OR Injury dictionary) AND (PII classifiers that are ORed together)

In other words, a message must contain something that matches one of the HIPAA dictionaries, as well a PII identifier, in order for the message to match the policy.

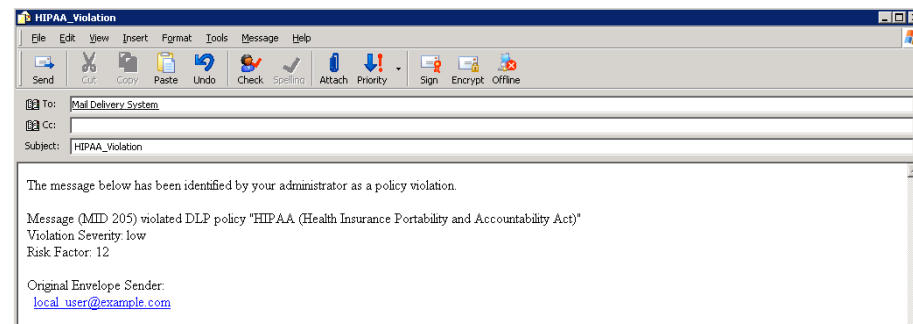
To test the outgoing mail policy, compose a test email that includes some illness-related terms, the text "Patient ID", and a patient ID number that matches the pattern defined in the HIPAA example configuration. The image below shows a simple test message. Send the test email to a destination outside the network.

Figure 18. Testing the Outgoing DLP Mail Policy



If the rule is being applied correctly, the sender will receive a notification e-mail similar to the one shown below, indicating the HIPAA violation.

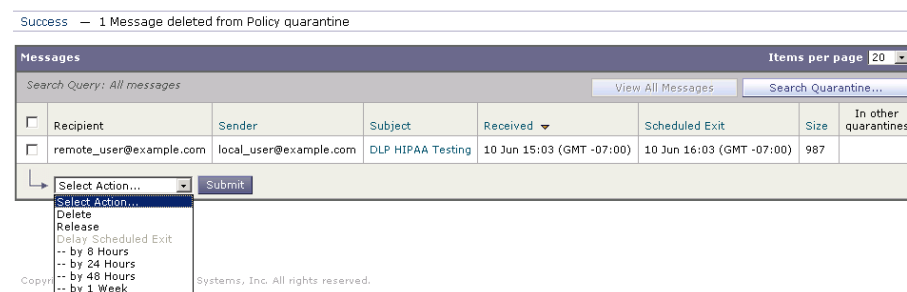
Figure 19. Example Notification Email



Because the HIPAA policy was configured to quarantine messages that contain DLP violations, manually inspect the test message, and either delete it or forward it. Quarantine areas also have a default action, which can be either to release the message or to delete it, and a time period after which the default action is automatically taken. In this example, manually release the message, allowing it to be delivered:

**Step 1:** Select **Monitor > Quarantines > Policy** to view quarantined messages, as shown in Figure 20.

Figure 20. Viewing Quarantined Email Messages



**Step 2:** Click the subject to view the details of the quarantined message, as shown in Figure 21 below.

Figure 21. Viewing Details of Quarantined Messages

Quarantine Details			
All	Quarantine	Reason	
<input type="checkbox"/> Policy	DLP Policy: 'HIPAA (Health Insurance Portability and Accountability Act)'	Time Received	10 Jun 15:03 (GMT -07:00)
		Time Scheduled to Exit	10 Jun 16:03 (GMT -07:00)
Select Action...		Submit	
< Back to Message List			

Message Details			
Test for Viruses:		Start Test	
Send Copy To:		E-Mail Addresses, comma separated: <input type="text"/> Send	
Envelope Sender:		local_user@example.com	
Recipients:		remote_user@example.com	
Subject:		DLP HIPAA Testing	

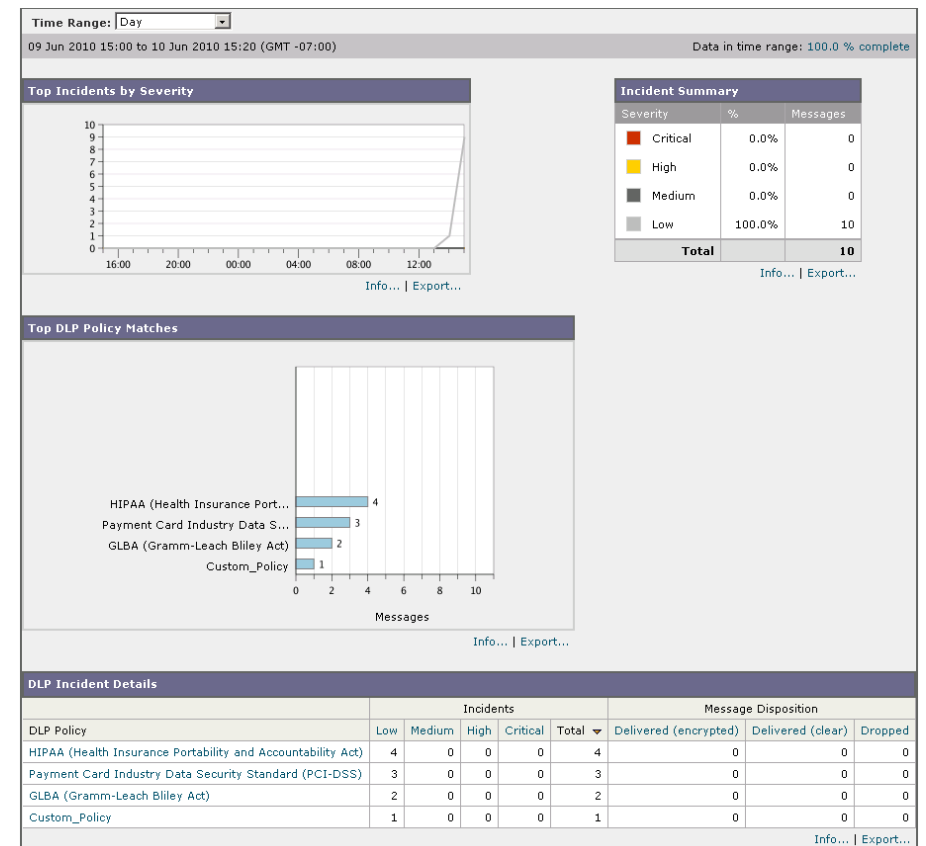
Matched Content		
Policy (DLP Violation: LOW severity, Risk Factor: 20)		
Attachment Name	Matched Content	Condition
[message body]	<ul style="list-style-type: none"> <li>2341234567 Patient ID</li> </ul>	DLP Classifier: Patient Identifiers
	<ul style="list-style-type: none"> <li>2341234567 Patient ID</li> </ul>	DLP Classifier: Patient Identification Numbers (HIPAA (Health Insurance Portability and Accountability Act))
	<ul style="list-style-type: none"> <li>Patient ID Hernia Appendicitis: Joe Black 290 woowoor drive , Milpitas , CA 95035 April 2</li> </ul>	DLP Classifier: HIPAA Dictionaries

**Step 3:** Under **Quarantine Details**, you have the ability to either delete the quarantined message or to release it, or to extend the quarantine period. To release the message to its destination, check the **Select** box for the test message, choose **Release** from the **Select Action** drop-down list, and then **Submit**.

## Procedure Monitoring DLP Policies

In the management GUI, select **Monitor > DLP Incidents**. From the DLP Incident Summary screen shown below, one can click on any of the policies to see the report for that specific policy violation. By clicking on the policy in "DLP Incident Details", one can view individual users who have violated that policy. This allows the administrator to see their mail profile, which provides information about what information assets are leaving the network by e-mail. Administrators can also search for DLP violations and see the specific content that triggered the DLP violation. This provides detail about what transpired in the DLP incidents during auditing and discovery.

Figure 22. Monitoring DLP Incidents



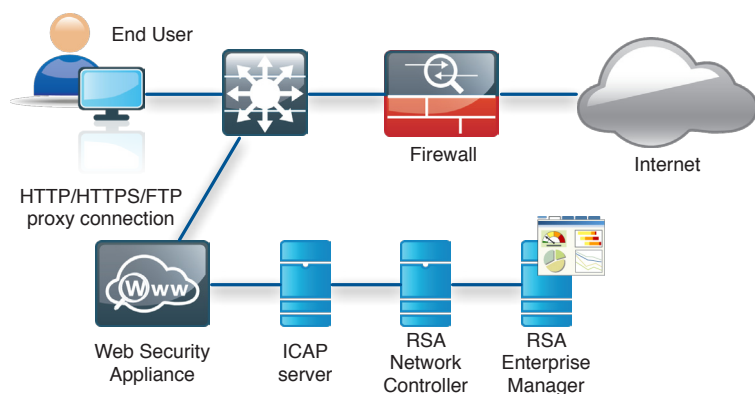
## Process

### DLP Configuration for Web Traffic

1. Enable DLP on the Appliance
2. Configure the RSA DLP Network
3. Validate the Setup

A Cisco IronPort Web Security Appliance deployed at the Internet edge interoperates with RSA DLP technology to identify and protect sensitive data. The appliance acts as a proxy server and uses ICAP to offload content scanning to external systems. RSA Enterprise Manager manages policies for the network, endpoints, and data-center. Cisco IronPort Web Security Appliance, RSA Enterprise Manager, and the RSA DLP Network Controller are the main components shown below.

Figure 23. Main Components for Web Traffic DLP



In this deployment guide, RSA DLP Network Controller, the ICAP server, and RSA Enterprise Manager are installed and configured in the SBA Borderless Networks for Enterprise Organizations architecture.

The following sections provide a recommended configuration for blocking sensitive information sent through webmail. Cisco IronPort Web Security Appliance version 6.3.3 is the verified platform. In this example, the pre-defined PCI-DSS policy for the network is used.

Implementing DLP with Web Security Appliances requires the following high-level procedures, each involving several steps, as listed below:

- Enable DLP on the appliance
- Configure the RSA DLP network
- Validate the setup
- Test and monitor policy violations

## Procedure

### Enable DLP on the Appliance

**Step 1:** Enable external DLP server, which in this example has IP address 10.4.200.118:

From the Web Security Appliance web management GUI, select **Network > External DLP Servers**, then click **Edit Settings**. In the **Server Address** field, enter the address of the RSA DLP server, in this case 10.4.200.118. The **Port** will usually be left set to the ICAP default port of 1344. The **Service URL** is of the form `icap://serverIP/srv_conalarm`, so in the example shown in Figure 24, it is `icap://10.4.200.118/srv_conalarm`.

Figure 24. Configuring an External DLP Server Using ICAP

External DLP Servers		
External DLP Servers:		
Server		
Server Address	Port	Reconnection Attempts
10.4.200.118	1344	3
Service URL		
icap://10.4.200.118/srv_conalarm		
<small>An ICAP URL must begin with icap:// and may not contain any whitespace. Consult your DLP appliance vendor documentation for correct service URL for your system.</small>		
Start Test		
Load Balancing: Fewest Connections		
Service Request Timeout: 60 seconds		
Maximum Simultaneous Connections: 25		
Failure Handling:		
<input checked="" type="radio"/> Permit all data transfers to proceed without scanning		
<input type="radio"/> Block data transfer for transactions where scanning was requested		
Cancel		
Submit		

To test the connection between the appliance and the external DLP server, click **Start Test**.

Click **Submit**, then **Commit Changes**.



## Step 2: Set Up External DLP Policy

Create external DLP policies that determine which traffic is sent to the ICAP server for content scanning.

Go to **Web Security Manager > External DLP Policies** and click **Add Policy**. Give the policy a name in the **Policy Name** field. In this example, use “Gmail Policy” as the name. Under **Policy Member Definition**, select criteria for the policy. In this example, apply the policy to all users and leave **Identities and Users** set to the default value of **All Identities**. For this setting, at least one further selection option is required. Click on **Advanced** and then set the **Protocols** definition to include HTTP, HTTPS, FTP over HTTP, Native FTP, and All others. Click **Submit**.

Click on the **Scan** settings under Destinations for the policy. Choose **Define Destinations Scanning Custom Settings** from the drop-down list, and set **Destinations to Scan** to **Scan all uploads**. The resulting policy should look like the “Gmail policy” entry shown below:

Figure 25. Configuring to Scan All Protocols

External DLP Policies			
Add Policy...			
Order	External DLP Policy	Destinations	Delete
1	<b>Homail</b> Identity: All	Scan: All	
2	<b>Gmail policy</b> Identity: All Protocols: HTTP, HTTPS, FTP over HTTP, Native FTP, All others	Scan: All	
	<b>Global Policy</b> Identity: All	Scan: All	

Step 3: Click **Submit** and then **Commit Changes**.

## Procedure

## Configure the RSA DLP Network

**Step 1:** In RSA Enterprise Manager, enable the ICAP server and Network Controller. The Network Controller communicates between RSA Enterprise Manager and network devices.

Go to **Admin > Network > Status** and verify that the Network Controller and ICAP servers are operating. For detailed instructions on setting up the DLP Network ICAP server and Network Controller, please refer to the RSA documentation for RSA Data Loss Prevention.

**Step 2:** Write a PCI-DSS policy to prevent the loss of sensitive information via Gmail.

Go to **Policies > New Policy > Use Policy Template**.

Click **PCI –DSS** policy. The PCI-DSS policy page opens.

Under the **Network** tab, select the following options:

- Under **Who**, select **all Users**.
- Under **Detect**, select **Protocols**.
- Under **Action**, **Audit only**.

Click **Save**.

Figure 26. Setting a Policy for Gmail

The screenshot shows the 'Network' tab in the RSA Enterprise Manager interface. The 'Policy Violation Rules' section is visible. The 'Who' field is set to 'All users'. The 'Detect' field is set to 'Protocols'. The 'Severity' field is set to 'Info'. The 'Action' field is set to 'Audit only'. The 'Protocol' field is set to 'FTP, Telnet, HTTP, HTTPS, POP3, SMTP, All IM, Google IM, IMAP, IMAP, IMAP, IMAP'.

**Step 1:** Configure a web browser to proxy outgoing traffic through the Cisco IronPort Web Security Appliance.

**Step 2:** Using the browser, access Gmail, compose a new message, and attach a file that violates the PCI-DSS policy.

**Step 3:** Verify that a Network ICAP discard message is displayed in the browser.

**Step 4:** Use RSA Enterprise Manager to view the resulting event and incident that were created as a result of this violation of policy.

Figure 27. Viewing Incidents and Events Caused by Policy Violations

The screenshot shows the RSA Data Loss Prevention console interface. The top navigation bar includes links for Dashboard, Incidents, Reports, Policies, and Admin. The 'Incidents' tab is selected, displaying a table of incidents. The table columns are ID, Date, Type, Severity, Status, Validity, Assignee, Sender/User/Owner, Protocol/ User Action, Policy, and Policy Action. The incidents listed are all of type 'Real Issue' with a severity of 'Low' or 'Medium' and a status of 'Open'. The policy violated is 'PCI-DSS (Payment Card Industry Data Security Stand...)'.

ID	Date	Type	Severity	Status	Validity	Assignee	Sender/User/Owner	Protocol/ User Action	Policy	Policy Action
8	05/28/2010, 04:34 PM	Real Issue	Medium	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit, block
6	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit, block
4	05/28/2010, 04:29 PM	Real Issue	Medium	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit, block
7	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit, block
5	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit
3	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit
2	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit
1	05/28/2010, 04:29 PM	Real Issue	Low	Open	Real Issue	admin	192.168.20.2	http	PCI-DSS (Payment Card Industry Data Security Stand...)	audit

# Endpoint Security

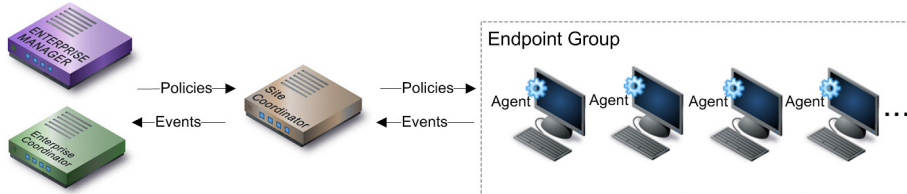
RSA DLP Endpoint allows you to monitor and control how end users interact with sensitive information. It tracks and controls a range of user actions as defined by policy, and it audits user actions involving sensitive data, sending alerts of policy violations, and creating audit logs.

## Configuration of RSA DLP Endpoint

A deployed instance of RSA DLP Endpoint includes the following components, shown in Figure 28.

- RSA DLP Endpoint Agents
- RSA DLP Enterprise Manager
- RSA DLP Site Coordinator
- RSA DLP Enterprise Controller

Figure 28. A Deployed Instance of RSA DLP Endpoint



Endpoint Agents run on each user's computer to monitor user actions and perform content analysis. The agents are responsible for enforcing usage policy and collecting audit data. The Site Coordinator controls the customer's deployment. It sends instructions to, and gathers results from, endpoint agents, defined into Endpoint Groups.

The Enterprise Manager is the interface to DLP Endpoint for both users and administrators. The Enterprise Manager sends configuration settings and policies to the Site Coordinator to be picked up by all endpoint agents on the network. At predefined intervals, the Enterprise Manager picks up events sent to the Site Coordinator by those endpoint agents, and based on policy, generates incidents for review and analysis.

## Process

### RSA DLP Endpoint Example

In this example, assume Enterprise and Site Coordinators "San Jose" are configured. This example shows that, if a user tries to copy files onto external media such as a USB drive, this action triggers a DLP violation.

#### Step 1: Create a new Endpoint Agent group

In RSA DLP Enterprise Manager, go to **Admin > Endpoint**. Click **New Endpoint Group**. Select the site **San Jose**.

In the **Computers (DNS names or IP addresses)** field, specify the IP address of the computer (for example, 192.168.21.36).

In the **Configure passwords** section, enter the GPO/Push Agent Password, which is the password for installing endpoint agents with push technology. If you have already installed endpoint agents on the target machines in the Endpoint group, enter the same password that was used for those installations.

#### Step 2: Activate RSA DLP Endpoint policy using pre-defined policy templates

Go to Policies tab.

Click **New Policy** at the top of the policy list.

Select **Use Policy Template Library** from the drop-down menu.

Under the Regulatory and Compliance section, select the PCI-DSS policy template and activate it for Endpoint.

Click the PCI-DSS policy and then select the **Endpoint** tab within the PCI – DSS template.

Figure 29. Policy Validation Rules



Create a policy violation rule. In the Who field, keep the default “All users” option.

Under Detect, the detection filter lets you specify user actions, file attributes, destination attributes and transmission attribute that can trigger DLP violation.

Add a “User action” detection rule, which lets you specify a user action that triggers a DLP violation. Select **Copy to Removable Drive**.

Figure 30. Defining a User Action Detection Rule for Removable Drives

### User Actions

☐ Any user action below

☐ Any print
 

☐ Print to local printer
 ☐ Print to internet printer
 ☐ Print to network printer
 ☐ Print to files

☐ Any copy
 

☐ Copy to CD/DVD
 ☒ Copy to Removable Drive
 ☐ Copy to Net Share

The following actions apply only when the user is disconnected from the corporate network.

☐ Any off-network actions below

☒ Send via HTTP / HTTPS
 ☒ Send via IM

Under Severity — Action, choose **Notify and Audit** as the action the policy should take if a violation occurs.

Click **Save**. The new or edited policy will appear in the policy list on the Policy Manager page. By default, the policy is enabled. To test the policy on the client machine, try copying a document or any other file type that contains a CCN with address information to a USB drive. This will generate DLP violation.

**View DLP Violation:** Click the Incident tab to display the DLP violation.

Figure 31. Console Messages Showing DLP Violations

Incidents

Events

Advanced Search

Select a Saved Search...

Manage Saved Searches

Quick Search

Go

Search Criteria is:

Date Range: Last 7 Days

Incident Status: Open, In Progress

Incident Assignee: admin

Incidents per page

20

Incidents 1 - 20 of 100

Next >>

Last

Assign

Set Severity

Set Validity

Close

Reopen

Delete

Delete All

Schedule

Email Report

Export

ID	Date	Type	Severity	Status	Validity	Assignee	Sender/User/Owner	Protocol/ User Action	Policy	Policy Action
99	04/21/2008, 12:15 PM		High	Open	Real Issue	admin	Jagat	copymove-usb	Credit Card Numbers	block
100	04/21/2008, 12:15 PM		Critical	Open	Real Issue	admin	Jagat	copymove-usb	Credit Card Numbers - By Issuer	block
70	04/21/2008, 12:14 PM		Medium	Open	Real Issue	admin		smtp	Credit Card Numbers - By Issuer	audit
85	04/21/2008, 12:14 PM		Low	Open	Real Issue	admin		smtp	Credit Card Numbers - By Issuer	audit
83	04/21/2008, 12:14 PM		Medium	Open	Real Issue	admin		smtp	US National Provider Identifiers (NPI)	audit
71	04/21/2008, 12:14 PM		Critical	Open	Real Issue	admin		smtp	US Social Security Numbers	audit



# Datacenter Security

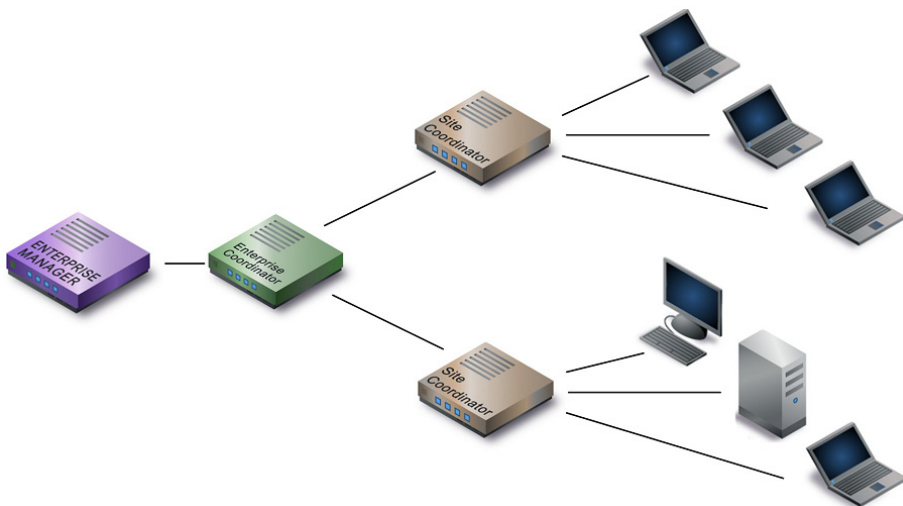
RSA DLP Datacenter is a software solution that permits locating and acting on sensitive information stored anywhere in the enterprise. In use, DLP Datacenter scans an organization's networks, examining files on all machines of interest.

## RSA DLP Datacenter Configuration

A deployed instance of RSA DLP Datacenter includes the following components, as shown in Figure 32.

- RSA DLP Endpoint Agents
- RSA DLP Enterprise Manager
- RSA DLP Site Coordinators
- RSA DLP Enterprise Coordinator

Figure 32. RSA DLP Datacenter Components



During a scan, endpoint agents perform the content analysis. Each agent receives instructions from, and returns results to, its Site Coordinator. An RSA DLP Datacenter installation can have as many Site Coordinators as required, possibly in widely dispersed locations. The Enterprise Coordinator is the master controller for the DLP Datacenter deployment. It sends

instructions to, and gathers scan results from, all Site Coordinators involved in all scans.

When it scans, DLP Datacenter accesses a specific scan group, which is a set of machines on the network that you specify as being of interest.

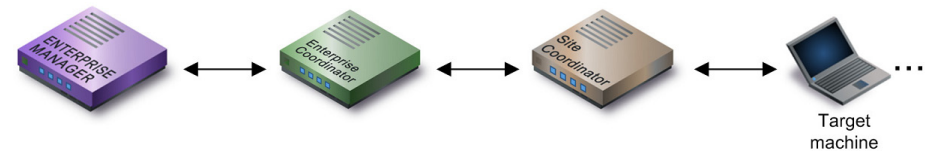
There are several types of scan groups available:

- **Agent:** Scan groups for agent-based scan
- **Grid:** Scan groups for grid scans
- **Repository:** Scan groups for scan

## Agent-Based Scanning

In this type of scan, an endpoint agent is installed on every machine whose content should be scanned. To perform a scan, Enterprise Manager sends a request to the Enterprise Coordinator, which sends a command to the appropriate Site Coordinator on a local or remote network. The Site Coordinator installs or connects to an endpoint agent on each target machine in the scan group and commands it to start scanning. Each agent accesses and analyzes all files on its local host and then sends results—information about files that violate the policies being scanned for—back to the Site Coordinator, which collates results and sends them to the Enterprise Coordinator and on to Enterprise Manager for display to the user.

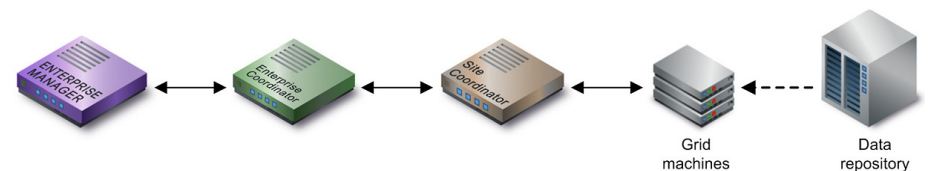
Figure 33. Agent-based DLP Scanning



## Grid Scanning:

Grid scanning provides for efficient, scalable analysis of very large file repositories (such as SAN or NAS systems), distributing the burden of analyzing the large amounts of data (up to terabytes) in the storage device.

Figure 34. Grid-based DLP Scanning



## Repository Scan and Database Scan

Specialized types of grid scans include database scanning of enterprise databases, and repository scanning of collaboration and document-management systems, such as SharePoint or Documentum.

In this guide, only agent-based scanning has been validated. Grid scanning is out of the scope of this guide.

## RSA DLP Datacenter Agent-based Scanning Example

This example scans a group of machines that contain specific dated files.

**Step 1:** In Enterprise Manager, click the **Admin** tab. The Administration Status Overview appears. Beneath the Admin tab, click **Datacenter**. The Datacenter administration page appears.

**Step 2:** Create a new agent-scan group

In the deployment tree, select the Site Coordinator that the new agent group belongs to. Above the tree, click **New Object** and select **New Agent Scan Group** from the drop-down menu. The New/Edit Agent Group panel appears on the right

**Step 3:** Activate Data Center DLP policy using pre-defined policy templates

Click the **Policies** tab and then **New Policy** at the top of the policy list. Select **Use Policy Template Library** from the drop-down menu. Under regulatory and compliance section select PCI-DSS policy template and activate it for Data Center. Click the PCI-DSS policy and then select the Datacenter tab within the PCI –DSS template.

- a. Create a policy violation rule. Click **All Agent and Grid Scan Groups** for selecting the scan group. Select the scan group “Agent\_Scan1”.
- b. Under Detect, add a detection filter that lets you specify by date those files that can be considered to be policy violations. Click the link (by default **Any File Dates**) to display this dialog box: Select **Files modified before May 2010**.
- c. Under **Severity — Action**, specify **Audit Only** as action the policy should take if a Violation occurs. You can specify different actions (allow, audit only, audit & encrypt, quarantine & audit , block & audit) for different event severities. In this example, set the severity to **High** and select the action **Quarantine**.

- d. Save the Policy. Click **Save**. The new or edited policy will now appear in the policy list on the Policy Manager page. By default, the policy is enabled.
- e. Start the Scan. In the deployment tree, select the scan group “Agent\_Group” used for the scan. The Agent Group panel appears, showing status information for the scan group that you have selected. In the Agent Group panel, click **Scan Now**. From the drop-down list, choose **Run Full Scan**. Scan all documents on all target machines in the scan group. After the files are identified, the system moves them automatically to a secure location, depending upon the severity. If the severity is high, then the security administrator should inspect it and check why the business processes were broken.
- f. View Logs. Click the **History** tab and then select **View Status Log**. A window displays all status messages as they are logged. This window displays the same status log that is visible when the Status tab is active—covering both the agent-deployment phase and the content analysis phase of the scan.

# Summary

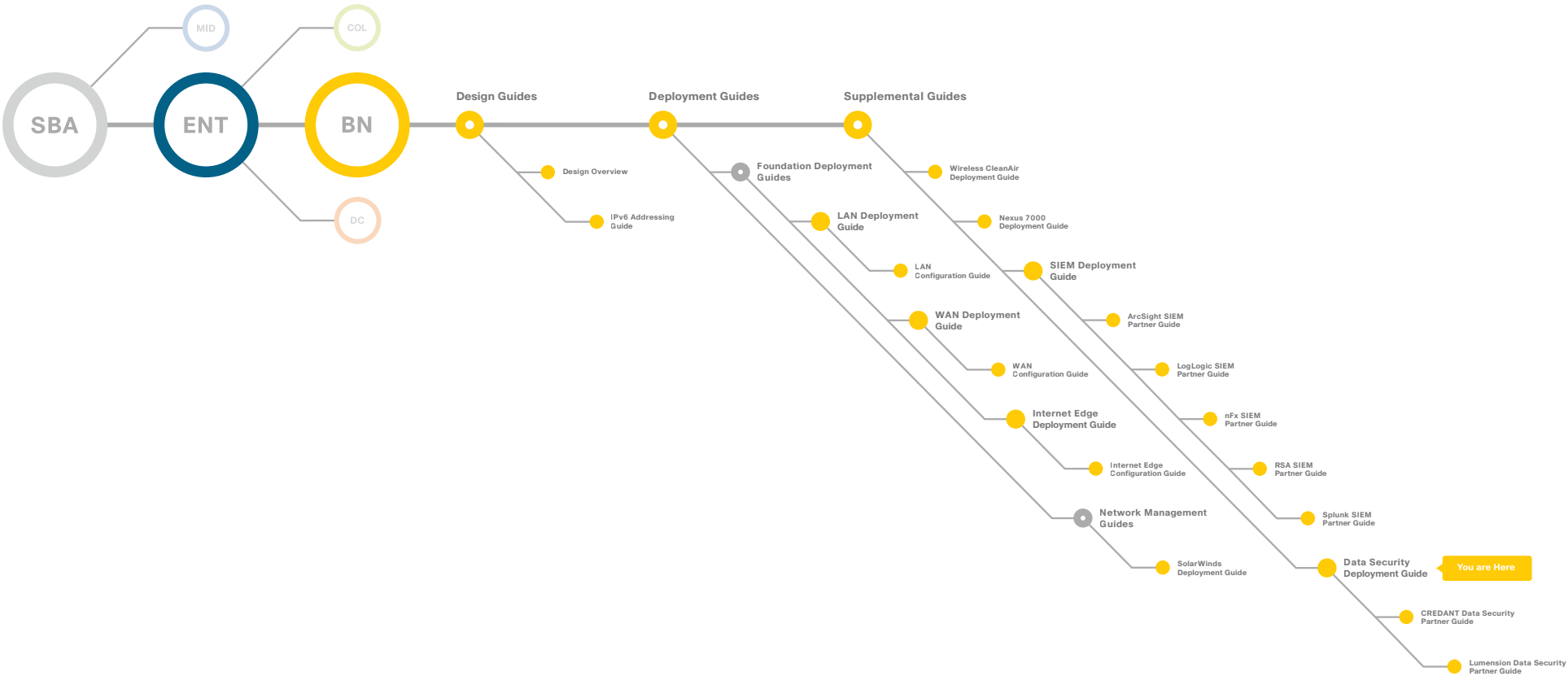
Data security challenges are growing as the second decade of the 21st century unfolds. Organizations want to protect intellectual property and comply with newly introduced regulatory requirements. To address these customer challenges and business problems, Cisco has introduced the Cisco Data Security System, which consolidates key data-security trends like DLP with other data protection technologies in a single framework. This guide provides a stepwise, streamlined implementation approach to enable the full suite of DLP in a prioritized order across the network, endpoints and data center.

## **Additional Information:**

Technology partner deployment guides can be found here:  
<http://www.cisco.com/go/securitypartners>.

## Notes

# Appendix A: SBA for Enterprise Organizations Document System







SMART BUSINESS ARCHITECTURE



**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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-609142-01 10/10