# Contents

## Topic 1
- **Overview** ................................................................. 3
  - Deployment ............................................................... 4

## Topic 2
- **Planning Data Security Deployment** .......................... 7
  - Deciding what data to protect ................................. 7
    - Geographical ....................................................... 8
    - Industry ............................................................ 8
    - Sector ............................................................... 8
    - General ............................................................. 8
  - Determining where your confidential data resides .......... 9
    - Corporate file servers and shared drives ................. 9
    - In-house databases .............................................. 9
  - Determining your information flow ................................ 10
  - Defining the business owners for the data .................. 10
  - Deciding who will manage incidents ........................... 11
  - Planning access control ........................................ 11
  - Analyzing network structure ................................... 11
    - Structural guidelines .......................................... 12
  - Planning network resources .................................... 13
    - Allocating disk space ........................................ 13
    - Modifying the disk space setting ........................... 14
    - Distributing resources ........................................ 15
  - Most common deployments ....................................... 17
    - Websense Web Security Gateway Anywhere .................. 22
    - Websense Email Security Gateway ............................ 23
    - Websense Data Monitor ......................................... 24
    - Websense Data Protect ......................................... 25
    - Websense Data Endpoint ....................................... 25
    - Websense Data Discover ...................................... 26
  - Planning a phased approach ...................................... 26
    - Phase 1: Monitoring .............................................. 26
    - Phase 2: Monitoring with notifications ..................... 27
    - Phase 3: Policy tuning ......................................... 28
    - Phase 4: Enforcing .............................................. 28
Phase 5: Discovery ............................................. 28
Phase 6: Endpoint deployments .............................. 28

Topic 3  Integrating Data Security with Existing Infrastructure .......... 31
Working with existing email infrastructure ..................... 31
   Using the SMTP agent .................................... 32
   Using the protector ......................................... 33
Working with Web proxies ...................................... 36
   Blue Coat Web proxy ...................................... 37
   Squid open source Web proxy ............................ 48
   ICAP server error and response codes .................... 49
Working with shared drives ................................. 50
   Performing discovery on Novell file systems .............. 50
   Performing discovery on Windows NFS shares .......... 52
Working with user directory servers ....................... 55
   Configuring user directory server settings ............... 56
   Importing user data ....................................... 57
   Rearranging servers ..................................... 57
Working with Exchange servers ............................. 57
Working with IBM Domino and Notes ....................... 62

Topic 4  Scaling Data Security ................................... 65
When does your system need to grow? .................... 65
   Adding modules to your deployment .................. 68
   Value of additional policy engines ................... 68
Overview

Data Security is a comprehensive data loss prevention (DLP) system that discovers, monitors, and protects your critical information holdings, whether that data is stored on your servers, currently in use or located in off-network endpoints. Data Security protects against data loss by quickly analyzing data and enforcing customized policies automatically, whether users are on the network or offline. Administrators manage who can send what information, where, and how. Data Security can also work as a part of Websense TRITON Enterprise to protect the whole of your enterprise.

The basic components of Websense Data Security are:

- The Data Security Management Server
- Optional Data Security servers
- The protector
- Agents
- Endpoints

The Data Security Management Server, a component of the TRITON management server, is the core of the system, providing complete data loss prevention analysis to the network. In addition, the Data Security Management Server gathers and stores all management statistics. For load balancing purposes, analysis can be shared among a number of Data Security servers. The protector can provide added blocking capabilities to the loss-prevention system.

The protector works in tandem with the Data Security Management Server. The Data Security Management Server performs discovery (performed by Crawler) and provides advanced analysis capabilities. The protector sits in the network, intercepts and analyzes traffic, and can either monitor or block traffic as needed. The protector supports analysis of SMTP, HTTP, FTP, Generic Text and IM traffic (chat and file transfer). The protector is also an integration point for third-party solutions that support ICAP. The protector fits into your existing network with minimum configuration and necessitates no network infrastructure changes.

In lieu of the protector, you can combine Data Security with Websense Content Gateway and Websense Email Security Gateway to block data leaks over the web and email.

Websense Data Security agents are also an integral part of the system. These agents are installed on the relevant servers (the ISA/TMG agent on the Microsoft ISA or TMG server, printer agent on the print server, etc.) to enable Data Security to access
the data necessary to analyze the traffic from these servers. Agents, such as the Data Endpoint, enable administrators to analyze content within a user’s working environment (PC, laptop, etc.) and block or monitor policy breaches. The mobile agent can prevent sensitive data from being synchronized from network email systems to mobile devices.

Deployment

A basic deployment might have just one management server and one protector, Content Gateway, or Email Security Gateway appliance. The protector includes several agents, including SMTP, HTTP, FTP, IM, and ICAP. The Content Gateway provides security for just the web channel. Email Security Gateway provides security for just the email channel.

The servers are easily configurable to simply monitor or monitor and protect sensitive data. It is ideal for small to medium businesses with a single Internet egress point. The following illustration is a high-level diagram of a basic deployment of Data Security. Such a deployment is ideal for a smaller- to medium-sized organization with a single Internet egress point. Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, internal firewalls, routing, switching, and so forth).
The following illustration is a high-level diagram of a larger deployment of Data Security.

This shows the extended capabilities of Data Security incorporated into a more complex network environment. It shows an extra Data Security server and several additional agents deployed for businesses with larger transaction volumes and numbers of users. Such a deployment is suited for large organizations with multiple Internet egress points distributed over multiple geographical locations. Very large deployments can have multiple Data Security servers and protectors.

For diagrams of the most common customer deployments, see *Most common deployments*, page 17.
Planning Data Security Deployment

Before you begin setting up your Data Security system, it is important to analyze your existing resources and define how security should be implemented to optimally benefit your specific organization. Plan your deployment by:

1. *Deciding what data to protect*, page 7
2. *Determining where your confidential data resides*, page 9
3. *Determining your information flow*, page 10
4. *Defining the business owners for the data*, page 10
5. *Deciding who will manage incidents*, page 11
6. *Planning access control*, page 11
7. *Analyzing network structure*, page 11
8. *Planning network resources*, page 13
9. *Planning a phased approach*, page 26

Deciding what data to protect

What data should you protect? What are the applicable regulations for your organization?

Answers to these questions depend on the geographical regions in which the organization operates, the industry and sector, whether it is a public company and other particulars of your organization.

Consider the following:

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>In this topic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>◆ Data Security, v7.8.x</td>
<td>◆ <em>Geographical</em>, page 8</td>
</tr>
<tr>
<td>◆ <em>Industry</em>, page 8</td>
<td>◆ <em>Sector</em>, page 8</td>
</tr>
<tr>
<td>◆ <em>General</em>, page 8</td>
<td></td>
</tr>
</tbody>
</table>
Planning Data Security Deployment

Geographical

- Each region may have its own regulations/laws that require protecting various types of sensitive information, such as private, financial, and medical.
- Global enterprises may be bound to multiple laws if they have branch offices in different regions. (For example, they may have to abide by different state laws if they have offices in several different states)

Industry

- Each type of industry may have its own laws and regulations. For example:
  - GLBA for finance
  - HIPAA for healthcare
- If your enterprise develops new technologies, you may want to protect intellectual property and trade secrets (such as designs, software code, drawings, or patent applications).

Sector

- Government agencies and organizations that are affiliated with the government are subjected to special requirements and regulations imposed by the government office, such as DIACAP for units and contractors related to the US Department of Defense and FISMA for US federal agencies and their contractors.
- For public companies, additional regulations may apply (such as the Sarbanes-Oxley Act in the U.S., or regulations that are published by the regulatory body of the relevant stock markets).

General

- Most organizations want to keep their marketing information away from competitors:
  - Upcoming press releases
  - Marketing campaigns
  - Leads
  - Existing customer data
- Many organizations have individualized needs for data protection that might not fall into typical categories, but Data Security can accommodate them.

The TRITON - Data Security first-time policy wizard assists you in defining your region and industry and it displays the relevant policies, making it easier to select them. Besides predefined policies, you may want to protect specific information, such as:

- Designs
- Drawings
Data Security Deployment Guide

- Marketing materials
- Legal documents
- Strategic planning documents, such as business plans
- Financial and pricing information
- All documents marked “Confidential”

Determining where your confidential data resides

Based on experience from numerous data-loss protection deployments, it’s evident that most sensitive company information resides within:

- Corporate file servers or shared drives
- In-house databases
- Personal laptops, workstations and removable media

Corporate file servers and shared drives

There are a few ways to determine where your confidential information is stored:

**Ask**

- Talk to appropriate data owners in your organization and they may point you to relevant locations. This may cover a big part of the information that needs to be protected and is a good start. Your review of locations based on their revelations will undoubtedly reveal other critical data branchings and parallel storage places.

**Discover**

- Use Websense Data Security to classify file servers, shared drives, and endpoints by running it with the relevant predefined policies enabled. This should give you bulk estimations of where data is located in your enterprise.

Combining the results gives you a good idea of the location of your confidential information.

In-house databases

In the case of file servers and shared drives, the best way to understand which databases are critical is:
Ask

- Talk to people that manage in-house applications relying on internal databases (such as customer relations, orders processing, and accounting).
- Talk to database administrators (DBAs) and find out what are the most accessed databases. The more a database is accessed, the more chances there are for data loss. Your IT department may also be able to elaborate on discoveries from both instances described above.

Discover

- Use Websense Data Security to classify databases by running it with the relevant predefined policies enabled. This should let you know primarily where your vital records are located.

Based on the above information, you can narrow down the most critical database servers, databases and tables to protect.

Determining your information flow

Analyze the flow of information through your enterprise today.

- Where is information typically coming from? Internal users? Partners? Vendors?
- Where does it need to be sent?
- What are all the potential pathways for information?
- What processes are in place, if any, to govern data flow?
- How many HTTP, SMTP and FTP exits or egress points are there in the organization?

These questions are vital to ensuring that protector(s) are placed appropriately so that nothing escapes analysis.

Defining the business owners for the data

The business owners of information normally come from the departments where the information was created. For example, if you wish to protect marketing materials, the head of marketing is normally the business owner, and should be consulted about deployments. (He/she may delegate the responsibility to other people in his/her department.) Normally, marketing principals—and principals from other departments—would want to get notifications about data losses containing information originating from their department (even and especially if the sender is from a different department).
Deciding who will manage incidents

How should you delegate incident management across your organization?

As in the case of business owners, you should identify who is responsible for data management in various departments. If you are unsure who that person is, you may either consult with the department manager or train one of the employees that you trust from that department.

Once incident managers are identified, you can assign the proper roles and policy category groups to the relevant users through the TRITON - Data Security Web user interface.

Planning access control

Standard network installations provide access control (preventing personnel from viewing unauthorized files) by giving each user a login and password, and authorizing each user to view only the network directories required for the user's job function. However, authorized users can still send content they are authorized to use to unauthorized recipients.

Websense Data Security augments access control by providing Information Distribution Management (IDM) capabilities, thereby greatly enhancing the level of information security. Websense Data Security protects digital content from being sent from your company’s network to people outside of the company, as well as protecting classified information from being sent to unauthorized users within the local network.

Typically, these user privileges were defined individually, without considering grouping or security clearances for groups of people. Utilizing data security capabilities involves delineating users as belonging to groups or security levels, enabling a more sophisticated, higher level of control over classified data.

Naturally, when considering the policies discussed in this chapter, it is important to consider how these policies are impacted by or impact other content policies in your company. The TRITON - Data Security software has the flexibility to accommodate the full range of enterprise security needs.

Analyzing network structure

To best employ data security, you need to analyze your network structure, determine the location of confidential information, note which documents need to be protected and where they are located, and whether you need to make changes to the network directory structure in order to group documents differently for security purposes.

In most organizations, user rights have been determined and built into the network directory structure, according to your organization's logic. You may conclude that the
network configuration is fine as it is, or that the internal network definitions change to some degree due to today's higher security needs.

Any changes you need to implement internally in the directory structure should be implemented with these increased security measures in mind.

**Structural guidelines**

It is possible to configure the system so that a particular user cannot access a certain document through the network, but can receive the document by email. For example, a manager would not want employees to access documents in his or her personal folder, but would want to be able to send the documents to them by email. It is therefore important that you perform this analysis together with the network administrator, so that your desired changes will be implemented internally in a smooth, logical fashion, as well as within the Websense structure.

Typically, your network directories are organized functionally, according to the different business units in the company. Within this structure, functional groups are usually entitled to look at documents within their business unit.

We recommended that you use this as your process map:

- Take a network map of all the directories, and look at how the network access is organized
- Determine what types of classified documents you have, and where they are located
- Determine whether documents of similar confidentiality are together in similar directories
  - Organize/group information that is critical to your organization and information whose security is legally mandated. For example, financial institutions may start by considering customer data (such as Social Security numbers or account numbers) and highly confidential business information
  - Organize/group important proprietary and confidential information with medium or low change-frequency
  - Arrange all major information assets within your organization so that you understand data locations, relationships and security-value hierarchies

The result of this analysis should be a table corresponding to the directories in the network that need to be protected, indicating what types of users should be able to receive those files and to provide a look at access issues.

You may want to rearrange some areas of your network access, and set the data security accordingly. See below for recommended procedures.
Planning network resources

To decide on things like disk space allocation, number of servers, and network distribution, start by answering these questions:

- What volume of daily data do you expect in the number of transactions?
- What is your user count?
- Are you covering geographically distributed offices?
- What is your user directory structure (Active Directory, ADAM, Domino) and the IP addresses of the LDAP servers?
- Which ports are used and what are the port numbers?

Allocating disk space

Disk space for archiving fingerprint and forensic repositories is allocated by the Websense Data Security by default. The default settings are the nominal values defined by Websense; however, you can modify these values. The tables below indicates the default and maximum disk space for archives, forensics repository and endpoint client incident storage, log file and fingerprint storage.
On the TRITON management server

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Default Setting</th>
<th>Max Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>The disk space of the incident archive folder on a local or external partition.</td>
<td>50 GB</td>
<td>Remote: No Max. Local: 50 GB (not configurable)</td>
</tr>
<tr>
<td>Forensic repository</td>
<td>The disk space of the forensic records stored in the archive folder.</td>
<td>40 GB</td>
<td>No Max.</td>
</tr>
</tbody>
</table>

On endpoint clients

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Default Setting</th>
<th>Max Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint client incident storage</td>
<td>The disk space that each endpoint client should allocate for incident storage when the endpoint host is disconnected from the TRITON Management Server.</td>
<td>100 MB</td>
<td>100 MB</td>
</tr>
<tr>
<td>Endpoint client log file</td>
<td>The disk space of the log file viewed on the endpoint client.</td>
<td>16 MB</td>
<td>100 MB</td>
</tr>
<tr>
<td>Endpoint client PreciseID fingerprint storage</td>
<td>The disk space that each endpoint client should allocate for storing directory and SharePoint fingerprints.</td>
<td>50 MB</td>
<td>1,000 MB</td>
</tr>
</tbody>
</table>

Modifying the disk space setting

Follow the instructions below to modify the default disk-space settings for either archives, endpoint client incident storage, PreciseID fingerprint or forensic repositories.

To modify disk space settings:

1. Access the Data Security manager and choose the **Settings** tab.
2. Depending on the disk space to modify, do the following:
   a. Archives:
      Select **Settings > Configuration > System > Archive Storage**. In the Maximum archive disk space field, modify the value. Only remote archives are configurable.
   b. Forensics repository:
      Select **Settings > Deployment > System Modules**. In the list of modules, select the **Forensics Repository** entry. In the Maximum Disk Space field, set the value.
   c. Endpoint client (incident storage, log file and fingerprint storage):
Select **Settings > Configuration > System > Endpoint**. In the section labeled Disk Space, modify the relevant disk-space value.

3. Click **OK**. The disk space values are set and changes saved.
4. Click **Deploy** to deploy your settings.

**Distributing resources**

Websense Data Security supports multi-site, distributed deployments. You can have a local policy engine on the Content Gateway module, for example, and distributed (primary and secondary) fingerprint repositories.

You can have a management server in one location and one or more supplemental Data Security servers in other locations.

You can utilize the crawlers on the Data Security servers alone to do your fingerprint and discovery scans, or you can install the crawler agent on additional servers to improve performance.

These are just a few of the possibilities.

Your network architecture and the geographical location of your offices determine how you will want to distribute your resources.

See *Most common deployments, page 17* for distributions our customers commonly use.

**Load balancing**

In a multi-component system, you can configure load-balancing by selecting **Settings > Deployment > System Modules** in TRITON - Data Security and then clicking the **Load Balancing** button at the top of the screen.

Load balancing enables you to manage how each module sends its data to specified policy engines for analysis. This lets you distribute the load, but more important, it ensures that your vital email and HTTP performance is never harmed. For example, you can designate 1-2 dedicated servers to analyze inline HTTP traffic (where analysis latency is critical) and use another set of servers to analyze other channels.

An agent or a protector service can be analyzed by all listed policy engines or it can be analyzed by specifically selected policy engines. (Note that protector services can be analyzed only by local or Windows-based policy engines.) In addition, you can choose which policy engine analyzes a specific agent or service of the protector.

---

**Note**

Websense recommends that you do not distribute the load to the TRITON management server.
The Load Balancing screen shows a list of items where each item represents a protector or agent.

Click each item to define which policy engine it should be analyzed by.

For further information on load balancing, refer to the Data Security Manager Help.
Most common deployments

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>In this topic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Security Gateway, v7.8.x</td>
<td>Websense Email Security Gateway, page 23</td>
</tr>
<tr>
<td>Web Security Gateway Anywhere, v7.8.x</td>
<td>Websense Data Monitor, page 24</td>
</tr>
<tr>
<td>Email Security Gateway, v7.8.x</td>
<td>Websense Data Protect, page 25</td>
</tr>
<tr>
<td></td>
<td>Websense Data Endpoint, page 25</td>
</tr>
<tr>
<td></td>
<td>Websense Data Discover, page 26</td>
</tr>
</tbody>
</table>

Websense Data Security is a flexible system that affords you various, customizable deployment scenarios. Each scenario is based on an organization’s practical needs and purposes—of course, individual hardware/software setups vary. Be sure to obtain guidance from your Websense sales representative to assure that the appropriate deployment option is tailored for your organization.
Below are the most common single and multi-site deployment scenarios.

**Scenario 1:**
- 1 TRITON Management Server
- 1 Protector

**Scenario 2:**
- 1 TRITON Management Server
- 1 Data Security Server
- 1 Protector
- Analysis is performed on the protector and supplemental server and the load is balanced between them
**Scenario 3:**
- 1 TRITON Management Server
- 2 Data Security Servers
- 1 Protector
- Analysis is performed on the protector and supplemental servers and the load is balanced between them

TRITON Management Server

---

**Scenario 4: Multi-site**
- 1 TRITON Management Server
- 2 Protectors – one for each site

<table>
<thead>
<tr>
<th>Site A</th>
<th>Site B</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRITON Management Server</td>
<td></td>
</tr>
<tr>
<td>Protectors (HTTP, SMTP, FTP, IM)</td>
<td>Protectors (HTTP, SMTP, FTP, IM)</td>
</tr>
</tbody>
</table>
**Scenario 5: Multi-site Deployment**

- 1 TRITON Management Server
- 2 Data Security Servers – one for each site
- 2 Protectors – one for each site

**NOTE:** Protector on site A performs its own analysis. It does not balance the load with the management server. No analysis is performed on the ISA Server.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Site B</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRITON Management Server</td>
<td>Data Security Server</td>
</tr>
<tr>
<td>Protector (HTTP, SMTP, FTP, IM)</td>
<td>Protector (HTTP, SMTP, FTP, IM)</td>
</tr>
<tr>
<td></td>
<td>Microsoft ISA Server (+ ISA agent)</td>
</tr>
</tbody>
</table>

---

**Scenario 6: Web Security Gateway Anywhere**

- 1 V-Series appliance
- 1 TRITON Management Server (with TRITON – Data Security and TRITON – Web Security enabled)
- 1 database server

**NOTE:** Larger deployments may have multiple appliances and management servers.

V-Series Appliance

SQL Server Log Database

TRITON Management Server
Data Security and Web Security modules
Scenario 7: Email Security Gateway

- 1 V-Series appliance
- 1 TRITON Management Server (with TRITON – Data Security and TRITON – Email Security enabled)
- 1 database server

**NOTE:** Larger deployments may have multiple appliances and management servers.
Websense Web Security Gateway Anywhere

Depending on your enterprise needs and requirements, a deployment can be subject to a variety of different combinations of components that make up Websense Data Security.

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
</table>
| • Monitoring or blocking for DLP over Web channels:  
  • HTTP  
  • HTTPS  
  • FTP  
  • FTP-over-HTTP | • 1 TRITON Management Server with Web Security and Data Security modules enabled  
  • 1 V-Series appliance  
  • 1 Windows server for Microsoft SQL Server and Log Database | **Scenario 1:**  
  • 1 TRITON Management Server with Web Security and Data Security modules enabled  
  • 1 Data Security Server  
  • Multiple V-Series appliances  
  • 1 Windows server for Microsoft SQL Server and Log Database  
  Larger organization with significant amount of traffic or multiple geographic locations. This will require load balancing between policy engines. |
| • Monitoring or blocking for DLP over Web channels:  
  • HTTP  
  • HTTPS  
  • FTP  
  • FTP-over-HTTP  
  • Monitoring or blocking of SMTP traffic | • 1 TRITON Management Server with SMTP agent and Web Security and Data Security modules enabled  
  • 1 Protector  
  • 1 V-Series appliance  
  • 1 Windows server for Microsoft SQL Server and Log Database | **Scenario 2:**  
  • 1 TRITON Management Server with Web Security and Data Security modules enabled  
  • 1 Data Security Server  
  • 1 Protector  
  • Multiple V-Series appliances  
  • 1 Windows server for Microsoft SQL Server and Log Database |
## Websense Email Security Gateway

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Monitoring or blocking for DLP over email channels:</td>
<td>• 1 TRITON Management Server with Email Security and Data Security modules enabled</td>
<td>• 1 TRITON Management Server with Email Security and Data Security modules enabled</td>
</tr>
<tr>
<td>• SMTP</td>
<td>• 1 V-Series appliance</td>
<td>• 1 Data Security Server</td>
</tr>
<tr>
<td>• Monitoring for:</td>
<td>• 1 Windows server for Microsoft SQL Server and Log Database</td>
<td>• Multiple V-Series appliances</td>
</tr>
<tr>
<td>• Web / FTP</td>
<td></td>
<td>• 1 Windows server for Microsoft SQL Server and Log Database</td>
</tr>
<tr>
<td>• IM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• User-defined protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Destination awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Larger organization with significant amount of traffic or multiple geographic locations. This will require load balancing between policy engines.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Websense Data Monitor

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Monitoring for:</td>
<td>• 1 Data Security Management Server</td>
<td>Scenario 1:</td>
</tr>
<tr>
<td>• Mail</td>
<td>• 1 protector</td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td>• Web / FTP</td>
<td>Small-to-medium business with one or more egress points (connected to the same protector) to monitor traffic. This scenario is tailored to organizations that are keen on monitoring traffic rather than enforcing traffic</td>
<td>• 1 Data Security Server</td>
</tr>
<tr>
<td>• IM</td>
<td></td>
<td>• 1 protector - load balancing with the Data Security server</td>
</tr>
<tr>
<td>• User-defined protocols</td>
<td></td>
<td>Larger organization with significant amount of traffic. In most cases, they will also plan to move to enforcement. This will require both load balancing between policy engines and building a load-balanced SMTP Agents environment (to avoid single points of failure). Note that Protector MTA can be used in those cases in which SMTP Agent is not supported on the operating system.</td>
</tr>
<tr>
<td>• Destination awareness</td>
<td></td>
<td>Scenario 2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 Data Security Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 protectors - one for each site</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organization having multiple geographical locations for monitoring traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scenario 3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 Data Security Servers - one for each site</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 protectors - one for each site</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Organization having multiple geographical locations for monitoring traffic with low latency between sites. Local policy engine is placed close to protector to avoid occupying bandwidth when sending transactions to analysis. Both protectors will do load balancing with the local policy engine.</td>
</tr>
</tbody>
</table>
# Websense Data Protect

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Data Protect module includes:</td>
<td>• 1 Data Security Management Server</td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td><strong>Data Protection:</strong></td>
<td>• 1 protector</td>
<td>• X Data Security Servers and Y protectors depending on traffic volume. The protect mode is very similar to the monitor mode; therefore, the same topologies mentioned in the monitor table apply here.</td>
</tr>
<tr>
<td>• HTTP and SMTP blocking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Policy enforcement for all channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Destination policy controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# Websense Data Endpoint

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Local discovery</td>
<td>• 1 Management Server</td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td>• Removable media &amp; CD/DVD security</td>
<td>• Endpoint clients</td>
<td>• 1 Data Security Server for every additional 15,000 endpoint clients</td>
</tr>
<tr>
<td>• Application controls for copy/paste, print, print screen, file access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Endpoint Web channels (HTTP/HTTPS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Endpoint LAN control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Planning a phased approach

Next, you need to consider the tactics you can employ in protecting your data, how to configure policies, manage incidents and control access.

To assess how to protect your data from compromise, we recommend using Websense Data Security in a multi-phased approach. Listed below is just one approach of many.

Phase 1: Monitoring

Start by monitoring data (auditing without blocking). The following steps usually constitute this phase (you may skip some of the steps if they are not relevant):

- Step A: Enable regulatory compliance, regional and industry-related predefined policies:
  - This supplies a solid first stage of DLP (data loss prevention) deployment
  - It will give you a good picture of what information is being sent out, by whom, to where and how
- Step B: Request custom policies from Websense:

<table>
<thead>
<tr>
<th>Topology</th>
<th>Small organization</th>
<th>Large org/Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Network and file discovery for data in file folders,</td>
<td>• 1 Data Security Management Server</td>
</tr>
<tr>
<td></td>
<td>SharePoint sites, databases, and Exchange servers</td>
<td>• Websense Technical Support will assess the number of Data Security servers with</td>
</tr>
<tr>
<td></td>
<td>• Automated remediation for data at rest</td>
<td>discovery and fingerprinting crawlers needed.</td>
</tr>
<tr>
<td></td>
<td>• 1 Data Security Management Server</td>
<td>• 1 Data Security Server</td>
</tr>
<tr>
<td></td>
<td>• 1 Data Security Server</td>
<td></td>
</tr>
</tbody>
</table>

**Applies to:** Data Security, v7.8.x

**In this topic:**
- Phase 1: Monitoring, page 26
- Phase 2: Monitoring with notifications, page 27
- Phase 3: Policy tuning, page 28
- Phase 4: Enforcing, page 28
- Phase 5: Discovery, page 28
- Phase 6: Endpoint deployments, page 28
Moving forward, you may identify that your enterprise has unique needs in terms of data identification that are not covered by predefined policies; for example, you may want to protect coupons that are issued or catalog numbers.

To request a policy, please apply to Websense technical support. We will escalate your request and engage the research team. The usual turnaround is approximately 3 weeks (the research team will generally provide an estimated time to completion within 3 days of reviewing the request).

- **Step C: Fingerprint data (can be also part of Phase 2):**
  - Data fingerprinting allows accurate and efficient data identification
  - Database fingerprinting (PreciseID database technology):
    - PreciseID database fingerprinting allows accurate and efficient detection of fingerprinted records coming from various sources:
      - Database tables
      - Database views
      - CSV files
  - Content policies can be flexibly defined on top of data sources. Detection rules can be configured as combinations of columns and thresholds for a given number of matches.
  - Database fingerprinting can be used in conjunction with PreciseID patterns. While patterns identify a full range of data (for example, all credit cards), database fingerprinting can narrow down the detection only to credit cards of your enterprise customers. You may want to set higher severity on PreciseID database policies than on PreciseID patterns.
  - Files, directory, and SharePoint fingerprinting (PreciseID files technology)
    - PreciseID files technology allows identification of unstructured data (free text)
    - The data that we identify can already be in a different format (e.g., after PDF conversion), different context (excerpt of confidential document that was fingerprinted), and so on
    - Advanced and efficient algorithms allow detecting fingerprints even on endpoints that have limited resources

**Phase 2: Monitoring with notifications**

At this stage, we recommend enabling email notifications to various people in the organization when a policy breach is discovered. The options are:

- Global security administrator (can be CISO)
- Data owners (specified for each policy)
- Senders (people that actually leak the information)—some enterprises prefer to use this option to educate users and watch the expected decrease in the amount of incidents over time in the Trends report.
- Managers—direct managers of people that leak information (based on data in the directory server).
Phase 3: Policy tuning

(Phase 3 can be ongoing, in parallel to Phases 1 and 2.) Make sure that you keep the amount of incidents manageable and that all incidents are relevant. The options are:

- Disable policies that do not bring value to your enterprise
- Make sure the selected channels are relevant for application of policies
- Identify incidents that are authorized transactions and make appropriate changes in the authorization for specific policies (e.g., allowing sending specific information from certain sources to certain destinations)
- Change thresholds to avoid too many incidents from some policies

Phase 3 is also good for making sure that you assign proper incident managers for various types of incidents, and that you create policy category groups in Data Security Manager and assign them to relevant incident managers.

Phase 4: Enforcing

This phase should begin after all the policies were successfully tuned and business owners, data owners and incident managers are trained and ready to handle the incidents:

- You can start with the SMTP channel only and then gradually move to HTTP enforcement as well. Or you could enforce FTP through ICAP and/or Websense Content Gateway integrations.
- Continue monitoring incidents and identify whether certain policies can be moved back to auditing only. (Consider this efficiency if you release the email regardless of incidents.)
- Encryption: As part of SMTP enforcement, you may want to integrate with encryption gateways. Websense can automatically route certain email transactions to be encrypted based on email content and/or policy definitions (actions).

Phase 5: Discovery

Again, this phase can start earlier, in parallel with other phases.

Establish discovery tasks on sensitive corporate servers, databases, Exchange servers, and SharePoint sites that are widely accessed to ensure you know what sensitive information is located where, and who is allowed to access it.

Phase 6: Endpoint deployments

As explained with other phases, this phase can also be instituted earlier in the security process.

Make sure you are controlling data in use (removable media, clipboard operations, file access) by deploying Websense Data Endpoint in your enterprise:

- It will allow controlling data in use even if users are disconnected from network
- You may decide to install it in stealth (invisible) mode

Local discovery will assist you in getting to the files that network discovery wouldn’t reach. (Essentially, local discovery is looking at the drives on a local machine, like a laptop, which can be disconnected from the network.)
Integrating Data Security with Existing Infrastructure

Websense Data Security is an integral piece of your network architecture, and can be combined with your existing systems to ensure seamless Web and email protection. See the following for information about integrating Websense Data Security with existing systems.

- Working with existing email infrastructure, page 31
- Working with Web proxies, page 36
- Working with shared drives, page 50
- Working with user directory servers, page 55
- Working with Exchange servers, page 57
- Working with IBM Domino and Notes, page 62

Working with existing email infrastructure

You can configure Websense Data Security within your existing email infrastructure to block and quarantine email that contravenes your policies.

You can do this by connecting Websense Email Security Gateway, the SMTP agent (through v7.8.2), or the Websense protector to the network directly in the path of the traffic, enabling traffic to be not only monitored, but also blocked, quarantined, or even terminated before it reaches its destination.

This section describes the SMTP agent and protector.
Using the SMTP agent

Important
This section applies to Data Security versions v7.8.1 and v7.8.2. Starting with v7.8.3, the SMTP agent is no longer available for new installations. You can use Email Security Gateway or the protector to monitor email activity, however.

If you want the option to block email that breaches policy, the SMTP agent is the easiest deployment option to configure, monitor, and debug in a production email environment. Do the following to set up the SMTP agent within your email infrastructure for this purpose:

1. Run the Websense installer as described in the Data Security Installation Guide. You install the SMTP agent as a stand-alone agent on a Windows server equipped with Microsoft IIS.
2. To configure the SMTP agent, in the Data Security manager, select Settings > Deployment > System Modules. Select the SMTP agent.
3. Complete the fields as follows:
   - In the General tab:
     - Set the Mode to Blocking.
     - Specify the action to take when an unspecified error occurs.
   - In the SMTP Filter tab:
     - Select the Enable filtering on the following internal email domains check box.
     - Enter the domain name or names to monitor and click Add.
   - In the Encryption & Bypass tab:
     - If you want encrypted or flagged email to bypass analysis, select the Enable redirection gateway check box, then enter the redirection gateway IP and port. Specify the encryption and/or bypass flags to use.
   - In the Advanced tab:
     - Specify the footer to add to analyzed email, if any.
   - Click OK to save all the above settings.
4. Select Main > Policy Management > DLP Policies. Select the policy rule that you wish to use for email management and click Edit.
5. Complete the fields as follows:
   - Select Destinations, and check the Network Email box.
   - Select Severity & Action, then select an action plan that includes notifications.
6. Click Deploy to activate the settings.
7. Configure your corporate email server to route email to the SMTP agent. (The agent becomes a MTA.)
Using the protector

There are 2 different SMTP modes:

- Monitoring mode (sometimes referred to as passive mode)
- Explicit Mail Transfer Agent (MTA) mode

In monitoring mode, the protector monitors and analyzes SMTP traffic, but does not enable policies to block transactions. It is important that not all networks have permission to send email via the protector’s SMTP service, otherwise the protector can be used as a mail relay. To avoid this, you should limit the networks that send email via the protector.

In explicit MTA mode, the protector acts as an MTA for your SMTP traffic and operates in protect mode. Protect mode allows you to block transactions that breach policy.

This section contains the basic steps required to configure Data Security for these 2 topologies.

For more information on deploying the protector inline, see “Deploying the protector” in the Data Security Installation Guide.

Pre-installation checklist

The figure below shows a common topology in which the protector is installed inline. The checklist in this section refers to the numbers in this figure.
Preparing for installation

- Verify that the required hardware is available - check the latest release notes for the list of certified hardware.
- If inline mode is selected, verify that the protector contains a certified Silicom Network card (either Dual or Quad).
- Have the following ready before installation:
  - Valid IP addresses for the Data Security server and the protector management port in the Data Security LAN
- Make sure the following IP addresses are known prior to installation - they are required in order to complete the procedure:
  - The complete list of internal networks (IP ranges and subnet masks) [1]
    If there is more than one site, the internal networks list should include the networks of all sites.
  - A list of the mail server’s IP addresses (in all sites) [4] [6]
  - The IP addresses of the mail relay, if one exists [5] [7]
  - The IP address of the outbound gateway for the protector - this will typically be the internal leg of the firewall [2]
  - The IP address of the inbound gateway for the protector - this will typically be the external leg of the backbone switch or router [6]
  - The HELO string the protector will use when identifying itself. This is relevant for the SMTP channel only.
  - If customized notifications will be displayed when content is blocked, these should be prepared beforehand.

Setting up SMTP in monitoring mode

1. Power up the protector.
2. Run the Websense installer as described in the Data Security Installation Guide. During installation make sure the time, date and time zone are precise, and map eth0 to verify it is located on the main board.
3. Connect eth0 of the protector to the LAN.
4. To configure the protector, in the Data Security manager, select Settings > Deployment > System Modules. Select the protector.
5. Complete the fields as follows:
   - In the General tab:
     - Select Enabled.
   - In the Networking tab:
     - Set Default gateway to the outbound gateway.
     - Set Interface to br0.
     - For the Connection mode, select Inline (Bridge).
     - In the Network Interfaces list, select br0 and click Edit. Select Enable bypass mode to allow traffic in case of Data Security Server software/hardware failure. Click OK.
   - In the Local Networks tab:
Integrating Data Security with Existing Infrastructure

- Select **Include specific networks**. Add all the internal networks for all sites. This list is used to identify the direction of the traffic. The mail servers and mail relays should be considered part of the internal network.
  
  - In the **Services** tab
    - Select the SMTP service. On the **General** tab, set the **Mode** to **Monitoring bridge**. On the **Traffic Filter** tab, set the **Direction** to **Outbound**. Click **OK**.
    - Select the HTTP service. On the **General** tab, set the **Mode** to **Monitoring bridge**. On the **Traffic Filter** tab, set the **Direction** to **Outbound**. On the **HTTP Filter** tab, select **Exclude destination domains** if required. Click **OK**.
  
  - Click **OK** to save all the above settings, and click **Deploy** to activate the settings.

6. Connect the protector to the outgoing connection and to the organization’s internal network. This should be done last, after the protector is fully configured.

**Setting up SMTP in MTA modes**

**Starting the protector**

1. Power up the protector.

2. Run the Websense installer as described in the [Data Security Installation Guide](#).
   Make sure the time, date and time zone are precise, and verify that eth0 (or whatever port you specified during installation) is mapped and located on the main board.

3. Connect eth0 or the designated port of the protector to the LAN.

**Configuring the protector**

1. In the Data Security manager, select **Settings > Deployment > System Modules**. Select the protector.

2. In the **General** tab:
   - Select **Enabled**.

3. In the **Local Networks** tab:
   - Select **Include specific networks**. Add all the internal networks for all sites. This list is used to identify the direction of the traffic. The mail servers and mail relays should be considered part of the internal network.

4. In the **Services** tab:
   - Select the SMTP service.
     - On the **General** tab, set the **Mode** to **Mail Transfer Agent (MTA)**.
     - On the **Mail Transfer Agent (MTA)** tab:
       - Set the **Operation Mode** to **Blocking** and select the behavior desired when an unspecified error occurs during analysis.
       - Set the **SMTP HELO name**. This is required.
       - Set the next hop MTA if required (for example, the company mail relay).
Set the addresses of all networks that are permitted to relay email messages through the protector. This is required, as it is important that not all networks have permission to send email via the protector’s SMTP service, otherwise the protector can be used as a mail relay. This list should include the addresses any previous hops, such as your mail server.

5. Click **OK** to save all the above settings for the protector.

6. Select **Main > Policy Management > DLP Policies**. Select the policy rule that you wish to use for email management and click **Edit**.

7. Complete the fields as follows:
   - Select **Destinations**, and check the **Network Email** box.
   - Select **Severity & Action**, then select an action plan that includes notifications.

   **Note**
   For more information about action plans, see the section “Action Plans” in the Data Security Manager Help.

   - Click **OK** to save all the above settings.

8. Click **Deploy** to activate the settings.

**Connecting the protector**

1. Connect the protector to the outgoing connection and to the organization’s internal network. This should be done last, after the protector is fully configured.

2. If a next hop server exists (for example, a company mail relay) you must add the protector’s IP address to its allowed relay list.

3. (Optional) Set your mail server’s next hop (smart host) to be the protector’s IP address.

**Working with Web proxies**

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>In this topic:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Data Security, v7.8.x</td>
<td>♦ <em>Blue Coat Web proxy</em>, page 37</td>
</tr>
<tr>
<td></td>
<td>♦ <em>Squid open source Web proxy</em>, page 48</td>
</tr>
<tr>
<td></td>
<td>♦ <em>ICAP server error and response codes</em>, page 49</td>
</tr>
</tbody>
</table>

If you want Websense Data Security to work with a Web proxy to monitor HTTP, HTTPS, and FTP traffic, we recommend that you use the Websense Content Gateway
Web proxy. Websense Content Gateway includes a Data Security policy engine on box and streamlines communication with the TRITON Management Server.

If you have Websense Web Security Gateway or Web Security Gateway Anywhere, the Content Gateway proxy is included in the solution.

Websense Data Security also supports the following Web proxies:

- Blue Coat
- Squid open source

These proxies integrate with Websense Data Security over ICAP, an industry-standard protocol designed for off-loading specialized tasks from proxies.

**Blue Coat Web proxy**

Blue Coat provides protocol support for HTTP, HTTPS, and FTP.

The integration solution described in this section is the recommended one. Other configurations can be implemented, but should be tested prior to deployment.

**Limitations**

- The solution does not support FTP GET method for request modification.
- The solution does not support HTTP GET method for request modification.
- The solution is limited to scan files of 10MB. The system is capable of generating an error if a file exceeds that size.
- In the described deployment caching is not in effect (Blue Coat SG does not cache PUTs and POSTs). However, you should exercise care if a response mode configuration is used.

**Deployment**

This deployment recommendation describes a forward proxy: a Blue Coat SG appliance connected to a Websense protector using ICAP. The Blue Coat SG appliance serves as a proxy for all HTTP, HTTPS, and FTP transactions. It is configured with rules that route data to the Websense ICAP server.

The Websense protector receives all traffic directed to it from the Blue Coat appliance for scanning,
The following diagram outlines the recommended deployment:

![Diagram of recommended deployment](image)

The deployment solution can be used in 2 modes:

- Monitoring mode
- Enforcement mode

You can change the mode as required.

**Enforcement mode**

In this mode, the Blue Coat SG appliance requires Websense Data Security to authorize each transaction before allowing the transactions to be posted or uploaded to
their intended destination. This is the recommended mode of operation for the solution as it provides the most security.

**Monitoring mode**

In this mode, the transactions that are redirected by the Blue Coat SG appliance are analyzed by Websense Data Security, which can then generate audits for confidential information usage as well as generate notifications for administrators and information
owners. However, in monitoring mode, the Websense ICAP server universally responds to all redirected transactions with Allow.

**Network integration**

The solution consists of 3 components:

- Websense protector
- Websense TRITON Management Server
- Blue Coat SG appliance
The Websense - Blue Coat ICAP integration component resides on the protector, and acts as a relay between the Blue Coat SG appliances and the TRITON Management Server as shown below:

![Diagram of the Websense - Blue Coat ICAP integration](image)

**Configuring the Blue Coat integration**

**System setup**

Refer to the [Data Security Installation Guide](#) for instructions on installing Websense Data Security. Refer to relevant Blue Coat documentation for more information on installing the Blue Coat appliance.

After connecting the systems, follow instructions to configure network parameters and other properties.

**Configuring Blue Coat**

The Blue Coat Proxy SG can be configured with its basic information. You will need several pieces of information to configure the Proxy SG:

1. IP address and netmask of the main interface
2. Default gateway IP address
3. DNS server IP address
4. Console user name and password
5. Enable password
6. IP address and netmask of the ICAP interface

Items 1-5 enable you to set up the initial configuration of the Proxy SG by following the steps configure the Proxy SG with a direct serial port connection in your Blue Coat installation guide.
Once you have completed those steps, you can configure the second interface on the Proxy SG for use with the Websense ICAP server.

First, log on to the Proxy SG management console following the instructions in the Blue Coat installation guide. Then configure Adapter #1 with the IP address and netmask of the ICAP interface using the steps in the Adapters section of your Blue Coat configuration guide. (Adapter #0 is configured during the serial port configuration)

**HTTPS forward proxy configuration**

To enable ILP scanning of HTTPS posted documents, the Proxy SG must be configured for HTTPS forward proxy.

To configure the HTTPS forward proxy, follow the steps in these sections of your Blue Coat configuration guide:

1. Setting up the SSL proxy in transparent proxy mode
2. Creating an issuer keyring for SSL interception
3. Downloading an issuer certificate

You can find this guide in the Documentation section of your Blue Coat account (https://bto.bluecoat.com).

**Configuring the protector for ICAP**

You configure the ICAP support on the protector in the Data Security manager.

1. Open the Data Security manager, and go to Settings > System Modules.
2. Under the protector you want to configure, select the ICAP server.

For more information, see the section “Configuring ICAP” in the Data Security Manager Help.

**Configuring the ICAP service on Blue Coat**

This section describes how to configure the Proxy SG to communicate with the Websense ICAP server on the protector.

This procedure assumes the Proxy SG is operating minimally with initial configurations, and you are logged on to the Blue Coat Management Console. If you have multiple protectors with ICAP servers, you must create a unique Proxy SG service for each one.

To configure the Proxy SG ICAP service:

1. Select **Configuration > External Services > ICAP**.
2. To add a new service:
a. Click New.

The Add list item window appears.

b. In the Add ICAP Service field, enter an alphanumeric name.

c. Click OK.
3. In the Services list, select the new ICAP service name and click **Edit**. The following screen appears:

![Edit ICAP Service window](image)

4. On the Edit ICAP Service window, configure the following options.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service URL</td>
<td>This includes the URL schema, the ICAP server host name or IP address, and the ICAP port number. For example, icap://10.1.1.1/reqmod/http or icap://10.1.1.1/reqmod/ftp. You can distinguish between encapsulated protocols using different service URLs.</td>
</tr>
<tr>
<td>Maximum number of connections</td>
<td>The maximum number of connections at any time between the Proxy SG and the ICAP server. This can be any number between 1 and 65535. The default is 5.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>The number of seconds the Proxy SG waits for replies from the ICAP server. This can be any number between 60 and 65535. The default timeout is 70 seconds.</td>
</tr>
<tr>
<td>Notify administrator</td>
<td>Check the <strong>Virus detected</strong> box to send an email to the administrator if the virus scan detects a match. The notification is also sent to the Event Log and the Event Log email list.</td>
</tr>
<tr>
<td>Method supported</td>
<td>Select <strong>request modification</strong> for this service. Also select <strong>Client address</strong> and/or <strong>Authenticated user</strong>.</td>
</tr>
<tr>
<td>Send</td>
<td>Optionally, check one or more of these options to specify what is sent to the ICAP server.</td>
</tr>
<tr>
<td>Sense settings</td>
<td>Optionally, click this to automatically configure the ICAP service using the ICAP server parameters.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
6. Click **Apply**.

**Policy setup**

This section describes how to configure the Proxy SG policy to redirect traffic across the ICAP service.

For full details of managing Data Security policies, refer to “Creating Custom Policies” in the Data Security Manager Help.

The procedure in this section assumes the Proxy SG is operating with initial configurations and ICAP configuration, and you are logged on to the Blue Coat Management Console.

To configure the Proxy SG ICAP policies:

1. Select **Configuration > Policy > Visual Policy Manager**.
2. Click **Launch**.

3. In the Visual Policy Manager, select **Add a policy**.
4. Add a content layer.
   a. Click the Web Content Layer tab.
   b. Click Add Rule.
5. Enter a policy name, and click **OK**.
6. Right click the **Action** option and select **Set** from the menu.

7. Under **Show**, select **Set ICAP Request Service Objects**.

8. Click **New > Set ICAP Request Service**.

9. Enter a name for the ICAP request service.
10. Select **Use ICAP request service**, choose a service from the drop-down list, and click **Add**.

11. Click **OK** twice.
12. Click **Install policy**.

**Configuring HTTPS policies**

To configure an HTTPS policy, follow the steps in these sections of your Blue Coat configuration guide:

1. Using the SSL intercept layer
2. Using the SSL access layer

You can find this guide in the Documentation section of your Blue Coat account (https://bto.bluecoat.com).

**Recommended Blue Coat filtering rules**

The table below lists filters that should be applied to the Blue Coat policy layer before the data is sent to the protector’s ICAP server.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Filter</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>GET</td>
<td>Allow always</td>
</tr>
<tr>
<td>HTTP</td>
<td>POST &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>HTTP</td>
<td>POST &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
<tr>
<td>HTTP</td>
<td>PUT &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>HTTP</td>
<td>PUT &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
<tr>
<td>HTTPS</td>
<td>GET</td>
<td>Allow always</td>
</tr>
<tr>
<td>HTTPS</td>
<td>POST &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>HTTPS</td>
<td>POST &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
</tbody>
</table>
Squid open source Web proxy

Squid provides protocol support for HTTP, HTTPS, and FTP. It integrates with Websense Data Security over ICAP, which is supported in Squid-3.0 and later.

Deployment

This deployment recommendation describes a forward proxy: a Squid Web proxy server connected to a Websense protector using ICAP. Squid serves as a proxy for all HTTP, HTTPS, and FTP transactions. It is configured with rules that route data to the Websense ICAP server.

The Websense protector receives all traffic directed to it from the Squid server for scanning.

The following diagram outlines the recommended deployment:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Filter</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>PUT &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>HTTPS</td>
<td>PUT &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
<tr>
<td>FTP</td>
<td>PUT &lt; 10MB</td>
<td>ICAP REQMOD</td>
</tr>
<tr>
<td>FTP</td>
<td>PUT &gt; 10MB</td>
<td>Block/Allow always</td>
</tr>
</tbody>
</table>

The deployment solution can be used in 2 modes:

- Monitoring mode
- Enforcement mode

You can change the mode as required.
Integrating Data Security with Existing Infrastructure

System setup

Refer to the Data Security Installation Guide for instructions on installing Websense Data Security, and refer to the relevant Squid documentation for more information on installing the Squid Web proxy.

After connecting the systems, follow instructions to configure network parameters and other properties.

Configuring Squid for ICAP

Set up your Squid proxy to send requests to the ICAP server that is part of the Websense protector.

This example is for Squid-3.1:

```
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
adaptation_access service_req allow all
```

This example is for Squid-3.0:

```
icap_service service_req reqmod_precache 1
icap://<protector_IP>:1344/reqmod
icap_class class_req service_req
icap_access class_req allow all
```

For full ICAP configuration details for Squid, see http://wiki.squid-cache.org/Features/ICAP?highlight=%28faqlisted.yes%29.

Configuring the protector for ICAP

You configure the ICAP support on the protector in the Data Security manager.

1. Open the Data Security manager, and go to Settings > System Modules.
2. Under the protector you want to configure, select the ICAP server.

For more information, see the section “Configuring ICAP” in the Data Security Manager Help.

ICAP server error and response codes

<table>
<thead>
<tr>
<th>Response Condition</th>
<th>Websense Block Decision</th>
<th>Control Exceeds Size Limit</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>“pana_response”</td>
<td>“huge_content”</td>
<td>“pana_error”</td>
</tr>
<tr>
<td>Error Code</td>
<td>500</td>
<td>500</td>
<td>512</td>
</tr>
<tr>
<td>“X-Response-Info”</td>
<td>PA-block</td>
<td></td>
<td>PA-error</td>
</tr>
</tbody>
</table>
Integrating Data Security with Existing Infrastructure

<table>
<thead>
<tr>
<th>Response Condition</th>
<th>Websense Block Decision</th>
<th>Control Exceeds Size Limit</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>“X-Response-Desc”</td>
<td>Websense blocked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plain URL</td>
<td>/usr/local/spicer/etc/blockmessageexample.plain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Markup URL</td>
<td>/usr/local/spicer/etc/blockmessageexample.markup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Working with shared drives

Discovery is the act of determining where sensitive content is located in your enterprise. If you have shared drives, whether on Windows or Novell, you can create a data discovery task that describes where and when to perform discovery on these drives, including specific network locations to scan.

### Performing discovery on Novell file systems

This section describes the steps required for Websense Data Security to be able to scan files and folders on Novell file servers.

The following definitions are used in this section:

- **NDS - Novell Directory Services** - Using NDS, a network administrator can set up and control a database of users and manage them using a directory with an easy-to-use graphical user interface (GUI). Users at remote locations can be added, updated, and managed centrally. Applications can be distributed electronically and maintained centrally. The concept is similar to Microsoft’s Active Directory.

- **Novell Client for Windows** - a client software used so that Windows machines can authenticate through NDS and access shared resources on Novell servers.
Preparing the Novell server

1. Create a user account in Novell eDirectory (NDS). This user will be used by the Websense Data Security crawler agent to authenticate with Novell eDirectory and access files and folders.
   The user account must have the same logon name and password as the Websense Data Security service account.

2. Make sure the newly created user has at least “Read” permissions on all files and folders that you wish to run discovery on.

Preparing the Data Security server

1. Download the latest Novell Client for Windows from the Novell Web site: http://www.novell.com/products/clients/
   Run setupnw.exe and select Custom Installation.
2. Make sure Novell Distributed Print Services is not checked and click Next.
3. Make sure NetIdentity Agent and NMAS are checked and click Next.
4. Select IP and IPX protocols and click Next.
5. Select eDirectory and click Next.
6. Wait for the installation to complete, then reboot the server.

8. After the reboot, the Novell logon window should appear instead of the regular Windows logon.

9. Log on to Windows and Novell using the Data Security service account (it should be the same user for both platforms as stated above).
   Under the eDirectory tab, you must select the tree and its relevant context for the folders you are about to run discovery on.

10. Right-click the Novell icon in the task bar and select Properties.
11. Click Cancel.
12. Ensure the files you are about to run discovery on are accessible from Windows by UNC (for example, \NovellFileSrv\vol1\Data).
13. Right-click the Novell icon in the task bar and select Novell Connections.
14. On all connections, click Detach until no connections remain.
15. Open the Data Security manager, and create a new data discovery task as follows:
   a. Select Main > Policy Management > Discovery Policies.
   b. Select Add Network Task > File System Task.
   c. On the Networks page, click Edit to select the Novell server’s IP address.
   d. Click Advanced, and add the Novell access port number 524.
   e. On the Scanned Folders page, use the Data Security service account for authentication.
   f. Set up all other options as you require.
Performing discovery on Windows NFS shares

If you want to perform data discovery on Windows file shares, you need to install NFS client on your Data Security server. If you have more than one Data Security server, install NFS client on the one with the crawler you will use to perform discovery.

Do not install Data Security on the same machine as the NFS server.

Windows Server 2003

1. On the Data Security server you will use to perform discovery, install the NFS client from the “Windows Services for Unix” package. You can download the package from Microsoft’s Technet.
2. During installation, select the following:
   - Utilities
   - NFS > Client for NFS
   - Authentication tools for NFS
   All others features must be disabled.
3. After installation has completed, select Start > Programs > Windows Services for UNIX > Services for UNIX Administration.
4. Navigate to Client for NFS and set the file permissions to All, Read, Write and Execute.
5. Under Performance, change the transport protocol from UDP to TCP and the Mount type from Soft to Hard.
6. Ensure that the buffer size is at the maximum of 32 KB.
7. Click Apply when done.
8. Navigate to User Name Mapping.
Integrating Data Security with Existing Infrastructure

9. On the Configuration tab specify whether the user name to be mapped will be imported from a Network Information Service (NIS) or from password/group files (/etc/passwd and /etc/group). For NIS mapping, enter the IP address or host name of the NIS server and the NIS domain name. Files are used in the example below.

10. On the Maps tab, select the machine or domain for the user account that will be specified in the discovery task and click List Windows Users.

11. Click List UNIX Users and specify an account that has access to the NFS share.

12. Select a user name from each list box, then click Add to map the names.

13. Log onto the TRITON Console, and select the Data Security tab.

14. Create a data discovery policy in the Data Security manager. (See the section “Creating a data discovery policy” in the Data Security Manager Help for instructions.)

Note
If you select User Password and Group Files, you only need to add the users and groups that need to be mapped.
Integrating Data Security with Existing Infrastructure

15. Create a file system task. Select Main > Policy Management > Discovery Policies, and then select Add Network Task > File System Task.

16. On the General screen, add a name and description for the discovery task and select the crawler to perform the discovery (the one where you installed the NFS client).

17. On the Networks screen, click Advanced and add port 2049 to the existing list of scanned ports.

18. On the Scanned Folders screen, specify the shared to be scanned and the user name and password of the Windows user mapped to the UNIX user name.

---

Note
Network discovery has a limit of 255 characters for the path and file name. Files contained in paths that have more than 255 characters are not scanned.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Shared folders   | Select the shared folders you want to scan:  
  - Administrative shares - Select this if you want to scan administrative share drives such as C$.  
  - Shared folders - Select this if you want to scan shared folders such as PublicDocs.  
  - Specific folders - Select this if you want to scan specific folders, then enter the name(s) of the folder(s) to scan, separated by semi-colons.  
| Method           | Select the method to use when scanning network shares:  
  - TCP - Select TCP if you want to scan the share drives using transmission control protocol.  
  - ICMP - Select ICMP if you want to scan the share drives using Internet control message protocol.  
| User name        | Enter the user name of an administrator with network access. |
19. Deploy your changes.

For more information on the wizard for creating file system discovery tasks, see the section “File System tasks” in the Data Security Manager Help.

**Working with user directory servers**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter a password for this administrator.</td>
</tr>
<tr>
<td>Domain</td>
<td>Optionally, enter the domain name of the network.</td>
</tr>
</tbody>
</table>

If you have one or more user directory servers, such as Microsoft Active Directory or IBM Domino, you should integrate your servers into Websense Data Security configuration. Once you have set up server details and imported users and groups using the Data Security manager, you can base your administrator login authentication on user directory credentials, resolve user details during analysis, and enhance the details displayed with the incident.
Configuring user directory server settings

You set up your user directory server settings as part of your initial Websense Data Security configuration:

1. Open the Data Security manager
2. Select **Settings > General > System**.
3. Select **User Directories**.
4. Click **New** in the toolbar.
5. In the Add User Directory Server dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the user directory server.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Click <strong>Enabled</strong> to enable this server as your user directory server.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of directory from the drop-down list: Active Directory, Domino, Sun, or another.</td>
</tr>
</tbody>
</table>

**Connection Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or host name</td>
<td>Enter the IP address or host name of the user directory server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the user directory server.</td>
</tr>
<tr>
<td>User distinguished name</td>
<td>Enter a user name that has access to the directory server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for this user name.</td>
</tr>
<tr>
<td>Use SSL encryption</td>
<td>Select this box if you want to connect to the directory server using Secure Sockets Layer (SSL) encryption.</td>
</tr>
<tr>
<td>Follow referrals</td>
<td>Select <strong>Follow referrals</strong> if you want Websense Data Security to follow server referrals should they exist. A server referral is when one server refers to another for programs or data.</td>
</tr>
</tbody>
</table>

**Directory usage**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get user attributes</td>
<td>Select this box if you want to retrieve user information from the directory server.</td>
</tr>
<tr>
<td>Attributes to retrieve</td>
<td>Enter the user attributes that you want Data Security to collect for all users (comma separated).</td>
</tr>
<tr>
<td>Sample email address</td>
<td>Enter a valid email address with which you can perform a test.</td>
</tr>
<tr>
<td>Test Attributes</td>
<td>Click <strong>Test Attributes</strong> to retrieve user information on the email address you supplied. Mouse over the information icon to check the user information imported.</td>
</tr>
</tbody>
</table>

6. Click **OK** to save your changes.
The server is listed on the User Directories page.

**Importing user data**

By default, Websense Data Security imports data from user directory servers daily at 3.00am. You can change the import time as follows:

1. In the Data Security manager, select **Settings > General > System**.
2. Select **User Directories**.
3. Click the **Import daily at** link.
4. Set a new time and click **OK**.

Once you have set up a user directory server, you can start an import at any time in addition to the daily schedule:

1. On the User Directories page, select the server and click **Import Now**.
2. Click **Yes** to continue.

To view user directory entries once they have been imported, go to **Main > Policy Management > Resources** and select **User Directory Entries**.

**Rearranging servers**

Once you have set up a user directory server in the Data Security manager, the server is listed on the User Directories page. If you have set up and enabled more than one server, users are imported from user directories in the order listed on this page. If a user is in more than one directory, the first directory record takes precedence.

To rearrange your servers in the order you want them:

1. Click **Rearrange Servers**.
2. Select a server and use the arrow buttons to move it up or down the list.
3. Click **OK** when done.

**Working with Exchange servers**

With Data Security, you can perform discovery on Microsoft Exchange servers. Before you begin, there are a number of steps you need to take.
**Exchange Online 365 (v7.8.2+)**

1. Create or identify an Exchange 365 account for Exchange discovery scanning.
2. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.
   - Organization Management
   - View Only Organization Management

The service account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery. Log onto OWA with this account, and try switching between mailboxes as shown below:

3. Configure Exchange impersonation. Exchange impersonation needs to be enabled for the service account used for the discovery
   a. Open the Windows PowerShell as administrator. Enter:
      ```
      $LiveCred = Get-Credential
      ```
   b. When prompted for credentials, enter the user name (email address) and password that you established for the Exchange 365 account in #1.
   c. Enter the following command:
      ```
      ```
   d. Read and ignore any warning that result. Enter the following command:
      ```
      Import-PSSession $Session
      ```
   e. Enter the following command:
      ```
      Set-ExecutionPolicy RemoteSigned
      ```
   f. When prompted if you want to change the execution policy, respond “Yes”.
   g. Enter the following command:
      ```
      Enable-OrganizationCustomization
      ```
New-ManagementRoleAssignment -Name "Impersonation-Websense" -Role "ApplicationImpersonation" -User user@mydomain.onmicrosoft.com

where:

- “Impersonation-Websense” is the name of the administrator role you’re creating for the Exchange 365 account.
- “user@mydomain” is the username you’re going to use in the discovery task.

4. Configure an Exchange discovery task.
   a. Log onto the TRITON Console and select the Data Security tab.
   b. Select Main > Policy Management > Discovery Policies > Add Network Task > Exchange Task.
   c. Complete the wizard as explained in the Data Security Manager Help. On the Exchange Servers page, enter the credentials you used in step 1 and 3b.

5. Check that Integrated Windows authentication is turned on (it should be on by default). If it is not:
   a. In the Exchange admin center, go to servers > virtual directories > EWS (Default Web Site).
   b. Select Integrated Windows authentication.

Exchange 2013

1. Define a service account for Exchange discovery scanning.

2. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.
   - Organization Management
   - View Only Organization Management

The service account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the
discovery. Log onto OWA with this account, and try switching between mailboxes as shown below:

![Image of OWA interface]

3. Configure Exchange impersonation. Exchange impersonation needs to be enabled for the service account used for the discovery
   a. Open the Exchange Management Shell.
   b. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate to the specified user.
      For example, to enable a service account to impersonate all other users in an organization, enter the following:
      ```
      New-ManagementRoleAssignment -Name:impersonationAssignmentName -Role:ApplicationImpersonation -User:ServiceAccount
      ```

4. Configure an Exchange discovery task.
   a. Log onto the TRITON Console and select the Data Security tab.
   b. Select `Main > Policy Management > Discovery Policies > Add Network Task > Exchange Task`.
   c. Complete the wizard as explained in the [Data Security Manager Help](#).

5. Check that Integrated Windows authentication is turned on (it should be on by default). If it is not:
   a. In the Exchange admin center, go to `servers > virtual directories > EWS (Default Web Site)`.
Exchange 2010

1. Define a service account for Exchange discovery scanning.
2. Grant the account one of the following roles. This is necessary so that Data Security can discover messages and display results.
   - Exchange Full Administrator
   - Exchange Administrator
   - Exchange View Only Administrator

The service account should now be able to access Exchange via Outlook Web App (OWA) and move between the mailboxes intended to be scanned during the discovery. Try switching between mailboxes as shown below:

3. Configure Exchange impersonation. Exchange impersonation needs to be enabled for the service account used for the discovery
   a. Open the Exchange Management Shell.
   b. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate to the specified user.

   For example, to enable a service account to impersonate all other users in an organization, enter the following:
Integrating Data Security with Existing Infrastructure

New-ManagementRoleAssignment -
Name: impersonationAssignmentName -
Role: ApplicationImpersonation - User: ServiceAccount

For more information on Exchange impersonation, see msdn.microsoft.com/en-us/library/bb204095.

4. Configure an Exchange discovery task.
   a. Log onto the TRITON Console and select the Data Security tab.
   b. Select Main > Policy Management > Discovery Policies > Add Network Task > Exchange Task.
   c. Complete the wizard as explained in the Data Security Manager Help.

Working with IBM Domino and Notes


Domino environments normally consist of one or more servers working together with data stored in Notes Storage Format (NSF) files. There are usually many NSFs on any given Domino server. NSF repositories contain documents and email messages, but Data Security performs discovery only on documents.

These sections describe how to integrate your system with Data Security.

Before you begin

Before you begin, make sure that you:
1. Install IBM Notes on the machine where you will install the Data Security crawler. This can be the machine where you plan to install the Data Security server software; or it can be a stand-alone machine where you plan to install the crawler agent.

   **Important**
   The crawler you will use for Domino fingerprinting and discovery must be on the same machine as Notes.

   Be sure that the installation is done for “Anyone who uses this computer.”

2. Log on to Notes and supply a user.id file and password.

3. Connect to the Domino server from the Notes client. This should be done by the user who will be installing the crawler. For best practice, do not run Notes on this machine again after the crawler is installed.

**Getting started**

To integrate Data Security with your Domino Server:

1. Run the Data Security installation wizard on a machine with the Notes client. For best practice, do not run the Notes client on the machine on which the Data Security crawler is installed.

2. During installation, the installer detects the Notes client and displays the Domino Connections page. On this page:
   a. Select the check box labeled Use this machine to scan Domino servers.
   b. In the User ID file field, browse to one of the authorized users, then navigate to the user’s user.id file.

   **Note**
   Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

   c. In the Password field, enter the password for the authorized user.

   **Note**
   If you need to update the **User ID** and **Password** fields, run the installation wizard and select **Modify**.

**Domino discovery**

Domino discovery treats a document (body and attachments) as one unit. This way, a breach is reported even if the sensitive content is scattered in different parts of the document that individually would not cause an incident.

To perform discovery on documents:
1. Log on to the Data Security manager, and create a discovery policy. To do so:
   a. Navigate to Main > Policy Management > Discovery Policies.
   b. Select Locate regulatory & compliance data or Create custom policy.
   c. Complete the steps in the wizard as described in the Data Security Manager Help. You can choose dictionary, RegEx, fingerprinting, or other classifiers as needed.

2. Create a Domino discovery task. To do so:
   a. Navigate to Main > Policy Management > Discovery Policies.
   b. Select Add network task > Domino Task.
   c. Complete the steps in the wizard as described in the Data Security Help.

3. To deploy the policy and task to the Domino server, click Deploy. The Domino server will be crawled for your sensitive data at the next scheduled time. Incidents are reported under Main > Reporting > Discovery.

**Domino fingerprinting**

Domino fingerprinting treats the body of a document and each of its attachments as a separate item. This enables the system to show the full path down to the item inside a document that caused a breach.

To fingerprint documents:

1. Log on to the Data Security manager, and create a Domino fingerprinting classifier. To do so:
   a. Navigate to Main > Policy Management > Content Classifiers > File Fingerprinting.
   b. Select New > Domino Fingerprinting.
   c. Complete the steps in the wizard as described in the Data Security Manager Help.

2. Create a Data Loss Prevention (DLP) policy using the following classifier:
   b. Select Create custom policy.
   c. Complete the steps in the wizard as described in the Data Security Manager Help. Be sure to select the fingerprinting classifier on the Condition page.

3. To deploy the policy and classifier to the Domino server, click Deploy. The data on your Domino server will be fingerprinted at the next scheduled time. Incidents are reported under Main > Reporting > Data Loss Prevention.
Scaling Data Security

As your network (and the security needs of your network) grows, Websense Data Security can grow with it. Our software is architected for scalability, even for networks with massive traffic and complex topologies. The sections below address network growth issues such as recognizing when system loads demand system expansion, single and multi-site configuration and how to deal with the growth of the various information repositories.

- **When does your system need to grow?, page 65**
- **Adding modules to your deployment, page 68**

**When does your system need to grow?**

There are numerous triggers that might prompt your system expansion. Among them:

- **Performance issues**
  
  You may or may not be aware of performance issues affecting your system. If you are experiencing slow discovery or fingerprinting scans, for example, this could be an indication of an overworked crawler. You may benefit from an additional crawler or Data Security server. If user are experiencing slow Web or email transactions, you may benefit from an additional policy engine. Even if you are not aware of performance issues, your system resources may not be fully optimized.

  To see how your system is performing, open the Data Security manager and select **Main > Status > System Health.** You can expand each module and view statistics on the load, the number of transactions, the latency, and more.

  Before adding modules, try balancing the load between your existing Data Security servers (policy engines). To do this, go to **Settings > Deployment > System Modules**, and click **Load Balancing.** Select a service and indicate which policy engine you’d like to assign to that service.

  **Note**

  Websense recommends that you do not distribute the load to the TRITON Management Server.
**The number of users grows**

In a typical small organization (1-500 users), you might only need a TRITON Management Server and a protector to monitor traffic. A larger organization (500-2,500 users) might have a TRITON Management Server, a supplemental Data Security server, and a protector, with load balancing between the protector and supplemental server. (You cannot balance the load with the management server.)

As your number of users grows, so does your need for a Data Security server.

**The number of transactions grows**

This is the most important requirement for determining your Data Security needs. Typically the number of transactions grows as your number of users grows.

*In monitoring mode*, Websense recommends having 1 protector per 20,000 users. This calculation assumes:

- The protector is monitoring HTTP and SMTP
- There are 9 busy hours per day
- There are approximately 20 million transactions per day with a ratio of 15:1 HTTP:SMTP. (HTTP includes GETs and POSTs.)

For more users, add an extra Data Security server and balance the load between the protector and the extra server.

In *blocking* mode, Websense recommends 1 TRITON Management Server, 1 SMTP agent, and 1 V-Series appliance with Websense Content Gateway software. This calculation assumes:

- There are 9 busy hours per day
- There are approximately 15 million transactions per day with a ratio of 15:1 HTTP:SMTP. (HTTP includes GETs and POSTs.)
For more users, add an extra Data Security server.

Note that your transaction volume can grow even if your user base does not. If you anticipate adding a significant amount of traffic, you’d benefit from adding one or more Data Security servers.

- **The number of endpoints grows**
  If you subscribe to the Data Endpoint and you are adding endpoints to the system, you may need additional servers. A general rule of thumb is to add 1 Data Security server for every 15,000 endpoint clients.

- **Moving your deployment from monitor to protect**
  Enforcement requires more resources, particularly because load-balancing must be enforced between policy engines and SMTP agents. If you are moving from monitor to protect, you may benefit from an additional Data Security server.

- **Moving from a single-site to multi-site configuration**
  Websense Data Security supports multi-site, distributed deployments. You can have a local policy engine on the protector, for example, and distributed (primary and secondary) fingerprint repositories. You can have a management server in one location and one or more supplemental Data Security servers in other locations.
  
  You can utilize the crawlers on the Data Security servers alone to do your fingerprint and discovery scans, or you can install the crawler agent on additional servers to improve performance. These are just a few of the possibilities, and of course, all are scalable.
  
  See *Most common deployments, page 17*, for distributions our customers commonly use.

  Regardless, organizations having multiple geographical locations need a protector for each site. If you have multiple geographical locations with low latency between sites, you may need 2 protectors and 2 supplemental Data Security servers.

- **Adding branch offices**
  Each branch office requires a protector. If you are adding or acquiring a branch office, you should add a protector.

- **Adding HTTP, SMTP and FTP egress points**
If you are adding egress points to your network structure, you need to protectors to monitor or protect those egress points.

**The network grows (in GB)**

If you are performing network discovery, your network size greatly affects your requirements, as does the frequency of full versus differential scans. If your network is growing, you may require an additional crawler or Data Security server.

**Repositories such as forensics, fingerprint, policy database are reaching their maximum**

The Data Security software has some default settings for the disk-space requirements of its fingerprint and forensic repositories, but you can modify all of the values. Businesses with larger transaction volumes and numbers of users can adjust values significantly upward. (See *Allocating disk space*, page 13.)

At some point, however, you may want to add another server to accommodate these repositories and increase your disk space. The forensics repository can get very large. It has a default setting of 40 GB. The archive has a default setting of 50 GB.

### Adding modules to your deployment

If network and security requirements dictate that you need to add new agents or other modules to your deployment, go to the machine where you want to install them and run the Data Security installation wizard.

When you install the module, you are asked to provide the FQDN of the TRITON management server and the credentials for a TRITON administrator with Data Security system modules permissions. When you do, the module is automatically registered with the management server.

If you accept the default configuration, all you have to do is click **Deploy** in the Data Security manager (on the management server) to complete the process. If you want to customize the configurations, go into the System Modules screen and click the module to edit.

Only a management user with system modules permissions can install new network elements.

For information on adding and configuring modules, see **Managing System Modules > Adding modules** in the Data Security Manager Help.

### Value of additional policy engines

Policy engines analyze transactions sent from various agents and protectors. The protector monitors network traffic and sends transactions to policy engines for analysis. The CPU load on the protector is much lighter than on a policy engine; therefore, when scaling up, you should add more policy engines (not protectors) and load-balance the analysis between them.
Assessing the need for additional policy engines

Check the number of transactions analyzed by the policy engine by selecting **Main > Status > System Health** and clicking on a policy engine.

View the “Analysis status” chart for the policy engine.

If there is red on the chart, this indicates a heavy load on the policy engine during the designated period.

If you are in monitoring mode, a few red bars may not be an issue. The system will process these incidents during a less busy period.

If you are in blocking mode, even one hour of red is undesirable. If you see this, you should perform load balancing and/or add a new Data Security server.

Optimizing

- Try to avoid analysis of incoming traffic. If incoming is a must, try to limit it to certain domains.
- Never scan all networks; establish limits.
- Check the top policies and see if there are any false positives or unwanted/not needed policies a week or two after first deployment.
- If possible, make sure no spam SMTP mail is undergoing analysis.