# Deployment Guide

Forcepoint DLP

v8.4.x

Wiz - EXHIBIT 1135
Wiz, Inc. v. Orca Security Ltd.
IPR2024-01191

©2017, Forcepoint
All rights reserved.
10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759

Published 2017

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint. Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

# Contents


Chapter 1 **Overview . . . . . 1**

Deployment options . . . . . 2
System requirements for Forcepoint DLP components . . . . . 3
What is the protector?. . . . . 4
What is mobile agent? . . . . . 6
What is the integration agent? . . . . . 7

Chapter 2 **Planning Forcepoint DLP Deployment . . . . . 9**

Deciding what data to protect. . . . . 9
Determining where confidential data resides . . . . . 11
Determining information flow . . . . . 12
Defining the business owners for the data . . . . . 12
Deciding who will manage incidents . . . . . 12
Planning access control . . . . . 12
Analyzing network structure . . . . . 13
Planning network resources . . . . . 14
Most common deployments . . . . . 16
Forcepoint DLP with Forcepoint DLP Endpoint . . . . . 17
Forcepoint DLP protector with ICAP . . . . . 18
Forcepoint DLP Network with Web Content Gateway . . . . . 18
Forcepoint Data Discover . . . . . 20
Forcepoint DLP with protector MTA and mobile agent. . . . . 21
Forcepoint DLP Cloud Applications. . . . . 22
Forcepoint DLP integrated with Forcepoint Web Security, Forcepoint Email Security, or both . . . . . 23
Planning a phased approach . . . . . 25

Chapter 3 **Integrating with Existing Infrastructure . . . . . 29**

Working with existing email infrastructure . . . . . 29
Pre-installation checklist . . . . . 30
Working with web proxies . . . . . 31

Chapter 4 **Scaling Forcepoint DLP . . . . . 37**

When does the system need to grow?. . . . . 37
Adding modules to the deployment . . . . . 40

# 1 Overview

Forcepoint DLP can protect organizations from information leaks and data loss at the perimeter and inside the organization, as well as in certain Infrastructure as a Service (IaaS) platforms. It can operate as a standalone product, or be paired with Forcepoint Web Security or Forcepoint Email Security to provide a comprehensive security solution.

- Forcepoint Data Discovery can be used to learn the location of sensitive data both on-premises an in supported cloud-based applications. It can be used to scan data on file servers, email servers, and databases, as well as in content collaboration applications, such as Microsoft SharePoint and Box.
- Forcepoint DLP Network can be used to prevent data loss through email and over web channels (HTTP, HTTPS and FTP). It also supports the scanning of content supplied by third-party solutions, such as Citrix FileShare, via the ICAP protocol.
- With Forcepoint DLP Endpoint, an endpoint agent can be used to prevent data loss over endpoint channels such as removable storage devices, mobile devices, browser uploads, and email clients and applications (such as IM and file share clients). It can also discover and remediate sensitive data stored on laptop and desktop systems. The endpoint agent lets administrators analyze content within a user's working environment and block or monitor policy breaches as defined by the endpoint profiles.
- Both Forcepoint DLP Network and Forcepoint DLP Endpoint include a mobile agent that can apply DLP policies to email traffic that is synchronized to mobile devices using Microsoft Exchange ActiveSync.

The basic components of Forcepoint DLP solutions are:

- Management server

  The management server hosts both the Forcepoint Security Manager (the graphical interface used to manage Forcepoint DLP and other Forcepoint security solutions) and core Forcepoint DLP components. It also acts as the primary Forcepoint DLP server.

  Although there is only one management server, additional Forcepoint DLP servers may be deployed for load balancing.
- Protector (requires a Forcepoint DLP Network subscription)

  The protector is a soft appliance that intercepts and analyzes traffic on SMTP, HTTP(S), and FTP channels, among others. It also supports DLP content scanning with third-party proxies and data sharing solutions via ICAP.

See *What is the protector?*, page 4.

- Analytics engine

  The analytics engine identifies and ranks high-risk behavior. It consumes incidents generated by DLP policies to create cases with a data loss or data theft risk score.

- Agents

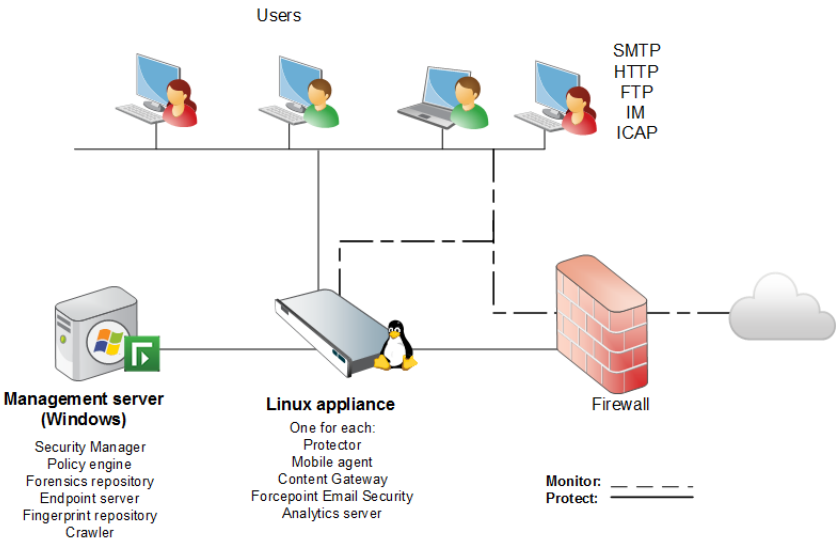
  A variety of agents extend Forcepoint DLP functionality to work with mobile devices (mobile agent), cloud-based services (cloud agent), and so on.

- Endpoint clients

  Endpoint client software runs on end user desktop and laptop machines

## Deployment options

A basic deployment might have just one management server and an analytics server. To extend enforcement capabilities, it might add a protector, mobile agent, Content Gateway, or Forcepoint Email Security appliance.



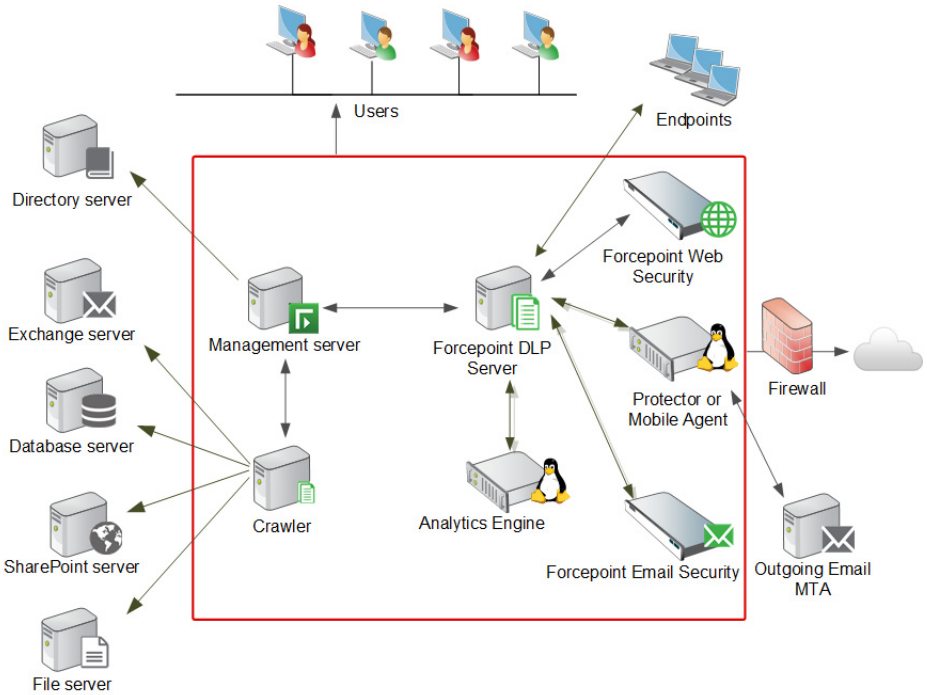

The high-level illustration shows a basic deployment ideal for a smaller- to medium-sized organization with a single Internet egress point. (The illustration is intended to show the general distribution of components and does not include network details, such as segmenting, internal firewalls, routing, switching, and so forth.)

- The analytics server is used for Incident Risk Ranking reports.
- The protector can protect several channels, including SMTP, HTTP, FTP, and ICAP.
- The mobile agent provides protection for mobile devices using Exchange ActiveSync.
- The Content Gateway provides security for the web channel.

- Forcepoint Email Security provides security for the email channel.

The servers can be configured to either monitor or monitor and protect sensitive data.

The following illustration is a high-level diagram of a larger Forcepoint DLP deployment:




This shows the extended capabilities of Forcepoint DLP incorporated into a more complex network environment. It includes an extra Forcepoint DLP server and several additional agents to support larger transaction volumes and numbers of users. A deployment might also include virtual appliances in cloud service infrastructures such as Microsoft Azure. Very large deployments can have multiple Forcepoint DLP servers and protectors.

For diagrams of the most common customer deployments, see *Most common deployments*, page 16.

## System requirements for Forcepoint DLP components

In preparation for deployment, the system requirements for all Forcepoint DLP components can be found in the *Deployment & Installation Center*.

- For operating system, hardware, and virtualization (VM) requirements, see System requirements for this version.
- For port requirements, see Forcepoint DLP ports (the “Forcepoint management server” section).

# What is the protector?

The protector is a component of Forcepoint DLP that can monitor and report on web traffic and act as an MTA to monitor, block, quarantine, and encrypt email traffic.

As an alternative, Forcepoint Email Security can be used as the MTA.

For enforcement over the HTTP/S channel, the protector can integrate with a third-party proxy that supports ICAP. (As an alternative, use the Web Content Gateway.)

## When to use the protector

The protector works in tandem with a Forcepoint DLP server.

- The Forcepoint DLP server provides advanced analysis capabilities, while the protector intercepts network traffic and either monitors or blocks it, depending on the channel.
- The protector supports analysis of SMTP, HTTP/S, FTP, and plain text. It can monitor or block email traffic, but only monitor web traffic. Blocking web traffic requires integration with a third-party proxy that supports ICAP.

The protector fits into the network with minimal configuration. It requires no network infrastructure changes.

The protector is the best choice for monitoring SMTP traffic. Just connect the protector to a SPAN or mirror port that reflects the SMTP traffic.

For email blocking capabilities, either use the protector's explicit MTA mode or use Forcepoint Email Security.

Do not use both options for the same traffic. Some organizations do, however, prefer monitoring on one point and enforcing policies on another, due to differences in network traffic content and load.

To monitor HTTP traffic, either use the protector or integrate Forcepoint DLP with Forcepoint Web Security or another web proxy.

To monitor FTP or plain text, use the protector. Note that the protector cannot block traffic on these channels. Use Forcepoint Web Security (as a DLP agent) to block FTP, or integrate with another web proxy that buffers FTP and supports ICAP.

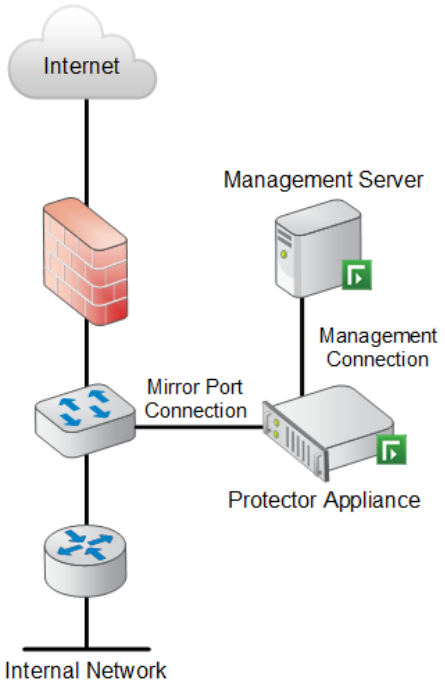
## Deploying the protector

Protectors can be used in monitoring mode for data loss detection. When deployed in this manner, they do not interfere with network traffic, but they also cannot prevent (block) data loss—only note and report losses that occur.

For each data loss detection channel, the protector can be deployed to use the following modes:

| Service | Function |
|---|---|
| **HTTP** | Monitoring |
| **SMTP** | Monitoring passive<br>Mail Transfer Agent (MTA) |
| **All Others** | Monitoring |
| **ICAP** | Monitoring<br>Blocking |

In monitoring mode, the protector is connected off the network via the SPAN/mirror port of a switch (or via a network TAP), as shown in the following diagram. This allows the protector to monitor and analyze traffic, but not block it.




The protector must connect both to the SPAN/mirror port or TAP, and the Forcepoint DLP management server.

For additional diagrams showing typical protector deployments, see *Forcepoint DLP protector with ICAP*, page 18, and *Forcepoint DLP with protector MTA and mobile agent*, page 21.

# What is mobile agent?

The mobile agent is a CentOS 7-based appliance used to secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

The mobile agent analyzes content when users synchronize their mobile devices to your organization's Exchange server. If content or data being pushed to their device breaches the organization's mobile DLP policy, it is quarantined or permitted accordingly.

The mobile agent is included with Forcepoint Email Security, Forcepoint DLP Endpoint, and Forcepoint DLP Network subscriptions.

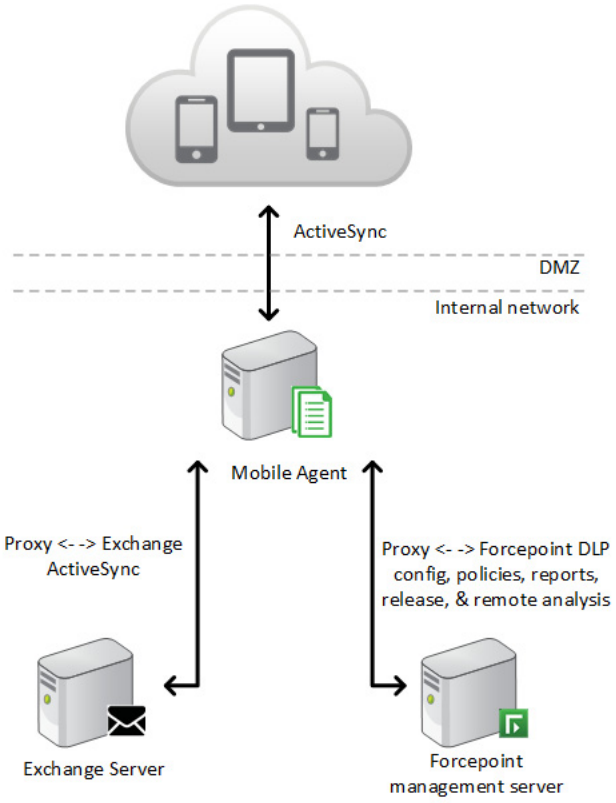
## Deploying the mobile agent

Within the network, the mobile agent appliance connects to the management server and to a Microsoft Exchange server. DLP analysis is done on the appliance or on other Forcepoint DLP servers (rather than on the management server) to optimize performance and balance the load.

Outside the DMZ, the mobile agent connects to any Microsoft ActiveSync-compatible mobile device (such as iPads, Android mobile phones, and iPhones) over 3G and wireless networks. (ActiveSync is a wireless communication protocol used to push resources, such as email, from applications to mobile devices.)

Unlike the protector, the mobile agent appliance acts as a reverse proxy, because it retrieves resources, such as email, from the Exchange server on behalf of the mobile device.

The following diagram illustrates the system architecture of a typical mobile agent deployment. Depending on your network and security requirements, you can also go through an edge device that acts as a reverse proxy to the mobile agent.




Mobile agent installations include:

- A policy engine
- Secondary fingerprint repository (the primary is on the management server)

## What is the integration agent?

The integration agent allows third-party products to send data to Forcepoint DLP for analysis.

Third parties can package the integration agent inside their own installer using simple, industry standard methods that are completely transparent to end users.

When the third-party product is installed on a users system, it needs to register the integration agent with the management server. This can be done transparently through the installation process or using a command-line utility.

The integration agent works on Windows Server, 64-bit machines.

The system treats third-party products that use the integration agent as it does any other agent.

It supports all relevant views and capabilities, including:

- Incident Management and Reporting
- Quarantine and Release of emails
- Traffic log view
- Load balancing capabilities

For information on configuring the integration agent, see “Configuring the integration agent” in the Forcepoint DLP Administrator Help.

# 2 Planning Forcepoint DLP Deployment

Before installing Forcepoint DLP, analyze the existing resources to make a comprehensive security plan, using the following steps:


1. *Deciding what data to protect*, page 9
2. *Determining where confidential data resides*, page 11
3. *Determining information flow*, page 12
4. *Defining the business owners for the data*, page 12
5. *Deciding who will manage incidents*, page 12
6. *Planning access control*, page 12
7. *Analyzing network structure*, page 13
8. *Planning network resources*, page 14
9. *Planning a phased approach*, page 25


## Deciding what data to protect

What data does the organization need to protect? What data privacy laws, regulations, and compliance concerns and obligations does the organization have?

Consider the factors described below to define the scope of what needs to be protected.

### Geographical factors

- Each region may have its own regulations or laws that require protecting various types of sensitive information, such as personal, financial, and medical data.
- 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 and Banking

  - HIPAA for Healthcare and Pharma
- Organizations that develop new technologies may need 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 subject to special requirements and regulations, such as DIACAP for units and contractors related to the U.S. Department of Defense and FISMA for U.S. 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

- Marketing data, like the following, may need to be kept secret from competitors:
  - Upcoming press releases
  - Marketing campaigns
  - Leads
  - Customer contact information and other customer data

Many organizations have individualized needs for data protection. Though these might remain outside typical categories, Forcepoint DLP can accommodate them.

The Forcepoint DLP first-time policy wizard assists administrators in defining the organization's region or regions and industry. It then displays relevant policies, making it easier to select them for monitoring and enforcement.

The policy wizard launches automatically when a Forcepoint DLP administrator logs on to the Forcepoint Security Manager after installation or upgrade.

After selecting the appropriate predefined policies, administrators can create policies to protect specific information or types of information, such as:

- Designs
- Drawings
- Marketing materials
- Legal documents
- Strategic planning documents, such as business plans
- Financial and pricing information
- All documents marked "Confidential"

# Determining where confidential data resides

Based on experience from numerous Forcepoint DLP deployments, it appears that most sensitive company information resides in:

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

## Corporate file servers and shared drives

To determine where confidential information is stored:

- **Ask**: Talk to appropriate data owners within the organization to find relevant file servers and data stores.

  This can uncover a large portion of the data that needs to be protected. Reviewing the locations that result from this process will likely reveal other critical data branchings and parallel storage places.
- **Discover**: Define policies for data discovery, then use Forcepoint DLP to classify file servers, shared drives, and endpoints. This helps identify where data is located in the network.

Combining the results can provide a good idea of the location of the organization's confidential information.

## In-house databases

To understand which databases are critical:

- **Ask**:
  - Talk to people that manage in-house applications that rely on internal databases (such as customer relations, order processing, and accounting).
  - Talk to database administrators to identify the most-accessed databases. The more a database is accessed, the more chances there are for data loss.

  The IT department may be able to elaborate on the results of talking to both of these groups.
- **Discover**: Define policies for database discovery, then use Forcepoint DLP to classify databases. This should let you know primarily where your vital records are located.

Combining the results can narrow down the most critical database servers, databases, and tables to protect.

## Determining information flow

Analyze the flow of information through the organization:

- Where is information typically coming from? Internal users? Partners? Vendors?
- Where does information need to be sent?
- What are 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 Forcepoint DLP protectors 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, for marketing materials, the head of marketing is normally the business owner. That person should be consulted about Forcepoint DLP deployments that protect marketing data.

Normally, principals from affected departments 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 incident management be delegated across the organization?

Identify who is responsible for data management in various departments. If this is unclear, consult with the department manager or train a trusted individual from that department.

Once incident managers are identified within the organization, they can be assigned appropriate roles and permissions in the Forcepoint Security Manager.

## Planning access control

Most networks provide access control (preventing personnel from viewing unauthorized files) by giving each user a login name and password, and authorizing each user to view only the network applications and content that the user requires.

Authorized users, however, can still send content they are authorized to use to unauthorized recipients.

Forcepoint DLP augments access control by providing Information Distribution Management (IDM) capabilities, thereby greatly enhancing the level of information security. Forcepoint DLP protects digital content from being sent from within the network to external recipients, as well as protecting classified information from being sent to unauthorized users within the local network.

To make the most of data security capabilities, delineate users as belonging to groups or security levels, enabling a sophisticated, high level of control over classified data.

Naturally, when considering the policies discussed here, it is important to consider how these policies are impacted by or impact other content policies within the organization.

# Analyzing network structure

To best employ Forcepoint DLP:

- Analyze your network structure.
- Determine the location of confidential information.
- Note which documents need to be protected and where they are located.
- Determine whether changes to the network directory structure are needed to group documents differently for security purposes.

In most organizations, user rights have been determined and built into the network directory structure. The existing configuration may be fine as it is. On the other hand, internal network definitions may need to change to accommodate current, higher security needs.

## Structural guidelines

It is possible to configure the system so that a particular user cannot access specified documents through the network, but can receive them 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 to perform this analysis with a network administrator, so that changes are implemented in a smooth, logical fashion.

Typically, 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.

The recommended process is:

- Take a network map of all the directories, and look at how the network access is organized.

- Determine what types of classified documents the organization has, and where they are located.
- Determine whether documents of similar confidentiality are together in similar directories.
  - Organize/group information that is critical to the 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 so that data locations, relationships, and security-value hierarchies are well understood.

The result of this analysis should be a table identifying the directories in the network that need to be protected, indicating what types of users should be able to receive those files. This should provide insight into access issues.

It may be desirable to rearrange some areas of network access, and set the data security accordingly. See below for recommended procedures.

# Planning network resources

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

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

## Allocating disk space

Forcepoint DLP allocates a default amount of disk space for archiving fingerprint and forensic repositories. Administrators can modify the allocation. The tables below indicate the default and maximum disk space for archives, the forensics repository, endpoint client incidents, log files, and fingerprint storage.

Modify disk space settings after installation using the Forcepoint Security Manager. Instructions can be found in the Forcepoint DLP Administrator Help.

### On the management server

| Type | Description | Default | Maximum |
|---|---|---|---|
| Archive | The disk space of the incident archive folder on a local or external partition. | 50 GB | Remote: None<br>Local: 50 GB |
| Forensic repository | The disk space of the forensic records stored in the archive folder. | 40 GB | None |

### On endpoint client

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

## Distributing resources

Forcepoint DLP supports multi-site, distributed deployments. Among other examples:

- In addition to the management server, there can be one or more supplemental Forcepoint DLP servers to balance the load.
- The Web Content Gateway includes its own local policy engine to supplement the policy engine on other servers.
- It is possible to have distributed (primary and secondary) fingerprint repositories.
- The crawlers on the Forcepoint DLP servers can be used for fingerprint and discovery scans, or standalone instances of the crawler agent can be added to improve performance.

Network architecture and geographical factors of the organization contribute to determining the best way to distribute Forcepoint DLP resources.

See *Most common deployments*, page 16, for examples.

### Load balancing

Load balancing allows administrators to configure how each Forcepoint DLP module sends its data to specified policy engines for analysis. This both distributes the load and, more importantly, ensures that the organization's email and HTTP performance are never harmed.

For example, designate 1-2 dedicated servers to analyze HTTP traffic (where analysis latency is critical), and use another set of servers to analyze other channels.

An agent or a protector service can have its traffic analyzed by all listed policy engines, or by specifically selected policy engines. (Note that protector traffic can be analyzed only by local or Windows-based policy engines.) Administrators can specify which policy engine analyzes a specific agent or service of the protector.

**Note**
Forcepoint recommends that you do not distribute the load to the management server.

Load balancing is configured in the Data Security module of the Security Manager. See the Forcepoint DLP Administrator Help for instructions.

## Most common deployments

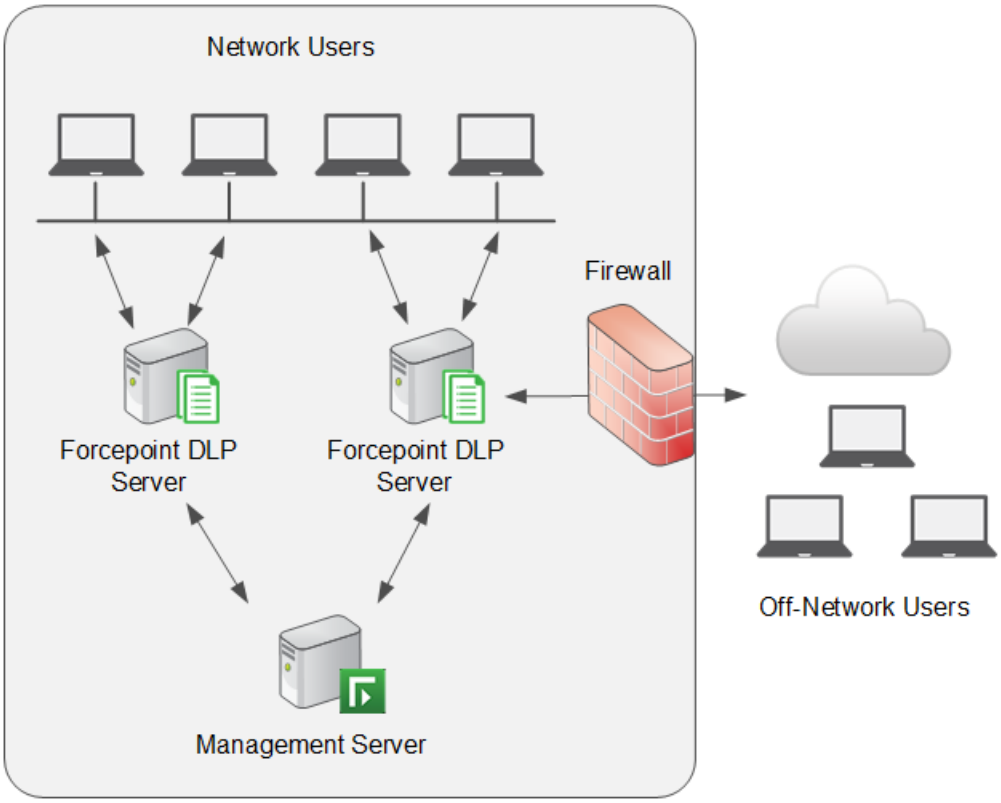
Forcepoint DLP is a flexible solution that affords various, customizable deployment scenarios. Be sure to obtain guidance from a Forcepoint Sales representative to find the best deployment option for your organization.

## Forcepoint DLP with Forcepoint DLP Endpoint

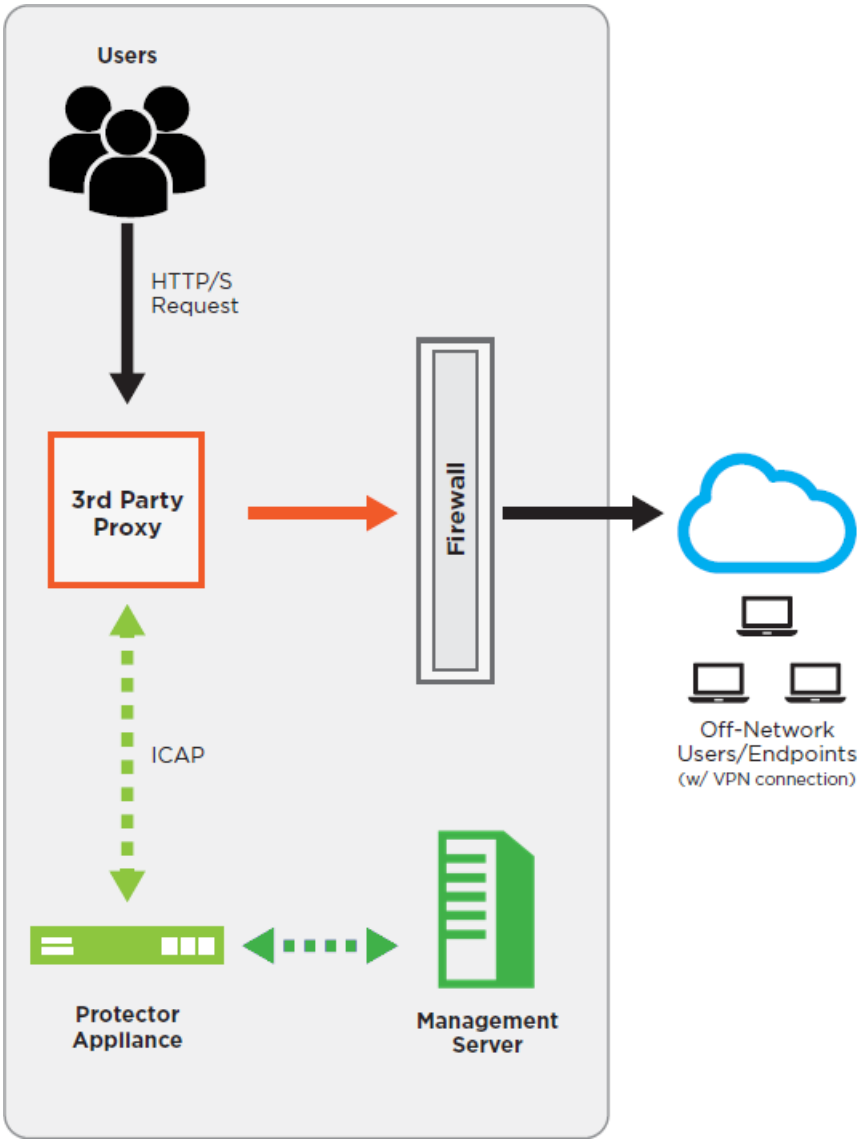
Forcepoint DLP Endpoint offers:

- Local discovery
- Removable media & CD/DVD security
- Application controls for copy/paste, print, print screen, file access
- Endpoint Web channels (HTTP/HTTPS)
- Endpoint LAN control
- Endpoint email
- Endpoint printing

| Small Organization | Large Enterprise |
|---|---|
| • 1 management server<br>• Endpoint clients | • 1 management server<br>• 1 Forcepoint DLP Server for every 15,000 endpoint clients |



## Forcepoint DLP protector with ICAP




## Forcepoint DLP Network with Web Content Gateway

The Forcepoint DLP Network includes the following forms of data protection:

- SMTP blocking
- HTTP blocking via built-in Content Gateway
- Cloud email inspection
- Policy enforcement for all channels
- Destination policy controls

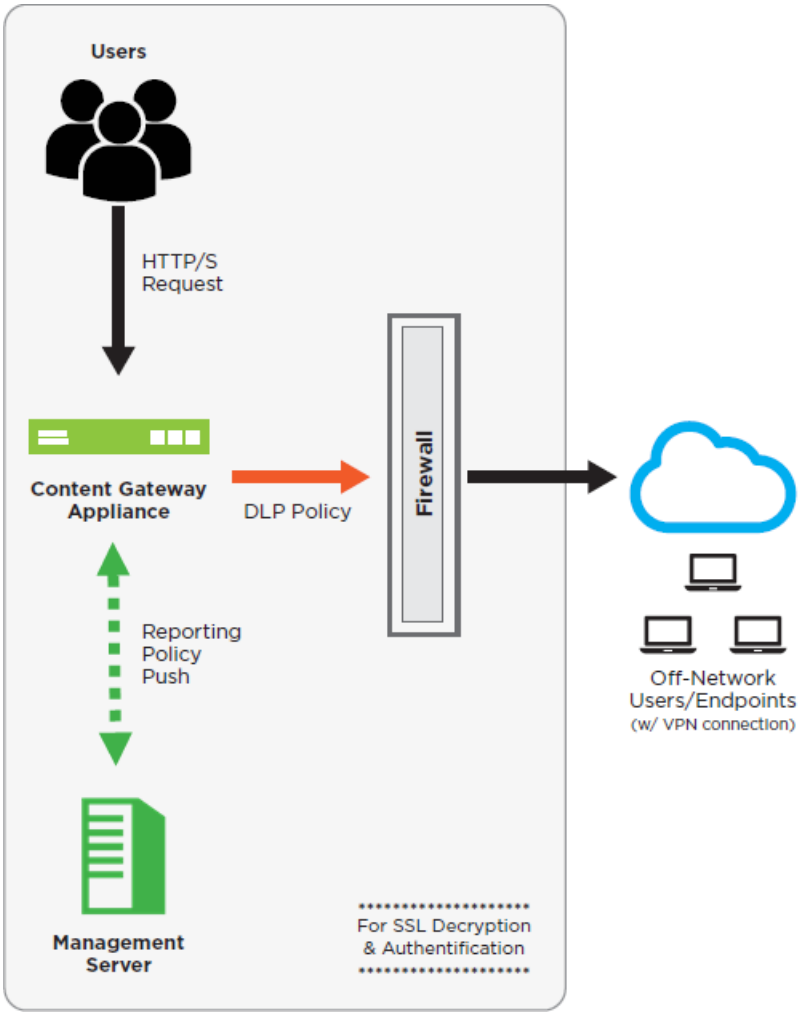
It also includes data monitoring for:

- Mail
- Web / FTP

Forcepoint DLP Network also includes support for:

- User-defined protocols
- Destination awareness

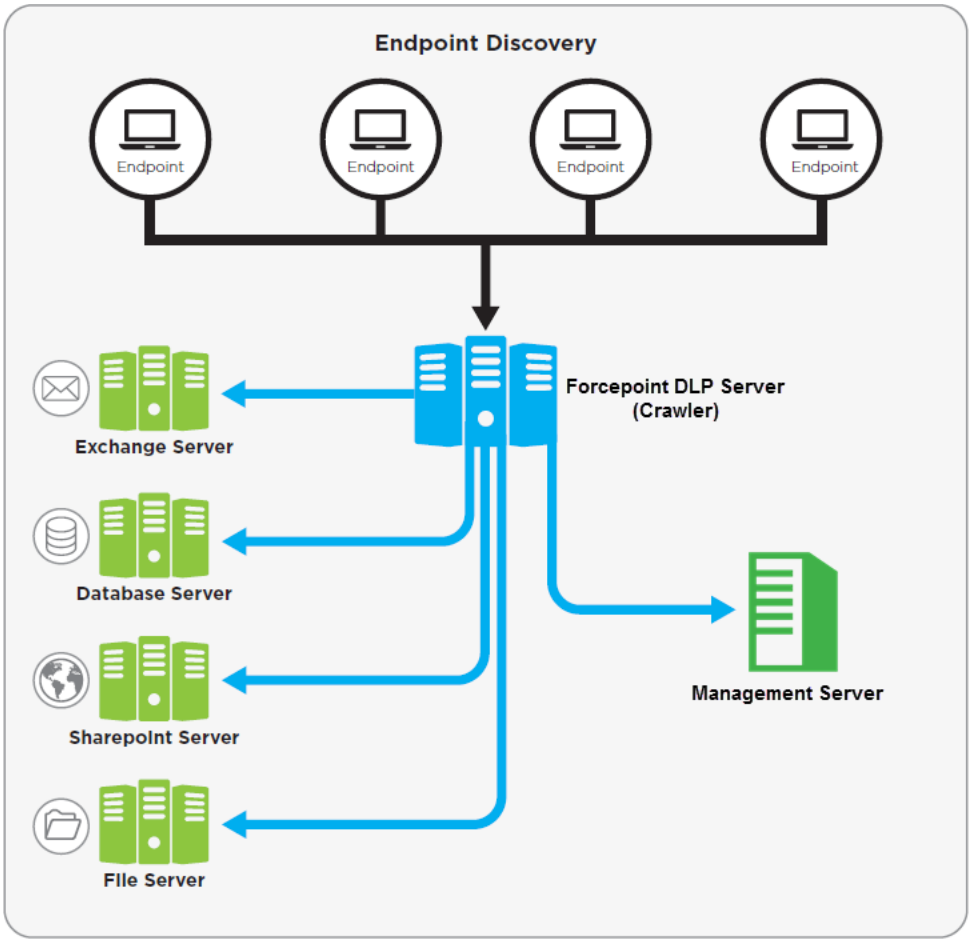
| Small Organization | Large Enterprise |
|---|---|
| • 1 management server<br>• 1 protector | • 1 management server<br>• Multiple Forcepoint DLP Servers<br>• Multiple protectors |



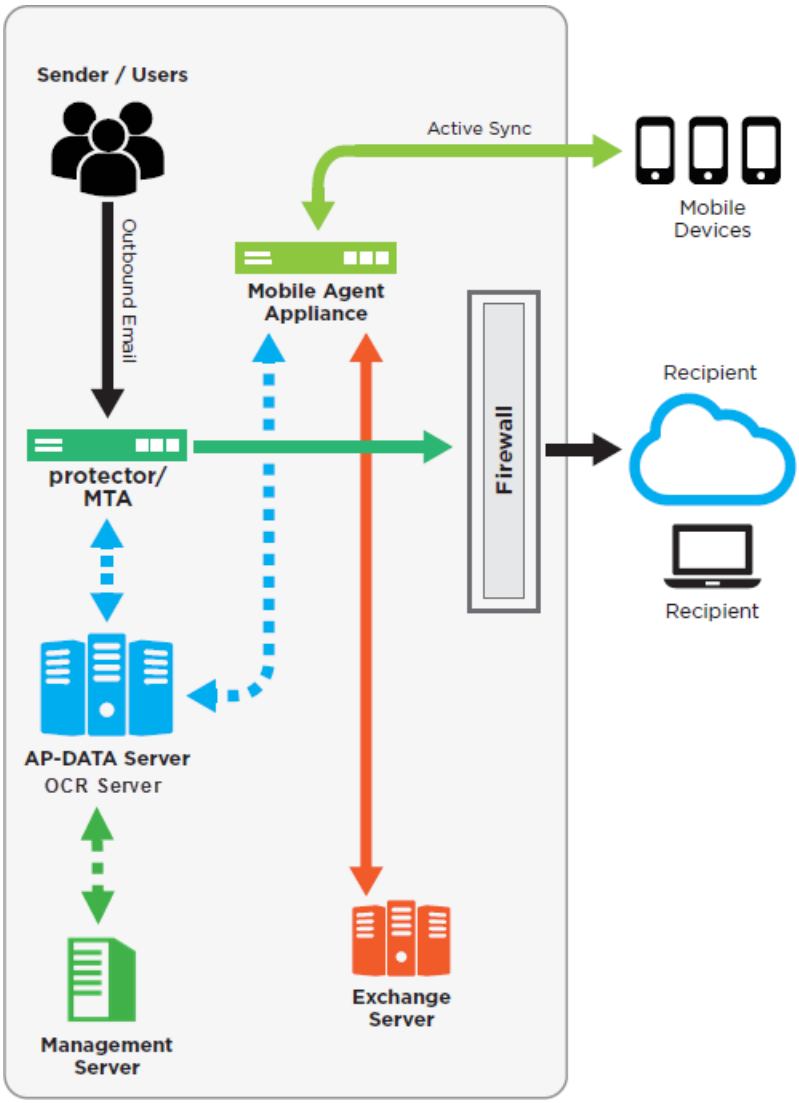
## Forcepoint Data Discover

Forcepoint Data Discover offers network and file discovery for data in file folders, SharePoint sites, databases, and Exchange servers. It also includes automated remediation for data at rest (for example, to remove the data from inappropriate network locations).

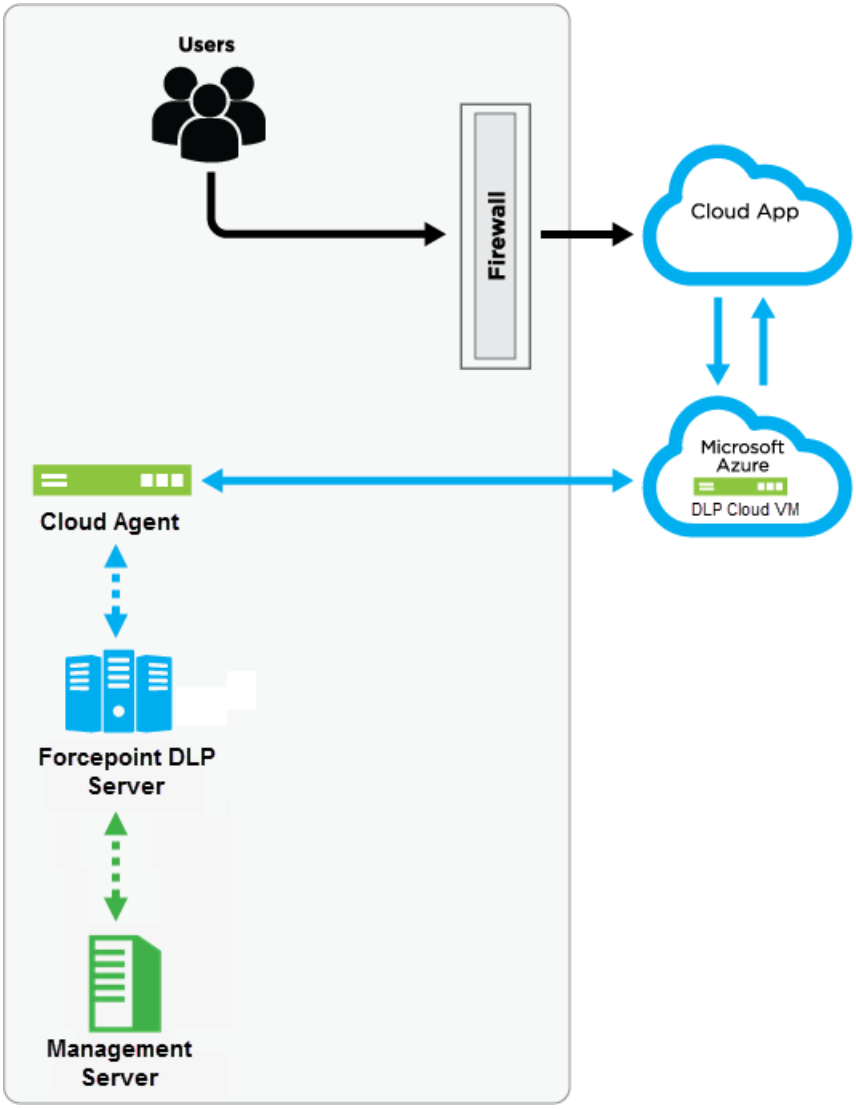
| Small organization | Large org/Enterprise |
|---|---|
| ● 1 management server<br>● 1 Forcepoint DLP Server | ● 1 management server<br>● Multiple Forcepoint DLP servers with discovery and fingerprinting crawlers.<br>Forcepoint Technical Support can help to assess the number of servers needed. |



## Forcepoint DLP with protector MTA and mobile agent



## Forcepoint DLP Cloud Applications



## Forcepoint DLP integrated with Forcepoint Web Security, Forcepoint Email Security, or both

Forcepoint DLP can integrate with Forcepoint Web Security to enable DLP over web channels (HTTP, HTTPS, FTP, and FTP-over-HTTP):

| Small Organization | Large Enterprise |
|---|---|
| ● 1 management server<br>● 1 V Series appliance<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases | ● 1 management server<br>● 1 Forcepoint DLP server<br>● Multiple V Series appliances<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases |

Forcepoint DLP can also integrate with Forcepoint Email Security to enable monitoring or blocking for DLP over SMTP:

| Small Organization | Large Enterprise |
|---|---|
| ● 1 management server<br>● 1 V Series appliance with Forcepoint Email Security<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases | ● 1 management server<br>● 1 Forcepoint DLP Server<br>● Multiple V Series appliances for Forcepoint Email Security<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases |

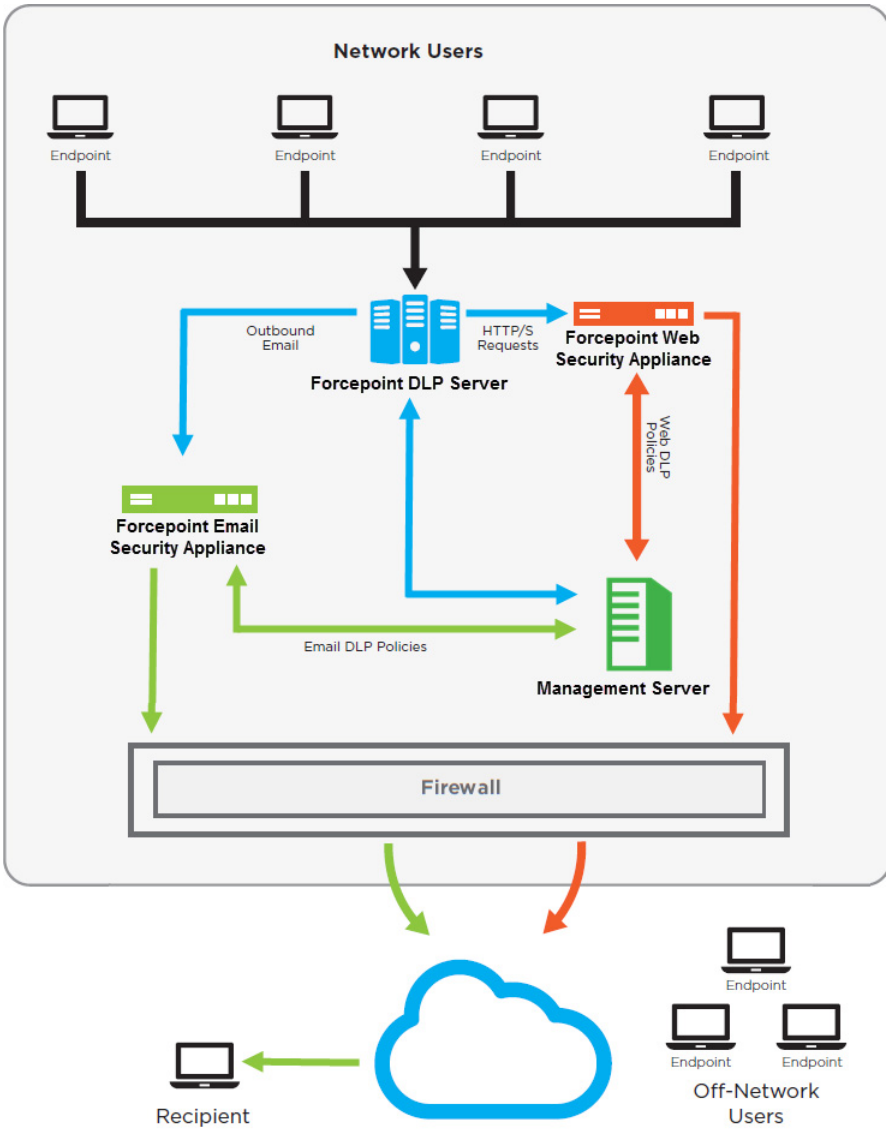
To combine monitoring and blocking DLP over SMTP with monitoring for web channels (including FTP) and IM, as well as user-defined protocols and destination awareness:

| Small Organization | Large Enterprise |
|---|---|
| ● 1 management server<br>● 1 Protector<br>● 1 V Series appliance with Forcepoint Email Security<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases | ● 1 management server<br>● 1 Forcepoint DLP Server<br>● 1 Protector<br>● Multiple V Series appliances with Forcepoint Email Security<br>● 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases |

To enable full DLP over both web and email channels, combine Forcepoint DLP with both Forcepoint Web Security and Forcepoint Email Security.

For example:

| Small Organization | Large Enterprise |
|---|---|
| • 1 management server<br>• 1 Protector<br>• 1 V Series appliance with Forcepoint Web Security<br>• 1 V Series appliance with Forcepoint Email Security<br>• 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases | • 1 management server<br>• 1 Forcepoint DLP Server<br>• 1 Protector<br>• Multiple V Series appliances to balance Forcepoint Web Security and Forcepoint Email Security load<br>• 1 Windows server for Microsoft SQL Server hosting Forcepoint reporting databases |



# Planning a phased approach

As part of the planning process, consider the tactics that can be employed in protecting data, configuring policies, managing incidents, and controlling access.

To assess how to protect data from compromise, Forcepoint recommends a multi-phased approach. One possible approach is outlined here.

## Phase 1: Monitoring

Start by monitoring data (auditing without blocking):

1. Enable regulatory compliance, regional, and industry-related predefined policies in order to:
   - Deploy solid, first stage DLP.
   - Get a good picture of what information is being sent out, by whom, to where, and via which methods.
2. If the organization has unique data identification needs that are not covered by a predefined policy, request custom policies from Forcepoint.
   - Data types requiring a custom policy might be items like coupons or catalog numbers.
   - To request a policy, contact Forcepoint Technical Support. They will escalate the request and engage a research team. The usual turnaround is approximately 3 weeks. (The research team can typically provide an estimated time to completion within 3 days of reviewing the request).
3. Fingerprint data (can be also part of Phase 2):
   - Data fingerprinting allows accurate and efficient data identification
   - Database fingerprinting (PreciseID database technology) allows accurate and efficient detection of fingerprinted records coming from database tables, database views, and CSV files.
   - Content policies can be flexibly defined for data sources, with detection rules based on combinations of columns and thresholds based on 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 belonging to the organization’s customers.
   - Files, directory, and SharePoint fingerprinting (PreciseID files technology) allow identification of unstructured data (free text).
     - Data can be identified in different formats (e.g., after PDF conversion), different contexts (excerpt of fingerprinted confidential document), and so on.
     - Advanced and efficient algorithms allow detecting fingerprints even on endpoints that have limited resources.

## Phase 2: Monitoring with notifications

In the second stage, enable email notifications to relevant members of the organization when a policy breach is discovered. The options are:

- Global security administrator
- 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

In this phase, provide tuning to keep the incident volume manageable, and to ensure that only relevant incidents are being reported.

This phase can operate in parallel to Phases 1 and 2.

- Disable policies that are not showing value.
- Make sure the channels selected for policy application are relevant.
- 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.

Also use Phase 3 to make sure that proper incident managers are assigned for various types of incidents. Create policy category groups in the Data Security module of the Security Manager and assign them to relevant incident managers.

## Phase 4: Enforcing

Begin this phase after all policies have been successfully tuned and business owners, data owners, and incident managers are trained and ready to handle the incidents.

- Start with the one channel (for example, SMTP), then gradually move to add enforcement for other channels (like HTTP).
- Continue monitoring incidents to identify whether certain policies should be moved back to auditing only. For example, if all quarantined email is released, it might be better to simply monitor the transactions.
- It may be desirable to integrate with encryption gateways as part of SMTP enforcement. Forcepoint DLP can automatically route certain email transactions to be encrypted based on email content and/or policy definitions (actions).

## Phase 5: Discovery

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. This ensures that administrators know where sensitive information is located, and who is allowed to access it.

## Phase 6: Endpoint deployments

This phase can also be instituted earlier in the security process.

Deploy Forcepoint DLP Endpoint to control data in use (removable media, clipboard operations, file access):

- The endpoint software can control data in use, even if users are disconnected from network.
- The endpoint software can optionally be installed in stealth (invisible) mode.

Local discovery investigates the drives on a local machine, like a laptop, which can be disconnected from the network. This can help to uncover sensitive files that network discovery doesn’t reach.

# 3 Integrating with Existing Infrastructure

Forcepoint DLP is an integral piece of the network architecture, and can be combined with existing systems to ensure seamless web and email protection. This section describes:


- *Working with existing email infrastructure*, page 29
- *Working with web proxies*, page 31


## Working with existing email infrastructure

Configure Forcepoint DLP to work with an existing email infrastructure to block and quarantine email that contravenes DLP policies.

This can be done by connecting Forcepoint Email Security or the Forcepoint DLP 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.

The protector has 2 SMTP modes:

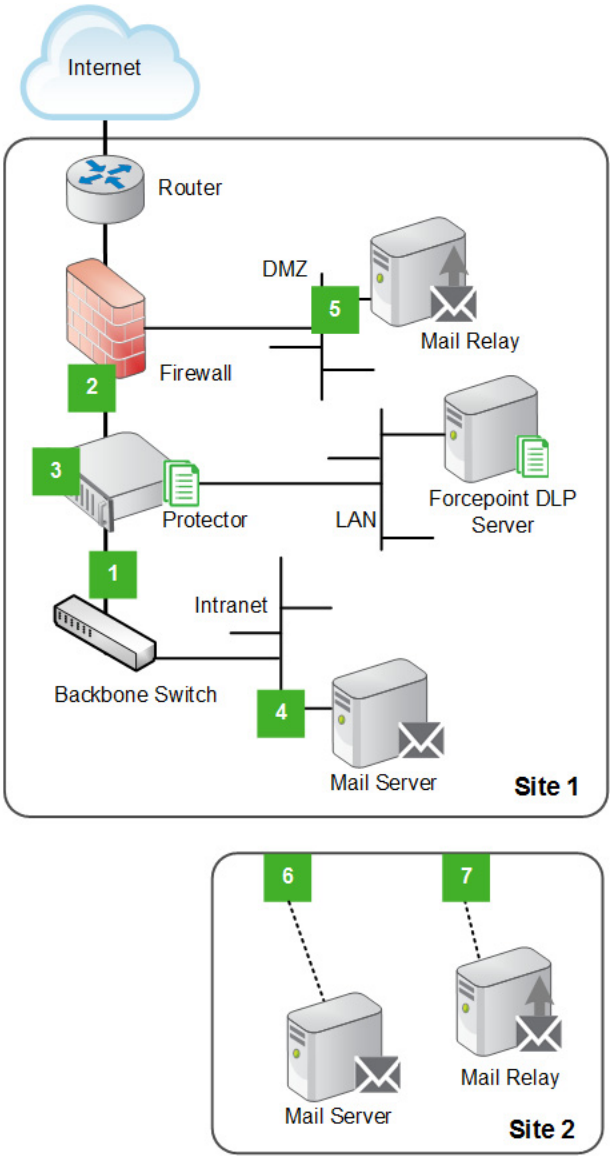
- Monitoring mode (sometimes referred to as passive mode)

  In this mode, the protector monitors and analyzes SMTP traffic, but does not block transactions. Limit the networks with permission to send email via the protector's SMTP service to prevent the protector from being used as a mail relay.
- Explicit Mail Transfer Agent (MTA) mode

  In this mode, the protector acts as an MTA for SMTP traffic and operates in protect mode. Protect mode allows transactions the breach policy to be blocked or quarantined.

## Pre-installation checklist

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




Before installation:

- ❑ Verify that the required hardware is available. Check the Deployment & Installation Center 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 valid IP addresses for the Forcepoint DLP server and the protector management port

- 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.

# Working with web proxies

The recommend web proxy for use with Forcepoint DLP is Content Gateway. Content Gateway includes its own Forcepoint DLP policy engine and streamlines communication with the management server.

Content Gateway is included with Forcepoint DLP Network and Forcepoint Web Security.

Forcepoint DLP also supports the following third-party Web proxies:

- Blue Coat (*Blue Coat web proxy*, page 31)
- Squid open source (*Squid open source Web proxy*, page 34)

These proxies integrate with Forcepoint DLP 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.

This section describes the recommended integration solution. Other configurations can be implemented, but should be tested prior to deployment.

### Limitations

- The solution does not support the FTP GET method for request modification.
- The solution does not support the HTTP GET method for request modification.
- The solution can only scan files 12 MB or smaller. The system can generate an error if a file exceeds that size.

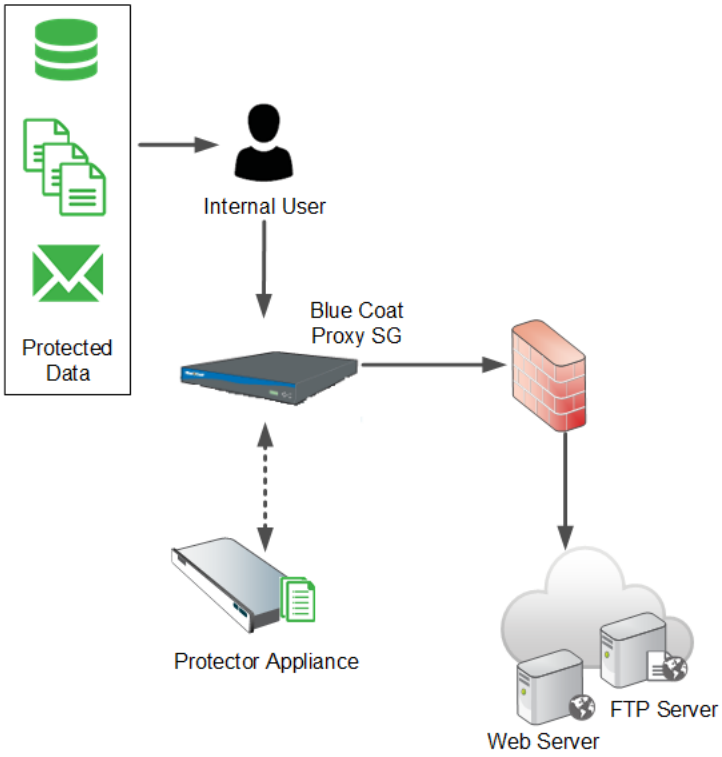
- The described deployment does not include caching (Blue Coat SG does not cache PUTs and POSTs). Nonetheless, exercise care if a response mode configuration is used.

## Deployment

This deployment recommendation describes a forward proxy: a Blue Coat SG appliance connected to a Forcepoint 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 Forcepoint ICAP server.

The Forcepoint protector receives all traffic directed to it from the Blue Coat appliance for scanning,

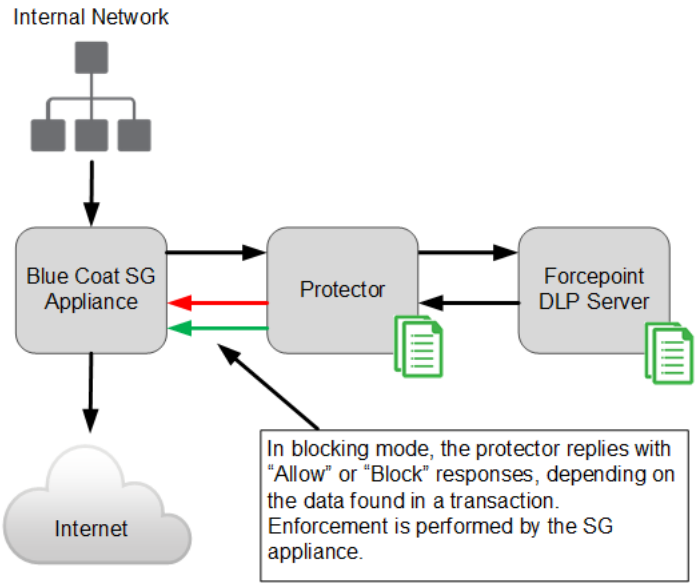
The following diagram outlines the recommended deployment:



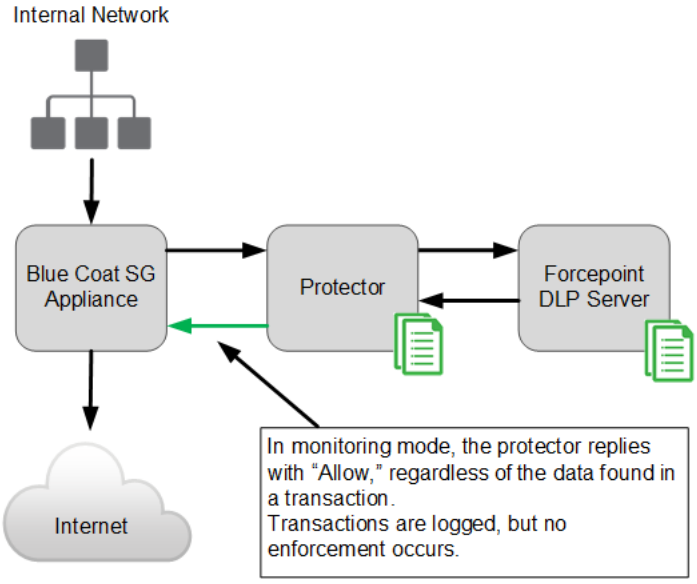

The deployment solution can be used in either monitoring or enforcement mode.

- In enforcement mode, the Blue Coat SG appliance requires Forcepoint DLP to authorize each transaction before allowing files to be posted or uploaded to their

intended destination. This is the recommended mode, because it provides the most security.




- In monitoring mode, the transactions that are redirected by the Blue Coat SG appliance are analyzed by Forcepoint DLP, which can then generate incidents for confidential information and send notifications to administrators and information owners. In this mode, the Forcepoint DLP ICAP server universally responds to all redirected transactions with Allow.

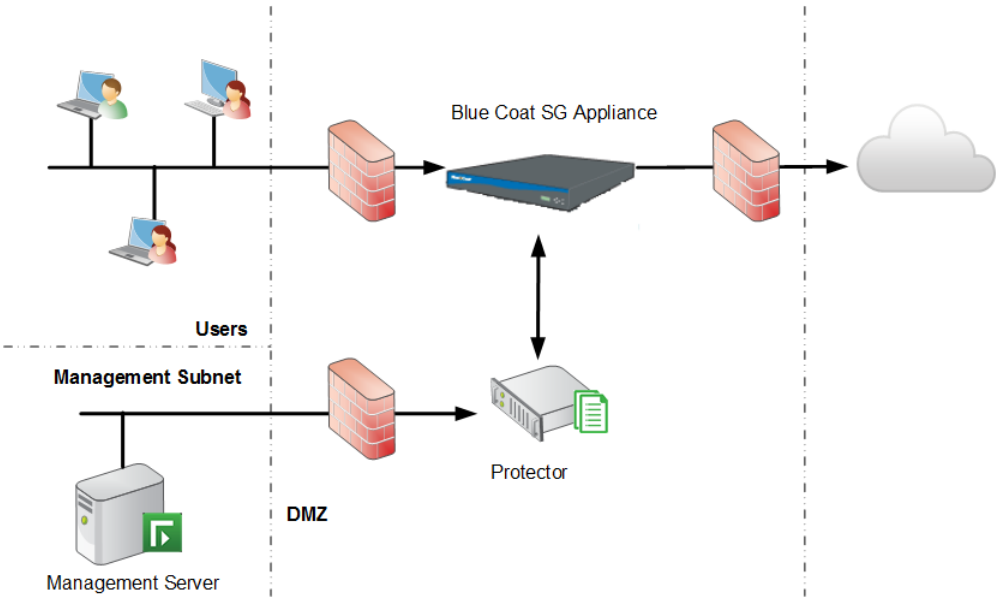


### Network integration

The solution includes of 3 components:

- Forcepoint DLP protector
- Forcepoint management server
- Blue Coat SG appliance

The ICAP integration component resides on the protector, and acts as a relay between the Blue Coat SG appliances and the management server as shown below:




### Configuring the Blue Coat integration

- Refer to the Forcepoint DLP Installation Guide for instructions on installing Forcepoint DLP.
- Refer to the Blue Coat documentation for Blue Coat appliance installation instructions.
- After installation, see the Getting Started Guide for configuration instructions.

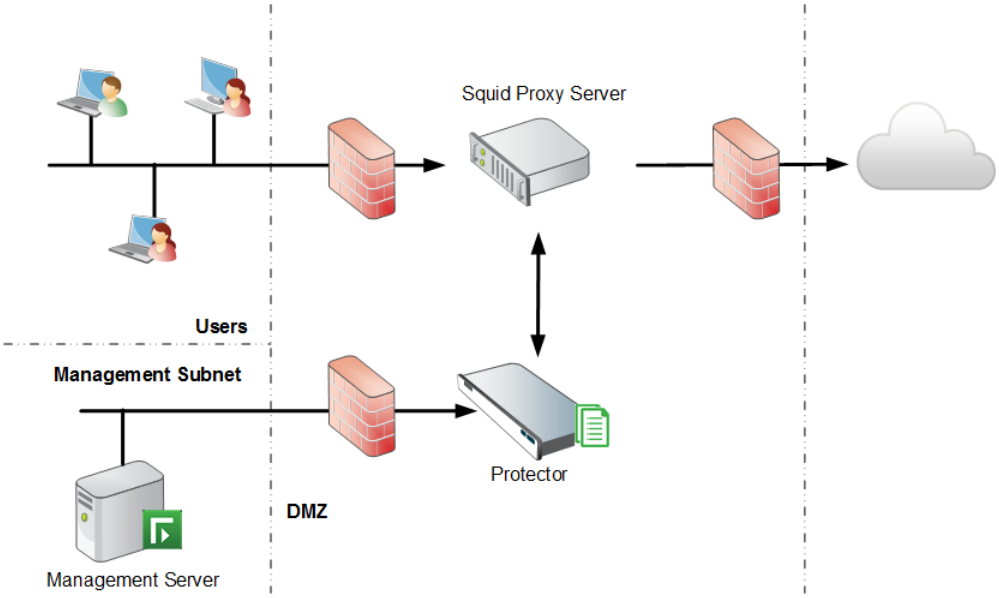
## Squid open source Web proxy

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

### Deployment

The recommended deployment uses a forward proxy: a Squid web proxy server connected to a Forcepoint 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 Forcepoint ICAP server.

The Forcepoint DLP protector receives all traffic directed to it from the Squid server for scanning, and, in enforcement mode, returns a response indicating whether to block or allow the transaction. In monitoring mode, the response is always allow.




## System setup

Refer to the Forcepoint DLP Installation Guide for instructions on installing Forcepoint DLP, 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.

# 4 Scaling Forcepoint DLP

As the organization's network and network security needs grow, Forcepoint DLP can grow with it. The 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 the system load demands system expansion.
- Configuring for single and multi-site deployments.
- Dealing with the growth of the various information repositories.

See:


- *When does the system need to grow?*, page 37
- *Adding modules to the deployment*, page 40


## When does the system need to grow?

There are numerous triggers that might prompt an organization to expand the Forcepoint DLP system. Among them:

- **Performance issues**

  Performance issues may vary in visibility and impact.

  - Slow discovery or fingerprinting scans, for example, could indicate an overworked crawler. This might be resolved by adding a crawler or Forcepoint DLP server.
  - If users are experiencing slow web or email transactions, an additional policy engine might help.

  Even if performance issues are not obvious, system resources may not be fully optimized.

  To see how the Forcepoint DLP system is performing, open the Security Manager and go to the **Main > Status > System Health** page. Expand each module to see load statistics, the number of transactions, latency information, and more.

  Before adding modules, try balancing the load between existing Forcepoint DLP servers (policy engines). To do this, go to the **Settings > Deployment > System**

**Modules** page, then click **Load Balancing**. Select a service, then indicate which policy engine to assign to that service.

> **Note**
> Forcepoint recommends that you do not distribute the load to the management server.

- **The number of users grows**

  A typical small organization (1-500 users) might only need a management server and a protector to monitor traffic. A larger organization (500-2,500 users) might have a management server, a supplemental Forcepoint DLP server, and a protector, with load balancing between the protector and supplemental server. (The management server cannot be used for load balancing.)

  As the number of users grows, so does the need for additional Forcepoint DLP servers.

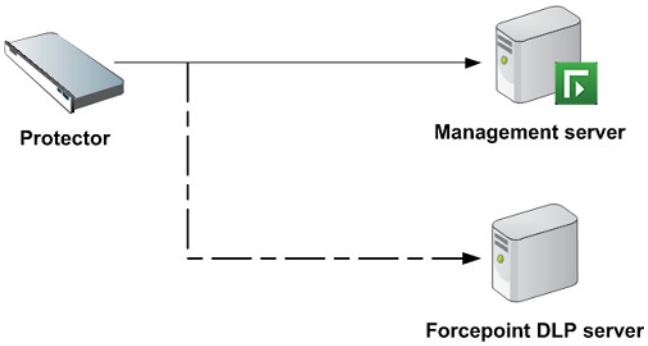
- **The number of transactions grows**

  This is the most important requirement for determining the number of Forcepoint DLP components needed. Typically the number of transactions grows as the number of users grows.

  In *monitoring* mode, Forcepoint 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.)

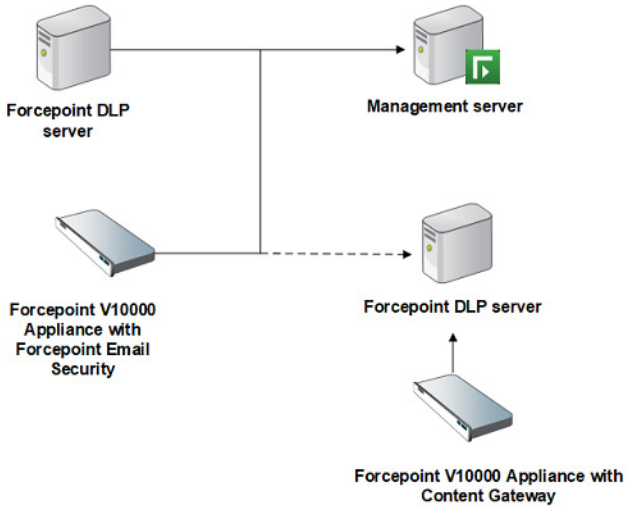
  For more users, add an extra Forcepoint DLP server and balance the load between the protector and the extra server.




  In *blocking* mode, Forcepoint recommends 1 management server, 1 V Series appliance with Forcepoint Email Security software, and 1 V Series appliance with 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 Forcepoint DLP server.




Note that the transaction volume can grow even if the user base does not. If a significant increase in traffic is anticipated, the system may benefit from adding one or more Forcepoint DLP servers.

- **The number of endpoints grows**

  With Forcepoint DLP Endpoint, when large numbers of endpoint clients are being deployed, additional endpoint servers may be required. A general rule of thumb is to add 1 Forcepoint DLP server for every 15,000 endpoint clients.

- **Moving the deployment from monitor to protect**

  Enforcement requires more resources than monitoring, particularly because load-balancing must be enforced between policy engines and other Forcepoint DLP modules.

  When a deployment is moving from monitor to protect, it may benefit from an additional Forcepoint DLP server. Note that the Forcepoint DLP Web Content Gateway or Forcepoint Web Security is required to enforce the HTTP channel; the protector or Forcepoint Email Security is required to enforce the SMTP channel.

- **Moving from a single-site to multi-site configuration**

  Forcepoint DLP supports multi-site, distributed deployments. An organization can have a local policy engine on the protector, for example, and distributed (primary and secondary) fingerprint repositories. There can be a management server in one location and one or more supplemental Forcepoint DLP servers in other locations.

  Administrators have the option to use the crawlers on the Forcepoint DLP servers alone to do fingerprint and discovery scans, or to install the crawler agent on additional servers to improve performance.

  Many scalable options are available. See *Most common deployments*, page 16, for typical component distributions.

  Note that organizations with multiple geographical locations need a protector for each site. A deployment with low latency between two geographically distributed sites might need two protectors and two supplemental Forcepoint DLP servers.

- **Adding branch offices**

  Each branch office requires a protector. When a branch office is added or acquired, add a protector.

- **Adding HTTP, SMTP and FTP egress points**

  If egress points are being added to the network structure, a protector is needed to monitor each egress point. Each one also needs a Web Content Gateway instance if HTTP protection is required.

- **The network grows (in GB)**

  In deployments that use network discovery, the network size greatly affects sizing requirements, as does the frequency of full versus differential scans. Growing networks may require an additional crawler or Forcepoint DLP server.

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

  The Forcepoint DLP software has default settings for the disk space requirements of its fingerprint and forensic repositories, but these values can be modified. Organizations with larger transaction volumes and numbers of users can adjust values significantly upward.

  At some point, however, it may be necessary to add another server to accommodate these repositories and increase available 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 the deployment

If network and security requirements dictate the need to add new agents or other modules, most can be added using the Forcepoint Security Installer (the Windows installer).

During installation, the administrator is prompted to provide the FQDN of the management server and the credentials for a Forcepoint Security Manager administrator with Forcepoint DLP system modules permissions. This allows the new module to register automatically with the management server.

After installation, to accept the default configuration, an administrator must click **Deploy** in the Security Manager to complete the registration process. To customize the configuration before deploying, go to the Settings > Deployment > System Modules page and select the module to edit.

Only a Security Manager administrator with system modules permissions can install or configure new network elements.

For information on adding and configuring modules, see “Adding modules” in the Forcepoint DLP Administrator Help.

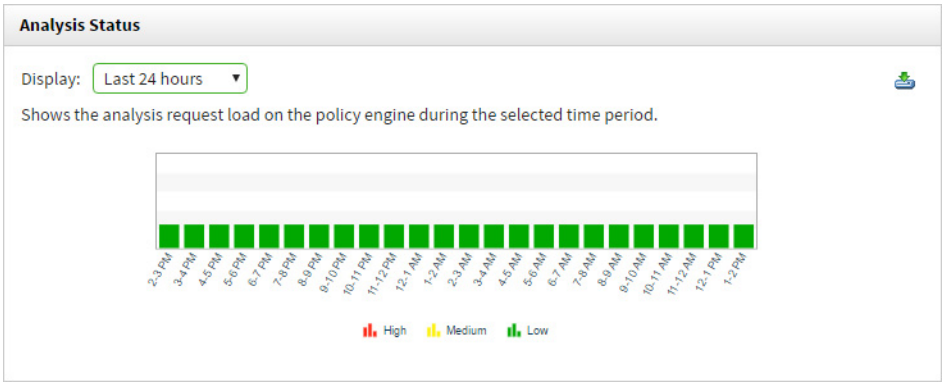
# Value of additional policy engines

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

## Assessing the need for additional policy engines

To check the number of transactions analyzed by a policy engine instance:

1. Log on to the Security Manager.
2. Go to the Main > Status > System Health page.
3. Select the policy engine instance, then review its “Analysis status” chart.




Red on the chart indicates a heavy load on the policy engine during the corresponding period.

In monitoring mode, a few red bars may not be an issue. The system will process the incidents during a less busy period.

In blocking mode, even one hour of red is undesirable. If a red bar appears, perform load balancing, and, if that does not resolve the issue, add a new Forcepoint DLP server.

## Optimizing policy engine performance

- Try to avoid analysis of incoming traffic. If incoming traffic analysis is a must, try to limit it to specific domains.
- Never scan all networks; establish limits.
- Check the top policies to see if there are:
  - Any false positives
  - Unwanted or unneeded policies
- If possible, make sure no spam SMTP mail is undergoing analysis.