

DATA LOSS PREVENTION



By

Hasnat Ahmed

Nabeel Abbas

Hamzah Javed

Submitted to the Faculty of Computer Software Engineering
Department, National University of Sciences and Technology, Islamabad,
in partial fulfillment for the requirements of a B.E. Degree in
Computer Software Engineering

June 2013

CERTIFICATE

Certified that the contents and form of project report entitled “**Data Loss Prevention**” submitted by 1) Hasnat Ahmed, 2) Hamzah Javed, and 3) Nabeel Abbas under the supervision of Lecturer Rabia Khan for partial fulfillment of Degree of Computer Software Engineering, have been found satisfactory.

Supervisor: _____
Lec. Rabia Khan

ABSTRACT

Leakage of your data could be embarrassing or worse, cost you industrial edge or loss of accounts. Allowing your organization to act in non-compliance with privacy acts and other laws could be worse than embarrassing; the integrity of your organization may be at stake.

Intellectual property is the term widely used in every professional aspect of life. Information plays a vital role in this topic the information must be secured in proper place that is only the person who is intended to see that information is able to see it. Forrest of the staff, information is given upon special requests only.

Today, all the leading antivirus companies like McAfee and Norton have developed the system to prevent the confidential and sensitive information from falling into the wrong hands. The system is mainly known as Data Loss Prevention System.

Data Loss Prevention is a comprehensive, content-aware technology that discovers, monitors, and protects confidential data wherever it is stored or used across network, storage and endpoint systems.

The thesis presents our project “Data Loss Prevention” (DLP), which is aimed at developing a system to secure the sensitive information from leaving the corporate network by any means possible. Main objective of DLP is to protect the critical information from any insider threats.

DECLARATION

No portion of the work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere.

COPYRIGHT NOTICE

Copyright in text of this thesis rests with the student authors. Copies (by any process) either in full or of extracts may be made in accordance with instructions given by the author and lodged in the Library of Military College of Signals, NUST. Details may be obtained from the Librarian. This page must be part of any such copies made. Further copies (by any process) or copies made in accordance with such instructions may not be made without permission (in writing) of the authors.

The ownership of any intellectual property rights which may be described in this thesis be vested in Military College of Signals, subject to prior agreement to the contrary, and may not be made available for use by third parties without the written permission of the Military College of Signals, which will prescribe the terms and conditions of any such agreement.

Further information on the conditions under which disclosures and exploitation may take place is available from the Library of Military College of Signals, NUST.

DEDICATION

In the Name of Allah, The Most Beneficent, The Most Merciful

This project thesis is devoted to our

Parents
&
Teachers

For their unwavering confidence in us, the continuous support and
Love without which we would not have been able to succeed.

ACKNOWLEDGEMENTS

**“All praises be to Allah Almighty, The Most Exalted and The Most Dignified,
Who guides us from the depths of darkness into the light and help us in
difficult times”**

We are grateful and thankful to Allah Almighty for His unremitting blessings, bestowed upon us throughout our project. Secondly, we are thankful to our families for their unending support that they have shown in good and hard times. Their perseverance and obstinate support helped us achieve much in the project.

We are extremely grateful to our project supervisor Lec. Rabia Khan, who led us from the start, encouraged us in the times of difficulties, and provided us with utmost technical knowledge about the project. She has been very supporting throughout our project and has played a pivotal role in making us successful. She has been there for us whenever we needed her. We again thank her for support and cooperation, without which this project would not have been possible.

Last but not the least we are also indebted to our classmates and friends, who provided every possible support that they could, and helped us achieve technical expertise and move further through difficult areas of the project. Their selfless support contributed much to our project in the form of discussions, ideas exchange, and as a source of encouragement.

TABLE OF CONTENTS

Chapter 1: Introduction	1
1.1 Introduction	1
1.2 Background	1
1.3 Problems Addressed	2
1.4 Goals and Objectives	3
1.5 Deliverables	6
Chapter 2: Literature Review	7
2.1 Literature Review	7
Chapter 3: System Requirements	11
3.1 Hardware Interfaces.....	11
3.2 Software Interfaces.....	11
3.2.1 WireShark.....	11
3.2.2 Dagsnap.....	11
3.3 Communication Interfaces	11
3.4 Configuring a User Account	12
3.5 Advanced Authentication Settings	14
3.6 Precision and Accuracy.....	15
3.7 Reliability and Availability	15
3.8 Reliability and Availability	15

3.9 Access	15
3.10 Integrity	16
3.11 Privacy	16
3.12 Usage Easiness	16
3.13 Error Rates	16
3.14 Trust	16
3.15 Learning	17
3.16 Maintenance	17
3.17 Adaptability Requirements.....	17
Chapter 4: Software Design Specification	18
4.1 Abstract System Overview	18
4.2 Use Case Diagrams	19
4.3 Sequence Diagrams.....	35
4.3 Activity Diagrams	40
Chapter 5: System Implementation	43
5.1 Architecture Diagram	43
5.1.1 Netwok	43
5.1.2 Storage.....	43

43	5.1.3 Endpoint	43
	5.2 Design Pattern	44
	5.2.1 Enforce Server.....	45
45	5.2.2 Detection Server	45
	Chapter 6: Testing and Results Analysis	46
46	6.1 Endpoint DLP Tests	46
48	6.2 Storage Prevent Tests	48
51	6.3 Network Prevent Tests	51
	Chapter 7: Conclusion and Future Work	53
	7.1 Conclusion	53
	7.2 Future Enhancements	53

APPENDIX A: User Manual	
54	
BIBLIOGRAPHY	63

List of Figures

Figure-1.1	Threats Statistics	2
Figure-1.2	DLP Architecture	4
Figure-2.1	DLP Modules.....	9
Figure-3.1	Hardware Recommendations	11
Figure-3.2	Software Recommendations	21
Figure-4.1	Add Role Use Case	19
Figure-4.2	Exact Match Use Case	23
Figure-4.3	Login Sequence	28
Figure-4.9	Maps View / Update Sequence	29
Figure-4.13	End Point Sequence.....	31
Figure-4.14	Network Prevent Activity.....	31
Picture-4.1	Different Screens of System	32
Picture-4.2	DLP Server Application	33
Picture-4.3	DLP Client Application	33
Picture-4.4	Synchronization	34
Picture-4.5	Route Marking	34
Picture-4.6	Contact Report	35
Picture-4.7	Incident Report.....	35
Figure-5.1	System Overview	36

Chapter 1: Introduction

1.1. Introduction

Data Loss Prevention (DLP) is a set of information security tools that are intended to stop users from sending sensitive or critical information outside the corporate network. Idea of DLP originated due to significant insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. A user who accidentally or maliciously attempts to disclose confidential information that's been tagged will be denied. DLP might prevent a sensitive financial spreadsheet from being emailed by one employee to another within the same corporation.

Endpoint: Monitor and control activities

Network: Filter data streams

Storage: Protect data at rest

1.2. Background

The idea of DLP originated due to significant inside threats and more rigorous state privacy laws, many of which have stringent data protection or access components. A user who accidentally or maliciously attempts to disclose confidential information that's been tagged will be denied and the related authorities would also be pinged. DLP might even prevent a sensitive financial spreadsheet from being emailed from one employee to another within same corporation. The figure demonstrates the need for such a system.

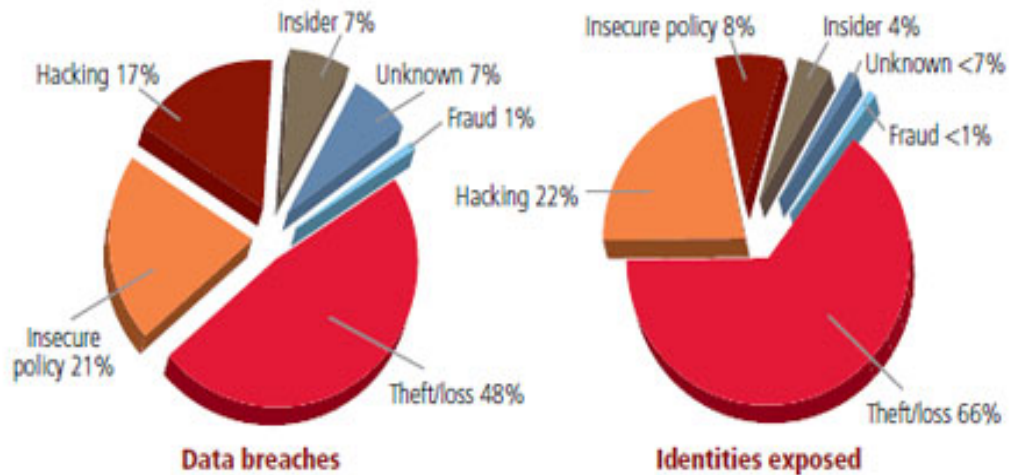


Fig. 1.1

1.3. Problems Addressed

Over the last few years, companies in every industry sector around the globe have seen their sensitive internal data lost, stolen or leaked to the outside world. A wide range of high-profile data loss incidents have cost organizations millions of dollars in direct and indirect costs and have resulted in tremendous damage to brands and reputations. Many different types of incidents have occurred, including the sale of customer account details to external parties and the loss of many laptops, USB, backup tapes and mobile devices, to name just a few. The vast majority of these incidents resulted from the actions of internal users and trusted third parties, and most have been unintentional.

As data is likely one of your organization’s most valuable assets, protecting it and keeping it out of the public domain is of paramount importance

According to a 2010 Ponemon Institute study, the average total cost per data breach has risen to \$7.2 million, or \$214 per record lost.

Employees do not clearly understand or feel accountable for the protection of sensitive data. Employees feel that there is no risk involved in breaking the rules (i.e., “no one is watching so I will not be caught”).

As above we assumed that organization will be without DLP solution there is no control so some issues may arise:

- a Insider threats anyone can copy and send any data
- b Accidental or malicious attempt to disclose the confidential information
- c Loss of reputation especially for organizations which involves user account and user information
- d Loss of trade secrets and marketing plans.
- e No check on emails because any one can email the confidential information on them
- f No check on printing devices what data one can print and what data cannot be printed
- g No check on use of portable devices (PDAs, telephones, USB flash drives, CD/DVD and other such devices.

1.4. Goals and Objectives

a. Objectives:

The technology components are designed to address the questions as follows:

- (1) Discover where confidential data is stored.
- (2) Monitor how data is being used.
- (3) And proactively Protect data to prevent its loss.

b. Goal

Our end goal is that to implement DLP solution to control and manage data security requirements and legal constraints regarding confidentiality of data in an organization. To control those extrusion prevention rules from a centralized location.

Define and deploy universal policies across the enterprise using a centralized policy management mechanism.

Ensuring control over the distribution of confidential information and preventing its transfer outside your organization. This is accomplished through control over all accessible data transmission channels, namely:

- Internet messengers (Skype, MSN and other such services);
- Corporate and personal e-mail (Mail, Gmail and other such services);
- Wireless systems (Wi-Fi, Bluetooth, 3G and other such services);
- Printing devices (printers);
- The use of portable devices (PDAs, telephones, USB flash drives, CD/DVD and other such devices.);
- FTP port connections.

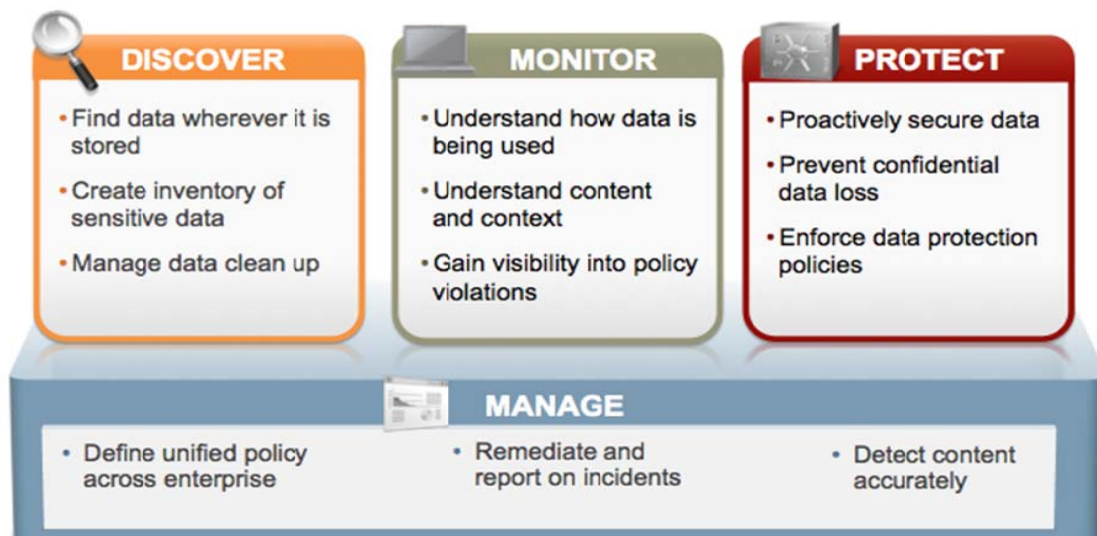


Fig 1.2

b. Scope of the Project:

- Research on Different DLP Solution in Market.
- Identify the best Solution available.
- Study storage and use of confidential data in target organization.
- Design a solution based on organization's needs.
- Design Policies to prevent data leakage from organization.
- Implement the Central policy management module.
- Setup VMware ESX infrastructure to implement DLP Solution.
- Design a virtual environment to demonstrate our solution.
- Demonstrate Solution.

1.5. Deliverables

Phase wise deliverables during the project development are as under:

- a. **Phase I.**
 - (1) Project Proposal & Synopsis.
 - (2) Requirements Analysis Report.
 - (3) Software Requirement Specifications
 - (4) First Progress Report.

- b. **Phase II.**
 - (1) 2nd Progress Report.
 - (2) Detailed Design Document.

- c. **Phase III.**
 - (1) Development and Implementation scheme.
 - (2) Development of modules separately.
 - (3) Software prototype produced.
 - (4) Software installation & configurations with customizations.

- d. **Phase IV.**
 - (1) Unit Testing.
 - (2) System Testing.
 - (3) Integration Testing.

- e. **Phase V.**
 - (1) Project Final Report.
 - (2) User Manual.
 - (3) Interface and functionality explanation.

Chapter 2: Literature Review

2.1. Literature Review

Today, just about anybody can share, access, and disseminate information in unlimited volume. Organizations have come to depend on it—in fact, it is enormously empowering. At the same time, the workforce has become increasingly mobile and the ubiquity of high-speed Internet access, smart mobile devices, and portable storage means that “the office” can be anywhere. As a consequence, it has become more difficult than ever for organizations to prevent the loss of sensitive data. Yesterday’s security approaches were aimed at securing the network. It’s time to shift the focus to securing the data itself

Data Loss Prevention answers three fundamental questions:

- a. Where is your confidential data?
- b. How is it being used?
- c. How do you prevent data loss?

As the volume of data continues to grow within an organization, data security teams may have little or no visibility into where confidential data is stored or who has access to that data. Symantec Data Loss Prevention discovers confidential data wherever it is stored throughout an organization. With this solution, companies can address key challenges around the Payment Card Industry (PCI) standard, data inventory, and data classification in order to demonstrate regulatory compliance, reduce risk, and safeguard their brand and reputation.

As organizations rely on high-speed networks and mobile computing to more easily share and access information, data security teams may have little or no visibility into what confidential data is leaving the organization and how employees are using it on and off the corporate network. With Symantec Data Loss Prevention, organizations can monitor how confidential data is being used at the endpoint and where it is being sent over the network. Symantec helps ensure that employees can work productively from the office or at home, and that organizations are aligned with corporate data security policies.

It has become more difficult than ever for organizations to prevent the loss of sensitive data. Yesterday's security approaches were aimed at securing the network. Today's approach is to focus on securing the data itself. With Data Loss Prevention, organizations gain visibility into policy violations to proactively secure data with automatic quarantine, relocation, and support for policy-based encryption. Symantec Data Loss Prevention enables active blocking at both the network and endpoint to prevent confidential data from leaving the organization inappropriately. Symantec helps ensure the highest level of risk reduction to automatically enforce compliance with data security policies and enable organizations to change employee behavior.

With Data Loss Prevention, you can:

- 2.1.1 Use automated sender and on screen notifications to educate employees on data security policies
- 2.1.2 Protect sensitive data from being stored in unauthorized places
- 2.1.3 Prevent internal product pricing lists from being posted on a partner Web portal
- 2.1.4 Prevent call center representatives from sending credit card numbers via email in violation of PCI standards
- 2.1.5 Prevent an employee from copying source code to a USB device.
- 2.1.6 Prevent employees from burning a DVD with hundreds of confidential CAD drawings

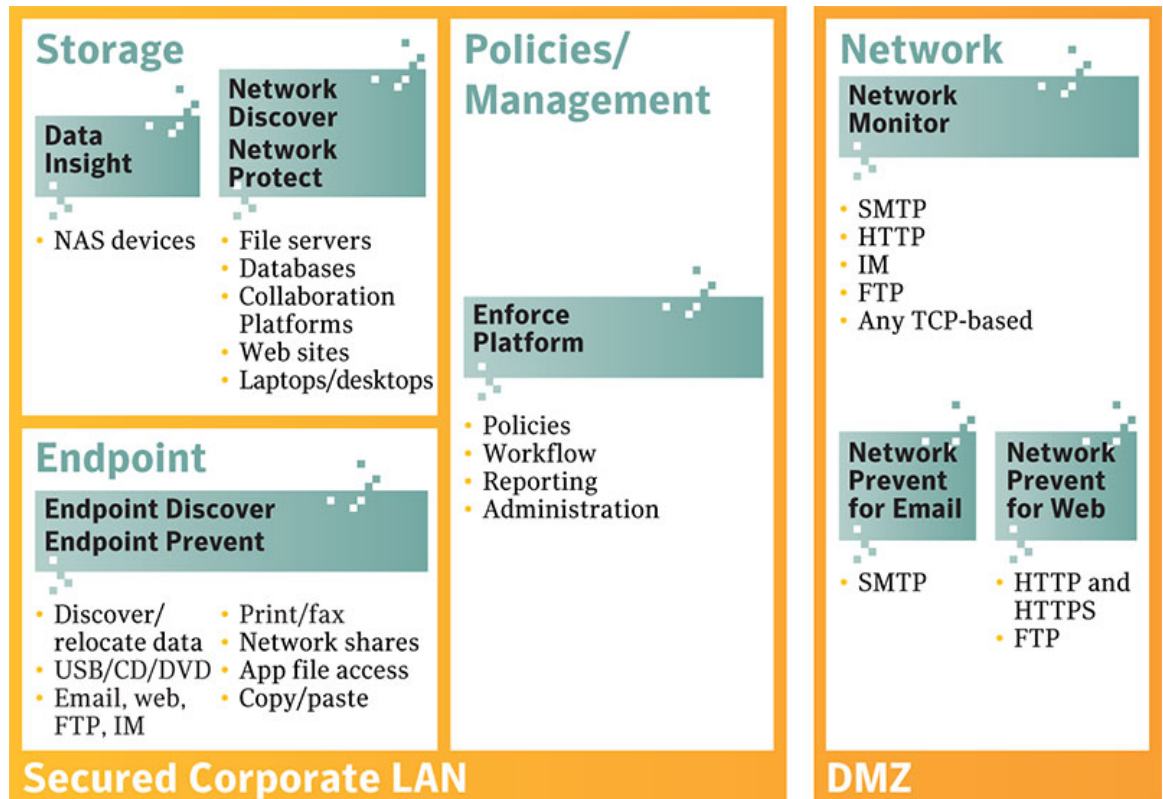


Fig 2.1

Organizations are increasingly facing the challenge of enforcing IT security policies. With rapidly growing workforces in geographically diverse locations and employees often working outside the corporate networks, rogue business processes that don't comply with internal regulations can easily manifest. The Symantec Data Loss Prevention Enforce Platform enables organizations to manage and apply unified data security policies across the enterprise. In one comprehensive management console, the Enforce Platform enables organizations to define policies once and enforce them everywhere. Designed for the business user, the Enforce Platform is easy to use for remediation and reporting on policy violations, which allows the lowest number of staff resources needed to manage the solution. Its advanced detection technology helps ensure the highest level of accuracy by analyzing both content and context on an enterprise scale. This helps organizations to prevent confidential data loss and maintain a low total cost of ownership.

We need to distinguish content from context. One of the defining characteristics of DLP solutions is their content awareness. This is the ability of products to analyze deep content using a variety of techniques, and is very different from analyzing context. It's easiest to think of content as a letter, and context as the envelope and environment around it. Context includes things like source,

destination, size, recipients, sender, header information, metadata, time, format, and anything else short of the content of the letter itself. Context is highly useful and any DLP solution should include contextual analysis as part of an overall solution.

A more advanced version of contextual analysis is business context analysis, which involves deeper analysis of the content, its environment at the time of analysis, and the use of the content at that time.

Content awareness involves peering inside containers and analyzing the content itself. The advantage of content awareness is that while we use context, we're not restricted by it. If I want to protect a piece of sensitive data I want to protect it everywhere — not just in obviously sensitive containers. I'm protecting the data, not the envelope, so it makes a lot more sense to open the letter, read it, and decide how to treat it. This is more difficult and time consuming than basic contextual analysis and is the defining characteristic of DLP solutions.

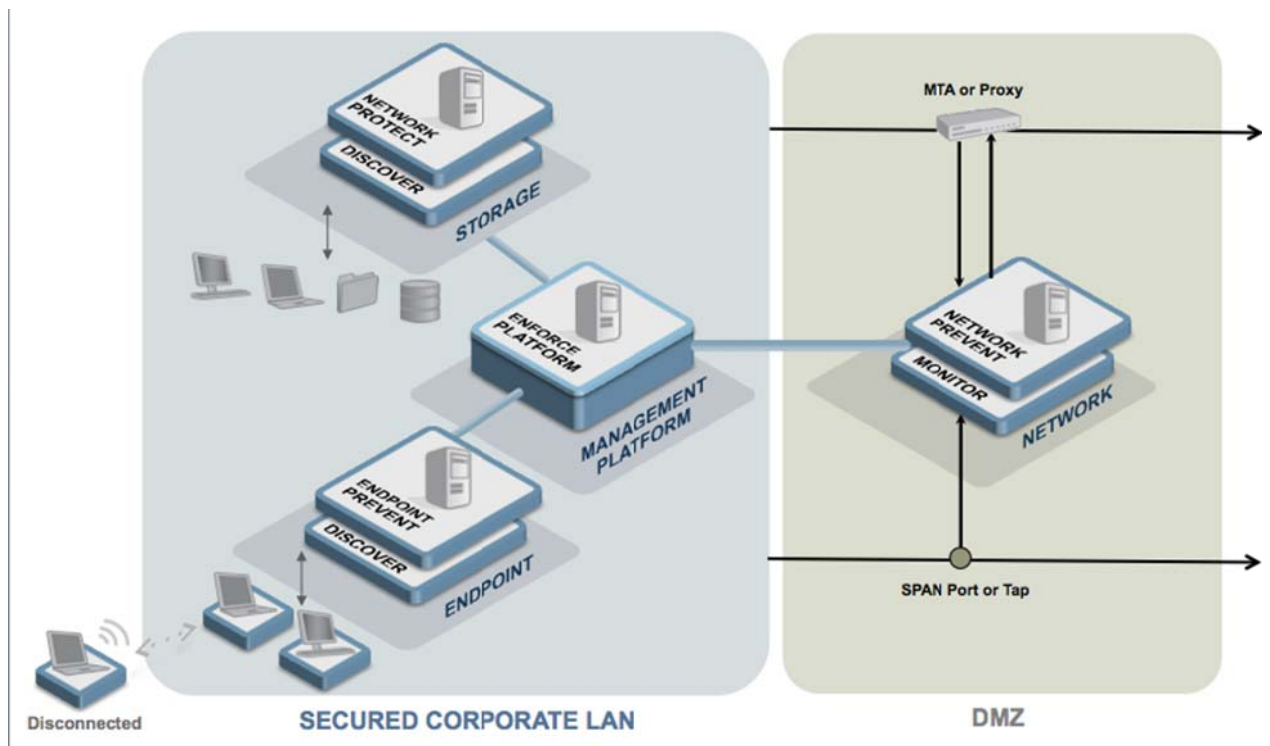


Fig. 2.2

Chapter 3: System Requirements

3.1. Hardware Interfaces

A simple mouse and keyboard is required to operate the proposed system.

3.2. Software Interfaces

Our system requires certain third-party software for troubleshooting or performing specific functions.

3.2.1 **WireShark** to verify that the detection server NIC receives the correct traffic from the SPAN port or tap. You can also use Wireshark to diagnose network problems between other servers.

3.2.2 **Dagsnap** in combination with Wireshark to verify that the detection server Endace NIC receives the correct traffic from the SPAN port or tap. dagsnap is included with Endace cards, and is not required with non-Endace cards.

3.3. Communication Interfaces

Both database and enforce server will be communicating with each other using standard TCP protocol.

Hardware requirements and recommendations

Hardware	Minimum requirements	Recommended
CPU	Pentium 4	Dual processor dual core
CPU Speed	1.8 GHz	2.53 GHz
RAM	1 GB	4 GB, DDR2
Cache	not checked	3 MB L2
Network	not checked	Gigabit
Hard disk	5 GB of free disk space	10,000 RPM SCSI or better. 10 GB of free disk space.

Fig. 3.1

3.4. Configuring a User Account

- 3.4.1 In the Enforce Server Administration Console, go to System > User Management > Users and click Add User.
- 3.4.2 Enter the user name in the Name field. The user name must be between 8 and 30 characters long, is case sensitive, and cannot contain backslashes (\).
- 3.4.3 Enter the user password in the Password and the Re-enter Password fields. The password must be at least eight characters long and is case sensitive. For security purposes the password is obfuscated and each character appears as an asterisk.
- 3.4.4 If you configure advanced password settings, the user must specify a strong password. In addition, the password may expire at a certain date and the user has to define a new one periodically.
- 3.4.5 If you configure Active Directory integration with the Enforce Server, users can authenticate using their Active Directory passwords. In this case the password field does not appear in the Users screen.
- 3.4.6 Optionally you can enter an Email Address for the user. You can intentionally lock a user out of the system by selecting the Account
- 3.4.7 For security, after a certain number of consecutive failed logon attempts, the system automatically disables the account and locks out the user. In this case the Account Disabled option is checked. To reinstate the user account and allow the user to log on to the system, clear this option by unchecking it.
- 3.4.8 Depending on the language pack(s) you have installed, you can set the language preference for the user.
- 3.4.9 In the Report Preferences section of the Users screen you specify the preferences for how this user is to

receive incident reports, including Text File Encoding and CSV Delimiter.

- 3.4.10 If the role grants the privilege for XML Export, you can select to include incident violations and incident history in the XML export.
- 3.4.11 Select the roles to assign data and incident access privileges to the user.
- 3.4.12 A user must be assigned to a role. If no role has been created the user is assigned to the default role.
- 3.4.13 Click Save to save the user configuration. Receives and records Tank Commander operational information and makes it available to the troop leader.

Software requirements and recommendations

Software	Minimum requirements for evaluation	Recommended for small business
Microsoft.NET	Microsoft.NET 3.5	Microsoft.NET 3.5
Microsoft Operating system	Microsoft Windows Server 2003 (Windows Server 2008 is not supported.)	Microsoft Windows Server 2003 (Windows Server 2008 is not supported.)
Web browser	Microsoft IE 7	Microsoft IE 7
Microsoft IIS	IIS 6	IIS 6
AJAX	AJAX 1.0	AJAX 1.0
Microsoft SQL Server	Microsoft SQL Server 2005 Express	Microsoft SQL Server 2005 Express for 500 or less managed computers. Microsoft SQL Server 2005 Standard or Enterprise for more than 500 managed computers.

Fig 3.2

3.5 Advanced authentication settings

- 1.1 Go to System > Settings > General and click Configure.
- 1.2 To require strong passwords, locate the Password Enforcement section and select Require Strong Passwords. Symantec Data Loss Prevention prompts existing users who do not have strong passwords to create one at next logon.
- 1.3 To set the period for which passwords remain valid, type a number (representing the number of days) in the Password Rotation Period field. To let passwords remain valid forever, type 0 (the character for zero).
- 1.4 The Role List screen displays an alphabetical list of the roles that are defined for your organization.
- 1.5 Roles listed on this screen display the following information:
- 1.6 Name – The name of the role
- 1.7 Description – A brief description of the role Assuming that you have the
- 1.8 appropriate privileges, you can view, modify, or delete roles as follows:
- 1.9 Click the red X icon (far right) to delete the role; a dialog box confirms the deletion. Before editing or deleting roles, note the following guidelines:
- 1.10 If you change the privileges for a role, users in that role who are currently logged on to the system are not affected. For example, if you remove the Edit privilege for a role, users currently logged on retain permission to edit custom attributes for that session. However, the next time users log on, the changes to that role take effect, and those users can no longer edit custom attributes.
- 1.11 If you revoke an incident-viewing privilege for a role, the Enforce Server automatically deletes any saved reports that rely on the revoked privilege. For example, if you revoke the privilege to view

network incidents, the system deletes any saved network incident reports associated with the newly restricted role.

- 1.12 When you delete a role, you delete all shared saved reports that a user in that role saved.

3.6 Precision and Accuracy

System should be able to accurately and precisely locate the data to be protected otherwise a lot of false alarms would be inconvenient for the administrator as well as the employees and incident response team.

3.7 Reliability and Availability

The Maximum Mean-Time-To-Repair (MTTR) of the system which is here equal to the Mean-Down-Time (MDT) should be less than 10 seconds so that if a system fails, the administrator can restore it and get the functionality up back within short time. Also, the mean-time-between-failures (MTBF) should absolutely not be less than 1 day. So with a MTBF of one day and a MTTR of 10 seconds, we get high availability. Maintenance should be performed during “quiet-hours” (usually at night), in order to avoid rush-hours and keep a high reliability.

3.8 Scalability

The system will be highly scalable, i.e. as the number of endpoints connected increases and communications will start to arise, the hardware infrastructure will be expanded according to the needs.

3.9 Access

Access to DLP management console will be limited to administrators only and will be restricted by issuing unique usernames and passwords to all administrators.

3.10 Integrity

The integrity of the information stored in the system has to be preserved. Every unauthorized attempt of altering the data stored has to be blocked. This will include all data that is flagged confidential in policy server. Also a backup of policy server data is to be maintained on daily basis to restore system as quickly as possible in case of a crash.

3.11 Privacy

Controlled access to system ensures data privacy.

3.12 Usage Easiness

90% of a test panel of system administrators should be able to successfully add, delete or edit a data rule within 5 minutes.

Ease of remembering: ninety-five percents of the test panel should be able to remember how to use all the functionalities he has experienced within two hours of use. With remembering it is meant that the user will be able to locate the functionality he wishes to use in 1 minute or less.

After having used the application once, 95% of users are able to locate the experienced functionality within 1 minute.

3.13 Error Rates

After two week use, the user should achieve an error rate of less than 0.5%. Errors include: use the wrong functionality, login failure (wrong credentials), delete the wrong entry (or more than wanted); this measure can be achieved by online anonymous questionnaire.

3.14 Trust

After having used for 3 months, 90% of the corporations should feel confident about the reliability, robustness and be convinced that the product does what it is expected to do.

3.15 Learning

Any user without computer skills should be able to read system logs, add a new business policy, and read past policy violations within the first 5 minutes of usage without referring to the user manual.

3.16 Maintenance

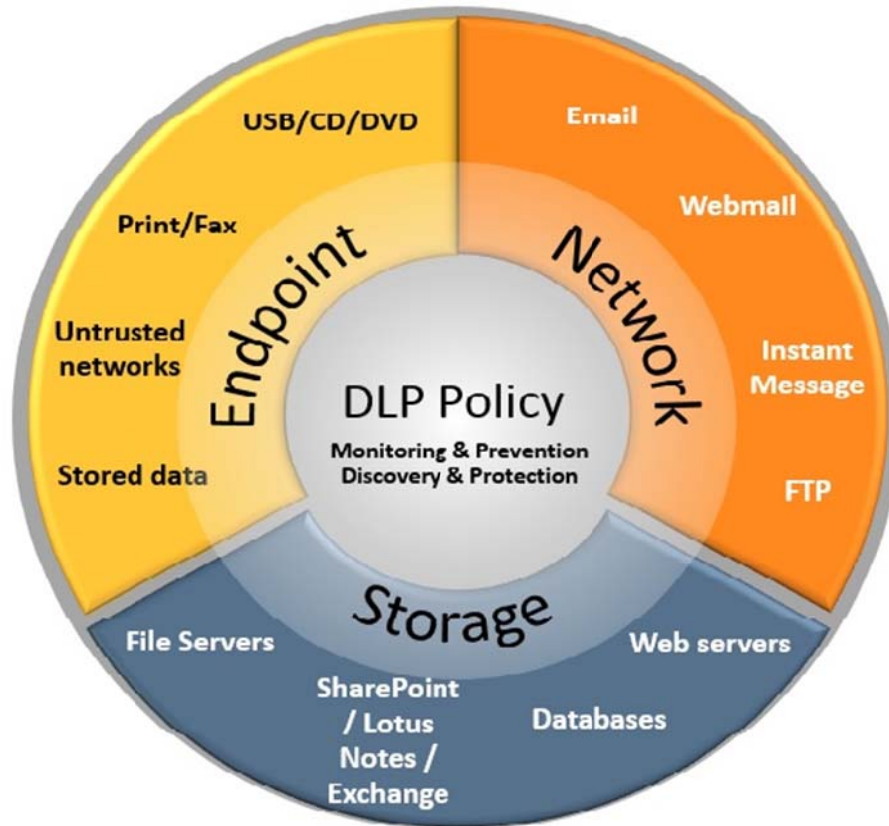
Maintenance will be offered along with the product in a separate contract.

3.17 Adaptability Requirements

The solution should be portable to other versions of Microsoft operating system.

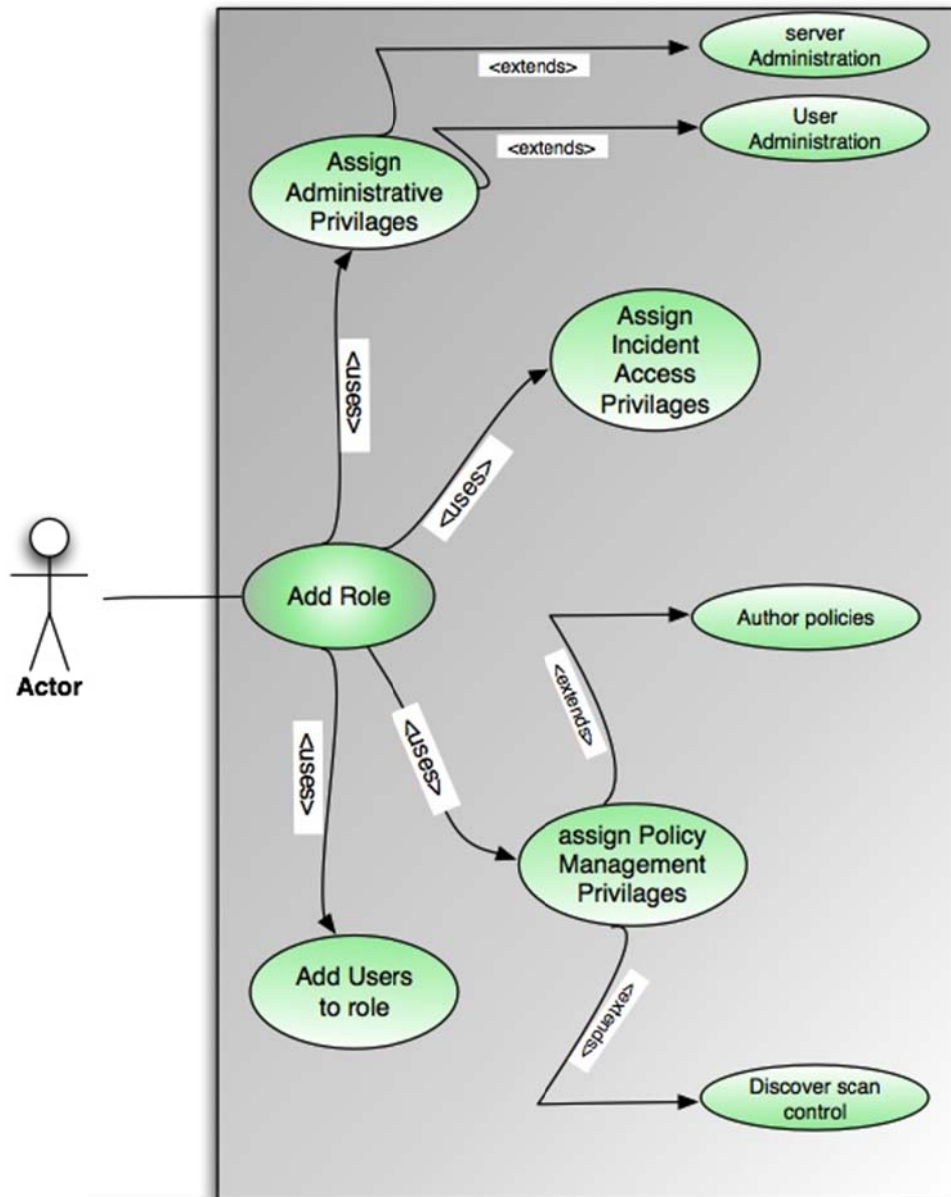
Chapter 4: Software Design Specification

4.1. Abstract overview of system



4.3 Use Case Diagrams

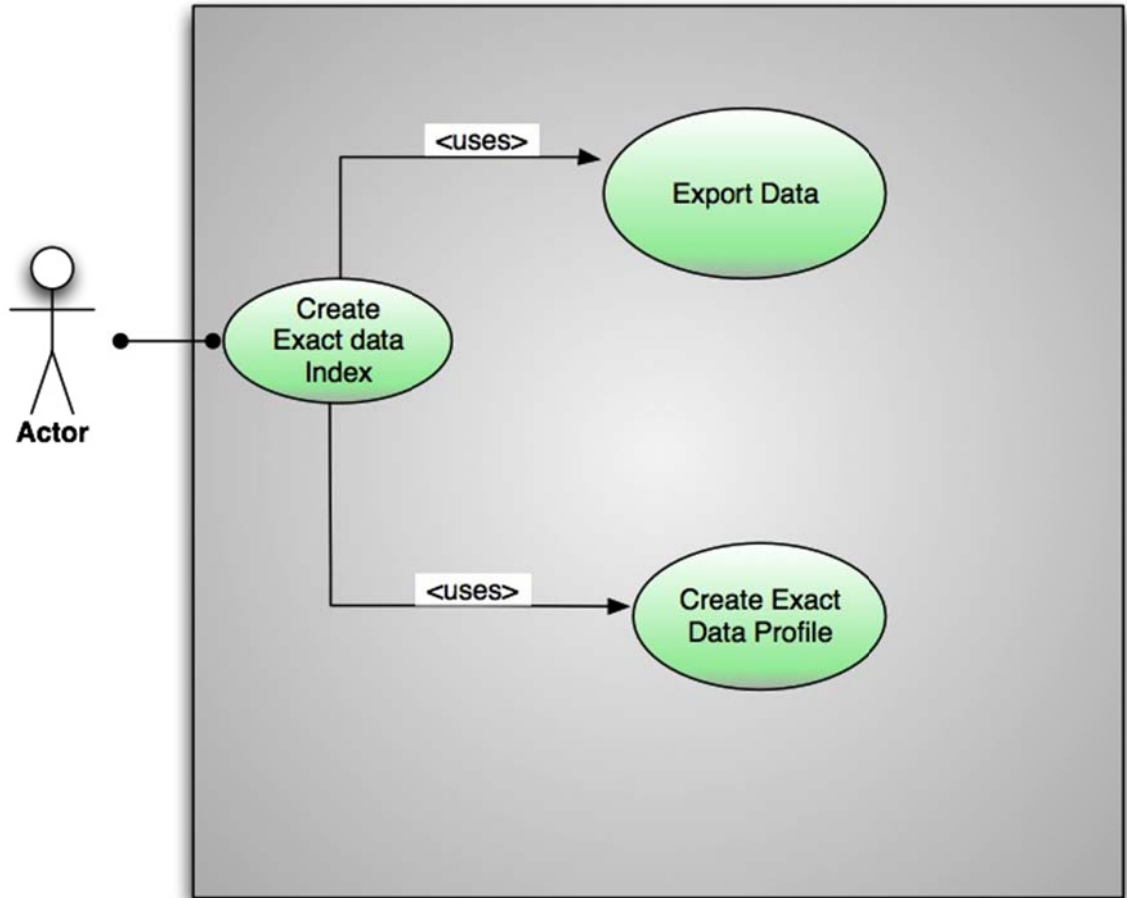
4.2.1 Add Role Use Case Diagram



Name	Add Role
ID	UC-L-01
Version	1
Author(s)	NC Hasnat , NC Hamzah , PC Nabeel
Primary Actor(s)	Administrator
Date	2 FEB 2013
Summary	This use case depicts how to add role and how to add users to a role. Assignment of policies management, incident access privileges and assignment of administrative privileges for both user and servers.
Basic Path	<ol style="list-style-type: none"> 1. Go to Administration > Users > Roles and click Add Role. 2. Type a role name and description. The name, which is case sensitive 3. Select one of the following administration privilege(s) for the role (Server Administration, User Administration) 4. Select incident access control preferences for this role. 5. On the Policy Management tab, select one of the following

	policy privileges for the role(Author Policies, Discover Scan Control)
Alternative Paths	None
Exception Paths	None
Extension Points	
Triggers	The roles are defined and also policy managements are done and who can view incidents are done
Assumption	
Pre-Condition	No roles were defined and noone who can view incidents and reports and who can do what
Post-Condition	After doing this everyone is given a role and who can see incidents and who can manage policies are clearly defined

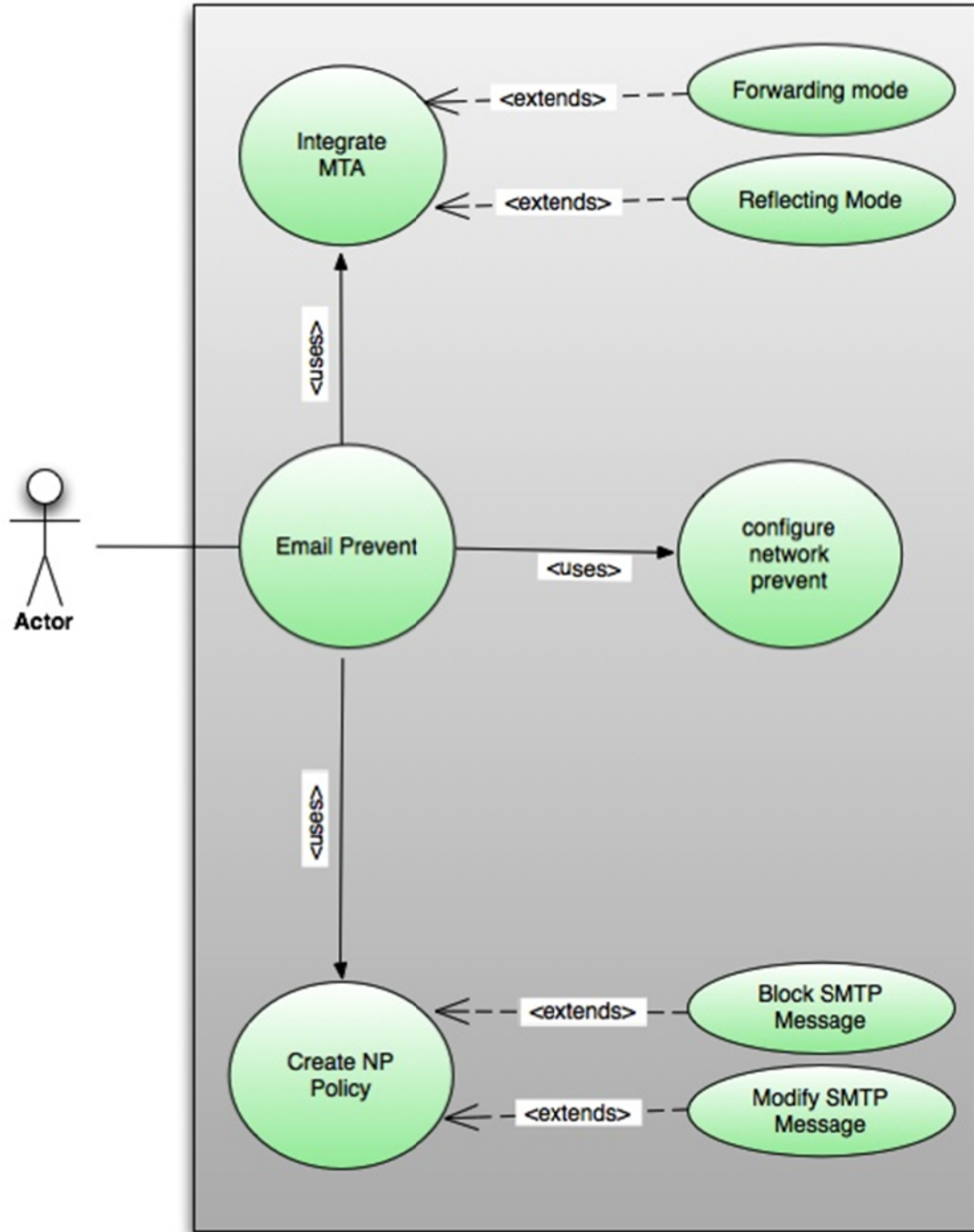
4.2.2 Exact Match Use Case Diagram



Name	Exact Match
ID	UC-L-02
Version	1
Author(s)	NC Hasnat , NC Hamzah , PC Nabeel
Primary Actor(s)	Administrator
Date	2 FEB 2013
Summary	To detect exact data, Data Loss Prevention requires a special indexed version of the data. Data Loss Prevention index is a secure file (or set of files). It contains hashes of the exact data values from each field in your data source, along with information about those data values. The index does not contain the data values themselves, so it is secure.
Basic Path	<ol style="list-style-type: none"> 6. Export the data from your database (or other data repository) into a tabular text file that is called the data source. 7. Prepare the data source for indexing. 8. Create an exact data profile (in the Enforce Server administration console) that specifies the data source, the indexing parameters, and the indexing schedule. 9. Create an index from the data source.
Alternative	None

Paths	
Exception	None
Paths	
Triggers	<p>This feature is useful when you do not want to copy the data source.</p> <p>To the Enforce Server. For example, when the originating department wants to avoid the security risk of copying the data to an extra-departmental host.</p>
Pre-Condition	
Post-Condition	<p>As soon as you create an exact data profile, you can reference it in a policy</p> <p>detection rule</p>

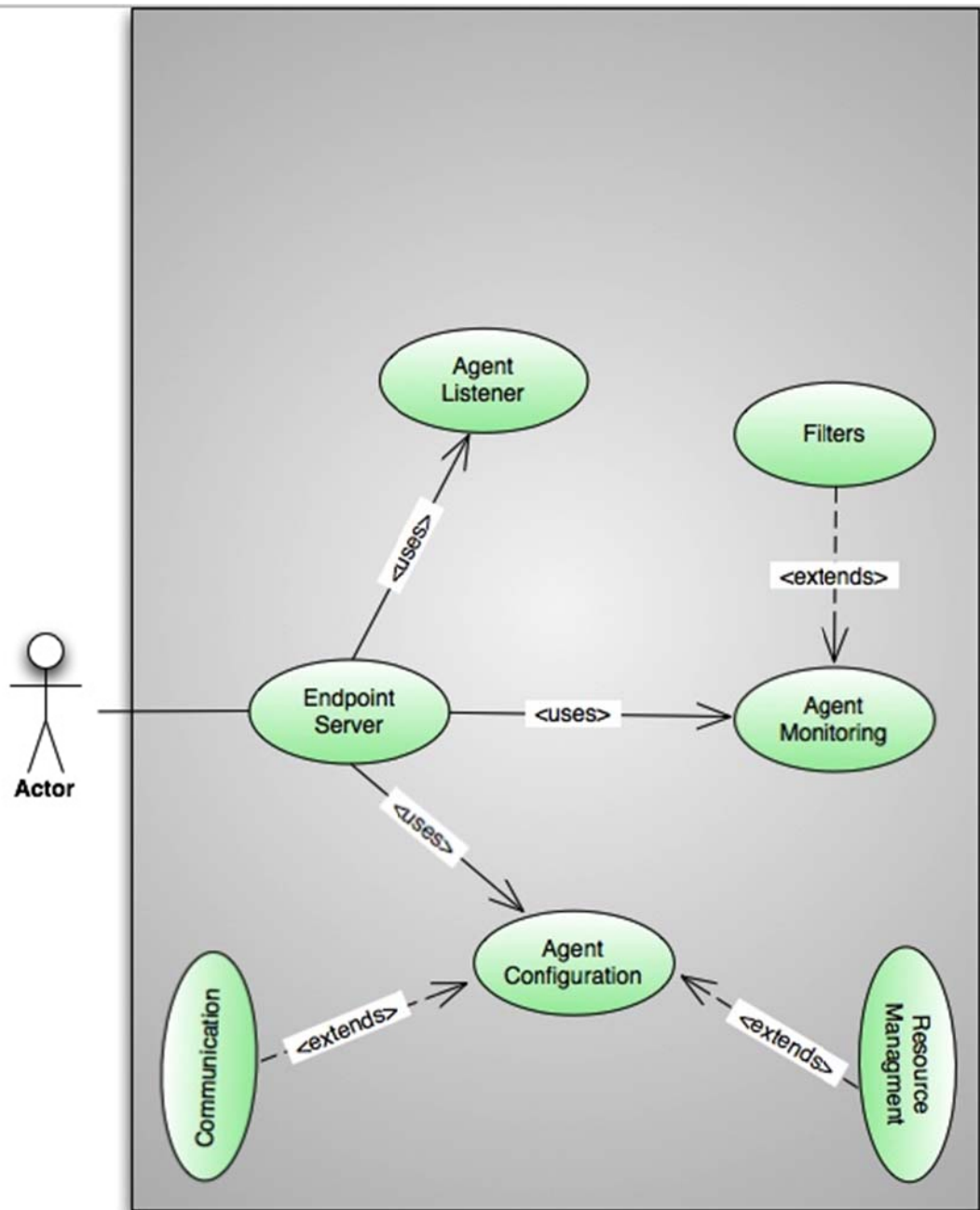
4.2.3 Email Prevent Use Case Diagram



Name	Add Email Prevent
ID	UC-L-03
Version	1
Author(s)	NC Hasnat , NC Hamzah , PC Nabeel
Primary Actor(s)	Administrator
Date	2 FEB 2013
Summary	This use case depicts how to add network prevent to DLP solution. Network Prevent monitors and analyzes outbound email traffic in-line and (optionally) blocks, redirects, or modifies email messages as specified in your policies.
Basic Path	<p>10. Choose an integration architecture and configure your Mail Transfer Agent (MTA) to work with the Network Prevent Server (Email).</p> <p>11. Configure the Network Prevent Server (Email) to work within your chosen integration architecture.</p> <p>12. If you plan to encrypt or quarantine email messages, configure the necessary third-party encryption server(s) or archiving servers.</p> <p>4. Create and deploy a policy for Network Prevent (Email).</p>

Alternative Paths	None
Exception Paths	None
Extension Points	
Triggers	Server is setup to monitor EMAIL activity on network and policies are defined for system to act in an automated manner on encountering a violation.
Assumption	
Pre-Condition	NO email prevent server has been deployed and corporate MTA is already up and running.
Post-Condition	Corporate MTA gets integrated to Email prevent server and all mails gets scanned to detect any policy violations.

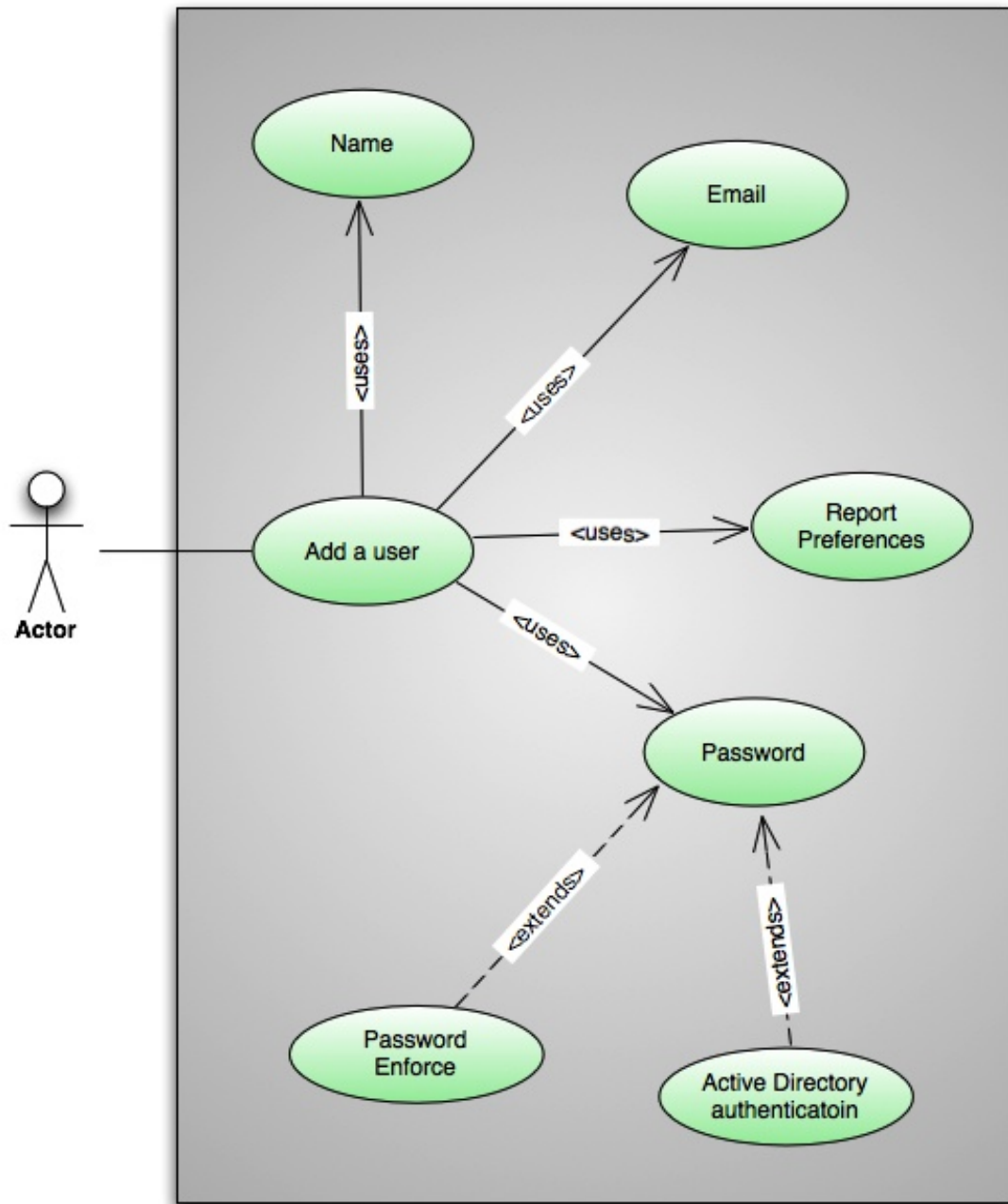
4.2.4 Endpoint prevent Use Case Diagram



Name	Endpoint Prevent
ID	UC-L-04
Version	1
Author(s)	NC Hasnat , NC Hamzah , PC Nabeel
Primary Actor(s)	Administrator
Date	2 FEB 2013
Summary	This use case depicts how to add Endpoint prevent to DLP solution. Endpoint Prevent monitors and analyzes the data copied printed faxed and blocks if violation in policy is found and redirect it to administrator
Basic Path	<p>13. Configure your agent listener, agent manager and agent configure to work on DLP endpoint server</p> <p>14. In agent listener add your local IP address and port number</p> <p>15. Enables Endpoint monitoring on endpoint computer destinations such as removable media, CD/DVD drives, local drives, printers, and other physical destinations.</p> <p>16. Limit the Agent Store size on the endpoint computer hard drive. You can limit the Agent Store by percentage of the hard drive or by bytes. The default is 5% of available hard drive space.</p>

	<p>17. Specify, in hours, how long you want backup data to remain in the recovery folder.</p> <p>18. Specify the path where you want to store copies of the sensitive data that the Symantec DLP Agent stops from transferring to removable media</p>
Alternative Paths	None
Triggers	Server is setup to monitor Endpoint activity on usb ports/printing machines and policies are defined for system to act in an automated manner on encountering a violation.
Assumption	
Pre-Condition	NO endpoint prevent server has been deployed and no policies are defined
Post-Condition	Now all data which is copied to USB device or printed will be monitored and examined

4.2.5 Add a user Use Case Diagram

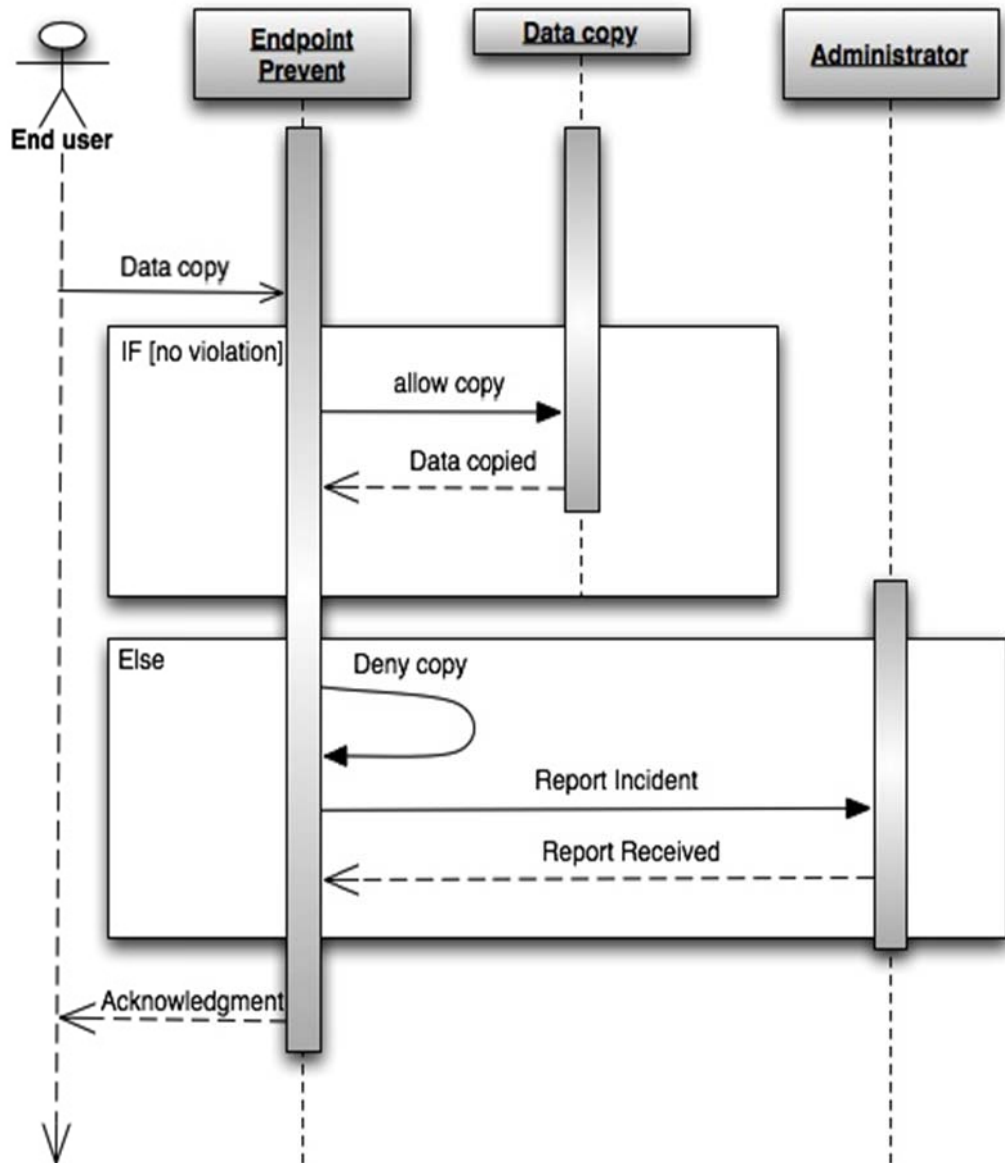


Name	Add a user
ID	UC-L-05
Version	1
Author(s)	NC Hasnat , NC Hamzah , PC Nabeel
Primary Actor(s)	Administrator
Date	2 FEB 2013
Summary	This use case depicts how to add user. What will be his access level assigning him a password and email
Basic Path	<p>19. Enter the name of user</p> <p>20. Enter the password</p> <p>21. Enter the password</p> <p>22. System will check the detail and assign him email if available</p> <p>23. Also system will assign him access level i-e user or administrator or investigator</p>
Alternative Paths	None
Exception Paths	None
Extension Points	

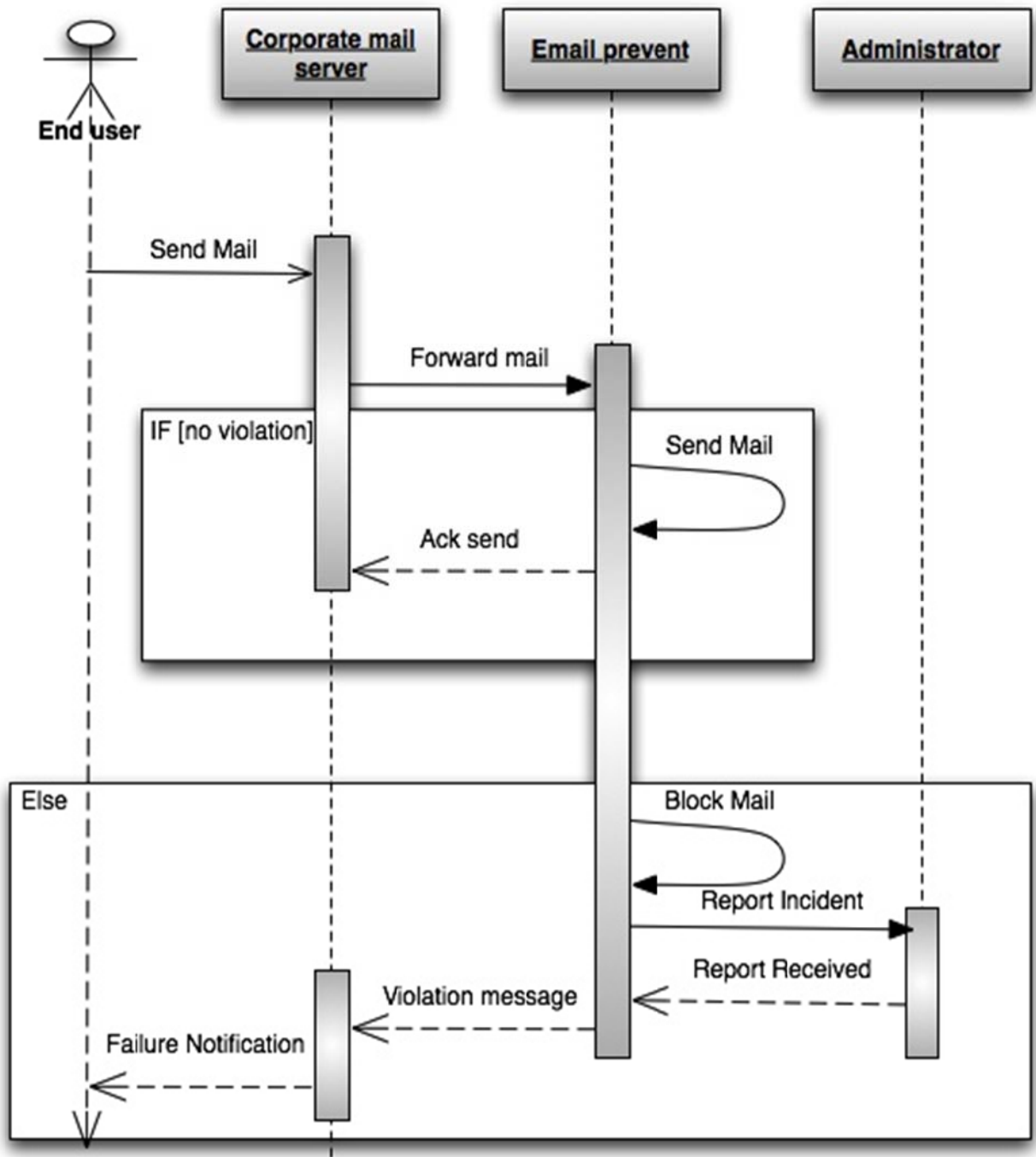
Triggers	New user added and access level assigned
Assumption	
Pre-Condition	
Post-Condition	

4.3 Sequence Diagrams

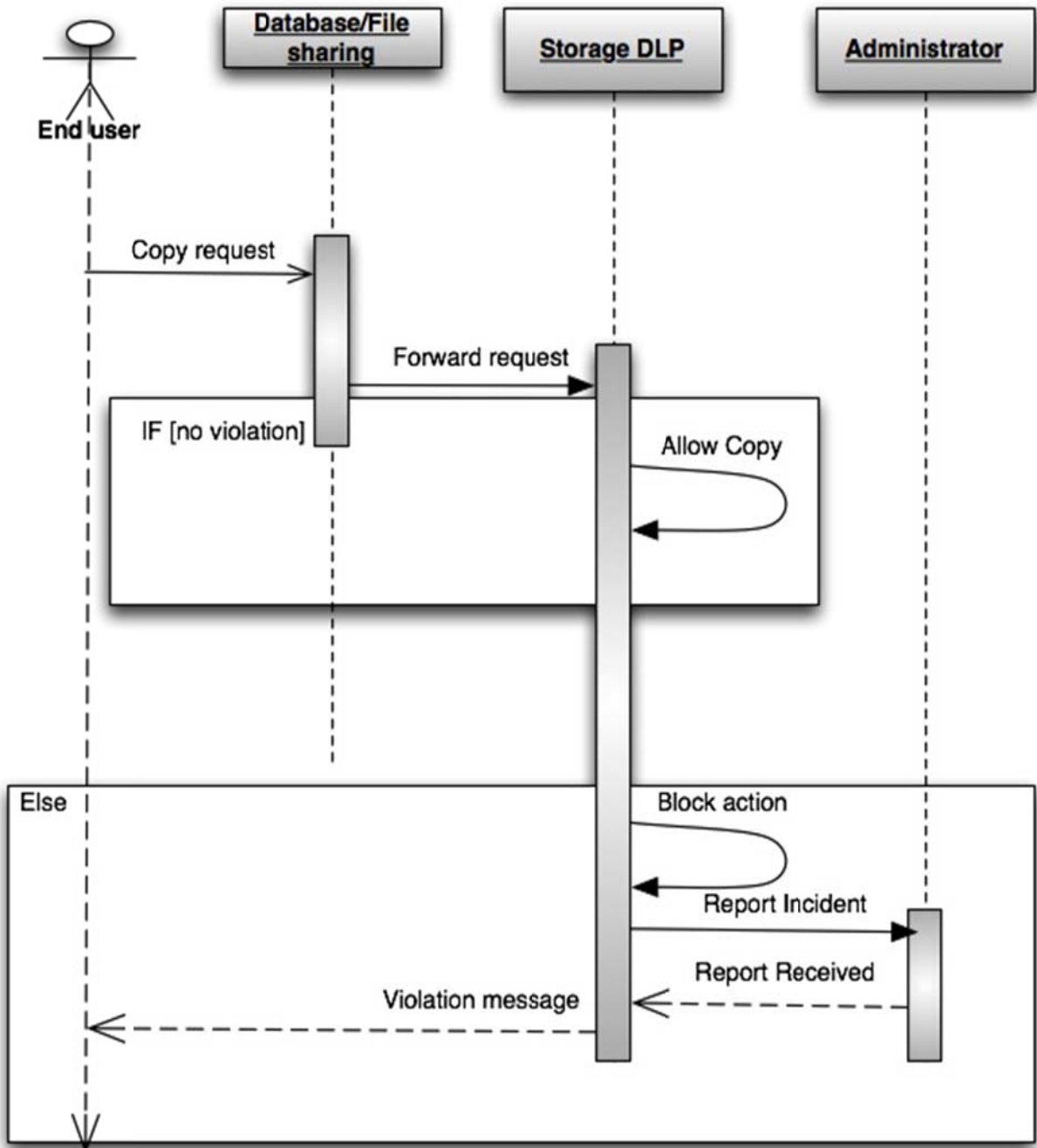
4.3.1 Endpoint Sequence Diagram



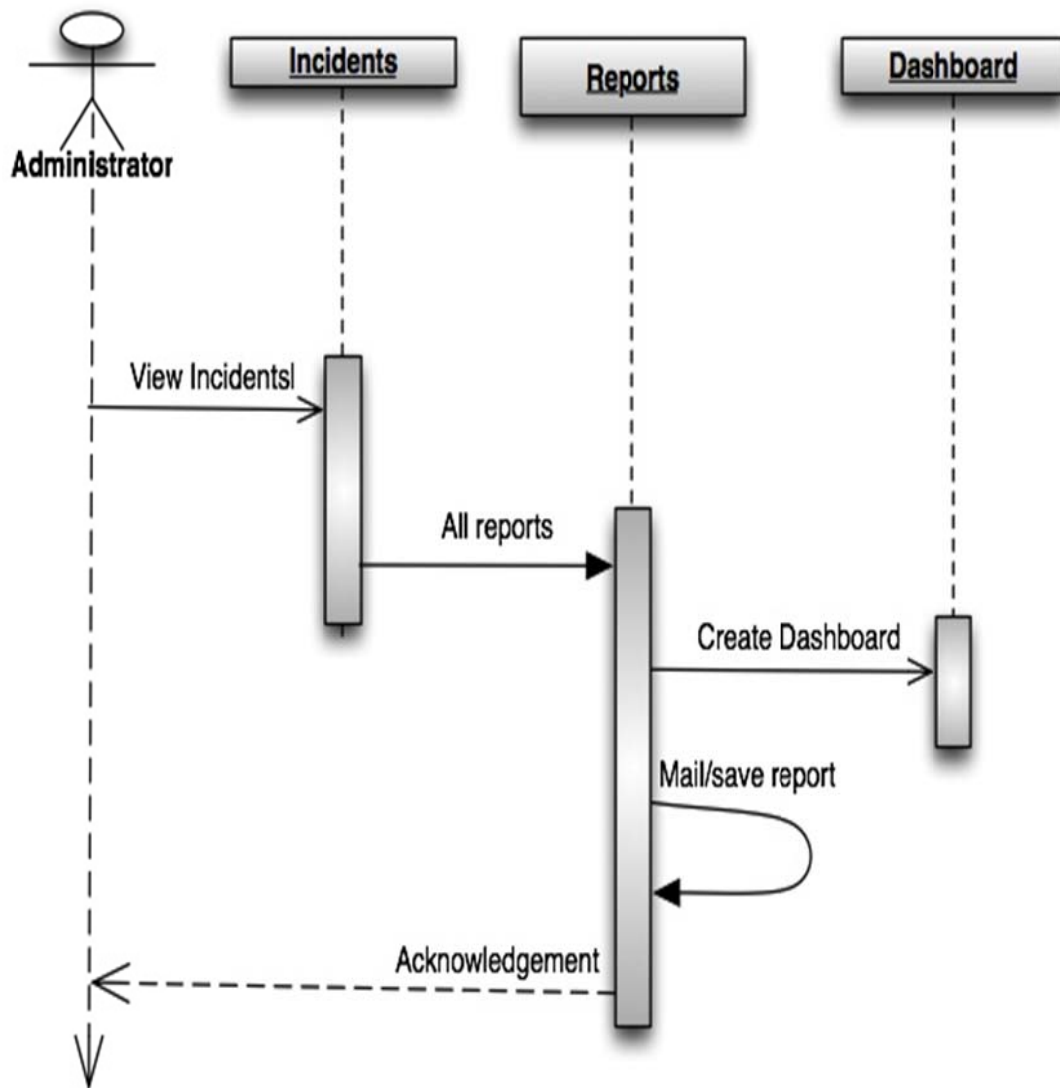
4.3.2 Network Sequence Diagram



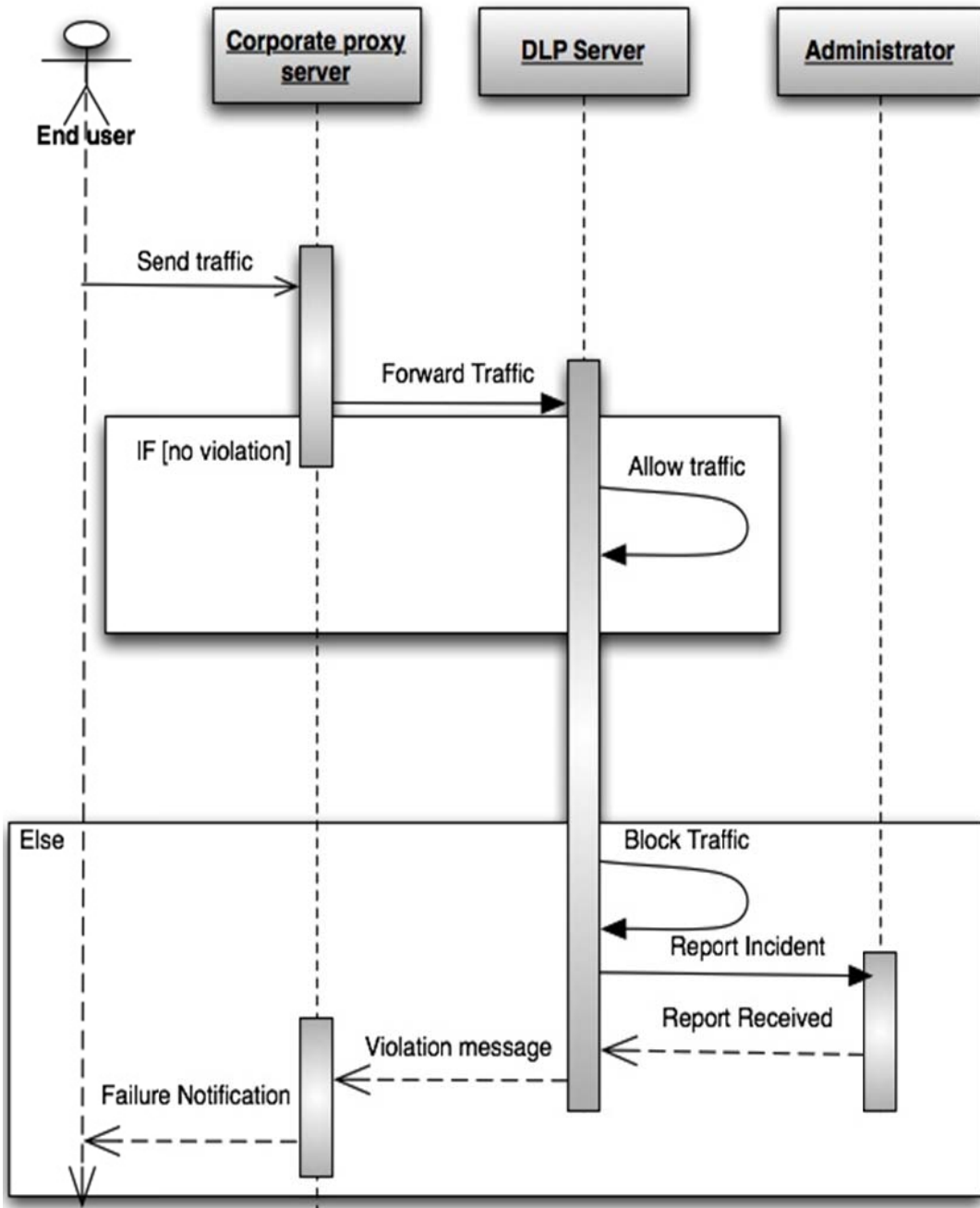
4.3.3 Storage DLP sequence Diagram



4.3.4 Report Check Sequence Diagram

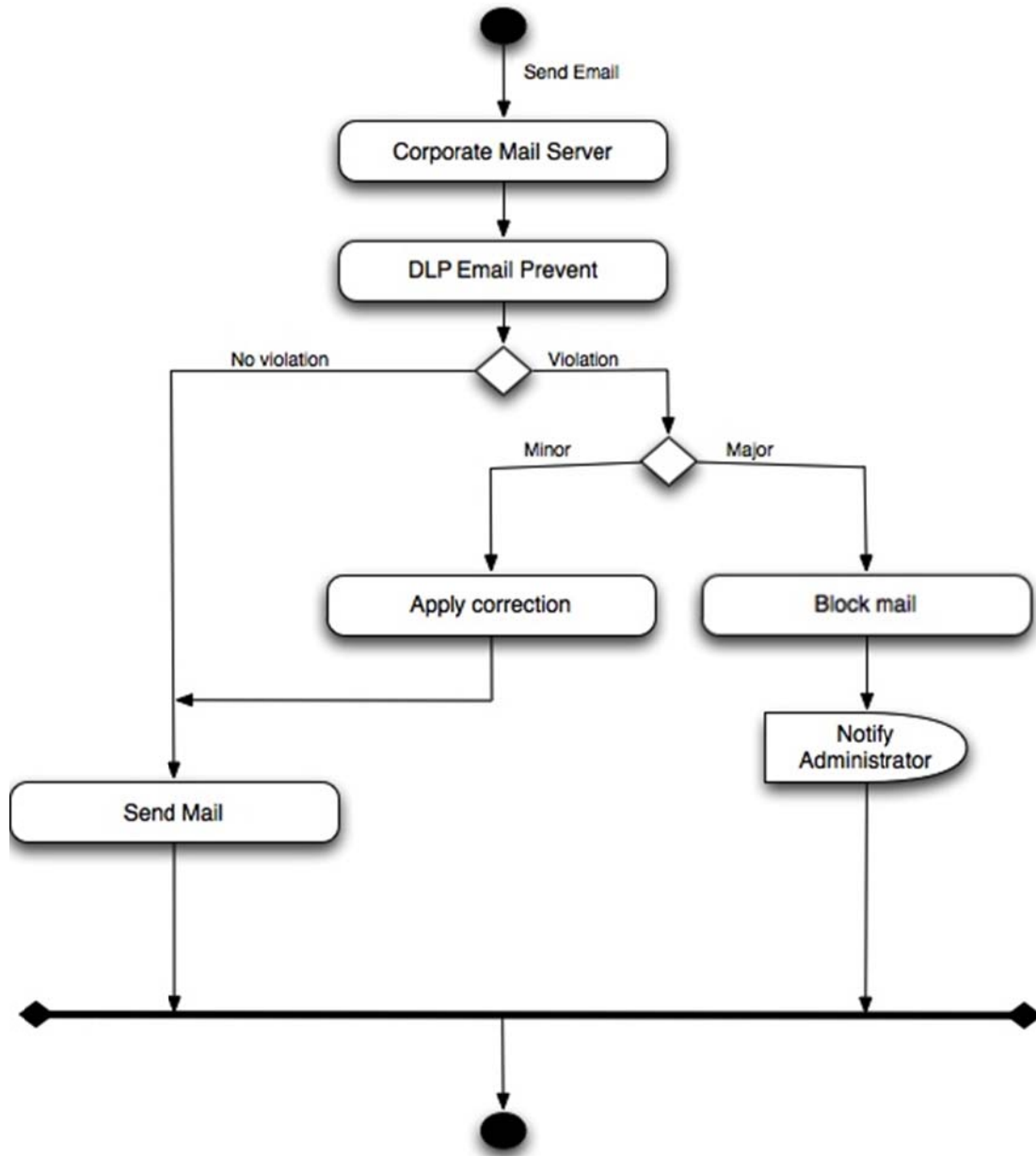


4.3.5 Secure Browsing Sequence Diagram

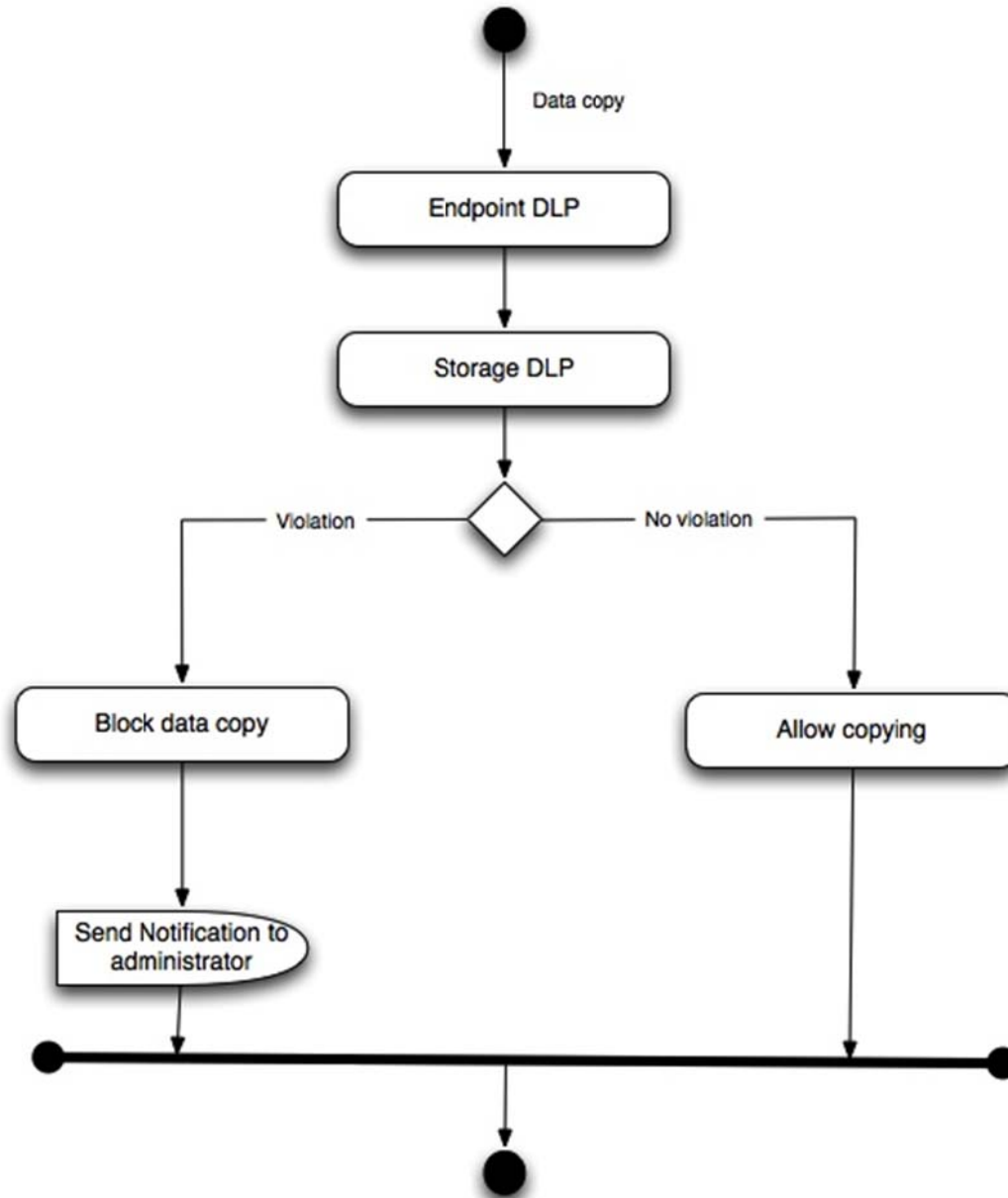


4.4 Activity Diagrams

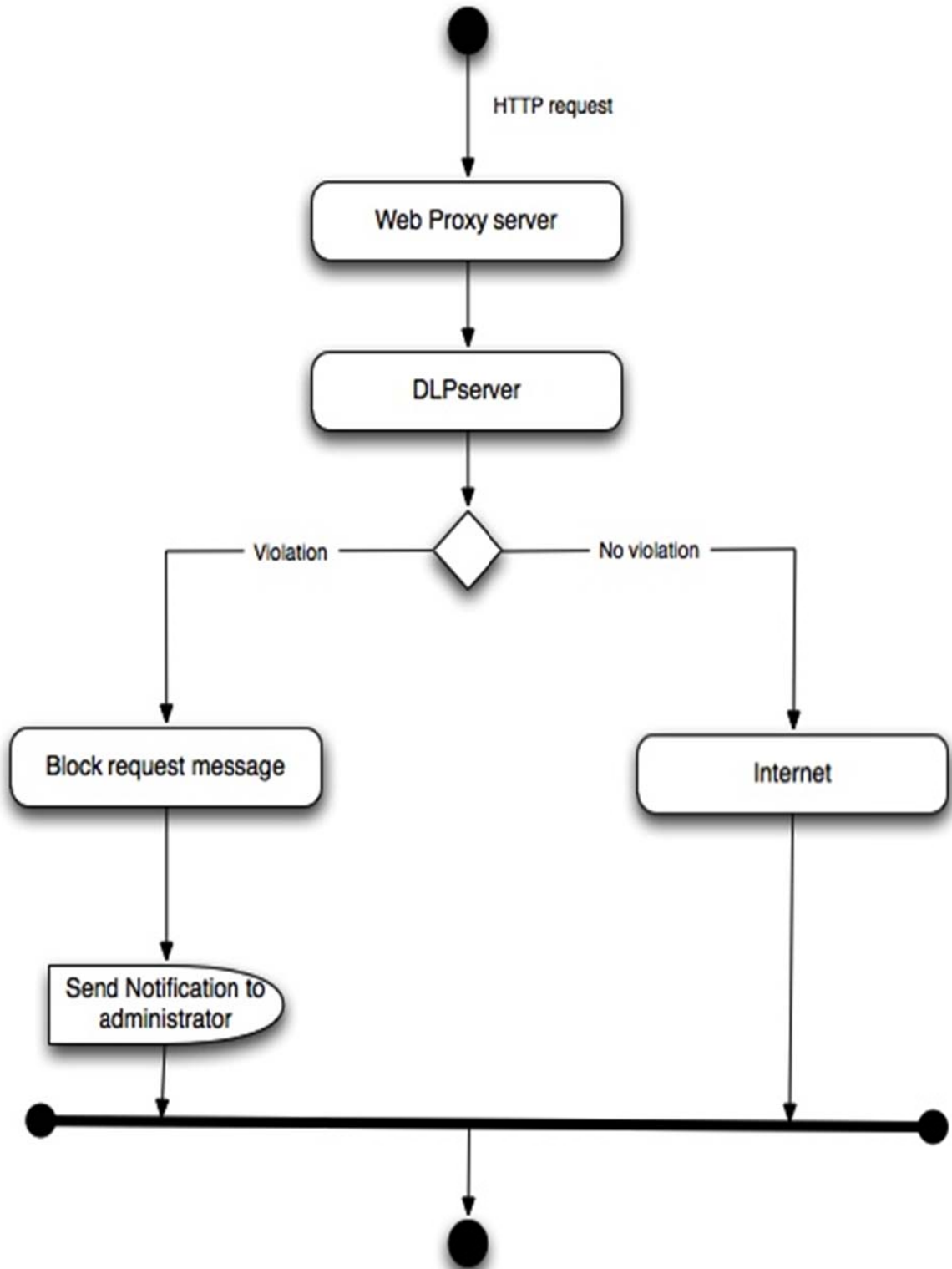
4.4.1 Email Prevent



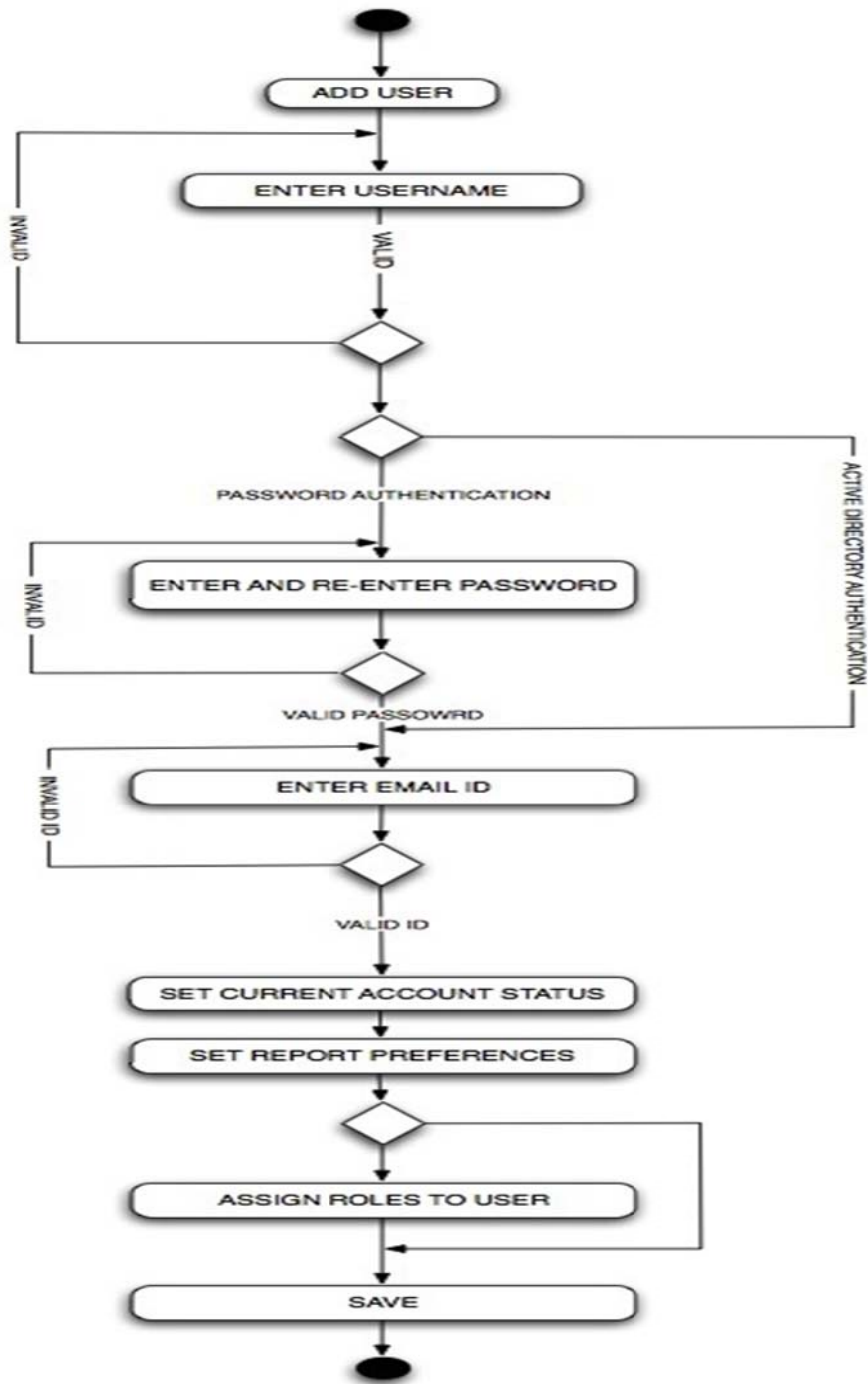
4.4.2 Storage DLP activity



4.4.3 Secure Browsing



4.4.4 Add User Activity



Chapter 5: System Implementation

5.1 Architecture Diagram

Data Loss Prevention offers a family of products designed to work together to monitor and protect your organization's sensitive data wherever the data is stored and however it is sent out of your organization.

The architecture is comprised of the management platform and a combination of one or more detection servers that detect and protect data in the following three (3) enterprise-wide security coverage areas:

5.1.1 Network - commonly referred to as data in motion. Network coverage monitors and protects data that is being transmitted over your network to the internet. Examples include common business applications such as email as SMTP, webmail as HTTP, IM and FTP.

5.1.2 Storage - commonly referred to as data at rest. Storage coverage scans and protects data that is stored in your enterprise data repositories. Examples include public and private shares, databases, and collaboration sites.

5.1.3 Endpoint - applicable to devices such as laptops, desktops, or workstations. Endpoint coverage monitors and protects data as it is moved to or off the endpoint machines. Examples include downloading data to the hard drive, copying data to removable media such as USB, and sending email while off the corporate VPN.

This multi-tier distributed architecture allows Symantec to meet the needs of the largest global enterprises in the world, as well as small to medium enterprises. The multi-tier distributed design allows organizations to deploy detection servers and system components across the global enterprise while managing them from a single console.

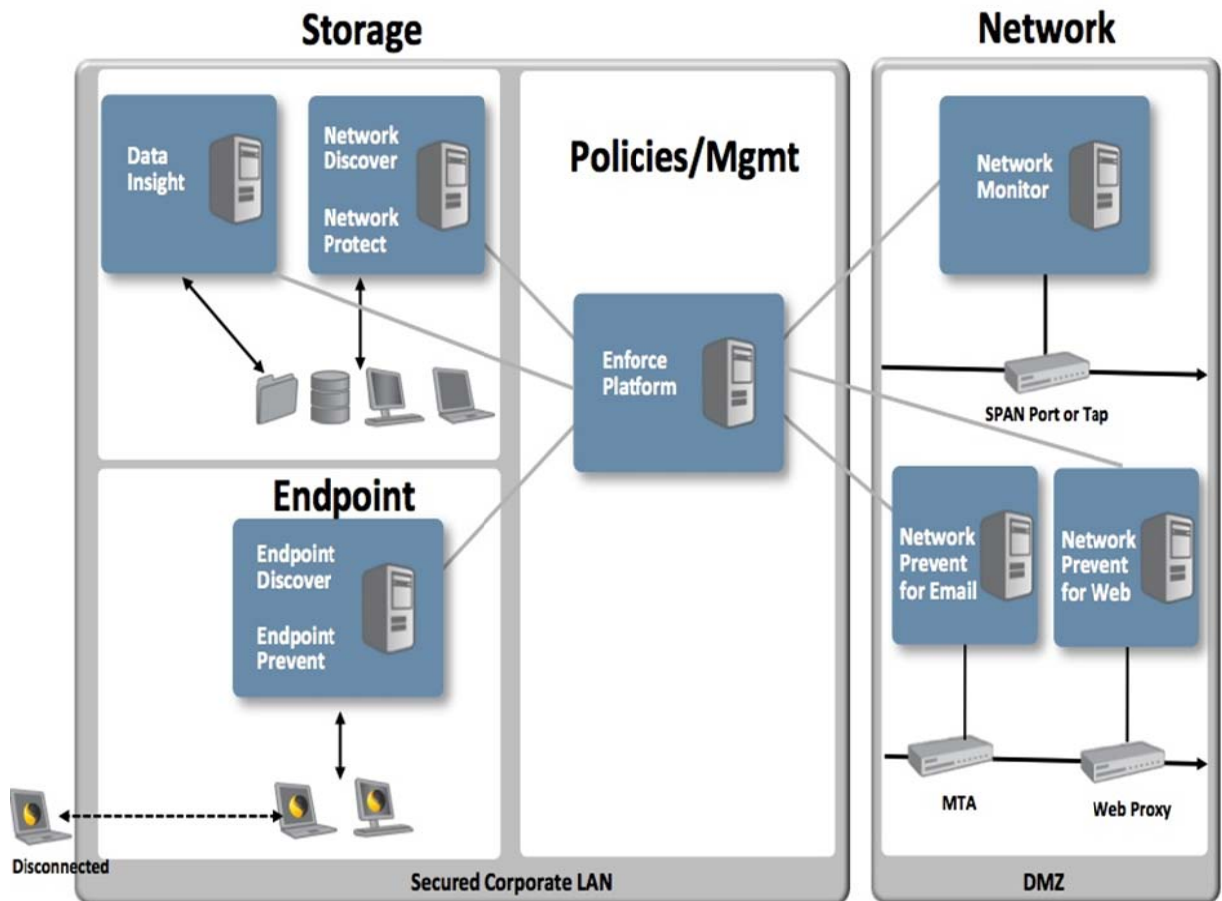


Fig 5.1

5.2 Design Pattern

We will follow multi-tier design pattern (Two tiers). To implement the two-tier installation, you install the Oracle database and the Enforce Server on the same computer. You then install detection servers on separate computers.

The key considerations in determining the deployment size are as follows:

- (a) Number of employees to be monitored
- (b) Amount of network traffic to monitor
- (c) Size of Exact Data Profile (EDP) or Indexed Data Profile (IDP)

5.2.1 Enforce Server

The Enforce Server is the central management platform for Data Loss Prevention. The Enforce Server enables organizations to define, deploy, and enforce consistent data loss prevention policies across Data Loss Prevention products.

5.2.2 Detection Server

Detection server occur in all three part that are endpoint, storage and network .DLP Network Monitor: Detection server is responsible of analyzing packets and data flow (file copies, P2P Protocols, IM messages and more) on your network

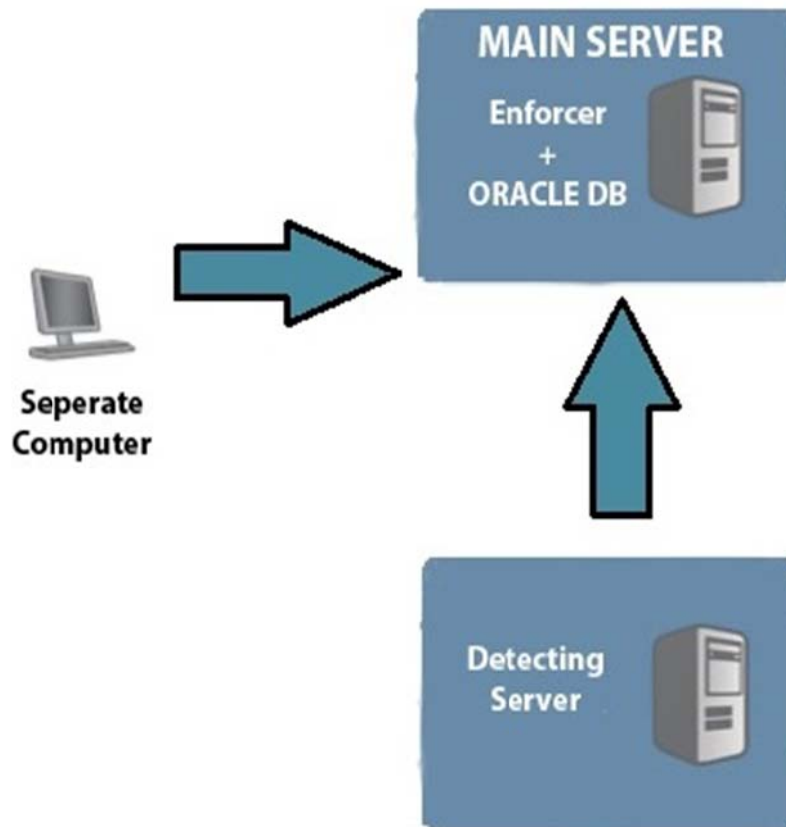


Fig 5.2

Chapter 6: Testing and Result Analysis

6.1 Endpoint DLP Test

6.1.1 A01:

Test Case ID	1
Unit To test	USB blocker at end point
Assumptions	<ol style="list-style-type: none">1. User is logged in2. User Exists3. User has read only rights
Test Data	A file of NIC data
Steps	<ol style="list-style-type: none">1. Insert usb to endpoint2. Right Click on file3. Select "Send-to USB"
Expected Result	File transfer monitored, detected and blocked while mail sent to security
Actual Result	Transfer blocked, Notification email sent
Pass/Fail	Pass

6.1.2 A02:

Test Case ID	2
Unit To test	Endpoint Mail attachment
Assumptions	<ol style="list-style-type: none">1. User logged in endpoint2. User exists3. Has legitimate access to file but read/write only.4. Has email account
Test Data	File containing NIC list
Steps	<ol style="list-style-type: none">1. Open mail account2. Click compose new message3. Click "Attach"4. Browse to Confidential File5. Select the file6. Click Ok
Expected Result	File attachment monitored and blocked along with notification
Actual Result	Attachment blocked, Mail sent to IT Security
Pass/Fail	Pass

6.1.3 A03:

Test Case ID	3
Unit To test	Endpoint
Assumptions	<ol style="list-style-type: none">1. User logged in to endpoint2. Has access to file
Test Data	A file containing NIC list
Steps	<ol style="list-style-type: none">1. Create a new text file2. Copy confidential contents to new file
Expected Result	Copying blocked and Notified authority.
Actual Result	Copy blocked and IT Security notified
Pass/Fail	Pass

6.2 Storage Prevent Testing

6.2.1 B01

Test Case ID	4
Unit To test	Storage monitor
Assumptions	<ol style="list-style-type: none">1. User logged to system2. User copies sensitive data to shared region3. Network scan is run
Test Data	A file Containing Credit Card List
Steps	<ol style="list-style-type: none">1. Right click on file and copy it.

	<ol style="list-style-type: none"> 2. Goto public shared directory 3. Right click and paste the file there
Expected Result	Scanner Detects the File and Warns of violation
Actual Result	File detected and violation reported
Pass/Fail	Pass

6.2.2 B02

Test Case ID	5
Unit To test	Storage prevent
Assumptions	<ol style="list-style-type: none"> 1. User logged to system 2. User copies sensitive data to shared region 3. Network scan run
Test Data	A file Containing Credit Card List
Steps	<ol style="list-style-type: none"> 1. Right click on file and copy it. 2. Goto public shared directory 3. Right click and paste the file there
Expected Result	File contents replaced by a warning message
Actual Result	File contents replaced by a message
Pass/Fail	Pass

6.2.2 B03

Test Case ID	6
Unit To test	Storage prevent
Assumptions	<ol style="list-style-type: none">1. User logged to system2. User copies sensitive image to shared region3. Network scan run
Test Data	An image containing confidential diagrams
Steps	<ol style="list-style-type: none">1. Right click on image and copy it.2. Goto public shared directory3. Right click and paste the image there
Expected Result	Image contents removed, violation detected, IT security Notified
Actual Result	Contents removed, violation detected, notified
Pass/Fail	Pass

6.3 Network Preventing Testing

6.3.1 C01:

Test Case ID	7
Unit To test	Network prevent
Assumptions	<ol style="list-style-type: none">1. User connected to network via his own machine2. User has copy of confidential data on his machine3. User tries to mail that data
Test Data	File containing NIC list
Steps	<ol style="list-style-type: none">1. Attach Confidential file to an email2. Send email through company network
Expected Result	Mail blocked and IT security notified
Actual Result	Mail blocked and IT notified
Pass/Fail	Pass

6.3.2 C02:

Test Case ID	8
Unit To test	Network Prevent
Assumptions	<ol style="list-style-type: none">1. User logged in to machine2. User has access to file containing NIC list
Test Data	.doc file containing NIC list
Steps	<ol style="list-style-type: none">1. User changed file extension from .doc to .zip2. User attaches file to an email3. User sends email outside network
Expected Result	Change in extension detected along with violation and mail blocked
Actual Result	Violations detected and mail blocked
Pass/Fail	Pass

Chapter 7: Conclusion and Future Work

7.1 Conclusion

The Project covers three main sources of data leakage using functionalities provided by Symantec solution. The projects main objective was to configure a system to prevent harmful use of confidential data. The endpoint takes care of activities at end host machine, storage prevent keeps a check on all shared files residing in system network while network prevent constantly monitors network traffic for any violations. In order to ensure uniform application of detection and response rule, we have used a central enforce platform that keeps a eye on working and performance of all these detection servers as well as provides a central access and control mechanism.

7.2 Future Enhancements

System configured in this project assumes a homogenous corporate environment where all end machines are using Microsoft OS and central server also has Microsoft server installed on it, however this is not the case for a real world scenario, real world environments can have machines running on multiple OS from different vendors like Ubuntu, Linux, Macintosh, Unix etc. So, for future enhancements we can procure and configure detection and response components for all these operating environments as well.

Appendix A: User Manual

Introduction to DLP

Data loss prevention (DLP) is a set of information security tools that is intended to stop users from sending sensitive or critical information outside of the corporate network. Idea of DLP originated due to significant insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. A user who accidentally or maliciously attempts to disclose confidential information that's been tagged will be denied. DLP might even prevent a sensitive financial spreadsheet from being emailed by one employee to another within the same corporation. DLP products generally have the following components Endpoint, Network, Storage.

Background:

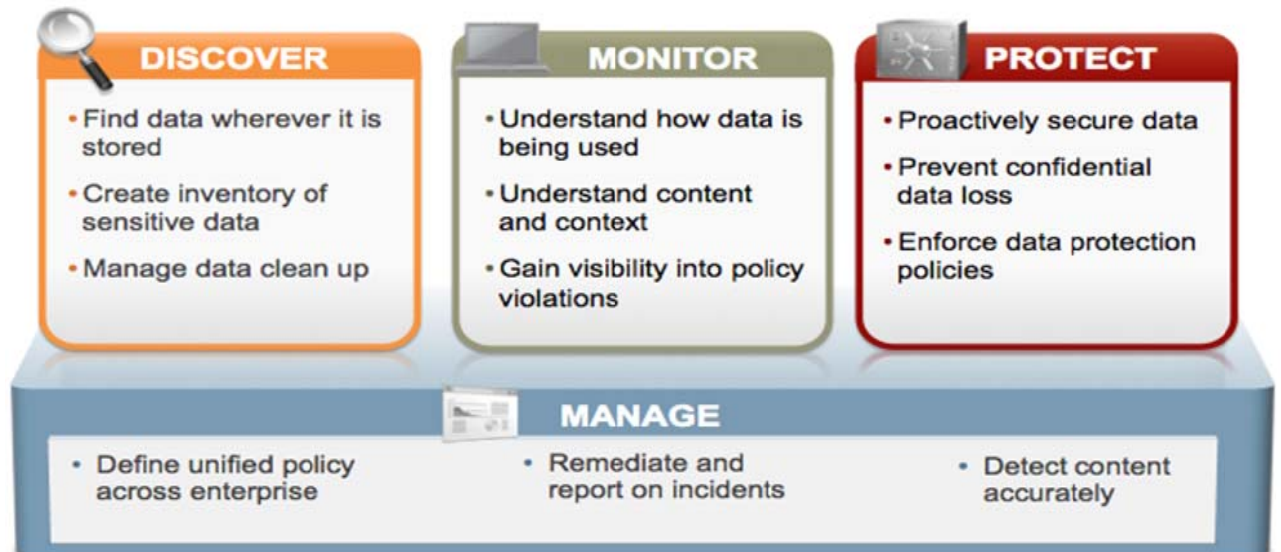
Data Loss Prevention is a comprehensive, content-aware technology that discovers, monitors, and protects confidential data wherever it is stored or used – across network, storage and endpoint systems.

Discover—Find confidential data wherever it is stored, create an inventory of sensitive data, and automatically manage data cleanup.

Monitor—Understand how confidential data is being used whether the user is on or off the corporate network, and gain enterprise visibility.

Protect— Automatically enforce security policies to proactively secure data and prevent confidential data from leaving an organization.

Manage—Define universal policies across the enterprise, remediate and report on incidents, and detect content accurately within one unified platform.



Logging on and off the Enforce Server administration console

Users who are assigned more than one role can only log on under one role at a time. They must specify the role name and user name at logon.

To log on to the Enforce Server

- 1 On the Enforce Server host, open a browser and point it to <https://localhost/>.
- 2 On the Symantec Data Loss Prevention logon screen, enter your user name in the Username field. For the administrator role, this user name is always Administrator.
- 3 In the Password field, type the password. For the Administrator at first logon, this password is the password you created during the installation.
- 4 Click logon. The Enforce Server administration console appears. The Administrator can access all parts of the administration console, but another user can see only those parts that are authorized for that particular role.

To log out of the Enforce Server

- 1 Click **logout** at the top right of the screen.
- 2 Click **OK** to confirm. Symantec Data Loss Prevention displays a message confirming the logout was successful.

Changing password

When your password expires, the system requires you to specify a new one the next time you attempt to log on. When this happens, the Password Renewal window appears.

To change your password from the **Password Renewal** window

- 1 Enter your old password in the **Old Password** field of the **Password Renewal** window.
- 2 Enter your new password in the **New Password** field of the **Password Renewal** window.
- 3 Re-enter your new password in the **Re-enter New Password** field of the **Password Renewal** window.

Adding a detection server

You add detection servers to your Symantec Data Loss Prevention system from the **System > Servers > Overview screen**. You can add the following types of servers:

- 1.1 Network Monitor Server which monitors network traffic.
- 1.2 Discover or Protect server which inspects stored data for policy violations.
- 1.3 Email Prevent server which prohibits SMTP violations.
- 1.4 Web Prevent server which prohibits ICAP proxy server violations such as FTP, HTTP, and HTTPS.

1.5 Endpoint Server which controls Symantec DLP Agents that monitor endpoint computers

To add a detection server

- 1 Go to the System Overview screen (**System > Servers > Overview**).
- 2 Click the **Add Server** button. The **Add Server** screen is displayed.
- 3 Select the kind of server you want to install and click Next. The **Configure Server** screen for that kind of detection server is displayed.
- 5 Click **Done** to return to the **System Overview** screen. Your new server is displayed in the **Servers** list with a status of **Unknown**.
- 6 Click on the server to display its **Server Detail** screen.
- 7 Click [**Recycle**] to restart the server.
- 8 Click **Done** to return to the **System Overview** screen. When the server is finished restarting its status is **Running**.
- 9 If necessary, use the **Server Settings** button on the server's **Server Detail** screen to perform advanced server configuration.

Working with saved system reports

The System Reports screen lists system and agent-related reports that have previously been saved. To display the System Reports screen, click **System > System Reports**. Use this screen to work with saved system reports.

To create a saved system report

- 1 Go to one of the following screens:
 - System Events (**System > Events**)
 - Agents Overview (**System > Agents > Overview**)
 - Agents Events (**System > Agents > Events**)
- 2 Select the filters and summaries for your custom report.
- 3 Select **Report > Save As**.

- 4 Enter the saved report information.
- 5 Click **Save**.

Setting Report Preferences

You can specify the reports that Symantec Data Loss Prevention displays in the navigation panel for each of the report types. To set reporting preferences

- 1 In the Enforce Server administration console, on the Incidents menu, click **Incident Reports**.
- 2 On the **Incident Reports** screen that appears, click Edit Preferences.
- 3 To specify a default report for the current role, locate the **Home Page** for current_role drop-down list and select a report.
- 4 To display a report in the list, check the **Show Report** box for that report. To remove a report from the list, clear **Show Report** for that report.
- 5 Click **Save**.

Configuring policies

Policies include detection rules and exceptions, and response rules. A valid policy must contain at least one detection rule. Exceptions are optional, as are response rules.

To configure a policy

- 1 The Policies screen lists all available policies and lets you configure new policies. To add a new policy, click **Add Policy**. To manage a policy, see the help topic "Managing policies."
- 2 At the **New Policy** screen that appears, select one of the following options and click **Next**:


Add a blank policy Lets you create an original policy.

Add a policy from a template Lets you base a policy on an existing template. Note that you can modify the template as needed.

3 If you selected **Add a blank policy, skip to step 5**. Otherwise, choose a template on which to base your policy and click **Next**. The **Choose a Template** screen lists all available templates with brief template descriptions.

4 The chosen template may call for an exact data index or a document index.

NOTE:If you have not created a profile, select **Do Not Use a Document Profile** or **Do Not Use Exact Data Matching**, as appropriate. **Click Next**.

5 If you use a policy template, the system displays all constituent detection rules and exceptions available to you. To save the policy as is, select a policy group from the Policy Group drop-down list and click **Save**. 

6 Review the detection methods available for use in rule conditions.

7 Review the detection methods available for rule exceptions

8 Review the available Response Rules.,

To add a response rule, select if from the drop-down list and click **Add Response Rule**.

9 When you finish adding detection rules and response rules, click **Save**.

Configuring detection conditions

The following procedure describes how to configure single and multiple detection rule conditions. To configure one or more detection rule conditions

1 In the Enforce Server administration console, go to the **Policies > Policy List > Configure Policy - Edit Rule** screen. On the **Detection** tab, click **Add Rule**. Or, if the rule is already configured, at the **Policy List** screen, click the rule or the pencil icon to edit it.

- 2 On the **Add Rule** screen, select a detection method. (For example, select **Content Matches Keyword**.) Then click **Next**.
- 3 In the **General** section, in the **Rule Name** field enter a name, or you can modify the name of an existing rule.
- 4 In the **Severity** section, select a **default** severity level.
- 5 To define a compound rule, you can add another match condition by selecting another match condition type from the **Also Match** drop-down list.
- 6 When you are done configuring your detection rule condition(s), click **OK**. You return to the **Configure Policy** screen where you can **Save** your policy

Configuring Network Prevent Server (Web)

To modify your Network Prevent Server (Web) configuration

- 1 Go to **System > Servers > Overview** and click the **Network Prevent Server (Web)**.
- 2 On the **Server Detail** screen that appears, click **Configure**. The tab is divided into several sections:

Request Filtering

Response Filtering

and Connection.

- 3 Verify or modify the filter options for requests from HTTP clients (user agents). The options in the **Request Filtering** section are as follows:

Ignore Requests Smaller Than

Ignore Requests without Attachments

Ignore Requests to Hosts or Domains

Ignore Requests from User Agents

4 Verify or modify the filter options for responses from **Web servers**.

5 Verify or modify settings for the **ICAP** connection between the **HTTP** proxy server and the Web Prevent Server.

6 Click Save to exit the **Configure Server** screen and then click **Done** to exit the Server Detail screen.

APPENDIX A: GLOSSARY

DLP	-	Data Loss Prevention
ICAP	-	Internet Content Adaptation Protocol
HTTP	-	Hyper Text Transfer Protocol
SDR	-	Software Defined Radio
PHP	-	Hypertext Preprocessor (Programming Language)
MySQL	-	My. Structured Query Language
Windows CE	-	Windows Compact Edition / Embedded Compact
SDK	-	Software Development Kit
API	-	Application Programming Interface

BIBLIOGRAPHY

1. http://en.wikipedia.org/wiki/Symantec_DLP
2. http://en.wikipedia.org/wiki/Windows_CE
3. https://en.wikipedia.org/wiki/Microsoft_Visual_Studio
4. http://en.wikipedia.org/wiki/Google_Maps#Google_Maps_API
5. <https://en.wikipedia.org/wiki/PHP>
6. <https://en.wikipedia.org/wiki/Mysql>