

Overview of Data Loss Prevention (DLP)

جلوگیری از نشت داده ها



رضا اخلاقی سنقری

شرکت مهندسی دمسان رایانه

اردیبهشت ۹۳



سازمان نظام مهندسی رایانه‌ای استان تهران

www.damsun.com | info@damsun.com

دمسان
راهکارهای فناوری اطلاعات



سازمان نظام مهندسی رایانه‌ای استان تهران

کمیسیون افتاء، کار گروه آموزش و پژوهش

سرفصل ها

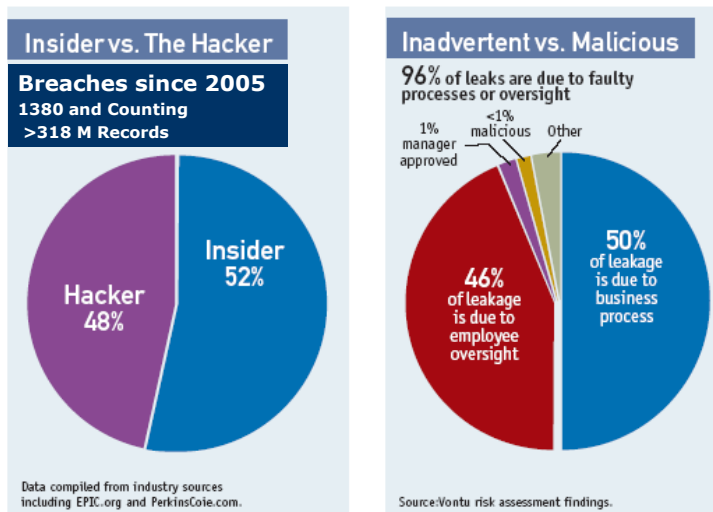
- مقدمه
- DLP چیست ؟
- ساختار DLP
- طبقه بندی و ممیزی اطلاعات
- تولید کنندگان سیستم DLP
- جمع بندی و نتیجه گیری

مقدمه

نیازمندی های سازمانی در حوزه اطلاعات

- جابجا کردن دارائی های اطلاعاتی به صورت امن
- جلوگیری از سرقت دارائی های اطلاعاتی
- حفاظت از حقوق معنوی دارائی های اطلاعاتی
- جلوگیری از حذف دارائی های اطلاعاتی به طور عمدی یا سهوی
- دریافت هشدار در مورد دسترسی غیر مجاز به اطلاعات
- نظارت به دسترسی های انجام گرفته به دارائی های اطلاعاتی
- اعمال سیاست های کنترل دسترسی به دارائی های اطلاعاتی
- امکان ممیزی محتویات بسته های ارسالی و دریافتی از شبکه
- امکان مدیریت یکپارچه و فراگیر دارائی های اطلاعاتی

تغییر رویه تهدیدات و مخاطرات امنیتی



5

انگیزه های توسعه سامانه DLP

Confidential Data Types	<div>Customer Data Social Security Numbers Credit Card Numbers Protected Health Info</div> <div>Corporate Data Financials Mergers and Acquisition Employee Data</div> <div>Intellectual Property Source Code Design Documents Pricing</div>
The Risk	<div>1:400 messages contains confidential data</div> <div>1:50 network files is wrongly exposed</div> <div>4:5 companies lost data on laptops</div> <div>1:2 companies lost data on USB drives</div>

سیستم DLP چیست ؟

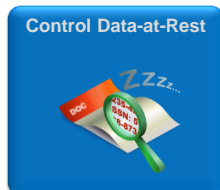
عبارت **DLP** در فرهنگ واژگان فنی دارای مفاهیم و معانی زیر می باشد.

- سامانه جلوگیری از دسترسی غیر مجاز به اطلاعات
- سامانه تشخیص و جلوگیری از دست یابی غیر مجاز به اطلاعات
- Information Leak Prevention (**ILP**)
- Information Leak Detection and Prevention (**ILDP**)
- **DLP**
 - Data Leak Prevention
 - Data Loss Prevention

سامانه DLP چیست ؟

- **DLP** راه کاری است برای تامین امنیت اطلاعات با هدف جلوگیری از رخنه در جریان اطلاعاتی سازمان در داده های:

- در حال استفاده کاربران
- در حال عبور از شبکه
- ذخیره شده



تأثيرات استفاده از DLP

➤ نتایج کلی راه کار DLP

- تحقق مقررات و استاندارد حکومتی (HIPAA, SOX, GLBA)
- حفاظت از دارائی های اطلاعاتی حساس سازمان (Docs- Plans, ...)
- حفاظت از حقوق معنوی اطلاعات سازمان

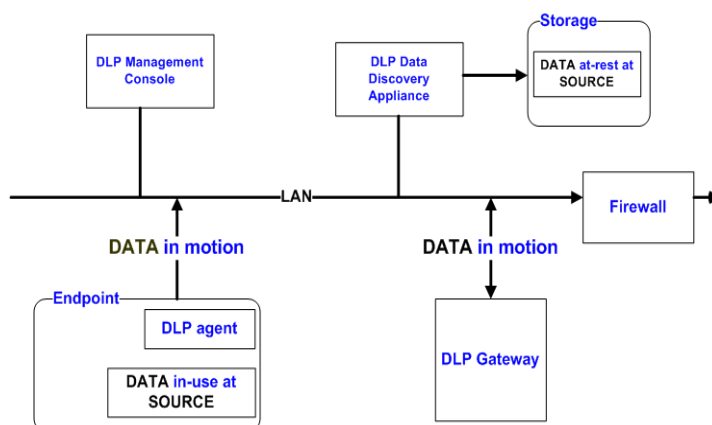
➤ تهدیدات و مخاطراتی که به وسیله راه کار DLP مرتفع می گردد

- از بین رفتن اطلاعات حساس سازمان به دلیل بی دقتی پرسنل
- جلوگیری از سرقت اطلاعات به دلیل عدم مهارت کافی پرسنل سازمان
- جلوگیری از سرقت برنامه ریزی شده توسط افراد خبره سازمان
- جلوگیری از سرقت اطلاعات از پیش برنامه ریزی شده توسط بد افزارها و هکرها

ساختار DLP

- معماری سیستم DLP

- DLP Management Console
- DLP Endpoint Agent
- DLP Network Gateway
- Data Discovery Agent (or Appliance)



ساختر DLP

: Data Discovery

فرآیند راه دور نرم افزاری است که با پایش منابع اطلاعاتی شامل File sharing servers, DB Servers, ایمیل سرورها و رایانه های شخصی، به کشف و طبقه بندی اطلاعات مهم روی آن سیستم ها می پردازد.

: Data Protection

فرآیند حفاظت از داده های حساس سازمان بر اساس سیاست ها و قوانیت کنترل دسترسی تبیین شده ای شامل Block, Log, Quarantine, Encryption, audit, notification ... است.

ساختر DLP

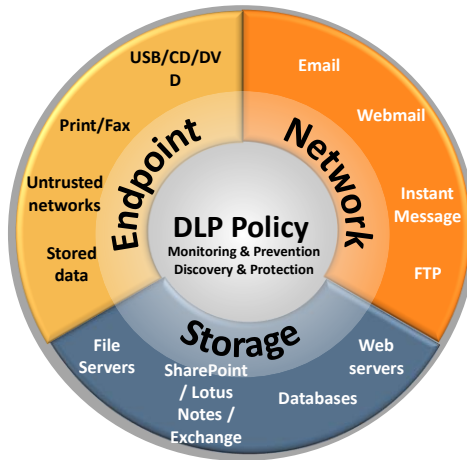
:Data Monitor

عبارت است از نظارت و تعیین دارائی های اطلاعاتی در معرض خطر، تعیین در لحظه افراد در حال استفاده از منابع اطلاعاتی و اینکه اطلاعات به کجا منتقل می شوند.

:Data Endpoint

فرآیند اعمال و نظارت بر سیاست های تعیین شده امنیتی مبتنی بر گروه های کاری است.

ساختر DLP



ساختر DLP

➤ The data in use at endpoints can be leaked via (Data-in-use)

- USB
- Emails , Web mails
- HTTP/HTTPS, FTP
- IM

➤ The data in motion can be leaked via (Data-in Motion)

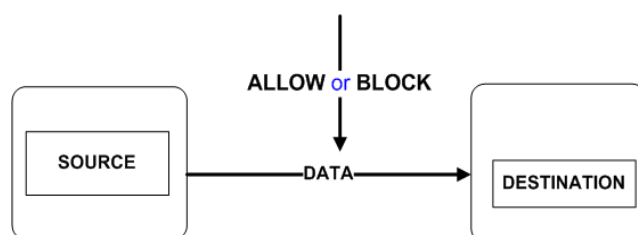
- SMTP
- FTP- HTTP/HTTPS
- Other Network Protocols

The data at rest could be Leaked Via (Data-at-Reset)

- reside at wrong place
- Be accessed by wrong person
- Be owned by wrong person

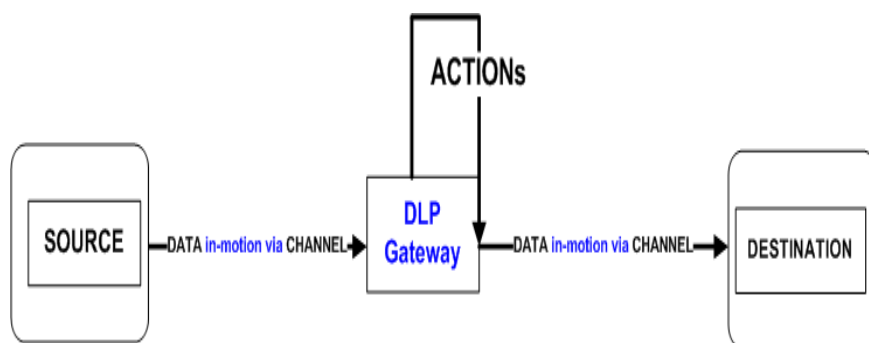
ساختر DLP

- نگاه مفهومی به موقعیت اطلاعات در حال استفاده کاربر نهایی (data-in-use)

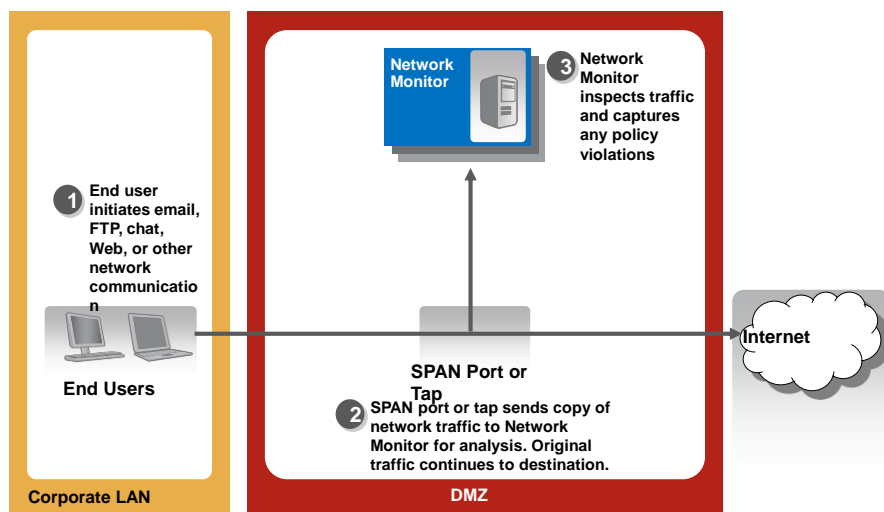


ساختر DLP

- نگاه فنی به جریان اطلاعات در سطح زیرساخت شبکه (data-in-Motion)

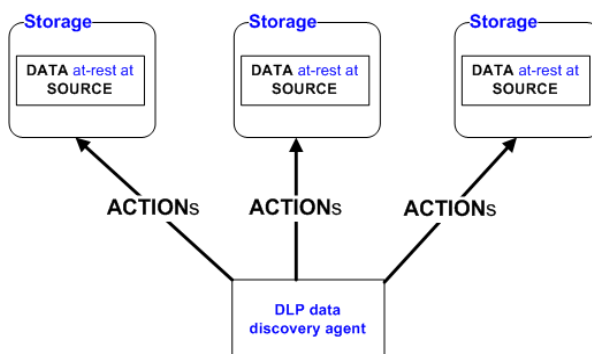


ساختر DLP



ساختر DLP

نگاه مفهومی به اطلاعات در موقعیت (Data-at-Rest)



طبقه بندی و تشخیص اطلاعات در سیستم DLP

- سیستم DLP می بایست پاسخگوی پرسش های زیر باشد:

- چه اطلاعاتی مهم تلقی می شود ؟
- چگونه اطلاعات مهم را می توان مشخص کرد ؟
- چگونه اطلاعات مهم را طبقه بندی کنیم ؟
- چگونه می توان عبارت و اطلاعات مهم را در فایل تشخیص داد ؟
- چگونه می توان اطلاعات با ارزش را وزن گذاری نمود ؟

- امکان تشخیص محتویات اطلاعات از قابلیت های سیستم DLP برای رفع نیاز های زیر می باشد.

- To define sensitive data, i.e., data classification
- To identify sensitive data in real time

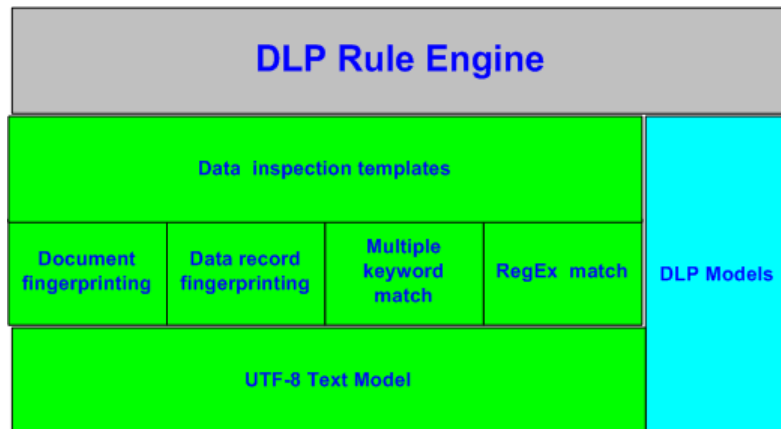
طبقه بندی و تشخیص اطلاعات در سیستم DLP

روشهای تشخیص اطلاعات به چهار روش کلی تقسیم می شوند

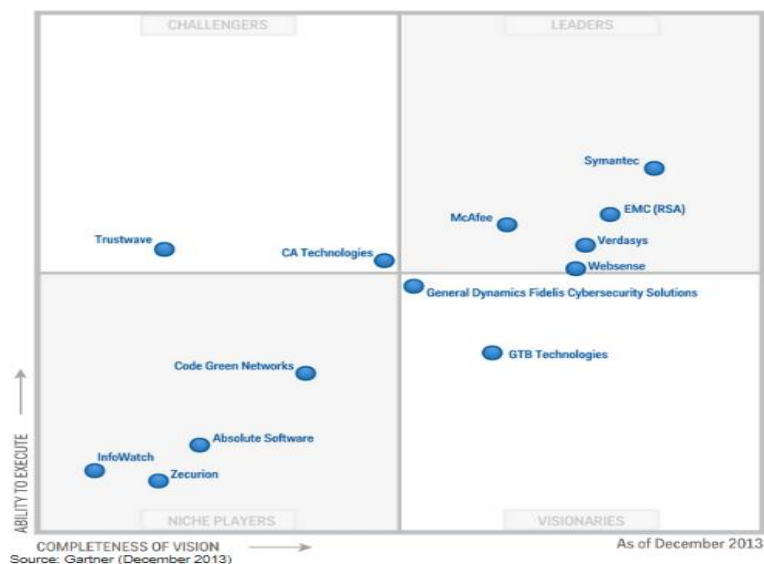
- Regular expression matching
- Multiple Keyword matching
- Document fingerprinting
- Database record fingerprinting

Data inspection templates			
Document fingerprinting	Data record fingerprinting	Multiple keyword match	Regex match
UTF-8 Text Model			

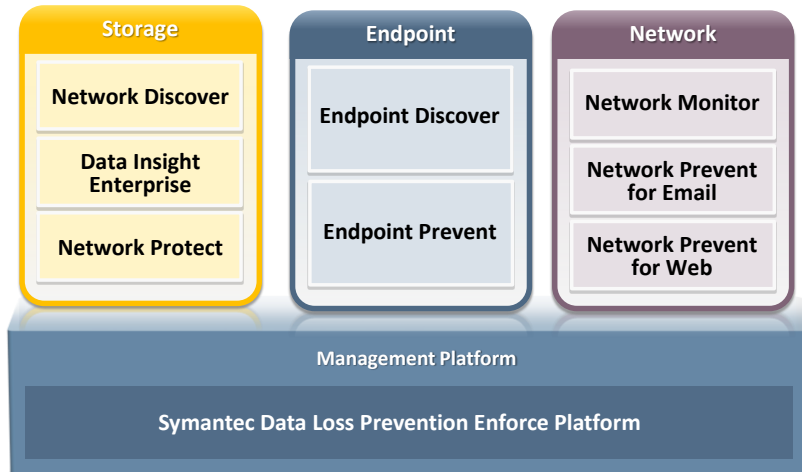
طبقه بندی و تشخیص اطلاعات در سیستم DLP



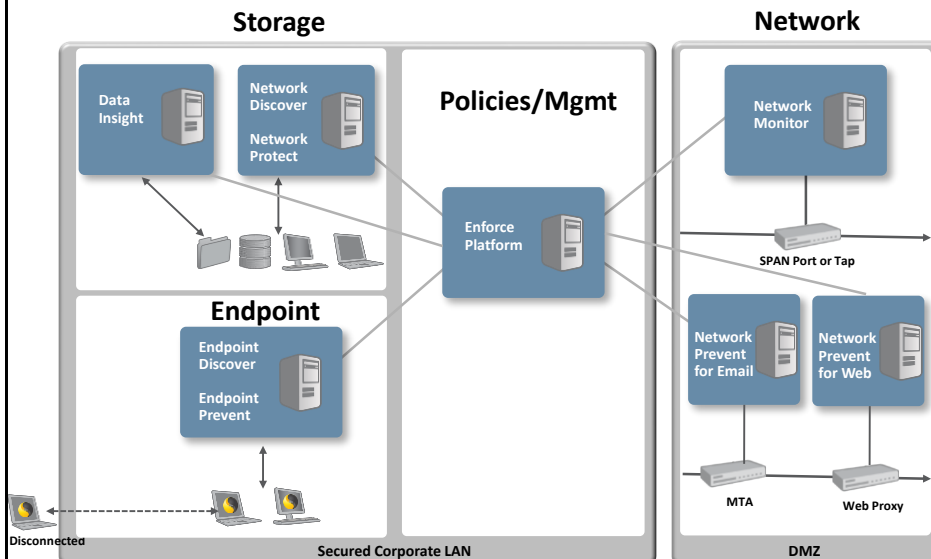
تولید کنندگان مطرح راه کار DLP



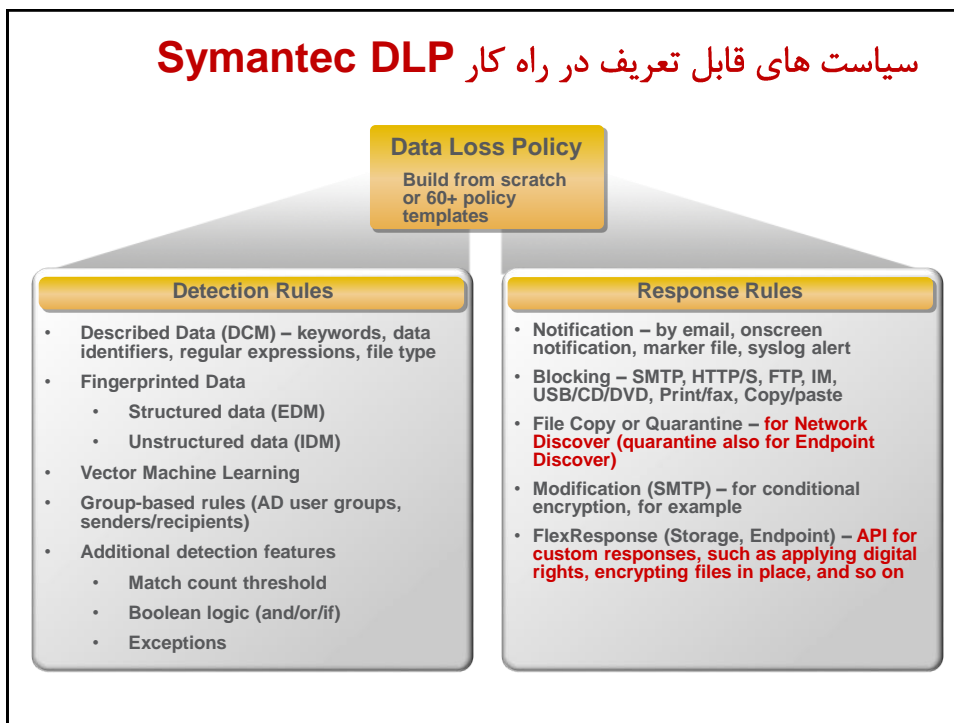
راه کار DLP شرکت Symantec



معماری راه کار Symantec DLP



سیاست های قابل تعریف در راه کار Symantec DLP



سیاست های سیستم DLP

- **Policies are the heart of Symantec DLP**
 - Main policy components: Detection, Groups, Response
 - Define how/what data detect
 - Define how to respond upon detection

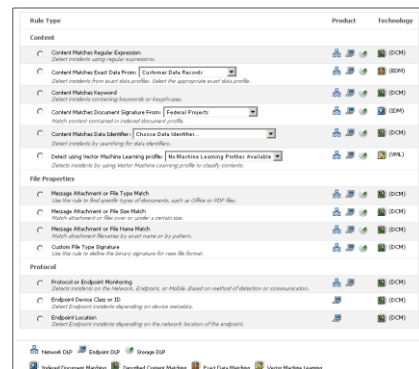
The screenshot shows the Symantec Data Loss Prevention console. The "Policies" tab is selected, displaying a list of policies. The table below represents the data shown in the screenshot.

Name	Description	Policy Group	Last Modified		
Competitor Communications	This policy detects communications with competitors.	Confidential Data Protection	March 10, 2011 6:19:17 AM PST	✎	✕
Confidential Documents	This policy detects company-confidential documents at risk of exposure.	Confidential Data Protection	March 10, 2011 6:19:53 AM PST	✎	✕
Customer Data (DCM)	This policy detects customer data at risk of exposure.	Customer Data Protection	March 22, 2011 3:06:49 PM PDT	✎	✕
Customer Data (EDM)	Protect customer data with Exact Data Matching	General Policy Group	February 23, 2011 10:30:25 AM PST	✎	✕
Custom File Type Detection	Custom File Type Detection using Filetype Analyzer	Intellectual Property Policies	February 2, 2011 3:56:14 PM PST	✎	✕
Design Documents	This policy detects various types of design documents such as CAD/CAM at risk of exposure.	Confidential Data Protection	February 2, 2011 8:19:04 AM PST	✎	✕
Employee Data (EDM)	Protect Employee EDM Data	Employee Data Protection	February 23, 2011 9:29:39 AM PST	✎	✕
Encrypted Data	This policy detects the use of encryption by a variety of methods including 5/ MIME, PGP, GPG, and file password protection.	Confidential Data Protection	January 11, 2011 1:38:21 PM PST	✎	✕
HIPAA (including PHI)	This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by detecting sensitive data, controlling its distribution, and...	Regulatory Enforcement	January 11, 2011 1:38:44 PM PST	✎	✕

مکانیزم های تشخیص

➤ Three main detection methods

- Described Content Matching (DCM)
- Fingerprinting
 - Exact Data Matching (EDM)
 - Indexed Document Matching (IDM)
- Vector Machine Learning (VML)



مکانیزم تشخیص بر اساس محتوی

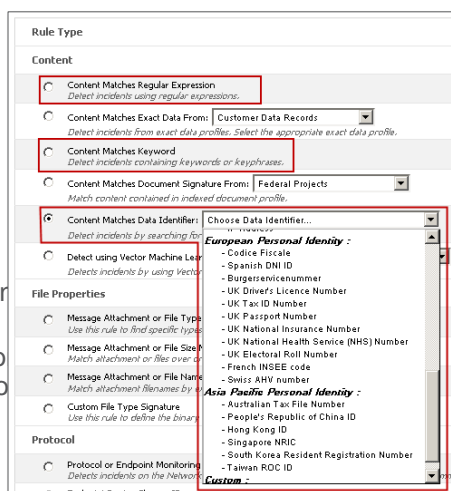
➤ Simplest form of detection

➤ Data is described, using:

- Keywords
- RegEx
- Data Identifiers

➤ Data Identifiers

- Built-in intelligence using pattern based detection
- Performs algorithmic formulas on data to ensure legitimate data lo



مکانیزم تشخیص بر اساس یکپارچگی اطلاعات

➤ Exact Data Matching (EDM)

- Designed for **structured data** (e.g., databases)
- Extremely accurate due to exact data matching
- Matches based on **data row** (e.g. First Name, Last Name, CCN)
- Data is securely indexed using **hashes** of the data
- Index can be updated automatically

➤ Index Document Matching (IDM)

- Designed for **unstructured data**
 - Confidential Legal or Financial Documents
 - Design documents
 - Pictures or Videos
- IDM creates **overlapping hashes** of files
- Detects **whole or partial file** content (for text-based files)

Script مکانیزم تشخیص بر اساس امکانات

- Designed for **unstructured data**
- **DLP “learns”** what to protect based on positive and negative sets of data
- VML detection executes on **endpoint** as well as server

Use Case: Customer wants to protect source code, but does not want to use IDM. Positive sets could be files containing proprietary/IP source code, while negative sets could be an open source project downloaded from the Internet.

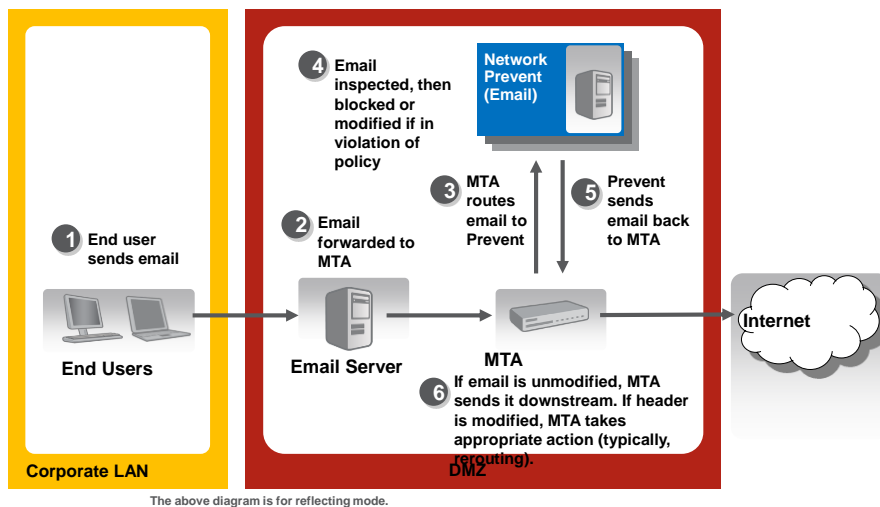
راه کار Symantec DLP در لایه Data-in-Motion

- **Inspects all network traffic** for confidential data
- **Prevent confidential SMTP, HTTP/S, FTP, and IM traffic** from leaving
- Resides at **network egress** points in the DMZ
- **Network DLP products**
 - **Network Monitor**
 - **Network Prevent for Email**
 - **Network Prevent for Web**

راه کار Symantec DLP برای ایمیل

- **Monitors and prevents confidential email from leaving organization**
- **Can take different actions on violating email**
 - Record incident, let email go
 - Record incident, notify user (via email), let email go
 - Enforce encryption (add SMTP header marking email for encryption gateway, such as Symantec Encryption Server)
 - Quarantine email (add SMTP header marking email for quarantine destination, such as Symantec Messaging Gateway) and notify user
 - Block email and notify user

Network DLP – Network Prevent for Email



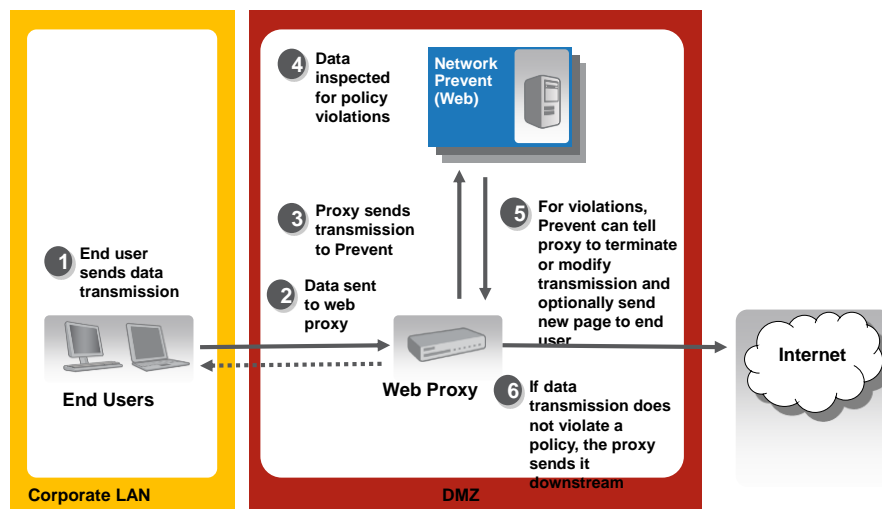
راه کار Symantec DLP برای ترافیک اینترنت

- Network Prevent for Web integrates with ICAP-compliant proxies to provide HTTP, HTTPS, and FTP protection
 - Symantec Web Gateway, Blue Coat, IronPort, MS ISA, Squid

		SYMC Web Gateway	Blue Coat	McAfee (Webwasher)	Cisco IronPort S-Series	Microsoft ISA	Squid
Monitor & Block Web Requests	HTTP	Y	Y	Y	Y	Y	Y
	HTTPS	Y	Y	Y	Y	n	n
Monitor & Block Web Responses	HTTP	n	Y	Y	n	Y	n
	HTTPS	n	Y	Y	n	n	n
Remove Web Content	HTTP	Y	Y	Y	n	Y	Y
	HTTPS	Y	Y	Y	n	n	n
Monitor & Block FTP		n	Y	Y	Y	Tunneled Only*	n

*Covers GET requests only (for FTP on Microsoft ISA).

Network DLP – Network Prevent for Web

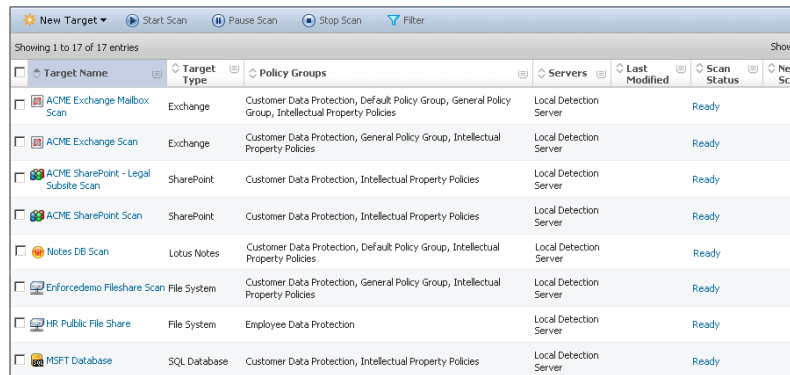


راه کار Symantec DLP در بخش Data-at-Rest

- Network Discover
- Network Protect
- Data Insight

Storage DLP: Network Discover

- Identifies confidential data exposed on file servers, NAS filers, databases, collaboration platforms, intranet sites, email servers, etc.

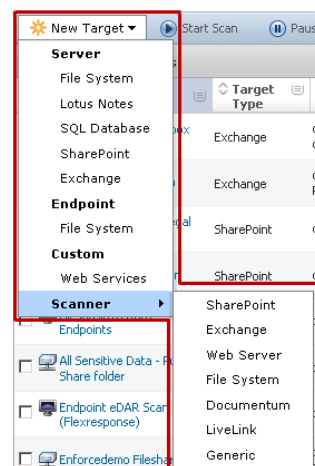


The screenshot shows the 'New Target' window with a table of discovered targets. The table has columns for Target Name, Target Type, Policy Groups, Servers, Last Modified, Scan Status, and Net Sc.

Target Name	Target Type	Policy Groups	Servers	Last Modified	Scan Status	Net Sc
ACME Exchange Mailbox Scan	Exchange	Customer Data Protection, Default Policy Group, General Policy Group, Intellectual Property Policies	Local Detection Server		Ready	
ACME Exchange Scan	Exchange	Customer Data Protection, General Policy Group, Intellectual Property Policies	Local Detection Server		Ready	
ACME SharePoint - Legal Subsite Scan	SharePoint	Customer Data Protection, Intellectual Property Policies	Local Detection Server		Ready	
ACME SharePoint Scan	SharePoint	Customer Data Protection, Intellectual Property Policies	Local Detection Server		Ready	
Notes DB Scan	Lotus Notes	Customer Data Protection, Default Policy Group, Intellectual Property Policies	Local Detection Server		Ready	
Enforcedemo Fileshare Scan	File System	Customer Data Protection, General Policy Group, Intellectual Property Policies	Local Detection Server		Ready	
HR Public File Share	File System	Employee Data Protection	Local Detection Server		Ready	
MSPT Database	SQL Database	Customer Data Protection, Intellectual Property Policies	Local Detection Server		Ready	

Storage DLP: Network Discover, cont'd

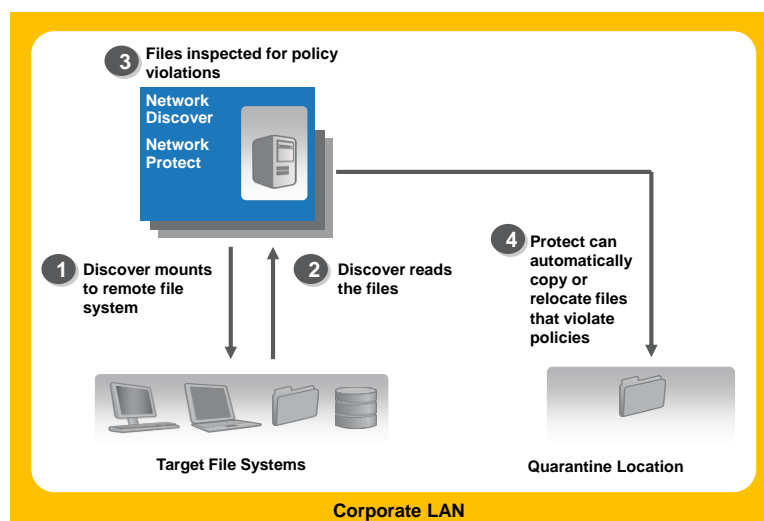
- What targets can it scan?
- Server & Endpoint targets natively supported
- Custom Web Services – Discover will act as a web service and accept content
- Scanners require agent on the target
 - Note:** Scanners are being phased out as native scanning is augmented



Storage DLP: Network Protect

- **Automatically protects files found during a Network Discover scan**
- **Uses DLP Policies to enforce response actions,** which include:
 - **Copy:** Copy a file and save it in another location.
 - **Quarantine:** Move the file to another, more secure location. Optionally, leave a “marker file” in the original location.
 - **Execute FlexResponse:** Call another product to execute an action (e.g., call PGP Netshare to encrypt a file)

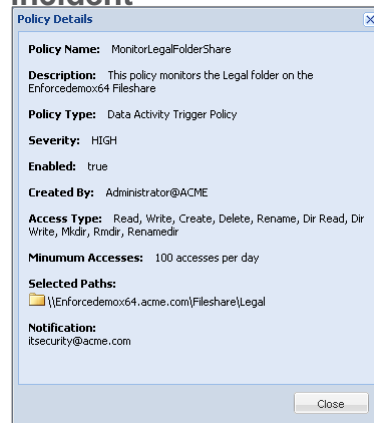
Architecture: Network Discover & Protect



The above diagram is for the agent-less deployment option.

Storage DLP: Data Insight

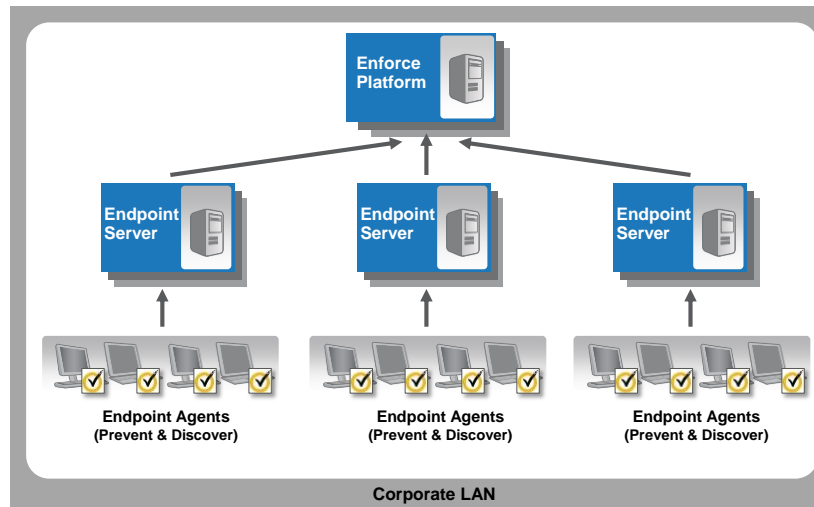
- Provides additional file access and usage details, which can be added to the DLP incident
- How does it work?
 - Monitors files & folders based on policy
 - Stores and displays access/usage details, which can be leveraged by Symantec storage and security products



راه کار Symantec DLP برای Data-in-use

- Endpoint DLP gives data security teams the insight and control they need to secure confidential data at the endpoint, whether for laptops, desktops, or Windows servers.
- Endpoint DLP products
 - Endpoint Discover
 - Endpoint Prevent

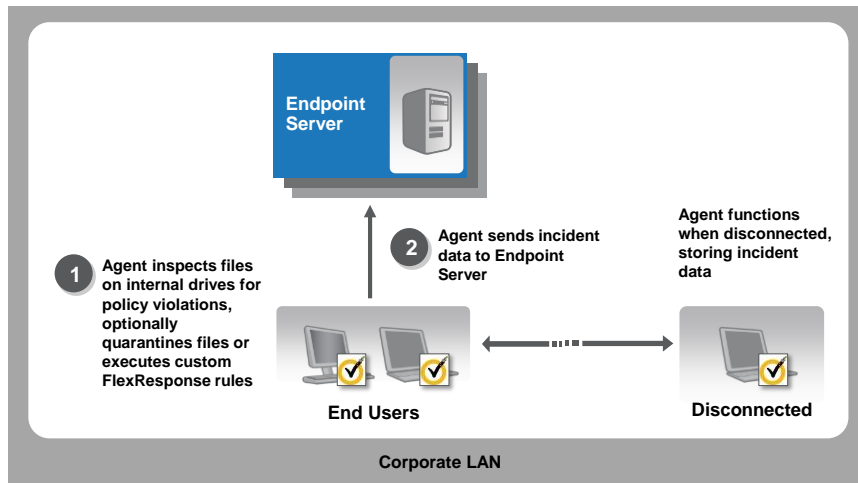
Symantec DLP for Endpoint معمار کلی راه کار



Endpoint DLP: Endpoint Discover

- Similar to Network Discover, Endpoint Discover **scans the internal hard drives of an endpoint identifying confidential data** so steps can be taken to inventory, secure, or relocate the data.
- It enables high-performance, parallel scanning of thousands of endpoints with minimal system impact.

Endpoint Discover

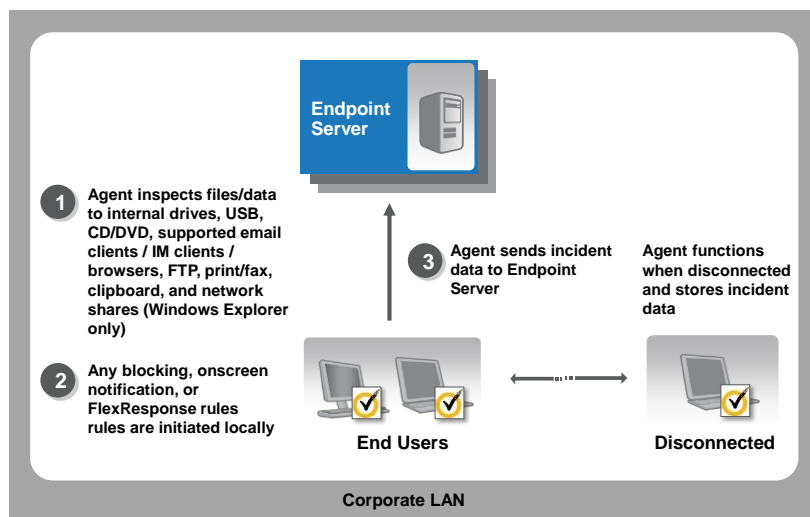


The above diagram assumes DCM and User Group detection methods only. Otherwise, inspection occurs at the server.

Endpoint DLP: Endpoint Prevent

- Endpoint Prevent monitors all information leaving the end-user machine whether on or off the corporate network.
- What does it monitor?
 - **Removable Storage** – USB, Firewire, SCSI, SD/CF Cards, PCMCIA storage, Floppies, eSATA, etc.
 - **Internal/Local Drives** – Monitors data as it is stored locally
 - **CD/DVD**
 - **Print/Fax**
 - **Copy/Paste** – Clipboard events
 - **Email**
 - **Web** – HTTP & HTTPS
 - **IM** – MSN, Yahoo & AOL
 - **FTP**
 - **Network Shares**
 - **Application File Access Control** – Configurable to monitor desired applications.

Endpoint Prevent



جمع بندی و نتیجه گیری

- سامانه DLP راه کار متوازن تامین کننده امنیت و دسترس پذیری به اطلاعات می باشد.
- سامانه DLP راه کار تامین کننده دست یابی و جابجا کردن اطلاعات به صورت امن می باشد.
- سامانه های DLP امکان ارائه خدمات امنیتی مبتنی بر مدل CIA را دارند.
- سامانه DLP به عنوان یکی از اهرم های زیر ساخت های SOC می تواند مطرح باشد.
- سامانه DLP به دلیل یکپارچه شدن با Active directory امکان اعمال سیاست های مد نظر بر اساس گروه های کاری و دیگر تقسیم بندی های قابل اجرا در محیط windows را دارد.
- سامانه DLP راه کار End-to-End و مکمل به منظور حفاظت از دارائی ها اطلاعاتی می باشد.



با تشکر از توجه و حوصله شما



سازمان نظام‌مندی رایانه‌ای استان تهران

کمیسیون افتا، کار گروه آموزش و پژوهش