BAROO DLP

Data Leakage Prevention

Information is seen as one of the most precious commodity of the vast majority of companies. Protecting critical information is so essential in sphere of commercial, military, social and national security. Fulfilling such achievement requires the use of suitable and efficient solutions that are in accordance with advanced guidelines, tools, and systems. These solutions are taken into account as comprehensive and complicated operating frameworks, should be comprised of a set of efficient solutions to handle a variety of leakage, manipulation, and loss of sensitive information.

The protected data can be categorized as:

- Data-in-use: It is defined as the data to be processed or applied while conducting the specific activities of the users or applications on the endpoints. These specific activities are comprised of copying files to removable devices, printing text files and images through the local printer, and taking screenshots. Protecting such data set, a lot of activities on the endpoints must be monitored, and if the specific activities are spotted, the data is analyzed at the same time and suitable action will be carried out.

- Data-in-motion: Live network traffic data. In this case, safeguarding such data, network traffic is required to be analyzed, categorized, and stored (briefly or in detail) aimed at preventing unauthorized traffic passing following predefined policies.

- Data-at-rest: It is inclined for resided data in databases, shared files, and information repositories. This data is supposed to be scanned, extracted for the objective of tracking and conducting remedial actions, such as changing access permissions and encryption. The tasks creates a process that is relevant to resided data and is called as the data discovery process.

Baroo DLP endpoint agents are accountable for enforcing data leakage policies on terminal systems. Fulfilling the responsibility requires following activities:

- Scanning data resided in the endpoint system and spotting sensitive data,
- Observing effective events on the data in the endpoint system,
- Live event analysis and detection of policy violations,
- Compensating and remediating for sensitive data discovered or for activities that violate policies,
- Control and restrict endpoint platform services in accordance with policies (such as restricting the ability to connect removable devices or the ability to store data on them).

Baroo DLP is comprised of agents that are installed on client/server end-points and a management server which enables the administrator to enforce policies, monitor clients, view agents' logs and other management activities.

The following is the feature list of Baroo DLP:

	FEATURE	**DESCRIPTION**
OVERVIEW	Windows Agent	Windows 7, 8 and 10
	AD Integration	Active Directory Integration
	Discovery	Discovering sensitive data in storages and databases
	Data Protection	Various capabilities for protection sensitive data
	Device Control	Control devices including printers
	Application Control	Control applications and their access to sensitive data
	Encryption	Disk and file encryption
	Monitoring	Monitoring various activities on agents including network activities even in SSL/TLS traffic
	Central Management	Central console management with web interface
STORAGE SCAN AND PROTECTION	Storage Scan	Endpoint files and mass storage scan for discovery. Endpoint discovery scans to locate local file system or share storage files with sensitive content.
	Databases Scan	DB agent discovery scans to locate local data records with sensitive content.

	File and Data Remediation	Remediate and restricts access for sensitive content.
	File Encryption	Ability to encrypt files on removable devices, hot directories and found sensitive contents.
	Disk Encryption	Ability to encrypt system and removable drives even windows drive (drive c:\)
	Quarantine Files	Ability to Quarantine sensitive files.
CONTENT AWARENESS	Exact Document Matching	Get file and calculate hash of files and correspond everywhere this hash be found.
	File Metadata Matching	The ability to match on file metadata.
	Keyword Matching	The ability to match content of file with keywords and data dictionary.
	Regular Expression Matching	The ability to match content of file with regular expressions.
	File Format and MIME type Matching	Get format of file and corresponding with mime types.
	Compressed File Extraction	The ability to extract and scan compressed files contents.
	Office and PDF Documents Scan	The ability to extract and scan data from office documents and PDFs.
MONITOR AND CONTROL	Device Control	Monitor and restrict user access to devices.
	Application Control	Monitor and restrict applications access.
	File Access Control	Monitor and restrict users' and applications' access to files.
	Removable Media Encryption	Encrypts removable mass storage data elements.
	Clipboard Control (Copy/Paste)	Monitor and restrict users' and applications' access to the clipboard.
	Restrict Screen Capture	Monitors and restricts users and applications access to capturing the screen as a picture or video.
	Keyboard Monitoring	Monitor keyboard stream, normalize stream per context.
	Network Traffic Monitoring	Monitor and restrict network traffics.

	Monitor Email Traffic	Monitor and restrict incoming and outgoing emails, scan email subjects, body and attachments, for POP3(s) IMAP(s) SMTP(s) protocols. This feature works even for SSL traffic.
	Monitor Web Traffic	Monitor and restrict web access, even SSL traffic.
	Firewall	Monitor and restrict network connections.
	Access Control List (ACL) / Hot Directory	The ability to define a hot directory and get access on it just for authorized processes.
	Desktop Monitoring	The ability to capturing and sending stream of desktop to DLP server.
	Printer Control	Monitor and restrict access for printing sensitive data.
	Application, DLL, Driver Whitelist	Define authorized executable applications, DLLs and drivers and prevents other Applications, DLLs and drivers to start.
CENTRAL MANAGEMENT CONSOLE	Policy Manager	Centralized console for policy enforcement plus the ability to import/export policies and configuration.
	Dashboard	Ability to create custom dashboard
	Task manager	Support whitelist scenarios (clean systems, update …), Support discovery scenarios and monitor and manage tasks status.
	User access control	The ability to restrict user access to tools and configurations.
	Report manager	Log collection and search all report type that sent from different agents.
	Pre-built and custom-built templates	Policy, pattern, dictionary, URL and other templates to help meet and create policies needs of different areas on organization.
OTHER	Self-Protection	DLP protect its files, processes, registry and drivers from falling and always staying up.
	Task Scheduling	Task Scheduler is a component that provides the ability to schedule the launch of scans or running scripts at pre-defined times or after specified time.
	File Format Change Protection	Prevent sensitive data file format change.
	Packet Capturing	The ability to capture and archive of specific connection packets in pcap format.
	Push install	The ability to install agents on a managed network.

Baroo DLP with its comprehensive features is available to help enterprises to protect their sensitive data. It can also be joined with Baroo Data Diode to even better protect data leakage in isolated networks and advanced scenarios.