Feature	Symantec DLP	Forcepoint DLP	McAfee DLP	Grayteq DLP
Known issues, Vulnerabilities and additional costs				
Administrator login failures	DLP Admin login information is stored in the Oracle database. In case of loss of the connection to the database, Admins cannot log into DLP system.	DLP admin login information is stored in SQL database, so in case of loss of connection with the SQL Server, Forcepoint DLP becomes unmanageable.	Similar to Forcepoint DLP, McAfee DLP Admin login information is stored in the SQL database, so by detaching SQL from the DLP, it is easy to make the whole McAfee DLP system unavailable and unmanageable.	DLP Admin login information is stored in Security Server, so in case of failure of a 3rd party database (if in use), DLP Admins still can login into and manage Grayteq DLP system.
Case-sensitivity problems	Symantec DLP's content scanner produces the utmost amount of case-sensitivity failures in comparison to the other two content aware DLPs named in this comparison	Content scanner and OCR (Optical Character Recognition) occasionally fails to distinguish between capital and non-capital English characters.	McAfee DLP has the silver medal in making mis-recognition of word with mixed letters of capital and non-capital.	Grayteq DLP is content-independent, so it does not matter which letter capitalization is in use.
International character sets and dictionaries	Content scanner and OCR fails to identify Non-English dictionaries and character sets	Content scanner and OCR fails to identify Non-English dictionaries and character sets	Content scanner and OCR fails to identify Non-English dictionaries and character sets	Grayteq DLP is content-independent, so it does not matter which dictionaries, character sets or languages are being used in documents.
USB monitoring problems	No data available	No monitoring and logging for USB devices that are not members of the protected USB device group. (Eg. When a group of USB devices is set for being monitored/alerted, all actions on USB devices outside of this group are not being and cannot be monitored.)	No data available	Grayteq DLP logs all USB interactions, no matter whether they are approved or denied, so if a USB device is member of a protected USB device group, all other USB devices are being monitored, logged and alerted as well.
Location-dependent security policies	There is no option for applying different security policies at different networks and physical locations in Symantec DLP. All policies are being applied at all locations. No difference for laptops and mobile devices when in the corporate's protected network, when out of it and when on VPN.	There is limited option for applying different security policies at different network states (connected and disconnected states only) in Forcepoint DLP. No differentiation capabilities for laptops and mobile devices when in the corporate's protected network or and when on VPN. Switch between Connected and Disconnected policies is not automatic and must be initiated by the user.	There is no option for applying different security policies at different networks and physical locations in McAfee DLP. All policies are being applied at all locations. No difference for laptops and mobile devices when in the corporate's protected network, when out of it and when on VPN.	Grayteq DLP is capable of applying different policies for different networks, subsystems and physical locations. There are different security policy sets available for Connected, Disconnected and On-VPN states of the client device and is is possible to create unique security policy set for unlimited number of physical locations and networks. Switching between locations is fully automated.
Policy limitation	No data available	Limited amount of policies. Forcepoint DLP allows you to create 35 pieces of security policies as per default only.	No data available	Grayteq DLP allows you to create unlimited number of policies in unlimited combinations.
Decision-making failures	Decision-making occurs in the Enforce Server meaning that in case of server failure or overload, the whole Symantec DLP system might become unresponsive.	Decision making slowdown: Security decision are made in Primary and Secondary Triton Server. In case of these servers become unavailable or overloaded, decision-making slows down or does not happen, so the whole system goes down.	Decision-making occurs in the DLP Prevent Server meaning that in case of server failure or overload, the whole McAfee DLP system might become unresponsive.	Decision-making occurs on the clients, where the specific action happens, so in case of failure of Grayteq Security Server, the whole system remains up and running, the client continue logging into their local log database and decision-making remains local and active.

DLP Comparison Chart

Feature	Symantec DLP	Forcepoint DLP	McAfee DLP	Grayteq DLP
Known issues, Vulnerabilities and additional costs				
High additional costs - Software	For Symantec DLP, it is necessary to purchase Oracle 11G licenses for all client devices that are made involved with Symantec DLP. Oracle 11G license prices are added to Symantec DLP license prices and to be purchased separately.	For Forcepoint DLP, Microsoft SQL 2012 licenses are to be purchased separately for all client devices that are connected to Forcepoint Triton Servers. Free SQL licenses (up to 10GB storage capacity), MySQL, PostgreSQL licenses do no work with Forcepoint DLP.	For McAfee DLP, Microsoft SQL 2012 licenses are to be purchased separately for all client devices that are connected to McAfee Discovery Server. Free SQL licenses (up to 10GB storage capacity), MySQL, PostgreSQL licenses do no work with McAfee DLP.	Grayteq DLP does not require any 3rd party database licenses. As per default, Grayteq DLP uses its own, embedded database system, while supports all external 3rd party databases like MS SQL, PostgreSQL, Oracle and Syslog systems.
High additional costs - Hardware	For reviewing additional, mandatory hardware requirements for Symantec DLP please, consult with Infrastructure, DB & VDI Support page of this file. That page shows all hardwares to purchase for making Symantec DLP work.	For reviewing additional, mandatory hardware requirements for Forcepoint DLP please, consult with Infrastructure, DB & VDI Support page of this file. That page shows all hardwares to purchase for making Forcepoint DLP work.	For reviewing additional, mandatory hardware requirements for McAfee DLP please, consult with Infrastructure, DB & VDI Support page of this file. That page shows all hardwares to purchase for making McAfee DLP work.	For reviewing additional, mandatory hardware requirements for Grayteq DLP please, consult with Infrastructure, DB & VDI Support page of this file. That page shows the one and only hardware that is required for making Grayteq DLP work.