SEQRITE
Enterprise Security Solutions by Quick Heal

Seqrite
Data Loss Prevention (DLP)

Get complete control over the data that belongs to you

www.seqrite.com

Overview

An increasing volume of business information assets are distributed digitally today. Organizations simultaneously have to accelerate business processes. Combined with BYOD policies and cloud-based storage services, the ever-growing risk of data leakage has pervaded IT policy makers and CSO's of enterprises of all sizes.

Seqrite DLP enables enterprises to combat data leakage threats by regulating data transfer channels such as removable drives, network shares, web-based apps & online services, print screen and the system clipboard. DLP also provides the ability to monitor sensitive data based on its nature and type. With this protocol, enterprises can monitor Office files, graphic files, programming files, confidential data, and implement customized user-defined dictionaries for data monitoring.

How to install Seqrite DLP on your endpoints

The Seqrite Data Loss Prevention (DLP) feature is available only as an add-on pack within the Seqrite Endpoint Security ecosystem.

» **For Seqrite Endpoint Security Business Edition users**

To acquire DLP, Business Edition will also need to acquire the Compliance feature pack.

» **For Endpoint Security Total Edition users**

Users of Endpoint Security Total Edition can acquire the DLP pack right away, as the features within Compliance pack are already included within the product by default.

NOTE - Learn more about Endpoint Security Total Edition and Endpoint Security Business Edition here.

Features of Seqrite DLP

Data Protection Within The Enterprise

With Seqrite DLP, enterprises can now accurately monitor data events in real-time and enforce security policies that are managed centrally. This helps enterprises to overlook the methods in which employee's access and transfer crucial information. Moreover, enterprises can achieve this without disrupting employee productivity. DLP allows companies to counter data threats that originate from inside sources such as outgoing emails, Instant Messengers, web-based applications and USB drives. Additionally, enterprises can also block data leakage propagated by worms, Trojans and other threats.

- DLP blocks all channels through which potential data loss can take place. These include, but are not restricted to, removable drives, network sharing, screen capture, clipboard, web-based apps, cloud storage services and email attachments.
- DLP identifies Office documents based on their origin, or based on rules set by the IT administrators. This helps prevent sensitive information from getting copied via web apps or other sharing technologies.
- DLP provides regular and timely user notifications so as to reinforce preset security compliance policies and to adjust user behavior as per the protocols in place. This enhances and solidifies security awareness training amongst employees.

Centralized Management And Visibility

The Seqrite Endpoint Security centralized management console allows enterprises to enumerate DLP security policies and reports across numerous endpoints in scattered locations. DLP also has the additional benefits of bringing down costs by making security management as simple as possible, and of enabling sensitive data visibility across the enterprise. Enterprise customers can also access detailed security reports and audits via the inbuilt security infrastructure and management console.

This integration with Seqrite DLP also provides event monitoring in real-time for enterprises and a centralized location for carrying out effective incident

management. All these facets also give companies the option to easily collect statistics about data access. This detailed information can ultimately be shared with data auditors, network administrators and senior stakeholders within or outside the organization itself.

Lowering Of Complexity And Cost Of Deployment

Seqrite DLP optimizes complexity and reduces the cost of data security within the enterprise by integrating DLP features with the existing Endpoint Security solution. Serving as a resource friendly add-on pack, DLP allows you to seamlessly gain visibility over your confidential data and block potential data leakage through transfer channels such as USB drives, email attachments and other web-based applications. Furthermore, DLP add-on does not require any extra on premise hardware. The integrated Seqrite DLP solution enables enterprises to deploy security to prevent data leakage at a minimal price and with no more extra investment of time over and above that required for their traditional endpoint security solution.

Key takeaways of Seqrite DLP

- Proactively prevent data leakage or theft of Intellectual Property within your organization.
- Get a bird's eye view of actions against confidential files.
- Get notified about unauthorized data leakages through sources such as removable drives, network sharing, emails and more.
- Ensure that confidential company data does not leave the organization.

Segregation of Enterprise Data

Enterprises need effective DLP strategies in place and for that purpose, segregating between the different data types and gauging their individual characteristics is a vital exercise. The following data storage aspects need to be taken into consideration.

Data Transferred Through Web-based Applications

Seqrite DLP allows enterprises to sniff network traffic in order to single out sensitive content across established communication channels. This data in motion is scanned passively or via inline proxies in order to inspect them and prevent the leakage of important data from within the enterprise. Code snippets are thus studied in various protocols such as email, instant messages and more.

Data Accessed Or Transferred Via Physical Devices

DLP protocols actively raise alerts whenever crucial data is acted upon on individual endpoints within the enterprise. Any files which are copied or transferred via applications or USB devices can be tracked. Seqrite DLP ensures that unwanted transfer of sensitive data is recognized and network administrators are notified in a timely fashion.

Business Benefits of Seqrite DLP

- Insulates data repositories and proprietary Intellectual Property for competitive, regulatory and reputational benefits.
- Prevents accidental or deliberate data leakage via assorted transfer channels such as emails, USB drives, web-applications and more.
- Reduces the extent of financial hits undertaken for the investigation or restoration of data breaches.
- Segregates data repositories as per customized enterprise policies so as to mitigate future data risks and strengthen blind spots with regards to crucial data.
- Allows enterprises to be future-ready for policy renewals or amendments. In this manner, policy compliance is maintained even in the face of changing circumstances.

» Provides real-time alerts and reminders to bolster the data security awareness of employees within the enterprise.

Seqrite DLP can also be used in conjunction with another feature – Advanced Device Control. With the help of this feature, Endpoint Security clients can get the following benefits:

- Configure access policies for more than 25 device types
- Block unverified devices from accessing the network
- Prevent Autorun infections through unknown devices
- Ensure maximum transparency about plugged-in devices

Supported Platforms

Windows Workstations supported:

» Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit/64-bit)

» Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)

» Microsoft Windows Vista Home Basic / Home Premium / Ultimate / Business / Enterprise (32-bit/64-bit)

» Microsoft Windows Server 2008 Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)

» Microsoft Windows Server 2008 R2 Web / Standard / Enterprise / Datacenter (64-bit)

» Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)

» Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)

» Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)

» Microsoft Windows SBS 2011 Standard / Essentials

» Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)

» Microsoft Windows MultiPoint Server 2012 Standard (64-bit)

» Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)

» Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit/64-Bit)

Mac Workstations supported:

» Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10

Note – Network Share & Removable Drive channels are not supported on Macs.

Corporate Office

Quick Heal Technologies Limited

Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune - 411014, Maharashtra, India

Email: info@seqrite.com | Website: www.seqrite.com