clearswift
by HelpSystems

DATASHEET *(Cybersecurity)*

Clearswift Endpoint DLP

With over 3 billion records lost through data breaches in 2017 and new data protections law being enforced across the globe, organizations need to understand where their critical information resides and ensure it can't be leaked through removable devices.

Business Problem

We live in a data centric world. Businesses provide employees access to data in order for them to do their job; to collaborate with internal staff and external organizations. However, care must also be taken to ensure that the critical data that resides on laptops, servers and in Cloud services is only used by the people that need to use it and that it is used for the correct purposes.

However, we've seen too many cases of accidental data loss, including:

- Laptops being stolen with critical information held in an unencrypted state
- USB sticks being left in taxis
- DVDs containing Personally Identifiable Information (PII) being lost in the mail
- Portable hard drives not being appropriately secured.

As well as accidental loss, employees can be tempted to take company data when they leave jobs, as well as deliberately leaking data for money, or decide that their employer's ethical beliefs are dubious and become a whistle-blower.

The challenge for organizations today is working out the most effective security technology for laptops, desktops and devices that enable users to operate efficiently, but with today's required level of protection.

Architecture

Protecting the endpoints require two components to be effective:

- A scalable server architecture permitting granular policy controls of users and groups through the product console. This architecture must have no single points of failure and must scale to thousands of end points
- Lightweight, feature rich endpoints that enforce the device control, Data at Rest and Data in Use policies and communicate back to the servers with violations, but also give feedback to the end-user to educate them when a mistake has been made.

Device Control

The ability to control users connecting personal USBs or smart devices to the corporate network has become a critical security requirement. Sensitive data can be lost and malicious applications can be introduced to networks due to the uncontrolled use of removable media. The Clearswift Endpoint DLP solution provides granular management of removable media, permitting the legitimate productivity-enhancing use of these devices whilst reducing network risks and support costs – resulting in increased data security.

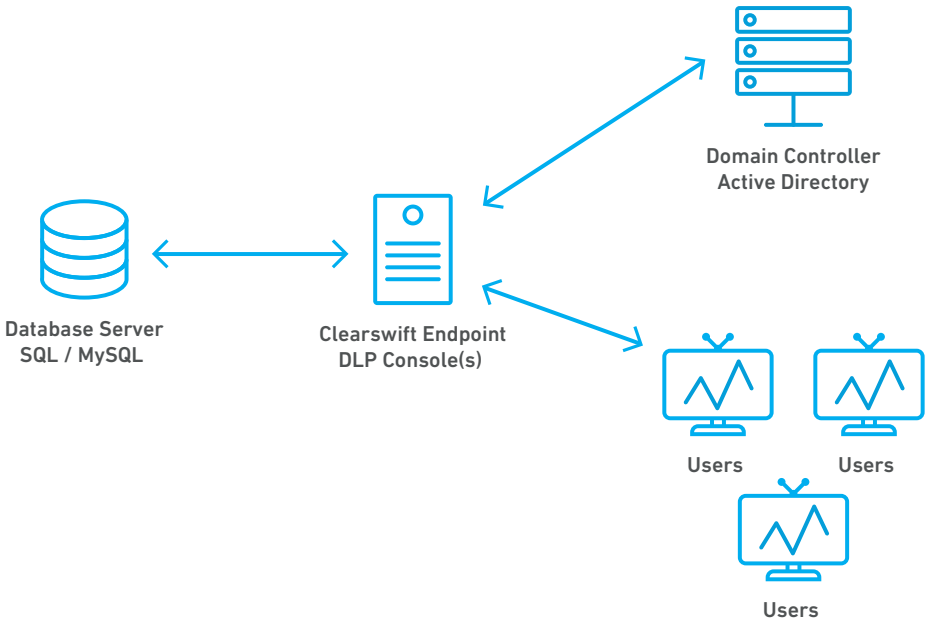
Context-aware Data In Use (DIU) Policies

Flexible policies and context-aware content inspection mean that you no longer have to choose between the productive use of removable media and unacceptable risk. A policy which is too restrictive means that people either cannot work effectively, or they will find ways to bypass their security policy. Rules can be created that block all spreadsheets containing particular keyword terms from being copied to external devices. Alternatively, files can be encrypted when transferred – which ensures that the contents of a USB cannot be read if it was to be left behind in a taxi or in another public place.

Discovering Data At Rest (DAR)
Working together with the Clearswift Deep Content Inspection Engine, critical data can be discovered wherever it is stored on desktops, notebooks, servers and shared networks. This enables organizations to audit and manage critical information clean-up within data at rest. As with 'data in use' policies, built-in and customizable lexical expressions are included, which enables discovery of critical information such as PII, PCI and other sensitive data. Running in the background, Clearswift Endpoint DLP silently discovers critical information without interrupting end user activity. This provides unprecedented insight into potential data protection vulnerabilities that exist on your networks and systems.

Deployment

The Clearswift Endpoint DLP console component is installed on a Windows Server and requires access to a SQL server or a MySQL database. It synchonizes with the corporate Active Directory to gather the list of computers and users so that policies can be created at the domain level, organizational unit level or down to a per user level. For high availability there can be multiple console servers connecting to the end-point agents.



The console is used to create and remotely deploy the installers for the supported client types:

- Windows 7 and 10
- Windows Server 2012 R2 and 2016
- Citrix environments

Comprehensive reporting across the whole deployment is available through the console.

For enterprise deployments, multiple administrators can be defined to permit regionalized management.

Features

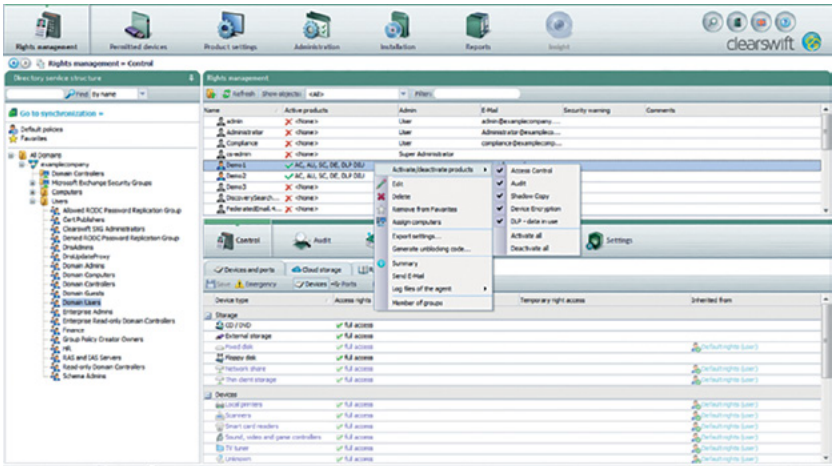
Designed to scale to enterprise deployments, the Clearswift Endpoint DLP solution provides:

- Granular policy control – allows controls on per user / OU levels
- Device management – controls by bus and device type
- Cloud access control – controls access to standard Cloud sharing services such as OneDrive, Dropbox, Box, etc.
- Data in Use – ensures that data written to external devices has been content checked and appropriate file types can only be used
- Data at Rest scanning – periodic scanning of the local hard disk and mounted shares can be swept for file types and file content
- Syslog support – centralized logging of event data can be exported to SIEM systems

Easy to Use GUI

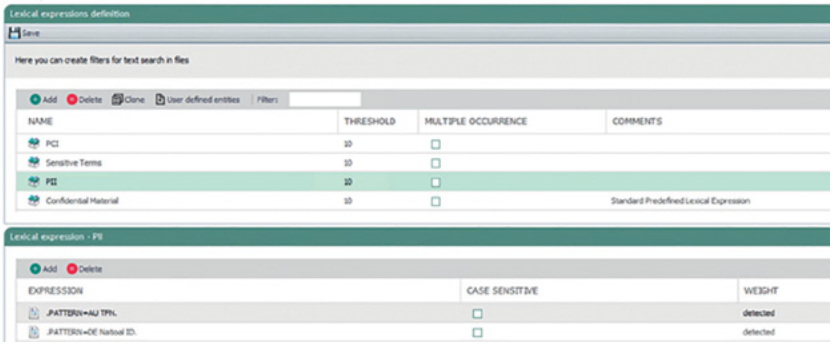
The Clearswift Endpoint DLP management interface is broken into logical sections where policies can be applied to organizational units harvested from Active Directory. This view also makes it easy to see what Access Control rules are applied as well as Content policies.

Features can be licensed as needed for the organization, or a user automatically enrolled.

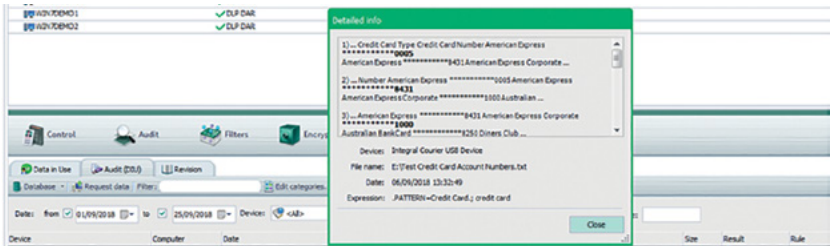


Lexical expression lists are created using words, phrases, tokens (such as Credit Card, IP Address, etc.) and regular expressions. These phrases are weighted and can be used together to form meaningful search criteria.

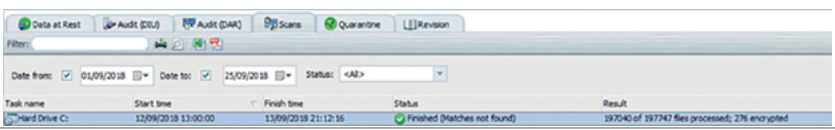
These expression lists are used to form DIU and DAR policies.



DIU scans show when attempts were made to exfiltrate sensitive data showing exactly what security policies were broken.



DAR scans can be viewed in real time to show their progress and whether items were found.



Feature	Benefit
Directory Integration	Integrates with directory servers with scheduled sync events to ensure that amendments such as new employees and computers can be reflected in policy. Policies for users and computers can be configured based on their structure within the directory, for example setting rules for the "Sales" organizational unit.
Policy Inheritance	Default policies can be created for all users and computers simply and easily, specific amendments to users/computers can be applied as and where necessary.
Data in Use Policies	Content inspection of files being written to removable devices allows for consistent definition of words, phrases and policies to detect and prevent potential data breaches.
Data at Rest Policies	Agents can be scheduled to scan fixed and/or removable devices at designated times or day or days of the week using the same content inspection policies created for Data In Use policies.
Access Control	Physical devices such as removable devices, printers, modems, etc. can be. blocked by name, type, serial number or ID.
Cloud Access Control	To reduce the changes of Shadow IT, controls are provided to restrict access to common Cloud file sharing applications such as Box, Dropbox, OneDrive and GoogleDrive based on policy whether on or off the corporate network.
File Filter	Files can be blocked by specific data type. Checks are made on headers and not just extensions to ensure files are not spoofed. Predefined types have been provided to help customers deploy quickly and easily.
Removable Device Encryption	Provides total security to cover all devices placed in removable devices whether they were marked as secret or confidential or contained PCI and PII. Encrypted USB devices can be shared internally with seamless interaction with appropriate users.
SQL Database Support	Allows customers to consume resource on existing SQL systems or deploy on Microsoft SQL Server, MySQL or SQL Express for small companies/evaluations.
Low Footprint Agent	Agents designed to mimimize resource usage to ensure maximum user experience.
Remote Deployment	Agents can be deployed remotely via the console or using standard windows mass deployment options.
Online / Offline modes	Agents that are offline will continue to operate using the last synced policy and will hold onto logs and alerts until the device is connected back to the corporate network.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.