

Clearswift Adaptive Data Loss Prevention

Clearswift Adaptive Data Loss Prevention (A-DLP) is the data and people centric solution to critical information protection. Unlike others, A-DLP is a non-disruptive solution which supports continuous collaboration, avoids business interruption and mitigates the risk of financial or reputational damage caused by the unauthorized disclosure of sensitive data wherever it lives – at the endpoint, on premise or in the cloud.

Data in Use

Endpoint devices come in many form factors, using a mixed array of information hungry applications, operating within corporate and external unprotected networks. The Clearswift Critical Information Protection Agent (CIP Agent) ensures data loss prevention whether online or offline.

Data in Motion

The Clearswift Secure Gateway and ARgon families provide critical information protection for sensitive data shared via the web and email both inside and outside of your corporate network and includes online collaboration tools and social media.

Data at Rest

Discovering the 'smoking gun' and discovering information you have stored is a critical component when preventing data loss. The Clearswift Critical Information Protection Agent (CIP Agent) will provide approved business units from compliance, audit, IT, HR, support amongst others with visibility of all information and the levels of protection and/or remediation required to mitigate non-compliance with their information governance policies and data extraction by unauthorized individuals and/or malware.

Functional Benefits

- Identify, manage and protect critical information
- Ensure compliance, protect against data leaks, enforce data usage policies, identify data duplication and manage obsolete documents
- Adopt low risk, modular approach
- Select solution(s) that meet immediate business needs
- Deploy additional solutions to provide consistent protection
- Complement existing solutions, not rip and replace

Business Benefits

- Protect brand/reputation
- Protect intellectual property and maintain a competitive edge
- Protect against financial fines and clean up costs

FEATURE SUMMARY

Adaptive Redaction

Data Loss Prevention (DLP) features that reduce effects of false positives and don't become a barrier to business communications

- Protect organization from risk, but allows underlying communication to happen
- Without management overhead of traditional DLP solutions

Data redaction

- Remove sensitive information (e.g. intellectual property, PCI, PII, etc.) and replace with asterisks
- Automatically apply consistent redaction policy, even when users forget
- Microsoft Office, OpenOffice, PDF, RTF, TXT and HTML

Document sanitization

- Remove meta-data, version and document history (e.g. personal details, network details, SharePoint information, etc)
- Users can share documents without exposing critical information
- Microsoft Office, Open Office, PDF, JPG images and other formats.

Structural sanitization

- Removes active content (typically used to launch targeted attacks to steal data)
- Users can still access underlying data
- Microsoft Office, OpenOffice, PDF, RTF and HTML

Encryption

- Secure data in transit (e.g. payroll information, client data, etc.)
- Automatically applied, even when users forget
- TLS, S/MIME, PGP and Portal



**Clearswift
Secure Email Gateway**

- Prevent data loss via email
- Automated on-box encryption (TLS, S/MIME, PGP and Portal)
- Adaptive redaction
- Integrated anti-virus/malware
- Multi-layered anti-spam
- Managed service/on premise solution
- Complements Office 365



**Clearswift
Secure ICAP Gateway**

- Prevent data loss via the Internet (e.g. webmail, cloud collaboration services, etc.)
- Integrates with Symantec/F5/Squid servers
- Forward and reverse proxy
- DLP controls
- Adaptive Redaction
- Optional anti-virus/malware



**Critical Information Protection
(Management Server and Agent)**

- Reduce risk of data loss at endpoint and discover unknown risks on network
- Enforce device policy
- Monitor/block/encrypt confidential data
- Data in use (e.g. USB, DVD, etc.)
- Data at rest (sensitive information stored on laptops, public areas of network, etc.)
- Adaptive Redaction



**Clearswift
Secure Web Gateway**

- Prevent data loss via the Internet (e.g. webmail, cloud collaboration services, etc.)
- DLP controls
- Adaptive Redaction
- HTML, Web 2.0 and HTTPS traffic
- Integrated cache, URL filtering, anti-virus/malware and spyware
- Remote Client



**Clearswift
ARgon for Email**

- Prevent data loss via email
- Mitigate risk of targeted attacks
- Adaptive redaction
- Complements boundary email solution
- Complements Office 365



Information Governance Server

- Reduces management overhead of enforcing DLP policy
- Provides visibility of information flows inside network and out of boundaries
- Register sensitive documents (full and partial fingerprints)
- Delegate registration to trusted users
- Integrates with other Clearswift solutions



**Clearswift
Secure Exchange Gateway**

- Extend DLP policies to internal traffic
- Adaptive Redaction
- Optional anti-virus/malware
- Exchange 2010, 2013 and 2016
- Complements boundary email solution

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.