Enforcer to Enabler

How Adaptive DLP is securing the agile enterprise

The next evolution of Data Loss Prevention technology is here

As security threats get smarter, enterprise security leaders need more intelligent tools and approaches too. Here's why the new breed of DLP – Adaptive DLP – is the answer.

Data is being lost even by the best.

Next time, it could be you.

Direct attacks

2017 USA Today Owner Gannett: Personal data of up to 18,000 current and former employees compromised in phishing attack.

Through the side door

2015 Office of Personnel Management (OPM): Cybercriminals gained entry to the system through a contractor. 21 million social security details stolen.

Malicious insider threats

2016 Sage: Unauthorised access to employee data of nearly 300 UK firms by using an internal log-in.

Accidental insider threats

Mobile, BYOD and cloud are changing the security landscape and creating new malware challenges. Broken internal processes and benign employee error pose a serious threat to security

Top 5 risks of data loss – deep and far-reaching

Organizations cite the following as being the key impacts of data loss [2]

One

53% Loss of customers and/or market share

Two

48% Reputational damage

Three

48%

Loss of competitive advantage through loss of intellectual property

Four

42% Fines and penalties

Five

41% Erosion of shareholder value

+

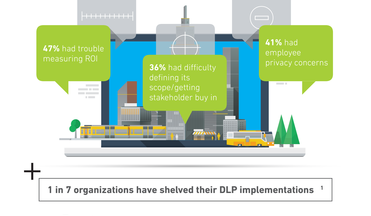
$445 billion

annual cost of Cybercrime and espionage to the global economy [3]

So, whats the plan to prevent data loss? Traditional 'stop & block' isn't smart enough...

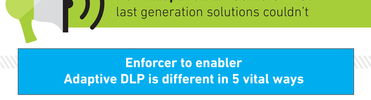
...and has a reputation for locking down and obstructing business.

52% of organizations say they haven't deployed DLP because:



+

1 in 7 organizations have shelved their DLP implementations [1]



New Adaptive DLP delivers what last generation solutions couldn't

Enforcer to enabler Adaptive DLP is different in 5 vital ways

Context-aware: makes policy-driven decisions on what to stop or allow – based on who is sending what to whom

Content-aware: performs deep inspection of information and attachments, both incoming and outgoing across multiple channels

Removes embedded content: including malware that might carry an Advanced Persistent Threat

Deploys Adaptive Redaction: removes visible and invisible content hiding in document properties and revision history

Maintains 100% visibility of critical information, 100% of the time: the authorized part of the communication continues on its way

Creating the perfect balance between

Control and collaboration

Security and access

Agility now and a protected future

No wonder 88% of businesses not using DLP, plan to in the next 12 months [2]

78% because of new EU Data Protection Regulations

67% to protect against malicious internal breaches

60% to defend against malicious cyber attackers

Find out how Adaptive DLP from Clearswift can help you maintain 100% visibility of your critical information, 100% of the time.

Please contact us at: **info@clearswift.com**, or call us on:

United Kingdom & Europe
Tel: +44(0)118 903 8903

Australia
Tel: +61 2 9424 1200

United States
Tel: +1 856 359 2360

Japan
Tel: +81 (3)5326 3470

Germany
Tel: +49 (0)89 904 05 206

1. World Economic Forum. Global Risks 2015 10th Edition
2. Research paper – The State of DLP. December 2016. Loudhouse
3. http://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

clearswift
Build Cyber Security