

LEAKWALL

by GENTLESECURITY



comprehensive, simple & effective
data leak prevention

loss of sensitive business data a serious issue for all industries



FACTS & FIGURES

- › 70% OF DATA LEAKS CAUSED BY INSIDERS.
(US COMMERCE DEPT.)
- › AVERAGE COST OF EACH DATA LEAK INCIDENT IS 1.5 MILLION EUROS (FORRESTER)
- › WHEN A DATA LEAK IS REVEALED COMPANIES LOSE 6.5% OF THEIR CUSTOMER BASE (PONEMON INSTITUTE, 2008)
- › 700 MILLION PEOPLE AFFECTED BY 2,300 DATA LEAK INCIDENTS IN 2009. (KPMG)

“It’s more important than ever to keep a firm control on those with access to data”

Edge Zarrella
Global Head of IT Advisory, KPMG

Loss of sensitive data may cost between **3% and 5% of revenue** for a company’s, compromising intellectual property, brand equity and customer relations in addition to causing massive direct and indirect costs. That alone can wipe out all hardly earned profits. Just in 2009 data leak incidents affected over **700 million people** and cost billions of Euros worldwide.

With **70% of all data leaks caused by insiders**, whether inadvertently or otherwise, traditional approaches focusing on limiting leak channels fail to address the number one cause of data loss.

Virtually all businesses in the modern economy rely heavily on their information systems and on the sensitive business data they contain. From simple spreadsheets and documents to more sophisticated databases, both a company’s strategic position and day-to-day operations can be severely impacted if sensitive data is compromised or allowed to leak outside of the company’s control. Examples abound, from a German telecommunication company that lost the data of 16 million of its customers in 2006, to details of 130,000 clients of large bank in Geneva or even disclosure of the information of thousands of Belgian customers of a private bank by former employees...

Traditional data leak prevention solutions, many of which were conceived over a decade ago, fail to address the new risks that have emerged with massive adoption by business of email, computer networks and Internet connectivity. Furthermore, with the advent of software as a service platforms (SaaS) and social networks, which are used for professional purposes, simply restricting the use of devices like USB stick is not enough. Traditional solutions fail to manage the number one risk of data leaks: insiders, i.e. employees or long term consultants who are granted access to work and, most often by mistake or lack of knowledge, cause data losses, which can have devastating consequences.

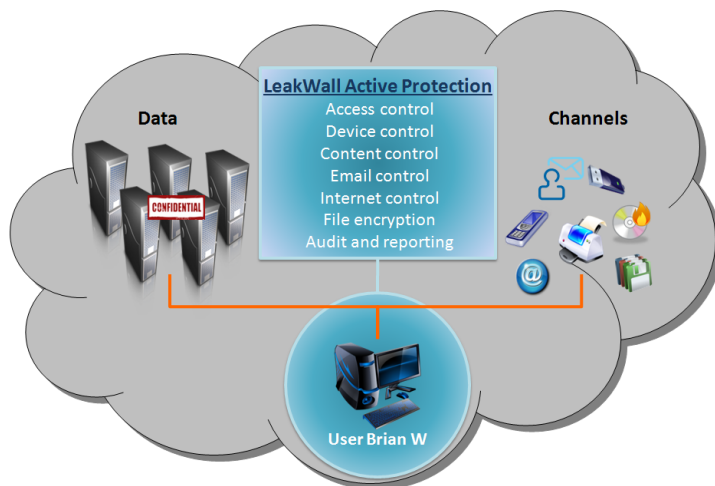
So the very burning problem of leaks of sensitive data cannot be adequately addressed by merely restricting devices and channels, let alone the fact that by limiting functionality of information systems these solutions destroy productivity.

covering 100% of channels of data leaks
LeakWall prevents leaks caused by insiders

true data leak prevention for sensitive content

THE LEAKWALL WAY

For companies relying heavily on sensitive business data, who are faced with the imperative to prevent leaks LeakWall is a **content-driven data leak prevention system** that covers all sources of data leaks without impacting productivity. LeakWall controls channels and is aware of data.



In stark contrast with traditional products, GentleSecurity has been able to build **truly effective solutions** that can be deployed and managed with only **minimal effort**.



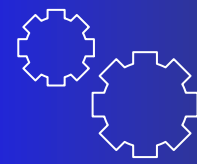
Furthermore, because it focuses on **business content**, i.e. the daily bread and butter of business users, LeakWall is particularly suited to networked environments involving email, online platforms and intensive interactions of insiders with suppliers, partners and customers.

PROTECTION OF CRITICAL BUSINESS CONTENT MUST NOT REDUCE USER FUNCTIONALITY AND PRODUCTIVITY.

YOUR CLEAR BENEFITS

LeakWall offers a set of distinctive benefits to professionals in charge of information system integrity:

- › **Easy setup** as there is no need to proceed to a detailed and time consuming inventory of sensitive data and locations
- › **Easy administration** through full integration with Active Directory
- › Ability to define **sophisticated information flows** to IT security personnel
- › **On-the-fly configuration** updates as required
- › **True 100% coverage**
- › An ideal combination of user **functionality** with necessary levels of **security** to comply with best practices and regulations



BANKING DATA PROTECTION

Despite the existence of device controls and other usual security measures, a private bank accidentally lost customer details of thousands of its most valuable customers. The data was subsequently offered to the highest bidder online. With the implementation of LeakWall and its ability to fully control content, the leak of such sensitive information is now simply impossible.



IP PROTECTION

With the essence of its business being in product engineering and software code developed to manage sophisticated industrial operations, a large manufacturing company was concerned about the risk of finding software code in the hands of competitors operating in the auto industry. With the deployment of LeakWall and its configuration on the basis of samples of text and rules on file types, the loss of core product engineering content is now extremely unlikely.



EASY ADMINISTRATION

A Senior System Administrator of a leading European media group is able to monitor his data leak risks and events on a daily basis and adapt LeakWall's configuration simply and on-the-fly. At any time he is able to check the situation, while he will be alerted by LeakWall about all serious events occurring on the company's sensitive data as users work on their daily tasks.

HOW DOES LEAKWALL PREVENT SENSITIVE DATA LOSS?

LeakWall is made aware of sensitive content through several mechanisms from content sampling, to file type, to user creator... Based on its knowledge of what is sensitive, LeakWall is able to track, block, warn the user, keep an audit trail and report to people in charge even as data is accessed by a user based on regular rules and rights as defined in the enterprise system. With its ability to control devices and channels LeakWall is able to deny specific actions of sensitive data transfer irrespective of the technical means used



to perform the transfer.

Content or parts of content identified as sensitive will not be allowed to get out of the controlled area. All content is tracked and necessary actions are taken to help users avoid mistakes. Furthermore, administrators & security personnel get full reports of activity.

WHAT YOU GET WITH LEAKWALL

- › Your sensitive business content is contained and under complete control
- › Your users remain completely productive with the tools you've chosen for them
- › You manage the risk of direct and indirect unplanned costs stemming from data leaks
- › You protect your brand equity and customer relationships
- › Your intellectual property, know-how and contacts are protected

lean administration & monitoring console integrated into Microsoft Active Directory

FEATURES

- › Comprehensive control of data leak channels including devices, printing, e-mail, HTTP, HTTPS, FTP, SSL, IM and more
- › Recognition of sensitive content in over 500 file formats
- › Recognition of partial, modified and derivative sensitive content
- › Encryption of sensitive data on desktops, laptops and removable drives
- › Controlling access to devices
- › Data access application policy
- › Centralized management via Microsoft Active Directory
- › Full audit of data usage, such as access, modification and transfer
- › Comprehensive reporting with flexible custom reports

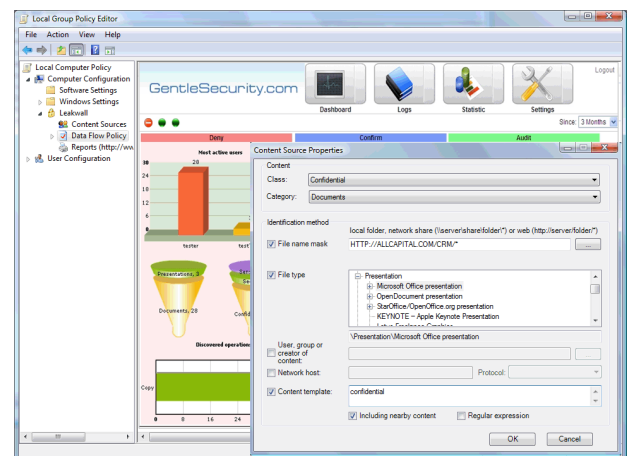
SYSTEM REQUIREMENTS

LeakWall client:

- › Windows XP, Windows 2003, Windows Vista, Windows 7, Windows 2008
- › RAM: 256 MB minimum
- › Disk space: 100 MB

LeakWall Reporting Server:

- › CPU: 1GHz or better
- › RAM: 1 GB
- › Disk space: 4 GB minimum



GENTLESECURITY

66, rue de Luxembourg
L-4002 Esch-sur-Alzette
GD de Luxembourg
+352 54.55.80.459 ph
+352 54.55.80.463 fax
www.gentlesecurity.com