

Data Leakage Prevention

Averting the Silent Threat
with SafeGuard LeakProof

utimaco[®]
s a f e w a r e

Data Leakage Prevention

Averting the Silent Threat with SafeGuard LeakProof

After years of effort and investment, many businesses feel confident in their ability to secure an organization's perimeter and prevent intruder access. After all, powerful firewalls, data encryption and anti-virus software guard against external forces trying to gain access into the company—and its most valued asset: data. And, while they are all necessary measures to prevent a loss of vital information, these solutions don't protect against misappropriated or stolen data from *internal sources*.

With a reported 50 percent—and as much as 80 percent—of security breaches being caused by insiders within the organization and behind the firewall, it is perhaps the biggest threat of all. But, increased awareness of the problem, along with regulatory pressure, and the potential for brand damage and bad press, has fueled the rapidly growing Data Leakage Prevention (DLP) market.

Data Leakage Prevention Defined

Analysts estimate that 70 percent of all corporate security incidents that result in financial loss come from insiders through inadvertent actions, or sometimes exploiting their authority inappropriately. DLP describes efforts to detect and prevent the unauthorized transmission of corporate data to anyone outside the organization. For the most part, this involves creating safeguards and warning systems that prevent the accidental misuse of sensitive information, but it also includes the ability to identify and block intentional acts.

DLP is an integral part of any organization's Information Risk Management (IRM) strategy in that it helps mitigate the risk associated with user handling of sensitive information and minimizes the occurrence of inappropriate data movement.

What's more, a successful DLP initiative is one that identifies and monitors data in all stages of the information lifecycle. This includes "data in motion," as it travels across the network, "data at rest," as it is stored in file shares, databases, and endpoints, and "data in use," as on user desktops or in mobile devices.

Preventing data leakage is much more challenging today than it was ten—or even five—years ago. The sharp increase in mobile workers has forced companies to allow access to data from outside the physical walls. And, messaging systems, wireless networking, and USB storage devices make it easier than ever for corporate and customer data to stealthily make its way outside the firewall.

To make matters worse, the stakes are higher than they were before. The emergence of a wide variety of data security and privacy regulations, such as the Payment Card Industry (PCI) Data Security Standard, the U.S. Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), European Union Data Protection Directive, Senate Bill 1386, and Sarbanes-Oxley, have forced organizations to implement policies and document measures to keep information confidential and protect customer privacy. And, this is where data leakage can cause the most damage. Non-compliance and breaches can result in fines and costly litigation—not to mention the bad press that results from publicized incidents.



An Introduction to SafeGuard LeakProof

SafeGuard LeakProof from Utimaco helps in the end-to-end discovery, classification, protection, and monitoring of data. Specifically, it helps companies prevent data leakage directly from the endpoint—where information is most commonly leaked. Ideal for mobile, branch, and corporate offices, SafeGuard LeakProof greatly minimizes the risk of data breaches by inspecting the content of files on corporate endpoints, identifying sensitive documents in motion, and either preventing the transmission of confidential documents, logging the operation, encrypting the document, or forcing a justification or reason for an action. It also enables compliance by establishing enforceable policies, providing preconfigured compliance templates, helping companies assess risk continuously, monitor, log, and prevent breaches, and educating employees on how to best handle enterprise information in a variety of situations.

SafeGuard LeakProof includes software for the client, as well as a management console. The components work together to protect sensitive information and prevent both intentional and accidental data leaks.

Client Software

SafeGuard LeakProof uses highly accurate, high-performance filtering at the endpoint and scans all data operations in real time and based on sensitive keywords, such as “secret” or “confidential.” When there are file movements to USB devices, Bluetooth, Webmail, FTP, HTTP, and IM, SafeGuard LeakProof works unobtrusively, behind the scenes, looking for attributes of known sensitive documents using content inspection intelligence for document fingerprinting. And, it identifies data structures, such as credit card numbers and other customer data. When sensitive information is detected, SafeGuard LeakProof proactively takes measures to ensure its safety. The software:

- Reduces the occurrence of accidental leakage by notifying the user and sending alerts
- Minimizes the occurrence of intentional leakage by logging and blocking the operation
- Protects the data in transit through encryption

According to analyst firm IDC, more than 70 percent of confidential data resides at the endpoint.

Management Console

Each organization defines confidential data differently. Therefore, SafeGuard LeakProof enables administrators to define a content policy with a unique set of sensitive keywords, fingerprinted documents, and regular expressions. With the console, administrators can identify the location of all sensitive data by scanning each and every endpoint, trace incidents, and start forensic investigations on suspect operations. What's more, it establishes a workflow that allows incidents to be handled by different roles within the organization. The console also offers a dashboard through which security violations can be viewed by endpoints, users, and data types—helping establish patterns and flag suspect operations.

Unique Fingerprinting Technology

SafeGuard LeakProof uses patent-pending technology to establish a “fingerprint” of each sensitive document. This is done by calculating a unique pattern that identifies markers on each piece of content. The “fingerprint” is then distributed and stored in a small file on each endpoint. At the time documents are moved to different media, the algorithm quickly scans them and if there is a match to a stored “fingerprint,” the document is flagged as confidential. The algorithm works on virtually all file types and documents in all languages, including Chinese and Japanese.

Key Benefits

- Protect privacy - Monitor and prevent improper use of customer and employee information
- Protect intellectual property - Discover, classify, protect and monitor critical company assets
- Comply with privacy regulations - Monitor usage, scan endpoints, and educate employees to reduce risk
- Educate employees - Customize interactive dialogs for employee education and workflows
- Discover sensitive data - Find sensitive data on laptops, desktops, and servers

Prevent Data Leaks

- Mobile, branch, corporate
- Endpoints online, offline
- Corporate networks
- Public networks
- USB, Bluetooth, WiFi, email
- Data in motion, at rest, in use



Conclusion

Utimaco has introduced SafeGuard LeakProof into its portfolio as a way to help businesses extend their security efforts to include data leakage prevention. It helps them identify all confidential data on laptops, desktops, and servers and track or prevent the movement of that information to unauthorized destinations. In doing so, SafeGuard LeakProof helps mitigate the risk of non-compliance, protects privacy, and safeguards corporate information.



www.utimaco.com

HEADQUARTERS

Utimaco Safeware AG

P.O. Box 20 26
61410 Oberursel
Germany
Phone +49 (61 71) 88 0
Fax +49 (61 71) 88 10 10
E-Mail: info@utimaco.com

Utimaco Safeware AG

Hohemarkstraße 22

61440 Oberursel
Deutschland
Phone +49 (61 71) 88 14 44
Fax +49 (61 71) 88 14 90
E-Mail: info.de@utimaco.com

USA

Utimaco Safeware Inc.

10 Lincoln Road
Foxboro, MA 02035
Phone: +1 (508) 543 1008
Fax: +1 (508) 543 1009
E-Mail: sales.us@utimaco.com

UNITED KINGDOM

Utimaco Safeware Ltd.

Ash House
Fairfield Avenue
Staines
Middlesex TW18 4AB
Phone: +44 1784 22 42 25
Fax: +44 1784 22 42 29
E-Mail: sales.uk@utimaco.co.uk

JAPAN

Utimaco Safeware K.K.

Nisso 16 Building, 3F
3-8-8 Shin Yokohama, Kohoku-ku
Yokohama 222-0033
Japan
Tel.: +81(0)45 470 1430
Fax: +81(0)45 470 1431
E-Mail: info.jp@utimaco.jp

HONG KONG

Utimaco Safeware Asia Ltd.

Unit 602, Stanhope House
734 King's Road
Quarry Bay
Hong Kong
Phone: +8 52 25 20 26 08
Fax: +8 52 25 29 26 18
E-Mail: info@utimaco-asia.com

FRANCE

Utimaco Safeware France

8, Place Boulnois
75017 Paris
Phone: +33 (1) 56 21 25 25
Fax: +33 (1) 42 67 30 00
E-Mail: info@utimaco.fr

SWITZERLAND

Utimaco Safeware (Schweiz) AG

Zürcherstrasse 20
8952 Schlieren
Schweiz
Phone: +41 (44) 7 35 40 80
Fax: +41 (44) 7 35 40 85
E-Mail: info.ch@utimaco.ch

AUSTRIA

Utimaco Safeware AG

im Regus TwinTower
Wienerbergstrasse 11/12
1100 Wien
Österreich
Phone +43 1 99 460 6517
Fax +43 1 99 460 5000
E-mail: info@utimaco.at

BENELUX

Utimaco B.V.

Hoevestein 11B
4903 SE Oosterhout (NB)
The Netherlands
Phone: +31 (162) 480 240
Fax +31 (162) 430 330
E-Mail: sales@utimaco.nl

SWEDEN

Utimaco Safeware AB

Box 16, Malaxgatan 1
16493 Kista
Phone: +46 (8) 5 84 00 600
Fax: +46 (8) 5 84 00 610
E-Mail: info.se@utimaco.com

FINLAND

Utimaco Safeware Oy

Airport Plaza Presto
Äyritie 12 B
01510 VANTAA
Phone: +358 9 855 3200
Fax: +358 9 855 32030
E-Mail: info.fi@utimaco.com