



Emerging Solutions for Strengthening Data Loss Prevention (DLP)

Data loss discovery and intelligence complements DLP
without disrupting business processes

Emerging Solutions for Strengthening Data Loss Prevention (DLP)

Data loss discovery and intelligence complements DLP without disrupting business processes

Abstract

The global market for data loss prevention (DLP) is both large and growing, with an estimated worth of over \$1 billion now and an annual growth rate of 20%.^{1,2} There is good reason for this, as there are tremendous costs associated with the loss of sensitive information, whether it is intellectual property (IP), personally identifiable information (PII), payment card information (PCI) or any data critical to business operations.

At the same time, new threats are evolving rapidly and security breaches continue to occur even at the most tech-savvy organizations. This paper examines the problem of data loss, the factors driving up the cost and complexity of DLP implementations and emerging technologies for addressing this problem—including data loss discovery and intelligence solutions from InDorse Technologies, Inc.

The Problem of Data Loss and the Need for DLP

The need to protect sensitive data is acute. Unauthorized use of information can incur enormous financial costs, including stiff penalties for non-compliance with government and industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley and California SB 1386.

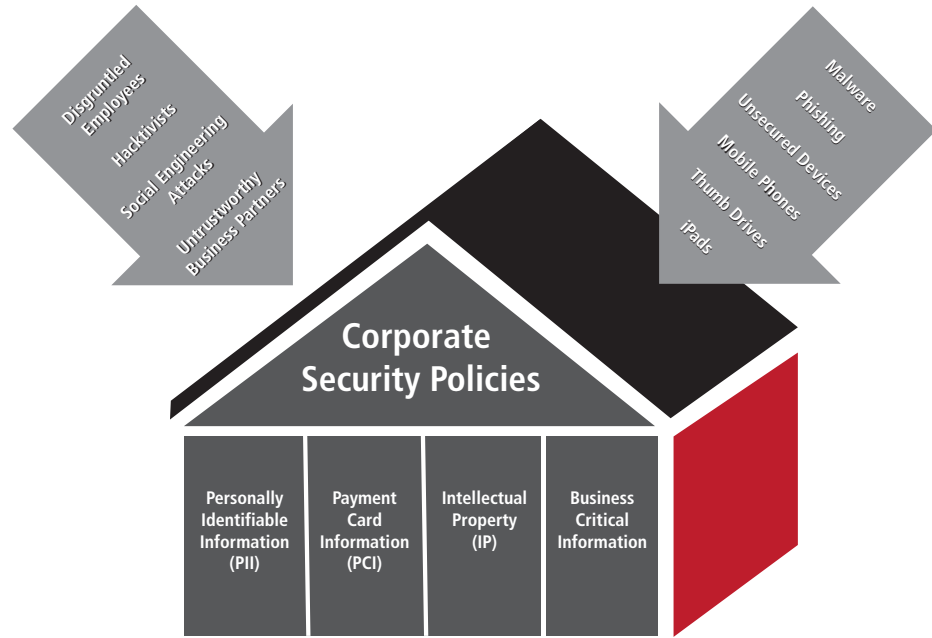
Real-world examples of data loss include:

- A spreadsheet containing personal medical data on 20,000 patients is posted to a public Web site and the error is left undiscovered for a year. As a result, the hospital could be liable for paying a six-figure fine.³
- A confidential bid is delivered to a potential client who downloads it to a USB device and gives it to a competitor; the competitor alters their bid to undercut the original pricing proposal.⁴
- A financial services firm produces valuable fee-paid research that is forwarded by a subscriber to unauthorized distribution channels, resulting in the loss of hundreds of thousands of dollars in potential revenue.
- Confidential product specifications from a major computer component manufacturer are leaked to a public Web site.⁵
- The hacktivist group *Anonymous* defaces the Web site of a leading security group, publishing over 50,000 client credit card numbers online.⁶

In each of these examples, data loss resulted in a financial cost to the organization, either from fines for non-compliance, loss of potential revenue or the need to provide restitution to victims of identity theft. (We will revisit these scenarios near the conclusion of this paper to illustrate the possibility of better outcomes enabled by emerging data loss discovery and intelligence technologies.)

Unauthorized use of information can incur enormous financial costs, including stiff penalties for non-compliance with government and industry regulations.

Figure 1 illustrates some of the many evolving security threats assaulting enterprises today.



DLP provides visibility into content ... identifying sensitive data and enabling actions to protect it.

How DLP Addresses Security Threats

Historically, information technology (IT) professionals have focused on defending the network perimeter and applications against intrusion and attacks. More recently, the protection of information itself has become a top priority of IT, giving rise to the market for DLP solutions.⁷

DLP provides visibility into the content residing in the enterprise by identifying sensitive data and enabling actions to protect it. More specifically, data loss prevention has three key objectives:⁸

- Locate/identify/monitor/protect sensitive data in storage (data at rest)
- Locate/identify/monitor/protect sensitive data across the network (data in motion)
- Locate/identify/monitor/protect data on end-user systems (data in use)

Table 1 lists some of the techniques and commercially available technologies used to achieve these objectives.

Table 1. Three Areas of DLP

1. Data at Rest	2. Data in Motion	3. Data in Use
<ul style="list-style-type: none"> • Crawl through data stores to find sensitive data • Conduct searches using keywords, regular expressions, partial document matching, etc. Fingerprinting techniques may also be used. 	<ul style="list-style-type: none"> • Analyze network traffic using deep packet inspection • Conduct contextual analysis of transactions • Classify/monitor outgoing emails 	Deploy agents on endpoints to apply policies controlling the ability of end-users to manipulate sensitive data (print, copy, edit, email, etc.) using: <ul style="list-style-type: none"> • Encryption • Blocking • Quarantine • Authentication • Access control lists

Comprehensive protection is an ever-moving target.

Once sensitive data is identified, the next step is to apply policies to protect the data. For example, policies may restrict printing and emailing of sensitive data, or block access to all users except for a select few. Therein lies one of the risks of DLP—if the techniques used for identification are not accurate, “false positives” will occur and non-sensitive data will be subject to misapplication of restrictive policies. When this occurs, business processes are disrupted and the effort to support secure business transactions backfires. For this reason, DLP is often implemented in “advice-only” mode to avoid hindering employee productivity.

Accurately identifying sensitive data can be a gargantuan task. As noted in a white paper by McAfee, “It’s impossible for IT to identify all of the sensitive data, interpret the regulations and translate them into effective policies. When faced with this dilemma, many companies simply fall back to ‘good enough’ solutions that don’t provide basic protection...”⁹

Factors Driving the Cost and Complexity of DLP Implementations

DLP technology has made significant advances in the past five years, and the marketplace is indeed active with innovation. At the same time, several trends are driving up the cost and complexity of DLP implementations. These trends, which show no signs of abating, include:

- **Mobile devices** – the consumerization of IT has enabled employees to “bring your own device” (BYOD) to work to access corporate resources such as contact lists and email. As noted in a white paper published by Symantec, “this back door connectivity results in loss of potentially sensitive enterprise data across business systems that are out of the enterprises’ direct control.”¹⁰
- **Collaboration** – businesses practices today increasingly demand the sharing of confidential data files with third parties (customers and business partners). The trustworthiness of these third parties cannot be guaranteed.¹¹
- **Web 2.0** – employees “share” confidential data on social networking sites such as Facebook, Twitter and LinkedIn, compromising enterprise security, either intentionally or unintentionally.
- **The employee “buy-in” factor** – educating employees about security is an ongoing process, and even when end-users do understand security policies, they may knowingly circumvent them in order to get their jobs done more efficiently.

The Result: DLP is Always Needed—But Never Easy

In addition to the aforementioned trends, new challenges, as yet unknown, are likely to arise. All of these pressures give rise to three factors which make DLP solutions more difficult to integrate in the enterprise:

- 1) **DLP solutions can be costly to implement.** In addition, they can be quite expensive to maintain.¹
- 2) **Comprehensive DLP may disrupt business workflow.** As noted in a white paper by PKWare, “Most leading DLP solutions provide options for blocking, quarantining or deleting the file. These remediation strategies may be viable preventive measures, but they are disruptive to the flow of data...”¹²
- 3) **Comprehensive protection is an ever-moving target.** Business processes change and new points of vulnerability appear continuously.⁸

For these reasons, it is wise to plan for data loss even when a strong DLP implementation is in place. The Web site of Code Green Networks offers eight steps for a successful DLP implementation—and five of the eight steps listed focus on what to do when prevention is not successful and a security breach occurs.¹³

Attention must be paid both to preventative measures as well as planning for instances when prevention doesn't work and data loss occurs.

This is indeed an intelligent approach—attention must be paid to preventative measures as well as planning for instances when prevention doesn't work and data loss occurs.

A comprehensive security plan should include methods for helping enterprises minimizing the impact of data loss by enabling forensics that can improve the accuracy and efficiency of investigations and, in the long run, act as a stronger deterrent to the unauthorized use of sensitive data.

Approaches for Addressing Data Loss

The following paragraphs examine several alternatives for addressing the event of data loss, including using algorithms that can help pinpoint the source of leaks, conducting post-mortem searches of logs and proactively embedding intelligence capabilities into content itself to support data loss discovery and intelligence.

Stanford University: Applying Mathematics to Identify the Source of Data Leaks

Two researchers at Stanford University (Papadimitriou and Garcia-Molina) authored a study on algorithms for identifying who, among authorized business users of information, is the most likely source of a data leak. The premise of their work is that organizations must collaborate with third parties "that may not be 100% trusted...and certain data cannot admit watermarks."¹¹ (Third parties are referred to as "agents" in their study.)

Their goal was to "explore non-obtrusive techniques for detecting leakage of a set of objects or records...where the owner discovers some of the objects in an unauthorized place (Web site etc.) and the problem is to pinpoint who leaked it."¹¹ In other words, the researchers acknowledge that data loss is inevitable, and that there is an acute need to balance security concerns against the need to conduct business without disruption. The researchers make an important observation:

"There are also lots of other works or mechanisms that allow only authorized users to access sensitive data through access control policies. Such approaches prevent, in some sense, data leakage by sharing information only with trusted third parties. However, these policies are restrictive and may make it impossible to satisfy [agents'] requests."

Their research shows it is possible to assess the likelihood a particular third party is responsible for a leak using a variety of algorithms including the nonpolynomial guilt model detection algorithm. The research, which was supported by a grant from the U.S. National Science Foundation, represents an important step in aiding digital forensics when data loss occurs.

Digital Forensics in the Field

Business is booming for identity protection firms who are called in to perform investigations after security breaches occur. These firms are proliferating precisely because the problem of data loss has yet to be solved. For example, Kevin Mandia, who runs a security firm specializing in data loss investigations, has responded to serious breaches at 22 companies in the Fortune 100 during 2010 and 2011 alone.⁶ His firm searches for the source of leaks by examining voluminous amounts of the attacked company's data as quickly as possible, including firewall logs, Web logs, and emails. It is a difficult task to weed through unstructured data, and time is of the essence. According to Mandia, "every minute you take to figure this [breach] out, you could be losing more emails and more credit data...the goal is to quickly determine the fingerprint of the intrusion and its scope."

Clearly, if data loss can't be prevented 100% of the time, then there is a critical need for powerful forensics that can drastically speed up these types of investigations, find the source of the leak, plug the holes and minimize the damage.

If data loss can't be prevented 100% of the time, then there is a critical need for powerful forensics that can drastically speed up these types of investigations, find the source of leak, plug the holes and minimize the damage.

Watermarking Technology

Digital watermarking technology has been in use since the mid-1990s to support content management copyright protection and copy control of digital content.¹⁴ A digital watermark carries the signature of its owner, enabling identification and copy control information to travel with the content itself.

For example, the watermarking technology offered by Digimarc® Corporation allows users to embed digital information into audio, images and videos in a way that is imperceptible to the human eye yet persistent and easily detectable by computers.¹⁵ Digimarc was founded by Geoff Rhoads, an astrophysicist with a background in deep space imaging, who developed and patented algorithms that can embed an invisible watermark into images to prove ownership.

As noted in the Stanford University research, watermarking technology has limitations in that, historically, the technology has not been available for all types of data such as PDF files, Microsoft Office documents, medical images and engineering drawings (CAD files). As noted in the next section, InDorse Technologies, Inc. has developed a solution that enables robust watermarking of many of these file types, building upon the technology pioneered by Digimarc.

Data Loss Discovery and Intelligence Technology

InDorse Technologies, Inc. has recently extended watermarking technology to support additional file types commonly used in business, including Microsoft Office documents as well as Adobe PDF files and medical images.

InDorse Watermark™ is built upon watermarking algorithms provided by Digimarc® Corporation. InDorse has built a sophisticated, patent-pending application on top of the Digimarc libraries to process files and extend watermarking capabilities to documents as well as images. Table 2 lists supported file types for InDorse Watermark.

Table 2. Supported File Types for InDorse Watermark

Input File Types	Output File Types*
<ul style="list-style-type: none"> • Microsoft Office (.doc, .docx, .ppt, .pptx) • Adobe .pdf • .xps • Images including .jpg, .jpeg, .png, .bmp, .gif • DICOM medical images (.dcm) 	<ul style="list-style-type: none"> • Adobe .pdf • .xps • Images including .jpg, .jpeg, .bmp, .gif <p>*All output files are in non-editable format.</p>

InDorse Watermark embeds a unique, invisible identifier into the pixels of documents and images. The input file is converted to a non-editable output file. Organizations may optionally add a visible watermark to educate users about ownership to create a stronger deterrent against unauthorized use of watermarked content.

InDorse watermarks are strongly encoded into the processed output files; they are also able to survive change-of-file format and screen capture. In order to destroy the invisible watermark, one must degrade the content to the point that it no longer resembles the original information.

When a watermarked file is shared with third parties and subsequently posted to a public Web site, the InDorse Web Crawler can be deployed to inventory the content of suspected Web sites. If a match is found, the watermark is read to prove ownership. The content owner receives an alert of the

violation with details about the Web site location as well as forensics data, which may help the owner determine how the file ended up at that location.

The operation of the InDorse Watermark is automatic, requiring no additional software on the end-user system. The recipient does not need to download any additional utilities to view the file; PDFs are still viewed in Adobe Reader, .docs in MS Word, etc. Integration of watermarking into a document workflow can be facilitated via Web service, command-line and GUI interfaces that can be set up internally on an intranet, as well as cloud service interfaces. Off-the-shelf plug-ins, scheduled for commercial availability in 2012, include those for Microsoft SharePoint, Microsoft Exchange and Salesforce.com.

Additional Support for Digital Forensics

While the InDorse Watermark addresses the problem of data loss by proving ownership of files, the tag remains passive i.e., one must initiate a targeted search of Web sites to find postings of unauthorized content.

To support proactive data loss discovery and forensics, InDorse has developed a patent-pending, active tagging mechanism, InDorse Call-Home™, which leverages native file elements to transparently track file open activity. Table 3 lists file types supported by Call-Home.

Table 3. Supported File Types for InDorse Call-Home

Input File Types	Output File Types
<ul style="list-style-type: none">• Adobe .pdf• Microsoft Office 2007-2010 file formats: .docx, .xlsx, and .pptx• Microsoft Office 97-2003 file formats: .doc, .xls, and .ppt	Other than embedding a small tag, Call-Home does not change the original file format, nor does it examine its contents.

InDorse Call-Home tags files in sub-second time using a process that is transparent to the end user; no additional software is required on the client. Once files are tagged, the Call-Home Listener in the cloud detects and reports on file opens within the enterprise network or anywhere on the Internet. (In most implementations, the Call-Home Listener resides on an external cloud for infinite scalability; however, some corporations use their own internal cloud for this purpose.)

The Call-Home workflow is as follows:

1. A document is submitted to the Call-Home Enterprise Tagging Server for local processing.
2. The Enterprise Tagging Server sends the filename, retrieves a unique ID (tag), embeds the tag in the file, records the tag's details in the database (which is either local or in the cloud), resaves the tagged file locally.
3. The Call-Home API records details in the Call-Home Activity Database.
4. The tagged document is opened somewhere on the Internet; the document sends a small message (an "open" event) to the Call-Home Listener in the Cloud.
5. The event is pushed to the Call-Home Activity Database. When a user checks for file usage information, the Web site pulls this information from the Call-Home Activity Database.

The InDorse solution gives enterprises significant leverage in promoting accountability among customers and business partners who have access to sensitive information.

When a document “calls home,” file open activity is visually displayed on the Call-Home Activity Map. InDorse also provides Call-Home File Open Activity Reports which display the location and time that the file was opened, providing insight into the chain-of-custody and unauthorized forwarding of confidential data. Call-Home tracks the document’s activity to a network address, physical location, and company name.

Call-Home is designed to preserve rights-to-privacy as it does not read file contents, nor does it expose any personally identifiable information contained with files. InDorse customers may create applications or workflows that choose to associate additional information with a document that has been Call-Home tagged, but that is completely in the control of the customer.

Data Loss Discovery and Intelligence Strengthens DLP

The data loss discovery and intelligence capabilities provided by InDorse products complement and strengthen DLP implementations in the following ways:

- **Data at rest:** Based on classification policies within the organization, data at rest that has been identified as sensitive can be automatically Call-Home tagged or InDorse Watermarked as an action in response to a predefined business rule or policy.
- **Data in motion:** InDorse products can be easily configured to dynamically Call-Home tag and InDorse Watermark files downloaded from email servers such as Microsoft Exchange or document and contact management systems such as Microsoft SharePoint and Salesforce.com to create an additional protective layer on top of the DLP solution. Also, organizations can use their internal proxy server traffic to correlate log data to Call-Home activity to provide a more complete, traceable audit trail of file opens.
- **Data in use:** Call-Home tracks file opens both within the organization and externally, for the life of the file. InDorse Watermark allows organizations to apply actions such as password protection, print restriction and restriction of copying/extracting of PDF content as part of the watermark tagging process.

Revisiting Data Loss Scenarios

InDorse Watermark and Call-Home can be used together to provide data loss discovery and intelligence capabilities to pre-emptively provide powerful forensics information (in near real-time) should a security breach occur, warranting an investigation. These technologies strengthen the degree of control over the IT environment to better support compliance efforts with numerous types of regulations including PCI DSS, HIPAA, etc.

In addition, if the enterprise chooses to inform third parties of the presence of the InDorse Watermark and/or Call-Home tags, this can act as a powerful deterrent to unauthorized use of data. The InDorse solution gives enterprises significant leverage in promoting accountability among business partners who have access to sensitive information.

The following section examines the data loss scenarios discussed previously, with revised outcomes made possible by proactive deployment of InDorse Watermark and/or Call-Home.

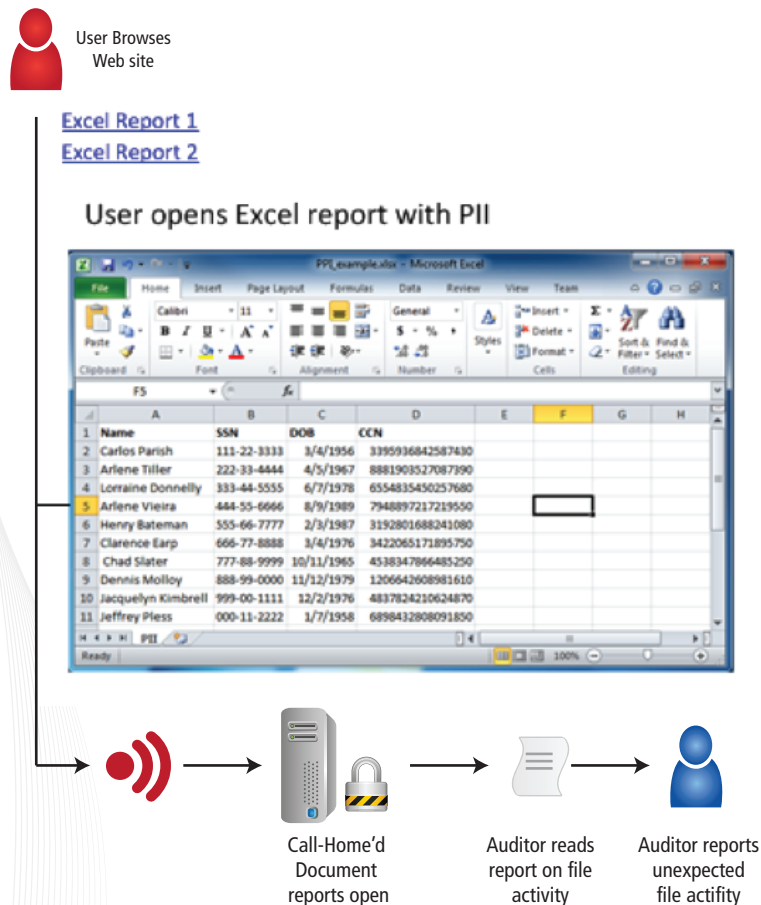
Scenario 1: Hospital Spreadsheet Containing Patient Data Posted to Public Web Site

The hospital implements InDorse Plug-Ins on its Microsoft SharePoint site to automatically Call-Home tag spreadsheets containing patient data, including those destined to be processed by business billing contractors. The hospital informs each outside contractor about these new security measures and requests their Auditors to sign off on periodic Call-Home Activity Reports to validate the legitimacy of file open activity.

One of the spreadsheets containing personally identifiable information (PII) is subsequently posted to a public Web site run by a subsidiary of one of the contractors. When the spreadsheet is downloaded from this site and opened, an unusual amount of file open activity is immediately seen on in the hospital's Call-Home Activity log.

Within hours, the hospital notifies the contractor's Auditor and requests sign off. However, upon inspection, the contractor's Auditor reports the existence of unauthorized file opens. Using the IP address information from the Call-Home Activity Log, the contractor is able to deduce that the spreadsheet was posted in error on its subsidiary's Web site, and it is removed within hours (instead of months!). The hospital is able to avoid substantial fines by showing a timely and proactive response to the breach, as well as proving that preventative measures were instituted to enforce shared liability and hold business contractors accountable for their actions.

Figure 2. Revised Hospital Scenario with Call-Home Tagging



Scenario 2: Confidential Bid Leaked to a Competitor

Suspecting foul play during a highly competitive bidding process, a company proactively tags all confidential bids using Call-Home. The tagging process is completed in minutes. One of the confidential bids is subsequently downloaded to a USB device and given to a competitor. The competitor alters its bid to undercut the company's pricing proposal.

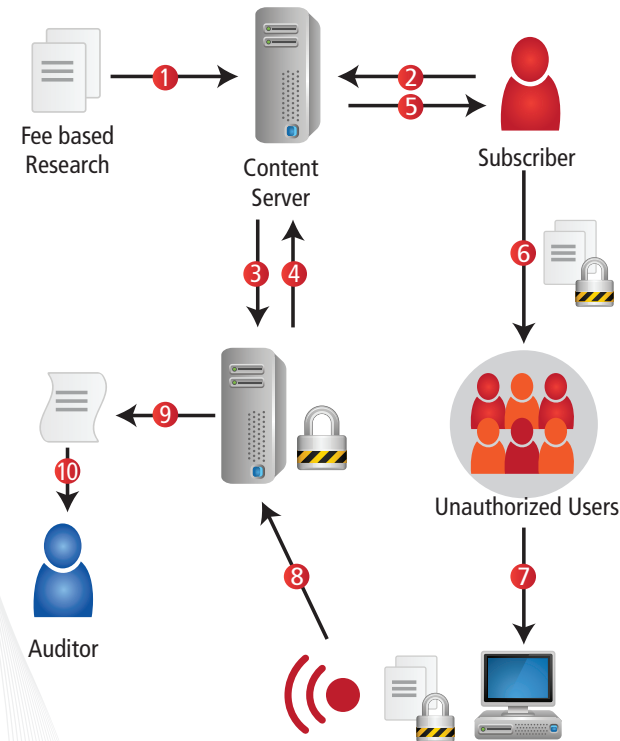
Using Call-Home, the company is able to track this and show it to the client. The competitor is removed from the bidding process and the company is awarded the business, which is worth millions. For more details on this actual case, see http://www.indorse-tech.com/sites/default/files/hh_global_case_study.pdf.

Scenario 3: Fee-Paid Research From a Financial Firm Forwarded to Non-Subscribers

Using the InDorse Call-Home API, the financial services team is able to quickly implement automated Call-Home tagging of all its fee-paid research. The tagging operation associates an encoded subscriber ID plus the document ID with the Call-Home tag.

When research documents are opened, Call-Home records file opens. The company uses the Call-Home Activity data to determine if research documents are being opened from unauthorized locations. Any unauthorized distribution channel of fee-paid research is immediately evident from the Call-Home Activity Map and traceable to subscriber ID.

Figure 3. Revised Fee-Paid Research Scenario



- 1) Paid content report published to Content Server
- 2) Subscriber requests paid content via Web portal or email
- 3) Content Server requests unique Tag ID from Call-Home Server, which sends associated Subscriber ID and Document ID
- 4) Call-Home Server assigns unique Tag ID to document and stores associated Subscriber ID and Document ID
- 5) Content Server embeds Tag into document and sends uniquely tagged report to Subscriber
- 6) Subscriber distributes paid content to unauthorized distribution channel
- 7) Unauthorized reader opens Call-Home tagged document
- 8) Document reports back to Server with Tag ID and IP address of file open
- 9) Call-Home Server generates a report of file open activity
- 10) Auditor sees unauthorized activity associated with Subscriber

Data loss discovery and intelligence solutions provide powerful forensics capabilities should security breaches occur, helping organizations to accelerate investigations and save money.

Scenario 4: Computer Manufacturer's Product Specs Posted on Public Web Site

The Manufacturer decides to take action to secure the company's pre-release specifications from leaking out during the development of its forthcoming product release. At the outset of the next new product development initiative, the company uses InDorse Watermark Server Edition to automatically watermark pre-release specifications to be shared with business partners. The implementation quickly applies a watermark, unique to each vendor, giving the Manufacturer the ability to definitively prove where any leak originates – deterring business partners from sharing sensitive information.

Since implementing InDorse Watermark and advising its business partners of its existence, the Manufacturer reports that business partners have been deterred from sharing sensitive documents and no unauthorized information on the upcoming product release has appeared on public Web sites.

Scenario 5: Anonymous Publishes Credit Card Numbers Online

This scenario is quite challenging and, while it may be impossible to prevent, the use of Call-Home tagging provides an early warning system and additional forensics data for investigators.

The company uses Call-Home to tag all spreadsheets and documents containing credit card data. When Anonymous invades the network, they download as much data as possible and as fast as possible (the typical modus operandi of a hacker). When these files are subsequently opened, the following occurs:

- The Call-Home file open count spikes dramatically in a very short time
- The Call-Home Activity Log reveals that the origin of these events are highly concentrated in a single location, coming from one or just a few "outlying" IP addresses that are external to the company network

Taken together, this indicates a high likelihood of a break-in and provides an early warning to the company's incident response team so they can react quickly. The outlying IP addresses may also prove helpful in tracking down the hackers.

Conclusion

Data loss prevention (DLP) is a necessity in today's world of security threats such as hacktivism, phishing, malware and disgruntled or careless employees. Unfortunately, multiple factors continue to drive up the cost, complexity and risk of DLP implementations, including the consumerization of IT (mobile devices, etc.) and the need to share data with untrustworthy business partners.

Fortunately, new technologies are emerging for strengthening DLP by addressing the inevitable problem of data loss. These technologies are critical as enterprises seek to leverage IT to increase their competitive advantage while cutting operational expenses.

Chief among these new technologies are data loss discovery and intelligence solutions from InDorse Technologies, which provide powerful forensics capabilities, should a security breach occur, helping organizations to accelerate investigations and save money. In addition, InDorse Call-Home provides an early warning of a breach, helping to minimize damage and the financial cost of data loss. By educating end-users and third parties about the use of InDorse products, the solution also acts as a strong deterrent to unauthorized use of sensitive data and helps hold third parties accountable for supporting enterprise security policies by engaging them to proactively protect sensitive data.

InDorse products are designed to be easy to implement and transparent to the end user so they do not disrupt business process and, as a result, improve the success rate of the IT security solution. By embedding the intelligence within the file content itself, the solution is also more readily adaptable to changes within IT infrastructure and business processes. These capabilities can help put enterprises in a stronger position for addressing security threats without disrupting the flow of business, thus enabling them to reclaim the promise of data loss prevention.

References

1. "Data Loss Prevention Market 2010-2014," The Radicati Group, Inc. December 15, 2010.
2. Ouellet, Eric and Rob McMillan, "Magic Quadrant for Content-Aware Data Loss Prevention," Gartner Group Research Note, August 10, 2011.
3. Vijayan, Jaikumare. "Stanford Hospital Investigates How Patient Data Ended Up on Homework Web Site," *ComputerWorld*, September 8, 2011.
4. "HH Global Case Study," www.indorse-tech.com.
5. Gorman, Michael. "Intel Springs Another Leak."
<http://www.engadget.com/2011/12/07/intel-springs-another-leak-mobile-ivy-bridge-cpus-abound/>
6. Perlroth, Nicole. "Finding the Cleanup Crew After a Messy Hack Attack," *The New York Times*, December 29, 2011.
7. "Pioneering a Systematic Information Management Risk Platform," Enterprise Management Associates, December 2007.
8. "Data Leak Prevention," an ISACA White Paper. © 2010 ISACA.
9. "McAfee Data Loss Prevention." *Solution Brief* © 2010 McAfee, Inc.
10. Nachenberg, Carey. "A Window into Mobile Device Security." © 2011 Symantec Corporation.
11. Papadimitriou, Panagiotis and Hector Garcia-Molina. "Data Leakage Detection," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 23, No.1. January 2011.
12. "Protecting Data-at-Rest with SecureZIP for DLP™." © 2011 PKWare, Inc.
13. Peck, I. "8 Steps for a Successful DLP Implementation." © 2011 Code Green Networks, Inc.
14. Morimoto, Norishige, "Digital Watermarking Technology with Practical Applications," *Informing Science Special Issue on Multimedia Informing Technologies*, Part 1, Vol. 2, No. 4, 1999.
15. "Identifying and Managing Digital Media." © 2010 Digimarc Corporation.

About the Author

Jill Huntington-Lee is an independent consultant providing market research and communications services to high-tech startups. Her publications include "Applications for Distributed Systems and Network Management" published by VNR/Thomson, and "HP Openview: A Manager's Guide," published by McGraw-Hill/Data Communications.

About InDorse

InDorse delivers data loss discovery and intelligence solutions that strengthen existing data loss prevention technology. Our unique, award-winning products are rapidly deployable and non-invasive to business processes, leveraging robust watermarks and native file security elements to detect, track and deter unauthorized usage of documents, images and screen captures containing confidential and proprietary information.

For more information, visit www.indorse-tech.com

InDorse Technologies, Inc.
424 West 33rd Street
New York, NY 10001
1.800.610.9210

info@indorse-tech.com

sales@indorse-tech.com

www.indorse-tech.com

© 2006-2011 InDorse Technologies, Inc. All rights reserved. International Patents-Pending. This data sheet is for informational purposes only. InDorse Technologies, Inc. MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS SUMMARY. Other products or services mentioned may be trademarks or servicemarks of other companies.