User Driven Security
5 Critical Reasons Why It's Needed for DLP

TITUS White Paper
At TITUS we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.
# Table of Contents

1.0 | Overview ........................................................................................................................................... 4  
2.0 | The Data Loss Prevention Challenge ................................................................................................. 5  
   | Why do these breaches happen? ............................................................................................................. 5  
   | DLP Solutions: Why They Are Not Enough ........................................................................................... 6  
3.0 | User Driven Security: 5 Reasons Why It’s Needed for DLP ................................................................. 7  
   | 1. Engages end users to actively identify sensitive content ................................................................. 7  
   | 2. Educates users by enforcing corporate policies and providing instant feedback ............................ 8  
   | 3. Improves productivity by enabling users to self-remediate policy violations ................................. 9  
   | 4. Raises awareness of the sensitivity of information by applying visual markings ............................ 9  
   | 5. Enhances DLP by adding metadata tags to email and documents ............................................... 11  
4.0 | The TITUS Advantage ...................................................................................................................... 12
1.0 | Overview

One of the biggest challenges for IT Security departments is the threat of authorized users causing inadvertent data breaches. Confidential data sent to the wrong people can result in embarrassing headlines, lost business, and large financial penalties.

To address this concern, organizations are increasingly turning to data loss prevention (DLP) solutions to protect and control the disclosure of sensitive information. Yet most DLP solutions overlook the most important aspect of security: the user.

In this white paper, we’ll look at five critical reasons why user driven security should be part of every DLP strategy. By involving the user, organizations can complement their existing DLP solutions and dramatically reduce their risk without disrupting business processes and productivity.
2.0 | The Data Loss Prevention Challenge

One of the biggest challenges for IT Security departments is the threat of authorized users causing inadvertent data breaches. It seems that every day we hear of a new major data loss event caused by insiders. Recent examples include:

- In November 2010, UBS AG was dropped as an underwriter for the General Motors IPO role after a UBS analyst sent an email to clients discussing the initial public offering. A similar data breach occurred in 2006 involving Deutsche Bank and the Hertz IPO.
- In April 2010, a Gwent Police employee accidentally emailed a document containing the criminal records checks of 10,000 citizens to a journalist. The journalist was inadvertently added to the distribution list after the email program used “auto-complete” to fill in the recipient name.
- In November 2010, a U.S. General Services Administration employee accidentally sent the names and Social Security Numbers of the agency’s entire staff to a private email address.

Why do these breaches happen?
A number of factors contribute to the problem of data breaches by authorized users, including:

**Large Volumes of Email**
According to an Osterman research report, the average user sends 44 emails per day and receives 123 emails. In just one year, an organization of 1500 users will generate almost 70 million emails. With the addition of other communication methods such as instant messaging and social media, the potential for a data breach is enormous.

**Portable Devices**
Technologies such as wireless internet access and inexpensive portable media have made it possible for employees to conduct business anytime, anywhere. Employees can easily transfer sensitive data to multi-gigabyte USB drives and DVDs, or access documents from laptops or home computers.

**Too Much Information Access**
Excessive access rights are another factor contributing to the problem. A Deloitte survey of top security executives at financial organizations found that that excessive access rights were the top problem identified in audits. With a workforce that is constantly changing due to outsourcing, mergers, and reorganizations, it is difficult to keep track of which users should have rights to which data. In most cases, organizations err on the side of giving too much access, because the alternative – too little access – impacts business productivity.

**Innocent Mistakes**
Today’s employees are often rushed and distracted, with security being one of the last things on their minds. Unfortunately, this lack of awareness can easily result in data breaches that violate any number of regulations, including: SOX, GLBA, BASEL II, PCI DSS, and SEC disclosure rules for financial information;
HIPAA and HITECH for health information; ITAR in the aerospace and defense industry; and various privacy protection legislation such as S.B. 1386 in California, MASS 201 in Massachusetts, PIPEDA in Canada, and DPA in the UK.

**DLP Solutions: Why They Are Not Enough**

To address the challenge of insider security threats, many organizations are looking to data loss prevention solutions. While these technologies go a long way toward detecting and preventing the unauthorized use and transmission of confidential information, they often overlook the most important aspect of security: the user.

When DLP solutions do not include a user driven security component, the following critical gaps exist in the organization’s security strategy:

- **Automated content scanners become the sole method of determining what is sensitive.** Most users know what information is sensitive, especially if they are the originators or owners of the content. However, when users don’t have the tools to identify that a document or email is sensitive, they have to rely on automated content scanners to correctly interpret the information and apply the right protection. This can lead to a high rate of errors, causing the DLP solution to either block non-sensitive data (false positives) or mistakenly release sensitive data (false negatives).

- **Organizations miss out on the opportunity for targeted security training.** Most DLP solutions are not integrated into the user’s email and document applications. Instead, policy decisions are made outside of the application, often at a gateway, with minimal user involvement. As a result, users are not receiving targeted, interactive security messages that help them avoid mistakes in the future.

- **Users are unable to self-remediate policy violations.** Typically when a user sends an email that violates security policy, the email is blocked at the gateway. Rather than being given the opportunity to fix the problem as the email is being composed, the content is simply blocked after the user clicks Send. Not only is this inconvenient for the user, it could have significant financial repercussions for an organization if the email is time-sensitive (such as submitting a bid proposal). Because of this, many organizations put their DLP solutions into “watch” mode only, because they do not want to interrupt business processes and productivity.
3.0 | User Driven Security: Why It’s Needed for DLP

User driven security is a critical component of any data loss prevention strategy. By involving users up front, organizations can dramatically lower their risk and increase the effectiveness of their security program.

A user driven security solution includes five key capabilities for an effective data loss prevention strategy:

1. **Engages end users to actively identify sensitive content**: Allows end users to identify sensitive content in email and documents, rather than relying solely on automated content scanners.

2. **Educates users by enforcing corporate policy and providing instant feedback**: Enforces policy within the application so that users receive targeted, interactive education that does not disrupt their workflow.

3. **Improves productivity by enabling users to self-remediate policy violations**: Enables users to self-remediate policy violations through options such as editing the content, redacting sensitive sections, and removing unauthorized recipients.

4. **Raises awareness by applying visual markings**: Adds visual markings to email and documents so that internal and external recipients know how to handle the information.

5. **Enhances DLP by adding metadata tags**: Adds metadata tags to email and documents to enable DLP solutions to make better policy decisions.

Let’s examine the benefits of each of these capabilities.

**1. Engages end users to actively identify sensitive content**

In many cases, users know exactly which information is sensitive and how it should be handled. This knowledge is based on the user’s familiarity with the subject matter, something that is not easily duplicated through automated content scanning.

A user driven security solution enables the information author or owner to clearly identify that an email or document is confidential and needs to be handled appropriately. There are several ways to do this, but the most common method is to prompt the user to select from a list of pre-configured categories before they can send, save, or print an email or document. For example, a user may be prompted to indicate whether the information is “Confidential”, “Export Controlled”, or “Attorney-Client Privileged”. The picklist choices are completely customizable by the solution administrator, and can range from a very simple dropdown list to a more advanced, hierarchical classification scheme.
By enabling users to identify information sensitivity, the organization does not have to rely solely on automated content scanning to determine what is sensitive. The originator, who knows the content best, can pro-actively indicate that the information is sensitive, without having to take a chance that the DLP content scanning engine will categorize it correctly.

2. Educates users by enforcing corporate policies and providing instant feedback

Educating users about security policy is one of the biggest challenges in any organization. The organization can hold regular employee training sessions, publish lengthy policy documents, and develop security experts within each business team – but ultimately, the end user is going to be making day-to-day security decisions on their own without consulting these resources.

Ideally, users should be educated as they perform their daily activities, with frequent policy reminders that are non-intrusive and relevant to their current task. Because so much sensitive information is stored and shared through documents and email, it makes sense to educate users directly within the email and document applications that they use each day. A user driven security solution will do exactly that; it is integrated into the email and document applications to provide policy education before the users sends, saves, or prints the information.

Here are some examples where a user can be alerted to security policy violations before the information leaves the desktop:

- Inadvertently sending an “Internal Only” document to external recipients via email
- Sending a spreadsheet with personally identifiable information (PII) to a home email account
- Forwarding an email with sensitive client information to unauthorized recipients within or outside of the organization
- Sending a “Confidential” document to a large number of recipients (such as in a “Reply All” email)
In each of these situations, the user can be warned before the information leaves the desktop. The policy warnings are timely and relevant to the user’s current tasks, and provide a highly effective way to educate users about security policy.

3. Improves productivity by enabling users to self-remediate policy violations

In addition to warning users about policy violations, a user driven security solution enables users to remediate any problems themselves. Security violations can be highlighted within the email or document, so that users have an opportunity to fix the problem from within the application.

Self-remediation options include the ability to:

- Remove unauthorized recipients before an email is sent
- Redact (i.e. black out) content so that sensitive information is removed, but the overall structure of the email or document is preserved
- Edit or remove the sections that have been identified as sensitive

Self-remediation provides several benefits to the organization. First, it is less disruptive because it enables users to fix problems themselves, without having to wait for a separate application (usually at the gateway) to determine whether the information can be released. Instead, users can see exactly which sections may violate security policy, and can self-remediate as required.

Self-remediation can also give users the ability to override security warnings in the case of false positives (provided the organization allows this option). False positives are one of the major challenges with DLP solutions. With a user driven security solution, users can assess whether a security warning is valid or not, and if necessary, override the warning to enable the flow of valid business communication.

Finally, self-remediation puts accountability on the user. All warnings and overrides can be logged, which means organizations can easily identify areas of concern, such as employees generating high numbers of warnings and overrides.

4. Raises awareness of the sensitivity of information by applying visual markings

After a user identifies the information sensitivity of an email or document, a user driven security solution can automatically add visual markings for increased security awareness. These markings are defined by the organization, and can be placed in the document header, footer, and/or watermark, or in the email message body and/or subject line, as shown below:
A significant benefit of visual markings is that the security instructions are visible to all recipients, including recipients outside the organization. The visual markings become part of the email and
document, and the recipient does not need any special software on their end to see the markings. For example, a large organization may work with several sub-contractors on a confidential project. The sub-contractors need to follow the same regulations as the larger organization, but may not be as well-educated on the rules as the prime contractor. A user driven security solution enables the originator to automatically include handling instructions, such as “Export Controlled” or “Confidential”, at the top and bottom of the email or document. This puts accountability on the recipient to handle the information appropriately.

5. Enhances DLP by adding metadata tags to email and documents

In addition to visual markings, a user driven security solution also creates metadata within the email or document. This step is completely automated, and is triggered by the user’s selection of a classification category for the email or document. For example, if a user selects “Confidential”, this value will be stored as metadata in the standard document or email properties.

This user driven metadata helps DLP solutions make more intelligent policy decisions. Most DLP solutions can read metadata in documents and email, and make policy decisions based on the metadata values. Here are some scenarios where this metadata can be used:

- Block users from copying documents to USB drives when the document contains the metadata value “SECRET”
- Automatically encrypt email at the gateway when the email has the metadata value “Personally Identifiable Information”
- Prevent the upload of documents to external websites where the document contains the metadata “Internal Only”

As mentioned previously, one of the benefits of a user driven security solution is that organizations do not have to rely solely on a content scanner to determine what is sensitive. Instead, users are able to identify sensitive documents up front. With the ability to add metadata, the user driven security solution easily integrates with DLP solutions to provide the best of both worlds: automated scanning combined with user knowledge of sensitive content.

Complete your DLP solution

A user driven security solution provides several critical components for an effective data loss prevention strategy. Most importantly, users become key partners in identifying sensitive content, raising security awareness, and remediating policy violations. When combined with a DLP solution, the result is a dramatic reduction in the risk of inadvertent data leaks from authorized insiders – all without compromising business productivity.