



Fulfilling the Vision of True Information Security:

*How a dynamic contextual approach ensures tight security
over an entire enterprise information life cycle*

Executive Summary

Situation: The Accidental Leak of Sensitive Business Documents Increases Both Risks and Costs

Enterprise Chief Security Officers (CSOs) face a myriad of challenges in protecting their organizations' most confidential business documents as they flow inside and outside of the firm. In addition to the arduous task of identifying where these documents reside, CSO challenges are compounded as users increasingly define their own workflows by exchanging documents via email or other user driven collaborative means.

When leaks do occur, the release of confidential information can cost an enterprise tens of millions of dollars in potential litigation expenses, poor public relations, high regulatory penalties, cancelled contracts, or lost business opportunities.

Problem: Existing Solutions Use Static Security Methods That Ignore Information Relationships/Needs

Everything in an organization changes over time, especially with items pertaining to sensitive information, such as the people working with it, the customers and partners that receive it, even the assigned security classifications for it. What is not considered confidential today may be confidential tomorrow.

When a document is designated as 'confidential', it is difficult to know at that time how future situations and needs will change that designated level of security. There is a risk that the user may assign the wrong security level or designate one that insufficiently encompasses all user access rights over time. Even worse, they may fail to assign any security to the document altogether, increasing the risk of an information leak. Existing security solutions that focus on one part of the information context, either the user or the document, often ignore these issues by assigning security designations that are assumed static.

Solution: A Contextual and Dynamic View of Information Based on Relationship and Need Over Time

Sensitive business information doesn't exist in a vacuum, and the situation(s) in which that information is considered 'sensitive' change over time. Circumstances such as dynamic business relationships; how the information is being used; and newly installed security rules, policies, procedures, and protocols require security management to adapt to changing conditions as they occur.

To fully secure confidential information, a security solution must consider the context of the situation and the relationship of the information to the circumstances, additional parties, and communication methods with designated recipients. By enacting a security strategy based on context and relationship, as opposed to the methods currently available, the enterprise can eliminate the malicious or accidental leakage of sensitive business information caused by human errors. For a security solution to accomplish this, it must be able to easily update information security strategies and tactics over the course of the entire life cycle of a document while taking into account the variables of context and relationship with both internal and external users.

Result: True Collaborative Security Without Data Leaks or Disruptions Over an Entire Life Cycle

TCG SecureZone provides the highest level of security for the most sensitive documents within the enterprise where any possibility of leakage must be completely eliminated. With the TCG SecureZone solution, CSOs can insure their most sensitive documents never leave the organization without proper authorization, a concept we call residency. In addition, CSOs can model the dynamic relationship between the underlying business processes and the levels of access to sensitive information users should have both within the firm and when sending information out of the firm. As that relationship evolves, whether it is by the user's role changing within the organization, evolving information security policies or changes to the recipients of sensitive documents, SecureZone automatically modifies the level of security accordingly.

The Goal: Achieving True Enterprise Information Security Without Workplace Disruptions

For enterprise CSOs, securing highly sensitive corporate documentation related to financial and stockholder information, intellectual property, employee health records, and strategic planning issues are more important than ever.

Given the ease with which users can circumvent existing security protocols, referred to as “information leakage,” many enterprise organizations face severe and costly repercussions for their failure to effectively secure sensitive information and prevent its unauthorized distribution.

In a recent survey conducted by industry research firm InsightExpress, over 200 enterprise end users and IT professionals were polled on the issue of information security. The results from the survey identify several high-risk behaviors that are often associated with information leakage:¹

- **Unauthorized Application Use:** 70 percent of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies’ data loss incidents.
- **Misuse of Corporate Computers:** 44 percent of employees share work devices with others without supervision.
- **Unauthorized Physical and Network Access:** 39 percent of IT professionals say they have dealt with an employee accessing unauthorized areas of a company’s network or facility.
- **Remote Worker Security:** 46 percent of employees admitted to transferring files between work and personal computers when working from home.

As a result of these information leakage events, the potential exists for tens of millions of dollars in increased litigation expenses, diminished public relations effectiveness, regulatory penalties, cancelled contracts, or lost business opportunities because sensitive enterprise information accidentally finds its way outside the firm and into unscrupulous hands due to lax information security policies and behaviors.

While some of these instances are malicious, most are due to accidental breaches of information via inappropriate document sharing and inadequate controls that fail to manage updated user roles and access rights over time. Unfortunately, this situation is the direct result of enterprise information security solutions that require users and systems to analyze and assign security on an *item-by-item* basis. When all forms of information distribution (emailing, copying, storing, etc.) are analyzed, the process of completely securing every piece of sensitive information under each usage scenario and across an entire global enterprise becomes an extremely challenging task.

As enterprise CSOs implement tighter security measures designed to thwart inappropriate information sharing, they also risk negatively impacting workplace productivity. By deploying solutions that impose strict employee controls over information use, they also increase the risk of creating an environment that stifles workplace communications.

Given these requirements, enterprise CSOs need a new approach to information security that protects the most sensitive corporate information on a **context and relationship** basis. Such an approach would ensure tight security but also allow employees to share sensitive information with appropriate parties internally and externally when the context of those business relationships warrants such action.

This white paper will show enterprise CSOs how a contextual approach to document security fulfills the vision of true information security while also protecting sensitive corporate information, without imposing restrictive employee requirements that diminish or disrupt workplace productivity.

¹ Source: Cisco Systems white paper, “*Data Leakage Worldwide: Common Risks and Mistakes Employees Make*,” June 2008

The Problem: A Static Approach to Information Security

Whether a breach of sensitive information is the result of an accidental or malicious act, the fact that a confidential document can bypass an established security system is the direct result of the 'static' approach that many of these solutions use to assess security threats.

Unfortunately, sensitive information doesn't remain static for very long. Business situations, partnerships, communication needs, and contract requirements change over time, especially with sensitive information. This includes the people working with it, the customers and partners that receive and read it, even the security classifications that are applied to it. What is not considered confidential today may be confidential tomorrow.

The failure to assign appropriate security designations either increases the probability of an information leak, or creates severe restrictions that stifle workplace communication and productivity.

Current solutions that allow a document to be marked as 'confidential' are hampered by the challenge of knowing at that time how situational changes impact future information security needs. If a user is required to assess/assign the tags, there is a risk that he/she may assign the wrong level of security, or use one that fails to encompass those access rights over time. Even worse, they may fail to assign the most appropriate security designation or fail to assign security altogether. If a systematic rule is used to mark the document, it will flag any document that follows that rule leading to a high rate of false positives and false negatives. The current solutions available today force CSOs to operate at either end of the security spectrum, resulting in lax security protocols that increase the probability of an information leak, or worse, creates severe restrictions that stifle workplace communication and productivity.

Worse yet, many existing information security solutions might identify a document as confidential but do little to actually secure the document and prevent unauthorized copying or distribution. In addition, these solutions do not take into consideration the subsequent situational, relational, or contextual changes that take place with sensitive information over the course of a typical working relationship.

The vast majority of existing information security solutions employ a static approach and have a unique set of advantages and disadvantages that ultimately impact enterprise security readiness. These solutions fall into three categories: **Tagging, Searching, and Digital Rights Management (DRM)**.

1. Tagging

Tagging security solutions require a user or system to assess a document's security level and assign a security designation that allows, restricts, or prevents specific actions associated with that information. These tags can be visual, such as a watermark placed within the document background, or as descriptive information within the header of the document that alerts the user of its security restriction. Tags can also be generated by a central security system that prevents specific actions such as emailing, copying, saving, or storing the document to unauthorized locations. As a result of the need for additional security policies surrounding document sharing, tagging has been found to be a less effective approach to information security that also increases the opportunity for leakage.

Tagging Advantages:

- **Data Categorization** - Security tags can be created in accordance with existing policies and individual levels of security can be assigned for each data category.
- **Ease of Implementation** - Procedures for the use of security tags can be quickly established, assigned, and implemented for all documents that have been designated as 'confidential'.
- **Simple Training** - Intuitive dropdown menus can be integrated into common applications that easily assign document security designations without the need for time-consuming or costly training.

- **Change Management** - Tags automatically change when security policies change, globally modifying existing security levels and the corresponding tagged documents. The new security tags remain with the document whenever and wherever it is moved.

Tagging Disadvantages:

- **The Human Factor** - Tagging solutions rely on users to assess security levels, then tag and inspect the documents to ensure that the tags have been properly assigned and fully enabled. Since the term "confidential" is often subjective, users may either not assign an appropriate security tag to the document, or select the wrong tag for the intended recipients. These mistakes eventually lead to greater errors and a higher likelihood of information security breaches.
- **Limited Application Support** - Applications must be modified to accept the plug-in modules that enable security tagging. Currently, these applications are limited to the most commonly used office productivity solutions, and exclude many specialty files such as graphics, design layout, and/or CAD. In addition, subsequent application upgrades can cause incompatibilities with plug-in modules causing security disruptions until a compatible update is made available.
- **Misdirection of Information** - Employees who use older documents as templates for new business projects often end up distributing classified information to unintended recipients associated with the original document. Unfortunately, tagging solutions cannot alert administrators of this misuse, resulting in one of the leading causes of accidental information leakage and security breaches.

2. Searching and Indexing

Searching technologies systematically scan all documents that reside on an end-user's machine or flow through the corporate network. These technologies use sets of rules to flag or otherwise suggest that a document may contain sensitive information. Searching may be a good first step towards an effective security safety net, but by itself, it is an incomplete solution since sensitive documents frequently do not get flagged while other, public documents often become quarantined.

Searching Advantages:

- **A Noninvasive Nature** - The security tools work in the background, automatically scanning for inappropriate uses of sensitive information, without requiring users to execute manual security tasks.
- **Leveraged Learning** - Rules can be improved over time based on prior security breaches, allowing administrators to learn, modify, and create new rules that enable stronger security policies.
- **Fact-Finding Capability** - The details of flawed business processes are illuminated, showing security administrators where and how users are using and storing sensitive information.
- **Solution Integration** - Searching can be combined with other security solutions (such as tagging) to form a more secure safety net for sensitive information.

Searching Disadvantages:

- **High Administrative Costs** - Administrators must frequently update search criteria to accommodate changing business rules and conditions. If the search criteria become too restrictive, they can impede document access and ultimately workplace productivity.
- **Static Human Assessments** - Determining the most appropriate rule sets requires balancing security and productivity. Too many rules or the assignment of incorrect assessments results in productivity disruptions. Too few (or ineffective assessments) and information leakage occurs. For many enterprises, finding this perfect balance is often unattainable.
- **Greater 'False Positive' Assessments** - Searching is often a 'hit and miss' proposition, resulting in sensitive documents that do not get flagged, or public documents that are quarantined. These mistakes are referred to as '*false-positives*'. As a result, many man-hours must be spent re-analyzing and re-assigning the missed and/or misclassified documents in order to update the security rule sets.

- **Post-Occurrence** - Newly established rules are based on problems that are uncovered after a security breach has already occurred, exposing the organization to costly fees, penalties, and litigation.
- **Lack of Intelligent Assessments** - Searching cannot determine whether a specific security breach was malicious or accidental, and cannot assess the relationship between the breached information and the intended recipients.

3. Digital Rights Management (DRM)

Digital Rights Management assigns authorized users with software-based “security keys” that provide access to classified information. DRM security keys remain with the information and can be assigned to a single user or a group of users. However, these keys must be synchronized with the central policy server within a certain period of time or the documents will not open.

DRM Advantages:

- **Data Relocation** - DRM allows key holders to move sensitive documents to various locations without triggering a security breach.
- **Key Expiration** - Security keys can be assigned expiration dates, rendering them ineffective once the date has lapsed.
- **Ease of Administration** - Security administrators can create new rules or modify existing policies to automatically update existing security keys that have been distributed to users.
- **Integration** - DRM can be integrated with other security technologies such as smart cards or biometrics.

DRM Disadvantages:

- **Application Management** - DRM requires the use of a separate application manager that keeps a record of the assigned security keys. Only the most popular office applications are supported under the manager, which must be updated along with third-party application updates.
- **Impact on External Users** - Users outside of the organization must first download and install additional software components, such as plug-ins and enhancements, before they can access confidential documents. Third-party software applications that have not been verified or approved by the IT department may not work with the application plug-ins.
- **Managing Scalability** - Maintaining an accurate accounting of assigned security keys can present a distinct management challenge once hundreds or thousands of keys have been distributed to internal and external users.
- **Split Policy Challenges** - Splitting policies (creating new/additional security policies from existing ones) requires reclassifying thousands of stored documents. Besides being extremely tedious, such a change makes it difficult to determine who should or should not have access to one or both of the new classifications.

Problem Assessment Summary

Each information security solution has its own set of advantages and disadvantages, but when it comes to truly protecting the most sensitive information within the corporation; traditional approaches often fall short in providing complete security from security breaches and information leakage.

To date, the goal of achieving complete information security has been elusive for many enterprise CSOs. To enable complete security for all sensitive/confidential documents, the CSO needs an information security solution that addresses the dynamic nature of information on a contextual basis and changes as designed parties/roles change. Second, the solution must also provide tight security without restricting user productivity and/or workplace communication. Finally, this solution must be compatible with existing application solutions that have already been deployed throughout the enterprise.

The Solution: A Dynamic, Contextual Approach Over an Entire Information Life Cycle

Confidential business information doesn't exist in a vacuum, and the circumstances in which that information is considered 'sensitive' change over time. While certain criteria may warrant such a label on one particular day, the criteria will ultimately change, requiring an entirely different security classification down the road.

This concept — *the context of sensitive content* — is what most traditional information security solutions lack. Each document has a purpose, and the business units that are responsible for the security of sensitive information must constantly be aware of the context and relationships of that information. This includes where that information is being sent, the individuals with whom it is being shared, and the need to communicate it over time.

To enable enterprise information security, a solution must incorporate these three elements related to the context and relationships of confidential information. By deploying solutions that support this strategy, enterprise CSOs can eliminate human errors that result in needless security breaches and the accidental distribution of sensitive business information.

Each document has a purpose, and the business units that are responsible for the security of sensitive information must constantly be aware of the context and relationships of that information.

TCG SecureZone is an enterprise-class information security management system that applies a unique approach to the distribution of classified corporate information based on the contextual and collaborative relationship between the owner and the recipient, and the need to communicate that information between those two parties. SecureZone incorporates a centralized model based on this context and relationship strategy that reduces document entitlements and provides a full range of data protections. With SecureZone, confidential documents remain secure and never leave the organization without proper authorization. Users are provided secure virtualized access to these documents, and can only email these documents as secure attachments to authorized recipients. Using this approach, complete control over the most sensitive information within the enterprise is assured.

The TCG SecureZone solution comprises four key principles that represent a unique view of enterprise information security:

1. **Simplicity** - Protecting sensitive information must be seamless to the end user so that the impact on their day-to-day activities is minimal.
2. **Residency** - Documents are stored in a central repository and accessed virtually by end-users. This design approach insures that sensitive information never leaves the organization without proper authorization.
3. **Automation** - Document entitlements are governed by their location in the repository. User feeds are used to monitor end-users rights based on their role in the company so that Information Barriers can be enforced as well as automatic de-provisioning of rights should the user leave or change roles within the organization.
4. **Reporting** - A complete and accurate accounting of each sensitive document, including usage history, user names, access dates, access times, distribution locations, and administrative changes can be quickly and easily accessed upon request by an authorized user.

How TCG SecureZone Provides Security Based on Context and Relationship

TCG SecureZone fulfills these essential enterprise information security principles by employing five critical solution attributes:

1. **Modeling Content Storage and Entitlements** - Applying the concept of "*the need to communicate*," SecureZone assigns security based on the relationship between information and users, and the need to access that information. With SecureZone, entitlements and security policies are applied to shared data structures where information is stored based on user's roles and the need to communicate that information. When a structure is created, an appropriate level of security is also automatically assigned to the structure, based on the policies that have been modeled for that structure.

2. **A Secure Central Repository** - All documents are stored in a highly secure central repository, which ensures that they will not be mistakenly distributed outside of the enterprise. When the documents from the central repository are opened, corresponding applications are also launched from the repository/server instead of from the user's local hard drive. This methodology ensures that the user never has access to the physical documents, eliminating any possibility that they can be copied (to a USB device, DVD, memory stick, etc.) or removed from the repository without authorization. This also eliminates any possibility of an accidental information breach, since the document always remains in a secure central location.

The user never has access to the original native documents. This eliminates any accidental information breach, since the document always remains in a secure central location.

3. **Virtualized Document Access** - TCG SecureZone provides users with references to documents within the secure repository. These references appear as standard documents in the local file system and end-users use them as such. However, the document reference is only a link to the actual document which always remains secure inside the protected repository. With appropriate authorization, the document references will open a corresponding native document using applications that are located in the central repository, rather than using applications located on the user's hard drive. Once a repository document is opened in a virtualized session, SecureZone controls how information can be copied, pasted or printed.

Document references are also used when sending email internally or externally. When end-users attach a document reference to an email, the TCG SecureZone Misdirected Email Guardian insures that the recipients listed on the message are authorized to receive this content.

The advantage of interacting with these document references ensures that unauthorized access to sensitive information is strictly controlled (such as moving it from a secured to an unsecured environment). Also, these references can be assigned an expiration date. Once that date has passed, the reference documents are rendered inoperable, providing an additional measure of security for the physical file.

4. **Seamless User Experience** - SecureZone does not require users to re-learn new security techniques or alter the manner in which they work with sensitive information. Reference documents appear like their physical counterpart to the end-user and access to them is presented through a familiar Windows Explorer interface. Existing information security solutions already deployed within the enterprise can coexist with SecureZone, creating an even greater level of security for all or specific enterprise departments.

5. **Comprehensive Auditing and Reporting** - SecureZone keeps track of all access and use of secure documents, creating a detailed audit trail for each document. This auditing capability acts as a conduit between companies and departments that use sensitive information. Auditing not only prevents accidental security breaches from occurring, but it also provides valuable information that can help

improve future security policies and protocols. More importantly, this auditing function eliminates the unfortunate situation of incurring a security breach to learn where security leaks exist.

SecureZone Solution Summary

TCG SecureZone provides the highest level of security for the most sensitive documents within the enterprise, where any possibility of leakage must be completely eliminated. This ensures true information security without the complex nature and technical challenges associated with static information security solutions. While TCG SecureZone is a comprehensive solution, it can also complement existing information security mechanisms currently in place, thereby improving overall enterprise security capabilities.

TCG SecureZone provides the highest level of security for the most sensitive documents, where any possibility of leakage must be completely eliminated.

TCG SecureZone security software was built specifically to address the dynamic relationships and context of information, providing a more intuitive and more secure environment over the entire life cycle of that information. As these conditions change, the security level associated with the information automatically changes as well providing a comprehensive solution to addresses tomorrow's information security challenges as well as today's.

Bottom Line: The TCG SecureZone virtualized environment enables users to have full access to information (with proper authorization) from a central secure repository, providing a truly secure business environment. This level of control leads to a more secure information environment without complex user requirements that impact essential workplace productivity and/or communication.

Concluding Summary

Solving the challenge of enterprise information security can no longer be based on an arbitrary level of perceived confidentiality or determined after a security breach occurs. The risks and costs associated with the accidental release of sensitive business information are simply too great.

While existing security solutions, such as tagging, searching and DRM have specific benefits, they apply a static approach to information analysis that relies too much on user intervention. This ultimately leads to a greater number of human errors that result in accidental security breaches of sensitive information.

CSOs must now take a dynamic, contextual view of their sensitive information that is based on the need to communicate information along with an ability to manage that information over its entire life cycle. They must also take into account how sensitive information is exchanged both within and outside of the organization.

TCG SecureZone is a confidential information management system that balances the need for greater information security with the need to maintain appropriate controls for the secure collaboration of sensitive documents inside and outside the firm. This is enabled without requiring extensive user intervention, training, or re-learning of new security methods. With TCG SecureZone, information leakage of an organization's most sensitive documents is eliminated without interfering with day-to-day information workflow and user productivity.

In summary, the TCG SecureZone approach to dynamic, contextual information security provides many advantages over existing solutions like Tagging, Searching/Indexing and DRM including:

- ❖ **Greater Security** - TCG SecureZone is based on information context and relationships, which provides a greater level of security and increases the confidence that sensitive information is fully secure.
- ❖ **Improved Control** - TCG SecureZone provides a true information security solution without relying on human responsibilities to assess threats and/or assign security levels.
- ❖ **Comprehensive Balance** - TCG SecureZone balances security and efficiency in a seamless operating environment that does not require users to learn new procedures to administer information security, thereby ensuring uninterrupted workplace productivity.
- ❖ **Facilitated Security Management** - TCG SecureZone provides a seamless approach that facilitates the management of security policies over the complete life cycle of information without the need for additional software plug-ins, security keys, or complex user training/procedures.

If your enterprise is evaluating a security solution to prevent the leakage of sensitive business information, and would like to control, monitor, and enable a more secure collaborative environment with your customers, partners and constituents, please contact us to arrange a demonstration of the TCG SecureZone information security solution.

For more information please visit the corporate website at www.tcgsecurezone.com, email sales@tcgsecurezone.com or call (646) 502 - 8778.



41 E. 11th Street
11th Floor
New York, NY 10003
(646) 502 – 8778
www.tcgsecurezone.com

© 2009 The Confidentiality Group, LLC. All rights reserved.