



A Websense® White Paper

# Justifying Data Security: An Investment in Competitive Advantage

## Introduction

Locks on doors do not protect sensitive data. Security measures intended to keep the outside world at bay do little to protect organization's data from internal leaks. Eighty-one percent of data loss comes from unintentional, internal leaks, according to a study by the Ponemon Institute. Yet, few businesses take action, even after a data loss incident has occurred. Most return to business as usual, exposed, even after information has undeniably and damagingly leaked.

The pressures of the contemporary climate have made the need for data loss prevention (DLP) solutions evident. Leaving internal data exposed has profound consequences. A data leak can cost a company its competitive advantage, disrupt operations, and compromise both regulatory compliance and corporate governance.

Complicating the operational environment while heightening the need for a DLP solution, regulatory compliance mandates what would otherwise simply be sound business practice. Control-oriented regulations such as the Sarbanes-Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the USA PATRIOT Act of 2001 require both the protection of information and the ability to demonstrate accountability through clearly documented and enforceable business policies and procedures.

For process improvement, regulatory compliance, and competitive advantage, DLP solutions are a vital part of securing internal data. The volume of communication that occurs through the normal course of business precludes exclusive reliance on human monitoring and protection. Automated solutions accelerate the effectiveness of security controls while helping to maintain regulatory compliance. Advances in DLP solutions have made it possible to flag and contain data that should remain inside the organization, and implement automated incident controls that integrate with existing business processes.

## Table of Contents:

The Challenge .....	3
• Risk .....	3
• Compliance .....	3
• Operational Efficiency .....	3
• Competitive Advantage .....	4
Secure Information and Pursue the Growth .....	5
Conclusion .....	6

## The Challenge

Competitive pressures and government intervention have reshaped the competitive landscape. While businesses have been slow to adopt internal data loss prevention measures, market and regulatory activity are making it unavoidable. The business community has been slow to respond to leaks, despite the flurry of attention they get in the press and new motions for regulatory controls. Plugging leaks is important, but an investment in data loss prevention delivers value beyond leak prevention itself. Ancillary benefits, such as streamlined operations and return on investment (ROI), result from DLP implementations.

In order to deliver a compelling ROI case and improve operations and competitive positioning, a DLP solution should focus on:

- Risk management
- Regulatory compliance
- Operational efficiency
- Securing a competitive advantage

### Risk Management

The management of risk relies on information control. Data loss could put sensitive information into the hands of competitors, cost credibility with clients, and lead to remediation expenses—from compensating damaged parties to the implementation of security measures and governance frameworks to prevent future loss incidents. Risk reduction essentially helps a company to safeguard revenue through the prevention of loss due to error or negligence. Keeping information in the enterprise implicitly adds top- and bottom-line revenue without a corresponding cost of sales.

### Compliance

While revenue recapture through risk mitigation is not mandatory, regulatory compliance is. A wave of legislation including HIPAA, USA PATRIOT Act, and SOX require the implementation, documentation, and auditability of information controls. This trend shows no signs of slowing, as state breach notification laws are spreading rapidly, and new legislation is being proposed in Congress. Process redesign is an essential component of regulatory compliance, and the rigor that auditors expect to find through the course of compliance remediation can be difficult to create without the use of workflow solutions to provide a platform from which to comply. Data loss prevention solutions provide consistent, documented controls with the predictability that auditors expect to find when evaluating a control system.

### Operational Efficiency

Through the mitigation of risk and implementation of controls for compliance, it is possible to derive additional business benefit. These measures require substantial operational changes, affording the opportunity to implement further change without disruption. Data loss prevention measures can be accompanied by enhancements to data center architecture, refinement of employee communication protocol, and even realignment with go-to-market strategy to improve business performance. Protective measures do not have to be purely defensive; data loss prevention can be used proactively to advance the objectives of the business, creating new and lasting operational efficiencies.

## Competitive Advantage

Ultimately, every business seeks a competitive advantage. For the data-driven company, information protection and DLP increase the value of sensitive information and deliver a foundation for aggressive growth. The cost reduction associated with data protection and process improvement free operating capital for investment in growth opportunities. Instead of reacting to data loss events, funds can be redirected to initiatives that will attract clients, increase sales, and otherwise advance the business. Once sensitive information improperly leaves the company, its value is decimated—along with the competitive advantage that it offered.

### Information Type

<b>Customer Information</b>	<b>Example</b> <ul style="list-style-type: none"> <li>• PII (Personally Identifiable Information)</li> <li>• NPHI (Non-public Health Information)</li> <li>• Customer preferences</li> <li>• Order history</li> </ul>
<b>Intellectual Property</b>	<b>Example</b> <ul style="list-style-type: none"> <li>• Product specifications and design details</li> <li>• Market research results</li> <li>• Focus group minutes</li> </ul>
<b>Confidential Information</b>	<b>Example</b> <ul style="list-style-type: none"> <li>• Sales plans</li> <li>• Distribution plans</li> <li>• Product roadmaps</li> <li>• Financial statements</li> </ul>
<b>Regulated Information</b>	<b>Example</b> <ul style="list-style-type: none"> <li>• PII</li> <li>• NPHI</li> <li>• GLBA</li> <li>• HIPAA</li> <li>• SOX</li> <li>• SB-1386</li> <li>• PIPEDA</li> </ul>

The loss of data has the potential to change a business completely, especially in a business climate characterized by increasing competition and rapid product obsolescence. Most leaks are completely preventable through the implementation of DLP solutions and corresponding governance models, which can be used as the backbone of improved operations to reduce risk while delivering a competitive advantage. Even though these solutions are not a panacea, they can be the hub of an information control program that helps to recapture the initiative in the marketplace.

## Secure Information and Pursue the Growth

Data loss prevention offers a clear path to business growth. DLP programs make information more valuable through a reduction in risk and the de facto implementation of a compliance and governance framework, securing a clear competitive advantage. Moreover, reduced remediation expenses and streamlined operations release systems, people, and capital from existing obligations. These assets can be reinvested in business areas that generate revenue and positively impact market share.

Planned thoroughly and implemented effectively, DLP solutions should keep sensitive information in the enterprise, away from competitors, the press, and criminals. Once this primary objective has been addressed, it is time to consider the broader opportunity afforded by a DLP solution. An overarching corporate governance environment for information management should protect data, facilitate compliance, and set a standard for operations. In doing so, a DLP solution will deliver a wider business advantage, positioning the company to compete more effectively and serve clients, fulfill orders, and cultivate long-term relationships.

DLP solutions monitor communication protocols, flag sensitive data, and alert stakeholders to potential data loss through the use of content identification and context analysis. Products that look at the data alone may miss substantive leaks while notifying management of communications in which no leak has occurred. The context makes a difference vis-à-vis an understanding of the meaning of data by noting related data elements, applications that use the data, and the value of the data to the company. An effective DLP solution must do more than look at a number or string; it needs to attach some meaning in order to render an accurate result and ensure compliance with pertinent state, federal, and self-regulatory organization (e.g., National Association of Securities Dealers) mandates.

The business advantages of DLP software are clear:

- Improved business and IT operations
- Cost-effective regulatory compliance and governance
- An actionable competitive advantage

When existing security apparatus do not address data loss prevention, leak prevention can be used to infuse a layer of security into existing operations with minimal disruption. Employees continue to work as they always have, and the solution intercedes when necessary. Thus, the solution is unobtrusive, and tools leverage existing business processes to increase productivity. The interaction between business applications and data loss prevention technologies does not disrupt business—it secures and expands it.

Data loss prevention technology therefore creates a more secure business environment with solution-driven business processes that have clear ownership, control over access, and a broader governance framework. The solution itself is only a small piece of the environment that it creates upon implementation. A cohesive DLP program draws its governance model and business processes from the solution, but the control environment itself encompasses people, processes, and technology. Consequently, regulatory compliance becomes much easier to attain.

Data loss prevention solutions make compliance faster and less expensive by delivering a framework for controlling the flow of data, setting boundaries on employee activity, and introducing a governance framework to manage the business environment. Process-based governance requires disproportionate human involvement. Automation, conversely, addresses the high-volume, transactional, and routine aspects of compliance, leaving IT executives and business unit managers to define remediation and enforcement policies and focus on revenue-generating projects.

The discipline and rigor of regulatory compliance, protection of valuable information, and improved operational effectiveness contribute to competitive advantage. Securing data from the eyes of the public preserves its market value. The launch of new products, for example, can make a bigger splash and stay ahead of competing products for a longer period of time. Operational efficiency can yield a lower cost of sales, expanding margins and freeing capital committed to overhead to be used for product development, marketing, and sales force growth. Securing sensitive information thus contributes directly and indirectly to a data-driven company's competitive advantage.

Among DLP solutions, the Websense® Data Security Suite distinguishes itself through the use of proprietary Deep Content Control™ technology to prevent data loss. Conventional DLP solutions rely on regular expression analysis, looking at data “as is” to determine its sensitivity. Through our PreciselD™ technology, Websense takes a fundamentally different approach, fingerprinting data based on a broader examination of its context, which includes systems, applications, related data, users, and destination. Consequently, stakeholders spend less time responding to false alarms and more time enabling the business.

## Conclusion

Data loss must be stopped. With increased regulation and the pressures of a changing marketplace, the value of data has skyrocketed. Allowing data to slip from the business is the equivalent of bleeding cash. DLP solutions automate the process of monitoring communication, securing data, and identifying risk, making the staff more effective in pursuing the organization's goals.

The Websense Data Security Suite has advanced the methods used to control information, with an approach that treats data as an integral part of the enterprise rather than a standalone entity. Data derives its meaning from where and how it is used, and Websense's Data Security Suite uses this broader context to catch leaks before they occur without negatively impacting business. Websense Data Security Suite prevents leaks so businesses can grow.

## About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection™ for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. For more information, visit [www.websense.com](http://www.websense.com).