

7 Requirements of Data Loss Prevention

A guide to evaluating solutions that protect your confidential information assets



What every Chief Security Officer and Chief Privacy Officer should know when evaluating data loss prevention solutions

Global organizations and government agencies require more than network security to guard their confidential data and sensitive information. They must protect the data itself. Yet most organizations have little insight into where their confidential data is stored, and where it is going.

A leading analyst firm estimates that insiders are responsible for 70 percent of security incidents that incur losses. With the total number of data breaches for 2007-2008 reaching almost 900¹, companies are looking beyond securing network perimeters from external threats. They are now implementing solutions that guard against the insider threat by delivering unified protection of data wherever it is stored or used. Charles Schwab, Equifax, Raymond James Financial, CIGNA and other FORTUNE 1000 companies are using Symantec Data Loss Prevention solutions to ensure the security of their vital information assets.

7 requirements a data loss prevention solution must address

Not all vendor solutions are alike and many do not provide essential elements that adequately protect your confidential data. This report will provide a clear understanding of the capabilities a successful data loss prevention (DLP) solution must deliver. It also incorporates insight into the capabilities that the companies above typically require from a DLP solution. If you are evaluating solutions, use this report as a high-level guide for establishing your organization's requirements. Of course, if you are interested in creating a more detailed requirements summary, your Symantec representative can provide a comprehensive RFP template to help ensure a successful evaluation.

▶ Did you know...

- 1 in 400 emails contains confidential information²
- 1 in 50 network files contains confidential data³
- 4 out of 5 companies have lost confidential data when a laptop was lost⁴
- 1 in 2 USB drives contains confidential information⁵
- Companies that incur a data breach experience a significant increase in customer turnover—as much as 11%⁶
- Over 35 states have enacted security breach notification laws.⁷

1. Identity Theft Resource Center (ITRC) 2008 Breach List.

2. Symantec Corporation: Data Loss Prevention Risk Assessment customer results, 2007.

3. Symantec Corporation: Data Loss Prevention Risk Assessment customer results, 2007.

4. Ponemon Institute LLC and Symantec Corporation end-user survey, August 2006.

5. Forrester Research, Inc. and Symantec Corp. survey, February 2007.

6. Forrester Research, Inc. and Symantec Corp. survey, February 2007.

7. Annual Study: U.S. Cost of a Data Breach, Ponemon Institute LLC, PGP Corporation and Symantec Corporation.

1 Discover and protect confidential data wherever it is stored or used

Statistics show that 1 in 50 files² stored on desktops and shared file servers contains confidential data that violates both internal security policy and regulatory compliance. What's more, most companies are not equipped to identify and quarantine this sensitive information. Because stored data is one click away from being data in motion, it creates auditing risks and can lead to potential loss of intellectual property and wrongful exposure.

A comprehensive solution that effectively lowers your risk must enable you to accurately discover exposed confidential data stored on file servers, document and email repositories, web sites, relational databases or other data repositories. Once confidential data is identified, the solution should enable you to protect it by automatically applying data protection policies. Leading DLP solutions will do this through integration with data encryption, storage tiering, and archiving systems. These capabilities are at the forefront of breach prevention because they can protect confidential information before it has a chance to be transmitted.

2 Monitor all data usage and prevent confidential data from exiting any network gateway or endpoint

Preventing confidential data from being transmitted outside your organization first requires comprehensive monitoring of multiple exit and endpoints. Email is only part of the problem. Experience shows that 50 percent of incidents occur via Internet protocols other than email, such as instant messaging or blogs. Yet some content monitoring solutions only screen email, leaving other Internet protocols uncovered. Other solutions are only capable of screening Internet protocols when the user is connected to the corporate network, leaving the organization exposed when users are off the network. Removable media also provides easily accessible endpoints to which confidential data can be copied. In addition, it's not enough simply to monitor security violations; the key is to prevent sensitive data from being transmitted by blocking it, in effect closing the door before the breach occurs.

A solution that effectively reduces your risk of data loss across all business processes must combine comprehensive monitoring with prevention. It should accurately monitor and prevent security violations for all data types and all network protocols, including email (SMTP), instant messaging (AOL, MSN, Yahoo), secure Web (HTTP over SSL), FTP, P2P, and generic TCP sessions over any port. An effective Data Loss Prevention solution should also discover and inventory confidential data stored on laptops and desktops and prioritize high risk endpoints for additional protection, and monitor and prevent confidential data from being copied to external devices, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.

2. Symantec Corporation: Data Loss Prevention Risk Assessment customer results, 2007.

In addition, make sure your solution can stop transmissions that violate security, acceptable use, and privacy policies before they leave the network. Some organizations elect to begin with monitoring, then take the next step to preventing. However, even if your plan is to phase in prevention capabilities over time, your software vendor should offer both monitoring and prevention today, giving you the flexibility to expand according to your timeline, not the vendor's timeline.

3 Accuracy is critical

It is essential to accurately detect every single security policy violation, whenever, wherever, and however it occurs. Most content monitoring solutions only yield approximate identifications which can actually increase your internal costs and risk. Inaccurate detection results in frequent false alarms that cause you to waste time sifting through false positives. It can also have a far worse impact—increased risk from continuing to allow confidential data to flow undetected out through the network.

To achieve high levels of accuracy, your software solution must keep false negatives low to reduce the risk of a data breach. It must also keep false positives low to minimize review time, enable automated enforcement and protect employee privacy. Advanced detection technology is an important element in detection accuracy, but it's not the only element. The highest level of accuracy in Data Loss Prevention requires three dimensions: content, context and scale.

The ability to screen all content types (structured and unstructured data) comprehensively protects all of the organization's digital assets. For example, consider the structural differences between customer data and intellectual property. Customer data is characterized by a high volume of records with similarly-formatted data elements, whereas intellectual property is often represented by unique files that require entirely different detection technology. The next element is the ability to find the content in any context and automatically assess which contexts present greater risks of data loss. For example, manufacturing specifications sent to a partner are considered a part of an essential business process. However, that same content sent to a competitor is considered data loss. Context may include individuals (senders, recipients, file owners, Window users), location (protocols, file shares, endpoint machines), language (Western and Asian languages), encryption, file format, or media. Finally, the third element to the accuracy solution is the ability to achieve high accuracy at enterprise scale. The detection technology should deliver at scale across throughput, across protected information, and across network architecture.

4 Automate policy enforcement

As confidential information breaches are identified, it is incumbent on the security team and others to take corrective action. However, implementing remediation policies without the ability to automate their enforcement can create a tremendous burden for security and human resource teams to manage. For example, without automated policy enforcement it is estimated that teams responsible for alerting offenders and managing remediation would experience an increase of 2-5 times their normal workload. The organization would also experience lower levels of risk reduction as a result of “human” enforcement and inconsistent response that may not always match the severity of the breach.

A best-in-class solution should employ intelligent, highly-productive incident response capabilities that enable you to automate policy enforcement with flexibility. For example, by utilizing contemporary technologies such as analytics and workflow, the system should calculate incident severity and automatically deliver the appropriate level of enforcement. By varying the level of response—such as remediate, notify, or prevent—you can better initiate behavioral change, support compliance, and mitigate future risk. Finally, your solution should deliver out-of-the-box industry best practices for incident response and remediation workflow, notification, blocking, quarantine, and encryption. These templates reduce configuration time and put years of experience from other companies to work for you immediately.

5 Visibility and control over encrypted data

When used properly, encryption is a powerful tool to ensure secure delivery and access to sensitive information. Unfortunately, just because information is encrypted doesn't mean it has been approved to leave your organization. Likewise, sensitive information that is permitted to exit your organization isn't always encrypted.

Make sure your solution employs features that enable you to monitor and prevent the transmission of data that violates encryption policies. First, you must have visibility and control over encrypted information that hasn't been approved for external distribution. For example, assume an employee has been inadvertently emailing or posting an encrypted file containing new product prototypes or customer records. If these files have not been approved for external distribution, the system should inspect the data and prevent its transmission regardless of whether it's encrypted. Second, you must be able to enforce encryption policies for confidential information that has been approved for external distribution. In this case the solution should be capable of identifying unencrypted data that should be protected, and automatically route it to an encryption server prior to being distributed. You should also be able to use the results from enterprise-wide scans to prioritize the rollout of full-disk encryption to higher-risk endpoints or the users who have the most

confidential data. Finally, you must be able to monitor employees' unauthorized use of desktop encryption to make sure they are not stealing confidential information or sending confidential information to unauthorized recipients.

6 Safeguard employee privacy

The process of monitoring internal data and employee communications carries with it the responsibility of safeguarding employee privacy. An effective data loss prevention solution can be seen by employees as a powerful tool for maintaining market leadership. It can protect irreplaceable research and development effort, valuable intellectual property, and trade secrets. It can also give employees the added assurance of brand protection by potentially saving the organization from an embarrassing incident. However, if not managed correctly it can also create an environment of employee mistrust—or worse; expose the organization to fines and lawsuits for privacy violations. For example, some solutions violate United States and European Union regulations by collecting all traffic. Others don't provide role-based access controls to determine which monitors can see what data. Without the appropriate safeguards built into their software, these solutions potentially expose your organization to violations.

An effective solution needs to balance the requirement for corporate protection with the need for employee privacy. It should deliver on the following three requirements of Global Employee Privacy Protection:

- Targeted, policy-based monitoring that allows you to define specific attributes of confidential data
- Highly accurate detection technology that finds targeted data while at the same time minimizing the risk of false positives
- Role-based controls that limit viewing of quarantined data to only those individuals who are approved to see it.

7 Proven global scale and architecture

To work effectively, a data loss prevention solution must operate without diminishing system performance or preventing workers from doing their jobs. If yours is a multi-billion dollar international organization, your solution may need to monitor millions of messages per day, dozens of exit points, hundreds of thousands of users, gigabit network speeds, and billions of data records in a single deployment. Solutions that do not scale can cause both false positives and false negatives that drain valuable resources. They can also increase your total cost of ownership by requiring significant investment in hardware. One of the key questions to ask potential providers is, “Is your solution proven in production at FORTUNE 100 customers?” If it can successfully perform in these environments, chances are it is a strong enterprise-scale application. Also, ask about integration partnerships with best-in-class security infrastructure vendors such as Symantec, ArcSight, Bluecoat, Cisco, Guidance Software, PGP, Ironport and Network Appliance. Since these systems control encryption, network access, and communications gateways, interoperability with these systems is critical to delivering high performance.

Conclusion: Evaluate Symantec Data Loss Prevention

In the growing market for data loss prevention solutions, only Symantec Data Loss Prevention delivers on all 7 requirements for protecting your confidential information assets. Other vendors lack the technology to protect confidential data wherever it is stored or used—across endpoint, network, and storage systems. Our layered architecture enables customers to prevent malicious and unintentional data breaches regardless of whether data is stored on the network or on a disconnected endpoint, as well as prevent data from exiting any network gateway or endpoint.

If you are currently evaluating information security software solutions, you owe it to your organization to carefully consider the advantages of the Symantec Data Loss Prevention solution. Talk to a Symantec representative about arranging a demonstration of the Symantec solution.

Finally, remember this report is designed to be a high-level guide for establishing your own requirements. If you are interested in creating a more detailed requirements summary, your Symantec representative can provide you with a comprehensive RFP template to help ensure a successful evaluation.

How to get started

Our team of Data Loss Prevention experts will work with you to understand your unique data security requirements, priorities, and share insight into our industry best practices. Contact Symantec to get started at +1.415.364.8100 or DLPinfo@symantec.com.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.



Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.