

5 KEYS TO PROTECTING YOUR SENSITIVE INFORMATION

WHAT EVERY ENTERPRISE
EXECUTIVE SHOULD KNOW



WHAT EVERY CHIEF SECURITY OFFICER, CHIEF PRIVACY OFFICER, AND INFORMATION SYSTEMS SECURITY OFFICER SHOULD KNOW

Preventing sensitive information from being sent outside your departments or company has become a top priority for enterprise organizations today. Your company information is now readily available to a wide variety of employees who also have instant access to email and the Web, as well as a range of removable media such as USB drives and CDs/DVDs. According to IDC, close to 73 percent of the U.S. workforce will be mobile by the end of 2011.¹ With information just a keystroke from being sent across the Internet, whether an employee is on or off the corporate network, every enterprise is at risk.

The so-called “insider threat” is well documented. According to industry analysts, 70 percent of security incidents resulting in data loss are perpetrated by insiders. Risk assessment studies by Symantec reveal that an organization with 20,000 employees is likely to suffer up to 400 potential data loss incidents per day.

To avoid significant legal and compliance exposures, you need software specifically designed to address the insider threat. Today, commercial companies such as CIGNA, Energen, Esurance and many Fortune 1000 organizations are using Symantec solutions to help ensure the security of their vital information assets. With privacy and information security awareness at an all-time high, and with cyberterrorism and crime steadily increasing, Symantec can help you and your department or agency manage information risk.

¹ IDC, “Worldwide Mobile Worker Population 2007–2011 Forecast,” December 2007

5 KEYS TO PROTECTING YOUR SENSITIVE INFORMATION

If you are evaluating a data loss prevention (DLP) solution, make sure you have a clear understanding of the requirements for successful data protection. Not all vendor solutions are alike, and many fail to provide the essential elements of a best-in-class solution. Use this report as a high-level guide for evaluating software vendor solutions.

STEP 1. ACCURACY IS MISSION-CRITICAL

To be successful, you must accurately detect every security policy violation, whenever, wherever, and however it occurs. Most content monitoring solutions only yield approximate identifications, resulting in frequent false alarms and unnecessary fire drills, while undetected data continues to flow out through the network. Make sure the software vendor you choose delivers the highest degree of accuracy, with no false positives.

Remember that email is only a portion of the problem. Research shows that 50 percent of incidents occur via Internet protocols other than email. Your solution should accurately monitor and detect security violations for all data types, all data endpoints (removable media, network activities, copy/paste, and print/fax), and all network protocols, including email (SMTP), instant messaging (AOL, MSN, Yahoo!), Web, secure Web (HTTP over SSL), FTP, P2P, and generic TCP sessions over any port.

STEP 2. DON'T JUST MONITOR VIOLATIONS, STOP THEM BEFORE THEY OCCUR

It's not enough to simply track security violations; the key is to prevent them from happening. Make sure your solution can stop transmissions that violate security, acceptable use, and privacy policies before they leave the network. Many organizations elect to begin with monitoring and then expand to prevention. Your software vendor should provide a development path that allows you to grow the solution over time.

STEP 3.

TIME IS OF THE ESSENCE

When information security violations occur, it is essential that you respond immediately. Rapid response can mean the difference between safe and sorry. Regulations such as PCI require immediate response to information security breaches regardless of whether they involve classified information. You need immediate, actionable information and process automation to enable rapid response. Your software vendor's solution should provide real-time alerts, customizable workflow, and a complete profile of each incident—including content, sender, recipient, timing, and policy information—as well as automatically identify and notify the sender.

STEP 4.

YOU CAN'T MANAGE WHAT YOU CAN'T MEASURE

Monitoring data loss incidents is only the first step. To meet your security and compliance goals, you need to measure the effectiveness of your information security plan over time, so you can weigh risks, fix broken processes, and identify potential compliance issues.

Your software vendor's solution should deliver centralized, one-click reporting that covers all of the multiple exit and endpoints on your network. Users should be able to easily aggregate data, drill down on details, and distribute reports, including historical trend analysis, investigative forensics, and regulatory compliance.

STEP 5.

MAKE INFORMATION SECURITY A DEPARTMENT/AGENCY-WIDE INITIATIVE

To elevate information security to a higher strategic priority, you need to educate employees about applicable information security regulations and enable staff at every level of your organization to actively participate in the protection of sensitive as well as classified information. Your software vendor's solution should be tailored to the business/process user. Look for role-based access control to enable business units to review and remediate only those incidents relevant to their role and privileges. Look also for executive dashboards that present the big picture for senior management. Ensure that you can do reporting by functional unit to support benchmarking and accountability.

CONCLUSION: EVALUATE SYMANTEC

In the growing market for information security software solutions, only Symantec delivers on all five keys to protecting your sensitive information assets. Other vendors lack the technology and experience to ensure accuracy, prevent violations, enable rapid response, measure risk reduction, and empower process owners.

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

HOW TO GET STARTED

Our team of Data Loss Prevention experts will work with you to identify your unique data security requirements and priorities, and share insight into our industry best practices. Contact Symantec to get started at +1 (415) 364 8100 or send an email message to 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.



Copyright © 2009 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. 06/09 20020495-1

For specific country offices
and contact numbers
please visit our Website.
For information in the U.S.,
call toll-free 1 (800) 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com