Data Loss Prevention and Endpoint Security

Survey Findings
Table of Contents

Overview 3
Executive Summary 4
Half of companies have lost confidential information through removable media 5
Paper controls for endpoints are common, but not dedicated solutions 6
Intellectual property and client information top data concerns 8
Removable media is the top concern for endpoint security 9
Organizations want visibility into information downloads 10
Data loss prevention is a top priority 11
Half of companies DLP in their budgets and are increasing their DLP spending 12
Two-thirds plan to adopt Endpoint DLP in 2007 13
Top Endpoint DLP solution requirements: architecture, manageability and features 14
Appendix: respondent demographics 16
   Respondent revenue 16
   Respondent job titles 17
   Respondent industry 18
Overview

Challenges around data protection and the insider threat have changed significantly over the past few years. The build out of digital business to encompass outsourcers, partners, and offshore centers, combined with the motivation of increasingly sophisticated hackers and identity thieves, puts more sensitive information at greater risk than ever before.

Today, companies are struggling to identify and protect sensitive information within their environments—protecting information such as personally identifiable or personal health information of employees and customers, intellectual property and trade secrets, marketing plans and legal documents is a top priority for them.

The need to protect key information assets in a wide open online environment has given rise to increasing demand for Data Loss Prevention (DLP) solutions. DLP enables organizations to detect confidential data and enforce data security policies. Early DLP solutions focused on protecting data in motion by monitoring of email, web, secure web and FTP, as well as proactive blocking of network communications. Next, organizations began to deploy DLP solutions for data at rest in order to discover and protect sensitive information on internal file shares and desktops. While previous DLP solutions have been network-based, the risk of data loss through mobile devices like laptops and USB drives has stimulated a growing demand for DLP solutions at the endpoint.

Endpoint security, which used to be synonymous with basic antivirus software, has been evolving over the past few years to include technologies that address the changing threats that companies must face. First, endpoint security vendors added anti-spyware technologies and personal firewalls to mitigate the threat of unwanted applications and hackers. In 2006, host intrusion prevention was the hot technology as companies demanded protection against the unknown. At the same time, the protection of companies’ information assets was emerging as a top priority for organizations. Consequently, endpoint security solutions quickly followed suit with basic features to control the use of external devices, hoping that these controls would help protect and restrict the movement of information.

However, protecting an enterprise’s information assets requires more than blocking use of a USB drive. Today’s CISOs understand that relying on keywords and phrases and creating “black lists” is also not enough. Data loss prevention technologies must be “content aware.” The tools should be able to identify confidential information such as source code and financial reports, so that the appropriate controls can be placed on data based on its sensitivity.

Content-aware detection of data at the endpoint—whether it is being downloaded to desktops, copied to USB drives, burned to CDs, or sent via printing or fax—is not available from traditional endpoint security vendors and must be achieved through dedicated data loss prevention solutions.
Executive Summary

In November 2006, Forrester Consulting fielded a commissioned online survey of 151 decision-makers at North American companies on behalf of Vontu. Respondents had specific responsibilities for information security and/or data security policy and strategy at companies with annual revenues of more than $200 million. Fifty-nine percent of the respondents came from enterprises with more than $1 billion in revenue. Respondents were asked about their concerns, priorities, current implementations, and plans regarding data loss prevention and endpoint security.

This report describes the results of this study, of which the significant findings were:

- More than half of respondents (52%) have lost confidential data through removable media such as USB drives in the past two years.
- Currently, organizations rely mainly on paper-based controls such as written policies that information security asks employees to sign (40%).
- Intellectual property, customer data and company financials are the top three concerns for data loss at the endpoint.
- Data loss via USB drives and other removable media is the top concern (72%) for endpoint security, followed by Trojans, spyware and other threats.
- Downloading confidential data to desktop and laptop PCs is a significant threat: 76 percent of respondents said they are not satisfied with the visibility they have into confidential data being downloaded to PCs.
- DLP is a major priority for nearly all respondents (95%) in 2007.
- Most organizations (82%) said that DLP was part of their 2007 budget, and 76 percent respondents indicated their DLP spending will increase in 2007.
- Most organizations (69%) are actively pursuing Endpoint DLP solutions. Forty-four percent of respondents said that they are either piloting or are planning to deploy an Endpoint DLP solution in the next 12 months. An additional 25 percent said that they are currently investigating solutions.
Half of companies have lost confidential information through removable media

More than half of the respondents (52%) said that their company had lost confidential data through removable media in the past two years. This applies only to known data loss. Respondents whose organizations don’t have any controls in place may answer that they did not lose confidential data through removable media because they have no means of knowing whether a loss occurred.

Figure 1: The Majority of Companies Have Experienced Security Breaches with Removable Media

*Question: Has your organization experienced a data security breach resulting in the loss of confidential information or data through removable media in the past two years?*

Don’t know 6%

Yes 52%

No 42%

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Paper controls for endpoints are common, but not dedicated solutions

Most organizations—64 percent—restrict, monitor or control the transfer of data to removable media (USB drive or CD-ROM), but when asked how they restrict the flow of confidential data, 40 percent of the organizations said they rely on written and signed policies by their employees. Another 25 percent relied on Microsoft group policy to restrict endpoints.

Figure 2: Most Companies Have Taken Some Measures to Limit Data on Removable Media

*Question: Do you currently restrict, monitor or control the transfer of data to removable media (USB drive or CD-ROM)?*

![Pie chart showing the responses to the question about restricting data transfer]

<table>
<thead>
<tr>
<th>Response</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>64%</td>
</tr>
<tr>
<td>No</td>
<td>35%</td>
</tr>
<tr>
<td>Don't know</td>
<td>1%</td>
</tr>
</tbody>
</table>

69 percent of $200M - $1B companies answered yes, compared to 61 percent of $1B+ companies

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Figure 3: Written and Signed Policies Represent the Most Common Means of Restricting Unauthorized Flow of Information from the Endpoint

Question: How has your organization restricted the flow of confidential information off the endpoint?

<table>
<thead>
<tr>
<th>Policy Description</th>
<th>Large Enterprises</th>
<th>All Respondents</th>
<th>Small Enterprises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Written and signed policy by all employees</td>
<td>3.6 (n=61)</td>
<td>3.8 (n=37)</td>
<td>3.4 (n=9)</td>
</tr>
<tr>
<td>Group policy from Microsoft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device control solution from a dedicated security vendor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical intervention</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>We don’t restrict information flow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Don’t know</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (please specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On a scale of 1 to 5, how successful has this policy been?

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Respondents listed intellectual property (60%) and customer information (55%) as their top concerns for data loss at the endpoint. Intellectual property is the top concern for all enterprises, with some variation by company size: 66 percent of large enterprises versus 58 percent of small enterprises consider it to be the top data protection concern for endpoints. On the other hand, a much larger number of small enterprises (53%) consider company financials to be a major concern versus only one-third (33%) of the larger enterprises.

Figure 4: Intellectual property and client information are the top data protection concerns

Question: What data are you most concerned about protecting at the endpoint? (Choose all that apply)

- Intellectual property
- Client/customer lists
- Company financials
- Source code
- Other

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Removable media is the top concern for endpoint security

Two years ago, viruses and Trojans were the top CISO concern for endpoint security, but the current data suggests today the threat of data loss through endpoints, whether inadvertent or intentional, is now the top concern.

Figure 5: Removable Media is the Top Concern for Endpoint Security

Question: On a scale of 1 to 5, how much of a concern are each if the following threats to data security?

![Bar chart showing the concern levels for different threats to data security.](chart)

Inadvertent data leak or data theft through removable media devices: 4.0
Trojans and spyware on your endpoints: 3.8
Unsecured connections: 3.8
Losing/theft of entire desktops/laptops: 3.7
Desktop sharing and remote login applications: 3.7
Screen capture technologies: 3.3

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Organizations want visibility into information downloads

Organizations want visibility into the data that is moving around in their environment. Seventy-six percent of respondents are not satisfied with the level of visibility they have into what their users are downloading onto their PCs. Furthermore, 57 percent of respondents agreed that they do not currently have visibility into the confidential data that resides on users’ machines, but would like to have such visibility in the future.

Figure 6: Most Companies Want More Visibility on Downloads to PCs

**Question: Do you have visibility into the information that users are downloading to their PCs?**

- Yes: 23%
- Yes, but want more: 55%
- No, don’t need it: 1%
- No, would like to have it: 21%

**Question: Do you have a complete inventory of all confidential data on user machines?**

- No, don’t need it: 5%
- No, I would like to have it: 57%
- Yes: 38%
- Yes, but want more: 16%

16% of $200M - $1B companies answered yes, compared to 27% of $1B+ companies

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Data loss prevention is a top priority

Data Loss Prevention (DLP) is a major priority for nearly all respondents (95%) in 2007. While only 19 percent of companies say they have addressed the problem of data loss within their organization, an overwhelming 76 percent say that data loss is something that they either plan on addressing or are in the process of addressing.

Figure 7: All Respondent Organizations Consider Data Loss Prevention a Priority

*Question: Is data loss prevention considered a priority within your organization?*

- Yes, it is a concern that we plan on addressing: 30%
- Yes, it is a concern that we are in the process of addressing: 46%
- Yes, it is a concern, but we don't have the resources to address it: 5%
- Yes, it is a concern that we have already addressed: 19%

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Half of companies DLP in their budgets and are increasing their DLP spending

A vast majority of respondents—82 percent—said that DLP was part of their budgets for 2007, and 51 percent of the respondents said that it was a significant enough issue that they had included it as a separate budget item. Additionally, 76 percent of respondents said that their DLP spending will increase in 2007, compared to the previous year. A quarter of large companies are planning to “significantly increase” their spending on DLP compared to only eight percent of the smaller companies surveyed.

Figure 8: A Majority of Companies Have DLP in their Budgets and are Increasing their DLP Spending

57% of $1B+ enterprises have data loss prevention as a separate budget item in the security budget

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Two-thirds plan to adopt Endpoint DLP in 2007

Forty-four percent of all respondents said they are currently piloting or are planning to deploy an endpoint DLP solution in the next 12 months, while an additional 25 percent of enterprises said that they are currently investigating Endpoint DLP solutions. The larger enterprises seem to be ahead in deploying endpoint security solutions: 52 percent reported that they will deploy a solution in the next 12 months or the solution is in pilot, versus 33 percent of the smaller enterprises.

Figure 9: Two-Thirds of All Enterprises Plan to Adopt an Endpoint DLP Solution in 2007

Question: When will you adopt an endpoint data loss prevention solution?

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Top Endpoint DLP solution requirements: architecture, manageability and features

Security managers consider stability, blocking, and manageability to be the top concerns, followed by universal policy, content awareness, and accuracy. Most respondents are now very cautious due to stability, manageability, and integration issues while deploying other endpoint security technologies. While most respondents consider blocking to be an important feature, 83 percent of the respondents say that they would initially want to run Endpoint DLP in “monitor only” mode until they are comfortable with it, and an additional 10 percent say that they would run it in “monitor only” mode.

Figure 10: Respondents Highlight Stability as the Area of Most Concern for an Endpoint DLP Solution

Question: On a scale of 1 to 5, how important are each of the following requirements for an endpoint DLP solution?

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Extreme concern</th>
<th>3</th>
<th>No concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stability</td>
<td></td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>Blocking</td>
<td></td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Manageability</td>
<td></td>
<td>40%</td>
<td></td>
</tr>
<tr>
<td>Universal Policy</td>
<td></td>
<td>60%</td>
<td></td>
</tr>
<tr>
<td>Content Aware Detection, Removable Devices</td>
<td></td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td>Content Aware Detection, Local Drives</td>
<td></td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

Mean value (2.5 = neutral)

- Stability: 4.0
- Blocking: 4.0
- Manageability: 3.9
- Universal Policy: 3.8
- Content Aware Detection, Removable Devices: 3.8
- Content Aware Detection, Local Drives: 3.8
- Accuracy: 3.7

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Figure 11: Users Wait to Engage Blocking

Question: When rolling out data loss prevention solutions, what approach does your company generally take?

- Run solution in monitor-only mode 10%
- Run solutions in monitor-only mode until comfortable with solution 83%
- Run solution immediately in blocking mode 7%

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Appendix: respondent demographics

Respondent revenue
The 151 technology decision-makers surveyed represent companies with more than $200 million in revenue. The respondents break out as follows:

Figure 12: Respondents by revenue

Question: Approximately what is your company’s revenue?

<table>
<thead>
<tr>
<th>Revenue Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10 billion or more</td>
<td>26%</td>
</tr>
<tr>
<td>$5 billion to less than $10 billion</td>
<td>12%</td>
</tr>
<tr>
<td>$1 billion to less than $5 billion</td>
<td>21%</td>
</tr>
<tr>
<td>$750 million to less than $1 billion</td>
<td>10%</td>
</tr>
<tr>
<td>$500 million to less than $750 million</td>
<td>11%</td>
</tr>
<tr>
<td>$200 million to less than $500 million</td>
<td>20%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Respondent job titles
Respondents represent a wide variety of IT decision-makers who have specific responsibilities for information security and/or data security policy and strategy at their companies. The respondents break out as follows:

Figure 13: Respondents by job title

Question: Which of the following most closely describes your job title?

<table>
<thead>
<tr>
<th>Job Title</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director of IT</td>
<td>24%</td>
</tr>
<tr>
<td>Senior manager of IT reporting directly to Executive Management</td>
<td>21%</td>
</tr>
<tr>
<td>Vice-President of IT</td>
<td>18%</td>
</tr>
<tr>
<td>Chief Technology Officer, CIO</td>
<td>17%</td>
</tr>
<tr>
<td>Chief Information Security Officer, Chief Security Officer</td>
<td>9%</td>
</tr>
<tr>
<td>Director of Security</td>
<td>3%</td>
</tr>
<tr>
<td>Senior manager of information security reporting directly to CIO</td>
<td>3%</td>
</tr>
<tr>
<td>Chief Risk Officer or Vice-President of Risk Management</td>
<td>3%</td>
</tr>
<tr>
<td>Vice-President of Security</td>
<td>2%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
Respondent industry
Respondents represent a wide variety of industries—they break out as follows:

Question: To which industry would you say that your company belongs?

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional services</td>
<td>13%</td>
</tr>
<tr>
<td>Financial services</td>
<td>13%</td>
</tr>
<tr>
<td>High-tech products manufacturing</td>
<td>13%</td>
</tr>
<tr>
<td>Industrial products manufacturing</td>
<td>10%</td>
</tr>
<tr>
<td>Retail</td>
<td>7%</td>
</tr>
<tr>
<td>Telecom carriers</td>
<td>7%</td>
</tr>
<tr>
<td>Media, entertainment and leisure</td>
<td>7%</td>
</tr>
<tr>
<td>Transportation and logistics services</td>
<td>7%</td>
</tr>
<tr>
<td>Consumer products manufacturing</td>
<td>7%</td>
</tr>
<tr>
<td>Construction and engineering services</td>
<td>4%</td>
</tr>
<tr>
<td>Government</td>
<td>3%</td>
</tr>
<tr>
<td>Public services</td>
<td>2%</td>
</tr>
<tr>
<td>Utilities</td>
<td>2%</td>
</tr>
<tr>
<td>Chemicals and petroleum manufacturing</td>
<td>2%</td>
</tr>
<tr>
<td>Primary products manufacturing</td>
<td>2%</td>
</tr>
<tr>
<td>Insurance</td>
<td>1%</td>
</tr>
<tr>
<td>Wholesale</td>
<td>1%</td>
</tr>
</tbody>
</table>

Base: All respondents, n=151

Source: Online study conducted by Forrester Consulting on behalf of Vontu, November 2006.
About Vontu

Vontu is the leading provider of Data Loss Prevention solutions that protect data anywhere—at rest, in motion or at the endpoint. By reducing the risk of data loss, Vontu helps organizations ensure public confidence, demonstrate compliance and maintain competitive advantage. Vontu customers include many of the world’s largest and most data-driven enterprises and government agencies. Vontu has received numerous awards, including IDG’s InfoWorld 2007 Technology of the Year Award for “Best Data Leak Prevention,” as well as SC Magazine’s 2006 U.S. Excellence Award for “Best Enterprise Security Solution” and Global Award for “Best New Security Solution.” For more information, please visit www.vontu.com.