THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM
1900 EMBARCADERO ROAD, SUITE 206 • PALO ALTO, CA 94303 • TEL. 650-322-8059 • FAX 650-352-8061

Content-Aware Data Loss Prevention Market, 2013-2017

Editor: Sara Radicati, PhD; Principal Analyst: Thomas Buckley

SCOPE

This study covers the Content-Aware Data Loss Prevention (DLP) market in 2013 and its expected evolution over the next four years. The report examines market trends, corporate demand, as well as leading vendor products and strategies.

Data Loss Prevention is the supervision and management of electronic data that enables organizations to prevent non-compliant information transfer activity from occurring. Content-Aware DLP solutions monitor data in motion, data in use, and data at rest on corporate servers, desktops, laptops, and other endpoints.

This report provides data on worldwide market size, installed base and revenue market share by vendor, as well as worldwide market growth forecasts in terms of both installed base and revenue from 2013 to 2017.

All market numbers, such as market size, forecasts, installed base, revenue information, and any financial information presented in this study represent worldwide figures. Geographical breakouts are also provided. All revenue numbers are expressed in $USD.

The revenue numbers listed for each vendor do not represent total company revenue. They only represent sales of solutions and support revenues as a direct result of the sales for the 2013 calendar year. Professional services revenue is not included.

METHODOLOGY

The information and analysis in this report is based on primary research conducted by The Radicati Group, Inc. in 2013. It consists of information collected from vendors, and corporate users via on-going interviews and surveys.

Secondary research sources have also been used, where appropriate, to cross-check the information collected. These include company annual reports and market size information from various related market segments of the computer industry.

EXECUTIVE SUMMARY

- Data Loss Prevention (DLP) solutions are electronic data supervision and management solutions that enable organizations to prevent non-compliant electronic information transfer activity from occurring.

- External threats to data exist in myriad forms via advanced persistent threats (APT), espionage, and other methods that try to gain unauthorized access to data. With a proper DLP solution in place, an organization can protect itself by knowing where confidential data lies and taking the necessary precautions, such as encrypting or moving confidential data, to avoid unauthorized access.

- While external threats pose a problem that needs to be addressed in the enterprise, the threat of data loss is actually larger from internal threats in an organization given insiders' easy access to data. Internal leaks can be malicious, such as a disgruntled worker copying sensitive data to a flash drive, or they can result from negligence due to an honest mistake, such as an employee sending a customer list to a business partner that shouldn't have access to it.

- We distinguish between different types of DLP solutions:

    - ***Content-Aware DLP solutions*** protect data in use, data at rest, and data in motion and are "aware" of content that is being protected.

  - ***Channel DLP solutions*** typically enforce policies on one specific type of data, usually data in motion, and one particular communication channel, such as email.

  - ***DLP-Lite solutions*** are typically an add-on to another solution in the enterprise (for instance, information archiving) and are not content-aware.

- This report deals primarily with Content-Aware DLP solutions. Channel DLP and DLP-Lite solutions are not included as they are normally part of some broader security or data retention product solution. This report does provide a quick overview of some popular Channel DLP and DLP-Lite solutions in section 1.5.

- Increased regulations worldwide are supporting the need for the deployment of DLP solutions, such as laws that mandate the disclosure of data breaches of customer data. Despite this continued increase in regulations, it is internal policies about corporate data protection that typically lead an organization to deploy a DLP solution.

- DLP solutions can be quite expensive to maintain. In addition to the technology piece, organizations should also have enough compliance officers to be able to monitor quarantined messages in a timely fashion. Today, however, many DLP solutions come with comprehensive self-remediation options to enable users to resolve issues before the message is blocked or is escalated to a level that requires the attention of a compliance officer.

- Microsoft Exchange Server 2013 was released in late 2012 and now includes DLP features that its predecessors did not. While the DLP features currently included in Exchange 2013 are not yet at a Content-Aware DLP level, we believe the next versions of Exchange will inevitably add more DLP content-aware functionality, which will certainly influence the Content-Aware DLP market in the coming years.

- The Content-Aware Data Loss Prevention (DLP) market continues to grow at a rate of over 20% annually. This growth is fueled by tangible and intangible consequences. Hefty fines that surpass seven figures can result from improper data protection in an organization. However, there is also the potential loss of customer trust and brand value in a data leak disaster. These losses are more difficult to quantify, yet they are often more devastating than any fine or other punishment imposed.

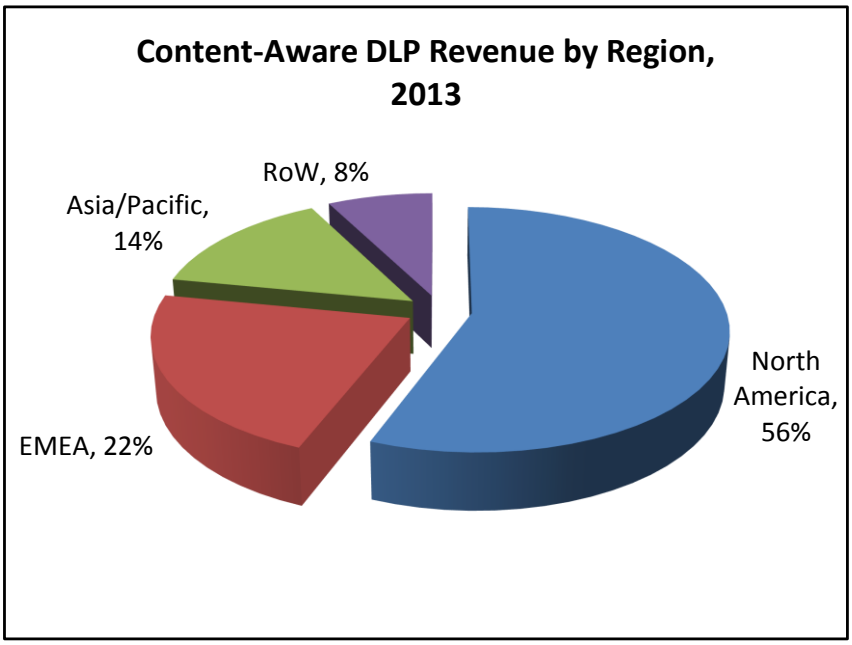

Figure 1: Content-Aware DLP Solutions Revenue by Region, 2013

To view the complete Table of Contents for this report, visit our website at www.radicati.com.