

June 6, 2008

The Forrester Wave™: Data Leak Prevention, Q2 2008

by Thomas Raschke
for Security & Risk Professionals



June 6, 2008

The Forrester Wave™: Data Leak Prevention, Q2 2008

Websense And Reconnex Top The Leaders Stack, Followed By Verdasys, RSA, And Vericept

by **Thomas Raschke**

with Jonathan Penn, Antonin Shanahan, and Alissa Dill

EXECUTIVE SUMMARY

Forrester evaluated leading data leak prevention (DLP) vendors across approximately 74 criteria and found that Websense and Reconnex came out on top because of their strong go-to-market strategy and automated learning capabilities, respectively. Verdasys is a Leader due to balanced functionality and rich context-based analysis at the desktop. RSA Security stands out for its integrated vision and leading discovery capabilities, while Vericept rounds out the Leader class of 2008 because of its very balanced DLP coverage and strong analysis features. The Strong Performer group is led by Workshare and Orchestra, both providing tight application integration at the desktop and a user-friendly approach to DLP. Code Green Networks is easy to use, cost-effective, and an ideal fit for small and medium-size businesses (SMBs). McAfee now offers strong integration with encryption and its popular ePolicy Orchestrator; Trend Micro has a strong international play featuring leading data-in-use protection. Russia-based InfoWatch is a Contender and offers a straightforward DLP solution for many organizations in Eastern Europe and the Middle East. Ultimately, DLP will be a must-have that is integrated with security infrastructure; longer term, it will extend into information management.

TABLE OF CONTENTS

- 2 Insider Threat Protection Becomes A Must-Have, And The Market Consolidates**
- 3 Data Leak Prevention Evaluation Overview**
- 6 Data Leak Prevention Tools Are Maturing And Being Integrated**
- 8 Vendor Profiles**
- 14 Supplemental Material**

NOTES & RESOURCES

Forrester conducted product evaluations in January 2008 and interviewed 12 vendor and more than 30 user companies, including: Code Green Networks, InfoWatch, McAfee, Orchestra, Reconnex, RSA Security, Trend Micro, Verdasys, Vericept, Websense, and Workshare.

Related Research Documents

[“Oops! Data Leaks Are Not Just An American Problem”](#)

January 16, 2008

[“EMC/RSA Drafts Tablus For Deeper Data-Centric Security”](#)

August 20, 2007

[“The Forrester Wave™: Information Leak Prevention, Q4 2006”](#)

December 15, 2006

INSIDER THREAT PROTECTION BECOMES A MUST-HAVE, AND THE MARKET CONSOLIDATES

During the past 18 months, few technology areas in security and risk management have seen similar levels of attention and activity as the data leak prevention (DLP) market.¹ This is because DLP has a strong stake in virtually all current broader trends in security and risk management, including: 1) deperimeterization and the fall of the network; 2) the shift toward more security at the endpoint; 3) data-centric and policy-based security and remediation; and 4) the move to business-driven information risk management.

As companies realize that they need to safeguard their information assets instead of protecting networks and infrastructure via perimeter-based security alone, data-centric and policy-based security approaches take the center stage.² Encryption; endpoint security; and, very importantly, data leak prevention solutions promise to help organizations get their own data house in order. Ultimately, these technologies discover, understand, manage, and protect information assets — and therefore are a vital part in any modern security and risk management strategy, which increasingly centers on business goals and benefits.

Email, Compliance, Removable Media, And More IP Data Are Key Drivers For DLP Adoption

Originally, organizations turned to DLP because they were either forced to by external regulations or because they wanted to protect sensitive data from leaving via the most important business communication channel, email. As the risks have evolved, so has the DLP market.

- **Most early solutions focused on finding personal data leaving the network.** Many of the first DLP vendors were only monitoring and interfering with data-in-motion (DIM) at the various network egress points. Email is still a key vector for data loss today — so, many companies start out with outbound email protection.
- **Removable media grew as a data loss and theft issue.** As removable storage devices like USB sticks, iPods, and external hard drives proliferated, companies began to focus on closing down different data loss activities at the endpoint. Consequently, agent-based DLP solutions stepped in and, for example, prevented copying to USB devices or CDs — even when the endpoint was off the network. Today, many organizations with loads of sensitive data on their endpoints choose to tackle the DLP problem from this angle.
- **The emerging challenge is on data proliferation and protection of IP.** Going forward, the biggest challenge for companies lies in protecting ever increasing amounts of sensitive data, which is increasingly found in an unstructured fashion in various parts of the network and in applications. Protecting various types of intellectual property (IP) like source code, customer lists, construction plans, or other types of “secret sauce” is more complex than, for example, finding files containing credit card numbers.³

DLP Is Stretching Beyond Technology — And Beyond Security

Forrester estimates that about 80% of all data leaks occur because of accidents — that is users being unaware of data policies, as opposed to having malicious intent. While DLP solutions address many non-technical aspects of data management, they continue to evolve and integrate into other technology domains in and beyond the security sphere. DLP customers experience that:

- **Technology is not the only element of a data leak protection strategy.** Security managers are beginning to understand that the data protection problem goes beyond that which technology alone can solve. Data leak prevention extends beyond the boundaries of the security organization. For example, information classification is one key component; to do that right involves including business line managers and data creators that possess the necessary visibility into the data. Leading DLP solutions today help companies automate the data classification process and provide greater visibility into data and devices — but coordination with information owners and users will remain a vital element going forward. DLP benefits go beyond the immediate technology sphere by promoting collaboration and awareness for processes and policies.
- **Advanced DLP features and uses often require additional services.** The DLP market has come a long way from standalone products that focused on just a few egress vectors, regulations, or use cases. Today's DLP solutions need to provide outbound protection for DIM at network egress points, data-in-use (DIU) at endpoints, and data-at-rest (DAR) discovery across all pieces of the network that can hold data. Data classification, policy creation, management, and reporting should ideally be fully unified across all data domains. Additionally, DLP engines must be able to set and enforce policies based on content or context. Due to this added complexity, Forrester increasingly sees customers consulting integrators and other services providers as they adopt such data-centric security into their environments.
- **DLP is becoming an integral part of security solutions and broader information management.** Companies today expect simplicity and integration with existing solutions. Therefore, DLP currently sees a first wave of integration into content security solutions, endpoint agents, and security information management (SIM) products to provide full inbound and outbound protection. Tight integration with various forms of encryption and post-leak technologies like digital rights management (DRM) and device-kill products is the next integration level. But DLP contains bits and pieces that add value to other non-security domains — most notably data classification and data life-cycle and knowledge management. Accurate classification and policy management are the backbone of broader information and asset management: all areas where DLP technologies play a vital role.

DATA LEAK PREVENTION EVALUATION OVERVIEW

To assess the state of the data leak prevention market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top DLP vendors.

Evaluation Criteria: Focus On Analysis, Breadth Of Data Domains, And Product Vision

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against approximately 74 criteria, which we grouped into three high-level buckets:

- **Current offering.** We selected 10 key areas of product functionality: solution breadth and technology, data-in-motion (i.e., the network piece), data-at-rest (i.e., discovery), data-in-use (i.e., desktop or host), unified management, policy management, administration, forensics, integration, and customer references.
- **Strategy.** To assess each vendor's overall strategy, we chose three sets of criteria: company vision and product strategy, go-to-market, and pricing and cost.
- **Market presence.** We examined each vendor's customer installed base and revenue.

Evaluated Vendors Protect Enterprises Holistically Against The Insider Threat

Forrester included 11 vendors in this assessment: Code Green Networks, InfoWatch, McAfee, Orchestra, Reconnex, RSA Security, Trend Micro, Verdasys, Vericept, Websense, and Workshare (see Figure 1). Vontu, now part of Symantec, declined to participate in the formal evaluation process, so its high-level assessment was largely based on publicly available information. Since Forrester was unable to use the same evaluation methodology it used with other Forrester Wave evaluation participants, the placement in the Forrester Wave graphic is based on an alternate approach for non-participating vendors.⁴ Therefore, there is not a detailed scoring spreadsheet for Symantec. We carried out the Wave evaluation between December 2007 and February 2008.

All of these vendors address the insider threat and have:

- **Multichannel and multi-activity capabilities.** Network-based DLP products must support analysis across multiple channels through a single product: Simple email or Web content security products are not enough. Desktop-based agent products must support multiple activities like copying to USB or other removable media devices: Mere email or browser plug-ins don't suffice.
- **Content- or context-aware policy mechanisms.** DLP solutions must be able to set policy and make enforcement decisions based on content or context. Content-based policy enforcement consists of identifying important structured information — personal information, for example — as well as unstructured information, such as documents that contain IP or other sensitive corporate material. Context-based policy enforcement consists of understanding the people, applications, and channels involved, as well as other aspects of the activity.

- **Unified management.** Data analysis and classification taxonomy, policy management, and incident response and reporting must be unified to some extent. While all management domains do not have to be unified across network and desktop, they should be fully unified on one end of the DLP solution (i.e., across network channels or across desktop activities).
- **Prevention and enforcement capabilities.** DLP customers increasingly want to not just monitor but also enforce their policies in order to fully safeguard their data assets. Therefore, DLP products must go beyond detection to include block, quarantine, encrypt, and archive as enforcement mechanisms across a broad range of user activities. Blocking either email or Web traffic is a minimum on the network; blocking file copy/save needs to be enabled on the desktop.

Figure 1 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated
Code Green Networks	Content Inspection Appliance, CI-1500; CI-750; CI-Agent, v. 5.0
InfoWatch	InfoWatch Traffic Monitor, v. 3.0
McAfee	McAfee Data Loss Prevention (DLP): Host 2.0, Gateway 3300, 3400
Orchestria	Orchestria v. 5.0
Reconnex	Reconnex 7
RSA Security	RSA Data Loss Prevention (DLP) Suite: Datacenter 3.1.1; Network 5.1.1; and Endpoint 3.0
Trend Micro	Trend Micro LeakProof, v. 3.0
Verdasys	Digital Guardian, v. 5.1
Vericept	Vericept Monitor, Protect, Discover, v. 8.2; Vericept Edge, v. 1.3
Websense	Websense Content Protection Suite, v. 6.5
Workshare	Workshare Protect, v. 6

Vendor selection criteria

Does the solution have multichannel and multi-activity capabilities?
Does the solution have content- or context-aware policy mechanisms?
How well does the solution support unified management?
Does the solution have both prevention and enforcement capabilities?
Does the vendor demonstrate strong brand recognition and market presence, with frequent mentions in Forrester client inquiries, requests for proposal, and other discussions with DLP buyers?

Source: Forrester Research, Inc.

DATA LEAK PREVENTION TOOLS ARE MATURING AND BEING INTEGRATED

The evaluation uncovered a market in which (see Figure 2):

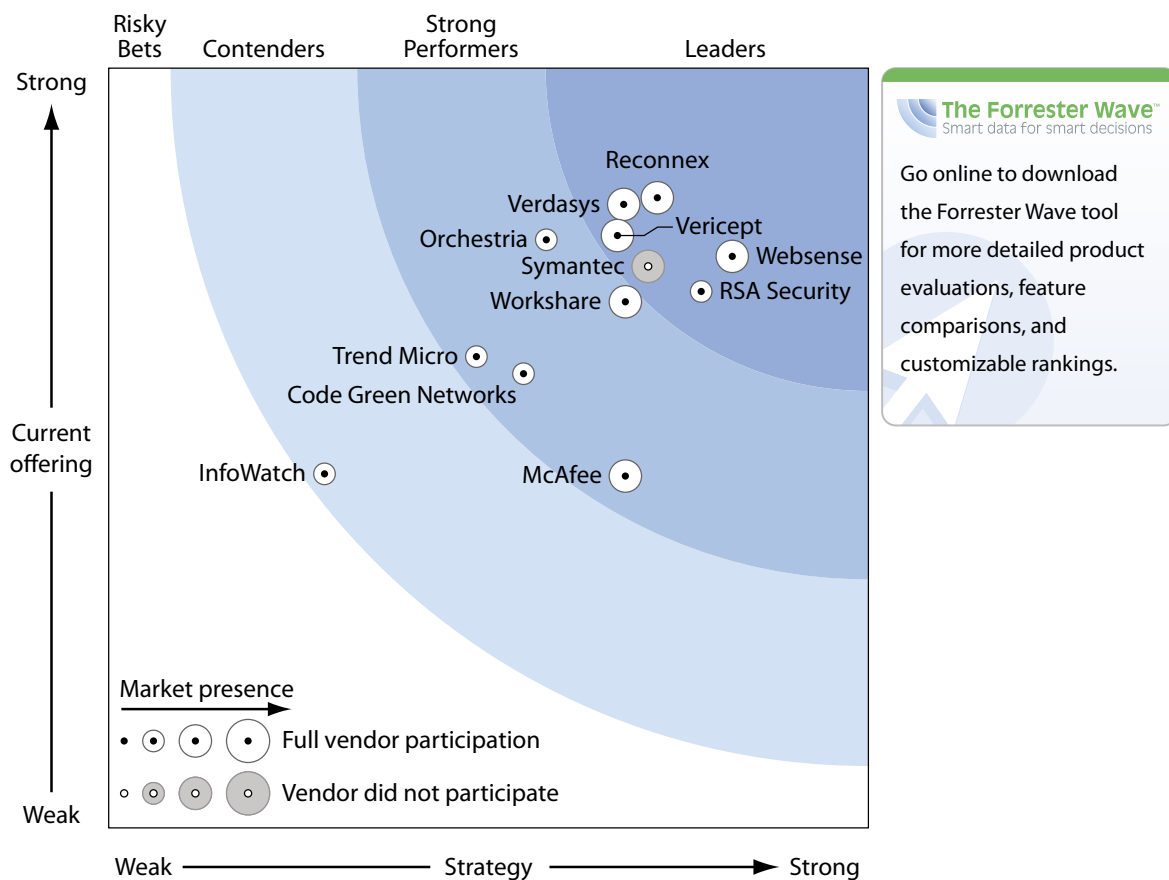
- **Websense and Reconnex are top Leaders; Verdasys, RSA, Vericept, and Symantec are next.** Websense and Reconnex have captured the lead in the current market. Websense successfully integrated PortAuthority into its content security portfolio and offers a strong go-to-market strategy. Reconnex offers best-in-class product functionality through its automated classification and analysis engine, which allows customers to sift through the actual data that the engine monitors to learn what is important to protect. Verdasys has clearly leading DIU capabilities and is providing rich context-based analysis and detection across all data domains. RSA Security articulates the best integrated vision for DLP and offers exceptional discovery capabilities it acquired from Tablus. Vericept offers a strong DIM product along with solid DIU and DAR capabilities and market-leading policy management capabilities. Meanwhile, Symantec (through the acquisition of Vontu) offers a DLP platform with balanced capabilities for DIM and DAR, and it holds the potential for providing deep integration across security, storage, and information management.
- **Strong Performers: Workshare, Orchestra, Code Green Networks, McAfee, and Trend Micro.** Workshare offers a balanced strategy and shines with tight integration into Microsoft Office. It is also the only vendor that can clean metadata in documents. Orchestra exhibits high accuracy, easy deployment, and great administration and reporting capabilities, but it comes up somewhat short in general strategy. The product is geared toward — but not limited to — the needs of the financial services sector. Code Green Networks targets SMBs and provides a solid, easy to implement and use DLP appliance that is very cost-efficient, clearly delivering value to most smaller companies and entities like subsidiaries. McAfee and Trend Micro seek to expand their broad security offerings with solid data protection capabilities. While both start at the endpoint, McAfee integrates into encryption (SafeBoot) and ePolicy management, whereas Trend Micro molds the strong Provillea DIU product into its security suite.
- **InfoWatch is a Contender.** Russia-based InfoWatch provides specialized value for customers in Russia and Eastern Europe. The product offers good administration and solid DIM capabilities — but lacks in many other areas.

There are many other DLP vendors that Forrester did not include in this evaluation, including Aungate (now Autonomy ZANTAZ), BigFix, Fidelis Security Systems, GTB Technologies, Intelligent Wave USA, Intrusion, Lumension Security (PatchLink and SecureWave), NextLabs, NextSentry, Palisade Systems, Proofpoint, Raytheon Company (Oakley Networks), and Secure Computing. Additionally, a number of vendors such as Tizor, Imperva, and Guardium provide leak prevention functionality for the specific use case of safeguarding databases.⁵

These vendors either failed to meet the full qualifying criteria or were omitted in favor of other vendors that Forrester clients inquired about more frequently. Their absence from this Forrester Wave™ evaluation does not constitute any judgment as to these vendors' capabilities or viability.

This evaluation of the data leak prevention market is intended to be a starting point only. Readers are encouraged to view detailed product evaluations and adapt the criteria weightings to fit their individual needs through the downloadable Forrester Wave Excel-based vendor comparison tool.

Figure 2 Forrester Wave™: Data Leak Prevention, Q2 2008



Source: Forrester Research, Inc.

Figure 2 Forrester Wave™: Data Leak Prevention, Q2 2008 (Cont.)

	Forrester's Weighting	Code Green Networks	InfoWatch	McAfee	Orchestra	Reconnex	RSA Security	Trend Micro	Verdasys	Vericept	Websense	Workshare
CURRENT OFFERING	50%	2.99	2.33	2.31	3.87	4.14	3.53	3.10	4.10	3.90	3.76	3.46
Solution breadth and technology	15%	3.70	2.60	3.70	2.55	3.15	3.00	3.50	4.50	3.40	3.30	3.45
Data-in-motion (i.e., the network piece)	10%	4.60	3.00	3.00	4.20	5.00	4.20	2.60	3.40	5.00	5.00	3.80
Data-at-rest (i.e., discovery)	12%	2.20	2.20	0.40	3.80	4.60	4.60	3.40	4.20	4.60	4.20	2.60
Data-in-use (i.e., desktop or host)	13%	3.00	1.80	2.60	4.20	3.80	2.60	4.20	5.00	3.40	3.00	3.40
Unified management	5%	0.00	2.40	1.00	5.00	5.00	0.30	4.40	5.00	4.40	4.40	4.40
Policy management	5%	3.20	2.60	1.80	3.80	4.20	4.00	2.40	4.20	4.60	4.20	2.80
Administration	5%	3.00	5.00	1.00	5.00	5.00	5.00	3.00	5.00	5.00	3.00	5.00
Forensics	10%	2.40	2.00	3.00	3.80	4.60	3.40	2.20	4.60	4.20	3.40	4.20
Integration	10%	2.00	1.60	0.80	2.90	3.70	2.90	1.70	2.50	3.10	4.40	3.30
Customer references	15%	3.80	1.90	3.30	4.70	3.90	4.50	3.20	3.40	3.10	3.40	3.00
STRATEGY	50%	2.73	1.42	3.40	2.88	3.61	3.90	2.42	3.39	3.35	4.10	3.40
Company vision and product strategy	70%	2.80	1.30	2.80	3.00	4.10	4.60	2.60	3.70	3.60	4.10	2.80
Go-to-market	30%	2.55	1.70	4.80	2.60	2.45	2.25	2.00	2.65	2.75	4.10	4.80
Pricing and cost	0%	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
MARKET PRESENCE	0%	2.85	2.35	3.38	2.70	3.30	2.58	2.40	3.75	3.38	3.60	3.08
Installed base	50%	2.90	1.80	4.50	1.50	2.90	1.80	2.10	3.60	4.20	4.50	4.70
Revenue	50%	2.80	2.90	2.25	3.90	3.70	3.35	2.70	3.90	2.55	2.70	1.45

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc.

VENDOR PROFILES

Leaders Are Functionally And Strategically Balanced

- Websense.** Content security frontrunner, Websense, sits atop the DLP market thanks to its balance of first-class product capabilities and solid strategy. The company leverages its partnership with Safend to offer a DLP product consisting of both a network appliance and endpoint software. Most of Websense's customers have implemented its original offering: appliance-based network DLP that safeguards DIM. But the Websense Data Security Suite now protects across DAR, DIM, and DIU. The product's analysis engine is language-agnostic and includes templates applicable to many regions. Websense uses PreciseID fingerprinting technology to identify both structured and unstructured data for more than 375 file formats, and it can correlate multiple data fields from a single record to define the exact data to protect

(e.g., name and social security number). Websense needs to integrate a fully functioning endpoint agent into the solution (planned for 2008) or risk losing its position as market leader. The product also needs a more advanced classification engine so that customers can both classify and categorize their data properly; additionally, it needs to interoperate with other knowledge management systems. Websense has bold, compelling plans to significantly expand upon its current capabilities as a leading content security vendor. The firm wants to provide DLP for both the network and the endpoint and integrate with business functions and technology to evolve past defensive security and toward an integral business insight and process control solution.

- **Reconnex.** DLP pure play Reconnex offers a leading appliance-based solution for DIM and DAR and also protects DIU through a desktop agent. This solution stands out because it is the only one that automatically discovers and classifies sensitive data without prior knowledge of what needs to be protected. Reconnex's inSight central management platform creates policy and responds to incidents across all three data domains, although customers primarily use the appliance-based network DLP capabilities to protect DIM. Reconnex's solution analyzes DAR and provides port-agnostic application classification. The endpoint agent can prevent information from being moved or copied based on the data's classification, but it does not enforce file permissions like opening and deletion. Reconnex needs to build on its automated data learning capabilities. On the technology side, it needs to further optimize and integrate. It also needs to get out of the technology ghetto and articulate these differentiating features in clear, simple business terms. The firm also has to solve the inherent "coopetition" challenges with at least two of its major partners, Trend Micro and Utimaco Safeware, which compete for the same DLP budgets. Reconnex is a good fit for US customers who are looking for an accurate, broad-based DLP solution and who have no insight into what types of information are floating around the organization and how important that data is for the ongoing success of the company.
- **Verdasys.** Verdasys has the broadest set of software agents and delivers the strongest offering for protecting DIU at the endpoint, which is what most customers use it for. Its unified solution has both network and client/endpoint pieces that leverage a multitude of agents in different locations. The firm's Digital Guardian product discovers, classifies, monitors, and controls data on desktops, laptops, servers, and handheld endpoints using context- and content-based data analysis, applying policies that warn, alert, block, and audit improper data usage. It can encrypt both emails and files based on policy, monitor the use of all files/data at the point of use — including when a device is off the network — and restrict the use of files based on application type. Customers can flexibly configure the product to distinguish between regular business processes and anomalous activity; the product uses contextual information like location, file type, application, and protocol to differentially enforce policy by path, user, and data quantity. Additionally, Digital Guardian's Document Similarity feature uses Bayesian analysis of representative documents to identify files, performing the analysis in real time for vulnerable content such as data held in the clipboard buffer. Digital Guardian needs to extend its capabilities to more mobile devices and information repositories; add support for additional

operating systems such as Mac; and integrate with SIM tools. No other vendor is as devoted as Verdasys to the idea that providing security at the endpoint is the alpha and omega of data security. Verdasys rightly believes that making data security information available to business users drives good data stewardship. Verdasys, partnering with IBM, Microsoft, and since Q2 2008 also with Fidelis for network-based extrusion prevention, is a great fit for customers looking for a broad, scalable, agent-driven DLP solution by an independent vendor.

- **RSA Security.** RSA, the security division of EMC, acquired the DLP startup Tablus in 2007 and is now a leading DLP vendor with the strongest discovery features in the market. The RSA solution has both a network appliance and an endpoint/agent piece offering protection for DIM, DIU, and DAR. Network appliances monitor and enforce network traffic, while software agents discover DAR on the desktop or in file shares, and users may deploy them as temporary (or permanent) agents or in high-performance dedicated grids. A rich desktop agent protects data in use. RSA's DLP suite can distinguish between probable and actual content through the use of word proximity, detection rule weighting, and detection rule grouping, and customers can set additional context rules. RSA provides not only rich content analysis but also an underlying modular design (content blades) that can be reused within many policies. RSA still needs to centralize its data policy management across all components, and it also needs to unify reporting, auditing, and case management (introduced in early 2008). RSA also has to improve its endpoint enforcement capabilities. RSA articulates the most ambitious DLP vision of all of the vendors that we rated. It wants to have a reusable set of core technologies for information discovery, classification, and policy orchestration that customers can leverage across various information risk management (RSA) and information management products (EMC). This stretches DLP beyond the realms of security and promises to unlock the greater potential of DLP. RSA has a promising DLP product for companies looking for best-in-class discovery capabilities and a holistic concept for the future that extends to broader information life-cycle management.
- **Vericept.** Vericept is an experienced, well-balanced leader in the DLP market with a proven track record. Most of the firm's many customers use its product as a software-based network DLP safeguarding DIM, but it does much more than that. Vericept protects outbound email with policy-based blocking and encryption, monitors DAR incidents with network and agent discovery products, and controls DIU with real-time content inspection and policy-based blocking and alerting. Vericept also has a broad suite of detection and classification methods to discern probable and actual content, detecting and identifying semantic structures, linguistic constructs, behavioral indications, and concepts. When combined, these techniques enable topical classifiers to discern risk based on the nature and composition of content, transaction, or content disposition. This contextual analysis enables Vericept to detect when content has been paraphrased or rewritten but still has the same meaning. Moreover, this analysis is highly transparent and customizable in implementations, providing a unique level of flexibility. At the desktop, Vericept plans to soon be able to control the print screen command, but it still does not have content-based clipboard copy/paste monitoring and control. More importantly, Vericept

should focus on ease of use and simplicity going forward, as it lost some ground in 2007 due to overly complex deployments and reports that its engine was difficult to manage. Vericept's strategic thinking is based on the idea that an integrated data-centric security model will supplant the current perimeter-centric approach to DLP. Vericept's DLP solution is a good fit for North American companies looking for an experienced vendor with powerful analysis tools, broad coverage across different data domains, and excellent unified management capabilities.

Strong Performers Shine In Specific Areas

- **Workshare.** Document control and protection vendor Workshare has both a DLP network appliance and an endpoint piece. It benefits from tight integration with Microsoft Office, email applications, and its ability to prevent the loss of metadata and hidden data in documents. However, the firm's customers primarily use its solution as a software-based endpoint DLP offering safeguarding DIU. Its network products monitor and filter content by functioning as a network monitor or mail relay; at the desktop, it functions as both an application layer filter and an OS driver. The product monitors all content that users create in office productivity applications such as Outlook and Lotus Notes and checks the content for content policy violations. Workshare Protect is tightly integrated with Microsoft's Rights Management System (RMS); it can automate the process of assigning rights via context-based, content-triggered actions, and it also supports full disk encryption (FDE) for laptops. Currently, Workshare's solution does not control clipboard data and does not protect encrypted channels. It also does not remediate DAR violations, and it lacks tight integration with SIM tools. Workshare's client DLP product has been on the market since 2004 and has almost 2 million installed clients. The firm also enjoys a broad reseller and partner base in many parts of the world. Its enterprise customers seek visibility, order, control, and accountability in a world of unstructured document assets — and they want to stop leaks. Workshare is attractive to customers looking for a bundle of content life-cycle management solutions, including leak prevention; mobile data encryption; data discovery and classification; and integration with change management, document management, and auditing.
- **Orchestria.** Orchestria provides a broad set of DLP, compliance, and other content control solutions. Its DLP product has both network and client/endpoint pieces that leverage a multitude of agents operating in various locations, including desktops, servers, and the network. However, the firm's customers primarily use the solution as software-based endpoint DLP safeguarding DIU. Orchestria has a hardened Network Boundary Appliance (NBA) based on its agent technology. The solution scales by adding processors to the NBA and adding policy engines to analyze data. All agents in the solution use the same policies and analysis techniques, including advanced keywords with proximity detection, negative indicators, weighting, and employee attributes. Orchestria is strongest when used to enforce communications compliance policies, such as those that detail appropriate use of email, PDAs, Web mail, Bloomberg terminals, IM, and blogging. Orchestria's client agents currently offer limited functionality, but

the firm plans to update them significantly in 2008. The product also needs additional agent discovery capabilities, better integration with SIM tools, and enhanced device control capabilities. Orchestria should expand its position beyond DLP and compliance into full information protection and control. The company's vision reflects this, as Orchestria wants to provide an enterprisewide information protection and control layer and a modular, expandable architecture. Orchestria sees the need for these solutions to control and classify all information in order to prevent loss. Orchestria is a great fit for compliance-driven organizations like financial services companies, as well as any company that requires flexible, agent-based DLP protection.

- **Code Green Networks.** Code Green Networks is the strongest DLP solution for smaller companies. The firm's customers primarily use its solution as an appliance-based network DLP offering safeguarding DIM. It includes two major components: one or more Content Inspection Appliances (network-based) and Content Inspection Agents (endpoint-based). Content Inspection Appliances monitor and control network traffic and recognize all TCP protocols, including encrypted traffic through Internet Content Adaptation Protocol (ICAP) integration with a Web proxy. The Content Inspection Agent monitors and controls all file activity on the desktop to and from supported media and communication channels in addition to controlling device-level read/write operations. The products are fully internationalized and localized into English and Japanese. Code Green Networks needs to improve its DAR enforcement capabilities, approach to unified management (particularly relevant for smaller customers), application activity coverage, and forensics features. While the company does not need to provide all enterprise-level DLP features, its SMB customers can certainly demand a broader selection of partners and resellers in all major geographies. Code Green Networks focuses on delivering a DLP solution that is cost-effective, easy to deploy, and easy to use for SMBs and smaller enterprise subsidiaries, and it is clearly dedicated to enhancing value for this clientele. Therefore, the company's road map is geared toward offering a complete DLP offering for this market segment: one that can detect, log, and prevent the unauthorized transmission of sensitive content between any entities, whether inside or outside the corporate network.
- **McAfee.** McAfee bought its way into the DLP market during the past two years by acquiring Onigma and SafeBoot. McAfee's current solution set includes a limited functionality desktop agent DLP piece and a DLP gateway appliance. Its customers primarily use it for its software-based endpoint capabilities safeguarding DIU through device management. McAfee's solution provides multiple layers of protection, including encryption, behavior control and monitoring, and data leak prevention at many activity points. The DLP host monitors all applications that connect to the network stack, monitors and protects access to sensitive data, monitors file activity, and has extensive capabilities for controlling DIU. The DLP Gateway monitors and compares HTTP and SMTP outbound traffic to content-based policies. McAfee did not really have an enterprise-ready product until September 2007, when it rolled out integration with ePolicy Orchestrator (ePO) and included Device Control. Its content analysis, based on keywords and regular expressions, lags the competition. McAfee needs to stick to its 2008 road

map and widen the range of its analysis engine, add DAR discovery capabilities, and improve both content analysis capabilities and enforcement options. McAfee also needs to utilize its host-based footprint and acquired cryptography expertise to enable the encryption of sensitive data once identified by discovery. Still, McAfee has more potential than most other DLP vendors. By carefully integrating its SafeBoot, security suite, and ePO assets, the firm is attractive to many security customers wanting to expand into insider threat prevention. Customers who want to source from fewer vendors and cover the most common insider threat vectors and activities — all managed centrally — will find McAfee's 2008 DLP portfolio attractive.

- **Trend Micro.** In 2007, Trend Micro acquired Provilla, a then-rising endpoint DLP vendor with a solid customer base in Asia Pacific. Today, Trend Micro LeakProof is primarily a software agent-based endpoint DLP offering safeguarding DIU, but it monitors file and network activity at the endpoint as well. The solution relies on network agents to monitor DIM, discovers sensitive DAR, and provides endpoint-based enforcement. Trend Micro offers appliance-based network DLP through a partnership with Reconnex. LeakProof installs a kernel driver that monitors all file system activity and enforces policy on copying files to removable storage media, but it does not filter cut/paste or clipboard operations. The LeakProof engine uses techniques like fingerprinting and matching of regular expressions, keywords, and metadata. Trend Micro supports content filtering in all languages, and it has built-in modules for various international data formats. Trend Micro needs to provide stronger policy management; in particular, it has to simplify the policy building process and enhance classification management. LeakProof must integrate more tightly with data repositories and identity stores. Trend Micro's DLP vision entails offering a range of products featuring DLP: a standalone product; offerings integrating encryption, inbound and outbound antivirus, endpoint software management, and security; and a complete endpoint/gateway security solution. Its ultimate destination is a single policy management point for complete data protection that encompasses technologies like DLP and encryption. Trend Micro is a good fit for international customers looking for a strong endpoint-first solution to integrate into existing security technologies.

Contenders Provide Special Value

- **InfoWatch.** Russia-based InfoWatch, a Kaspersky Lab company, has a solution that provides protection for many DLP use cases. While most customers leverage InfoWatch as a software-based network DLP solution safeguarding DIM, the product also has an endpoint agent that monitors file and network activity to cover DIU. InfoWatch Traffic Monitor filters outgoing mail (SMTP), Web traffic (HTTP), and IM activity, detecting and preventing attempts to transfer confidential data. The product can also prevent copying files to removable devices, printing them, or distributing them via email, IM, and the Web. The product has strong administration capabilities, offers an English-language user interface, and supports multilingual content analysis. InfoWatch has an endpoint agent called Device Monitor, but the agent does not control application-level activity. Customers can define policies based on the type of the removable

device, but they cannot differentiate between specific device manufacturers and serial numbers. Further reasons for its Contender status are the limited range of analytics and shortcomings regarding most forensic and integration criteria. InfoWatch's vision centers on product enhancements and expanding its presence in Europe, the Middle East, and Africa (EMEA), along with introducing a dedicated solution for SMBs. Product enhancements include extending the list of the languages for context filtering; adding support for more protocols like FTP, P2P, IMAP, and MAPI; and supporting more instant messaging platforms. InfoWatch will also support fingerprint analysis in the near future. InfoWatch is a competitive solution for many Russian, Central European, and Middle Eastern customers seeking solid DLP functionality.

SUPPLEMENTAL MATERIAL

Online Resource

The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution:

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their product's functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and readers are encouraged to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve.

ENDNOTES

- ¹ EMC expects Tablus to play a key role in its information-centric security and storage lineup. Tablus' balanced information leak prevention (ILP) offering will benefit both sides of the EMC/RSA house, boosting the latter's run at the title of information and risk market leader. Tablus' data classification capabilities will broaden EMC's Infoscage beyond understanding unstructured data at rest; its structured approach to data detection and protection will provide a data-centric framework that will benefit RSA's security offerings like encryption and key management. While holding a lot of potential, this latest acquisition by one of the industry's heavyweights will require comprehensive integration efforts at both the technology and strategic level. It will also increase the pressure on other large security and systems management vendors to address their organization's information risk management pain points. More importantly, it will be remembered as the turning point that led to the demise of the standalone ILP market as we know it today. See the August 20, 2007, "[EMC/RSA Drafts Tablus For Deeper Data-Centric Security](#)" report.
- ² Today, organizations assume greater accountability for the data they store and process; at the same time, rapidly changing business models force them to make data access more open and allow for greater data and user mobility. The challenge for the security and risk professional is to support these changes while ensuring that data is protected in the way the business demands. Companies are responding to this by shifting their emphasis from traditional measures of bolted-on perimeter and infrastructure protection to deploying a more data-centric approach to security and new approaches to infrastructure architecture. See the February 5, 2008, "[Making Data-Centric Security Real](#)" report.
- ³ Data breaches are embarrassing, painful, and costly — no matter where your organization resides. The UK tax agency, Her Majesty's Revenue and Customs (HMRC), has recently discovered this firsthand after losing 25 million UK citizens' personally identifiable information. Despite well-written policies and good intentions, similar breaches could happen in most European organizations today. Enterprises risk losing customer confidence, reputation, and shareholder value, and the impact of an extensive leak of corporate data could result in losses of similarly epic proportions for their business. Data-centric security and data leak prevention (DLP) technologies don't fix inherently broken processes and eliminate human error, but they do ultimately enable enterprises to better safeguard their information assets based on policies and risk. Ultimately, the HMRC breach — and the others that will undoubtedly follow — will boost European and global enterprise interest in a DLP and data-centric security approach. See the January 16, 2008, "[Oops! Data Leaks Are Not Just An American Problem](#)" report.

- ⁴ To determine Symantec's position in the Forrester Wave evaluation of data leak prevention vendors, Forrester mapped our criteria against information on Symantec's (Vontu's) DLP offerings that were either publicly available or obtained in conversations with the vendor as well as its prospects and customers.
- ⁵ Forrester's evaluation of leading enterprise database auditing and real-time protection vendors across 116 criteria found Guardium and Imperva to have established leadership positions thanks to their enterprise database auditing capabilities, breadth of focus, and strong product and corporate strategy. Tizor Systems, Application Security, and Lumigent Technologies also emerged as Leaders able to handle and support most enterprise database auditing requirements. Symantec, IBM Consul InSight (recently renamed Tivoli Compliance Insight Manager), RippleTech, Embarcadero Technologies, and Oracle are Strong Performers best suited, because they lack a comprehensive set of auditing, real-time protection, and other features and functionality, to basic to moderate auditing requirements. Oracle's database management system (DBMS) tops other DBMS vendors by having the best set of native auditing features; Microsoft, Sybase, and IBM DB2 trail, largely because they have only basic auditing capabilities. Although IBM Audit Management Expert (AME) offers only basic auditing capabilities, it integrates well with IBM's DB2 and IMS DBMSes running on the mainframe. See the October 26, 2007, "[The Forrester Wave™: Enterprise Database Auditing And Real-Time Protection, Q4 2007](#)" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations,
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866.367.7378, +1 617.617.5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. For more than 24 years, Forrester has been making leaders successful every day through its proprietary research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.