The Forrester Wave™: Endpoint Encryption, Q1 2015
by Chris Sherman, January 16, 2015

KEY TAKEAWAYS

Sophos And Intel Security Are Leading Vendors
Forrester’s research uncovered a market in which Sophos and Intel Security (McAfee) lead the pack. Wave Systems, WinMagic, Symantec, Novell, and Kaspersky Lab offer competitive options.

The Encryption Market Is Growing As S&R Pros Look For Comprehensive Support
The endpoint encryption market is growing because more S&R pros see full disk, file-level, and media encryption as ways to address their top challenges. This market growth is in large part due to the fact that S&R pros increasingly must use endpoint encryption to protect against device loss and the possible fallout of noncompliance.

Deployment And Support For Future Tech Are Key Differentiators In The Market
As hardware-based encryption technology becomes outdated and less effective, support for self-encrypting drives and other emerging encryption technologies will dictate which providers will lead the pack. Vendors that can provide encryption position themselves to successfully deliver comprehensive and efficient security solutions to their customers.

Access The Forrester Wave Model For Deeper Insight
Use the detailed Forrester Wave model to view every piece of data used to score participating vendors and create a custom vendor shortlist. Access the report online and download the Excel tool using the link in the right-hand column under “Tools & Templates.” Alter Forrester’s weightings to tailor the Forrester Wave model to your specifications.
The Forrester Wave™: Endpoint Encryption, Q1 2015
Tools And Technology: The Data Security Playbook
by Chris Sherman
with Stephanie Balaouras and Andrew Hewitt

WHY READ THIS REPORT

Security and risk (S&R) professionals often turn to endpoint encryption technologies to protect corporate data, meet regulatory requirements, and prevent accidental data leaks. Full disk, file-level, and media encryption are three of the most commonly used technologies, with many vendors offering multiple options within the same product/suite. In Forrester's 52-criteria evaluation of endpoint encryption vendors, we identified the seven most significant providers in the category and researched, analyzed, and scored them. This report details our findings about how well each vendor fulfills our criteria and where they stand in relation to each other, to help S&R professionals select the right partner for their endpoint encryption strategy.

Table Of Contents

2 Unencrypted Endpoints Place Your Organization At Risk
3 Endpoint Encryption Offers Protection Beyond Simple Compliance
4 Endpoint Encryption Evaluation Overview
6 Evaluation Analysis
8 Vendor Profiles
10 Supplemental Material

Notes & Resources

Forrester conducted product evaluations in August and September 2014 and interviewed seven vendor companies: Intel Security (McAfee), Kaspersky Lab, Novell, Sophos, Symantec, Wave Systems, and WinMagic.

Related Research Documents

The State Of Endpoint Security Adoption 2014 To 2015
September 24, 2014

TechRadar™: Data Security, Q2 2014
April 22, 2014

Market Overview: Endpoint Encryption Technologies, Q1 2013
January 16, 2013
UNENCRYPTED ENDPOINTS PLACE YOUR ORGANIZATION AT RISK

Employees work with corporate data at home, work, and everywhere in between. An explosion of consumer devices and services has fueled on-the-go computing and a blurring of work and personal lives; consider that 52% of information workers report taking their work outside the office at least a few times per month (see Figure 1). More likely than not, your digital workers are carrying sensitive corporate data on their endpoints, ultimately increasing the risk that a data leak or compliance breach event could occur.

Figure 1 Your Employees (And Your Corporate Data) Are On The Move

“How often do you work in your job from the following locations?”

<table>
<thead>
<tr>
<th>Location</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>From your home (e.g., telecommuting)</td>
<td>36%</td>
</tr>
<tr>
<td>From a client site</td>
<td>29%</td>
</tr>
<tr>
<td>While traveling or commuting (e.g., train)</td>
<td>22%</td>
</tr>
<tr>
<td>Other/public work site (e.g., coffee shop, library)</td>
<td>18%</td>
</tr>
</tbody>
</table>

Base: 7,032 global information workers (multiple responses accepted)

Source: Forrester’s Business Technographics Global Telecom And Mobility Workforce Survey, 2014

Device Loss — A Top-Of-Mind Risk To Your Firm’s Endpoint Security

Considering the mobile nature of today’s workforce, a laptop, tablet, smartphone, or thumb drive holding unprotected sensitive data can all be ticking time bombs for security incidents. According to Forrester’s Business Technographics® Global Security Survey, 2014, device loss or theft precipitated 23% of all data breaches. One healthcare CISO recently told Forrester that employee device loss caused him more concern than the threat of attack from malicious outsiders. If S&R pros don’t protect sensitive data stored on those devices, they are simply inviting a serious security incident to occur. Common data types that S&R pros consider most at risk include:

- **Customer data.** This includes your customers’ credit card numbers; personally identifiable information (PII) such as name, address, phone numbers, and social security numbers; and sensitive records such as personal health information (PHI). It’s common for employees to download and work on client deliverables locally on their machine while they’re on the road, commuting, or simply working from home. News stories of lost or stolen laptops containing sensitive data abound.
■ **Employee data.** Human resources handle employee records that contain PII and PHI and thus are subject to the same data privacy and protection laws as customer data.

■ **Company confidential data.** Organizations often consider any nonpublic company data confidential. This may include company financial data, sales record, revenue breakdown, or market data on individual product lines.

■ **Intellectual property.** A company’s intellectual property data, such as source code, design drawings, or research and development data, can erode or permanently erase that company’s long-term competitive advantage if lost or stolen.

---

**Legislative Pressures Augment The Potential Fallout From A Data Loss Event**

Fallout from data loss precipitated by a lost laptop or any other data vehicle, such as a smartphone, tablet, or USB drive, can also lead to major regulatory fines, depending on the type of data exposed. Most S&R pros are concerned with regulations and fines originating from:

■ **A patchwork of data protection laws across the globe.** In the European Union (EU), for example, there is the overarching EU Data Protection Directive, but each of the 28 member-states also has its own national laws to implement the directive locally. Look to Forrester's data privacy heat map for a country-by-country comparison of 54 data protection frameworks around the globe.

■ **Governments and other bodies that implement industry-specific regulations.** For example, at the federal level in the US, both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009 target the protection of personal health information. The Financial Services Authority in the UK has had a strong role in ensuring the protection of financial clients' information.

■ **Breach notification laws enacted by a majority of US states.** In the US, state laws such as California Senate Bill 1386 (SB-1386) and the Massachusetts Data Protection Law (MA 201) require notification of security breaches involving personal information. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands have enacted breach notification legislation.

---

**ENDPOINT ENCRYPTION OFFERS PROTECTION BEYOND SIMPLE COMPLIANCE**

While many S&R pros initially turn to endpoint encryption in order to meet regulatory requirements for data protection, endpoint encryption offers significant benefits beyond compliance. S&R professionals should view endpoint encryption not merely as a compliance “check box,” but as an essential tool in their arsenal of data protection. More specifically, endpoint encryption:
■ **Discourages would-be attackers by eliminating their ability to monetize the stolen data.** When you encrypt your endpoint data and properly protect the keys, a captured endpoint is essentially useless to malicious individuals. Encryption helps to devalue or “kill” your sensitive data, such as intellectual property or customer data, and to deter would-be attackers from device theft and other malicious activities. As a general rule, cybercriminals cannot sell encrypted data in the open markets on the invisible Internet; encrypted data has no value, thus destroying malicious actors’ primary incentive to steal it.9

■ **Reduces scope for compliance.** When you encrypt your data and protect your keys properly, your data can be declared out of scope for compliance by several regulation and industry standards. The HITECH Act, for instance, includes stringent data breach notification requirements. The only way around that is if the data breached is in an encrypted format.

■ **Provides a tool for secure data life-cycle management.** When you decommission your endpoints, cybercriminals can extract data resident on the device even if you’ve reformatted the hard disk. Endpoint encryption provides a safe way of device decommission — simply encrypt and destroy the key, and your hard disk will be indistinguishable from a pool of random bits.

### The Encryption Market Is Mature With Several Key Areas Of Innovation

Endpoint encryption vendors typically offer a combination of endpoint full disk/volume encryption, file/folder encryption, and/or media encryption, ideally managed through a single console or integrated suite. These three “core” technologies are relatively mature; differentiation between vendors occurs primarily in their deployment flexibility and support for current and future encryption technologies.

For example, an organization with a variety of old and new hardware may benefit from a vendor that supports both self-encrypting drives and native encryption (BitLocker, FileVault) as well as software encryption for older hardware. Other organizations may prioritize a need for preboot network authentication to decrease operational friction with other IT processes, while multi-factor authentication support (TPM, smart cards, biometrics) may be a priority in higher-risk environments. Each of these technologies is a key area of innovation in the endpoint encryption market today.

### ENDPOINT ENCRYPTION EVALUATION OVERVIEW

To assess the state of the endpoint encryption market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top endpoint encryption vendors.
This Evaluation Highlights Product Capabilities, Vendor Strategy, And Market Reach

After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 52 criteria, which we grouped into three high-level buckets:

- **Current offering.** The vertical axis of the Forrester Wave graphic reflects the strength of each vendor’s product offering.

- **Strategy.** The horizontal axis measures the viability and execution of each vendor’s strategy, which includes the company’s market experience, future vision, integration strategy, global presence, and engineering staff.

- **Market presence.** The size of each vendor’s bubble on the Forrester Wave graphic represents each vendor’s presence in the endpoint encryption market, based on metrics such as install base, revenue, and partner ecosystem.

This Evaluation Focuses On The Top Seven Endpoint Encryption Products

Forrester included seven vendors in the assessment: Intel Security (McAfee), Kaspersky Lab, Novell, Sophos, Symantec, Wave Systems, and WinMagic. Each of these vendors has (see Figure 2):

- **Components that were available as of September 9, 2014.** Any feature or product releases after September 9, 2014 were not part of the product evaluation.

- **Multiple endpoint encryption technologies under one roof.** Full disk/volume encryption, file-level encryption, and some form of media protection are all requirements for inclusion in this study.

- **A sizable enterprise market presence.** Vendors must have over 1,000 enterprise (defined as firms with 1,000 or more employees) customers and/or 1 million endpoint encryption licenses sold since the product’s release.

- **Significant enterprise interest.** Vendor participants are all frequently mentioned and asked about by our clients via Forrester inquiries and projects.
Figure 2 Evaluated Vendors: Evaluation Criteria And Product Information

To be included in this evaluation, selected providers had to meet the following criteria:

- Components that were available as of September 9, 2014
- Full disk/volume, file level, and media protection support
- A sizable enterprise market with either 1,000 enterprise customers or 1 million endpoint licenses sold
- A sufficient level of interest from the Forrester client base

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Security</td>
<td>McAfee Complete Data Protection Advanced</td>
</tr>
<tr>
<td>Kaspersky Lab</td>
<td>Kaspersky Endpoint Security Advanced</td>
</tr>
<tr>
<td>Novell</td>
<td>Novell ZENworks Suite</td>
</tr>
<tr>
<td>Sophos</td>
<td>SafeGuard Enterprise</td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Endpoint Encryption</td>
</tr>
<tr>
<td>Wave Systems</td>
<td>EMBASSY Remote Administration Server (ERAS)</td>
</tr>
<tr>
<td>WinMagic</td>
<td>SecureDoc Enterprise Server</td>
</tr>
</tbody>
</table>

EVALUATION ANALYSIS

The evaluation uncovered a market in which (see Figure 3):

- **Sophos and Intel Security lead the pack.** Both security vendors have a deep focus on serving enterprise customers, offering the flexibility and depth required by the most demanding environments. Strong hardware and native encryption support, combined with solid operating system support across a range of endpoint encryption technologies, sets the Leaders apart from the rest in this study.

- **Wave Systems, WinMagic, Symantec, Novell, and Kaspersky offer competitive options.** Each of the vendors offering competitive options are strong in specific areas such as support for self-encrypting drives (SEDs), native encryption management, and file sharing, but none have the overall breadth of offerings and enterprise focus demonstrated by the Leaders in this study.
This evaluation of the endpoint encryption market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

**Figure 3 Forrester Wave™: Endpoint Encryption Market, Q1 2015**

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.
Figure 3 Forrester Wave™: Endpoint Encryption Market, Q1 2015 (Cont.)

<table>
<thead>
<tr>
<th>CURRENT OFFERING</th>
<th>Forrester’s Weighting</th>
<th>Intel Security</th>
<th>Kaspersky Lab</th>
<th>Novell</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Wave Systems</th>
<th>WinMagic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint full-disk/volume encryption</td>
<td>50%</td>
<td>3.56</td>
<td>2.65</td>
<td>2.57</td>
<td>4.04</td>
<td>3.30</td>
<td>2.84</td>
<td>3.34</td>
</tr>
<tr>
<td>File/folder encryption</td>
<td>30%</td>
<td>4.28</td>
<td>2.12</td>
<td>2.52</td>
<td>4.40</td>
<td>2.62</td>
<td>2.97</td>
<td>4.17</td>
</tr>
<tr>
<td>External media encryption</td>
<td>20%</td>
<td>2.92</td>
<td>4.10</td>
<td>2.92</td>
<td>4.74</td>
<td>4.13</td>
<td>1.71</td>
<td>2.06</td>
</tr>
<tr>
<td>Management console functionality</td>
<td>13%</td>
<td>3.50</td>
<td>2.57</td>
<td>2.81</td>
<td>4.60</td>
<td>3.78</td>
<td>4.04</td>
<td>4.08</td>
</tr>
<tr>
<td>Agent</td>
<td>12%</td>
<td>3.80</td>
<td>2.90</td>
<td>2.40</td>
<td>3.00</td>
<td>2.90</td>
<td>3.30</td>
<td>3.00</td>
</tr>
<tr>
<td>Cryptographic certifications</td>
<td>9%</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>5.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Data loss prevention capabilities</td>
<td>8%</td>
<td>4.40</td>
<td>1.00</td>
<td>1.80</td>
<td>4.40</td>
<td>3.20</td>
<td>3.00</td>
<td>3.20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STRATEGY</th>
<th>Forrester’s Weighting</th>
<th>Intel Security</th>
<th>Kaspersky Lab</th>
<th>Novell</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Wave Systems</th>
<th>WinMagic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product strategy</td>
<td>50%</td>
<td>3.60</td>
<td>3.09</td>
<td>3.24</td>
<td>4.00</td>
<td>3.33</td>
<td>4.24</td>
<td>3.73</td>
</tr>
<tr>
<td>Corporate strategy</td>
<td>35%</td>
<td>4.30</td>
<td>4.40</td>
<td>2.30</td>
<td>4.40</td>
<td>3.70</td>
<td>4.40</td>
<td>4.30</td>
</tr>
<tr>
<td>Cost</td>
<td>20%</td>
<td>3.00</td>
<td>1.00</td>
<td>1.50</td>
<td>4.00</td>
<td>2.00</td>
<td>4.00</td>
<td>4.00</td>
</tr>
<tr>
<td>Customer references</td>
<td>20%</td>
<td>2.10</td>
<td>2.10</td>
<td>4.40</td>
<td>3.80</td>
<td>4.40</td>
<td>3.60</td>
<td>3.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MARKET PRESENCE</th>
<th>Forrester’s Weighting</th>
<th>Intel Security</th>
<th>Kaspersky Lab</th>
<th>Novell</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Wave Systems</th>
<th>WinMagic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed base</td>
<td>0%</td>
<td>3.93</td>
<td>2.63</td>
<td>2.56</td>
<td>4.17</td>
<td>4.37</td>
<td>3.10</td>
<td>2.27</td>
</tr>
<tr>
<td>Financial viability</td>
<td>20%</td>
<td>3.67</td>
<td>0.67</td>
<td>1.98</td>
<td>4.33</td>
<td>5.00</td>
<td>2.67</td>
<td>3.33</td>
</tr>
<tr>
<td>Services</td>
<td>20%</td>
<td>3.50</td>
<td>1.00</td>
<td>3.00</td>
<td>4.50</td>
<td>4.00</td>
<td>3.50</td>
<td>2.50</td>
</tr>
<tr>
<td>Employees</td>
<td>20%</td>
<td>4.50</td>
<td>5.00</td>
<td>3.00</td>
<td>4.00</td>
<td>5.00</td>
<td>3.50</td>
<td>3.00</td>
</tr>
<tr>
<td>Technology partners</td>
<td>20%</td>
<td>4.00</td>
<td>2.50</td>
<td>1.50</td>
<td>5.00</td>
<td>3.50</td>
<td>4.50</td>
<td>1.50</td>
</tr>
</tbody>
</table>

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

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

VENDOR PROFIL ES

Leaders

- **Sophos.** Sophos was the breakout star in this Forrester Wave evaluation, touting strong hardware-based encryption support, external media encryption policy flexibility, and file-level encryption functionality. Security and operations admin will appreciate Sophos’ deep policy granularity and deployment flexibility in a variety of environments and use cases. Sophos has also demonstrated a commitment to supporting Mac OS across its entire product portfolio, which includes a full spectrum of endpoint security offerings. When we surveyed them, Sophos’ user support offerings and ease of deployment were consistently rated as exemplary by customers.
However, customer feedback regarding the overall functionality of Sophos’ SafeGuard Encryption uncovered only a modest level of user satisfaction. Certain enterprise buyers may also be turned off by Sophos’ reliance on native encryption technologies for full disk/volume encryption on Mac OS and Windows 8 and 8.1. Despite this, their broad portfolio of endpoint encryption offerings, combined with an easy-to-use user interface and strong product support capabilities, should warrant Sophos’ inclusion on any enterprise buyer’s shortlist.

- **Intel Security.** Intel’s 2010 acquisition of McAfee has benefited the McAfee endpoint encryption line through integration of multiple R&D efforts between the hardware teams at Intel and McAfee’s software engineers. For example, buyers will appreciate enhanced deployment flexibility and management capability offered through the use of Intel’s vPro AMT technology and the endpoint encryption agent’s preboot environment. Additionally, McAfee’s use of Intel’s AES-NI hardware encryption technology has been optimized beyond what most other vendors in this study offer.

It is worth noting, however, that the McAfee Complete Data Protection — Advanced suite was one of the most expensive in this study. Furthermore, despite a focus on supporting Mac OS throughout most of its product portfolio (which includes a number of larger endpoint security suite offerings), its breadth of supported operating systems is lacking for folder/file encryption. These issues aside, Intel’s dominant market presence, combined with strong support for current and future encryption trends, reaffirms its position as a Leader in the endpoint encryption space.

**Strong Performers**

- **Wave Systems.** Wave Systems offers a number of endpoint encryption products focused on endpoint encryption management and data loss prevention. As one of the early supporters of self-encrypting drives, Wave Systems has a comprehensive level of support for SEDs and hardware encryption. It is also the only vendor that offers a hosted model for endpoint encryption management. On the downside, Wave Systems’ file encryption solution is not as broad in its feature set as others in this study, lacking ancillary technologies such as centralized file sharing or mobile device encryption. Recent financial issues with the company may also give some enterprise buyers pause.

- **WinMagic.** WinMagic groups all of its endpoint encryption and mobile device management solutions under the SecureDoc product line. As one of the earliest vendors to offer self-encrypting drive and preboot network authentication support, its endpoint encryption technologies are some of the most forward-leaning in this study. WinMagic’s network-aware preboot technology (PBConnex) also received positive mentions on a number of Forrester customer inquiry calls due to its usefulness in reducing the operational overhead associated with encryption management. On the downside, its data loss prevention and central reporting capabilities lack some of the more advanced features offered by others in the study.
■ Symantec. Symantec’s full disk/volume encryption solution comes from its 2010 acquisitions of PGP and GuardianEdge. Symantec has recently released a new Endpoint Encryption product that combines best-of-breed technologies from these two acquisitions into a single console, consolidating both disk and removable media encryption. Symantec’s file/folder and email encryption solutions continue to be managed by their original solution consoles, which are separate products. During our interviews, customers reported frustration with the overall product functionality and deployment ease. Additionally, Symantec lacks mobile OS support for many of its endpoint encryption functions as well as support for many popular hardware and native encryption technologies such as SEDs, BitLocker, and Trusted Platform Modules. Despite these drawbacks, Symantec’s solution can deliver on a strong data loss prevention strategy through multiple DLP product offerings and integrations at an extremely attractive price point.

■ Novell. Novell offers endpoint encryption as either a standalone product or integrated component to its overall ZENworks IT management suite. Customers of both will enjoy seamless integration between the two from both a management and policy point of view. Enterprise users of Novell report to Forrester an overall high level of satisfaction with the product due to its ease of use and strong product support. However, due to limited hardware encryption and native encryption/OS support, Novell performed in the bottom of the pack in this study. Enterprise buyers looking for an inexpensive point product or existing customers of ZENworks looking for a consistent user experience/management platform will have strong interest in Novell solutions. Others will likely be disappointed by the lack of overall functionality when compared with some of the more advanced solutions on the market.

■ Kaspersky Lab. Kaspersky’s endpoint encryption solution is unique in that its endpoint encryption offerings are not sold separately from its overall endpoint security suite. Thus, security and operations professionals benefit from a high level of management and policy integration between the two. Its mobile offerings for file level and media encryption are also comprehensive and span its endpoint encryption, file/folder encryption, and media control. However, Kaspersky has the distinction of being the only vendor to lack support for self-encrypting drives as well as native OS encryption in this study. While Kaspersky’s endpoint encryption offerings may work well for firms looking to source an all-in-one endpoint security suite at an attractive price point, its lack of deployment flexibility and support for advanced encryption features may be enough to give certain enterprise buyers pause.

SUPPLEMENTAL MATERIAL

Excluded Vendors
We invited Microsoft and Dell to participate in this Forrester Wave, and they accepted. However, both withdrew after the evaluation criteria were released to the vendors. Since neither vendor participated during the evaluation stage of the Forrester Wave process, Forrester excluded them from the final analysis.
Online Resource

The online version of Figure 3 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 surveys.** To validate product and vendor qualifications, Forrester also conducted reference surveys with at least 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 we encourage readers 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. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.
Survey Methodology

Forrester’s Business Technographics® Global Telecom And Mobility Workforce Survey, 2014, was fielded to 7,032 information workers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester’s Business Technographics and was fielded during January 2014 and February 2014. Toluna fielded this survey online on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.

Integrity Policy

All of Forrester’s research, including Forrester Waves, is conducted according to our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

ENDNOTES

1 We define work outside the office as work “from a client site,” “from your home (e.g., telecommuting),” “while traveling or commuting (e.g., train),” or “other/public work site (e.g., coffee shop, library).” Source: Forrester’s Business Technographics® Global Telecom And Mobility Workforce Survey, 2014.

2 Protecting customer data such as credit card information, log-in credentials, and personally identifiable information is an important part of enterprise IT security. Such data fuels a large and lucrative underground market economy. However, as the threat landscape continues to evolve, chief information security officers (CISOs) must adjust their risk management strategies accordingly to counter the next frontier: intellectual property theft. For more information on protecting customer data, see the June 5, 2014, “The Future Of Data Security: A Zero Trust Approach” report.

3 The threat landscape for cybercriminals is growing, and S&R professionals must update their risk management programs to include intellectual property. For more information, please see the August 6, 2014, “The Cybercriminal’s Prize: Your Customer Data And Competitive Advantage” report.

4 Stealing such information directly — or purchasing such information on the side — can shave off years and millions if not billions of dollars in research and development. The theft also provides a company’s competitors with deep insight into what the company is thinking and doing. See the August 6, 2014, “The Cybercriminal’s Prize: Your Customer Data And Competitive Advantage” report.

5 This heat map allows you to view data security policies through a number of filters, including privacy and data protection by country, scope of protection, covered entities, and much more. See the August 6, 2014, “Forrester’s 2014 Data Privacy Heat Map” report.

6 The American Recovery and Reinvestment Act of 2009 (ARRA) includes a section that expands the reach of HIPAA. This section, also known as the HITECH Act, expands the reach of HIPAA to include “business associates,” also known as service providers to HIPAA-covered entities. Under the HITECH Act, the business associates are now directly subject to HIPAA’s security and privacy requirements.
7 The FSA is an independent body that regulates the financial services industry in the UK. Source: Financial Services Authority (FSA) (http://www.fsa.gov.uk/Pages/About/index.shtml).


9 For more information, see the July 12, 2012, “Kill Your Data To Protect It From Cybercriminals” report.
About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world’s top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION
To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT
For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On
Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester’s subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

Sean Rhode S, client persona representing Security & Risk Professionals