Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

COMPETITIVE ANALYSIS

IDC MarketScape: Worldwide Messaging Security 2013–2014 Vendor Assessment

Phil Hochmuth

IN THIS EXCERPT

The content for this paper is excerpted from the IDC MarketScape: Worldwide Messaging Security 2013-2014 Vendor Assessment, (Doc # 244065). All or parts of the following sections are included in this Excerpt: IDC Opinion, In This Study, Situation Overview, Future Outlook, Vendor Summary, Essential Guidance and Learn More. Figure 1 is also included.

IDC OPINION

While messaging security is a mature market, experiencing slowing growth, email remains the single greatest threat vector for some of the most sophisticated, targeted attacks on organizations and individuals. Instead of the broad spam campaigns of the past, attackers now focus on individuals with access to potentially valuable data or people with credentials that could be hijacked and used for other types of cyberattacks and break-ins. Typically, these attacks involve an email, targeting an individual or a small group, with either a Web link leading to malware or an attachment with malicious code not seen before by threat research labs, which create antivirus signatures. Another key challenge in enterprises is the rise in mobility. Organizations struggle to know what types of sensitive data end users are sending as messages or attachments, especially as they access corporate email systems from personal or BYO-type devices. In this IDC MarketScape, IDC assesses the current messaging security vendor landscape and considers the future of the market with regard to new delivery models and feature requirements. Vendor attributes considered include:

- **Breadth of capabilities.** Key capabilities required from messaging security solutions go beyond basic antispam and malware blocking capabilities. Core requirements from enterprises now include advanced encryption options, data loss prevention, integrated management of on-premise/cloud services (i.e., hybrid), and integration with adjacent technologies such as email archiving and storage.
- **Range of form factors and delivery models.** Enterprises are increasingly looking to offload antispam and malware inspection capabilities to cloud-based or software-as-a-service (SaaS) messaging security services. Vendors not offering these solutions are ignoring the future of the market. Meanwhile, many enterprises still have specific on-premise email filtering requirements, especially around data loss prevention (DLP) traffic inspection. Compliance and data residency issues also require some organizations to filter on-premise. For these reasons, having a broad spectrum of delivery models is key.
- **Adjacencies to other security technologies.** Email security solutions do not operate in a vacuum; these platforms must correlate threats across adjacent security technologies — from endpoint to network and Web security — as well as integrate with identity solutions and backend security information and event management (SIEM) platforms.
- **Scalability and availability.** In spite of its maturity, and the rise of other communications medium (social, mobile, and collaborative applications), email is still the primary business communications platform for most organizations. Interruption of service due to influxes of spam and viruses, or failure of gateway solutions to provide service continuity, can cripple workforce productivity

Filing Information: November 2013, IDC #244065, Volume: 1
Security Products: Competitive Analysis

IN THIS STUDY

Methodology

This IDC MarketScape is designed to provide an overview of the competitive fitness of the global solutions providers in the messaging security market. A single chart displays each company's market share and indicates whether the company is overperforming or underperforming and how well it is suited to compete in the market today and in the future (in the next three to five years). The accompanying text explains each vendor's major strengths and weaknesses.

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

IDC employs the following methodology to arrive at each company's ranking:

- **Sources.** This study is based on a model that is populated with data provided to IDC from a vendor questionnaire, companies' quarterly and annual reports, earnings calls, industry analyst events, interviews with company representatives, interviews with end users, IDC research, and news coverage. For this IDC MarketScape, IDC conducted interviews with over 20 end users from private enterprises, government, and education who make purchasing decisions for messaging security technology. IDC also spoke with over a dozen resellers and integrators of messaging security technology for the participating vendors in this study, to gauge the overall business strategy and relationship the vendors had with these key channel partners. IDC also used data from its *2013 U.S. Cloud Security Survey* and *2013 U.S. Mobile Security Survey* as the basis for scoring and weighting criteria and assumptions.

- **Market shares, growth rates, and revenue numbers.** This IDC MarketScape covers the messaging security market. For companies that do not publicly disclose this revenue, IDC estimates revenue and growth rates based on public information, discussions with vendors, knowledge of the industry, and input from regional IDC analysts.

- **Competitive fitness.** Each major competitor's preparedness for current and future market conditions is expressed as a set of two scores. One score expresses a given vendor's current "capabilities," while the other score expresses the appropriateness of its "strategies" for the future. (IDC bases its assessment of future market conditions on what most likely will be the market's major trends and disruptors.) Each of the two scores is broken down into three criteria (product offerings, go-to-market capabilities, and business capabilities), each of which is in turn broken down into

several subcriteria. Both criteria and subcriteria are weighted by importance for a particular market. For each company, we score its qualities with regard to each of the subcriteria, assigning a numeric value. The IDC MarketScape model uses these values to calculate each company's score for each of the criteria and rolls these values to arrive at the described set of two scores.

Messaging Security Market Definition

Messaging security includes antispam, antimalware, content filtering, encryption, data loss prevention (DLP), and information protection and control (IPC) products for messaging applications such as email and other types of collaborative applications. Messaging security products are deployed on software, appliance, SaaS, and virtual security platforms.

For the purposes of this study, IDC included vendors and products largely defined as secure email gateways, which integrate most of the features outlined in the previously mentioned market definition onto a single product offering, delivered via on-premise software and appliances or via the cloud. Special consideration was given to bundled deployments of these form factors, or hybrid deployments, as well. Vendors with individual feature-based messaging security technologies, such as messaging encryption gateways or antispam-only services, were not evaluated.

SITUATION OVERVIEW

Introduction

The worldwide messaging security market is a mature market, with 3% growth over the past two years. Vendors in this market are well established and have had solutions for as long as a decade. Traditionally, messaging security solutions — antispam or antimalware — were deployed as software applications on servers, either along with or directly on email servers in the enterprise. As the market matured, appliances emerged as a popular form factor for message scanning, as large volumes of spam and email attachment viruses often bogged down server-based or email systems–based scanning engines.

Cloud/SaaS solutions also evolved to help cut down on spam and email-based malware. Cloud-based messaging security solutions offload compute-intensive tasks such as sender reputation scoring, suspicious attachment, or embedded URL inspection and leverage a wider base of intelligence and information on email threats via connections to Internet-based reputation services and service provider network blacklists.

Antispam and malware scanning of email is largely a commoditized market that is very sensitive to price — the lowest per-seat cost per end user often wins. However, more advanced requirements from messaging security solutions are emerging from enterprises, such as data loss prevention, specialized threat detection, integrated e-archiving and message traffic management, and integrated content security capabilities.

Deployment requirements for messaging security also vary widely among customers, based on the size, vertical market, and geography of the customer. One deployment model — whether appliance, software, or SaaS — does not fit all buyers. Organizations

with particular data sensitivity concerns often consider on-premise hardware/software deployments over cloud services, as some providers cannot guarantee that message data will be processed and archived in a specific country or region. Meanwhile, other organizations looking for flexibility and low cost turn to cloud-based solutions. Additionally, some organizations want both on-premise messaging scanning for sensitive data inspection or specialized encryption capabilities and cloud-based filtering to offload more commoditized spam and malware screening (known as a hybrid deployment model).

While spam and infected email attachments can still inhibit enterprise infrastructure stability and productivity, more acute threats include the loss or exposure of sensitive data via messaging platforms and targeted or specialized attacks aimed at individuals in an organization, which use email as the initial point of interaction. To that end, enterprises IDC spoke with for this study cited DLP and targeted attack protection (TAP) as two key features required in messaging security gateways.

In the majority of organizations IDC spoke with for this IDC MarketScape, the teams purchasing and using messaging security solutions were from part of their company's messaging, email, or communications infrastructure groups, as opposed to the network or information security or risk management teams. As such, requirements beyond pure security were also key for many end users. Users were interested in the ability to bundle message archiving with security features as well as more advanced features such as ediscovery and legal hold of email messages.

FUTURE OUTLOOK

IDC MarketScape: Worldwide Messaging Security Vendor Assessment

The IDC vendor assessment for the enterprise messaging security market represents IDC's opinion on which vendors are well positioned today through current capabilities and which are best positioned to gain market share over the next few years. Positioning in the upper right of the grid indicates that vendors are well positioned to gain market share. For the purposes of discussion, IDC divided potential key strategy measures for success into two primary categories: capabilities and strategies.

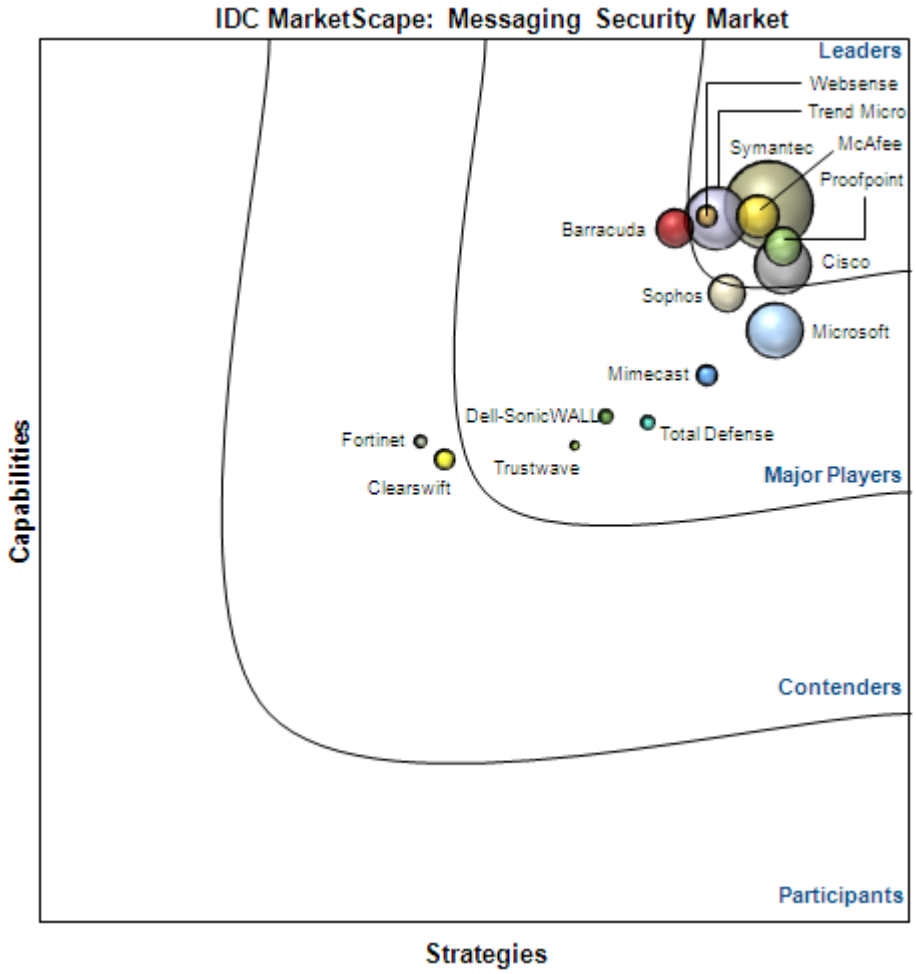
Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned it is to customer needs. The capabilities category focuses on the capabilities of the company and the product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in the next three to five years. The strategy category focuses on high-level strategic decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the future, in this case defined as the next three to five years. Under this category, analysts look at whether or not a supplier's strategies in various areas are aligned with customer requirements (and spending) over a defined future time period. Figure 1 shows each

vendor's position in the vendor assessment chart. A vendor's market share is indicated by the size of the bubble.

FIGURE 1

IDC MarketScape: Worldwide Messaging Security Vendor Assessment



Source: IDC, 2013

Vendor Profiles

Trend Micro

Trend Micro offers software, virtual appliance, and SaaS gateways and software for Microsoft Exchange and IBM Domino servers. Trend Micro's InterScan messaging security products are focused on enterprises and SMBs. The vendor has been in the market since 1995 and is among the first security companies to offer a mail protection product. As a top-tier antimalware vendor, Trend leverages a vast threat intelligence and

research organization and a global threat intelligence cloud service for correlating information on new types of malware and threats, as well as a delivery mechanism for updating products via the cloud. Trend is also one of the five content security "triple threat" messaging security vendors, with Web and DLP technologies also among its offerings. In addition, Trend's Deep Discovery solution is a specialized threat product the company plans to tightly integrate with its messaging security solutions providing advanced threat detection.

IDC has placed Trend Micro in the Leaders section in this IDC MarketScape. This reflects Trend Micro's completeness of portfolio across on-premise, cloud-based, and hybrid messaging security offerings, with extra consideration of the vendor's efforts around DLP and STAP integration into these platforms.

Strengths

- Trend has strong DLP capabilities, which are built into its messaging security solutions as base features, as opposed to add-on upgrades or modules. Its DLP technology includes both channel-based DLP as well as advanced document fingerprint recognition and support for complex remediation workflows.

- A complementary Web security gateway solution allows enterprises to deploy Trend messaging and Web security technologies in concert with the ability to correlate potentially malicious Web-based URLs embedded in emails at the Web gateway, allowing active detection of click activity of end users following malicious links.

- Trend's Smart Protection Network — a global threat intelligence cloud — is an invaluable asset behind the company's messaging security SaaS solution, as well as its on-premise software/VA offerings. The tight integration of SPN with Trend's cloud security services allows the vendor to quickly identify and react to emerging threats in the cloud and rapidly deploy defenses via its security SaaS to protect customers.

- Trend has offerings in the STAP category, including a standalone STAP appliance, as well as an integrated functionality within its on-premise email gateway. The ability to detect unique malware and block targeted attack attempts via email is a top priority among messaging security technology buyers.

- With over 1,200 threat researchers, Trend has the greatest security intelligence and research teams among its competitors.

Challenges

- Trend is among the only on-premise messaging security product vendors without an appliance-based product offering. This limits Trend from some opportunities as many enterprises prefer an integrated hardware appliance for message filtering. However, Trend has a strong support for virtual appliances, which are an increasingly popular deployment option, and it can also deploy its software-as-a-"bare metal" appliance image on the standard x86 hardware.

- Trend's cloud service is relatively low in scale with regard to the number of messaging-processing datacenters deployed and the amount of messages the company processes per day, compared with large competitors of a similar size.

- While Trend's tightly integrated security solutions approach appeals to enterprise security and risk teams, the vendor lacks some messaging infrastructure–focused offerings (such as message archiving, ediscovery, and collaboration tools management), which appeal to the enterprise messaging infrastructure technology staff who are the primary buyers of email security solutions.

Opportunities

- Trend Micro has all the core messaging and adjacent security technologies required to address the top challenges to enterprises, such as data loss, targeted attacks, and protecting mobile and remote users. As it increases capabilities around its cloud-based security products beyond messaging security, Trend will be well positioned to meet customers' transitions to cloud and SaaS IT service models.

ESSENTIAL GUIDANCE

The messaging security market is in a state of transitions in terms of delivery models, moving from on-premise to cloud, and with regard to core functionality, shifting from commoditized antispam/antimalware capabilities to more high-value capabilities, such as preventing targeted attacks and data loss. Over the next three to five years, the most successful messaging security vendors will be those that can offer a diverse range of delivery models (cloud, appliance, and virtual appliance), with strong capabilities in both specialized threat analysis and prevention and data loss prevention.

Advice for End Users/Enterprise IT

Enterprises should choose a messaging security technology that integrates well into existing enterprise collaboration platforms, such as email, as well as content sharing and collaboration platforms, such as SharePoint. At the same time, integration with enterprise storage/archiving architectures is also critical, as these are responsible for securing messaging systems from malicious traffic and protecting and storing message data are consolidating.

First and foremost, enterprises should adopt messaging security products from vendors with a strong road map for combating advanced, or specialized, threats. Technology such as network-based sandboxing, real-time file analytics, and forensics and detection of botnet source destinations and command/control traffic are essential in stopping the most pressing threats facing the enterprise. These capabilities are emerging as the new antimalware or antithreat technology of the 21st century. Email inboxes are still the primary beachhead for advanced attackers to gain entry into target machines or network infrastructure.

With so much sensitive data traversing corporate, strong DLP capabilities, either built into messaging security platforms or offered as complementary tie-in solutions, are also essential requirements for messaging security buyers.

Advice for Vendors

Messaging security vendors must have a cloud strategy to compete for the future of this market. On-premise solutions offering only basic antispam or malware protection will be commoditized and are best delivered, for most organizations, as a SaaS-based service. However, this does not make on-premise solutions complete obsolete. Many enterprises will require more on-premise appliances for advanced inspection tasks, especially around DLP or specialized threat prevention. Regulatory requirements, especially for European customers around data privacy and retention laws, will also make relevant on-premise solutions, or at least the option to have this deployment.

It will also be hard for vendors to compete in the future with only messaging security–focused solutions. Specializing in this technology is no longer a differentiator. Customers require deeper integration of messaging security technology with other security solutions, such as endpoint, Web security, STAP, and security information and event management. Additionally, vendors should look to expand — either by product development or through partnerships — technology offerings which complement messaging security and email platforms overall, including message archiving, ediscovery, collaboration protection, and enterprise rights management and encryption technologies.

LEARN MORE

Related Research

- *Worldwide Messaging Security 2013–2017 Forecast and 2012 Vendor Shares* (IDC #242250, October 2013)
- *Worldwide Web Security 2013–2017 Forecast and 2012 Vendor Shares* (IDC #242033, July 2013)
- *IDC MarketScape: Worldwide Web Security Products 2011–2012 Vendor Analysis* (IDC #236980, October 2012)

Synopsis

This IDC study uses the vendor assessment model called IDC MarketScape. This assessment discusses both quantitative and qualitative characteristics that explain a vendor's success in the marketplace and help anticipate its ascendancy.

"While the messaging security market matures and becomes commoditized, it is still critical for enterprises to protect email inboxes from advanced threats and targeted malware, as well as prevent loss of sensitive information sent via email," says Phil Hochmuth, program manager, Security Products research at IDC. "However, this market has matured well beyond the better mousetrap phase of evolution. Enterprises require messaging security technologies that integrate tightly with adjacent and supporting security solutions and that are available via flexible delivery models, such as SaaS and virtualized appliances."

Copyright Notice