Market Share

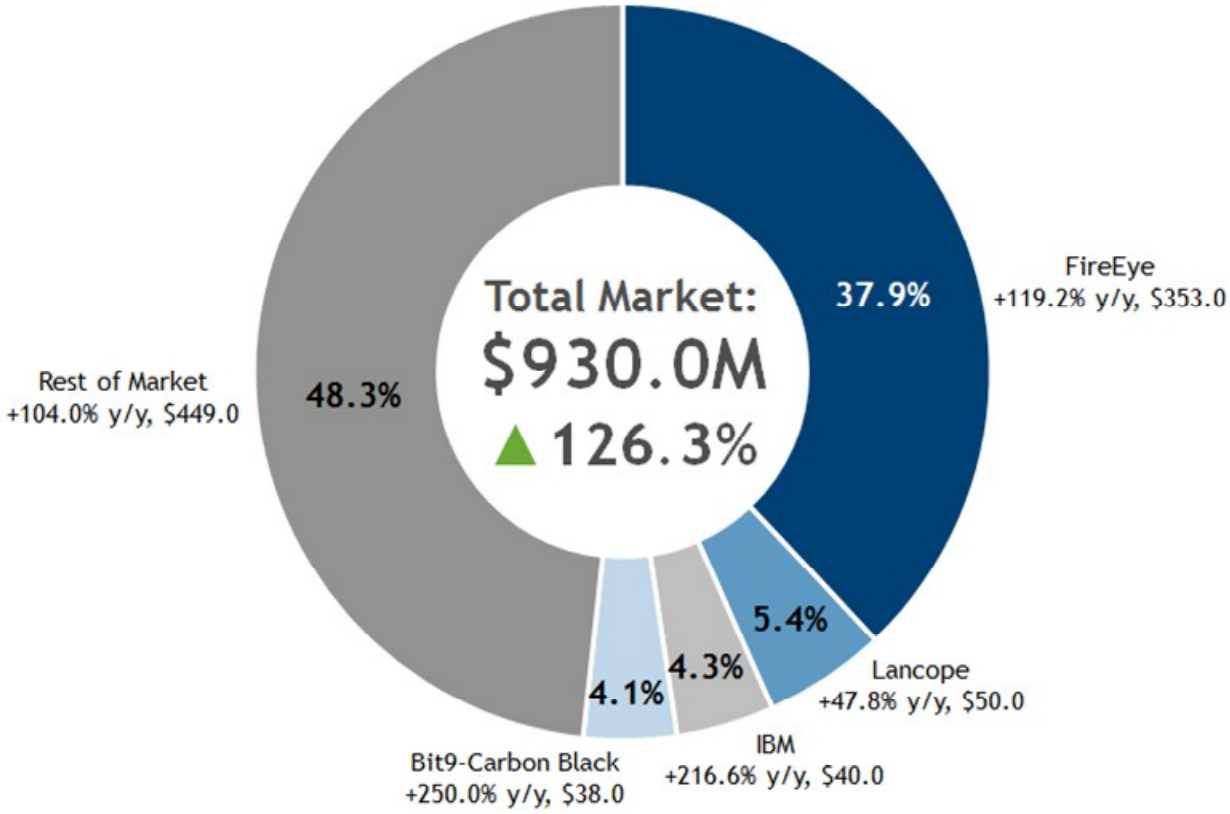
Worldwide Specialized Threat Analysis and Protection Market Shares, 2014: Rapidly Evolving Security Defenses

Robert Westervelt
Rob Ayoub
Pete Lindstrom
Elizabeth Corr

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Specialized Threat Analysis and Protection 2014 Share Snapshot



Note: 2014 Share (%), Growth (%), and Revenue ($M)

Source: IDC, 2015

October 2015, IDC #259667

EXECUTIVE SUMMARY

The specialized threat analysis and protection (STAP) market continued to gain traction in 2014 with widespread adoption of SaaS and on-premises sandboxes and a renewed focus on emerging endpoint security technologies. Organizations are also increasingly evaluating network inspection solutions designed to detect attacker movement to sensitive resources.

Significant STAP trends are:

- **Vendors converting proof of concepts (POCs).** Security vendors converted a significant number of STAP proof of concepts in 2014. IDC estimates that the market in 2014 had revenue of $930 million. It is forecast to grow to over $3 billion by 2019, with a total market CAGR of 27.6%.
- **Identifying attacker movement.** High-profile attacks, data breaches, and critical vulnerabilities in 2013 and 2014 drove interest in NetFlow and other products designed to detect lateral movement within a corporate network. FireEye, Lancope, IBM, and Bit9-Carbon Black were the top 4 security vendors selling STAP solutions in 2014.
- **Calling for incident response (IR) support.** Early adopters of STAP solutions sought incident response expertise, increasing demand for digital forensics specialists, data breach support, and other professional services. Vendors responded by adding or bolstering their services offerings in 2014.

IDC believes that emerging endpoint solutions designed to detect advanced threats will gain momentum. Vendors are combining monitoring with behavioral analytics with other non-signature-based detection capabilities to identify zero days. There is some evidence that end customers are beginning to shed standard antivirus in favor of some endpoint STAP solutions.

The STAP market will continue to evolve with established security vendors adding STAP features to their portfolio organically or acquiring emerging STAP solutions. In 2014, Palo Alto Networks acquired Israeli start-up Cyvera for an estimated $200 million and, later in the year, introduced Traps, a STAP endpoint product that integrates with its WildFire file sandboxing service. Cisco Systems acquired ThreatGRID, adding suspicious file analysis sandboxing capabilities to its portfolio. FireEye further built out its portfolio with the acquisition of nPulse Technologies to support forensics and threat remediation activities.

This IDC study examines the competitive market for this specialized security technology. It aims to identify the market leaders and significant trends that will impact the broader market for security products and services. Security vendor products that fit into the STAP market must be sold as a dedicated product and purchased from customers to specifically address the problem of identifying custom malware.

"The specialized threat analysis and protection market is rapidly evolving, with established vendors adding STAP offerings that compete against a growing cadre of security start-ups. The innovative security technologies in this market modernize many of the outdated approaches that attackers are easily bypassing today. Organizations are showing significant interest and adoption of STAP products to address the growing need for advanced threat detection." – Robert Westervelt, research manager, Security Products, IDC

ADVICE FOR TECHNOLOGY SUPPLIERS

The specialized threat analysis and protection market continues to be challenging for vendors, buyers, and sales channel resellers. The competitive market continues to evolve with STAP security products often overlapping a variety of adjacent security technology areas.

Security vendor products that fit into the STAP market must be sold as a dedicated product and purchased from customers to specifically address the problem of identifying custom malware, sophisticated attack techniques, and other activity associated with advanced persistent threats. The products must not be signature based.

Buyers are seeking to bolster their existing security infrastructure by making an investment in products designed to detect advanced threats from each of the three STAP submarkets: endpoint, boundary, and internal network analysis. Some vendor solutions provide functionality from each of the submarkets, integrating emulation products designed to analyze suspicious files with behavioral analysis to identify function calls and suspicious file activity on the endpoint, and network analysis to detect attacker reconnaissance activity and lateral movement within the network.

Endpoint STAP products use behavioral analysis of memory and application operations. It primarily consists of an agent or sensor on devices that monitor system processes and files for signs of anomalous behavior or attempt to prevent suspicious files from executing. IDC anticipates future consolidation of the endpoint STAP submarket, with traditional endpoint security vendors adding STAP endpoint capabilities to their platforms.

Boundary STAP products consist mainly of virtual sandboxing/emulation and behavioral analysis technologies. These safe zones are used to detonate and monitor the behavior of suspicious files, which are designed to evade signature-based defenses. Buyers have increasingly purchased SaaS-based sandboxing services, but on-premises and hybrid deployments are also common with enterprise customers.

Internal network analysis STAP products monitor network flow to detect indications of attacker reconnaissance activity, malware movement, and botnet or malware command and control activity. Products should be equipped to help responders pinpoint endpoint infections and interrupt command and control communication provide context to incident responders.

The strongest STAP solutions appear to come from vendors that have created strong technology partnerships, and IDC has determined that a security vendor's technology partner ecosystem is being examined thoroughly in product evaluations. To remain competitive, security vendors should also consider the following recommendations:

- **Strike key differentiators:** Product evaluations are becoming a significant challenge for buyers planning to adopt STAP technology. Channel resellers are also strained when attempting to determine if a STAP product can fit in their portfolio without conflicting with top-tier technology partners. Make clear all differentiating management features and capabilities against competitive solutions.
- **Expand deployment options:** A key buying requirement is the ability to integrate products with existing security infrastructure. This requirement may result in the need for full SaaS, on-premises, or a mixture of SaaS and on-premises solutions. While usability and effortless deployment are advantageous, buyers are also choosing STAP solutions with flexible deployment models.

- **Create services offerings:** An analysis of early adopter buying behaviors found that vendor services offerings are not a primary buying requirement; however, a second inquiry with customers identified a significant need for follow-up services engagements. The services requirement was prompted by a lack of routine maintenance, deficient incident response processes, and poorly configured deployments.
- **Develop risk scoring models:** Buying trends suggest the addition of a configurable risk scoring methodology to assist responders in prioritizing alerts captures the attention of C-suite executives during sales engagements. Despite the growing number of risk-based scoring capabilities incorporated into security products, STAP vendors can use risk scoring as a product differentiator. It could also foster the comfort level required to prompt organizations to embrace automated response and remediation features.

MARKET SHARE

The worldwide STAP security market rose to $930 million in 2014, an increase of 126.3% from 2013. FireEye remains the STAP market leader, with 37.9% share of the market in 2014. It saw its share of the market decline 5.2% based on additional market entrants and widespread availability of competing sandboxing solutions. A notable competitor is Palo Alto Networks and the rapid adoption of its subscription-based WildFire sandboxing service in 2014.

Table 1 displays 2011–2019 worldwide revenue and market share for the STAP security market.

Tables 2–4 display 2014 revenue and market shares for the top vendors in each submarket.

STAP boundary is the largest market segment, with FireEye continuing to be the sole dominating vendor. Sandboxing technologies have quickly come to market from network security competitors and security start-ups. Boundary STAP includes products from Check Point, Cyphort, iBoss, Fortinet, Intel Security, Proofpoint, Symantec, and others. It also includes a share of sandboxing components that exist within standalone vendor advanced threat defense solutions (see Table 3).

STAP endpoint is the fastest-growing market segment and one that is quickly evolving as endpoint security vendors, including Symantec and Intel Security, add endpoint advanced threat detection capabilities to their platforms to meet their established customer requirements.

Lancope has gained significant adoption of its advanced threat detection solution, leveraging its close relationship with Cisco Systems. RSA and Blue Coat are each transforming their network packet capturing appliances, which had been focused for digital forensics investigations, into breach detection and analysis platforms (see Table 4).

TABLE 1

Worldwide Specialized Threat Analysis and Protection Revenue by Segment, 2011–2019 ($M)

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2014–2019 CAGR (%)
Boundary	80.6	150.5	309.0	709.8	1,119.7	1,444.3	1,653.4	1,845.3	2,001.6	23.0
Endpoint	9.0	16.0	39.0	101.8	212.7	353.2	494.4	618.0	716.9	47.8
Internal network analysis	21.0	35.0	63.0	118.4	202.5	287.6	342.2	386.7	421.5	28.9
Total	110.6	201.5	411.0	930.0	1,535.0	2,085.0	2,490.0	2,850.0	3,140.0	27.6

Source: IDC, 2015

TABLE 2

Worldwide Specialized Threat Analysis and Protection Revenue of Boundary Segment by Vendor, 2014

	Revenue ($M)
FireEye	353
AhnLab	25
Trend Micro	25
Cisco	25
Fidelis	23
Websense	23
IBM	20
Lastline	20
Palo Alto Networks	17
Other	178.8

Source: IDC, 2015

TABLE 3

Worldwide Specialized Threat Analysis and Protection Revenue of Endpoint Segment by Vendor, 2014

	Revenue ($M)
Bit9-CB	38.0
Cylance	13.0
Bromium	13.0
CrowdStrike	12.0
Invincea	12.0
Other	13.8

Source: IDC, 2015

TABLE 4

Worldwide Specialized Threat Analysis and Protection Revenue of Internal Network Analysis Segment by Vendor, 2014

	Revenue ($M)
Lancope	50.0
IBM	15.0
Damballa	15.0
Blue Coat	13.0
RSA	13.0
Other	12.4

Source: IDC, 2015

WHO SHAPED THE YEAR

Bit9 acquired Carbon Black at the beginning of 2014 and was able to highlight the effectiveness of its modern whitelisting approach with Carbon Black's endpoint forensics capabilities. Carbon Black had been tremendously successful with its approach prior to the acquisition gaining adoption with SOC personnel and incident response teams for its ability to take a complete inventory of every file on an endpoint system and monitor for system changes. The acquisition shifted attention on ways organizations can modernize their endpoint security solutions.

FireEye gained attention with the launch of its Endpoint Security (HX Series) appliance in 2014. This product uses Mandiant's proprietary technology for incident responders to monitor endpoints for threat indicators and alert the security operations center team about possible compromised endpoints. Engineers are working on embedding Mandiant's MIR functionality into the HX Series, enabling responders to rapidly investigate potential threats. The appliance can be purchased separately or be integrated with the FireEye NX Series appliances.

Palo Alto Networks acquired Morta and Cyvera in 2014 to add endpoint visibility to its portfolio. The resulting endpoint STAP product called Traps is designed to block attacker exploitation techniques. Traps integrates with WildFire, Palo Alto's SaaS-based sandboxing service.

Cisco Systems acquired ThreatGRID, adding a sandbox for cloud-based suspicious file analysis. The company also showed progress in extending the Advanced Malware Protection component of its Sourcefire acquisition as an add-on to its ASA UTM appliances.

Lancope leveraged its existing partnership with Cisco Systems to gain traction in the STAP market with its StealthWatch System for advanced threat detection. Lancope competes against other vendors in the internal network analysis submarket, which is designed to identify lateral movement within tracking network reconnaissance, internal malware propagation, command and control traffic, and data exfiltration.

A Note on Symantec and Intel Security

Intel Security is making gains with its Advanced Threat Defense offering, which consists of a standalone appliance, designed to integrate with other products in its portfolio. Intel Security uses a local blacklist to detect known malware and a virtual sandbox environment for suspicious file analysis. It connects to Intel Security's cloud-based Global Threat Intelligence for further protection.

Symantec announced that it would split into separate security and information management businesses in 2014. The company also announced plans to invest in its portfolio of security products and enter the STAP market with an Advanced Threat Protection product that integrates its existing email, networking, and endpoint solutions with file inspection technology called Symantec Cynic, a cloud-based sandbox environment for file inspection. Symantec also leverages a technology it calls Synapse to correlate event information between the network, endpoints, and email to provide context to alerts for incident responders.

MARKET CONTEXT

The STAP market gained considerable traction in 2014 as end users increased security spending to stem the ever-increasing number of data breaches. The Target breach in particular raised the stakes for security accountability as the CEO was forced to resign in part as a result of the massive data

breach. STAP products are representing the first significant shift in the security stack in some time, and IDC predicts that organizations will continue to deploy these products either through on-premises devices, through endpoint clients, or via the cloud.

The three STAP subsegments that IDC is tracking – boundary, internal network, and endpoint – have strong enterprise interest and adoption. However, these reasons vary based on each segment:

- **Boundary.** The interest in boundary devices has been prompted primarily by the success of FireEye and others to deliver sandboxing and other identification techniques on the network. Many security administrators are very comfortable with adding security devices to the network and as a result these devices fit easily into the day-to-day security operations function.
- **Internal network.** Internal network STAP products are primarily focused on botnet detection and determining if malware has infected the network. Instead of trying to evaluate the traffic flowing through the network boundaries, internal network STAP products rely on user behavior, flow traffic, and DNS traffic to determine whether there is malicious behavior on the network. One key advantage touted by internal network STAP products over boundary products is a reduction in the amount of false positives.
- **Endpoint.** Endpoint STAP products are being heralded as the next generation of endpoint security. As enterprises have become more disillusioned with legacy endpoint security products, the interest in solutions that are faster and more accurate has increased. Endpoint STAP vendors are approaching endpoint security using a wide variety of methods to improve the detection and prevention capabilities of malware on the endpoint. Other endpoint STAP products are more focused on analytics collection and visibility into the endpoint and then coordinate that data with network-based products.

IDC does not believe that any single approach or product will solve an organization's security challenges, but by using a combination of STAP products with traditional security products, that many blind spots can be eliminated.

Significant Market Developments

Security vendor FireEye's continued success has resulted in an influx of advanced threat defense offerings that use virtual sandboxes to analyze suspicious files and identify advanced threats. The solutions, which first appealed to large enterprises, have experienced growth by capturing a broader segment of the market, which quickly embraced cloud-based sandboxing services. A variety of pure-play vendors with sandboxing offerings continue to make the boundary submarket extremely large compared with endpoint and internal network analysis.

Bit9's acquisition of Carbon Black has helped fuel interest in modernizing endpoint defenses, which have been relying heavily on signature-based technology to detect malware. New concepts are being introduced that incorporate endpoint agent or sensor technology to increase visibility and give incident responders more context into alerts and control over infected systems.

Endpoint STAP is rapidly evolving. The attention given to pure-play vendors has prompted established security vendors to add similar specialized threat analysis and protection capabilities. The root of many of these emerging technologies is in host-based intrusion prevention and digital forensics capabilities that identify threats in underlying system memory, abnormal application function calls, and other signs of unusual system behavior.

IDC is aware of AccessData, FireEye MIR, Guidance Software Encase, RSA ECAT, and other forensics tools that help responders gain visibility while investigating the scope of an infection. IDC

analysts examine these products closely to determine whether there is real-time monitoring and alerting capabilities and the customer requirements and use cases that the products fulfill.

METHODOLOGY

This IDC software market sizing and forecast is presented in terms of packaged software and appliance revenue. IDC uses the term *packaged software* to distinguish commercially available software from custom software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of these are counted by IDC as packaged software revenue. Appliances are defined as a combination of hardware, operating environment, and application software where they are provided as a single product.

Packaged software revenue excludes service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of the product included in a service that offers software functionality by a different pricing scheme. It is the total product revenue that is further allocated to markets, geographic areas, and operating environments.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2014 as of the end of September 2015.
- **IDC's Software Census interviews.** IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area models on more than 1,000 worldwide vendors.
- **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC's best estimates based on these data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

The data in this study is derived from all these sources and entered into IDC's Software Market Forecaster database, which is then updated on a continuous basis as new information regarding software vendor revenue becomes available.

Note: All numbers in this document may not be exact due to rounding.

MARKET DEFINITION

The specialized threat analysis and protection market overlaps the endpoint, messaging, network, and Web functional markets. The products help protect enterprises from new malware attacks that cannot be detected by traditional signature-based techniques. The STAP products use a variety of non-signature-based protection methods including, but not limited to, sandboxing, behavioral analysis, file integrity monitoring, telemetric heuristics, containerization, netflow analysis, and threat intelligence, which can detect a malware attack or compromise by identifying attacker activity or subtle system process changes. Some of the products only detect and alert, while others may contain malware to prevent it from causing damage. Although these features may appear in other products, this category is only for dedicated STAP solutions.

The STAP market is made up of distinguishable products as opposed to embedded features within a product. The ability to find and prevent advanced malware ultimately requires dedicated activities, and in this way, it is possible to measure the extent that enterprises are consciously taking actions to deal with advanced malware.

The STAP market is a competitive market that overlaps other logical security products markets (e.g., IAM, network, endpoint, messaging, Web, SVM, and "other" security products). The STAP market must be reported separately and, furthermore, not added to the seven logical security products markets, otherwise the total security products market figure will be incorrect.

RELATED RESEARCH

- *IDC's Forecast Scenario Assumptions for the ICT Markets and Historical Market Values and Exchange Rates, Version 3, 2015* (IDC #259115, September 2015)
- *Worldwide Specialized Threat Analysis and Protection Forecast, 2015–2019: Defending Against the Unknown* (IDC #256354, May 2015)
- *Market Analysis Perspective: Worldwide Security Products, 2014* (IDC #252908, December 2014)
- *Worldwide IT Security Products 2014–2018 Forecast and 2013 Vendor Shares: Comprehensive Security Product Review* (IDC #253371, December 2014)
- *IDC's Worldwide Security Products Taxonomy, 2014* (IDC #250802, September 2014)
- *Worldwide Specialized Threat Analysis and Protection 2013–2017 Forecast and 2012 Vendor Shares* (IDC #242346, August 2013)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com