The Forrester Wave™: Automated Malware Analysis, Q2 2016

Tools And Technology: The Security Architecture And Operations Playbook

by Jeff Pollard and Kelley Mak

April 21, 2016

Why Read This Report

In our 36-criteria evaluation of automated malware analysis providers, we identified the 11 most significant ones — Blue Coat, Check Point, Cisco, Cyphort, Fidelis Cybersecurity, FireEye, Fortinet, Intel Security, Palo Alto Networks, Lastline, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Portfolio Vendors Lead While Two Startups See Traction

Forrester's research uncovered a market in which Palo Alto Networks, Check Point, Blue Coat, Cyphort, Trend Micro, Lastline, FireEye, and Intel Security lead the pack. Fidelis Cybersecurity and Cisco offer competitive options. Fortinet lags behind.

S&R Pros Are Looking For Usability And Integrations

The automated malware analysis market is growing because more security professionals see malware analysis as a way to address their top challenges. This market growth is in large part due to the fact that security and risk pros increasingly trust automated malware analysis providers to act as their highest fidelity alert, trusting them beyond other security technology.

Flexibility And Delivery Models Are Key Differentiators

As signature-based technologies become outdated and less effective, improved flexibility will dictate which providers will lead the pack. Vendors that can provide SaaS, on-premises, and hosted solutions position themselves to successfully deliver scalable and adaptable solutions to their customers.

The Forrester Wave™: Automated Malware Analysis, Q2 2016

Tools And Technology: The Security Architecture And Operations Playbook

by Jeff Pollard and Kelley Mak
with Stephanie Balaouras, Josh Blackborow, and Peggy Dostie

April 21, 2016

Table Of Contents

Notes & Resources

Forrester conducted lab-based product evaluations in November 2015 and interviewed 11 vendor and 33 user companies, including: Blue Coat, Check Point, Cisco, Cyphort, Fidelis Cybersecurity, FireEye, Fortinet, Intel Security, Lastline, Palo Alto Networks, and Trend Micro.

Related Research Documents

Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Advanced Capabilities

The Forrester Wave™: SaaS Web Content Security, Q2 2015

TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2016 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

Automated Malware Analysis Is A Necessity In Your Security Stack

Despite significant investments in the signature-based defenses of today's network, email, and endpoint security solutions, since 2010, these solutions have been ineffective and inefficient against the sheer volume of evolving and evasive malware. S&R pros desperate to find a way to identify and analyze the growing number of unknown security threats at scale have turned to a new class of security technology: automated malware analysis (AMA). These tools have transformed the specific skill sets of manual practitioners into an automated technology solution that uses static and dynamic analysis methods to detect existing malware while also discovering brand new exploit tools. In 2016, these technologies have shifted from possible to necessary investments in a security stack designed to prevent the known and detect the unknown.[1] Those investments see reward through:

- **Generation of the most important alerts in the environment of any technology.** Forrester clients noted that AMA technology generated the most important alerts of any technology in their environment.[2] By focusing on actual execution of malware samples and watching behaviors, AMA solutions provide higher fidelity alerts and earlier in the attack life cycle. This means security teams can save time by prioritizing the results of AMA alerts over other technologies.
- **Organic threat intelligence created by real attacks on the organization.** Since these technologies extract and analyze objects that traverse the network, email, and endpoint for behaviors, an organization now has a source for specific threat intelligence derived from its actual traffic. This intelligence includes nonunique attacks targeting large numbers of potential victims down to specific and unique attacks against their organization. AMA technologies offer the definitive set of organic threat intelligence that an organization requires.
- **Incidents driven by concrete analysis results, not wild hunts based on anomalies.** Deconstruction of objects inside malware analysis sandbox environments can provide S&R pros concrete clues and information about threats and what to look for next. For example, capturing command and control addresses can allow packet capture sessions, or finding a mutex leads to an endpoint indicator enabling a sweep of the enterprise for infected endpoints. Details from automated malware analysis solutions provide specific feedback criteria for further exploration or enforcement.

Technical Complexity Clouds The Differentiation Of AMA Technologies

Due to varying approaches within the dynamic malware analysis space, S&R pros considering investment, or reinvestment, will find obtuse messaging and ambiguous explanations about how technologies work and why one approach is better than others. Get ready to dust off old knowledge, or develop some new areas of expertise like:

- **Visibility differs when using virtualization versus emulation.** Each approach has technical merits and limitations. Teams should consider the widest net possible as key criteria. A solution that relies only on virtualization can analyze objects quickly but could lose visibility if malware attempts to

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

interact directly with hardware. Emulating systems provide maximum visibility but can slow down when analyzing malware that leverages interpreted languages like Python, and pays a performance penalty overall.

- **What it blocks is just as important as whether it blocks.** If a sample is truly brand new, using techniques never seen before, no technology will block it. This fundamental fact manages to get left out of vendor messaging. AMA technologies can and do block malware based on signature or reputation, but the shiny debut of a sophisticated attack will always require time to analyze and get delivered to end users. It's important to remember and communicate that silver bullets don't exist; remember to plan for failure.
- **Visibility of a seemingly infinite attack surface challenges defenders.** More coverage of an attack surface equals higher detection possibility. If a technology can't analyze certain file types, it can't find unknown malware there. If corporate assets are a heterogeneous mix of Windows, Apple, and Android, then the solution picked must have the ability to analyze all those types or it isn't a fit. Avoiding self-created gaps in coverage takes priority over deep analysis of heaps, stacks, sprays, ROPs, and NOPs.
- **Detection efficacy doesn't dictate superiority of technology.** Letting efficacy dictate purchase begins the process with a flawed premise ending with dissatisfaction. Detection efficacy from appliances can vary. Ransomware authors will vary the file types they deliver to exploit flaws and evade detection. Seeing more is better, and better detection of those types is great, but usability, integrations, and flexibility should rank equal or higher. Enhancing detection capability is far easier for a vendor compared with redesigning a user interface since one impacts customers indirectly and the other directly.

Automated Malware Analysis Evaluation Overview

To assess the state of the automated malware analysis market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top automated malware analysis vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 36 criteria, which we grouped into three high-level buckets:

- **Current offering.** We evaluated the technologies based on their ability to analyze and execute malware, manual malware analysis capabilities, solution deployment model and architecture, threat intelligence and technology integrations, and reporting and administration functionality. We also interviewed vendor customer references to get feedback on their satisfaction with the technology and the vendor.
- **Strategy.** We evaluated vendors on product strategy and corporate strategy to understand technology direction and corporate focus.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Market presence.** We evaluated vendors on their current customer base, revenue, revenue growth, vendor size, and technology partners.

Evaluated Vendors And Inclusion Criteria

Forrester included 11 vendors in the assessment: Blue Coat, Check Point, Cisco, Cyphort, Fidelis Cybersecurity, FireEye, Fortinet, Intel Security, Lastline, Palo Alto, and Trend Micro. Each of these vendors is able to (see Figure 1):

› **Utilize network-based dynamic analysis methods to automatically detect malware.** Technologies needed to have a product that was network-based and performed dynamic analysis that extended beyond signatures and reputation lists providing scores, indicators, and behavioral information for security operations teams.

› **Inspect network traffic (HTTP).** Since most malware requires network traffic for delivery or instructions, technologies needed to inspect traffic and objects sent via HTTP.

› **Inspect email traffic (SMTP).** With spearphishing emails commonly seen as a primary method of infection for the most sophisticated attacks, the ability to inspect objects extracted from SMTP is critical. This offers visibility without direct integration with email servers, providing a straightforward deployment.

› **Generate mindshare with Forrester's clients.** The vendor must have a significant market share or come up frequently in client conversations and inquiries.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Evaluated Vendors: Vendor Information And Selection Criteria

Vendor name	Evaluated in
Blue Coat	Q4 2015
Check Point	Q4 2015
Cisco	Q4 2015
Cyphort	Q4 2015
Fidelis Cybersecurity	Q4 2015
FireEye	Q4 2015
Fortinet	Q4 2015
Intel Security	Q4 2015
Lastline	Q4 2015
Palo Alto Networks	Q4 2015
Trend Micro	Q4 2015

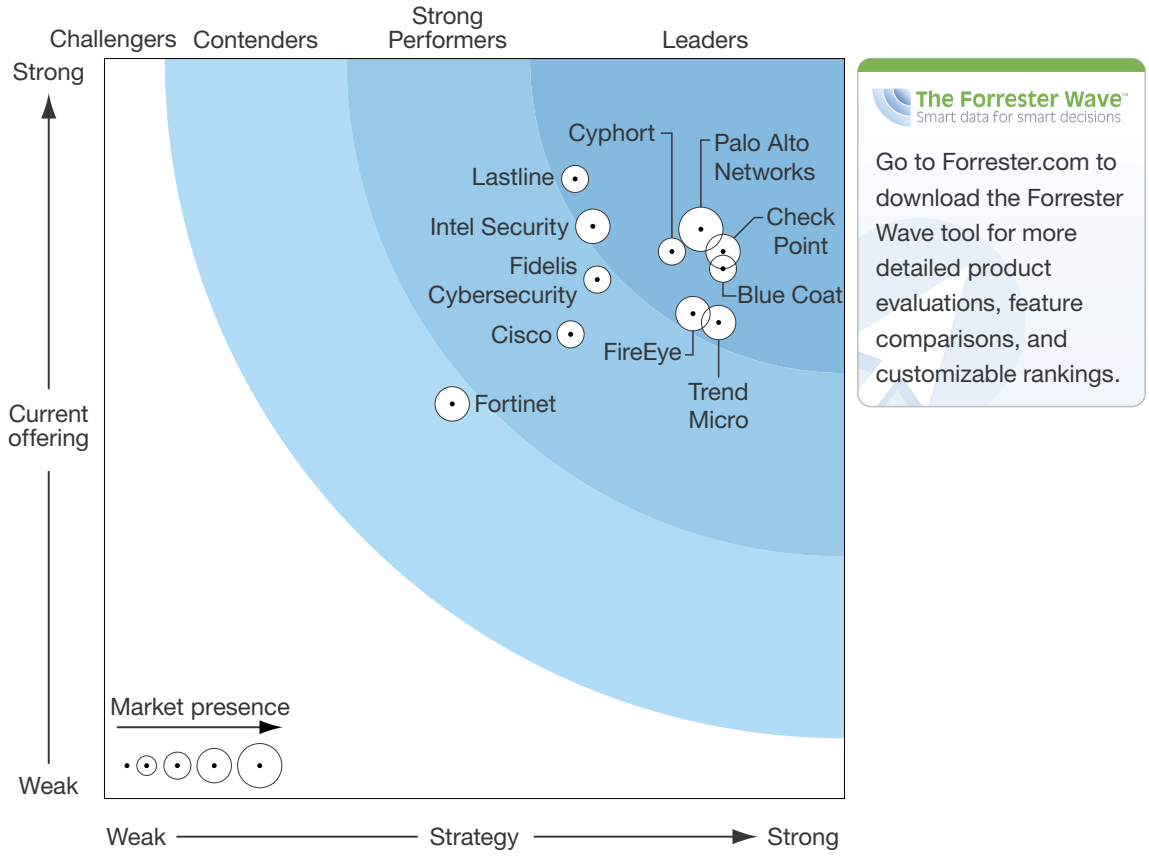
Vendor selection criteria
The vendor's solution utilizes network-based dynamic analysis methods to automatically detect malware.
The vendor's solution inspects network traffic (HTTP).
The vendor's solution inspects email traffic (SMTP).
The vendor generates mindshare with Forrester clients.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Vendor Profiles

This evaluation of the automated malware analysis 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 (see Figure 2).

FIGURE 2 Forrester Wave™: Automated Malware Analysis, Q2 '16



© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Automated Malware Analysis, Q2 '16 (Cont.)

	Forrester's Weighting	Blue Coat	Check Point	Cisco	Cyphort	Fidelis Cybersecurity	FireEye	Fortinet	Intel Security	Lastline	Palo Alto Networks	Trend Micro
CURRENT OFFERING	50%	3.59	3.70	3.14	3.70	3.51	3.28	2.67	3.87	4.19	3.85	3.22
Analysis techniques	25%	4.21	3.77	2.61	3.65	2.58	4.50	2.65	4.55	4.41	3.32	3.59
Manual malware analysis	3%	3.00	3.00	5.00	3.00	1.00	3.00	3.00	5.00	3.00	3.00	3.00
Deployment model	10%	1.00	3.00	5.00	3.00	3.00	1.00	3.00	1.00	5.00	3.00	1.00
Architecture	10%	5.00	5.00	5.00	5.00	3.00	1.00	3.00	5.00	5.00	5.00	5.00
Encrypted traffic inspection	2%	5.00	5.00	5.00	0.00	5.00	0.00	5.00	5.00	0.00	5.00	5.00
Threat intelligence	10%	3.00	2.00	2.00	3.00	5.00	5.00	1.00	5.00	5.00	5.00	2.00
Intelligence network	5%	2.00	5.00	3.00	3.00	3.00	5.00	2.00	2.00	3.00	3.00	3.00
Integrations	10%	5.00	3.67	4.33	5.00	4.33	3.67	1.67	4.33	5.00	4.33	2.33
Reporting	10%	3.00	3.00	1.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Administration	5%	3.00	5.00	1.00	5.00	5.00	3.00	5.00	5.00	5.00	5.00	5.00
Customer references	10%	4.00	4.00	3.00	4.00	5.00	3.00	3.00	3.00	3.00	4.00	4.00
STRATEGY	50%	4.18	4.18	3.15	3.83	3.33	3.98	2.35	3.30	3.18	4.03	4.15
Product strategy	70%	4.25	4.25	3.00	3.75	3.25	3.75	2.50	3.00	3.25	4.25	4.00
Corporate strategy	30%	4.00	4.00	3.50	4.00	3.50	4.50	2.00	4.00	3.00	3.50	4.50
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%	2.87	3.53	2.77	2.23	2.45	4.00	3.15	3.77	2.37	4.30	3.83
Installed base	20%	3.33	3.67	3.33	2.67	3.00	5.00	5.00	3.33	2.33	5.00	4.67
Product revenue	20%	3.00	4.00	2.00	1.00	3.00	5.00	3.00	4.00	1.00	5.00	4.00
Revenue growth	20%	3.00	4.00	2.00	5.00	3.00	3.00	3.00	5.00	5.00	5.00	4.00
Employees	20%	2.50	3.50	4.00	1.50	2.00	4.50	3.50	4.00	2.00	4.00	4.50
Technology partners	10%	5.00	5.00	5.00	2.00	2.50	5.00	2.50	5.00	3.00	5.00	4.00

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

Leaders

› **Palo Alto Networks pushes automated malware analysis into the NGFW feature stack.** First released in 2012, WildFire offers existing Palo Alto Networks customers dynamic malware analysis as a bundled add-on to the next-generation firewall (NGFW) stack, making deployment simple. Use of cloud-based analysis eases integration and minimizes additional hardware requirements. Enterprises with privacy or data residency concerns should consider whether the cloud delivery model makes sense. Palo Alto Networks provides on-premises analysis as an option, but this

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

removes the simplicity of deployment and sizing. WildFire has a wide array of supported file types, including Android APKs for dynamic analysis, and supports many threat intelligence import and export formats.

Palo Alto Network's strategy going forward is comprehensive, covering prevention as well as detection and response, and its development of AutoFocus to leverage threat intelligence looks promising. Some limitations exist specific to types of files analyzed and available operating systems. Organizations with existing Palo Alto Networks appliances deployed should consider adding WildFire to licensing, and organizations with less sophisticated security teams will find working with the technology straightforward.

- **Check Point's AMA offering analyzes malware and innovates with interception.** Customers can add cloud-based analysis capability or on-premises analysis depending on preference. Check Point's overall philosophy and strategy is targeted toward prevention, and underlying this approach is a strong technical offering with intriguing features. Check Point has deep dynamic analysis capability acquired through its purchase of Hyperwise in February 2015. Perhaps the most impressive element of Check Point's malware analysis approach is the ability to capture an email attachment, analyze it, and render the content for the end user or security team while the malware is mitigated.

  Check Point is the only vendor in the Forrester Wave with this unique email capability, setting it apart from competitors. However, Check Point lacks coverage for Mac OS X, and Android analysis requires a separate purchase of Check Point's Mobile Threat Prevention product. The user interface is not as informative for understanding malware behavior and its risk, compared with competitors.

- **Blue Coat integrates malware analysis into a strong investigation-focused suite.** Blue Coat continues its reinvention after private equity acquisition by building a security suite that focuses on the elements of instrumentation important to security teams investigating threats. The sandboxing component of this includes robust malware analysis capabilities and flexibility via scripting that allows security practitioners to extend sandbox capabilities with other tools. By leveraging delivery mechanisms from proxies, packet capture, and external integrations, Blue Coat can receive objects in multiple ways native to its portfolio and via third-party API-based integrations.

  Existing clients of Blue Coat will find adding automated malware analysis capability requires hardware sizing, purchase, and licensing adjustments, but an easy deployment and integration. Analysis results aren't as easy to interpret as those of competitors, and Blue Coat requires multiple appliances to get the full value out of the solution. Security teams looking to extend their current Blue Coat investment and who are looking to add sandboxing, customize analysis capabilities, and focus on life-cycle investigations will find the technology valuable.

- **Cyphort approaches analysis differently in both messaging and technology.** The second of the Forrester Wave's nonportfolio leaders, Cyphort has built an analytic offering focused on behaviors and machine learning rather than pure malware analysis. Strong object analysis across

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Windows, Apple, and Android operating systems and object types provides a comprehensive solution. Integrations with other security technologies provide capabilities for object analysis across numerous delivery mechanisms. The technology's clear explanations of malware behavior make it easy to use for both experienced personnel and newer personnel unfamiliar with malware analysis.

Cyphort's approach attempts to differentiate it from traditional sandboxes, but digging into specifics behind its behavioral-based detection and machine learning in comparison to competitors can be difficult for customers. The impact that approach has on detection efficacy and malware analysis results can vary across clients and deployments and is something that potential customers should evaluate during the purchase process with a programmatic proof of concept. A strong go-to-market strategy relying on partners with dedicated account teams makes purchasing simple, with Cyphort fitting well with clients that want standalone innovative vendors and deployment flexibility.

- **Trend Micro goes deep with dynamic analysis offerings.** Deep Discovery's sandbox element extends Trend Micro's antivirus heuristics and static analysis feature set into a comprehensive approach to security visibility. The solution requires physical or virtualized hardware for analysis with no hosted cloud model provided by Trend Micro. Trend Micro's dynamic analysis covers the basics of Windows-specific analysis, supported file types, and employs many anti-evasion techniques. Trend Micro also provides the ability for customers to load their custom images as analysis environments. Application, OS, and some hardware-level analysis grant solid visibility into samples and their behavior.

  Portfolio integration within Trend Micro is straightforward, and Trend Micro's continued investment in threat investigation across products is appealing. Trend Micro's acquisition of TippingPoint gives it more skin in the network security game, but its long-term effect on the automated malware analysis solution remains unclear. However, a limited web services API isn't impressive compared with those of competitors, and the solution lacks integrations with third parties. Customers with basic requirements looking for network visibility and ease of use should consider Trend Micro.

- **Lastline builds its research pedigree into it dynamic analysis, and it shows.** Experience years ago building Anubis and Wepawet give the Lastline founders and team an excellent background in understanding how to detect malware. It is one of only two leaders that offer a standalone solution instead of a portfolio-based add-on. Focusing on instrumenting hardware and software gives Lastline the ability to detect evasive malware and exploits in both software and hardware. A clean user interface, clear behavior scoring, and explanations make the technology easy to use. Lastline offers a cloud-based or on-premises solution, giving flexibility in deployment, and a robust API makes integrations a priority.

  Where Lastline excels in its current offering for detection and visibility, the go-to-market strategy and OEM partnerships muddle client experiences in working with them. Multiple OEM partnerships mean clients have little reason to go direct and creates confusion for prospects. Client feedback

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

mentioned concerns with high employee turnover and support responsiveness. Those looking for an easy user interface and a nonportfolio offering, and who are willing to sort through OEM versus direct challenges, will find Lastline a solid technology with potential strategic setbacks.

› **FireEye's origin and development of the malware analysis space is clear.** The original and most successful commercial sandbox enters the Forrester Wave in an interesting space as its offering grows with managed and professional services, endpoint, and more. With unique detection capabilities especially at the network and object level, FireEye is one of the only entries to replay the network session inside the dynamic analysis environment. This functionality, combined with strong exploit detection, led FireEye to numerous discoveries of malware over the years, and its value is hard to replicate for competitors, but clear to customers. Lack of a cloud environment for analysis makes FireEye an on-premises and appliance-only offering.

FireEye's success is one of its major weaknesses, as the appliance-only offering makes scaling and sizing difficult. Separate network, email, file, and direct submission appliances create a product set where analysis environment is the same, but the extraction method is not. For clients without concerns about the number and different types of appliances and who prefer to work with an original innovator in a space, FireEye makes sense as a potential partner. Careful consideration should be given to FireEye's evolution as a vendor, with malware detection still an important, but not only, aspect of its strategy.

› **Intel Security brings strong CPU-based detection and analysis.** Perhaps not surprisingly, Intel excels at CPU-based detections and assembly-level detection capabilities with advanced threat defense (ATD). Intel's solution instruments below the operating system API that leads to substantial visibility into evasive malware. Intel also offers a user interactive mode that allows an analyst to work directly with the sample while it's in the dynamic analysis environment. Integrations with the broader Intel platform offer multiple ways to send files for analysis, and its management with ePO makes it easy for enterprises that already use Intel Security products.

However, Intel's divestiture of its NGFW and email gateway will limit the traffic inspection capabilities of the portfolio in the future, which will rely on strategic partnerships. The user interface isn't the simplest, but Intel Security offers differentiated capabilities for an experienced analyst or reverse engineer, which customers with sophisticated teams will find intriguing. Long-term strategic planning around Intel Security and its divestiture and acquisition strategy should take place, as the implications to ATD through the context of the Intel offering in a portfolio purchase could cause issues in the future.

Strong Performers

› **Fidelis Cybersecurity adds value to dynamic analysis with analytics.** Fidelis Cybersecurity features capable dynamic analysis and a product suite focused on investigation across network and endpoints. Multiple integrations within the Fidelis Cybersecurity security portfolio, as well as third parties, give flexibility to customers regarding how they deploy technologies inside the

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

environment. Fidelis Cybersecurity offers physical and virtual appliances for on-premises or cloud-based deployments but doesn't offer hosted analysis capabilities, meaning clients will have to think about sizing and scale when building a solution.

Fidelis Cybersecurity suffers when it comes to dynamic analysis environments, operating systems, and applications. The inability to analyze Mac OS X and Android malware will prove problematic to heterogeneous IT environments with multiple surface areas. Fidelis Cybersecurity does provide sophisticated enhancements to the dynamic analysis capabilities it lacks with solid network analytics and signatures presented well in its user interface. Customers with an appetite for an investigation-oriented platform who value the use of network signature detection should consider Fidelis Cybersecurity due to the user interface and sophisticated signature set.

› **Cisco integrates ThreatGrid into the Advanced Malware Protection offering.** With a cloud and on-premises offering, Cisco proves itself once again capable of integrating acquisitions quickly by combining dynamic analysis capabilities of ThreatGrid with the legacy Sourcefire FireAMP line of network and endpoint tools. API-based external integrations plus a comprehensive internal portfolio allow multiple mechanisms to send objects to ThreatGrid. The ability to interact with objects as they execute is a strength of the Cisco offering, something advanced users will appreciate compared with fully automated solutions. A good user interface with a robust API gives flexibility in reporting, administration, and customization. Artifacts of analysis are also available by API query.

Unfortunately, the primary drawback of ThreatGrid comes in its limited support for Windows environments, with only Windows XP and Windows 7 supported. The inability to dynamically analyze Mac OS X and Android and a limited set of applications available in each dynamic environment make the offering quite specific regarding coverage. ThreatGrid also has limited instrumentation beyond the operating system at a hardware level. Customers seeking Windows-specific advanced detection capabilities at the software level and a full featured API should evaluate ThreatGrid, as well as Cisco customers exploring the AMP stack in its entirety.

Contenders

› **Fortinet sticks to a strategy of portfolio appliances with diverse feature sets.** The overall Fortinet approach of integrating various features of one-time specific technologies works well for them, and that remains true in the automated malware analysis space. Ability to instrument email, endpoint, and network give multiple options for file analysis, and a straightforward user interface with similar functionality to other Fortinet technologies make interacting with the technology easy for users. Fortinet's dynamic analysis offering is limited in operating systems supported (Windows XP and Windows 7), file types supported, manual analysis, and threat intelligence support.

Heavy reliance on other elements of the Fortinet suite for signature, reputation, and static analysis also make the FortiSandbox offering dependent on other technology, so that it won't be an isolated purchase, but part of an overall Fortinet solution already deployed. Customers familiar

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

with Fortinet technology, fans of its licensing and user interface, and those not focused on deep analysis capabilities or diverse analysis environments will find Fortinet straightforward and useful in a Fortinet-based ecosystem.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

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 four data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by September 21, 2015:

- **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.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Product demos.** We asked vendors to conduct demonstrations of their products' 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 evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and 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.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] Cybersecurity is now part of regular executive discussions and is being allocated budgets accordingly. Chief information security officers (CISOs) and their teams must exhibit business acumen in spending these budgets and demonstrate how they're reaching an appropriate state of cybersecurity readiness. For more, see the "Cybersecurity Budgets Remain Strong, Skills Lag In 2016" Forrester report.

[2] To see more about AMA alerts, see the "Planning For Failure" Forrester report.

© 2016 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

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 Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.