The Forrester Wave™: Endpoint Security Suites, Q4 2016

The 15 Providers That Matter Most And How They Stack Up

by Chris Sherman

October 19, 2016

Why Read This Report

In our 25-criteria evaluation of endpoint security suite providers, we identified the 15 most significant ones — Bromium, Carbon Black, CrowdStrike, Cylance, ESET, IBM, Intel Security, Invincea, Kaspersky Lab, Landesk, Palo Alto Networks, SentinelOne, Sophos, Symantec, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up and helps S&R professionals make the right choice.

Key Takeaways

Trend Micro, Sophos, And Symantec Lead The Pack

Forrester's research uncovered a market in which Trend Micro, Sophos, Symantec, Kaspersky Lab, Intel Security, and Carbon Black are Leaders. Cylance, Landesk, CrowdStrike, ESET, Palo Alto Networks, IBM, SentinelOne, and Invincea offer competitive options. Bromium lags behind.

Security Pros Are Looking For A Balance Of Threat Prevention And Detection

The endpoint security market is growing because more security professionals see the endpoint security suite vendors as a way to address their top challenges. What's more, security pros increasingly trust providers in this space to act as strategic partners, advising them on top endpoint security decisions.

Threat Analysis And Automatic Containment Capabilities Are Key Differentiators

As traditional approaches to endpoint security become outdated and less effective, improved threat detection accuracy and automatic containment measures will dictate which providers lead the pack.

The Forrester Wave™: Endpoint Security Suites, Q4 2016

The 15 Providers That Matter Most And How They Stack Up

by Chris Sherman
with Christopher McClean, Salvatore Schiano, and Peggy Dostie

October 19, 2016

Table Of Contents

Notes & Resources

In this evaluation, Forrester only considered products that were generally available as of July 15, 2016. We interviewed 15 vendors and over 45 of their user companies. The vendors were Bromium, Carbon Black, CrowdStrike, Cylance, ESET, IBM, Intel Security, Invincea, Kaspersky Lab, Landesk, Palo Alto Networks, SentinelOne, Sophos, Symantec, and Trend Micro.

Related Research Documents

The 2016 State Of Endpoint Security Adoption

Brief: Endpoint Security Innovation Is Intensifying

TechRadar™: Mobile Security, Q1 2016

FORRESTER®

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

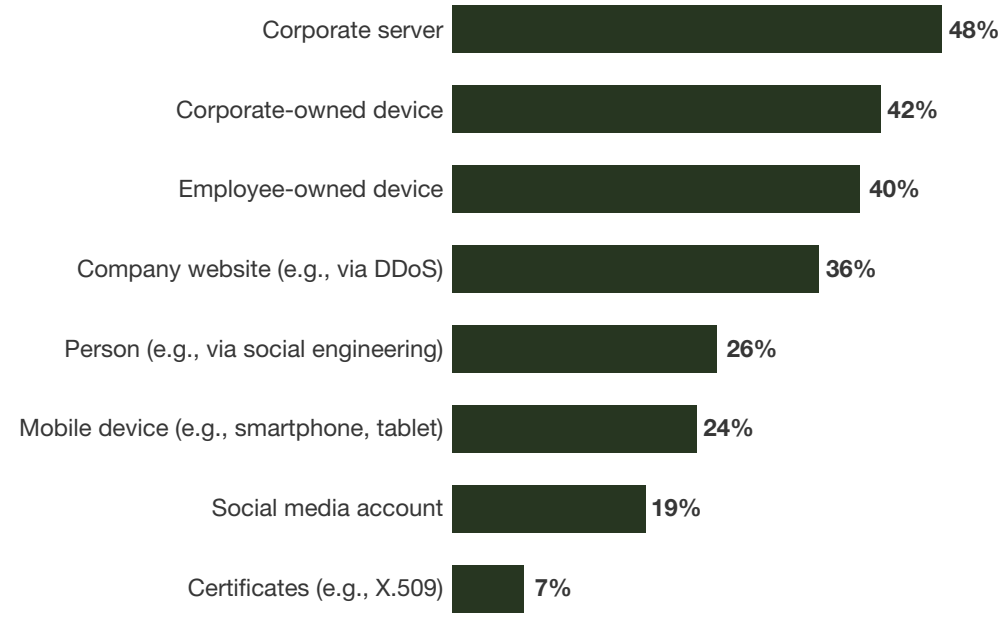
Choose The Right Endpoint Security Solution, Or Risk Compromise

Endpoint security represents the frontline in your fight against cyberattackers. Breaches have become commonplace among enterprises, and your employee endpoints and servers are targeted more than any other type of asset (see Figure 1). The effects from these security breaches can be devastating, causing a company to lose revenue, market reputation, and market competitiveness.[1] Unfortunately, inadequate endpoint security leaves the doors wide open to a variety of attacker techniques and tools, including malware, software exploits, and social engineering. Now, more than ever, it's critical to have the right endpoint protection in place.

Security budgets have risen significantly in the past few years, with endpoint security budgets commanding, on average, 10% of the overall IT security budget in 2016.[2] Despite the available budget for new investments, security pros struggle to find the right tools to protect the expanding attack surface posed by employee devices.

FIGURE 1 Corporate Endpoints Are Your Most Targeted Group Of Assets

"Which of the following was targeted as a part of this external attack?"



Base: 192 network security decision-makers whose firms have had an external security breach in the past 12 months (1,000+ employees)
Source: Forrester's Global Business Technographics® Security Survey, 2016

Endpoint Security Buyers Are Faced With A Highly Fragmented Market

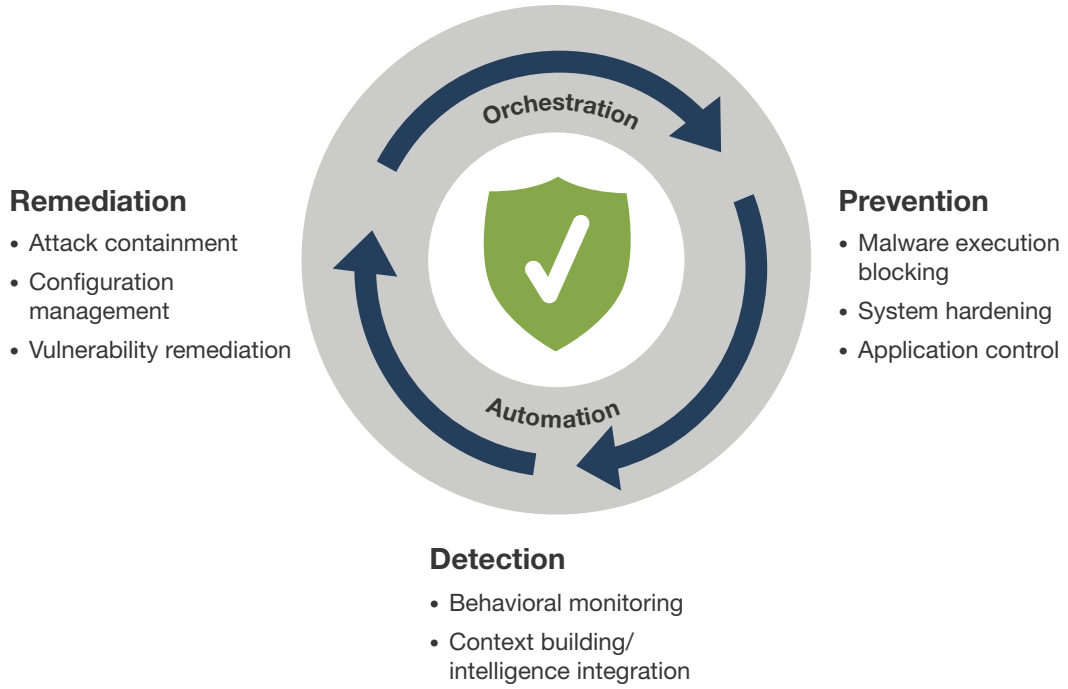
As the numbers of new malware variants and methods of obfuscation rise, antivirus technologies have become less effective at protecting employee endpoints and servers. Numerous competing technology vendors have risen up to take aim at the stagnant antivirus market as a result. On the other hand, many of the traditional antivirus vendors have not taken this lying down. Some have adapted by either building or acquiring new technologies that do not rely on older, blacklist-based malware protection. Others have augmented their antimalware engines with additional analysis capabilities that go beyond static blacklisting. This has led to a highly fragmented market with a number of different approaches to endpoint security, each with its own set of benefits and challenges.

Endpoint Security Suites Must Address Three Core Buyer Needs

To cut through the market confusion, it's useful to categorize vendor capabilities into three core needs: attack prevention, detection, and remediation (see Figure 2). Point products generally meet one need, while endpoint security suites meet two or all three, with varying levels of automatic policy enforcement between each. Before making any new purchases, consider a vendor's ability to meet each of these needs, specifically how well they are able to:

- **Prevent malware and exploits from executing.** Functionally, an endpoint security suite should create an environment where malware can't load into memory or an exploit is unable to take advantage of a running process. It may also prevent threats by reducing the attack surface, with measures such as system hardening and application control.
- **Detect malicious activity post-execution.** Knowing attackers will inevitably get past preventive controls, modern endpoint security suites monitor running memory to identify malware and exploited applications before they achieve their malicious goals. Some solutions focus solely on process behavior, while the most advanced solutions include user behavior in their analysis to build context for a complete picture.
- **Remediate and contain malicious activity and potential vulnerabilities.** Once a modern endpoint security suite identifies malicious endpoint activity or a potential vulnerability, it should be able to launch automated remediation without significant admin involvement. Remediation functions include executable/file quarantining, configuration roll-back, and targeted blocking of process/user behaviors, among others. Vulnerability remediation techniques (such as patch deployment) are included here as well; these often augment prevention measures.

FIGURE 2 The Modern Endpoint Security Suite Balances Threat Prevention, Detection, And Remediation



Endpoint Security Evaluation Overview

To assess the state of the endpoint security suite market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top endpoint security suite 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 25 criteria, which we grouped into three high-level buckets:

- **Current offering.** For each endpoint security solution, we evaluated: 1) prevention capabilities, including malware execution prevention, system hardening, and application control; 2) detection capabilities, including attack detection and threat intelligence; 3) remediation capabilities, including attack remediation and vulnerability remediation; 4) other security capabilities, including ancillary endpoint security functions and mobile security; 5) architecture, including general architecture, OS support, automation and orchestration, and scalability and flexibility; and 6) customer input, including feedback on the product's impact on endpoint user experience, prevention effectiveness, detection effectiveness, and quality of vendor support.
- **Strategy.** We evaluated the vendors': 1) cost and licensing model; 2) product road map; and 3) go-to-market strategy, including channels and partner presence.
- **Market presence.** We evaluated the vendors': 1) enterprise presence and 2) license partner program.

Evaluated Vendors And Inclusion Criteria

Forrester included 15 vendors in the assessment: Bromium, Carbon Black, CrowdStrike, Cylance, ESET, IBM, Intel Security, Invincea, Kaspersky Lab, Landesk, Palo Alto Networks, SentinelOne, Sophos, Symantec, and Trend Micro. Each of these vendors has (see Figure 3):

- **An endpoint security suite that can prevent, detect, and remediate endpoint threats.** We consider solutions that offer only one of these three capabilities to be point products, not suites.
- **An enterprise market presence.** We only included vendors who could meet one of the following: at least 100 enterprise customer accounts or at least 1.5 million business user seats under management.
- **A high level of interest from enterprise buyers.** We only included vendors with high Forrester client interest. Clients should mention the vendor's name in an unaided context ("We looked at the following vendors for endpoint security") on Forrester's inquiries and interactions.

FIGURE 3 Evaluated Vendors: Product Information And Selection Criteria

Vendor	Product evaluated
Bromium	Bromium Endpoint Protection
Carbon Black	Cb Response & Cb Protection
CrowdStrike	Falcon Host
Cylance	CylancePROTECT
ESET	ESET Endpoint Security
IBM	IBM BigFix & MaaS360
Intel Security	McAfee Complete Endpoint Protection Enterprise
Invincea	X by Invincea
Kaspersky Lab	Kaspersky Endpoint Security for Business
Landesk	Landesk Security Suite
Palo Alto Networks	Palo Alto Networks Traps
SentinelOne	SentinelOne Endpoint Protection Platform
Sophos	Sophos Endpoint Protection
Symantec	Symantec Endpoint Protection
Trend Micro	Trend Micro Smart Protection Suite

Inclusion criteria
Vendor must have on or before July 15, 2016:
An endpoint security suite that can prevent, detect, and remediate endpoint threats. We consider solutions that offer only one of these three capabilities to be point products, not suites.
An enterprise market presence. We only included vendors who could meet one of the following: at least 100 enterprise customer accounts or at least 1.5 million business user seats under management.
A high level of interest from enterprise buyers. We only included vendors with high Forrester client interest. Clients should mention the vendor's name in an unaided context ("We looked at the following vendors for Endpoint Security") on Forrester's inquiries and interactions.

Relevant Vendors That Did Not Make The Cut

There are many endpoint security vendors that we did not include in this evaluation, each with capabilities worth considering given the right situation:

- **Microsoft now offers native endpoint security capabilities.** Given the advances in Windows 10 security, many organizations are evaluating it as a viable option for endpoint security as they plan their migration. Because this evaluation process is substantially different than for typical endpoint security suites, Forrester plans to publish a separate study of Microsoft's Windows 10 endpoint security functions in late 2017.
- **Some endpoint security providers target consumers and small business.** This category includes AVG Technologies, Malwarebytes, and many others. Because this evaluation is for the enterprise market, we did not include any of these.
- **Other vendors targeting enterprises didn't make the cut.** Other notable vendors that offer endpoint security products to enterprises include Check Point Software, Cisco Systems, Cybereason, Digital Guardian, and Webroot. These providers did not have at least one of the inclusion criteria for participation.

Vendor Profiles

This evaluation of the endpoint security suite 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 using the Forrester Wave Excel-based vendor comparison tool (see Figure 4).

FIGURE 4 Forrester Wave™: Endpoint Security Suites, Q4 '16

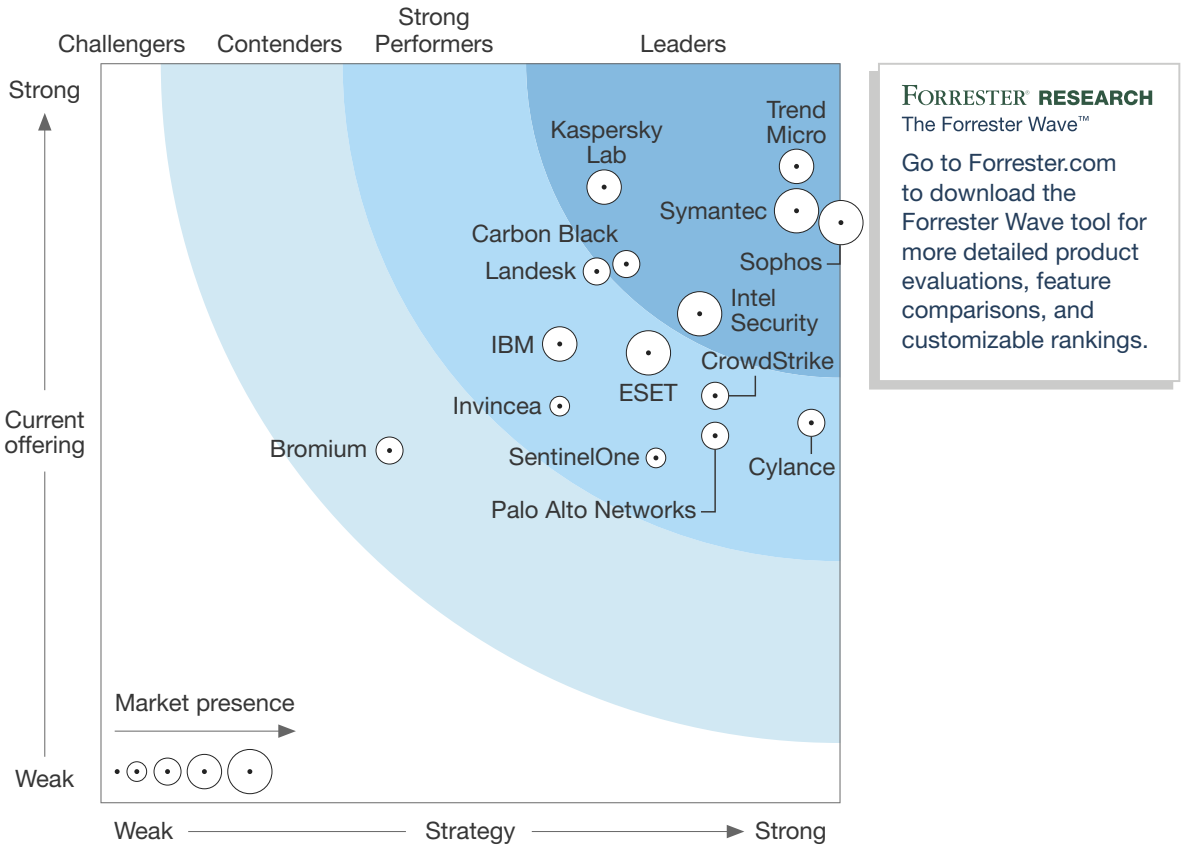


FIGURE 4 Forrester Wave™: Endpoint Security Suites, Q4 '16 (Cont.)

	Forrester's weighting	Bromium	Carbon Black	CrowdStrike	Cylance	ESET	IBM	Intel Security	Invincea	Kaspersky Lab	Landesk	Palo Alto Networks	SentinelOne	Sophos	Symantec	Trend Micro
Current Offering	50%	2.38	3.64	2.75	2.54	3.04	3.10	3.29	2.68	4.16	3.59	2.48	2.33	3.92	4.00	4.30
Prevention capabilities	17%	1.88	4.52	2.04	3.44	2.32	2.00	3.88	3.52	4.12	3.24	2.60	1.36	3.76	3.16	3.76
Detection capabilities	16%	3.60	5.00	5.00	3.20	3.40	3.00	3.60	4.60	4.00	3.00	4.40	4.60	3.40	4.40	5.00
Remediation capabilities	20%	1.50	3.50	2.50	2.00	2.50	4.00	2.50	1.50	4.50	4.50	2.00	2.00	3.50	4.50	4.00
Other security capabilities	20%	1.75	1.50	0.00	0.00	2.75	3.25	3.00	0.00	4.75	4.00	1.00	0.00	5.00	5.00	4.25
Architecture	15%	3.55	4.00	4.05	3.65	3.95	3.10	3.95	3.40	3.60	2.85	2.00	3.55	4.50	3.30	4.70
Customer feedback	12%	2.50	3.90	4.10	4.10	3.80	3.00	3.00	4.50	3.60	3.60	3.60	3.60	3.00	3.00	4.20
Strategy	50%	1.95	3.55	4.15	4.80	3.70	3.10	4.05	3.10	3.40	3.35	4.15	3.75	5.00	4.70	4.70
Cost and licensing model	15%	3.00	1.00	5.00	5.00	5.00	1.00	3.00	5.00	3.00	1.00	5.00	5.00	5.00	3.00	3.00
Product road map	65%	2.00	4.00	4.00	5.00	3.00	3.00	4.00	3.00	3.00	4.00	4.00	4.00	5.00	5.00	5.00
Go-to-market strategy	20%	1.00	4.00	4.00	4.00	5.00	5.00	5.00	2.00	5.00	3.00	4.00	2.00	5.00	5.00	5.00
Market Presence	0%	2.25	2.75	2.25	2.25	4.25	3.50	5.00	1.75	3.75	3.00	2.25	1.50	4.50	5.00	4.00
Enterprise presence	75%	2.00	2.00	2.00	2.00	4.00	3.00	5.00	2.00	4.00	3.00	2.00	1.00	5.00	5.00	5.00
License partners	25%	3.00	5.00	3.00	3.00	5.00	5.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00	5.00	1.00

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

Leaders

› **Trend Micro offers one of the most technically capable products on the market.** Trend Micro offers a complete endpoint security suite with the flexibility to be deployed in a wide variety of enterprise environments either on-premises or through a managed SaaS offering. The company's current offerings balance prevention with detection capabilities very well, despite the lack of patch deployment capabilities and the fact that its detection-focused capabilities are delivered through a separate product (Endpoint Sensor).

Trend Micro's customers gave the product one of the highest scores for threat protection effectiveness of all the suites evaluated in this Forrester Wave, as well as a lower-than-average detriment to endpoint user experience. Overall, Trend Micro's current portfolio, combined with its short- and long-term road maps, aligns very well with the current and (likely) future needs of enterprise buyers.

- **Sophos delivers the most enterprise-friendly SaaS endpoint security suite.** Sophos offers a tightly integrated suite of endpoint security capabilities, with a good balance of advanced threat prevention, detection, and automatic remediation. Buyers will appreciate its intuitive administrative interface along with the flexibility and scalability required for most enterprise deployments, both large and small. Sophos is also one of the few endpoint security suite vendors in this Forrester Wave to offer a full-featured suite either on-premises or through a SaaS-based service. However, the solution's lack of patch management and flexible application default-deny whitelisting options for employee devices may be an issue for some enterprise buyers.

  Overall, customers report a high level of satisfaction with the product's effectiveness, with minimal detriment to endpoint user experience. In a field crowded with both new and legacy endpoint security technologies, Sophos' road map to develop strong signatureless prevention and detection capabilities (including the new Intercept X product, released after the Forrester Wave cutoff date but prior to publication) should make the product highly competitive over the long term.

- **Symantec offers the most complete endpoint security suite on the market.** Symantec's deep bench of endpoint security technologies spans a range of prevention, detection, and remediation capabilities. Almost every possible attack surface is covered when buyers utilize the full extent of this portfolio. However, customers are required to purchase multiple products for all these functions, and integration is lacking between some crucial components. Due to this, buyers report a low level of satisfaction with the admin user experience as well as a moderate detriment to endpoint performance. This may change as the company shifts to a signatureless prevention strategy (scheduled on the product's short-term road map, beginning with the upcoming Symantec Endpoint Protection 14 update), which means it will rely less on previous generations of the product.

  The continued development of advanced post-compromise detection techniques, as well as integrations with recently acquired Blue Coat Systems, should lead to improved levels of effectiveness and a more competitive offering over the next six to 12 months.

- **Kaspersky Lab meets most enterprise requirements in a tightly integrated package.** Kaspersky Lab has one of the most complete endpoint security solutions on the market, with strong prevention, detection, and remediation capabilities. The company developed each of these capabilities in-house, so integration between the different components is strong and meaningful.

  Enterprises that wish to get deep threat investigation capabilities will have to look elsewhere, although the company has planned expansion into this area on its short-term road map with KATA 2.0 (scheduled for release in Q1 2017). Overall, customers report a high level of effectiveness in both malware and exploit prevention, with solid post-execution detection capabilities.

› **Intel Security's scalability makes it especially good for very large enterprises.** Intel Security offers one of the most powerful endpoint management platforms on the market today, McAfee ePolicy Orchestrator (ePO). This product is the underlying management tool for all of the company's security products, and it offers the power and flexibility that enterprise buyers desire. The security capabilities are broad and tightly integrated through a common policy engine and intelligence stream, spanning multiple prevention, detection, and remediation functions. This comes at a cost, with many customers reporting frustration with the complexity of the user interface.

Product effectiveness scores are solid, although buyers should be aware that customers have reported an above average detriment to user experience on older machines. There are also a few significant functionality gaps, most notably a lack of patch management and mobile security capabilities. However, assuming the company executes on their current short- and long-term road maps (such as delivering advanced behavioral-based detection and containment measures), the solution should regain its competitive edge and remain a viable product for many years.

› **Carbon Black continues to move beyond app control with advanced detection.** Carbon Black offers a strong balance of prevention, detection, and remediation functions without relying on signature blacklists. This is mainly due to the company's history as Bit9, which was known for its best-of-breed whitelisting technology with post-attack forensics. While app control continues to be a core offering, the company offers strong detection and response capabilities with its 2014 acquisition of Carbon Black. With its more recent acquisition of Confer in 2016, the company demonstrates its commitment to a more balanced portfolio, with prevention and detection capabilities.

Customers rate the product as having excellent prevention capabilities with very strong detection effectiveness, although this comes with a higher-than-average detriment to user experience. Forrester expects the user experience to improve as the integration between the Confer agent and Carbon Black technologies begins to bear fruit and the product's reliance on the default-deny model decreases.

Strong Performers

› **Cylance offers strong malware prevention capabilities without the use of signatures.** Cylance is another young vendor that has enjoyed a high level of interest and growth over the past couple of years. The company offers one of the few endpoint security point products on the market today that showcases strong malware execution prevention capabilities without the need for an internet connection or frequent blacklist/whitelist updates. The product accomplishes this through an artificial intelligence engine that scans every executable launched on an endpoint in order to predict its behavior.

Overall, the product has earned a high level of satisfaction with customers and has a low negative impact on employee endpoint experience. While the currently available product lacks some of the post-execution detection components seen with competitors, an expansion of its detection

capabilities has been planned for an upcoming release in late 2016. Buyers should also keep in mind that Cylance Protect will likely require additional investments in ancillary endpoint security/ management technologies to complement the offering.

› **Landesk aims to be the next major player in the endpoint security space.** Many security buyers think of Landesk primarily as a systems management company, but over the past several years this has clearly changed. Through both acquisition and in-house development, Landesk now offers a number of strong security technologies that place it among the top endpoint security suites. These include full application control capabilities (through the acquisition of AppSense), best-of-breed patch management (through the Shavlik acquisition), solid mobile security capabilities (through the LetMobile acquisition), and endpoint detection capabilities developed in-house. While integration between these different components is not complete, integration is on the company's short-term road map.

Customers report a high level of satisfaction with Landesk's prevention and detection capabilities, but they report a moderate detriment to endpoint user experience. As integration between the company's different security capabilities continues, the user experience should improve.

› **CrowdStrike is looking to evolve into an endpoint antimalware suite replacement.** CrowdStrike has evolved significantly since its first release in 2012, building out a number of prevention capabilities and automated remediation functions that don't rely on admin involvement or oversight. While the product was initially focused on augmenting existing endpoint security products in the enterprise, it can now be used as a standalone replacement for antimalware tools in certain environments. However, the product's focus is still on attack detection; Falcon Host's cloud architecture and Threat Graph give admins the ability to easily correlate endpoint activity across their enterprise and compare that with what's occurring globally.

Buyers report a high level of satisfaction with CrowdStrike's ability to prevent and especially detect threats to their environment, with a very low detriment to endpoint user experience. While the product is still not a fully featured suite, the company's 2017 road map is focused on building out enterprise features — including modules for encryption, device control, and user behavior analytics (UBA) — that will make it more competitive with leading endpoint security suite vendors.

› **ESET delivers strong antimalware protection in a lightweight package.** ESET has historically focused on the consumer and SMB markets, but over the past few years has introduced more features that give its endpoint security suite the flexibility and breadth typically sought by enterprise buyers. This includes a solid balance of endpoint prevention and automated remediation functions, bolstered by a number of ancillary endpoint security technologies such as endpoint encryption, media control, and mobile security.

ESET's product gets very high marks from users for prevention effectiveness, along with a very low detriment to endpoint user experience. However, the lack of flexible application control and vulnerability remediation capabilities may give certain enterprise buyers pause and will need to be addressed in future iterations of the product if it is to remain competitive.

› **Palo Alto Networks offers strong malware-prevention and exploit-blocking capabilities.** Palo Alto Networks' Traps product offers attack prevention through its cloud-based pre-execution malware analysis engine, WildFire, as well as post-execution exploit blocking through its Traps core engine. Buyers should note, however, that blocking unknown malware requires an internet connection to WildFire's servers; if an immediate verdict from WildFire is not available due to lack of connection, administrators can set a policy to block unknown executables at the potential detriment of endpoint user experience, which may be acceptable only for high-risk or static endpoints.

Users report a higher-than-average detriment to endpoint user experience when running the product in full protection mode (both cloud analysis and behavior blocking). However, the most recent version (Traps v3.4, not evaluated in this Forrester Wave but released prior to publication) addresses this through static analysis on the endpoint. Overall, the product receives high marks for both prevention and detection despite the lack of a dedicated endpoint visibility and control function.

› **IBM is a solid choice for those who already have threat detection in place.** IBM's endpoint security portfolio encompasses endpoint management and vulnerability remediation (through BigFix), signature-based malware prevention (licensed from Trend Micro), and signatureless application integrity protection through its Apex technology. Customers report strong malware prevention effectiveness scores and a reasonably low detriment to user experience.

Enterprise buyers will appreciate the integration between Apex and BigFix; however, the company still relies on integration with Carbon Black for threat detection capabilities. This is a gaping hole in (and an opportunity for) IBM's endpoint security portfolio, given the company's expertise in threat research through the IBM X-Force division as well as its expertise in big data analytics. Overall, current customers of IBM and those who already have Carbon Black (or another endpoint detection technology) will benefit the greatest from IBM's endpoint security portfolio.

› **SentinelOne focuses on stopping compromises once they begin.** SentinelOne has received a high level of attention compared with its modest size and age. This is because its core product uses behavioral detection methods instead of signatures (although basic blacklisting can be enforced pre-execution to stop known threats), leading to a low detriment to the endpoint user experience. However, compared with other solutions in this evaluation that focus on prevention, SentinelOne's pre-execution prevention capabilities and attack surface-reduction technologies are modest; it's really aimed at malicious-activity blocking as malware or exploits begin to load into memory. Therefore, the product received high marks for detection effectiveness and only modest marks for prevention effectiveness.

While many enhancements are planned for the product to allow it to compete head-to-head with full endpoint security suites (most notably on-endpoint signatureless malware execution prevention), buyers should note that SentinelOne will likely require additional investments in ancillary endpoint security/management technologies to complement the technology.

› **Invincea is not just another security point product focused on sandboxing.** Invincea is the only vendor evaluated to offer staged protection measures that include signatureless prevention, application containment, and behavior-based detection. Depending on their level of risk, certain applications can run within user-mode sandboxes that protect against exploits and malware escapes, with the broader endpoint environment covered through a combination of blacklist antimalware and advanced protection measures. However, this comes at the expense of user experience, which can vary greatly depending on the customer's configurations and environment (such as whether application sandboxing is enabled).

While Invincea lacks many ancillary endpoint security technologies that enterprise suite buyers require, the product still gets high marks for product effectiveness. With its strong prevention and detection capabilities, Invincea would be well-suited in enterprises with existing security technologies in place (data security, media control, configuration management) as well as high-risk environments where additional threat prevention is required.

Contenders

› **Bromium focuses on threat prevention, although it's ahead of its time.** Bromium uses hardware-based virtualization techniques to prevent malware and exploits from compromising the endpoint. The technology runs files and executables within virtual machines, with behavior-based controls enforced at logical boundaries in order to limit the impact an exploit can have on the endpoint. Bromium offers a high level of protection without the use of signatures or application whitelists.

Buyers should note, however, that the product can have a negative impact on user experience on endpoints that do not meet RAM or CPU minimum requirements. Overall, Bromium is a solid choice for organizations with supported hardware that don't require a full-featured endpoint security suite.

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

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource

The online version of Figure 4 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Survey Methodology

The Forrester Global Business Technographics® Security Survey, 2016 was fielded in March-May, 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services.

Data Sources Used In This Forrester Wave

Forrester used a combination of three 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 20, 2016.

- **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 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] Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal information of your customers, partners, and employees. Their motivations run the gamut from financial to retaliatory. With enough time and money, they can breach the security defenses of even the largest enterprises. You can't stop every cyberattack. However, your customers do expect you to respond quickly and appropriately. A poorly contained breach and botched response have the potential to cost millions in lost business and opportunity, and ruin your firm's reputation. For more information, see the "Planning For Failure: How To Survive A Breach" Forrester report.

[2] Security technology decision-makers were asked to divide their security budget between 10 security technology areas. Client threat management represented 10% of spend, on average. Source: Forrester's Global Business Technographics Security Survey, 2016.

Every year, Forrester surveys thousands of security decision-makers and information workers globally from a wide range of industries and organization sizes. This report presents the most relevant endpoint security data from these surveys, with special attention given to trends affecting small and medium-size businesses and enterprises. As you review your 2016 security budget, use this report to help benchmark your organization's spending patterns and priorities against those of your peers — while keeping an eye on current trends affecting endpoint security in the context of the overall security landscape. To learn more, see the "The 2016 State Of Endpoint Security Adoption" Forrester report.

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.