The Forrester Wave™: Endpoint Security Suites, Q3 2019

The 15 Providers That Matter Most And How They Stack Up

by Chris Sherman

September 23, 2019

Why Read This Report

In our 25-criterion evaluation of endpoint security suite providers, we identified the 15 most significant ones — Bitdefender, BlackBerry Cylance, Carbon Black, Check Point, Cisco, CrowdStrike, ESET, FireEye, Kaspersky, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

CrowdStrike, Trend Micro, And Symantec Lead The Pack

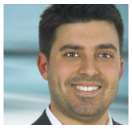
Forrester's research uncovered a market in which CrowdStrike, Trend Micro, Symantec, Microsoft, Sophos, Kaspersky, and Check Point are Leaders; ESET, McAfee, Carbon Black, Bitdefender, and BlackBerry Cylance are Strong Performers; and Cisco, Palo Alto Networks, and FireEye are Contenders.

Behavioral Protection, OS Support, And Risk-Based Policies Are Key Differentiators

As legacy technology becomes outdated and less effective, improved behavioral protection will dictate which providers will lead the pack. Vendors that can provide strong behavioral protection across multiple OSes, combined with risk-based security policies, position themselves to successfully deliver a strong frontline of endpoint defense to their customers.

The Forrester Wave™: Endpoint Security Suites, Q3 2019

The 15 Providers That Matter Most And How They Stack Up



by Chris Sherman
with Stephanie Balaouras, Merritt Maxim, Matthew Flug, and Peggy Dostie
September 23, 2019

Table Of Contents

Related Research Documents

The Forrester Wave™: Endpoint Security Suites, Q2 2018

The Future Of Endpoint Protection, 2019 To 2024

The State Of Endpoint Security, 2019

FORRESTER®

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

Endpoint Security Suite Buyers Prioritize Automatic Threat Protection

Security leaders are concerned with increasing complexity in their endpoint environment, compounded by advanced, multistage attacks going beyond typical malware.[1] Endpoint security suites are now more than ever being tasked with protecting against targeted-style threats that utilize multiple stages involving user interactions, exploit chaining, and script-based attacks.[2] As mass threats increase in sophistication, buyers and vendors have begun focusing on behavioral detection with automatic response. As a result of these trends, endpoint security suite customers should look for providers that:

› **Tightly integrate threat prevention, detection, and response.** Many organizations have experimented with endpoint point-products such as endpoint detection and response (EDR) and app isolation tools but failed to see significant business value due to the steep operational requirements of managing these solutions. Endpoint security suites help address this gap by automating and orchestrating multiple threat prevention, detection, and response capabilities into a single product.

› **Extend visibility and control over a broad endpoint ecosystem.** Endpoint buyers are looking to protect an increasing number of devices brought into the workplace. Mature suite offerings today offer threat prevention and detection capabilities across Windows, Mac, and Linux. Chromebooks and embedded device coverage are also offered by some of the suites on the market.

› **Offer flexibility in a variety of environments and risk tolerances.** Endpoint security suites generally offer a myriad of configurations and deployment models (i.e., cloud-managed, on-prem) to meet the needs of the most restricted to the most culturally relaxed environments. The best solutions use risk-based approaches to policy architecture and enforcement in order to help support a Zero Trust device posture.

Evaluation Summary

The Forrester Wave evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in Forrester's annual state of endpoint security report.[3]

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Endpoint Security Suites, Q3 2019

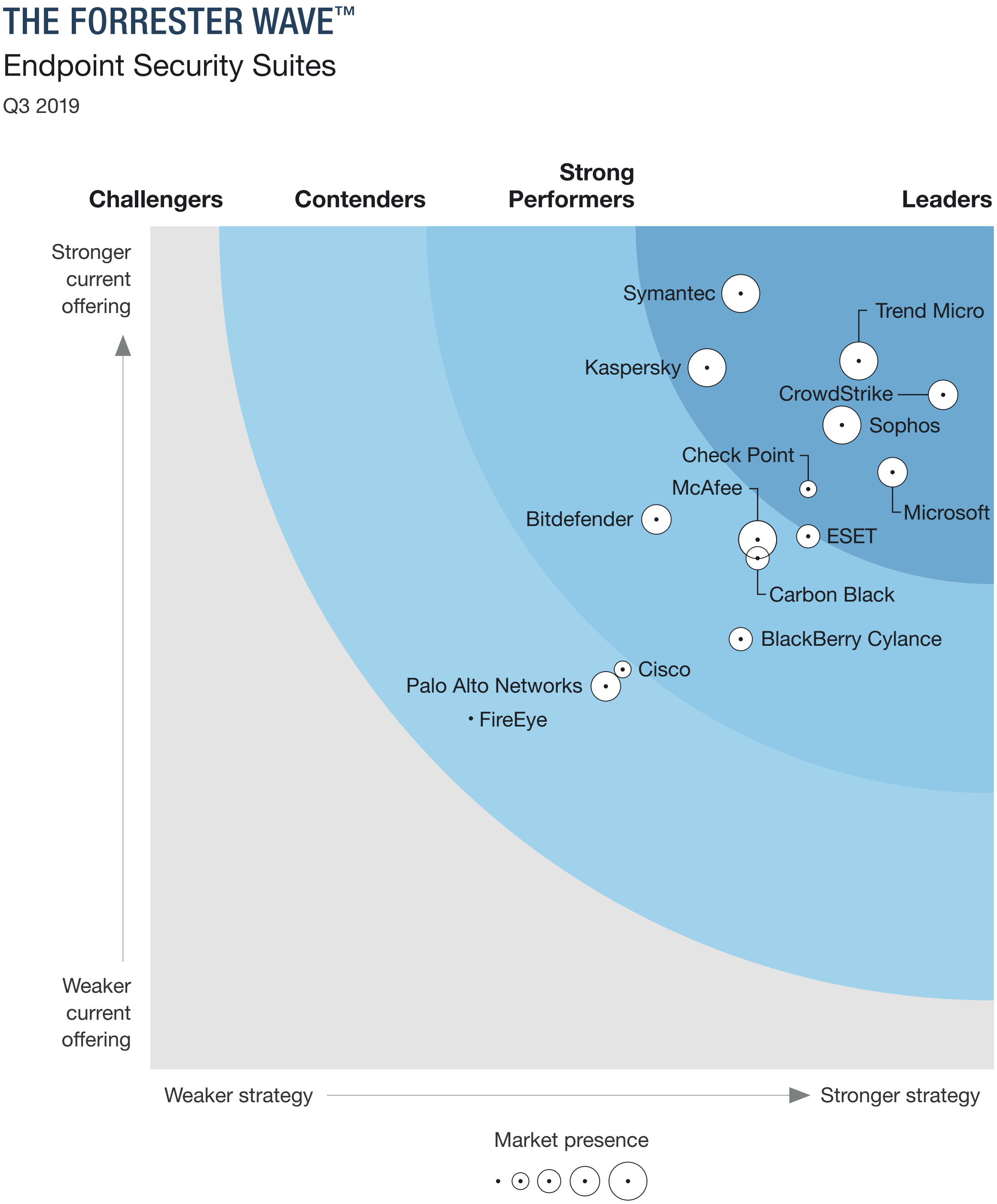


FIGURE 2 Forrester Wave™: Endpoint Security Suites Scorecard, Q3 2019

	Forrester's weighting	Bitdefender	BlackBerry Cylance	Carbon Black	Check Point	Cisco	CrowdStrike	ESET	FireEye
Current offering	50%	3.26	2.55	3.03	3.44	2.37	4.00	3.16	2.08
Threat prevention	20%	3.60	2.00	4.00	3.80	2.20	3.80	2.60	2.20
Threat detection	20%	2.50	3.00	4.50	2.50	2.50	5.00	4.00	4.00
Control	15%	3.00	1.67	2.33	4.33	1.33	3.00	2.33	1.33
Data security	10%	3.00	0.00	0.00	5.00	0.00	1.00	3.00	0.00
Mobile	5%	3.00	0.00	0.00	5.00	3.00	5.00	3.00	0.00
OS support	10%	5.00	5.00	3.00	3.00	5.00	5.00	5.00	1.00
Product performance	20%	3.20	4.00	3.40	2.40	2.90	4.70	2.70	2.70
Strategy	50%	3.00	3.50	3.60	3.90	2.80	4.70	3.90	1.90
Product road map	40%	3.00	5.00	3.00	3.00	1.00	5.00	3.00	1.00
Corporate vision and focus	30%	3.00	3.00	5.00	5.00	3.00	5.00	5.00	3.00
Zero-Trust framework alignment	15%	1.00	1.00	3.00	5.00	5.00	3.00	3.00	1.00
Security community involvement	15%	5.00	3.00	3.00	3.00	5.00	5.00	5.00	3.00
Market presence	0%	4.00	3.00	3.00	2.00	2.00	4.00	3.00	1.00
Partner ecosystem	50%	5.00	3.00	5.00	3.00	3.00	5.00	3.00	1.00
Enterprise customer base	50%	3.00	3.00	1.00	1.00	1.00	3.00	3.00	1.00

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

FIGURE 2 Forrester Wave™: Endpoint Security Suites Scorecard, Q3 2019 (Cont.)

	Forrester's weighting	Kaspersky	McAfee	Microsoft	Palo Alto Networks	Sophos	Symantec	Trend Micro
Current offering	50%	4.16	3.14	3.54	2.27	3.82	4.60	4.20
Threat prevention	20%	4.60	3.00	4.00	2.20	4.60	5.00	4.20
Threat detection	20%	4.50	3.00	3.50	3.50	2.50	4.00	4.00
Control	15%	3.67	3.00	4.33	1.33	3.00	5.00	3.67
Data security	10%	5.00	5.00	5.00	0.00	5.00	5.00	5.00
Mobile	5%	3.00	3.00	3.00	3.00	5.00	5.00	5.00
OS support	10%	5.00	3.00	1.00	3.00	5.00	5.00	5.00
Product performance	20%	3.20	2.70	3.20	2.40	3.50	4.00	3.80
Strategy	50%	3.30	3.60	4.40	2.70	4.10	3.50	4.20
Product road map	40%	3.00	3.00	5.00	3.00	5.00	5.00	3.00
Corporate vision and focus	30%	3.00	3.00	5.00	1.00	3.00	1.00	5.00
Zero-Trust framework alignment	15%	3.00	5.00	3.00	5.00	3.00	5.00	5.00
Security community involvement	15%	5.00	5.00	3.00	3.00	5.00	3.00	5.00
Market presence	0%	5.00	5.00	4.00	4.00	5.00	5.00	5.00
Partner ecosystem	50%	5.00	5.00	5.00	3.00	5.00	5.00	5.00
Enterprise customer base	50%	5.00	5.00	3.00	5.00	5.00	5.00	5.00

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

Vendor Offerings

Forrester included 15 vendors in this assessment: Bitdefender, BlackBerry Cylance, Carbon Black, Check Point, Cisco, CrowdStrike, ESET, FireEye, Kaspersky, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec, and Trend Micro (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated	Product version evaluated
Bitdefender	GravityZone Ultra	2019
BlackBerry Cylance	Cylance PROTECT	2.0.1530
Carbon Black	Predictive Security Cloud	
Check Point	SandBlast Agent Endpoint Security	Client-E81.00, Management-R80.30
Cisco	Advanced Malware Protection for Endpoints (AMP for Endpoints)	Windows 6.4 MacOS 1.10 Linux 1.10 Android 1.0 iOS 1.4
CrowdStrike	Falcon	
ESET	ESET Endpoint Security	7.1
FireEye	FireEye Endpoint Security	4.8
Kaspersky	Kaspersky Endpoint Security for Business	11.1
McAfee	McAfee Endpoint	10.6
Microsoft	Microsoft Defender Advanced Threat Protection	
Palo Alto	Cortex XDR	Cortex XDR 1.2 and Traps 6.0
Sophos	Central Intercept X Advanced with EDR & Forensics Console	
Symantec	Symantec Complete Endpoint Defense	
Trend Micro	Smart Protection for Endpoints	

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **CrowdStrike has the most fully featured endpoint security suite with an EDR lineage.** Most EDR tools are increasing their native support for threat prevention technologies, but CrowdStrike has managed to outpace the other EDR players and, based on its recent IPO, is now one of the largest overall endpoint security suite vendors.[4] Its cloud-based Falcon platform was one of the first to offer direct technology-sharing partnerships through an open app marketplace, giving buyers the ability to extend endpoint capabilities quickly and directly through the console. This has positioned the company with one of the most active third-party development communities around their endpoint platform.

  CrowdStrike is the only vendor with an EDR background in this study to compete in complex AV-replacement deals with extensive suite requirements. Aside from active threat prevention and detection capabilities, it offers application control, mobile security, and secure configuration. Its trust and reputation-based framework allows for granular control over automated remediation. However, its data security capabilities are weak compared with others in this evaluation. Customers also cite a desire for more vulnerability management capabilities. For most organizations looking for an alternative to the traditional suite vendors, CrowdStrike is likely to meet many shortlist criteria.

- **Trend Micro continues to offer the most complete endpoint security solution.** Trend Micro has a long history of success in the endpoint threat protection market as demonstrated through continued interest from enterprise buyers. Its Connected Threat Defense architecture provides integrated threat intelligence and control over an extensive portfolio of email, endpoint, network, cloud, and security products aimed at enterprise buyers. Based in Japan, Trend Micro is removed from much of the geopolitical friction associated with other foreign-based vendors. Its strategy is to provide a tightly integrated suite of threat prevention, detection, and response capabilities without a lot of third-party product involvement.

  Since the last Forrester Wave, Trend Micro consolidated its offerings around a single agent, made several enhancements to its EDR product, and began offering a SaaS version of its management console, Apex Central. Its endpoint security offerings span the full gamut of threat prevention and detection with market-leading capabilities in both categories. Extensive services are also offered, including MDR services for network, endpoints, messaging, cloud workloads, and servers. Trust levels are factored into most decisions made by the engine, although they aren't always transparent or configurable by the admin. Behavioral analysis capabilities also don't offer enough depth to compete with the best in this study, for example, allowing the admin to block specific custom behaviors preexecution. Overall, Trend is well positioned for large or small organizations looking for a complete endpoint security suite, especially those with complex deployment requirements.

- **Symantec has an extensive technology portfolio, but its future is questionable.** Symantec has long been a leader in the endpoint security space. After the Bluecoat acquisition, its development of new endpoint security technologies sped up considerably and addressed many gaps in its portfolio and strategy when compared with newer entrants in the market. Two years later, customers are once again raising questions about its focus amid executive turnover, financial performance issues, and most recently in August 2019, its acquisition by Broadcom.

  Nonetheless, Symantec's investments in endpoint security technologies have positioned it well against the current field of suites. It offers one of the most in-depth security portfolios with a mix of traditional threat prevention and advanced behavioral controls. Since the last Forrester Wave, Symantec has improved its EDR and mobile security offerings significantly, in addition to several enhancements to its data security, asset management, and behavioral security offerings. It's worth noting that Symantec's customer satisfaction scores dropped slightly from the previous year due to customers expressing frustration regarding the complexity of the management console when trying to conduct threat detection and remediation workflows. If Broadcom continues to execute on its goal of building out endpoint security offerings, Symantec is likely to remain relevant for enterprise buyers for the foreseeable future.

- **Microsoft wants to be your primary endpoint security provider.** Microsoft's E5 licensing level for Windows 10 gives buyers access to Microsoft Defender ATP along with a number of advanced enterprise security functions that can be managed using Intune or SCCM. These capabilities are meant to replace third-party endpoint threat prevention and SOC-oriented EDR tools. Combined with Microsoft's enormous presence and deep bench of current and planned security capabilities, there has never been more enthusiasm for adopting Microsoft security capabilities among Forrester's enterprise clients.

  Microsoft has a compelling vision for the future where endpoint threat prevention and detection are completely integrated and inseparable. Windows' attack surface reduction technologies are effective, and customers are excited about the fast pace of development of its ATP product line, especially as it expands to cover non-Windows endpoints. Its position as the leading OS vendor gives Microsoft an obvious advantage over other vendors in this study, yet its integration partner network is small. This is changing as it expands to cover non-Windows OSes such as Apple and Linux. Management complexities still come up frequently in customer conversations; these will need to be addressed in the future if Microsoft is to succeed. Overall, Forrester expects Microsoft to fit well in environments with a lower security staff maturity, especially in environments where IT ops is heavily involved in the endpoint security suite selection and availability of services is a top criterion.

- **Sophos offers tight integration between endpoint, network, and cloud security layers.** Sophos has traditionally focused on the midenterprise market (firms with 2,000 to 5,000 employees) where security maturity is lacking yet advanced protection is needed. Its Intercept X product supplies on-host machine learning classification along with telemetry for its cloud-based Intercept X EDR tool to meet the needs of larger organizations as well. Automation between network and endpoint security workflows is provided with all major functions of the product, accessible via its cloud management console, Sophos Central.

Sophos' malware and exploit protection are rated highly by customers. Its extensive suite offerings in areas such as full disk encryption, device management, attack remediation, and mobile security give it breadth to work in the most demanding environments. However, threat-hunting workflows are not intuitive, and capabilities offered in its forensics console may not meet the needs of a sophisticated SOC. It's important to note that Sophos will be releasing an MDR offering in the fall of 2019 to address this need. Overall, Sophos is a good option for small to medium-size enterprises and larger enterprises without extensive threat hunting requirements.

› **Kaspersky has worked hard to prove you can trust it with your data.** Kaspersky's portfolio includes one of the highest-performing threat prevention engines in our study according to customer references and public tests. Still, Forrester clients in the US frequently tell us they won't purchase from Kaspersky due to past concerns over the company's allegiances. The company has made a number of moves to win back customer trust in the past year, such as making its code available for review by third parties, and business has continued to be strong outside of the US.

The product performs best in threat prevention, malicious behavior protection, and attack remediation. Additionally, its policy engines are extremely granular and risk-triggered, with a number of endpoint management functions available to the admin when needed. On the downside, the firm has fewer external integrations than other vendors, and customers cited console complexity as an issue. If you're looking for an alternative to the US-based security suites or don't have concerns regarding Kaspersky's allegiances, its product is likely to meet most of your threat prevention and detection requirements.

› **Check Point designed its endpoint security suite with network integration in mind.** Check Point's strategy begins with reducing the attack surface of the endpoint and providing a series of behavioral protection measures to detect and automatically remediate ongoing threat activity. Its portfolio consists of a number of core endpoint security capabilities as well as NGFW capabilities. The company designed both their endpoint and network security technologies to work closely with one another and provide a number of benefits to buyers when deployed side by side.

Check Point's focus on integrating the endpoint security capabilities with its network security portfolio has led to one of the tightest integrations between the two layers in this study, helping customers to enforce a Zero Trust approach on their endpoint devices. Additionally, its asset management capabilities benefit remediation by allowing admins to take more granular endpoint action without leaving the Sandblast console. Unfortunately, Check Point doesn't participate with many well-known public antimalware performance tests, and its user experience impact is higher than average in this study. Its threat-hunting capabilities are also very limited and don't offer centralized storage or custom behavioral detection rules. Nonetheless, Check Point offers a strong portfolio of traditional and new endpoint security technologies, making it suitable for a variety of customer needs.

Strong Performers

- **ESET now offers a full portfolio of enterprise offerings.** ESET historically focused on small business and consumer markets, but over the past several years, the company has increasingly catered to enterprise market demands. The company's Endpoint Security product has some of the largest deployments in this study, and during the past year the company has developed several capabilities aimed at enterprise buyers such as EDR, managed detection and response, threat intelligence services, and vulnerability management.

  ESET is perfect for buyers who value a simple, straightforward UI with more advanced functions easily invoked when required. Every year that ESET has participated in this evaluation, customers have rated it exceptionally well for its low impact to user experience as well as a low false positive rate. Two weaknesses made clear in this study were a lack of deep behavioral analysis for more advanced buyers and application control. Overall, ESET should easily fit the needs of most organizations looking for a vendor that offers a full portfolio of endpoint, email, network, and mobile security technologies.

- **McAfee's future is cloud-native behavioral detection and security management.** McAfee provides flexible options for endpoint security with its flagship McAfee Endpoint Security Product (ENS), MVISION Endpoint, MVISION EDR, and SaaS-based MVISION ePolicy Orchestrator (ePO). It provides asset management as well as security capabilities such as disk encryption, machine learning, and firewall management. With these recent moves, including steps to pull in management over native security functions, McAfee is betting on the market's need for more integrated, extensible, risk-based endpoint security products.

  McAfee's value lies in its behavioral detection, centralized management across multiple devices, and AI-guided investigations, with many useful integrations and automated workflows offered between ePO and third-party products. Its large suite of ancillary capabilities such as DLP, endpoint file/folder encryption, application control, and secure configuration easily meet the criteria of the most demanding threat prevention-focused RFPs. However, McAfee is still catching up on detection efficacy compared with others in this study. Forrester customers still express concern that its threat hunting capabilities are not on par with the competition. Updates to its agent architecture since our last evaluation have led to improvements in its reported stability, although overall performance is still a concern of many buyers. Overall, McAfee is an easy shortlist addition for any organization looking for integrated EPP and EDR delivery, a simple management experience, and a growing list of integrated, cloud-native security solutions.

- **Carbon Black offers strong threat detection and automatic remediation.** Carbon Black began life as Bit9 with a focus on best-of-breed application control combined with basic endpoint visibility. After acquiring Carbon Black, a startup focused on EDR, Bit9 took that name and began integrating the two technologies along with another well-regarded startup in the behavioral protection space, Confer. Over the past couple of years, the company has moved most functionality to its cloud console, the Predictive Security Cloud (PSC). This serves as a single point for consuming product telemetry and handling management over its CB Defense and CB Protection products (both evaluated in this study). In August 2019, VMware announced its intent to acquire Carbon Black; customer sentiment about the acquisition was not taken into account in our scoring.

We rated Carbon Black's threat-hunting capabilities higher than most of the other suite vendors in this study due to its maturity, level of behavioral analysis, and risk-triggered rules. However, while it often replaces other AV-focused suites in customer environments, its support for ancillary suite functions such as data security, vulnerability management, and secure configuration management is weak compared with others in this study. Carbon Black is well-suited in environments requiring advanced EDR tightly coupled to EPP, especially when extensive threat-hunting capabilities are required.

› **Bitdefender benefits from having one of the broadest sensor networks.** Bitdefender delivers its suite of threat prevention and behavioral protection tools through a single-agent architecture accessible via the GravityZone management console. Malware and exploits are prevented automatically, with basic threat-hunting capabilities offered through the same console. Its inclusion in dozens of popular third-party security tools as an OEM partner, along with a strong consumer IoT presence, feeds Bitdefender's analysis engine with a broad representation of customer environments and associated threats, ultimately benefiting product efficacy.

Since the 2018 Forrester Wave, Bitdefender most notably added new behavioral protection/EDR capabilities, began offering an MDR service, and significantly improved its UI. Its utilization of risk scores based on dynamic endpoint configuration is useful for admins looking to prioritize alerts more effectively. Customers also report higher than average threat prevention performance but cite frustration with the product's flexibility when it comes to threat hunting and behavioral analysis. Overall, Bitdefender is well suited for buyers who prioritize ease of use and automated endpoint security capabilities with few advanced threat-hunting requirements.

› **BlackBerry Cylance's future depends on the opportunities presented by BlackBerry.** CylancePROTECT pioneered the first machine learning-based on-host AV, paving the way for almost every other endpoint security vendor in the market. Today, the company's endpoint product includes many other threat prevention and detection tools, with the aim of establishing a complete endpoint protection strategy for buyers with low overhead and no network requirement. These were likely key reasons that BlackBerry decided to acquire the company earlier this year.

BlackBerry Cylance has a compelling vision for its product line, leveraging the ongoing data science projects at Cylance with the unified endpoint management capabilities and IoT device footprint held by BlackBerry. To succeed, the new BlackBerry Cylance must quickly execute on this road map as customers have begun to express concern over its future focus. Currently, the suite lacks data security, mobile security, and out-of-the-box granular remediation capabilities compared with others in this study. With its low admin overhead and resource utilization, BlackBerry Cylance is perfect for environments where network connectivity is unreliable or in replacement of other endpoint threat prevention products where performance is an issue.

Contenders

- **Cisco offers a strong vision but struggles to deliver new features fast enough.** Cisco has demonstrated a commitment to security through development of multiple endpoint security and network security technologies, each sharing threat intel and management infrastructure within the Cisco Threat Grid and Threat Intelligence Cloud. Its AMP security offering is the primary endpoint protection product in its portfolio and is focused on providing a behavioral threat protection layer with shared policies and remediation actions across its wider portfolio.

  Cisco offers one of the least obtrusive security products in the study, as customers reported low impact to endpoint user experience while the endpoint agent is in operation. Its OS support is also extensive, covering a number of server and endpoint operating systems. However, its lack of endpoint capabilities beyond basic prevention and more advanced behavioral protection holds it back in this study. Buyers report its conceptual vision of a risk-based endpoint-network security system is compelling, but that promised features don't come fast enough. Overall, Forrester sees Cisco AMP as a top solution for existing Cisco customers and those looking to augment an existing endpoint security investment.

- **Palo Alto focuses on behavioral protection with broad coverage.** Palo Alto's Traps endpoint product provides the vendor's main endpoint security protection measures, with its Cortex platform ingesting telemetry from the single-agent endpoint architecture. Its strategy has been to enable third-party technologies to offer new capabilities and integrations directly from the Cortex platform. These capabilities are highlighted in the first app on the platform, Cortex XDR, enabling threat hunting and analysis across PAN's portfolio of products and third parties, including endpoint, network, cloud, and email telemetry sources.

  Palo Alto's main value on the endpoint is in providing automatic behavioral protection indicative of exploits, as well as advanced behavioral analysis with granular levels of protection based on risk thresholds. On-host machine learning is also used to classify executables before they load; however, performance is only rated as average by customers in this evaluation. Ancillary suite technologies like data security and application control are lacking. Also, having two consoles, one for its EDR/partner platform, and another for the Traps management, adds a layer of complexity to the solution. Forrester expects Palo Alto to do well in environments where automation and risk-based security policies are highly valued, as well as existing customers of Palo Alto's network security offerings looking for tighter segmentation policy integration between network and endpoint assets.

- **FireEye's endpoint product offers the essentials — backed by extensive services.** FireEye boasts one of the largest private armies of incident responders on the planet, and the firm's endpoint security solution, FireEye Endpoint Security (formerly HX), is oriented toward advanced detection workflows that utilize the intelligence gathered by its intelligence and services. Its threat prevention capabilities focus on preventing malicious behavior indicative of exploit. FireEye offers preexecution threat prevention capabilities through a white-labeled AV engine, along with a FireEye machine learning engine and behavioral analysis engine, managed through a common console.

FireEye's solution can replace an endpoint security suite, but typically we see customers use it in conjunction with other threat prevention-focused tools. Its lack of support for ancillary suite capabilities puts it at a disadvantage in this study. However, with the complexity of detection increasing and prevention increasingly falling to the operating system vendor, FireEye's lack of differentiating prevention-oriented tools may be less of an issue in the future, especially as it improves its detection precision. Today, we see the most value in FireEye Endpoint Security when the customer has already deployed the FireEye platform, including FireEye's Email/Network security solutions.

Evaluation Overview

We evaluated vendors against 25 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include threat prevention, threat detection, control, and product performance.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product road map, corporate vision and focus, Zero Trust framework alignment, and security community involvement.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's partner ecosystem and enterprise customer base.

Vendor Inclusion Criteria

Forrester included 15 vendors in the assessment: Bitdefender, BlackBerry Cylance, Carbon Black, Check Point, Cisco, CrowdStrike, ESET, FireEye, Kaspersky, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec, and Trend Micro. Each of these vendors has:

- **A security suite that can prevent, detect, and remediate endpoint threats.** We consider solutions that offer only one or two of these three capabilities to be point products, not suites.
- **A high degree of interest from enterprise buyers.** We only included vendors that have substantial interest from enterprise security decision makers. For example, Forrester clients ask questions about each vendor by name during inquiries and other interactions.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by June 11, 2019 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] See the Forrester report "The State Of Endpoint Security, 2019."

[2] Source: Ian Beer, "A very deep dive into iOS Exploit chains found in the wild," Project Zero, August 29, 2019 (https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html).

[3] See the Forrester report "The State Of Endpoint Security, 2019."

[4] Software maker CrowdStrike Holdings soared in its trading debut after raising $612 million in one of the biggest-ever initial public offerings for a cybersecurity company. Source: Crystal Tse and Liana Baker, "CrowdStrike Almost Doubles in Debut as Tech IPOs Rush Ahead," Bloomberg, June 12, 2019 (https://www.bloomberg.com/news/articles/2019-06-12/crowdstrike-s-ipo-is-said-to-raise-612-million-amid-tech-rush).

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.