# The Forrester Wave™: Enterprise Detection And Response, Q1 2020

## The 12 Providers That Matter Most And How They Stack Up

by Josh Zelonis

March 18, 2020

## Why Read This Report

In our 14-criterion evaluation of enterprise detection and response providers, we identified the 12 most significant ones — Bitdefender, BlackBerry Cylance, CrowdStrike, Cybereason, Elastic, Kaspersky, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Trend Micro, and VMware Carbon Black — 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, Microsoft, And Trend Micro Lead The Pack**

Forrester's research uncovered a market in which CrowdStrike, Microsoft, and Trend Micro are Leaders; SentinelOne, Cybereason, Bitdefender, VMware Carbon Black, and Elastic are Strong Performers; and Kaspersky, McAfee, Palo Alto Networks, and BlackBerry Cylance are Contenders.

**Security Analytics Is The Key Differentiator**

As the enterprise detection and response (EDR) space continues to evolve, security analytics will dictate which providers will lead the pack. Vendors that can differentiate with superior security analytics position themselves to successfully deliver detection, triage, and response capabilities to their customers.

# The Forrester Wave™: Enterprise Detection And Response, Q1 2020

## The 12 Providers That Matter Most And How They Stack Up

by Josh Zelonis
with Joseph Blankenship, Matthew Flug, and Peggy Dostie
March 18, 2020

## Table Of Contents

## Related Research Documents

The Forrester MITRE ATT&CK Evaluation Guide

The Forrester Wave™: Vulnerability Risk Management, Q4 2019

Now Tech: Enterprise Detection And Response, Q1 2020

FORRESTER®

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

## The EDR Space Is In An Arms Race Extending Beyond The Endpoint

Extended detection and response (XDR) is a next-generation capability EDR vendors will bring to maturity over the next two years by integrating endpoint, network, and application telemetry into their solutions. While the current state of these capabilities is very nascent, security pros can position themselves for long-term success by recognizing that the underlying security analytics capabilities that enable detection, triage, and response will form the engine for integrating these other technologies into their EDR solutions.

As a result of these trends, security pros should look for EDR providers that:

- **Empower SOC analysts with incident-driven security analytics.** No compromise is the product of a single event without external factors such as misconfiguration coming into play. The ability to leverage analytic capabilities for root-cause analysis of the events on a compromised system and associate related alerts into a single incident, potentially across the entire environment, reduces investigation time and alert volume.
- **Provide a prescriptive remediation plan and the ability to orchestrate it.** The analytic qualities of a good EDR product should extend beyond detection into helping security pros understand the remediation actions which must take place in order to return the environment to an uncompromised state. Depending on the extent of the compromise, it may still make sense to reimage impacted devices, but having a remediation plan that can be executed at the click of a button is part of a good EDR product's value proposition.
- **Facilitate advanced use cases for MITRE ATT&CK.** Labeling an alert as being associated with a particular ATT&CK technique is informative but doesn't impact SOC workflows. Organizations need to be able to perform threat hunting using the abstraction provided by ATT&CK techniques and chain them into complex queries that describe behaviors, instead of individual events. Further, it's imperative that security products provide reporting capability for exporting information about observed ATT&CK techniques in the environment so clients can understand the coverage they provide.

## 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 our reports on enterprise detection and response.

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™: Enterprise Detection And Response, Q1 2020

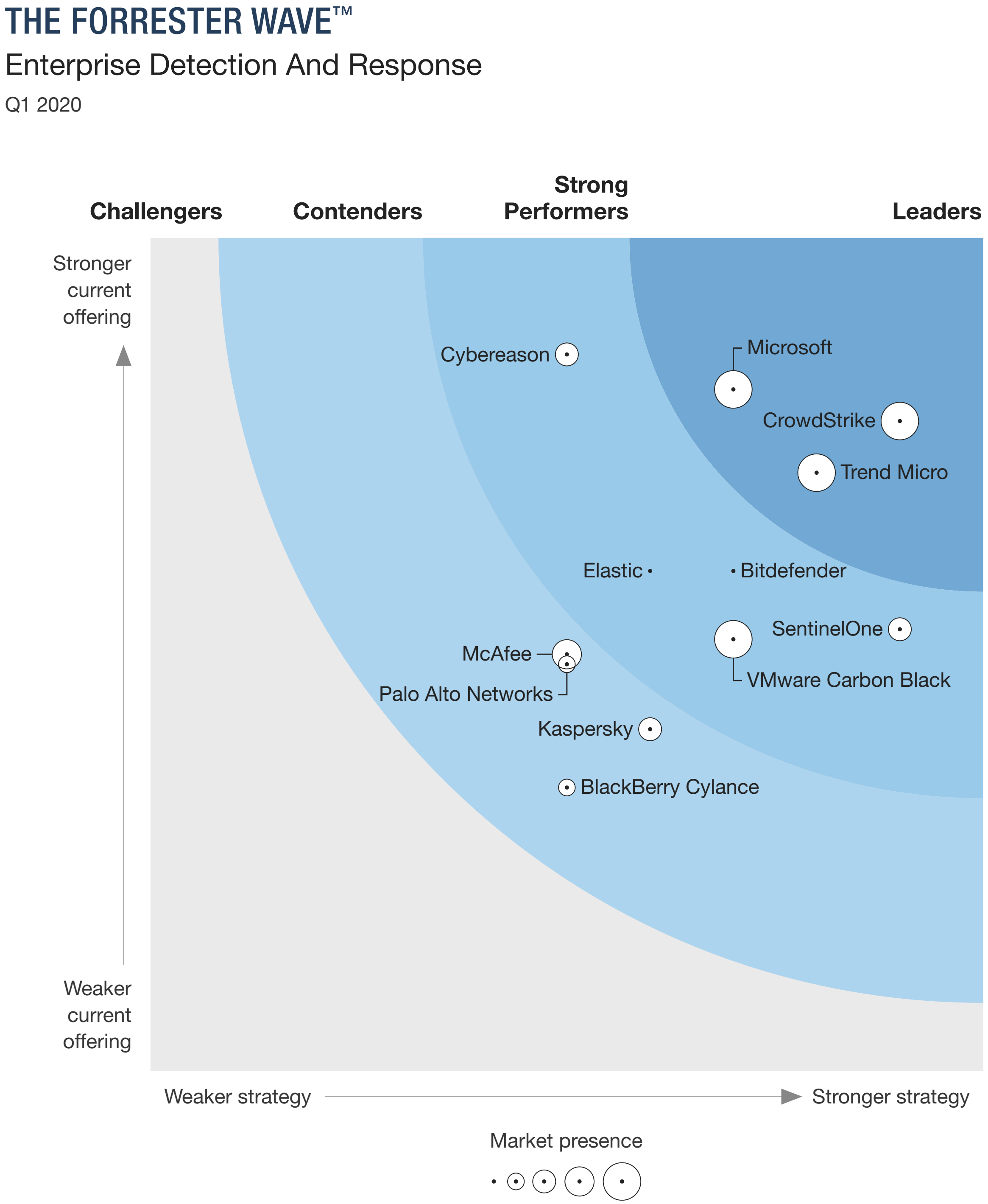

**FIGURE 2** Forrester Wave™: Enterprise Detection And Response Scorecard, Q1 2020

| | Forrester's weighting | Bitdefender | BlackBerry Cylance | CrowdStrike | Cybereason | Elastic | Kaspersky | McAfee | Microsoft | Palo Alto Networks | SentinelOne | Trend Micro | VMware Carbon Black |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Current offering** | 50% | 3.00 | 1.70 | 3.90 | 4.30 | 3.00 | 2.05 | 2.50 | 4.10 | 2.45 | 2.65 | 3.60 | 2.60 |
| Supported systems | 20% | 3.00 | 1.00 | 3.00 | 5.00 | 5.00 | 1.00 | 5.00 | 1.00 | 3.00 | 3.00 | 3.00 | 3.00 |
| Endpoint telemetry | 15% | 1.00 | 3.00 | 5.00 | 5.00 | 3.00 | 1.00 | 3.00 | 5.00 | 1.00 | 3.00 | 5.00 | 3.00 |
| Security analytics | 15% | 5.00 | 1.00 | 5.00 | 5.00 | 3.00 | 3.00 | 1.00 | 5.00 | 3.00 | 3.00 | 5.00 | 1.00 |
| Threat hunting | 5% | 3.00 | 5.00 | 5.00 | 5.00 | 5.00 | 3.00 | 1.00 | 5.00 | 5.00 | 5.00 | 1.00 | 5.00 |
| ATT&CK mapping | 15% | 3.00 | 1.00 | 5.00 | 5.00 | 1.00 | 3.00 | 1.00 | 5.00 | 0.00 | 5.00 | 3.00 | 1.00 |
| Response capabilities | 15% | 5.00 | 3.00 | 3.00 | 5.00 | 3.00 | 3.00 | 3.00 | 5.00 | 3.00 | 1.00 | 3.00 | 3.00 |
| Extended capabilities | 15% | 1.00 | 0.33 | 2.33 | 0.33 | 1.67 | 1.33 | 1.67 | 4.33 | 3.67 | 0.00 | 3.67 | 3.67 |
| **Strategy** | 50% | 3.50 | 2.50 | 4.50 | 2.50 | 3.00 | 3.00 | 2.50 | 3.50 | 2.50 | 4.50 | 4.00 | 3.50 |
| Product vision | 25% | 3.00 | 3.00 | 5.00 | 3.00 | 5.00 | 3.00 | 5.00 | 3.00 | 3.00 | 5.00 | 5.00 | 5.00 |
| Planned enhancements | 25% | 1.00 | 3.00 | 3.00 | 5.00 | 3.00 | 3.00 | 1.00 | 5.00 | 1.00 | 5.00 | 3.00 | 1.00 |
| Performance | 25% | 5.00 | 1.00 | 5.00 | 1.00 | 3.00 | 3.00 | 1.00 | 5.00 | 3.00 | 3.00 | 5.00 | 3.00 |
| Commercial model | 25% | 5.00 | 3.00 | 5.00 | 1.00 | 1.00 | 3.00 | 3.00 | 1.00 | 3.00 | 5.00 | 3.00 | 5.00 |
| **Market presence** | 0% | 1.00 | 1.67 | 5.00 | 2.33 | 1.00 | 2.33 | 3.67 | 5.00 | 1.67 | 3.00 | 4.33 | 4.33 |
| Enterprise clients | 33% | 1.00 | 1.00 | 5.00 | 1.00 | 1.00 | 3.00 | 3.00 | 5.00 | 1.00 | 1.00 | 5.00 | 3.00 |
| Deployed endpoints | 33% | 1.00 | 3.00 | 5.00 | 3.00 | 1.00 | 3.00 | 3.00 | 5.00 | 1.00 | 5.00 | 3.00 | 5.00 |
| Product line revenue | 33% | 1.00 | 1.00 | 5.00 | 3.00 | 1.00 | 1.00 | 5.00 | 5.00 | 3.00 | 3.00 | 5.00 | 5.00 |

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

## Vendor Offerings

Forrester included 12 vendors in this assessment: Bitdefender, BlackBerry Cylance, CrowdStrike, Cybereason, Elastic, Kaspersky, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Trend Micro, and VMware Carbon Black (see Figure 3). Forrester agreed at Symantec's request not to include them due to the difficulty of recommending a product in the absence of client reference availability for the vendor, and the unpredictability which follows from the Broadcom acquisition coinciding with this Forrester Wave.[1]

**FIGURE 3** Evaluated Vendors And Product Information

| Vendor | Product evaluated | Product version evaluated |
|---|---|---|
| Bitdefender | GravityZone Ultra | 6.2.21.46 |
| BlackBerry Cylance | CylanceOPTICS | 2.4 |
| CrowdStrike | Falcon | 5.2 |
| Cybereason | Cybereason Ultimate | 19.2 |
| Elastic | Elastic Security | 3.15 |
| Kaspersky | Kaspersky Endpoint Detection and Response | 1.6 |
| McAfee | McAfee MVISION EDR | 3 |
| Microsoft | Microsoft Defender Advanced Threat Protection | |
| Palo Alto Networks | Cortex XDR | 2.0 |
| SentinelOne | SentinelOne Complete | 3.5 |
| Trend Micro | Apex One with Endpoint Sensor enabled | 14 |
| VMware Carbon Black | Carbon Black Cloud | 3.x |

## Vendor Profiles

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

### Leaders

- **CrowdStrike continues to lead on strategy and execution.** It should come as no surprise that CrowdStrike Falcon is seldom purchased as a standalone product, since the company's adjacent services, such as threat hunting and cyber intelligence, are often the benchmark other client references use when describing capabilities they wish were available in their selected products. CrowdStrike has accomplished this by building service offerings designed to collect and enrich threat intelligence and feeding it back into their product and OverWatch service to ensure they're detecting even the most bleeding-edge attacks.

While clients rave about the detection capabilities CrowdStrike offers, it's not uncommon to hear from references and prospective customers that the macOS and Linux capabilities aren't quite on par. This is likely a state-of-the-market issue, as when clients leave, it's because something else was comparable and cheaper, as opposed to hearing the product has fallen behind competitors. Customers buy an EDR solution for its detection capabilities, and there simply are no other vendors in the space that have an intelligence organization of CrowdStrike's scale to enable the development and services to deliver that capability. Enterprises looking for strong detection capabilities, backed by threat intelligence and services, should consider CrowdStrike.

- **Microsoft wins on features and native integration.** Microsoft is a cash flush company, which has allowed it to build the most competitive product possible without the small company pressure of driving growth and appeasing venture capitalists. The result is an elegant solution that does just a little bit more than competitor offerings. Little things like having an "undo" button on the remediation page are unique and reflect the thoughtfulness that has gone into developing this product.

  If there is criticism to be levied against the product, it's bundling the price into Microsoft's E5 licensing, which leaves clients unsure if they're underpaying or overpaying for the solution, and the lack of clarity in its licensing for non-Windows environments. As a cloud infrastructure company, Microsoft should be able to deliver the same product at a lower price point than competitors that have to pass infrastructure costs on to the end user, so this confusion should not exist. Security buyers should look for a shift to a more transparent licensing model as a signal to buy. This solution is an excellent choice for organizations primarily running Windows due to the ease of deployment and management provided through native integration into the Windows 10 operating system.

- **Trend Micro delivers XDR functionality that can be impactful today.** Phishing may be the single most effective way for an adversary to deliver targeted payloads deep into an infrastructure. Trend Micro recognized this and made its first entrance into XDR by integrating Microsoft Office 365 and Google G Suite management capabilities into its EDR workflows. In doing so, the vendor's security analytics capabilities are able to perform root-cause analysis from the filesystem into the actual emails that delivered payloads, while surfacing similar emails delivered in the environment and removing them from user inboxes.

  One feature of the vendor's EDR product that is particularly thoughtful is the highlighting of noteworthy objects when doing a root-cause analysis. These objects provide hints for pivoting threat hunts to identify where else in the environment an adversary may have been. Client references universally appreciate the customer engagement they get from Trend Micro and the benefits of working with a portfolio vendor. While there is plenty to be positive about, it should be noted that the threat hunting capabilities lack the ability to create custom alerts or build complex queries to find interesting sequences of events. Trend Micro has a forward-thinking approach and is an excellent choice for organizations wanting to centralize reporting and detection with XDR but have less capacity for proactively performing threat hunting.

## Strong Performers

- **SentinelOne offers a competitive product that frequently wins on price.** The SentinelOne solution delivers an autonomous capability that assigns an identifier to sequences of events occurring on a system to allow an indictment to revert any behaviors within the context of that identifier. The vendor shifted its architecture to centralize telemetry in the cloud, thereby enabling the next step in its evolution — bringing cloud, network, and identity telemetry together to build out a complete security analytics platform.

  References most frequently cited the SentinelOne customer success team as the reason for initially selecting the product, as well as their continued satisfaction over time. Pricing flexibility is another advantage frequently cited by clients. Critically, the automated response capability is a bit of a gamble as it doesn't provide insight into the actions it will be performing. Further, SentinelOne was the only evaluated product that lacks an easy way for obtaining audit logs for their remediation actions. SentinelOne is a good choice for companies looking for a competitive solution with exceptional customer support.

- **Cybereason was founded on a vision for where the market is still going.** The technical founders of Cybereason futureproofed their EDR product by architecting it with the vision of combining the detection analytics synonymous with the EDR market, with the breadth of collection associated with the security information management (SIM) space. The vendor demoed some planned XDR capabilities that may reshape customer expectations for future EDR solutions, but the current offering isn't there yet.

  Cybereason's solution looks elegant, but many operations in the UI require multiple clicks that only provide an abridged view of the data that may take additional clicks to unroll. References were generally positive but indicated issues with customer support. Despite having a robust vision of the future, there are concerns about a lack of native integrations — so getting from proof of concept to reality with their XDR vision may present its own challenge. Cybereason has a competitive product and a unique UI that may be appealing to less technical analysts.

- **Bitdefender is the biggest EDR vendor you haven't considered but should have.** Bitdefender is democratizing advanced security technologies by focusing on the prevention of early kill chain events and the delivery of automated remediation postexecution. This strategy, delivered through direct, OEM, and managed service channels, makes Bitdefender one of the biggest EDR vendors. The vendor came up infrequently, however, when references were surveyed about products they had evaluated.

Clients praised not just the security performance of the product but also appreciated the management capabilities. Being able to isolate machines or even apply custom security profiles for specific users from a handheld device was seen as a big win. Critically, multiple references expressed a desire for more-granular reporting features. For example, they want to know not just how many users had been impacted by a security incident, but which ones. Bitdefender generally targets small and medium enterprises but is a good choice for organizations of any size.

› **VMware Carbon Black is building toward the future with a strong product vision.** Much of VMware Carbon Black's recent development effort has been on the back end. The vendor focused on bringing what was previously two different endpoint products together and moving to a cloud back end. This development effort positions the vendor to be more competitive in the future but unfortunately means that the current product, on the surface, doesn't appear to have matured much in the last two years.

While threat hunting capabilities have been synonymous with the VMware Carbon Black solution for years, customer references also noted the antimalware capabilities as one of the differentiators they continue to appreciate over time. The Confer acquisition from almost four years ago appears to be paying dividends. Carbon Black was struggling prior to acquisition but is a good option based on the strength of the VMware brand driving confidence in the vendor's continued viability post acquisition.

› **Elastic is poised to disrupt this market if their commercial model doesn't kill them.** The acquisition of Endgame by Elastic was exciting from a technology perspective due to the combination of an EDR with a security analytics platform. Unfortunately, by shifting its licensing to the much-maligned consumption model common in the enterprise SIM space, Elastic is creating downward pressure on adoption instead of encouraging people to broadly deploy its EDR solution. Endpoint products are long-term investments due to the difficulty of ripping and replacing them. This licensing model makes it difficult for enterprise buyers to buy into this licensing model and have a predictable budget.

Elastic is what happens when you get a bunch of hackers in a room together: You get good vision, what gets built is really interesting, but the total package feels less like a single product and more like a collection of really cool proof of concepts. Clients are extremely positive about the solution's detection capabilities, with configurability of what's being collected a frequently cited benefit. Elastic has a good solution for enterprises looking for mature endpoint capabilities with a strong vision for the future, if you can stomach the consumption model.

## Contenders

› **Kaspersky has a functional product but lacks refinement in messaging and design.** Kaspersky's product vision feels like it's an extended pitch deck for helping clients understand the product portfolio. One message that did land was an illustration of the frequency of different types of attacks an organization is likely to face — which may actually lead prospects to select a less feature-rich version of their product because their threat model doesn't justify the extra expenditure. In an era of fearmongering about advanced persistent threats, this was a breath of fresh air.

Reference customers generally noted that they selected the Kaspersky product based on price and reputation. They also mentioned commodity, table stakes features such as host isolation, and having a single agent for both endpoint protection and EDR. While Kaspersky EDR has standard levels of functionality, it can be difficult to differentiate shortcomings in analytic capabilities versus weaknesses in user experience. An example is the root-cause analysis tracing an issue to a particular file but not making it easy to discern the origin of the file on the system. Kaspersky can be a polarizing brand in the cybersecurity security space, but the vendor remains a popular choice based on portfolio and price.

› **McAfee has made great strides into the market but still has a way to go.** Any discussion of McAfee has to start by recognizing the tumultuous journey the vendor has undergone over the past 10 years and the resulting impact on direction and innovation.[2] Positively, over the past two years, McAfee has gone from being a late entrant into the EDR market to having a product that is worthy of consideration. However, with the current CEO transition, the organization is headed into another period of uncertainty, which must be a consideration before making a multiyear commitment to the solution.[3]

MVISION EDR was designed to provide guided investigations to help uplevel junior analysts without getting in the way of more senior analysts. Clients report being satisfied overall, with specific criticisms about a lack of both native and third-party integrations. This solution is ideal for organizations that have been contacted by their managed security service provider about an incident and then felt abandoned to go through the investigation by themselves.

› **Palo Alto Networks' (PANW) messaging has fallen behind its innovation.** PANW has brought a strong EDR product to market, but the question of how it will find success in an endpoint market where it has not had success in the past looms as a dark cloud. Unfortunately, the vendor's strategy lacks a compelling vision in a space it claims to have invented (XDR), and it was unable to generate excitement for the future by speaking to specific features or timelines on its roadmap.

PANW is leaning on its current firewall client base to gain market traction with some success, and clients frequently state that integration with other PANW technologies is a major selling point. Interestingly, when asked about other products they evaluated, many respondents didn't mention competing EDR products, referring instead to other product categories (like network analysis and visibility or NAV) — raising questions about how the solution is marketed. The Cortex XDR technology is both extremely powerful and well-integrated with other PANW products, making it a strong choice for current clients of the vendor's other products, but it's not recommended as a jumping off point into the PANW ecosystem.

- **BlackBerry Cylance has been slow to execute on its EDR product.** Cylance has some big ideas ranging from how it can use machine learning to continuously validate user sessions to how BlackBerry's own embedded operating system will provide it with a huge market advantage for deploying EDR in operational environments. Unfortunately, the market imperative of having a combined EDR and endpoint protection platform means the vendor needs to focus on bringing a more competitive EDR offering to market now, or risk going the way of the traditional endpoint vendors it was displacing five years ago.

  Customer references noted that they choose Cylance for the antimalware capabilities and appreciate the additional EDR capabilities offered by the vendor's Optics solution. Optics, however, does not appear to be leading deals. While one reference customer stated that they chose the CylanceOPTICS solution because of their belief in the Cylance vision and roadmap, multiple references expressed concern that Cylance has been struggling to deliver features on time. CylanceOPTICS is worth consideration as a line item for organizations that chose to go with the CylancePROTECT endpoint protection solution in order to leverage the benefits of a combined endpoint protection and EDR solution.

## Evaluation Overview

We evaluated vendors against 14 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 supported systems, endpoint telemetry, security analytics, threat hunting, ATT&CK mapping, response capabilities, and extended capabilities.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, planned enhancements, performance, and commercial model.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise clients, deployed endpoints, and product line revenue.

### Vendor Inclusion Criteria

Forrester included 12 vendors in the assessment: Bitdefender, BlackBerry Cylance, CrowdStrike, Cybereason, Elastic, Kaspersky, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Trend Micro, and VMware Carbon Black. Each of these vendors has:

- **Product efficacy.** The vendor has demonstrated confidence in the efficacy of this product through participation in the MITRE ATT&CK Evaluation against the tactics, techniques, and procedures elicited by APT29.
- **Enterprise adoption.** This product is being marketed and sold to enterprise customers. Each of these products is deployed by at least 250 enterprise clients.

- **Forrester mindshare.** To ensure relevance to Forrester clients and the quality of the references being provided, it is required that the product has been generally available and not undergone significant changes in the past six months.

## 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 January 28, 2020 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] Source: Anthony Spadafora, "Broadcom completes Symantec deal, rebrands as NortonLifeLock," TechRadar, November 6, 2019 (https://www.techradar.com/news/broadcom-completes-symantec-deal-rebrands-as-nortonlifelock).

[2] Source: Jeff Pollard, Josh Zelonis, Sandy Carielli, Sean Ryan, Jinan Budge, Merritt Maxim, Joseph Blankenship, Amy DeMartine, and Stephanie Balaouras, "Decade Retrospective: Cybersecurity From 2010 To 2019," Forrester Blogs, December 17, 2019 (https://go.forrester.com/blogs/decade-retrospective-cybersecurity-from-2010-to-2019/).

See the Forrester report "Quick Take: Intel Spins Off McAfee As Synergies Fail To Materialize."

[3] Source: Kimberly Chin, "McAfee CEO Chris Young to Depart," The Wall Street Journal, January 16, 2020 (https://www.wsj.com/articles/mcafee-ceo-chris-young-to-depart-11579217891).

FORRESTER®

forrester.com

## We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- › Research and tools
- › Analyst engagement
- › Data and analytics
- › Peer collaboration
- › Consulting
- › Events
- › Certification programs

## 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.