The Forrester Wave™: Endpoint Security Software As A Service, Q2 2021

The 12 Providers That Matter Most And How They Stack Up

by Chris Sherman

May 13, 2021

Why Read This Report

In our 24-criterion evaluation of endpoint security SaaS providers, we identified the 12 most significant ones — Bitdefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro, and VMware — 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.

The Forrester Wave™: Endpoint Security Software As A Service, Q2 2021

The 12 Providers That Matter Most And How They Stack Up

by Chris Sherman
with Merritt Maxim, Allie Mellen, Shannon Fish, and Peggy Dostie
May 13, 2021

S&R Buyers Want Comprehensive Endpoint Security Delivered As SaaS

As the COVID-19 pandemic created pressure on security teams to migrate on-premises security products to cloud-managed, Forrester saw a significant uptick in client interest in SaaS-delivered endpoint security products. This was aided by many endpoint vendors' having close to feature parity between their on-premises endpoint security suite and their software-as-a-service (SaaS) version, making the migration to the SaaS version an easier decision. Today, most endpoint security suite providers offer all the major endpoint security capabilities managed via cloud-hosted consoles, with development efforts and new product features aimed predominantly at the SaaS versions.

The focus on endpoint security has increased as cyber risks shift from the network to the endpoints, prompted by increasing amounts of homeworkers and the bulk movement of data from enterprise network-connected data centers to edge devices. As a result, endpoint security SaaS customers should look for providers that are:

- **Current.** Providers must innovate and adapt to the demands placed on modern endpoints as new risks and business pressures emerge. When selecting a solution, buyers want to see strong evidence of corporate leadership, continuous development with new features relevant to current use cases, and a track record of innovation.
- **Effective.** Endpoint security tools must balance effective threat prevention with automatic and precise threat detection, validated through continued participation in lab tests such as MITRE ATT&CK and AV-Comparatives Endpoint Prevention and Response Test, both of which combine threat prevention and detection performance assessments. Buyers should also look for SaaS platforms that are mature with global coverage and built on agent architectures that enable fast and efficient network communications with limited impact to endpoint user experience during active protection measures.

FORRESTER®

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

- **Built to integrate.** Endpoint security can't operate in a vacuum considering the multifaceted nature of most attacks. Modern endpoint security vendors recognize this and offer integrations with other security and non-security layers beyond the endpoint (e.g., IT service management, cloud security, network security, and identify and access management). Buyers should look for endpoint security providers that support extended detection and response (XDR) capabilities and integrations, along with Zero Trust-aligned policies and enforcement levels.

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.

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 Software As A Service, Q2 2021

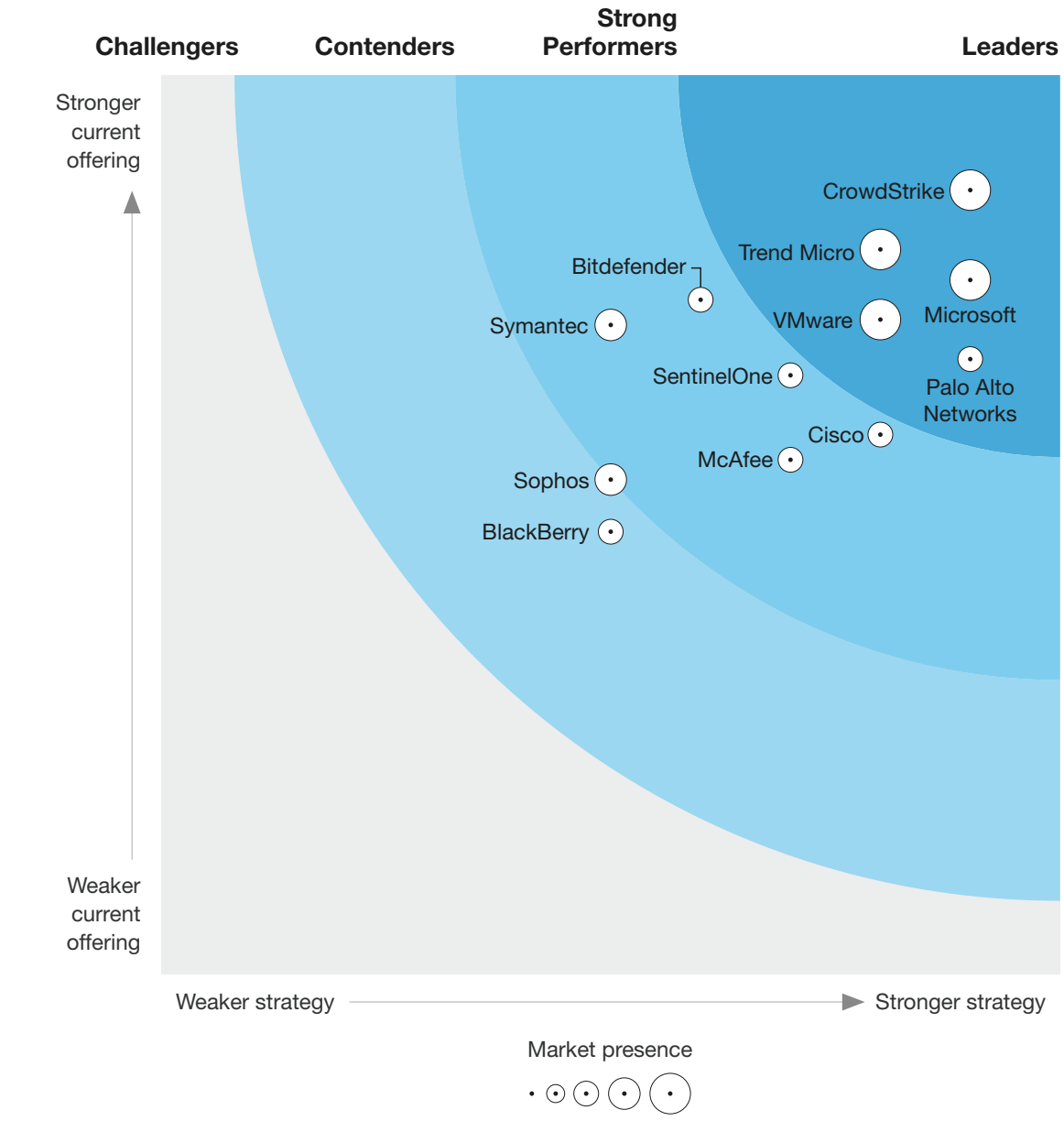

FIGURE 2 Forrester Wave™: Endpoint Security Software As A Service Scorecard, Q2 2021

	Forrester's weighting	Bitdefender	BlackBerry	Cisco	CrowdStrike	McAfee	Microsoft	Palo Alto Networks	SentinelOne
Current offering	50%	3.75	2.46	3.00	4.36	2.86	3.86	3.42	3.33
Threat prevention	20%	4.20	3.00	3.40	4.60	3.40	3.80	4.20	3.00
Threat detection	20%	2.50	1.75	3.50	4.50	2.00	4.00	5.00	4.50
Control	20%	3.67	1.67	2.33	4.33	3.67	5.00	3.00	3.00
Data security	5%	3.00	1.00	0.00	1.00	3.00	5.00	1.00	1.00
Mobile security	5%	3.00	5.00	3.00	5.00	5.00	5.00	1.00	1.00
OS support	5%	5.00	5.00	5.00	5.00	3.00	1.00	5.00	5.00
Product performance	25%	4.50	2.50	3.00	4.50	2.00	3.00	2.50	3.50
Strategy	50%	3.00	2.50	4.00	4.50	3.50	4.50	4.50	3.50
Product roadmap	25%	3.00	5.00	3.00	5.00	3.00	3.00	3.00	5.00
Corporate strategy	25%	5.00	1.00	3.00	5.00	3.00	5.00	5.00	5.00
Zero Trust framework alignment	25%	1.00	3.00	5.00	3.00	5.00	5.00	5.00	3.00
Security community involvement	25%	3.00	1.00	5.00	5.00	3.00	5.00	5.00	1.00
Market presence	0%	3.00	2.33	3.00	4.33	3.00	5.00	2.33	2.33
Partner ecosystem	33%	5.00	1.00	5.00	5.00	5.00	5.00	3.00	3.00
Enterprise customer base	33%	1.00	3.00	1.00	3.00	1.00	5.00	3.00	1.00
Enterprise penetration	33%	3.00	3.00	3.00	5.00	3.00	5.00	1.00	3.00

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

FIGURE 2 Forrester Wave™: Endpoint Security Software As A Service Scorecard, Q2 2021 (Cont.)

	Forrester's weighting	Sophos	Symantec	Trend Micro	VMware
Current offering	50%	2.75	3.61	4.03	3.64
Threat prevention	20%	3.00	5.00	5.00	3.40
Threat detection	20%	2.00	3.00	4.00	4.00
Control	20%	3.00	3.67	3.00	3.67
Data security	5%	5.00	3.00	5.00	1.00
Mobile security	5%	5.00	5.00	5.00	5.00
OS support	5%	3.00	5.00	5.00	5.00
Product performance	25%	2.00	2.50	3.50	3.50
Strategy	50%	2.50	2.50	4.00	4.00
Product roadmap	25%	1.00	3.00	5.00	3.00
Corporate strategy	25%	3.00	1.00	3.00	5.00
Zero Trust framework alignment	25%	3.00	3.00	3.00	5.00
Security community involvement	25%	3.00	3.00	5.00	3.00
Market presence	0%	3.67	3.67	4.33	4.33
Partner ecosystem	33%	1.00	5.00	3.00	5.00
Enterprise customer base	33%	5.00	3.00	5.00	5.00
Enterprise penetration	33%	5.00	3.00	5.00	3.00

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

Vendor Offerings

Forrester included 12 vendors in this assessment: Bitdefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro, and VMware (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated	Product version evaluated
Bitdefender	Bitdefender GravityZone Ultra Security	2021
BlackBerry	BlackBerry Cyber Suite, BlackBerry Spark Suite	N/A
Cisco	Cisco Secure Endpoint (CSE)	Console v5.4
CrowdStrike	Falcon	N/A
McAfee	McAfee Endpoint Security	v10.7
Microsoft	Microsoft Defender for Endpoint (MDE)	N/A
Palo Alto Networks	Cortex XDR	v2.7
SentinelOne	Singularity Complete	Platform: Machu Picchu release
Sophos	Intercept X Advanced	v3
Symantec	Endpoint Security Complete	N/A
Trend Micro	Apex One	N/A
VMware	Carbon Black Cloud	N/A

Vendor Profiles

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

Leaders

- **CrowdStrike offers superior endpoint security with a cloud-native architecture.** CrowdStrike has enjoyed rapid growth since it first launched its endpoint security SaaS platform in 2011 in the US. Its portfolio covers endpoint security, public cloud security, identity security, workload protection, and IT operations tooling. Customers continue to praise CrowdStrike's automatic detection and response features and overall effectiveness, especially as the company progresses with an XDR strategy while pulling data in from a growing ecosystem of sensors. Further, the Falcon Store is one of the most active third-party app ecosystems in this study and provides additional endpoint and non-endpoint capabilities, extending CrowdStrike's capabilities into areas such as DLP and ICS/IoT security.

While CrowdStrike offers comprehensive threat prevention and detection, users report a high level of skill required to operate the product effectively. The Falcon agent also lacks DLP and data security capabilities, relying instead on partners through their app ecosystem to provide more-comprehensive data security features. Also, CrowdStrike's customer reference and third-party test scores for malware prevention were average when compared with others in this study, although references feel this is offset by their much higher detection performance. Customers looking for strong threat protection efficacy and comprehensive threat hunting capabilities will find CrowdStrike a good option.

- **Microsoft strikes a balance between endpoint security and user experience.** Microsoft offers its endpoint security capabilities as a stand-alone product, Microsoft Defender For Endpoint (formerly Advanced Threat Protection), supporting Android, iOS, Linux, macOS, and Windows. Third-party labs and customer reference scores both point to continued improvement over antimalware and anti-exploit efficacy where Microsoft frequently outperforms third-party competitors. Its impact on the endpoint is also notably low when actively running on the endpoint, and the number of reported false positives by customers is also the lowest in this evaluation.

  On the downside, integration and workflow challenges persist. Administrators complain about the amount of screen switching and lack of integration between threat prevention and detection screens. Also, while Microsoft offers protection for non-Windows endpoints, the depth and breadth of features offered is lacking when compared with competing offerings. For organizations that are heavily dependent on Windows, especially those that are using Office 365 or have an E5 license, Defender for Endpoint is an excellent option.

- **Trend Micro offers a comprehensive endpoint security portfolio focused on detection.** As one of the original antimalware vendors, Japan-based Trend Micro offers comprehensive endpoint threat prevention, threat detection, secure configuration, attack response, and data security capabilities within a wider portfolio of security products and services. Buyers enjoy complete feature parity between the company's on-premises and managed versions of Apex Central, allowing for easy transitions during the "hybrid" phase. Its extended detection capabilities are robust and accessible from Trend Micro Vision One, a separate console designed to consume telemetry and environment data from both Trend Micro and third parties spanning network, cloud workload, email, and endpoint sources.

  Buyers complain that the admin experience can be cumbersome at times, and the separation between Trend Micro Vision One and Apex Central is likely to cause some administrator friction until additional functionality is migrated to the new platform. There have also been recent reports of customers having challenges removing old versions of the agent, but overall customer satisfaction remains consistently high. Forrester expects Trend Micro will continue to serve large organizations well, especially those with comprehensive endpoint security requirements.

- **Palo Alto Networks (PAN) integrates endpoint threat prevention with extended detection.** US-based Palo Alto Networks' SaaS offerings focused on endpoint security and extended detection and response are all branded under Cortex XDR. For the past couple of years, PAN

has been rapidly growing its endpoint security capabilities and security portfolio breadth through acquisitions and product development. The company replaced its legacy on-premises endpoint security platform with Cortex XDR, showing improvements in areas including automatic behavioral protection and threat analysis. As the first vendor to promote an XDR strategy, PAN's is the most comprehensive in this study, offering threat prevention, detection, and access controls spanning endpoint, IoT, network, and cloud apps. Acquisitions into SOAR (Demisto) and cloud CASB give buyers who have invested in multiple PAN products access to powerful automation sequences and cloud access policies between native and third-party products.

This growing portfolio of capabilities and consoles comes at the expense of simplicity, with buyers rating the deployment and operation of the product as above average in difficulty. Agent performance issues have been reported when deployed on endpoints with less-than-standard performance specs. Cortex XDR also doesn't offer all the traditional suite capabilities such as application control, data security, and comprehensive native security management. Palo Alto Networks is an easy shortlist addition for enterprise buyers looking to adopt a modern endpoint security solution or a broad XDR strategy with strong threat prevention.

- **VMware aims to reduce the friction between IT security and operations.** US-based VMware offers a full portfolio of device security, digital workspace, and virtualization technologies and services supporting its vision to unify infrastructure, security, and IT management for its customers' environments. Its primary endpoint security offering, Carbon Black Cloud, offers SaaS-delivered threat prevention, device hardening, secure configuration, automatic attack detection, and threat hunting. Its integrations between access controls, device management, device security, network security, and applications allow for granular, risk-based security policies in support of a Zero Trust strategy.

  VMware's attack remediation capabilities are not as automated compared with others in this study. Reference customers complained of poor analyst workflows when responding to attacks (e.g., configuration rollback and certain remediation actions require analysts to move between consoles). While the pace of endpoint security innovation has been improving post-VMware acquisition, there is still some concern around future strategy given the recent CEO departure and an impending VMware spinoff from Dell. For buyers willing to work through this transition, especially those who are existing VMware customer or interested in their managed services, VMware is an excellent option.

Strong Performers

- **Cisco has built a compelling portfolio of SaaS-delivered security capabilities.** Cisco's Secure Endpoint focuses on endpoint threat prevention, automatic behavioral protection, and threat hunting through the Orbital Advanced Search capability. Cisco's SecureX platform pulls in and correlates security telemetry from the customer's devices, workloads, and applications through Cisco products and third-party integrations (which already has 50 partners and has grown

significantly in the past year). While the company has primarily focused on core antimalware and behavioral security capabilities, its commitment to building granular network and application access controls based on endpoint device posture and user risk is compelling for those looking to adopt a Zero Trust strategy.

Cisco doesn't offer common ancillary suite capabilities, with limited support for patch management, data security, application control, and device control (the latter planned for a future release). Also, Secure Endpoint's more advanced attack investigation and response tasks can be cumbersome, with customers complaining of convoluted workflows between policy management and threat investigation. For organizations looking for only core threat prevention and behavioral protection without a lot of extra endpoint security requirements, Cisco Secure Endpoint is a solid choice.

- **SentinelOne focuses on broad and automatic protection with low admin overhead.** SentinelOne was founded in Tel Aviv in 2013 but has since moved its headquarters to the US, enjoying rapid growth in enterprise buyer interest over the past three years. Its main endpoint security platform, SentinelOne Singularity, offers customers full antimalware, anti-exploit, runtime behavior protection, and excellent remediation capabilities including full file and configuration rollback. Its SaaS architecture is highly scalable and easy to manage, with comprehensive coverage beyond the endpoint (e.g., cloud workloads, network, and IoT). Its IoT Ranger agent capability is the only product in this evaluation that offers IoT device discovery and policy enforcement via its endpoint-based agent (uses host-based deep packet inspection).

  SentinelOne lacks some of the ancillary suite features that more-traditional enterprise buyers still look for, such as vulnerability management, DLP/device control, encryption, and host firewalls. Forrester clients and reference customers complained about the stability of staffing during new agent updates; however, support was generally faster and more responsive compared with others in this study. SentinelOne is a solid option for large and small enterprises looking to simplify their endpoint security stack and detection workflows while supporting a broader security strategy.

- **Bitdefender offers simple SaaS management and an extensive partner ecosystem.** Bitdefender focuses on endpoint security and has broadened to include cloud workload protection and managed services. It features market-leading antimalware and anti-exploit capabilities as validated through third-party tests and customer-supplied efficacy scores. Bitdefender's extensive partner ecosystem utilizes telemetry gathered from a variety of consumer and enterprise sources. This is combined with a corporate commitment to automate threat prevention and detection across a variety of current attack and environment types while preparing customers for future threats through its commitment to research and community participation (e.g., Bitdefender's involvement in postquantum cryptography standardization efforts).

  Bitdefender has moved to a SaaS platform to manage most of its endpoint security capabilities, although its on-premises application control capabilities are not supported from its SaaS platform. Its behavioral analysis capabilities likely won't satisfy advanced buyers looking for more user behavior analysis and correlation. Headquartered in Romania with sales and support

coverage around the world, Bitdefender is an attractive option for small to large global enterprises looking for an easy-to-manage solution with a low staffing requirement and limited manual threat hunting needs.

- **McAfee is transitioning to cloud-native solutions under new ownership.** The past several years have seen lots of change for US-based McAfee as it transitioned its strategy from on-premises-centric to cloud-native solutions; the March 2021 announcement of its enterprise group's sale to Symphony Technology Group is just the latest. While its endpoint security customer base is still heavily on-premises, McAfee has been working to move customers to its new MVISION Complete cloud-only service that combines endpoint threat prevention, data protection (encryption/DLP), web security, and a cloud security gateway. Its focus on risk-based security policies is also frequently cited as a benefit by customers, with admin-defined risk thresholds and strong contextual information provided by ePO, MVISION Insights, and other sources within their portfolio.

  Several features of its endpoint portfolio are still in process of migration to cloud management, leading to dependencies for buyers. Also, its extended detection strategy is immature and doesn't pull data from cloud, web, network, and third-party sources at this time. While reference customers expressed concern for McAfee's future direction, it will remain a viable candidate for many organizations' shortlists if it can execute on its roadmap fully over the next year and build out its detection platform to include more non-endpoint sources.

- **Symantec offers technical breadth but must be given room to innovate under Broadcom.** Symantec has been a dominant player in the endpoint security market for decades. After Symantec was acquired by US-based Broadcom in 2019, Forrester customers expressed concern that the company would fall behind competitively. While there were initial sales and support issues after the acquisition, these have all been resolved. With a large portfolio of endpoint security technologies, it's important for Symantec to not lose focus under Broadcom and continue to innovate. Currently, Symantec can offer a complete SaaS solution that integrates endpoint security with other non-endpoint sources in their cloud. It has a leg up on competitors with its deep bench of network, email, web, data, and cloud security services and products.

  Customers complain that there are too many correlation efforts between the different Symantec products. Also, customer satisfaction over its remediation granularity and level of automation was low compared with the average in this study. If Symantec executes on its roadmap, enterprises already invested in Symantec will find compelling reasons to remain with Symantec over the long term.

- **Sophos offers a full suite of capabilities but struggles with agent performance.** UK-based Sophos was acquired by Thoma Bravo in early 2020, adding to the private equity firm's growing portfolio of security and IT service management vendors. Intercept X was one of the first endpoint security products on the market to leverage deep learning (via the Invincea acquisition) and today represents Sophos' primary endpoint agent with integrated prevention and detection. Sophos' customers appreciate the tight integration between its offered security services and the product, as

well as the integrated web filtering and automatic ransomware remediation capabilities. Its mobile security offerings are differentiating, including mobile threat defense and the level of integration between the mobile and endpoint security management.

Several Sophos customers have expressed concern to Forrester over declining threat prevention performance and difficulty in reaching resolutions with support. It's worth noting that Sophos has a long history of excellent support reported by customers from earlier Forrester Wave evaluations; likewise, Forrester expects this to be remedied. Also, admins have complained about the complexity in trying to move from policy creation to product management and operations, including manual threat hunting work. While Sophos remains a solid choice for small- to medium-sized enterprises looking for one vendor with a full portfolio of endpoint and non-endpoint security technologies, larger enterprises should adequately test the Sophos agent in their environment to ensure environmental fit and alignment with other security investments.

Contenders

- **BlackBerry extends threat prevention beyond traditional endpoint security.** BlackBerry Cyber Suite (formerly Cylance Protect) combines machine learning-based malware protection with suite capabilities such as application control, attack remediation capabilities, and native security management. Customers report low performance impact scores and high satisfaction with the core malware prevention capabilities. BlackBerry's continuous authentication capabilities through Persona continue to be unique among competitors and serve both authentication and risk management capacities, especially when combined with the vendor's plans to extend its coverage beyond user endpoints (e.g., IoT and automotive).

  A lack of behavioral analysis and exploit prevention capabilities holds it back in this evaluation, along with limited SaaS-managed endpoint security functions (some still require on-premises management). BlackBerry's EDR data is not hosted in its cloud, a standard today among competitors, but Forrester is informed this will be addressed in Optics 3 in the second quarter of 2021. Overall, BlackBerry has several opportunities between its endpoint management and security investments, and its identity-focused Zero Trust story will likely be compelling to organizations looking for unique approaches to tracking and protecting against endpoint risk.

Evaluation Overview

We evaluated vendors against 24 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 roadmap, 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 12 vendors in the assessment: Bitdefender, BlackBerry, Cisco, CrowdStrike, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Symantec, Trend Micro, and VMware. Each of these vendors has:

- **A SaaS-based 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. Product must have been in the market for 12 months prior to the Forrester Wave survey submission deadline.
- **A high degree of interest from Forrester buyers.** We only included vendors that have substantial interest from enterprise security decision makers as determined through Forrester client inquiry mentions. For example, Forrester clients ask questions about each vendor by name during inquiries and other interactions.
- **A strong enterprise market presence.** We only included vendors with at least 600 enterprise customers (each with 1,000+ nodes deployed) on their SaaS platform as of the Forrester Wave cutoff date.

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 February 23, 2021 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™ and New 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.

We help business and technology leaders use customer obsession to 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.