The Forrester Wave™: Endpoint Security Suites, Q2 2018

The 15 Providers That Matter Most To Enterprises And How They Stack Up

by Chris Sherman and Salvatore Schiano

June 21, 2018

Why Read This Report

In our 21-criteria evaluation of endpoint security suite providers, we identified the 15 most significant ones — Bitdefender, Carbon Black, Check Point, Cisco, CrowdStrike, Cylance, ESET, Ivanti, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, Sophos, Symantec, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up to help security professionals make the right choice.

Key Takeaways

Trend Micro, CrowdStrike, And Symantec Lead The Pack
Forrester's research uncovered a market in which Trend Micro, CrowdStrike, Symantec, Check Point, ESET, Sophos, and Bitdefender are Leaders; Carbon Black, McAfee, Kaspersky Lab, Cisco, Cylance, Microsoft, and Malwarebytes are Strong Performers; and Ivanti is a Challenger.

Security Pros Want An Effective Endpoint Security Suite From Vendors They Trust
Buyers want an endpoint security suite that is effective at stopping modern threats without adding to their security team's complexity. They also want to trust the vendor, both as a strategic partner and as a steward of their data.

Behavioral Analysis, Automation, And Real-World Performance Are Key Differentiators
As traditional approaches to endpoint security prove less effective, behavioral protection and suite automation have become key differentiators in today's market. Buyers also want to see real-world performance that backs up vendor claims.

The Forrester Wave™: Endpoint Security Suites, Q2 2018

The 15 Providers That Matter Most To Enterprises And How They Stack Up

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

June 21, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Endpoint Security Suites, Q4 2016

The State Of Endpoint Security, 2018

TechRadar™: Endpoint Security, Q1 2017

FORRESTER®

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

Security Pros Are Demanding More-Effective Endpoint Security Suites

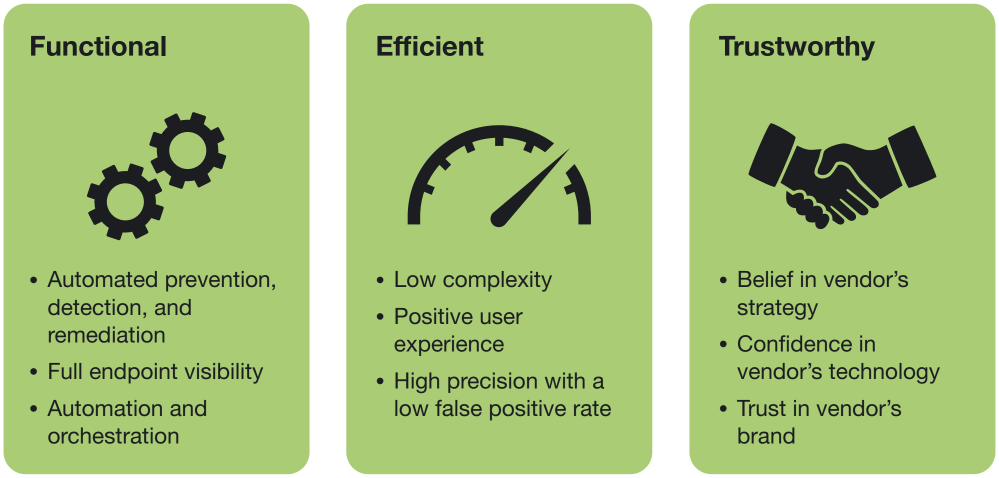
It's 2018, and employee endpoints continue to be the most targeted asset type in the enterprise.[1] Over the years, security teams have deployed a wide range of technologies to address threats to their corporate endpoints, and now many are opting for endpoint security suites with integrated prevention, detection, and automatic response. As vendors race to consolidate new methods of threat prevention with detection and response technologies, security teams have often found themselves unprotected due to gaps in coverage between products or they are otherwise unhappy with their choice of vendor and technology. Fundamental enterprise requirements are clear (see Figure 1):

- **Endpoint security suites must protect against modern threats.** It's no surprise that global enterprise security decision makers rate the evolving nature of IT threats as a top challenge.[2] As attackers continuously advance their methods to target gaps in traditional endpoint products, security pros look to their vendors to advance their protection capabilities. This includes the ability to block the global-scale attacks that are increasingly using techniques similar to those previously seen in targeted attacks (e.g., file-less malware and user exploitation), raising the bar substantially for security suite functional expectations.

- **They should decrease endpoint complexity.** IT environment complexity is another top challenge for global enterprise security decision makers; in fact, Forrester survey data shows that it's the most frequently cited challenging issue.[3] Complexity can come in many forms, but security teams are especially frustrated by deployment complexities that leave gaps in coverage, poorly laid out consoles that lead to challenging admin experiences, too many screens involved in day-to-day operations, and resources-draining performance issues like false positives and false negatives. Buyers want an endpoint security suite that consolidates capabilities and minimizes complexity when possible.

- **Vendors need to have strategies that inspire confidence.** More than ever, trust is critical in the endpoint security market. Buyers need to trust that their vendors will keep products up-to-date and effective against new attacks without significantly disrupting their business or exposing new vulnerabilities. Buyers also want to trust their endpoint security vendor to serve as a strategic partner in times of need, while inspiring confidence that the leadership team's vision will help prepare them for future challenges. Finally, buyers must trust that their vendors will be, without exception, good stewards of their corporate data.

FIGURE 1 A Modern Endpoint Security Suite Must Meet Three Fundamental Buyer Demands



Functional

- Automated prevention, detection, and remediation
- Full endpoint visibility
- Automation and orchestration

Efficient

- Low complexity
- Positive user experience
- High precision with a low false positive rate

Trustworthy

- Belief in vendor's strategy
- Confidence in vendor's technology
- Trust in vendor's brand

Endpoint Security Suites Evaluation Overview

To assess the state of the endpoint security suites market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of the top vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of 21 criteria, which we grouped into three 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 this evaluation include malware and exploit prevention, behavioral detection, and product performance, which Forrester validated using customer feedback and third-party test results.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. Here, we evaluated corporate vision and focus, security community involvement, and product road map.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise customer base and licensing partner presence.

Evaluated Vendors And Inclusion Criteria

Forrester included 15 vendors in the assessment: Bitdefender, Carbon Black, Check Point, Cisco, CrowdStrike, Cylance, ESET, Ivanti, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, Sophos, Symantec, and Trend Micro. Each of these vendors has (see Figure 2):

- **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 strong enterprise market presence.** We only included vendors with at least 100 enterprise customer accounts (1,000+ nodes deployed per enterprise) and at least one deployment with 100,000+ nodes.
- **A high degree of interest from enterprise buyers.** We only included vendors that garner substantial interest from enterprise security decision makers. For example, Forrester clients ask questions about each vendor by name during inquiries and other interactions.

FIGURE 2 Evaluated Vendors: Product Information And Inclusion Criteria

Vendor	Product evaluated	Version number
Bitdefender	GravityZone Endpoint Security	6.2
Carbon Black	Cb Defense	
Check Point	SandBlast Agent Complete Endpoint Protection	E80.81
Cisco	Advanced Malware Protection for Endpoints	6.0.9
CrowdStrike	CrowdStrike Falcon	4.1
Cylance	CylancePROTECT	2.0
ESET	ESET Endpoint Security	6.6
Ivanti	Ivanti Endpoint Security for Endpoint Manager	2017.3
Kaspersky Lab	Kaspersky Endpoint Security for Business (KESB)	11
Malwarebytes	Malwarebytes Endpoint Protection	1.1 (Windows); 1.5 (macOS)
McAfee	McAfee Endpoint Security	10.5.3
Microsoft	Windows Enterprise E5	E5
Sophos	Sophos Intercept X and Endpoint Protection	
Symantec	Symantec Endpoint Protection (SEP)	14.1
Trend Micro	Smart Protection Suite with Endpoint Sensor	

Vendor inclusion criteria
Integrated prevention, behavioral detection, and automatic remediation
More than 100 customers that have deployed vendor’s endpoint software to 1,000+ nodes and at least one customer with more than 100,000 nodes
An established presence in the enterprise market with continuous interest from Forrester clients

Relevant Vendors Not Included In This Evaluation

There are many notable endpoint security vendors that receive interest from Forrester clients, but we didn't include them because they didn't meet one or more of our inclusion criteria. These vendors include Barkly, Comodo Cybersecurity, Cybereason, Endgame, FireEye, Palo Alto Networks, SentinelOne, and Webroot. Each of these vendors receive positive feedback from Forrester clients and are worthy of consideration, depending on your environment and requirements.

Vendor Profiles

This evaluation of the endpoint security suites market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 3 and see Figure 4). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 3 Forrester Wave™: Endpoint Security Suites, Q2 2018

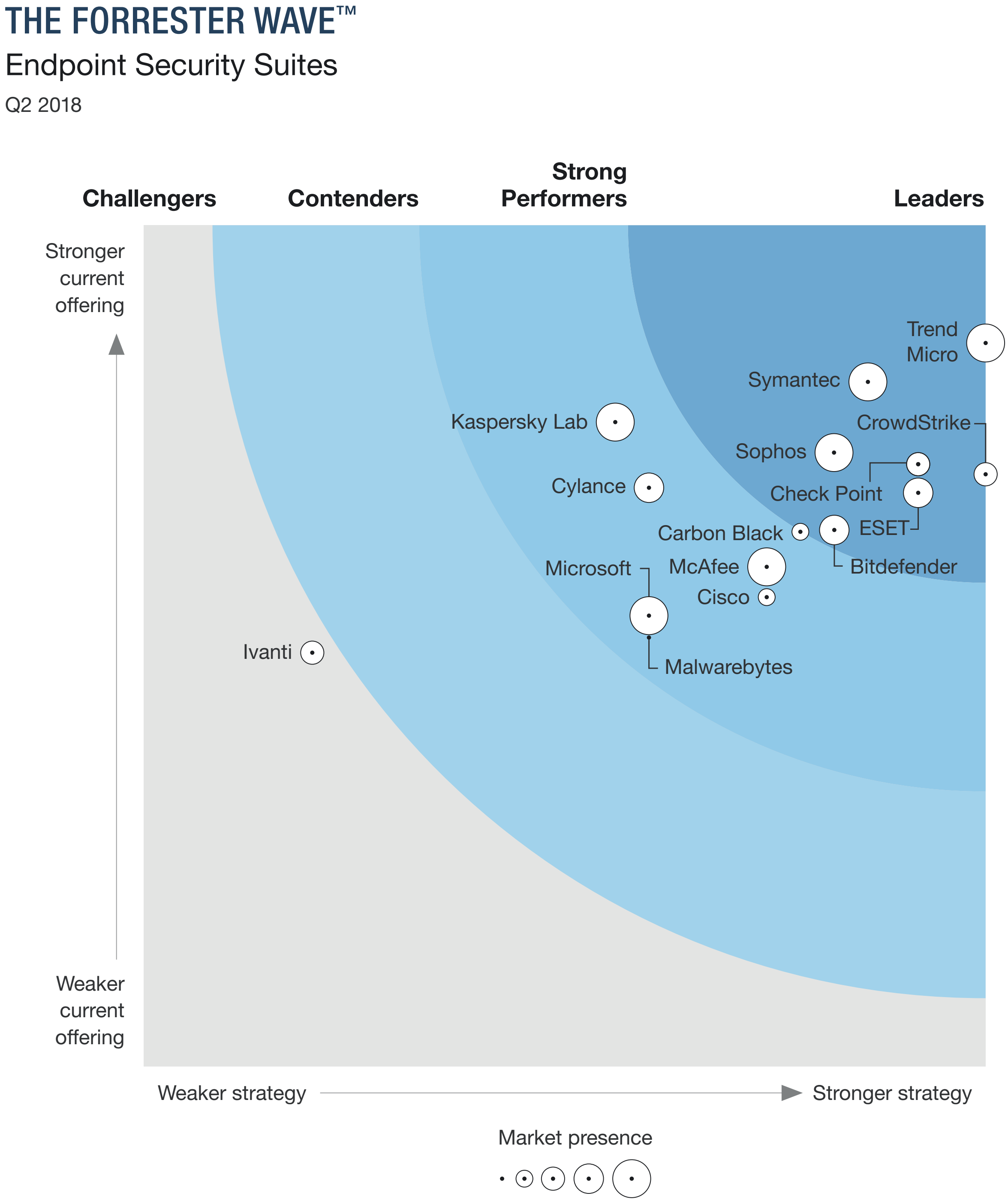


FIGURE 4 Forrester Wave™: Endpoint Security Suites Scorecard, Q2 2018

	Forrester's weighting	Bitdefender	Carbon Black	Check Point	Cisco	CrowdStrike	Cylance	ESET	Ivanti
Current Offering	50%	3.19	3.18	3.58	2.79	3.52	3.44	3.41	2.46
Threat prevention	20%	3.80	2.60	3.80	2.60	3.80	4.60	3.40	1.80
Threat detection	15%	2.00	5.00	3.00	4.00	5.00	3.00	4.00	1.00
Control	15%	2.20	3.40	3.00	1.00	1.80	3.00	2.20	5.00
Data security	8%	3.00	1.00	5.00	1.00	1.00	1.00	3.00	3.00
Mobile security	7%	3.00	1.00	5.00	3.00	3.00	1.00	3.00	3.00
Platform support	5%	5.00	3.00	3.00	5.00	5.00	3.00	5.00	5.00
Product performance	20%	4.00	3.50	2.60	3.90	4.00	4.10	4.00	1.00
External integrations	5%	3.00	5.00	5.00	1.00	5.00	5.00	3.00	1.00
Product support	5%	3.00	3.00	5.00	3.00	3.00	5.00	3.00	5.00
Strategy	50%	4.10	3.90	4.60	3.70	5.00	3.00	4.60	1.00
Product road map	20%	5.00	3.00	3.00	3.00	5.00	3.00	3.00	1.00
Security community involvement	35%	5.00	3.00	5.00	5.00	5.00	3.00	5.00	1.00
Corporate vision and focus	45%	3.00	5.00	5.00	3.00	5.00	3.00	5.00	1.00
Market Presence	0%	3.20	1.40	3.00	1.20	3.00	3.20	3.20	3.00
Enterprise customer base	90%	3.00	1.00	3.00	1.00	3.00	3.00	3.00	3.00
Licensing partner presence	10%	5.00	5.00	3.00	3.00	3.00	5.00	5.00	3.00

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

FIGURE 4 Forrester Wave™: Endpoint Security Suites Scorecard, Q2 2018 (Cont.)

	Forrester's weighting	Kaspersky Lab	Malwarebytes	McAfee	Microsoft	Sophos	Symantec	Trend Micro
Current Offering	50%	3.83	2.55	2.97	2.68	3.65	4.07	4.30
Threat prevention	20%	5.00	1.80	3.40	2.20	4.60	4.20	5.00
Threat detection	15%	4.00	4.00	2.00	3.00	2.00	4.00	3.00
Control	15%	3.40	3.40	5.00	2.20	2.20	4.20	4.20
Data security	8%	3.00	1.00	5.00	3.00	5.00	5.00	5.00
Mobile security	7%	3.00	1.00	1.00	3.00	5.00	5.00	5.00
Platform support	5%	5.00	1.00	3.00	1.00	5.00	5.00	5.00
Product performance	20%	4.10	2.40	1.60	2.30	4.50	3.00	4.10
External integrations	5%	3.00	3.00	5.00	5.00	1.00	5.00	5.00
Product support	5%	1.00	5.00	1.00	5.00	3.00	3.00	3.00
Strategy	50%	2.80	3.00	3.70	3.00	4.10	4.30	5.00
Product road map	20%	3.00	3.00	3.00	3.00	5.00	5.00	5.00
Security community involvement	35%	5.00	3.00	5.00	3.00	5.00	3.00	5.00
Corporate vision and focus	45%	1.00	3.00	3.00	3.00	3.00	5.00	5.00
Market Presence	0%	5.00	1.00	5.00	4.80	5.00	4.80	4.80
Enterprise customer base	90%	5.00	1.00	5.00	5.00	5.00	5.00	5.00
Licensing partner presence	10%	5.00	1.00	5.00	3.00	5.00	3.00	3.00

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

Leaders

- **Trend Micro continues to offer the most flexible and fully featured suite on the market.** Trend Micro maintains its position as a market leader with continuous evolution of its prevention and detection engines along with best-in-class suite capabilities. Customers give the product high marks for its malware and exploit prevention efficacy, with a low negative impact on endpoint user experience. Admins appreciate the product's high level of automation along with its flexibility and scalability to adapt to different operating environments. On the downside, Trend Micro's lack of integrated EDR (plans for this in 2H 2018) and only average customer scores for threat detection efficacy both present challenges for certain buyers. Regardless, Trend Micro is still an easy shortlist addition for most enterprise environments requiring a full endpoint security stack.

- **CrowdStrike has helped shape the mold for the modern endpoint security suite.** CrowdStrike started as an EDR vendor in 2012 but has evolved its offering into a highly automated suite, complete with threat prevention and multiple layers of automated detection and response. Compared to others in this study, CrowdStrike has superior exploit and behavioral detection capabilities, with customers reporting an above-average admin experience and easy deployments. Buyers appreciate the large ecosystem of partners and services, especially the aggressively priced OverWatch service, which provides proactive threat hunting for teams without advanced security expertise. However, some buyers will be turned off by CrowdStrike's high overall price and relatively little support for data security capabilities such as data encryption or data loss prevention. Nonetheless, Forrester expects CrowdStrike to continue showing up on the endpoint security suite shortlist among large and small enterprises for the foreseeable future.

- **Symantec's latest release shows its leadership is in touch with customer demands.** As the largest endpoint security company, Symantec often takes the brunt of the industry's backlash against ineffective antimalware. Customer feedback for Symantec had been low for years, and management turnover seemed to indicate Symantec was unwilling or unlikely to innovate in the near future. However, with the November 2016 release of SEP 14 and subsequent updates, the situation improved dramatically. Symantec delivered on its vision for a single-agent endpoint security product with consolidated signatureless malware prevention, best-of-breed detection capabilities, and automated response. These additions led to improved customer feedback on security efficacy and user experience. And while the company's customer feedback scores still reflect a nagging perception that Symantec is complex and ineffective, this will change as the company rebuilds trust and as more existing customers upgrade.

- **Check Point offers a fully featured, traditional suite with modern updates.** With its roots in network security, Check Point has expanded into other areas such as endpoint and mobile security over the years and today delivers an endpoint security suite that includes threat prevention, detection, data security, endpoint management, and mobile security. The product ships with multiple signatureless detection capabilities for malicious file/behavior, with tight integration to share policy and threat intel between the company's endpoint, network, and cloud offerings.

Unfortunately, customers reported a higher impact to endpoint user experience compared to other products in this report. Overall, for customers looking for a solid combination of new technology and traditional suite capabilities in a single console, Check Point should easily make the shortlist.

› **ESET combines threat prevention and detection with a focus on user experience.** ESET's endpoint security suite brings together multiple scanning and behavioral detection engines to deliver strong malware and exploit prevention, while preserving the endpoint user experience. The company has been focused on maintaining a low false positive rate and a light touch on the endpoint since its first enterprise product, and customers continually rate them above average in endpoint user experience. In addition to the core threat prevention and detection tools, the product also includes a handful of ancillary endpoint security tools such as native encryption management and mobile antimalware. On the downside, ESET's detection and response functionality will likely be a deterrent for teams looking for advanced response workflows. The relative basic vulnerability management capabilities may also be an issue for some buyers. Overall, ESET is best for enterprises looking for a full suite that requires low expertise for operation.

› **Sophos shows that machine learning can keep traditional suite vendors relevant.** Sophos offers a broad, tightly integrated portfolio of endpoint security tools that target smaller enterprises. When customers began to demand better protection against fileless malware and advanced attacks from their traditional endpoint security suite vendors in 2017, Sophos acquired Invincea and subsequently integrated its machine learning (ML) models into the Sophos Intercept X product, which provides exploit prevention, anti-ransomware features, and root cause analysis for incident forensics. Today, Sophos offers most of the major suite capabilities important to enterprise buyers, all managed through a cloud platform, with the exception of patch management. Customer satisfaction is very high for both the admin experience and low impact to endpoint performance. One drawback is that it currently lacks an EDR capability in the market (planned in an upcoming release). For enterprise buyers looking for a full prevention-oriented suite, Sophos is an easy shortlist addition.

› **Bitdefender offers threat prevention across a wide range of endpoint platforms.** Enterprise interest in Bitdefender has increased over the past two years as the company has expanded its reach through licensing partnerships and has focused on delivering an integrated, easy-to-use threat prevention and detection solution. One of Bitdefender's major differentiators is the reach of its sensor network. Since Bitdefender has specialized in licensing its core engine to vendors outside of the traditional endpoint security space (everything from network appliances to IoT devices), its threat research covers a broad range of attack vectors. Customers report above-average prevention capabilities and a low detriment to endpoint user experience. However, for teams looking for more advanced threat hunting and detection capabilities, Bitdefender lacks many of the analysis and response capabilities offered by market leaders. Bitdefender is well-suited for large and small environments with less need for sophisticated detection.

Strong Performers

- **Cb Defense moves Carbon Black into the broader market.** Carbon Black's Cb Defense (formerly Confer) is a cloud-based single-agent suite that provides integrated threat prevention and detection. While Cb Defense delivers above-average detection efficacy (determined through customer feedback), strong behavioral analysis, and superior endpoint visibility, it lacks some features found in established products such as patch management, data loss protection, and mobile security. Because of the sophisticated customizable rules available for detection configuration, admins also report a high level of expertise required to run the product. Overall, Cb Defense is best for security teams looking to build or augment their endpoint behavioral protection, especially those with the expertise to take advantage of the product's more advanced features.

- **McAfee is working to regain customer confidence with technical improvements.** McAfee's endpoint security products have been plagued with deployment challenges and low efficacy, but the latest version of Enterprise Security (ENS) seems to have solved these issues with a re-architected console and machine learning capabilities integrated into the local prevention engine. McAfee is hoping these technical improvements will help convince the company's large customer base to migrate to the latest version instead of opting for a replacement product. But there will be challenges; McAfee still gets low scores for admin experience and efficacy, and its products still don't support mobile devices. McAfee will likely improve customer perceptions and increase adoption of its new versions if it executes on its vision to simplify security through third-party integrations and automation.

- **Kaspersky Lab is struggling to win back customer trust despite having strong tech.** Kaspersky Lab has offered one of the most technically capable enterprise endpoint security products for years. This technical dominance continues in 2018, with the company getting above-average customer feedback for the product's malware and exploit prevention technologies, along with improvements to the suite's admin capabilities and UI. Unfortunately, this functional breadth and depth is overshadowed by a high level of distrust among US and EU buyers due to multiple government bans of Kaspersky software and perceived corporate instability. While buyers in other geographies are likely to continue to use Kaspersky products due to their technical merit, it remains to be seen whether Kaspersky's recent corporate initiatives (e.g., Global Transparency Initiative and movement of key business operations to Switzerland) will be successful at regaining customer trust in those markets where bans are in place.

- **Cisco's endpoint security offering delivers the modern essentials.** Cisco's AMP for Endpoints delivers malware and exploit prevention, behavioral detection, and automated response in a single agent on a broad number of endpoint types, with few ancillary capabilities outside of these fundamentals. Cisco relies heavily on its own threat research as well as customer-derived data from the Cisco Threat Grid and Threat Intelligence Cloud; data collected can be easily consumed by other Cisco security services/offerings (such as its managed detection and response service). While some of the product's detection capabilities are quite advanced, admins rate the product as easy to use with very positive feedback on admin experience and user experience preservation compared to the overall average. For existing customers of Cisco services or buyers with few suite requirements, AMP for Endpoints may be ideal.

- **Cylance offers superior threat prevention but falls short on detection.** When Cylance released its first product in 2012, the company proved to enterprises that prevention isn't dead; it had simply evolved to a new level using machine learning. Cylance was the first to show that machine learning technology, when trained correctly, can accurately classify files without constant model updating or signatures. Today, CylancePROTECT still stands as one of the best prevention-focused tools on the market, but customers reported that their detection efficacy is a clear weak point. Suite capabilities such as mobile security and data security are also lacking today. Forrester sees most large enterprises layering Cylance on top of detection-focused products today, but as Cylance executes on its vision to build out more suite capabilities and ML-based detection (released after the evaluation period but before publication), Forrester expects this to change.

- **Microsoft offers a serious alternative to third-party endpoint security suites.** Microsoft has slowly ramped up its focus on endpoint security over the past five years, giving Windows 10 improved efficacy against unknown malware and exploits, stronger application security, and innovative data security measures. The company also offers endpoint detection and basic response capabilities with its Advanced Threat Protection (ATP) offering, but it requires additional partner tools to cover non-Windows endpoints. Buyers complain that the various components in a full Microsoft Windows 10 security stack require multiple consoles to manage policies. However, companies that have standardized on Windows 10 and have the latest hardware and security features enabled would be hard pressed to find another vendor in this study with better exploit protection. Buyers with a more fragmented device environment or more advanced detection requirements are likely to get more value augmenting Microsoft's security features for prevention with a detection-focused suite.

- **Malwarebytes aims to move beyond its supporting role in your security stack.** Malwarebytes has only recently shown interest in the enterprise security suite space, while the company's free remediation tools have been a staple for security and IT ops admins for over a decade. With the latest version of Malwarebytes Endpoint Protection, enterprise buyers get malware and exploit prevention, detection, and best-of-breed remediation in one product. Customer feedback is very high for the product's behavioral detection and remediation capabilities, but this is countered by lower-than-average malware prevention scores as determined by Forrester analysis and customers of the product. Likely for this reason, enterprises still primarily use Malwarebytes in a supporting role side by side with other prevention-oriented security point products and suites, but this will change as the company builds more enterprise-grade functionality (e.g., more third-party integrations, modern suite functions covering data security and vulnerability management, more robust malware execution prevention, etc.) into the product. Overall, Malwarebytes is perfect for enterprises looking for a basic suite replacement or as an additional layer of protection where behavioral detection/remediation is lacking.

Challengers

- **Ivanti bridges the divide between IT ops and security.** Ivanti formed in 2017 when LANDESK and HEAT Software merged. This background gives the company a deep bench of application control, patch management, and endpoint management product capabilities, leading to a high amount of credibility with IT ops professionals compared to most endpoint security suite vendors. However, rather than continue developing its own threat prevention and detection solution, the company offers customers a range of threat prevention and detection technologies through OEM partnerships. This means that the company's security offerings aren't better or worse than many others in this study, although large enterprise security teams looking for strong app control with a low requirement for advanced threat detection or prevention capabilities beyond AV should consider Ivanti.

Supplemental Material

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by March 20, 2018.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls or surveys with at least three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

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

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2017 was fielded between May and June of 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] See the Forrester report "The State Of Endpoint Security, 2018."

[2] Source: Forrester Analytics Global Business Technographics Security Survey, 2017.

[3] Source: Forrester Analytics Global Business Technographics Security Survey, 2017.