

The Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021

October 13, 2021

Summary

In Forrester's evaluation of the emerging market for extended detection and response (XDR), we identified the 14 most significant providers in the category — Bitdefender, Cisco, CrowdStrike, Cybereason, Elastic, FireEye, Kaspersky, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Trend Micro, and VMware — and evaluated them. This report details our findings about how well each vendor scored against 10 criteria and where they stand in relation to each other. Security and risk professionals can use this report to select the right partner for their XDR needs.

- [XDR Products Are A Jumble Of Features Rooted In A Vision To Displace SIEM](#)
- [XDR Evaluation Overview](#)
- [Vendor QuickCards](#)
- [Supplemental Material](#)

XDR Products Are A Jumble Of Features Rooted In A Vision To Displace SIEM

Extended detection and response (XDR) is an early-stage market, and current vendor capabilities reflect that. XDR products have variegated feature sets based on their maturity, native portfolio, and vision for the SOC. Mature providers offer native, cross-telemetry detection and investigation, with limited response ability and no orchestration capabilities. These vendors combine the best elements of their portfolios, including industry-leading products, to simplify incident response and build targeted, high-efficacy detections. In contrast, less mature providers use XDR as a unifying layer for their portfolio, adding little value to the practitioner. Vendors in between have emerging native and hybrid XDR features but are still very early stage and mostly highlight their endpoint detection and response (EDR) capabilities. Given the diversity of capabilities, customer references were mixed. Some customers seek to outright replace their SIEM with XDR, and others use it as no more than a contextualized EDR tool. Many of the vendors with nascent capabilities have aggressive roadmaps fueled by acquisitions and a heavy focus on R&D to get them up to speed in the next year. Overall, there is a deep divide in the XDR market between those far along the path and those just starting to deliver on [the vision of XDR](#).

XDR Evaluation Overview

The Forrester New Wave™ differs from our traditional Forrester Wave™. In the Forrester New Wave evaluation, we assess only emerging technologies, and we base our analysis on a 10-criterion survey and a 2-hour briefing with each evaluated vendor. We group the 10 criteria into current offering and strategy (see Figure 1). We also review market presence.

We included 14 vendors in this assessment: Bitdefender, Cisco, CrowdStrike, Cybereason, Elastic, FireEye, Kaspersky, McAfee, Microsoft, Palo Alto Networks, SentinelOne, Sophos, Trend Micro, and VMware (see Figure 2 and see Figure 3). Each of these vendors has:

- EDR efficacy. The vendor has demonstrated confidence in the efficacy of its EDR product through participation in the MITRE ATT&CK evaluation against the tactics, techniques, and procedures elicited by APT29 and/or Carbanak+FIN7.
- Supported telemetry sources. The vendor has the ability, either natively or through a hybrid approach, to integrate non-EDR telemetry.
- Forrester mindshare. To ensure relevance to Forrester clients and the quality of the references being provided, Forrester considers the level of interest from our clients based on inquiries, advisories, consulting engagements, and other interactions.

Figure 1 Assessment Criteria: Extended Detection And Response (XDR) Providers, Q4 2021

Assessment criteria	Platform evaluation details
Visibility	How does the offering help prioritize which telemetry sources are most important? How does the offering validate the quality of the telemetry ingested, and how does it reduce costs associated with the consumption of that data pre- or post-ingestion?
Detection	What unique approach does the offering take to minimize false positives? How does the offering perform detection and correlation for various types of telemetry? What default analytics are included, how can analytics be added, and how are they tuned?
Investigation	How does the offering support analysts with triage, investigation, and collaboration? How does the offering provide criticality metrics for incidents? How does the offering facilitate investigative workflows for customers, and what data can the analyst investigate?
Response & remediation	How does the offering enable and prioritize response actions? How does the offering log response actions, and what audit log data does the offering provide for all actions? How does the offering help customers understand security posture improvements?
Product architecture	What software dependencies exist for the offering? How does the vendor handle compliance requirements? How does the vendor approach data modeling and integration? How does the offering's architecture uniquely handle native and third-party data?
Threat hunting	What search syntaxes are available? How does the offering allow hunts to become rules? How does the offering handle retrospective analysis? How does the offering correlate an in-process hunt with a new detection or incident?
Product security	Does the vendor include an SBOM for customers? How does the vendor test the security of its offering? What processes are used to ensure code is developed and updated securely? What is the vendor's vulnerability disclosure policy?
Product vision	What is the vendor's vision for the product and the business outcomes it supports? How do users of the offering provide feedback to the vendor? How does the vendor engage with the security and open source community?
Planned enhancements	What planned enhancements support the vendor's vision? How does the vendor envision client requirements changing over the next three years, and how does that affect its roadmap? How does the vendor share roadmap details with clients?
Commercial model	What policies does the vendor have for data retention? How does the vendor adjust pricing based on features? What telemetry sources are included versus being purchased as an add-on? What factors influence pricing? What is the vendor's MSRP?

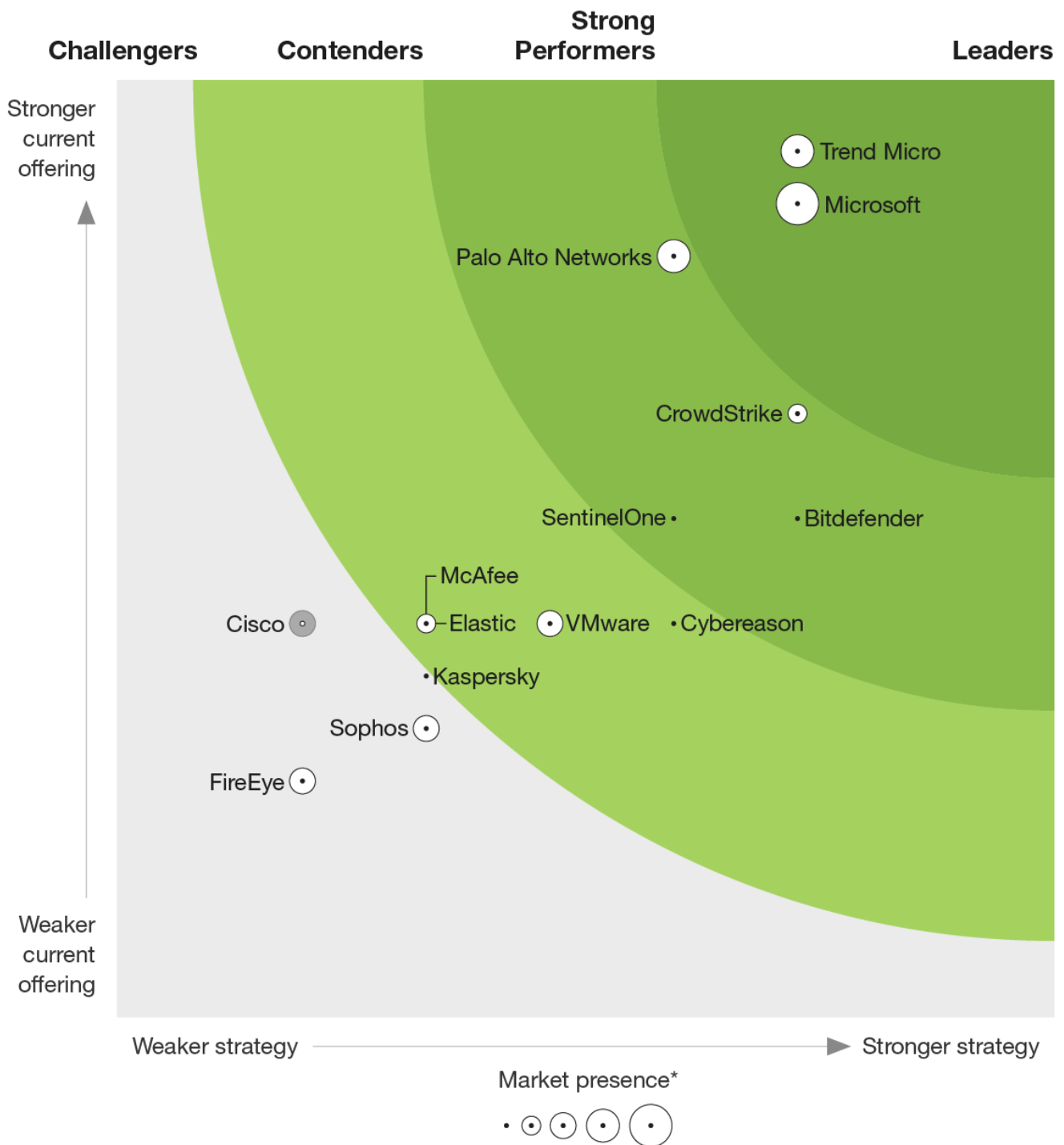
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2Forrester New Wave™: Extended Detection And Response (XDR) Providers, Q4 2021

THE FORRESTER NEW WAVE™

Extended Detection And Response (XDR) Providers

Q4 2021



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 3Forrester New Wave™: Extended Detection And Response (XDR) Providers Scorecard, Q4 2021

Company	Visibility	Detection	Investigation	Response & remediation	Product architecture	Threat hunting	Product security	Product vision	Planned enhancements	Commercial model
Trend Micro	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Microsoft	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Palo Alto Networks	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
CrowdStrike	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Bitdefender	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
SentinelOne	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Cybereason	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
VMware	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Elastic	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
McAfee	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Kaspersky	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Sophos	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
Cisco	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆
FireEye	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆	⬆

⬆ Differentiated ⬆ On par ⬆ Needs improvement ⬆ No capability

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor QuickCards

Forrester evaluated 14 vendors and ranked them against 10 criteria. Here's our take on each.

Trend Micro: Forrester's Take

Our evaluation found that Trend Micro (see Figure 4):

- Offers strong cross-telemetry detection, investigation, and response. Trend Micro's capabilities provide separate and cross-telemetry detection, investigation, and response natively for endpoint, cloud workloads, email, and network, with integrations for SIEM and Azure AD.
- Still needs to add customizability. Trend Micro lacks in two key areas: strong reporting and custom detections. These limitations prevent advanced security teams from getting full value out of the

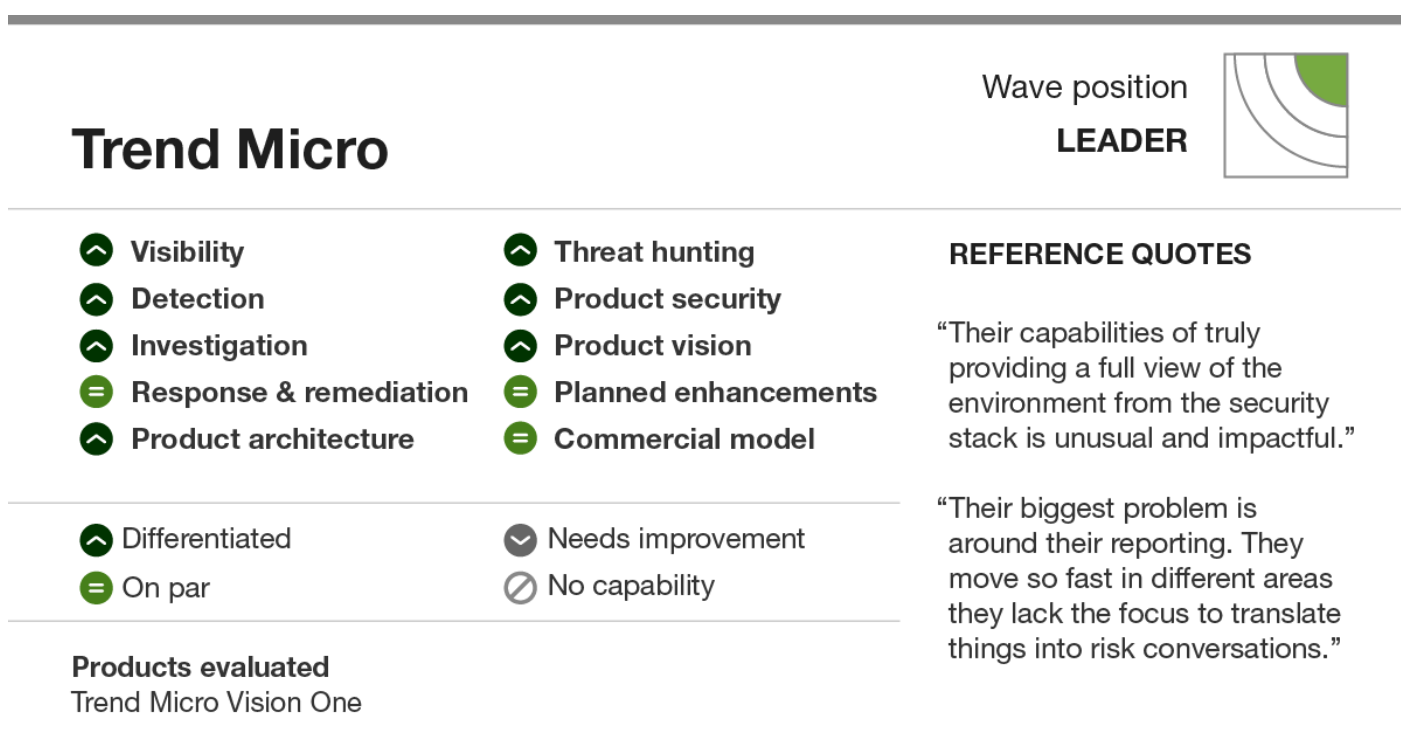
platform and from considering it as a replacement to their SIEM.

- Is the best fit for companies that need a robust, easy-to-operate security suite. Organizations that want a platform to deliver cross-telemetry integration of traditional security tools and top customer service will benefit from a relationship with Trend Micro.

Trend Micro Customer Reference Summary

Trend Micro has loyal customers confident in the security efficacy of the offering. They cite Trend Micro's roadmap transparency and above-and-beyond customer support (including support at the prospect stage) as key to its success. There is, however, customer frustration with a lack of strong reporting capabilities to communicate value.

Figure 4Trend Micro QuickCard



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Microsoft: Forrester's Take

Our evaluation found that Microsoft (see Figure 5):

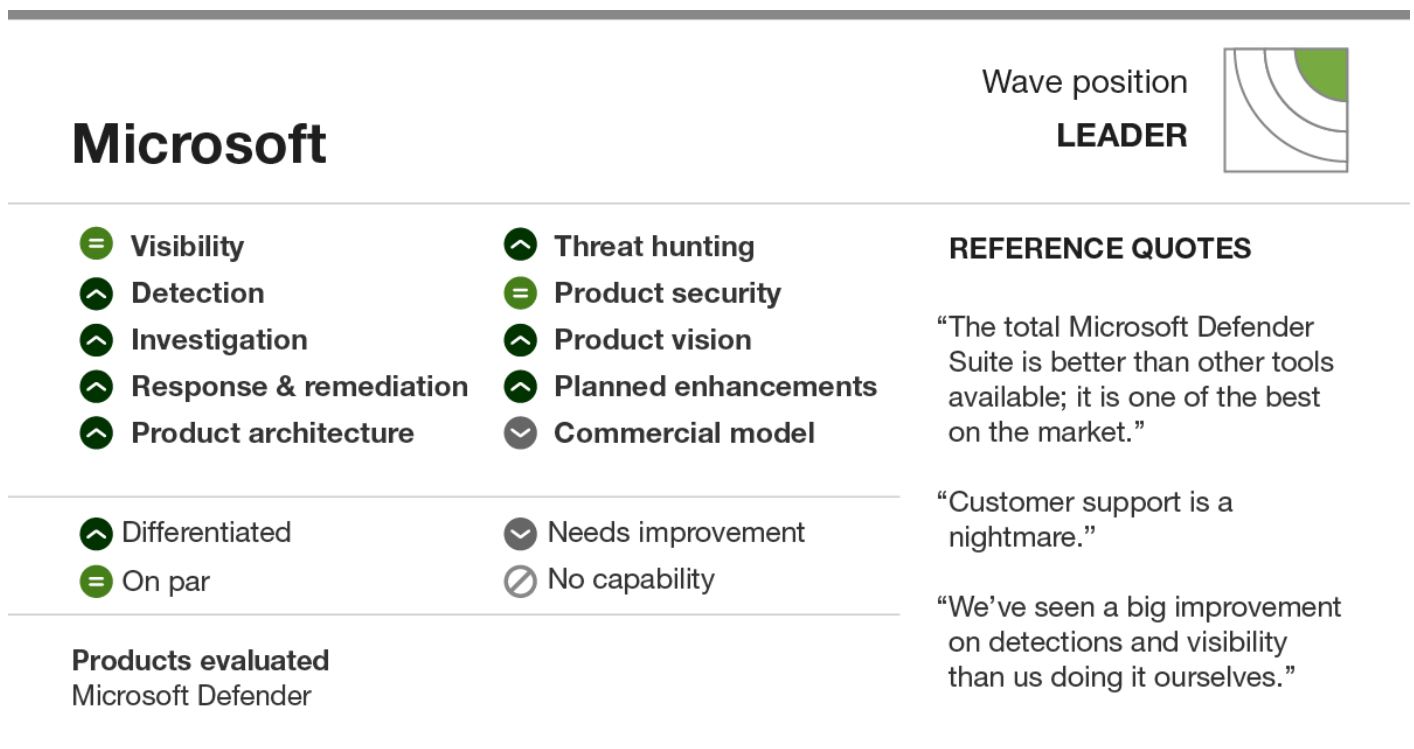
- Offers robust, native endpoint, identity, cloud, and O365 correlation. Defender provides singular and cross-telemetry detection, investigation, and response for Microsoft's native offerings in one platform. The vendor's decision to regulate inputs into XDR, specifically to rich, native telemetry, yields tailored detection, investigation, response, and mitigation capabilities.
- Still needs to make dramatic improvements to customer support. Microsoft customer support has a reputation for being and continues to be extremely difficult to work with. Like it or not, security is an industry where the community matters, and Microsoft needs to start listening.

- Is the best fit for companies moving to or already on an E5 license. The vendor's rigid licensing structure all but requires security to adopt its tech when the rest of the IT org does so. Clients get the most value by adopting the entire suite.

Microsoft Customer Reference Summary

Customer references cite the united technology stack as Microsoft's biggest strength. They especially highlight Microsoft's detection engineering quality as adding consistent, cutting-edge value. However, they continue to lament customer support and warn against using Microsoft without strong connections to the Microsoft team or a third-party partner.

Figure 5 Microsoft QuickCard



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Palo Alto Networks: Forrester's Take

Our evaluation found that Palo Alto Networks (see Figure 6):

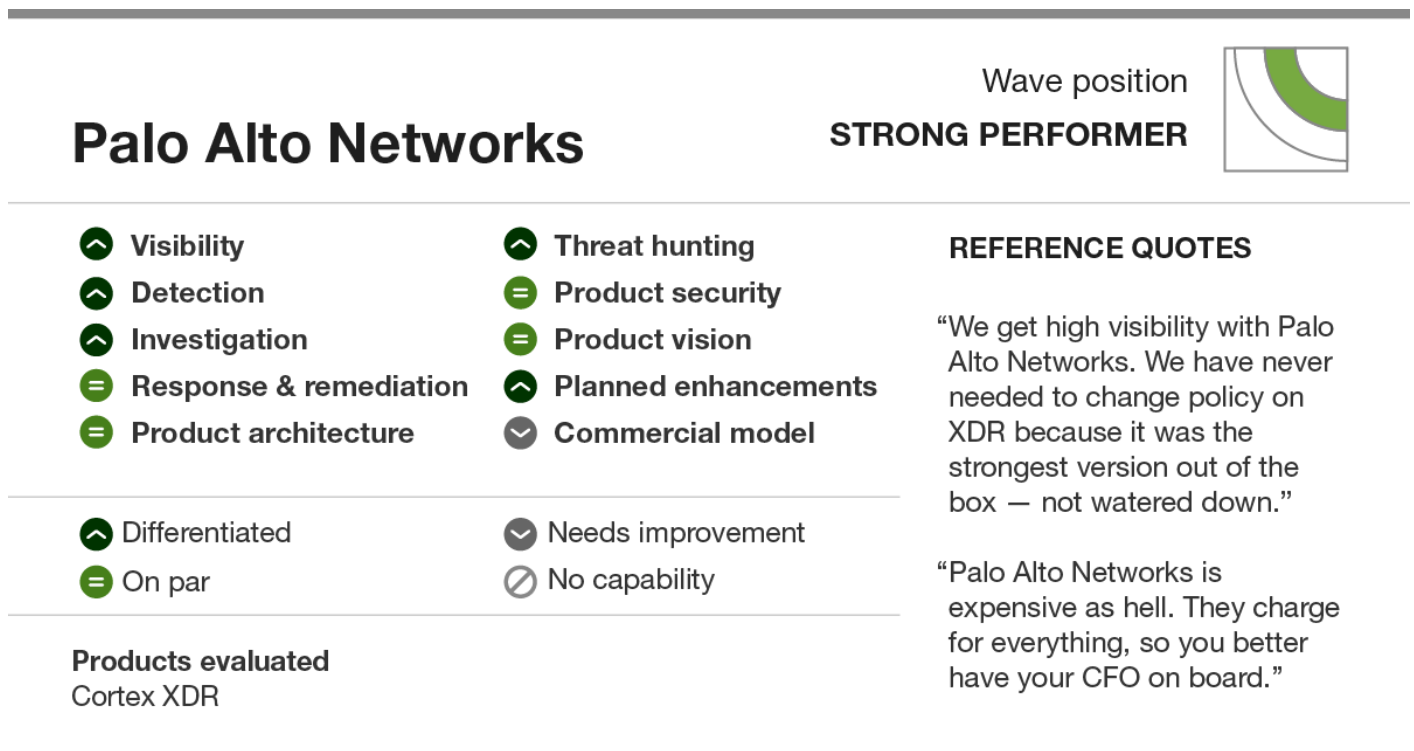
- Offers a strong combination of native endpoint, network, and cloud ingestion. Cortex XDR delivers unified detection and investigation for native endpoint, network, and cloud telemetry as well as third-party sources.
- Still needs to build response capabilities that stand on their own. Cortex XDR has built-in response for endpoint and firewall, but relies on XSOAR for response with other integrated tools and for the orchestration of all response actions. This needlessly adds another tool to the incident response process and another item in the CISO's budget. Response across integrated tools is core to XDR and should be built into the platform, not sold as an add-on.

- Is the best fit for companies that love Palo Alto's network expertise and want more. Companies that use Palo Alto's NGFW will find increased value by adding more elements of Cortex, especially the vendor's native endpoint and cloud offerings.

Palo Alto Networks Customer Reference Summary

Palo Alto Networks reference customers consider it bleeding-edge security technology. They highlight the power of the unified platform and continual improvements, while noting that updates are typically buggy and that it's an expensive product.

Figure 6 Palo Alto Networks QuickCard



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

CrowdStrike: Forrester's Take

Our evaluation found that CrowdStrike (see Figure 7):

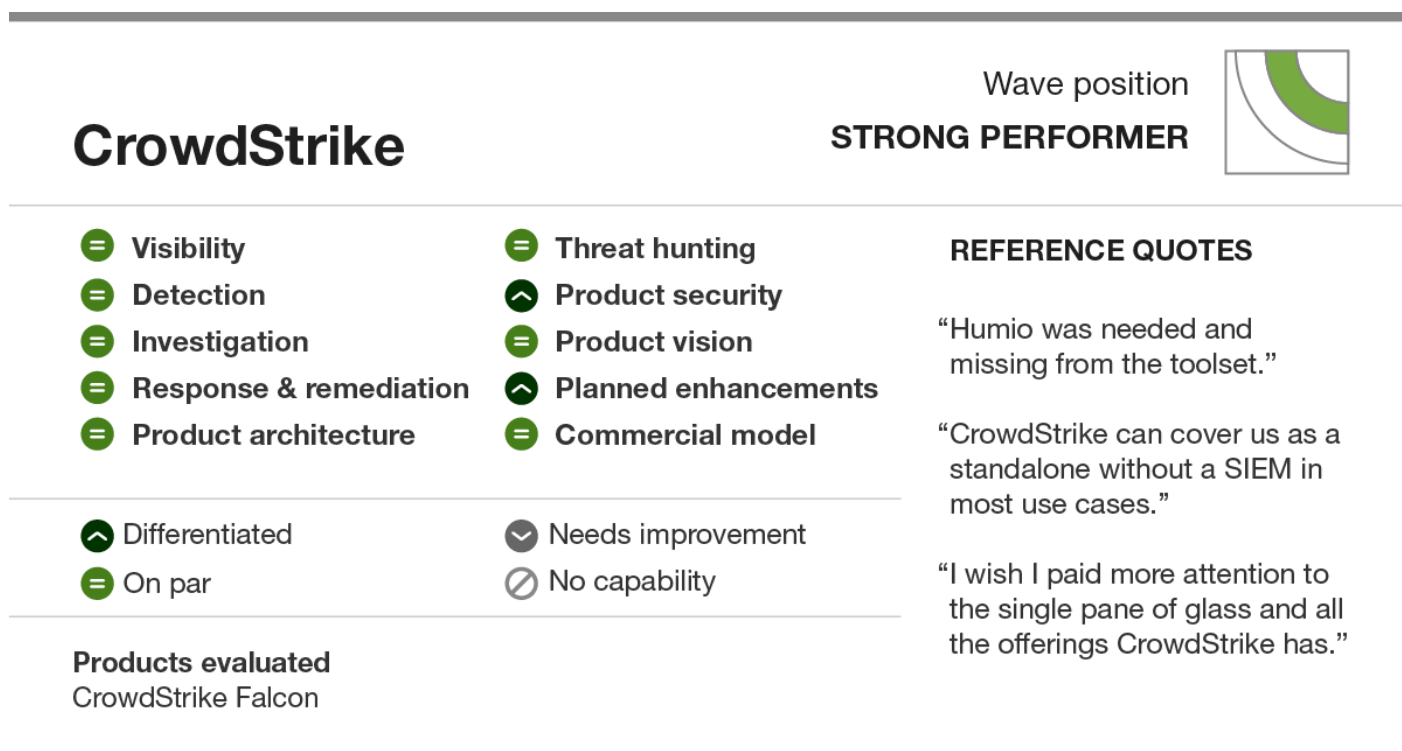
- Offers distinct capabilities with an aggressive roadmap for a fully fledged, native XDR. CrowdStrike integrated its cloud, identity, and endpoint offerings for separate detection, investigation, and response workflows in a single platform. These capabilities are strong for native telemetry detection, investigation, and response, but remain divorced from one another.
- Still needs to put all the pieces together. CrowdStrike needs to bring together its offerings for cross-telemetry detection, investigation, and response. The vendor's offering lacks correlation for its native telemetry and does not yet fully integrate Humio into the CrowdStrike platform.
- Is the best fit for companies prioritizing EDR that want to grow into XDR. CrowdStrike's EDR offering is the most compelling reason to use CrowdStrike today. But with the acquisition of Humio

and rate of integration of their identity and cloud offerings, the vendor is well-positioned to bring a more compelling and differentiated XDR offering in the next year.

CrowdStrike Customer Reference Summary

CrowdStrike has built a portfolio of products and services that customers rave about. Reference customers, however, found the vendor lacked in the ability to correlate logs and build advanced dashboards, which they hope will now be addressed with the acquisition of Humio.

Figure 7CrowdStrike QuickCard



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Bitdefender: Forrester's Take

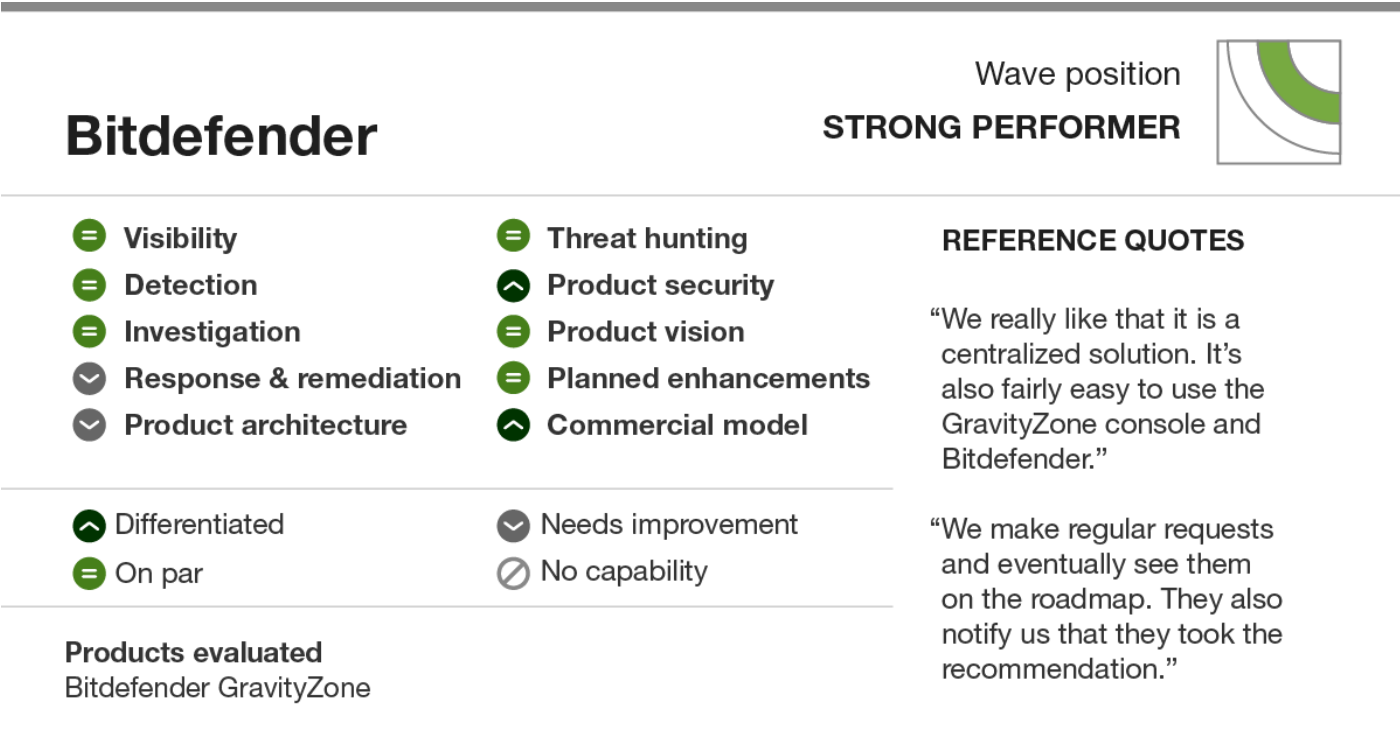
Our evaluation found that Bitdefender (see Figure 8):

- Offers endpoint and native network telemetry alongside transparent product security. Bitdefender combines endpoint and network telemetry and alerts for detection and investigation, with response capabilities for endpoint. The vendor gives customers incredible transparency and works closely with the community to improve its product security.
- Still needs to prioritize more key integrations and expand response capabilities. Bitdefender needs to strategically target important telemetry sources such as cloud while improving the depth of its native response capabilities.
- Is the best fit for companies that need a reliable and easy-to-use offering. Bitdefender brings a straightforward combination of endpoint and network telemetry but lacks other native or third-party telemetry sources and in-depth response capabilities.

Bitdefender Customer Reference Summary

Bitdefender has solid endpoint detection and response technology that customers find simple and easy to use. However, customers noted that extended capabilities remain limited.

Figure 8Bitdefender QuickCard



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

SentinelOne: Forrester's Take

Our evaluation found that SentinelOne (see Figure 9):

- Is leaning into its EDR heritage as it introduces new telemetry. SentinelOne is incrementally broadening its EDR differentiators — Storyline and Storyline Active Response — with native telemetry from Ranger and third-party telemetry from its Marketplace apps.
- Still needs to build out its cross-telemetry capabilities. XDR inputs are still limited to native sources and are not comprehensive for cross-telemetry detection, investigation, and response. The Scalyr acquisition will provide much-needed log management capabilities and scalability for the SentinelOne offering but has yet to be fully integrated.
- Is the best fit for companies that want customizability and to grow into XDR. Organizations focused on custom detection, investigation, and response workflows in EDR will get immediate value from SentinelOne with the ability to grow into XDR as SentinelOne executes on its roadmap.

SentinelOne Customer Reference Summary

SentinelOne’s reference customers say it has an edge over the competition when it comes to the quality of behavioral detections. However, they share concerns over enterprise readiness given some performance and scalability issues, which customers hope will be assuaged with the Scalyr acquisition.

Figure 9SentinelOne QuickCard

SentinelOne

Wave position
STRONG PERFORMER



- | | |
|--------------------------|------------------------|
| ⊞ Visibility | ⊞ Threat hunting |
| ⊞ Detection | ⊟ Product security |
| ⊞ Investigation | ⬆ Product vision |
| ⊞ Response & remediation | ⊟ Planned enhancements |
| ⊞ Product architecture | ⊞ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ⊟ Needs improvement |
| ⊞ On par | ⊟ No capability |

Products evaluated
Singularity Complete

REFERENCE QUOTES

“For SentinelOne, we use everything for endpoint. All SentinelOne data gets piped into Splunk and then we correlate that against WAFs and firewalls.”

“There have been some issues with performance, problems with RAM consumption.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Cybereason: Forrester's Take

Our evaluation found that Cybereason (see Figure 10):

- Offers early-stage, services-led extended capabilities. Cybereason's Hybrid XDR relies on services to deliver integrations with select partners, including Google Workspace, O365, Okta, and Fortinet. The vendor also recently acquired Empow to enhance its XDR offering, though it has yet to be integrated into the platform.
- Still needs to build an XDR product to stand on its own. The vendor's XDR product capabilities are available to design partners and EDR customers with services. MDR providers have been [offering XDR capabilities for a year now](#), some longer. In order to stay competitive, Cybereason must execute on the product side.
- Is the best fit for companies that want to be design partners for Hybrid XDR. Companies that want EDR and are technologists at heart with interest in giving input into the design of a Hybrid XDR offering will find a potential partner in Cybereason.

Cybereason Customer Reference Summary

Cybereason won over customers with its product vision and the concept of the MalOp, but there is hesitation on whether Cybereason can execute. Customer support is spotty by region, and standalone product features without the support of services can be delayed in the roadmap.

Figure 10Cybereason QuickCard

Cybereason

Wave position
CONTENDER



- | | |
|--------------------------|------------------------|
| ▼ Visibility | ⊞ Threat hunting |
| ▼ Detection | ▼ Product security |
| ⊞ Investigation | ⊞ Product vision |
| ⊞ Response & remediation | ⊞ Planned enhancements |
| ⊞ Product architecture | ⊞ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ▼ Needs improvement |
| ⊞ On par | ⊘ No capability |

Products evaluated
Cybereason XDR Platform

REFERENCE QUOTES

"We looked at several cloud SIEMs, but they seemed too old-fashioned."

"Execution is where others may be better, but I see the most potential in them."

"If you are a regular customer, support is OK."

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

VMware: Forrester's Take

Our evaluation found that VMware (see Figure 11):

- Offers an extensive partner network and a vision for XDR. VMware has continued to sustain a strong partner network and a highly technical EDR tool. The vendor's XDR capabilities, however, are limited to endpoint and cloud workload telemetry.
- Still needs to build in native telemetry capabilities. VMware has limited native telemetry capabilities for detection, investigation, and response beyond the ingestion of cloud workload telemetry. The vendor needs to build additional native integrations for the entirety of the incident response lifecycle to be competitive in the XDR market.
- Is the best fit for companies that want to outsource XDR. Carbon Black is an EDR to the core and is not ready for mainstream XDR product adoption. Organizations should consider VMware if they want to outsource to a service provider that can deliver managed XDR as a service based on VMware's product stack.

VMware Customer Reference Summary

VMware reference customers have bought in on the VMware vision and broad ecosystem but have yet to see the outcomes support it.

Figure 11 VMware QuickCard



- | | |
|--------------------------|------------------------|
| ▼ Visibility | ⊞ Threat hunting |
| ⊞ Detection | ⊞ Product security |
| ▼ Investigation | ⊞ Product vision |
| ⊞ Response & remediation | ▼ Planned enhancements |
| ▼ Product architecture | ⊞ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ▼ Needs improvement |
| ⊞ On par | ⊘ No capability |

Products evaluated

VMware Carbon Black Cloud

REFERENCE QUOTES

“We became an early adopter of VMware with the vision to replace SIEM.”

“We use VMware for endpoints but don’t have the ability to integrate other telemetry yet.”

“Carbon Black is a technical solution where you need an MSSP.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Elastic: Forrester's Take

Our evaluation found that Elastic (see Figure 12):

- Offers strong customizable SIEM and open source capabilities. Elastic is a free and open SIEM that gives security teams the freedom and flexibility to deploy and fully customize the offering as they see fit. Customizable detection engineering with Elastic is a core strength for its simplicity.
- Still needs to reconcile its vision and its offering. One of the reasons end users choose XDR over SIEM is because it provides deep security expertise in detection engineering that most teams cannot afford to hire. This is at odds with the value Elastic provides in flexibility, free use, and customization, which may be part of the reason the Endgame integration has taken so long.
- Is the best fit for companies that need a SIEM with flexibility and customizability. The Elastic stack is infinitely adaptable, which best serves security teams that want complete control over detection engineering, deployment, and inputs. Elastic will not best serve those looking for a complete XDR offering.

Elastic Customer Reference Summary

Elastic is easy to get started with thanks to its free and open approach. Customers praise its flexibility and ease of use but struggle with the limited integration between Endgame and Elastic.

Figure 12Elastic QuickCard

Elastic

Wave position
CONTENDER



- | | |
|--------------------------|------------------------|
| ▼ Visibility | ≡ Threat hunting |
| ▼ Detection | ≡ Product security |
| ≡ Investigation | ≡ Product vision |
| ▼ Response & remediation | ▼ Planned enhancements |
| ≡ Product architecture | ▼ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ▼ Needs improvement |
| ≡ On par | ⊘ No capability |

Products evaluated
Elastic Security

REFERENCE QUOTES

“The integration with Endgame is still immature.”

“We saw the value of Elastic right away and eventually had more data in Elastic than our previous SIEM.”

“There is no functionality to do response in Elastic, but we also can’t make decisions without it.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

McAfee: Forrester's Take

Our evaluation found that McAfee (see Figure 13):

- Offers a unifying security analytics layer for its portfolio. MVISION XDR ingests telemetry natively from McAfee EDR, ePO, Web, CASB, and SIEM. Detections are enriched with native telemetry, arguably to the point of having too much information to sift through. Response recommendations are available for endpoint only.
- Still needs to improve product reliability and expand investigation and response. Security tools that serve as the center of the SOC need to be reliable. McAfee needs to improve the reliability of the features it releases before building out more robust response capabilities.
- Is the best fit for companies that have MVISION Complete and want a free upgrade. MVISION XDR is enabled for free to MVISION Complete customers for the time being, which makes it an easy way for EDR customers to experiment with their XDR offering.

McAfee Customer Reference Summary

McAfee customers tend to use MVISION as an aggregator to bring their McAfee products into one domain. They highlight that it’s a low-cost offering but also stated that some features on the product simply don’t work and that communication with support is challenging.

Figure 13 McAfee QuickCard

McAfee

Wave position
CONTENDER



- | | |
|--------------------------|------------------------|
| ⊞ Visibility | ⌵ Threat hunting |
| ⊞ Detection | ⊞ Product security |
| ⌵ Investigation | ⌵ Product vision |
| ⌵ Response & remediation | ⌵ Planned enhancements |
| ⊞ Product architecture | ⊞ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ⌵ Needs improvement |
| ⊞ On par | ⊘ No capability |

Products evaluated
MVISION XDR

REFERENCE QUOTES

“Some features don’t work; response can be slow.”

“It’s unclear when updates will happen because of the disconnect between local support and HQ.”

“Visibility is covered for endpoint, network, and logs — and cost is a plus.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Kaspersky: Forrester's Take

Our evaluation found that Kaspersky (see Figure 14):

- Offers the ability to aggregate alerts from endpoint and email in one place. Kaspersky is able to consolidate the view of alerts into one place for email and endpoint detection and response. However, detections are not correlated for alike-telemetry or otherwise, nor are alerts enriched with telemetry from other sources.
- Still needs to tie the pieces together and integrate more telemetry sources. Kaspersky can present alerts from email and endpoint telemetry sources in one place but puts the burden on the analyst to identify the link between detections and perform manual investigation and response. The vendor needs to take the next step and integrate these pieces together to deliver automated correlation.
- Is the best fit for companies with a heavy EMEA presence. Although the vendor operates globally, wider market adoption in the United States remains a significant challenge due to [a negative reputation](#). Organizations that are based in Russia or Europe will find that Kaspersky has a strong local presence.

Kaspersky Customer Reference Summary

Kaspersky customers highlight the product is a low-cost EDR offering. However, they also mentioned reliability issues and a limited feature set.

Figure 14Kaspersky QuickCard

Kaspersky

Wave position
CHALLENGER



- | | |
|--------------------------|------------------------|
| ⊞ Visibility | ⊞ Threat hunting |
| ⊟ Detection | ⊟ Product security |
| ⊟ Investigation | ⊟ Product vision |
| ⊟ Response & remediation | ⊟ Planned enhancements |
| ⊞ Product architecture | ⊞ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ⊟ Needs improvement |
| ⊞ On par | ⊟ No capability |

Products evaluated

Kaspersky Anti Targeted Attack Platform

REFERENCE QUOTES

"We have regular issues with updating — we don't know what will happen when we update, and sometimes lose data."

"We gather endpoint data with Kaspersky, no other telemetry."

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Sophos: Forrester's Take

Our evaluation found that Sophos (see Figure 15):

- Offers a consolidation of its tech stack for querying. Sophos integrates native endpoint, NGFW, and email telemetry into its offering for querying through Live Discover. The products are available in one platform, but there are no cross-product detection, investigation, and response capabilities.
- Still needs to align the product to what practitioners want. Sophos gives practitioners access to a lot of data, but practitioners already have that with their SIEM. Sophos needs to focus on delivering high-efficacy detections and enabling faster investigation and response.
- Is the best fit for companies that need a single integrated console for data access. Security teams that currently use Sophos products will find that Threat Center offers a unified querying interface for customizable scheduled queries.

Sophos Customer Reference Summary

Sophos can gather telemetry from a variety of sources and aggregate it in one place but struggles to bring forth the most critical and important information in a timely manner. Customers find Sophos is falling behind competitors.

Figure 15Sophos QuickCard

Sophos

Wave position
CHALLENGER



- | | |
|--------------------------|------------------------|
| ⊞ Visibility | ⌵ Threat hunting |
| ⌵ Detection | ⊞ Product security |
| ⌵ Investigation | ⌵ Product vision |
| ⌵ Response & remediation | ⊞ Planned enhancements |
| ⌵ Product architecture | ⌵ Commercial model |

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ⌵ Needs improvement |
| ⊞ On par | ⊘ No capability |

Products evaluated
Sophos XDR

REFERENCE QUOTES

“We only use Sophos for servers and endpoints. We expect there will be some crossover at some point where we can get third-party products in there.”

“Sophos were ahead of the game at the time we first deployed, though other products have since caught up.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Cisco: Forrester's Take

Our evaluation found that Cisco (see Figure 16):

- Offers SOAR capabilities and a better user experience than Cisco point products. SecureX makes accessing Cisco and third-party products from one place easier with big improvements to its UI. The offering also enables orchestration of response across products.
- Still needs to expand beyond orchestration of response. While all integrated Cisco security tools are accessible through SecureX, they are not unified. SecureX lacks cross-telemetry detection and investigation capabilities and serves more as SOAR than XDR.
- Is the best fit for companies that are already invested in Cisco security software. SecureX is a free addition to Cisco security software, providing a unified layer and better experience to access Cisco products. This is a straightforward addition for customers already invested in Cisco that brings them a step closer to tool unification.

Cisco Customer Reference Summary

Cisco did not participate in this evaluation and chose not to provide references.

Figure 16Cisco QuickCard



- | | |
|--------------------------|------------------------|
| ⊞ Visibility | ⊟ Threat hunting |
| ⊞ Detection | ⊞ Product security |
| ⊟ Investigation | ⊟ Product vision |
| ⊞ Response & remediation | ⊟ Planned enhancements |
| ⊟ Product architecture | ⊟ Commercial model |

REFERENCE QUOTES

Cisco did not participate in this evaluation, and Forrester was unable to obtain references.

- | | |
|------------------|---------------------|
| ⬆ Differentiated | ⊟ Needs improvement |
| ⊞ On par | ⊘ No capability |

Products evaluated

Cisco SecureX

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

FireEye: Forrester's Take

Our evaluation found that FireEye (see Figure 17):

- Offers a SIEM with a new name. This evaluation began prior to the announcement of the FireEye and Mandiant split when FireEye was positioning [Mandiant Advantage as its XDR offering](#). Following the split, the vendor opted to rebrand Helix as XDR (publicly [announced on Aug 16, 2021](#)) and demo that offering for this evaluation. The vendor's XDR offering is, for all intents and purposes, the exact same as its Security Analytics Platform offering.
- Still needs to focus its R&D efforts before time runs out. Following the split, FireEye has limited time before customer contracts expire to improve native integrations and investigative workflows for faster and more complete incident response.
- Is the best fit for companies invested in FireEye that want Mandiant intel ... for now. FireEye and Mandiant have a three-year agreement in place that gives FireEye Helix customers access to Mandiant Advantage Threat Intel. Customers already using FireEye tech will find this integration advantageous for the time being.

FireEye Customer Reference Summary

FireEye lost customer confidence following a lack of innovation over the past several years. Customer references were heavily invested in FireEye because of its connection to Mandiant, and laud Mandiant's services as the best part of Helix, leading current customers to revisit their FireEye contract end date.

Figure 17 FireEye QuickCard

FireEye

Wave position
CHALLENGER



- | | |
|--------------------------|------------------------|
| ▼ Visibility | ▼ Threat hunting |
| ▼ Detection | ■ Product security |
| ▼ Investigation | ▼ Product vision |
| ▼ Response & remediation | ▼ Planned enhancements |
| ▼ Product architecture | ▼ Commercial model |

- | | |
|------------------|---------------------|
| ▲ Differentiated | ▼ Needs improvement |
| ■ On par | ⊘ No capability |

Products evaluated
FireEye XDR

REFERENCE QUOTES

“Their tech isn’t that novel anymore. It’s the intel provided by Mandiant that make it a key differentiator and what made their tech so special.”

“FireEye is fine for base-level stuff. The sales team and implementation engineers are rockstars that go the extra mile.”

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Supplemental Material

The Forrester New Wave Methodology

We conducted primary research to develop a list of vendors that met our criteria for the evaluation and definition of this emerging market. We evaluated vendors against 10 criteria, seven of which we based on product functionality and three of which we based on strategy. We also reviewed market presence. We invited the top emerging vendors in this space to participate in an RFP-style demonstration and interviewed customer references. We then ranked the vendors along each of the criteria. We used a summation of the strategy scores to determine placement on the x-axis, a summation of the current offering scores to determine placement on the y-axis, and the market presence score to determine marker size. We designated the top-scoring vendors as Leaders.

Integrity Policy

We conduct all our research, including Forrester New Wave evaluations, in accordance with the [Integrity Policy](#) posted on our website.

About Forrester Reprints

<https://go.forrester.com/research/reprints/>

© 2023, [Forrester Research, Inc. and/or its subsidiaries](#). All rights reserved.

This website uses [cookies](#) to deliver functionality and customize your experience. By using this website, you are agreeing to our use of cookies. View our [cookie policy](#) for more details.

[Accept cookies](#)

