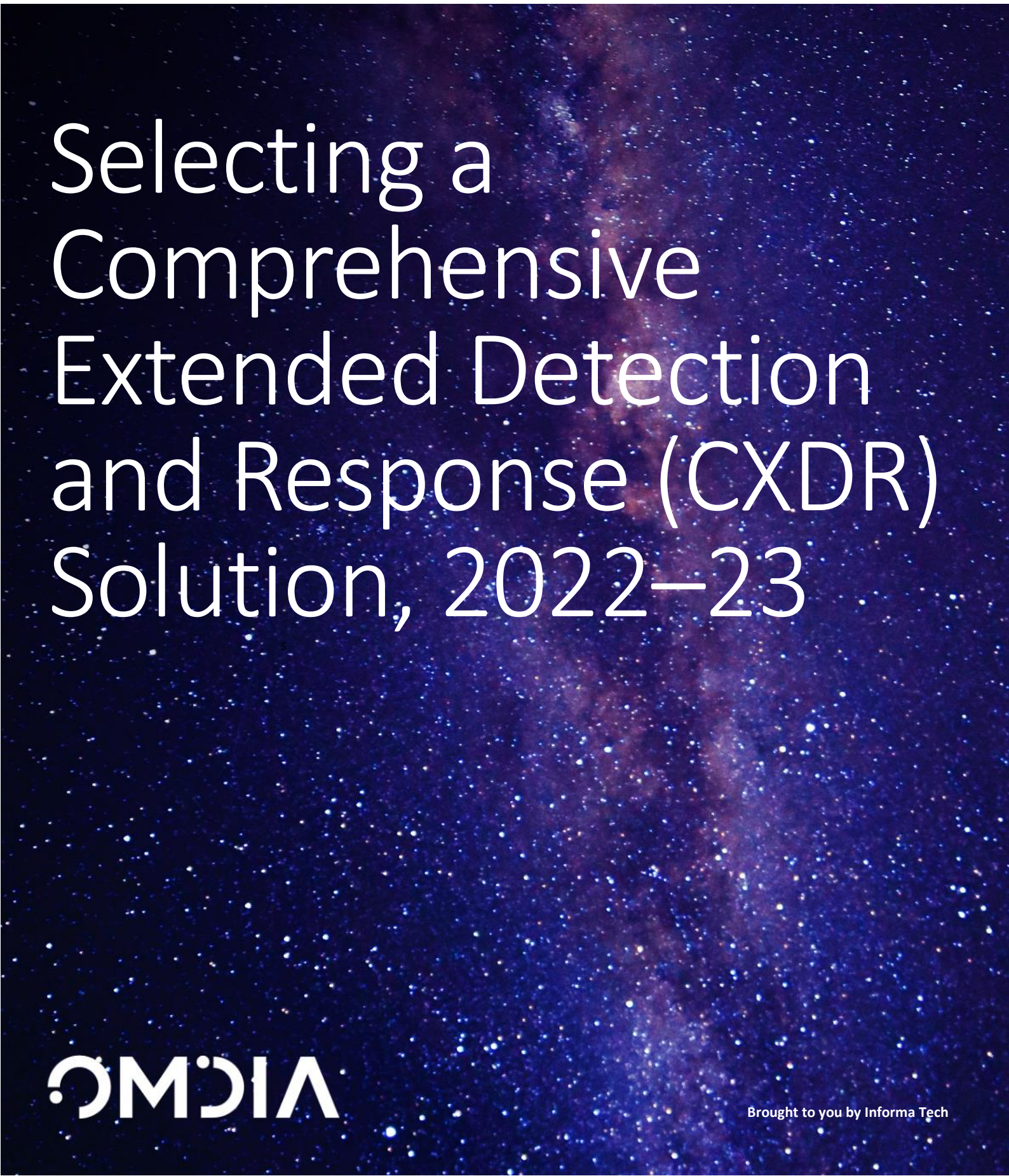
OMDIA
UNIVERSE

Publication date
30 Nov 2022
Authors
Eric Parizo
Managing Principal Analyst
Andrew Braunberg
Principal Analyst

Selecting a Comprehensive Extended Detection and Response (CXDR) Solution, 2022–23



OMDIA

Brought to you by Informa Tech

Summary

Catalyst

The enterprise threat detection, investigation, and response (TDIR) lifecycle is critical to every organization. Cyberattacks are many, varied, and growing in volume all the time and even the best preventative cybersecurity solutions can only do so much. Hence having a solution set to conduct TDIR—and all the related processes involved with finding, studying, and fixing cyberattacks—quickly, easily, and affordably is essential.

However, TDIR has always been plagued with problems. Gathering threat detection data from a variety of siloed IT and security systems, putting it together, and identifying true threats remains an ongoing challenge. Threat investigations often require a variety of tools, again mostly siloed, and highly skilled threat analysts to use them. Furthermore, determining how best to respond to threats, ideally doing so in an orchestrated, automated manner has been haphazard at best.

Longstanding TDIR solutions—including vulnerability management, security information and event management (SIEM), and security orchestration and automated response (SOAR) among others—were often too expensive, too hard to deploy, configure, and manage and often too inconsistent in their ability to meet key enterprise threat detection and response requirements including in support of broader cybersecurity resiliency efforts.

The industry needed a new approach. Enter extended detection and response, or XDR.

Omdia defines XDR as an enterprise-grade, unified TDIR solution that offers a guided human-analyst experience across the entire lifecycle from telemetry gathering and analysis to alerting and investigation, and to remediation–response, validation, and process improvement. XDR breaks down the siloed approach with a single, unified system to manage the entire TDIR lifecycle, including key activities across essential IT estate regions including endpoints, networks, and cloud environments.

First researched in 2018 by Omdia Senior Principal Analyst Rik Turner, XDR, according to Omdia's most-recent market forecast, is likely to become the largest single market segment by revenue in enterprise cybersecurity operations (SecOps) by the end of the decade.

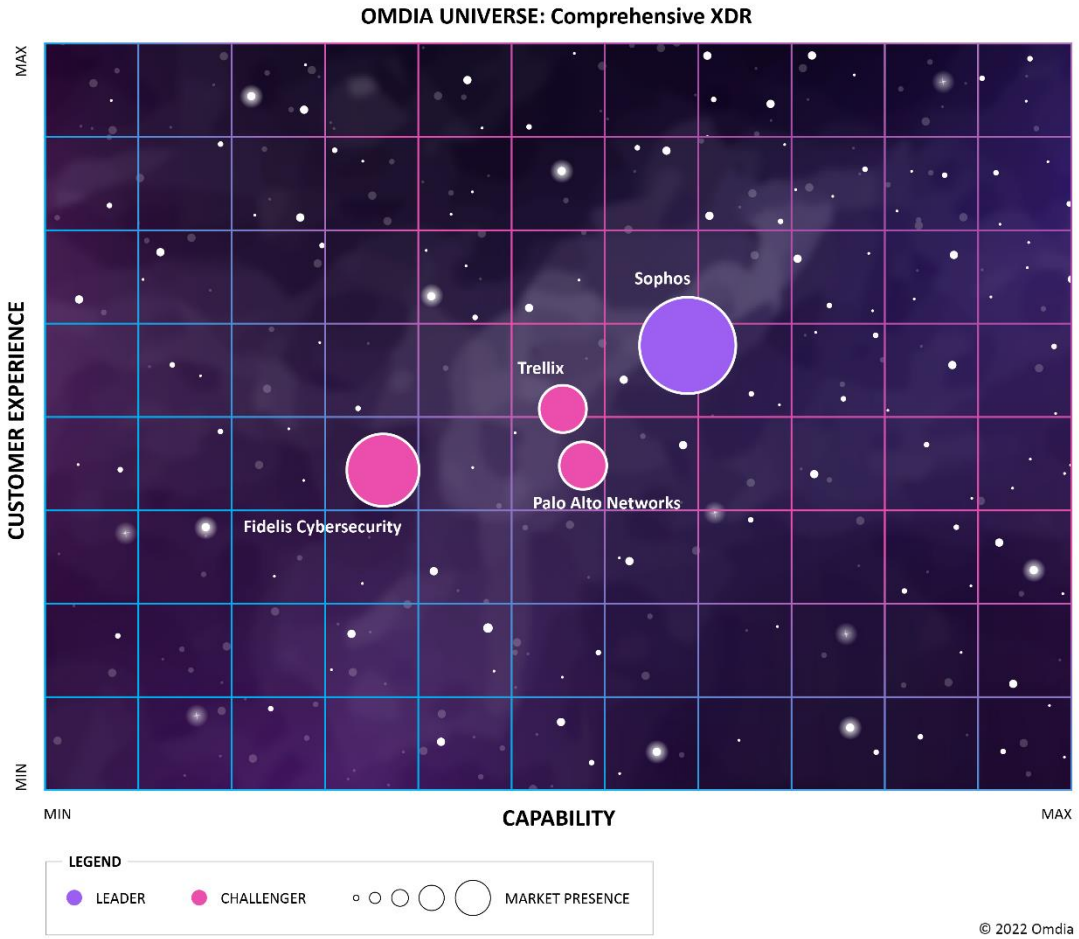
As a single solution or unified solution architecture, XDR has the potential to revolutionize enterprise TDIR, making it faster, easier, and potentially even cheaper to find, analyze, and fix cybersecurity threats. XDR is the game-changer enterprises have long needed to even the play field against adversaries.

Omdia view

Despite its promise, XDR isn't quite as easy as it sounds. A key reason why is that in most cases XDR is not a single solution. It has two flavors: comprehensive XDR and open XDR. Open XDR is a best-of-

breed approach in which point solutions with strong integration and interoperability are brought together to form a single XDR architecture. Alternatively, comprehensive XDR (CXDR) is the all-in-one single-vendor platform, covering—at a minimum—endpoints, networks, and cloud environments.

Figure 1: The Omdia Universe for comprehensive extended detection and response (CXDR)



Source: Omdia

While open XDR is useful in a variety of contexts, Omdia believes the game-changing potential of XDR lies largely with comprehensive XDR. These solutions manage the TDIR lifecycle from start to finish, ensuring that threat detection data is unified across endpoints, networks, cloud environments and beyond; that critical insights and context aren't lost as investigations move across multiple toolsets; and that the same solution that provides the data and detects the threat actually conducts the remediation–response action, making sure the resolution effort is successful, and lessons learned are cycled back in to improve the process.

In this report, Omdia offers the industry's first detailed head-to-head CXDR product analysis. While the market is undoubtedly young and the maturity of even essential features remains somewhat uneven, Omdia is cemented in its belief that XDR, and CXDR in particular, is the cybersecurity industry's best hope so far to empower enterprises with the technology and tactics they need to keep pace with the broad and evolving scope of adversaries they face.

Key messages

- Omdia found that each solution offers a unique set of strengths: one solution excels with data collection, another with threat detection. While overall solutions in this segment are nascent, and a dramatic maturation of capabilities is expected during the next 12 months, Omdia is confident that enterprise buyers can find value today based on their own criteria, with any of the solutions included in this review.

- By a considerable margin, **Sophos** Central Intercept X Advanced with XDR earned its place not only as the top-ranked product in this *Omdia Universe* but also as the sole leader. The solution was on par with competitors in Threat Investigation features, but it led or was close to leading in every other capability category. It delivered a dominant showing in Threat Response and Resolution, an area in which other solutions were underwhelming.

- The Omdia Universe graphic above does not truly capture just how close **Palo Alto Networks** and **Trellix**, both ranked as Challengers, were in Omdia's scoring, separated in total capability score by just 1%. Palo Alto Networks received top marks for its threat detection capabilities, while Trellix earned superior scores in data collection and threat investigation.

- Despite some separation in scoring, Omdia chose to also rank **Fidelis Cybersecurity** as a Challenger, not a Prospect, due to the way in which its solution stands out as arguably the industry's premier network-centric XDR offering as well as a maturity of features in important areas such as network session reconstruction and investigation workspace.

- The most consistently mature capability area across all the solutions evaluated was Data Collection. Omdia observed strong ability to take in a variety of data from endpoints, networks, and clouds, customize which types of data is collected, commonly conduct additional source queries for richer data on-demand, and even supplement with additional posture-related information in some cases.

- However, Omdia was generally disappointed with the lack of progress participants have made on remediation–response. Automation, in particular, has much maturing to do, as CXDR solutions offer varying levels of integrated orchestration (integrations of standalone SOAR solutions were not in the scope of this evaluation). Additionally, efficacy validation was inconsistent, "learning" or cycling results back into the system to improve future outcomes was broadly lacking, and innovation was minimal. Omdia sees this as a clear area of opportunity for CXDR vendors looking to differentiate.

- Finally, vendors must do better on simplifying their pricing and licensing schemes. The number of unique SKUs involved and complexity of scaled pricing models makes the business and financial aspects of acquiring a CXDR solution simply too challenging.

Analyzing the CXDR Omdia Universe

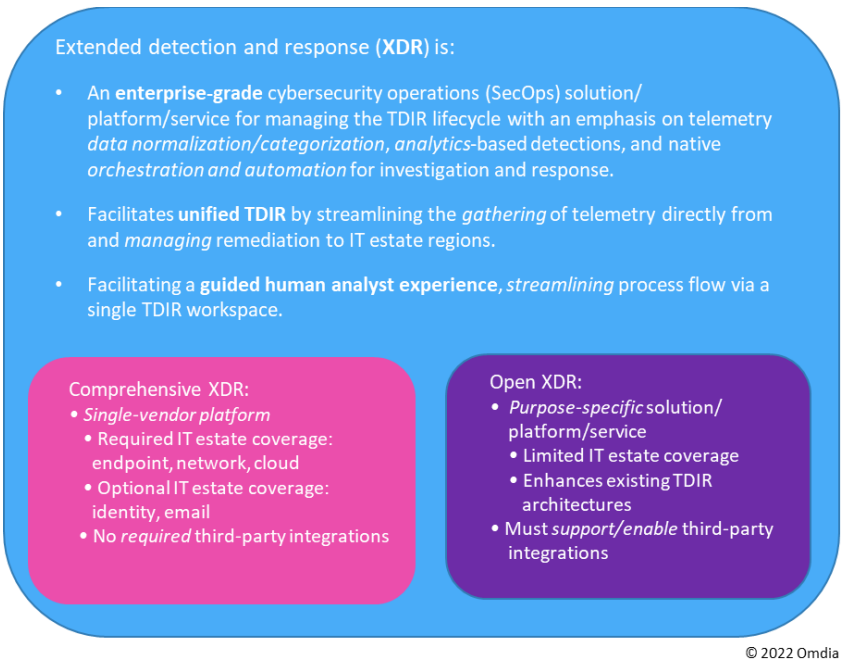
How to use this report

The *Omdia Universe* report is not intended to advocate an individual vendor but rather to guide and inform the selection process to ensure all relevant options are considered and evaluated in an efficient manner. The report findings gravitate towards the customer's perspective and likely requirements—characteristically those of a medium–large multinational enterprise (5,000+ employees). Typically, deployments are considered across the financial services, TMT (technology, media, and telecoms) and government sectors, on a global basis.

Market definition

In an effort to drive the market toward a consensus, Omdia defined XDR as follows:

Figure 2: Omdia's definition of XDR

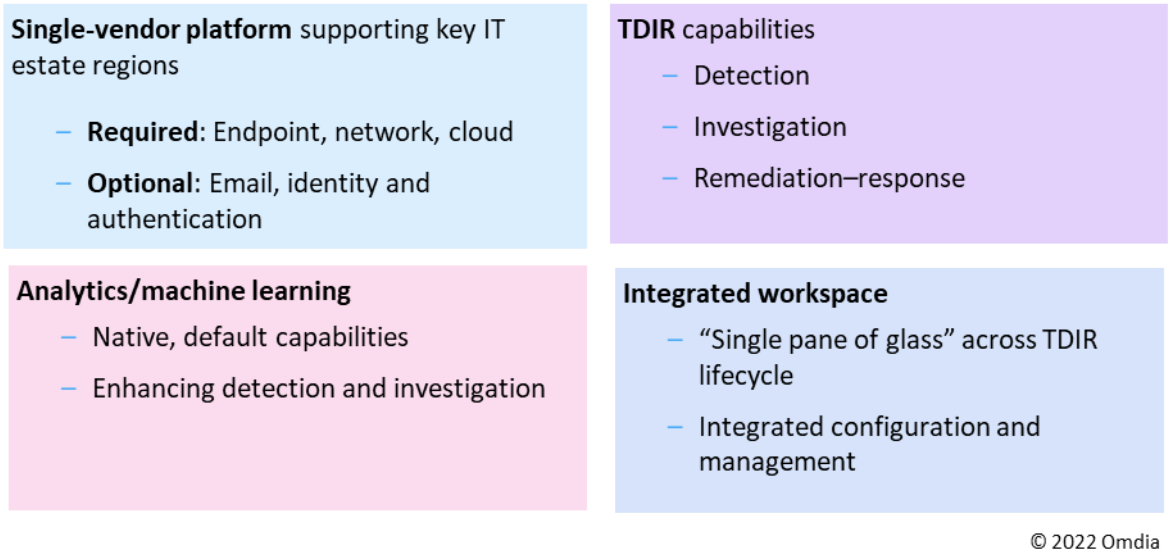


Source: Omdia

Segment definition

CXDR offerings are single-vendor platforms or solution sets (or services, in some cases, albeit typically managed services) with integrated threat detection, investigation, and remediation–response capabilities. There are several key criteria that separate CXDR solutions from open XDR solutions or broader SOC platforms.

Figure 3: Comprehensive XDR: key criteria



Source: Omdia

- **Single vendor**: The overall XDR solution may consist of multiple discrete products or components often provided via or facilitated by managed services, but each is made by the same vendor and hence designed to work with others more easily and with higher efficacy than a set of integrated third-party solutions. The three critical data sources that Omdia believes a comprehensive XDR solution must have are endpoint, network, and cloud. That usually means EDR on the endpoint; NTA or NDR on the network, though sometimes it can be firewalls with network sensors; and in the cloud: cloud workload protection usually, but alternatives such as CASB or cloud security posture management that provide telemetry and remediation–response are also feasible. (Note: Omdia also believes email and identity systems are important, but at present are considered optional; support for either can potentially detect threat events sooner, but ultimately any threat event would be detected on an endpoint, network, or cloud-based system as well.)
- **Closed-loop TDIR**: Additionally, CXDR solutions are designed to facilitate a closed-loop process for the detection, alerting, investigation, and remediation–response actions to actually stop the threat and mitigate the impact on affected systems.

- **Analytics/machine learning (ML)**: CXDR solutions should be designed to include behavioral-based analytic detection capabilities and ML for the purpose of discovering new anomalous patterns and/or facilitating prealert event enrichment.

- **Integrated workspace**: While open XDR solution sets and SIEM/SOAR-based SOC stacks often require multiple user interfaces to complete the full spectrum of TDIR tasks, CXDR offers a "single pane of glass" set of integrated workspaces to facilitate the start-to-finish TDIR lifecycle from detection through alerting and investigation, and ultimately initiating a remediation–response action and validating its success. CXDR also often eases or even largely obviates configuration and management tasks from the end users.

There are benefits and drawbacks, respectively, to both the CXDR and OXDR approaches. These are discussed in detail in Omdia's previously published report, *Fundamentals of Comprehensive Extended Detection and Response* (see Further Reading in the Appendix).

Figure 4: XDR: Comprehensive vs. open

Comprehensive XDR: Strengths	Comprehensive XDR: Weaknesses
• Data is sourced from one vendor in preunified format • Data normalization and correlation are ideally trivial • Smooth reaction, response, resolution. • Represents democratization of enterprise-grade TDIR capabilities	• Significant vendor lock-in risk/cost; rip-and-replace • Often requires commitment to vendor's data lake • Not all created equal (some better with endpoint and others networks) • NOT a viable alternative/replacement for SIEM/NG-SIEM

Open XDR: Strengths	Open XDR: Weaknesses
• Central XDR engine, but supports integration with third-party solutions. • Positioned as a "drop in" to many existing SOC architectures; no "rip and replace"; often more affordable • Often enables flexible data repository decisions (combined vs. distributed)	• Requires work to integrate logs from third-party solutions • Requires data management to ensure useful data for detection • Can require purpose-specific data lake for data storage • Response options may be limited based on third-party functionality/ interoperability

Source: Omdia

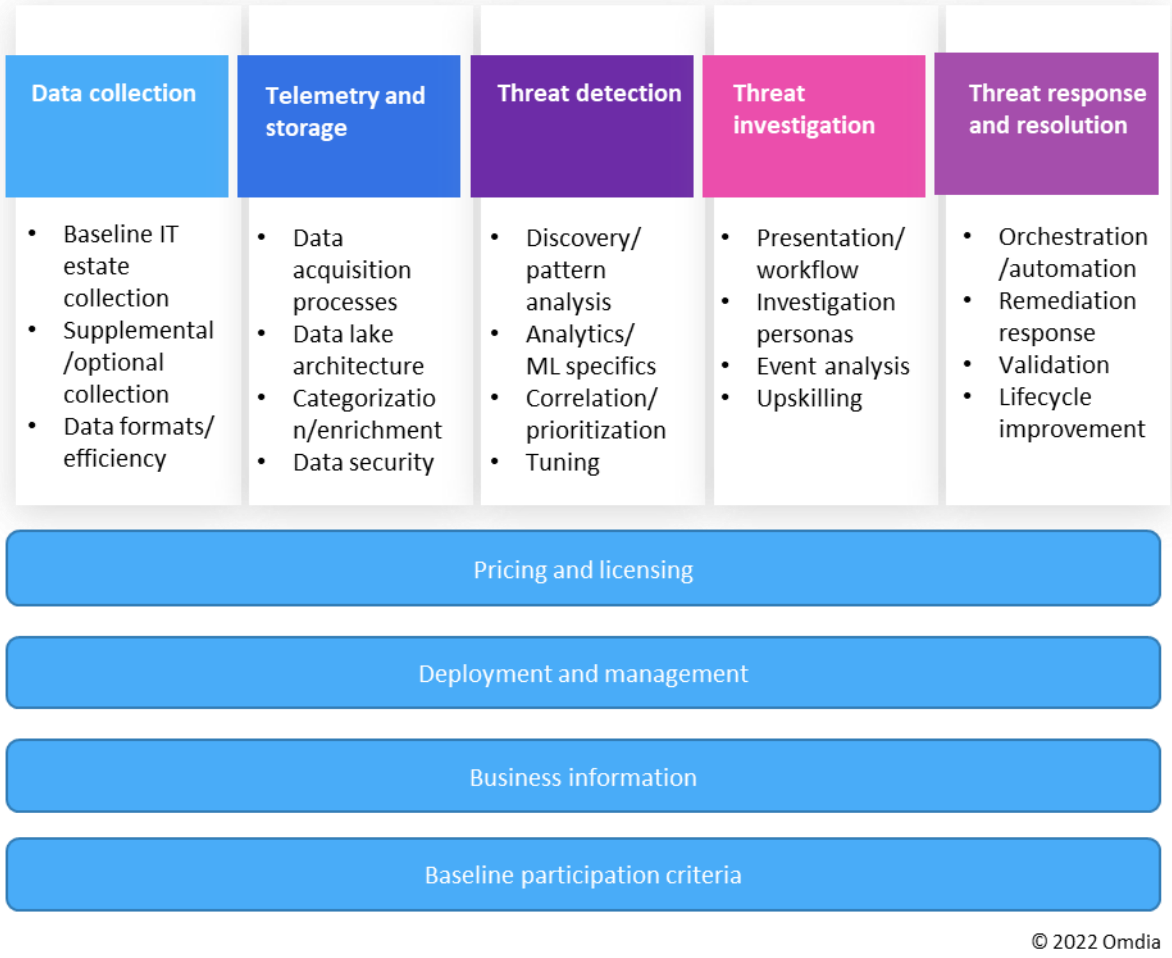
Solution evaluation criteria

For its evaluation of CXDR solutions, Omdia identified nine criteria categories. In addition to business fundamentals, pricing and licensing, and deployment and management considerations, Omdia requires solutions to meet several baseline criteria in order to be labeled by Omdia as CXDR:

- It must be a **single-vendor platform or solution** (or service if applicable) that offers its own agents or sensors or the equivalent without third-party technology or OEM partnerships to support TDIR activities across the following IT estate regions: endpoints (Windows, Mac, and Linux), networks (traditional and hybrid/east–west), and cloud environments (workloads deployed in one or more specific public or hybrid cloud environments).
- It must provide TDIR capabilities **across the required IT estate regions** (identified above).
- It must incorporate **analytics** (behavioral baseline development and deviation awareness) and **machine learning** (ML) as native, default capabilities for the purpose of both threat detection (i.e. non-rules-based detection) and investigation (i.e., automated correlation of artifacts).
- It must provide a **"single pane of glass" workspace** for all TDIR activities as well as integrated configuration and management functions.

Omdia also evaluated five solution-specific CXDR evaluation criteria categories as outlined below. Omdia also evaluated innovation across all of the capabilities areas.

Figure 5: Comprehensive XDR evaluation criteria overview



Source: Omdia

- **Data collection**: In the context of CXDR, data collection covers the sources and data types from which the solution can collect data. With specific areas of the IT estate, Omdia evaluates the extent to which data collection takes place natively ("out of the box"), requiring merely GUI-based enablement on the part of the customer and little to no custom configuration, scripting, etc. Omdia evaluated data collection specifically from endpoints, networks, cloud environments, additional optional locations from other standalone solutions from the same vendor (such as email or deception), and third-party integration.

- **Telemetry and data storage**: Per Omdia's research, TDIR solutions are dependent on input—that is, data—to find threats. When threat detection data challenges go ignored, the TDIR solutions that rely on that data input are unable to deliver accurate, consistent, and high-performance threat detection, prioritization, and analysis. In this research, Omdia evaluated:

  - Data acquisition: the processes and ease with which data is collected.
  - Data lake: architecture, location, supported data types, and default storage duration.
  - Data categorization: how event category attributes, or classifiers, facilitate one or more data classification schemas for the purpose of linking related events and enabling detailed system queries.
  - Data enrichment: how collected data elements are enriched to add context or create logical connections to other data, system-defined attributes, or events.
  - Data security: measures employed to safeguard and validate data. confidentiality and integrity.

- **Threat detection**: Omdia prioritizes fast, consistent, accurate, and manageable anomaly and threat detection with a special emphasis on the way in which CXDR solutions use of a common data format among the core CXDR data sources and enables the surfacing of deeper and more meaningful detection insights or fosters other advantages. In this research, Omdia evaluated:
  - Threat discovery: ongoing and varied analysis of data to update existing threat detection patterns, identify new ones, or pinpoint anomalous behavior indicative of a possible threats.
  - Analytics: ML, behavioral analytics, and other emerging techniques to continuously determine whether an event is anomalous or suspicious based on constantly evolving indicators.
  - Event enrichment: prior to alerting, the CXDR solution automatically initiates an event enrichment process without human analyst involvement for the dual purposes of accelerating/automating the investigation process and minimizing “alert fatigue” by relegating events of lesser importance.
  - Correlation: proactively corelate and review artifacts simultaneously and as a whole to make convictions with the greatest possible accuracy and provide clear, transparent insight as to how those convictions are made.
  - Prioritization: quickly and clearly delineating the highest-priority events and what attributes the solution has used to make that assessment, with customization.

- **Threat investigation**: Omdia believes CXDR solutions should facilitate the analysis of security events with greater ease and simplicity than existing alternative TDIR solutions. In this research, Omdia evaluated:
  - Presentation: delivery of pertinent information in an informative, compelling, intuitive way, typically with an interactive visualization interface.
  - Guided investigation: the extent to which the solution assists inexperienced or overburdened human analysts with their investigations.

  - Manual investigation: facilitating human-conducted investigations by easing key processes such as examining alerts, reviewing artifacts, and ensuring access to integrated core telemetry sources for on-demand data queries.
  - Event analysis: reviewing investigation findings using machine learning and a corpus of past similar investigation resolutions across its customer base to assist with the drawing of conclusions as well as suggesting specific follow-on remediation–response actions.

- **Threat response**: This covers remediating, confirming, resolving, and ultimately closing out a ticket for the corresponding event or investigation. In this research, Omdia evaluated:
  - Orchestration: facilitating a built-in (non-SOAR) "closed loop" unified process for detection, alerting, investigation, and remediation–response actions often including the use of orchestration templates or other technical or process-oriented capabilities within the unified workspace.
  - Validation: ensuring the efficacy of each remediation–response action, either automated or manual, after they are deemed completed.
  - Progress: Omdia believes CXDR solutions should effectively "learn" from the conclusions of each detection/investigation/response process, examining both desired and undesired conclusions to evaluate and improve future outcomes.

Market dynamics

The CXDR market is nascent; most of the solutions included in this research have been on the market for approximately 12 months or less. At the same time, buyers are largely in the early stages of learning about XDR. Awareness of CXDR specifically and the difference between CXDR and OXDR are low and a wide variety of XDR definitions being floated by vendors and providers, often to align with their own worldviews, has in Omdia's view muddled the emerging market.

However, the rapidly growing interest in XDR has been driven by a variety of factors. Perhaps most notable is the long-standing frustration with traditional SIEM/SOAR-based SOC architecture stack, in which cost and complexity often fail to yield consistently effective TDIR outcomes, as well as the desire for an integrated solution or architecture from which to manage the entirety of the TDIR lifecycle.

Figure 6: Vendor rankings in the CXDR Omdia Universe

Vendor	Product(s) evaluated
Leader	
Sophos	Sophos Central Intercept X Advanced with XDR
Challengers	
Fidelis Cybersecurity	Fidelis Elevate
Palo Alto Networks	Cortex XDR (version 3.3)
Trellix	Trellix XDR

Source: Omdia

Market leaders

Many *Omdia Universe* evaluations result in multiple market leaders. The results of Omdia's scoring in this instance, however, definitively pointed to a single solution rising above the rest.

Sophos earned the honor of not only Omdia's overall top-ranked CXDR vendor but also our sole recommended leader. Omdia believes its six-plus years of experience building XDR and its precursor technology—its Security Heartbeat feature was one of the industry's first offerings that directly integrated threat detection and response capabilities between endpoint and network security solutions—was a major factor contributing to a broad maturity of capabilities that competing solutions largely could not match. For example, its data acquisition process captures key data elements from all three major IT estate regions and delivers it to the centralized cloud-based data lake with minimal configuration and management. Its remediation–response features also clearly excelled with strong process automation, remediation validation, and its use of machine learning to cycle new conclusions back into the threat detection process to improve efficacy was unmatched.

Market challengers

Fidelis Cybersecurity may not be synonymous with XDR, but the vendor has integrated its suite of TDIR solutions to develop a compelling offering. Its more-than-capable standalone network and endpoint technologies serve as the core of its solution, its Halo cloud threat detection is promising, and its integrated deceptive threat detection capabilities provide unique differentiation versus competing offerings. In a landscape where CXDR vendors tout their all-in-one platforms, Fidelis positions itself as offering a hybrid approach, aiming to help customers understand and address any alert from any detection technology, including third-party solutions.

Palo Alto Networks, as expected in every market segment in which it participates, is highly competitive in CXDR. In particular, the cybersecurity giant's best-in-class CXDR threat detection capabilities uses a wide variety of potential indicators of compromise (IoCs), using behavioral and analytics-based detections as well as traditional stateful detections. The Cortex XDR workspace

offers analysts multiple investigative viewpoints to enable rapid drilldown into relevant artifacts and related data. In line with the vendor's overall SecOps strategy, the solution has shown early success with customers in easing key TDIR pain points, such as disparate and siloed tools, too many alerts, and not enough useful automation to accelerate mean time to response (MTTR)

Trellix may not yet have the name recognition of some of its competitors, but the company created from the former enterprise divisions of McAfee and FireEye is leveraging a broad, mature, and proven solution set as the technical underpinnings of its XDR solution. With the former Helix analytics platform and the McAfee MVISION Insights threat analysis solution at its core, Trellix XDR is focused heavily on usability both from a technical side in regard to depth and breadth of integrations and also operationally, building functionality based on several unique user personas. Of the four solutions in this review, Trellix XDR may be poised to advance its capabilities the most in the next 12–18 months.

Market outlook

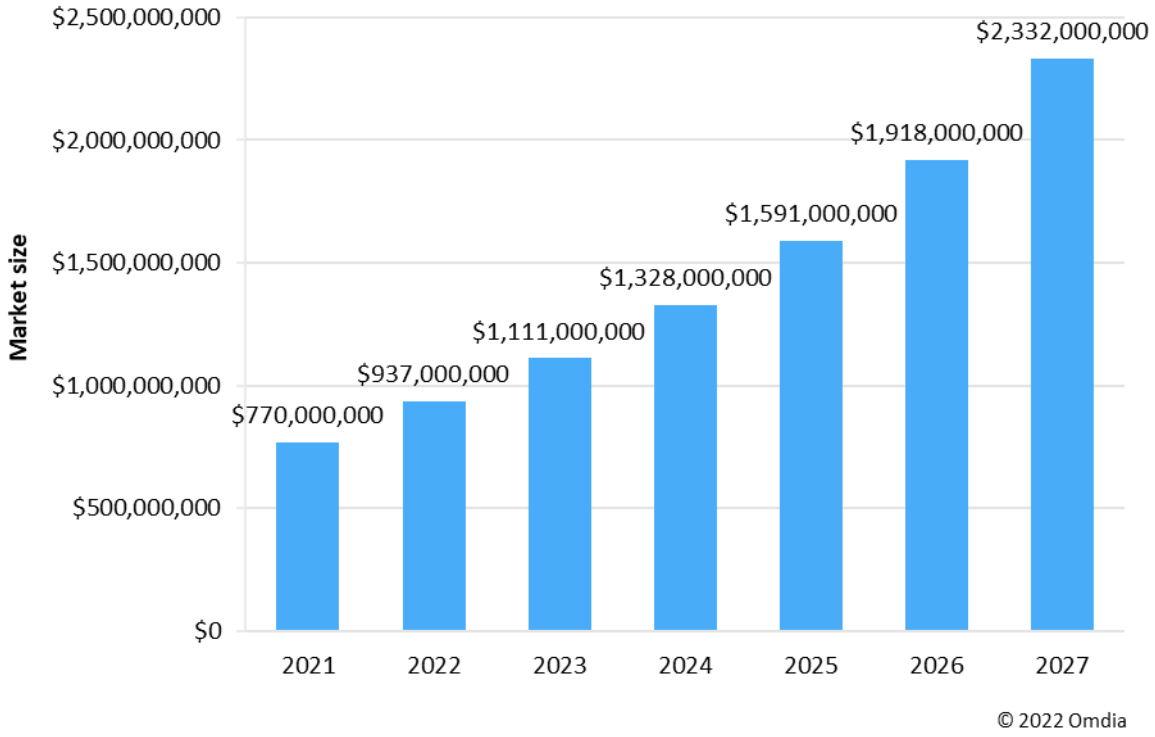
The market presence (segment revenue) of the vendors in this evaluation is somewhat misrepresented by the illustration in **Figure 1**. Sophos and Crowdstrike are among the EDR vendors that either took early steps to morph their EDR products into XDR, or simply offered all of their EDR customers an XDR entitlement. Both scenarios can create an immediate shift in revenue recognition from EDR to XDR, which in turn creates the illusion of an outsized market advantage. Nearly all EDR vendors are in the process of shifting revenue to XDR; hence, Omdia expects the market presence among these and other top-tier XDR vendors to tighten considerably in the next 12 months.

Looking ahead, Omdia is bullish on the long-term growth outlook for the XDR market segment, but the coming global economic challenges are projected to have a significant impact.

While Omdia previously forecasted the segment to top $4bn in revenue by 2027, the expected turbulence in global macroeconomic conditions in addition to signs of contraction within the cybersecurity industry specifically, indicate that XDR's growth potential is somewhat reduced.

Omdia's most up-to-date XDR segment forecast now anticipates revenue of $965m for 2022, and growing to $2.39bn by 2027. Still, by any measure, this is healthy growth that will rival or surpass most other SecOps market segments currently tracked by Omdia.

Figure 7: XDR market forecast: 2022–27



Source: Omdia

Methodology

Omdia Universe

For the purposes of this report, vendors were subjected to a detailed comparative analysis, which examined many aspects of CXDR solution. In some cases, this was a single product or solution; in other cases, vendors submitted an integrated set of standalone products.

The comparative analysis featured a detailed questionnaire in which vendors provided responses to specific queries about solution capabilities. Each vendor was also invited to provide a briefing and product demonstration to Omdia analysts. Customer experience data was collected via primary research conducted or overseen by Omdia.

Inclusion criteria

Omdia has closely tracked the emergence and rapid evolution of XDR segment. Inclusion criteria for this Omdia Universe on CXDR were largely dictated by Omdia's own research, including, but not necessarily limited to, the following:

- The product(s) submitted for consideration must have been generally available at the time which Omdia's research was formally initiated, no later than April 1, 2022. The product(s) did not have to be available in all markets globally or any specific geographic regions or subregions as defined by Omdia.
- The product(s) submitted for consideration must meet the four baseline criteria for inclusion mentioned above. The product(s) do not necessarily have to be named/branded as CXDR in technical documentation for public-facing marketing materials.
- Each vendor whose products were submitted for consideration must generate a minimum annual revenue of $10m, as determined through publicly available information, vendor-provided information, or Omdia research.
- The product(s) submitted for consideration must have active customers as demonstrated by the vendor. A minimum number of customers established by Omdia must provide customer experience survey data to Omdia in the form of surveys fielded by Omdia or its research partner.

Invited nonparticipants

- The following vendors (listed in alphabetical order) were invited to participate in this research but declined: Check Point, Cisco Systems, Fortinet, Trend Micro, and VMware.

Vendor analysis

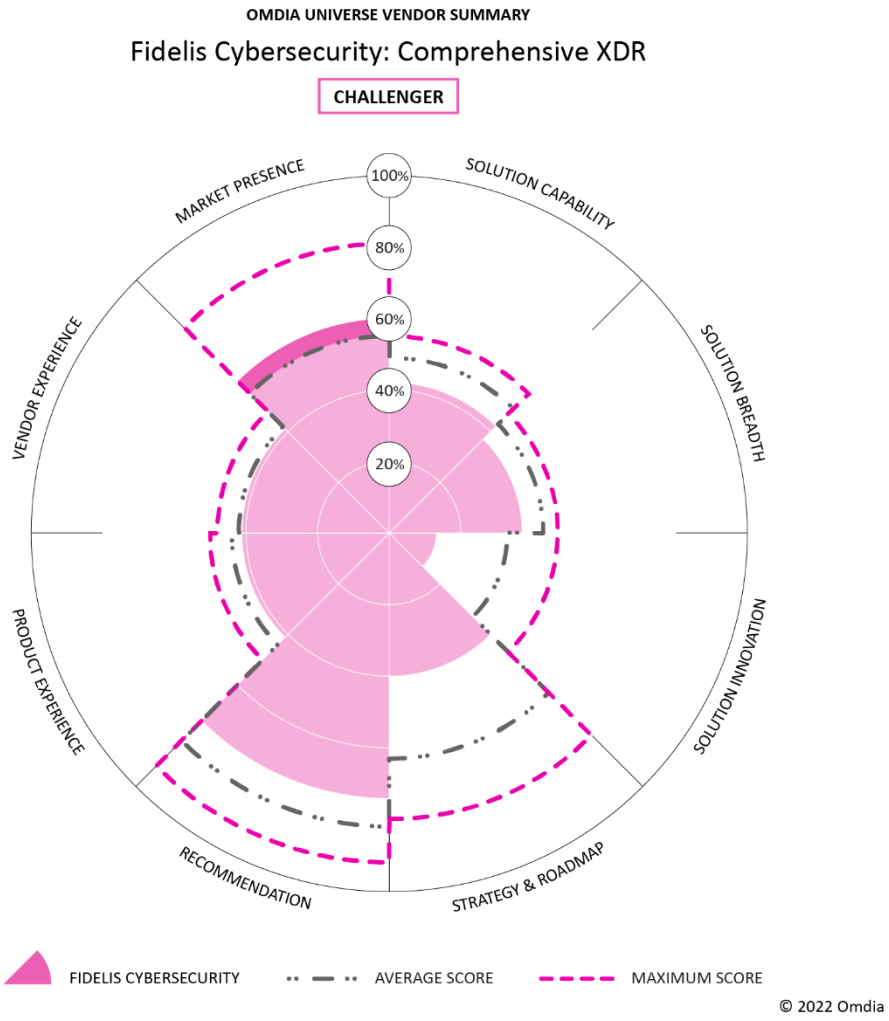
Fidelis Cybersecurity (Omdia recommendation: Challenger)

Table 1: Fidelis Cybersecurity solution profile

Product name(s)	Fidelis Elevate
Target market(s)	North America, EMEA, and Asia & Oceania
Number of customers	200+
Key customers	Declined to provide

Source: Omdia

Figure 8: Omdia Universe CXDR ratings—Fidelis Cybersecurity



Source: Omdia

Fidelis Cybersecurity should appear on your shortlist if…

- A network-centric XDR solution is preferred.
- Automated consolidation of related events is a priority in order to reduce alert noise by shifting focus to a smaller number of related conclusions.
- Dynamic deception technology is a desired element of an integrated TDIR architecture.

Market position overview

Fidelis Cybersecurity has undergone multiple transformations in its 20-year history, but with its pivot to comprehensive XDR the vendor may have found its true identity.

Previously focused on enterprise network security and data protection, the Bethesda, Maryland-based company began to assemble its CXDR solution in 2015 with the acquisition of EDR vendor Resolution1 followed three years later by the purchase of deception vendor TopSpin and most recently scooping up cloud workload protection/cloud security posture management startup CloudPassage in 2021.

Fidelis Cybersecurity is owned by private equity firm Skyview Capital and in July 2022 received a new investment package from Skyview and Runway Growth of at least $13.6m. Omdia research indicates Fidelis Cybersecurity earned nearly $46.5m in revenue in 2021, and XDR revenue specifically accounted for approximately $26m of that.

Technology details

The Fidelis Elevate is a comprehensive XDR platform that incorporates several of the vendor's standalone solutions:

- **Fidelis Network**: Its NDR solution that deploys sensors across kinetic and virtual networks to provide terrain mapping, asset classification, network, cloud, and email traffic analysis, threat detection and response, and integrated data loss prevention.
- **Fidelis Endpoint**: Based on the former Resolution1 technology, the EDR solution features integrated forensics, ransomware defense, and supports Windows, Linux, and Mac endpoints.
- **Fidelis Deception**: A unique feature set among XDR offerings, this seeks to alter the appearance of networks and other assets via automation to lure in adversaries and detect postbreach intrusions.

The solution is supplemented by dynamic malware analysis (sandboxing) and threat intelligence from the Fidelis Threat Research Team (TRT), Fidelis Insights, and selected third-party partners. Integration with its Fidelis CloudPassage Halo hybrid cloud workload and container security product allows for ingestion of alerts and terrain information into Fidelis Elevate XDR, providing a holistic view of the terrain and risk across on-premises, hybrid, and multicloud environments in a single console. Deployment options include custom-premises, customer-operated cloud VPC, or the Fidelis Cloud SaaS model.

Data collection: Fidelis Cybersecurity offers a wide array of network sensors for data collection: east–west, north–south, email, and ICAP-integrated solutions. Fidelis Network analyzes all content and collects more than 300 metadata attributes to provide contextual threat intelligence and detect threats from initial compromise through data exfiltration. Using a patented technology called Deep Session Inspection, Fidelis Network unpacks and extracts files to detect data exfiltration at line-speed across direct, internal, cloud, email, and web traffic. Fidelis Endpoint is compatible with all contemporary versions of Windows and MacOS plus several Linux versions. Native collection of cloud data is not available. Fidelis Elevate also supports direct third-party log ingestion for Zscaler and Microsoft Active Directory, and packet-level data integration for products from SentinelOne, VMware Carbon Black, Trellix (McAfee) ePO, Forescout eyeInspect, and others.

Telemetry and storage: Fidelis Network metadata is compiled from its sensors and stored in an embedded Vertica instance. Events are classified at the sensor level; detection processes, including behavioral analytics, are run separately across the endpoint and network datasets; and any deception decoy activity is automatically included by Fidelis Elevate. Fidelis Endpoint metadata is compiled and stored separately in Elastic to facilitate analysis of process data (trees, libraries, registries, etc.). The vendor seeks to differentiate by keeping detection data where it originates as opposed to a single unified data lake or data warehouse, to avoid the cost and performance issues related to data duplication. The default storage limit is 30 days, but it can optionally be extended to 365 days or more.

Threat detection: Machine learning (ML), supervised and unsupervised, is used broadly by Fidelis Elevate to detect malicious code, identify anomalous activity and patterns, find PII, and dynamically score alert severity. Network and endpoint data is augmented with additional insight such as usernames, IPs, geographic location, and threat intelligence. Using its baseline understanding of the environment via its network and asset-mapping capabilities, its detection engine uses queries and API-based integration to develop insights and surface events. Detections can be triggered based on data from one or multiple sources. In-line decryption and reencryption enables the solution to conduct threat detection in encrypted files moving into, out of, and across the network.

Threat investigation: Fidelis Elevate's workspace is built around a customizable dashboard that supports dozens of data widgets and several persona-based views. Alerts that look related are consolidated into sets of events called Conclusions. Conclusions are then sorted by priority score, highest on top, with key information and affected assets visually prioritized. Drilling down gives analysts a timeline of all applicable events, and quick access to enriched and related data elements, up to 300 unique data types. Fidelis Elevate supports custom queries with its own query language. It incorporates its own ticketing system for investigation management.

Threat response and resolution: Using its own playbook feature, Fidelis Elevate can conduct an extensible set of script-driven remediation–response actions, such as email quarantining, dropping network packets, process termination, or endpoint forensic collection, quarantining, and behavior blocking. Additionally, its Live Console feature grants full remote access to any Fidelis-managed endpoint, accelerating the process of acquiring additional log data or implementing a remediation–response action without a script or playbook. Additional remediation–response actions require integration with a supported third-party SOAR solution.

Strategy and roadmap

Fidelis Cybersecurity has based its overall product strategy on a concept it calls proactive cyberdefense, which is summarized as the iterative and continuous process of seeking out and neutralizing threats via a variety of means before adversaries can damage an organization. In turn, it positions Fidelis Elevate as the key to successful proactive cyberdefense.

The most complicated and important item on its product roadmap is the integration of its Fidelis Halo cloud security technologies into Fidelis Elevate. Today, the solution requires virtual instances of its Endpoint and Network sensors to be deployed in public and hybrid cloud environments via containers in order to pull in cloud telemetry. Once integrated, native cloud workload protection and cloud security posture management information will be made available to Fidelis Elevate when Elevate is deployed in the cloud. Additional integration points, such as orchestrated playbooks, are on the roadmap. The vendor recently completed the integration of asset inventory and risk calculation capabilities, and further integrations are expected throughout 2023.

Opportunities

Fidelis Cybersecurity is at a significant competitive disadvantage today due to its lack of cloud-native TDIR capabilities. While components from all three major pieces of Fidelis Elevate can be installed in the cloud, the friction involved with deploying and managing them in various cloud environments is notable, particularly compared with competing solutions that are quickly making cloud-native CXDR capabilities a priority.

Its separate data stores for endpoint and network data are also notable. While there are differing philosophies, Omdia asserts that vendors choosing not to integrate and standardize their data stores on a single, unified data format face increased challenges in successfully navigating what Omdia outlines as the threat detection data lifecycle, specifically steps including normalization, categorization, enrichment, indexing and analysis. It remains to be seen how its architecture ultimately affects its ability to ensure accurate, consistent, and performant threat detection, prioritization, and analysis.

The solution leaves much to be desired in the area of multi-stage threat event visualization, relegated to a secondary event view and not at all intuitive to find or use. Fidelis Elevate's communication map feature seems capable of offering similar functionality in a more intuitive format, but it isn't being used in that way.

Omdia analysis

Though some may say XDR starts with EDR, Fidelis Cybersecurity proves that a network-centric CXDR solution is more than viable. Perhaps its greatest strength is the terrain mapping that provides deeper visibility than its NDR technology alone provides. Coupled with Fidelis Deception, this supercharges ongoing and early discovery of new and potentially risky assets before they can ever be exploited. Its built-in network traffic decryption feature, which includes full network session reconstruction, also eases the process of handling hard-to-inspect encrypted network traffic. Yet Fidelis Endpoint can hold its own as well, and together they represent a powerful combination at the heart of Fidelis Elevate.

Fidelis Cybersecurity also offered one of this evaluation's strongest investigation workspaces, not only offering one of the industry's better threat scoring methodologies, but also adeptly

consolidating relevant related events into a far smaller number of conclusions, which is critical for streamlining investigations and reducing alert noise. The solution offers a lot of granular detail presented intuitively, and numerous ways to quickly drill down to acquire even more data from individual network and endpoint sensors.

Many potential buyers may inadvertently leave Fidelis Cybersecurity off their shortlists perhaps overlooking the vendor's evolution into CXDR and the more-than-capable network and endpoint technologies at the core of its solution. In a landscape where CXDR vendors tout their all-in-one platforms, Fidelis earns credit for its hybrid approach, aiming to help customers understand and address any alert from any detection technology, including third-party solutions. Like a number of its CXDR competitors, however, the cohesion of its solution in unifying threat data across endpoints, networks, and clouds is a work in progress. Still, enterprises would be wise to monitor Fidelis Cybersecurity; with improved usability and the integration of its Fidelis Halo technology (both of which are forthcoming), Fidelis Elevate has the potential to earn a place among the industry's top CXDR solutions.

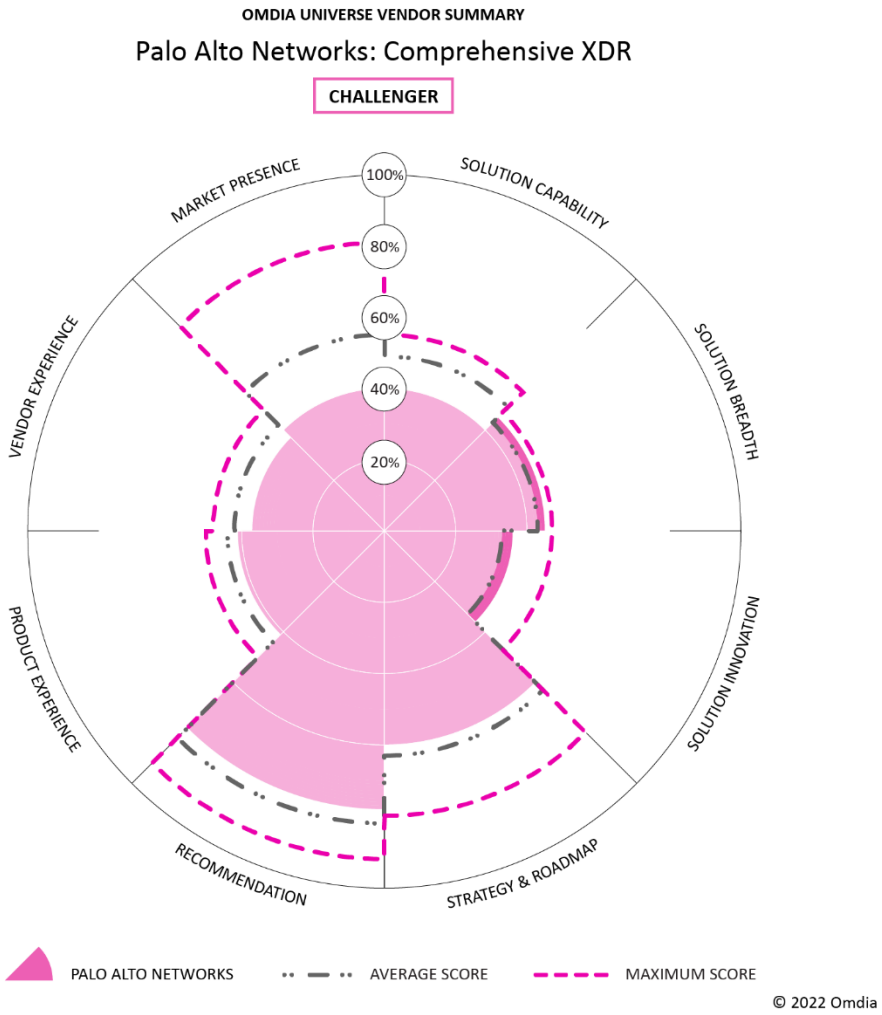
Palo Alto Networks (Omdia recommendation: Challenger)

Table 2: Palo Alto Networks solution profile

Product name(s)	Cortex XDR (version 3.3)
Target market(s)	Global
Number of customers	Approximately 3,600
Key customers	Better Mortgage, Pokemon Company International, and WestJet

Source: Omdia

Figure 9: Omdia Universe ratings—Palo Alto Networks



Source: Omdia

Palo Alto Networks should appear on your shortlist if…

- Strong integration across IT estate regions is required today.
- Granular threat detection, with strong auto-enrichment and correlation, is a top priority.
- Vendor credibility and a successful track record are essential to get purchasing buy-in.

Market position overview

Plain and simple, Palo Alto Networks is an industry titan.

The world's largest pure-play cybersecurity vendor by revenue, the Santa Clara, California-based vendor's humble beginnings in the late 2000s as a firewall and malware sandboxing vendor are a distant memory.

Today, it is on a mission to be the go-to cybersecurity vendor for enterprises globally with more than 75,000 customers in more than 150 countries. It competes in most major enterprise cybersecurity areas, including network, endpoint, cloud, and security operations.

While many of the vendor's most successful solutions have been built in-house, Palo Alto Networks is one of the industry's most aggressive technology acquirers particularly in SecOps. Some of the acquired companies whose former technology now supports its Cortex XDR solution include Cyvera (endpoint protection, 2014), LightCyber (analytics, 2017), Secdo (EDR, 2018), Demisto (SOAR, 2019) PureSec (serverless, 2019), Twistlock (cloud workload, 2019), Zingbox (IoT, 2019), Crypsis (incident response, 2020), Expanse (ASM, 2020), and Sinefa (monitoring, 2020).

The vendor's fiscal year 2022 revenue was $5.5bn. Omdia research indicates its XDR revenue for calendar year 2021 was $18.7m.

Technology details

Cortex XDR relies on capabilities of some of the industry's strongest point products across multiple domains.

On the endpoint, the company's agent (based on technology from Cyvera and Secdo) offers unified endpoint protection and EDR functionality. On the network, Cortex XDR natively integrates with physical and virtual versions of its top-tier next-generation firewall platform (via PANOS). And in the cloud, the endpoint agent can be deployed to protect cloud workloads or the solution can integrate with its Prisma Cloud platform.

The solution is optionally supplemented by its Xpanse external attack surface management technology, its XSOAR security orchestration solution, as well as its Unit42 threat intelligence and incident response offerings. The XDR engine, data lake, and workspace are all cloud-based (GCP).

Data collection: Palo Alto Networks makes a concerted effort to bring together data from a wide variety of sources. Endpoint, firewall, and cloud data are all sent data (optionally via collectors) to its Cortex Data Lake (CDL) via APIs (broker VMs can be deployed to capture additional telemetry via syslog, NetFlow, and other common formats). The solution is compatible with all contemporary

versions of Windows and MacOS plus several Linux versions. From the endpoint, process, file, network, registry, services, scheduled tasks, and user activity is all captured by default.

Telemetry and storage: The vendor ingests and normalizes all data for Cortex XDR in its XQL Schema format, and its minimal data model makes data from nearly all sources available for its analytics engine. Cortex Data Lake employs pubsub but with enhancements such as event replay to manage state (where significant for detection logic), using key-value pairs for fast lookups, staging tables, and streaming APIs for its active data/passive query model. Data elements are "stitched" together or linked based on common attributes or patterns. Custom parsing rules can be created for nonsupported data sources. Data is retained for 30 days by default; additional retention in "hot" or "cold" storage can be purchased in 30-day increments. Palo Alto Networks has a detailed product and data security plan called Trust 360 that it makes available publicly for review.

Threat detection: Cortex XDR detects a wide variety of potential indicators of compromise (IoCs), using behavioral and analytics-based detections as well as traditional stateful detections. It uses supervised machine learning models to predictively analyze files, and applies stateful and stateless engines to assess current behavior, time profiles, peer profiles, and entity profiles. The solution's behavioral analytics capabilities include intra-customer and cross-customer peer group analysis as well as temporal analysis that compares an entity to itself over time. Analytics profiles are updated daily with new information. Causality chains are developed to understand process relationships, and common data elements from different sources are stitched together into a single event to reduce alert volume. When anomalous or suspected malicious activity is detected, automatic data enrichment occurs on both the endpoint and firewall level using threat intelligence and other elements like IP addresses. Alert prioritization occurs automatically using a custom-built, customizable scoring engine for Cortex XDR, which is based on alert source(s), volume, category, similar incident history, and assessed severity. Alerts are categorized across kill chain steps, as well as with MITRE TTPs.

Threat investigation: The Cortex XDR workspace offers multiple views to enable rapid drilldown into relevant artifacts and data points. The type of alert, the number of involved hosts, and MITRE ATT&CK TTPs are all prominently displayed. An incident is visually displayed as a process flow chart showing all related events. Incidents with predefined criteria can be tagged either for additional sorting and prioritization, or to be assigned to specific analysts for investigation. Using XQL query language, analysts can conduct advanced searches in Cortex Data Lake. Analysts can also pivot from an existing alert or asset to conduct a dynamic and in-context query in XQL without having to exit into the Query Builder tool. Dashboards and reporting features enable investigation status tracking.

Threat response and resolution: Incident remediation suggestions are provided by the solution automatically, with a one-click "easy" button to initiate all suggested options. Suggestions are based on the specific events that occurred on a given asset so that cleanup efforts can be targeted. Specific response actions include employment of external dynamic lists for inline blocking at the firewall level, live terminal for interactive response, response scripting via a built-in Python interpreter, forensics collection, and endpoint isolation. Cortex XDR also has a "search and destroy" option: if an artifact is found to be malicious it can be identified and purged in all instances across the environment. Advanced orchestrated and automated remediation actions fall into the purview of the optional XSOAR product.

Strategy and roadmap

The overarching Cortex XDR strategy is to differentiate by solving key challenges in the security operations center that have plagued enterprises for years, such as disparate and siloed tools, too many alerts, and not enough useful automation. Cortex XDR is positioned as the best solution to collect data across endpoints, networks, and clouds, stitch it together into a single data source, detect known and unknown threats, and enable rapid, thorough investigation followed by real-time and ideally automated response.

A key priority going forward is tighter integration with other elements of the Palo Alto Networks product portfolio, most notably its Xpanse EASM solution. The vendor plans to make greater use of Xpanse data in Cortex XDR, stitching threat detection data with vulnerability information, eventually enabling Cortex XDR to identify incidents tied to vulnerable applications.

Additional upcoming initiatives include a new prototype endpoint agent designed to significantly streamlines the volume of data collected (and, in turn, stored) from endpoints; new detection capabilities for cryptomining, shellcode, and compromised credentials; cloud-driven DLP support (via Prisma Access integration); and expanded support for MSSPs.

Opportunities

Omdia questions whether Palo Alto Networks' approach of using a single agent on both traditional endpoints and cloud-based hosts is sensible. Because cloud workload protection (CWPP) exists as part of a separate product portfolio (Prisma Cloud) within Palo Alto Networks, this essentially means customers must either use the vendor's traditional endpoint agent in the cloud (which, to be fair, does include cloud-specific threat detection mechanisms for virtual machines and containers) or also purchase Prisma Cloud in order to get CWPP. Given the unique characteristics of hybrid cloud workloads and the customized threats they face, Omdia believes Palo Alto Networks should work through its challenges and combine its CWPP and XDR capabilities.

The solution is lacking in the area of guided investigations—features to assist inexperienced or overburdened analysts with investigations. Though it offers remarkable granularity of features and customization, a moderate degree of experience and solution-specific training is needed to ensure customer success.

Perhaps the biggest opportunity for improvement is in regard to built-in incident response automation. While an array of incident response features are available in Cortex XDR—and some are quite compelling, such as its endpoint isolation, remediation for a variety of specific scenarios, and full system restoration—complex multistep response orchestration requires also employing XSOAR. Palo Alto Networks admits that without XSOAR, automated response options are limited. One of the most important benefits of XDR is easy, on-the-fly response automation without the requirement to build complex playbooks.

Omdia analysis

What may turn heads for those looking at Cortex XDR for the first time is the extent to which Palo Alto Networks has invested in developing its endpoint security capabilities. With little fanfare, through numerous above-mentioned acquisitions, it now boasts endpoint protection and EDR offerings with capabilities that rival those of any vendor in the industry.

It has effectively leveled up those advancements in Cortex XDR, adding cutting-edge TDIR capabilities such as customized endpoint data collection, technique and behavioral threat prevention controls, in-depth endpoint forensics with memory imaging and kernel analysis, and a variety of point-and-click remediation options including restoration to a previous state. Adding to that the benefit of enriching its endpoint data with telemetry from other sources, it offers broad third-party solution integration and data ingestion compatibility, seeking to deliver a “hybrid” XDR experience.

In Omdia’s analysis, where Cortex XDR truly shines is in threat detection. Its remarkably comprehensive and adaptive set of rules-based, behavioral, and ML-driven detection capabilities as well as its demonstrable ability to distill billions of events down to a few hundred alerts—with only a handful requiring analyst intervention—is astoundingly mature, and among the most effective triage and event prioritization offerings on the market today.

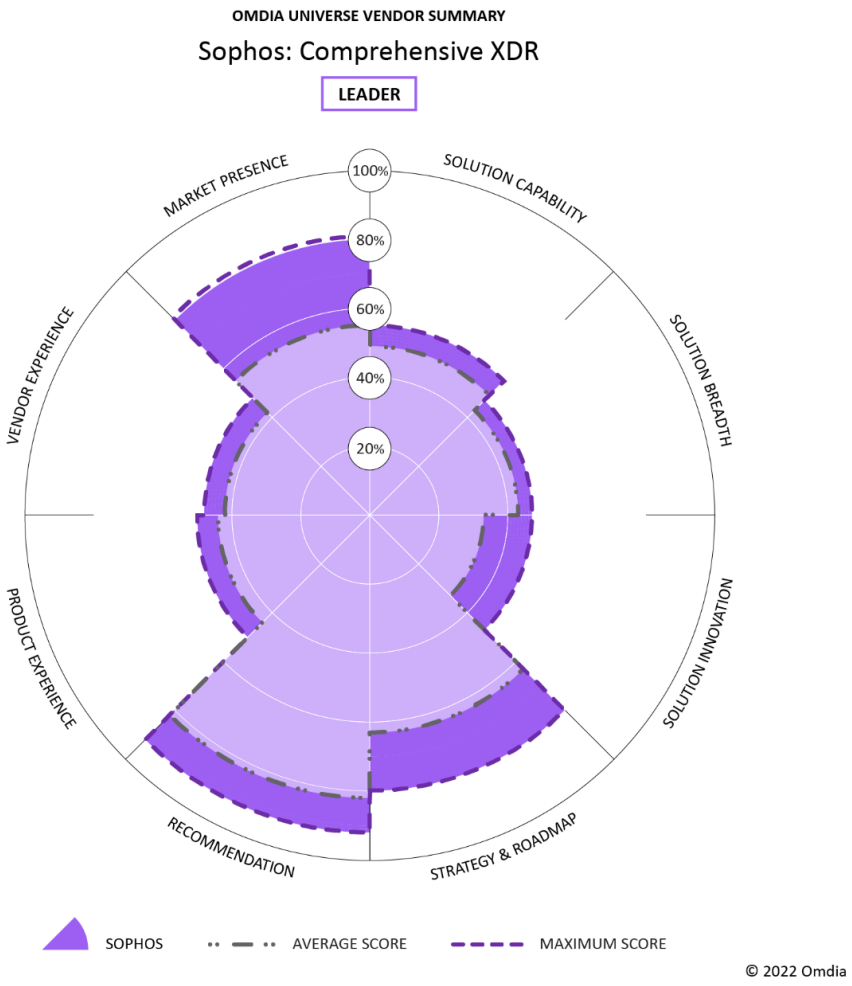
Despite being a capable overall solution, Cortex XDR was hindered in Omdia’s evaluation by its complicated cloud agent approach, its SOAR-dependent threat response automation capabilities, and its pricing and licensing, which requires a number of individual purchases in order to acquire the full slate of capabilities. But there’s little question that for organizations already inclined toward Palo Alto Networks, Cortex XDR is a worthy choice upon which to base a forward-leaning Comprehensive XDR platform.

Sophos (Omdia recommendation: Leader)

Table 3: Sophos solution profile

Product name(s)	Sophos Central Intercept X Advanced with XDR
Target market(s)	Global
Number of customers	39,000
Key customers	Del Monte, Five Guys, Krispy Kreme

Figure 10: Omdia Universe ratings—Sophos



Source: Omdia

Sophos should appear on your shortlist if…

- An enterprise-grade solution with intuitive usability across the board is critical.
- Superior threat remediation with automated response actions for common scenarios is needed.
- Straightforward pricing and licensing are important, plus support from Sophos and its partners.

Market position overview

Omdia believes that the best comprehensive XDR solutions deliver a fundamentally different approach to TDIR: one that's faster, easier, more automated, and ultimately more effective. With those criteria in mind, it should be no surprise that Sophos Central Intercept X Advanced with XDR is the overall top-ranked solution in the XDR *Omdia Universe*.

Sophos has undergone several turning points since its founding as an encryption software vendor nearly 40 years ago. The most recent was in early 2020 when private equity firm Thoma Bravo took Sophos private in a $3.9bn deal. But its transformation into a leading XDR vendor has been years in the making, boosted by a number of notable acquisitions, including Cyberoam (next-generation firewall, 2014), SurfRight (endpoint protection, 2015), Invincea (analytics, 2017), DarkBytes (UX and telemetry, 2019), Rook Security (MDR and threat intelligence, 2019), Capsul8 (cloud and Linux security, 2021), Braintrace (XDR and data lake, 2021), Refactr (orchestration, 2021), and SOC.OS (alert management, 2022).

While it maintains a strong presence in the UK where it was founded, the company is now headquartered in Santa Clara, California. Sophos does not report revenue publicly, although Omdia research indicates its 2021 XDR product revenue was approximately $128m (due largely to shifting EDR revenue). It sells only through its global network of 78,000 channel partners.

Technology details

Sophos Central Intercept X Advanced with XDR was built on top of the former Intercept X EDR solution (it also offers a version specifically for servers). In addition to Intercept X on the endpoint, the XDR platform incorporates Sophos Firewall for native network data and the Sophos Cloud Optix solution for cloud workloads and containers. Data is centrally stored in the cloud-based Sophos Data Lake, and the solution is managed from the Sophos Central SaaS-based unified management system.

The endpoint deployment covers all supported versions of Windows and MacOS and most popular versions of Linux. On the network, when XDR is used in conjunction with the Sophos Managed Detection and Response service, direct integration is supported for firewalls from Cisco Systems, Check Point, Forcepoint, Fortinet, Palo Alto Networks, and SonicWall, as well as other select products. All three major public cloud platforms are supported. The solution also optionally incorporates Sophos Email Security (Microsoft 365), mobile device security via Intercept X for Mobile, and threat intelligence from Sophos Labs. The platform also serves as the basis for the Sophos MDR managed service.

Data collection: Sophos collects detailed data across IT estate regions. On the endpoint, it directly gathers data on the file system, registry, network (via Snort), process, threads, system logs, as well as on device detection/protection events. On the network, full Sophos Firewall logs are available,

from classification events to connections and protection details. Through Cloud Optix, it has access to security scan data, anomalous and high-risk events, and other notables such as credential compromise.

Telemetry and storage: Sophos Data Lake is based on AWS with redundancy in multiple regions. Upon ingestion, data is normalized into a common schema although original log data is also retained. Data is then enriched automatically using Sophos threat intelligence lookups, IP/URL, and geolocation lookups, and finally stored in a relational database.

Sophos recently extended its data capacity to 90 days of “hot” storage, with optional add-on support for up to one year. Policy options allow customers control over what data is sent to Sophos, which devices send data, turn off sample submission, or turn off threat case detail telemetry.

Threat detection: The solution primarily relies on heuristic rules and on-device behavioral analytics for speed and efficiency, but more complex classifications based on machine learning analysis and model-based pattern matching are also performed. Each event is scored on a scale of 1–10 in regard to its likelihood of being malware, otherwise malicious, or unwanted. ML models are maintained by Sophos and automatically deployed to devices as they are improved. It ingests threat intelligence daily from 40 unique providers to further add to its detection capabilities.

Customers can craft and maintain their own rules and a robust community forum is maintained for the sharing of ideas and code. Sophos incorporates a detection suppression feature to further refine how its detections are implemented for the purpose of eliminating false positives.

Threat investigation: Known malicious events are automatically remediated when the system deems a discovery as high risk. When further review is required, an alert is triggered in the Threat Analysis Center of Sophos Central to automatically create an investigation (manually created investigations are also supported). When additional artifacts or events are found related to the original event, they are automatically incorporated into the existing investigation.

All detections are mapped to the MITRE ATT&CK knowledge base of adversary tactics, techniques, and procedures. For detections based on a process execution, the system creates a threat graph showing the chain of events and process tree showing activity related to file systems, networks, and registry activity. The investigation interface offers contextually relevant functionality to help analysts pivot to facilitate the collection of more evidence, or explore other information related to the detection artifacts. It is also an option to pivot to view specific external threat intel. Suspicious executable files in the graph can be submitted to Sophos for detailed analysis.

From a workflow standpoint, multiple analysts can simultaneously work on the same investigation. If a device is suspected of being compromised, it can be temporarily isolated but still connected to Sophos Central to allow for deeper investigations. When further information is needed, Sophos Data Lake can be queried with SQL using one of several hundred prebuilt queries or via custom queries. Intercept X endpoints support OSQuery and custom extension tables, and detailed forensic records can also be pulled, all from the Sophos Central console.

Threat response and resolution: In cases where the system identifies a known threat, the product will attempt automatic remediation. Common scenarios include ransomware rollback of encrypted files, process

termination, malware removal, device isolation, registry repair, and critical system file restoration. Such automated remediation–response actions are further facilitated by Synchronized Security, a precursor capability added to its XDR solution that facilitates direct integration between endpoints and Sophos Firewall, so that firewall-based mitigations can be employed to remediate threats against endpoints and workloads.

Strategy and roadmap

The current capabilities offered by Sophos Central Intercept X Advanced with XDR are generally on par with or exceed those of competing solutions, but the vendor also has one of the industry's most ambitious product development roadmaps.

Its strategic priorities for the solution are to drive increased user efficiency for analysts, enhance collaboration and reporting functions, and provide customers with more flexibility to meet various use cases.

On efficiency, its key initiative is the integration of technology from its SOC.OS alert management acquisition. This will enable Sophos to incorporate third-party telemetry in such a way that that data related to an ongoing investigation is automatically pulled into enrich that investigation. Improvements to case generation, guided investigations, and scripted response actions are also planned.

Regarding collaboration and reporting, integration with IT service management (ITSM) and collaborative automation tools is planned for next year as is a new set of templated and custom reports. And the Sophos Central user interface is scheduled for redesign in 2023, adding more customizable dashboards, visualizations, and improved performance.

On flexibility, plans include improved third-party integration support for Open XDR use cases, an updated set of managed services, and the incorporation of Sophos Factory, a built-in workflow engine that offers an array of pre-built playbooks for the purpose of orchestrating and automating complex workflow events.

Opportunities

To its credit, Sophos has focused on native integration and consistent, successful outcomes, but it has provided fewer details than most competitors on its underlying XDR architecture, specifically Sophos Data Lake. Omdia would like the vendor to provide customers more readily with details on its data lake-house design, schema formats, and performance assurance. Similarly, Omdia believes customers would benefit from more transparency into its threat detection methodologies.

The solutions' automatic collection of associated events is restricted to the first 24 hours from when the initial triggering event occurred. Subsequent detections that may be related will result in an additional investigation being created. While this is reasonable, the design choice may inadvertently create unnecessary alert noise in the environment, plus make multistage attack detection, particularly low-and-slow attacks, more difficult.

The layout of the Threat Analysis Center is intuitive and the data made available to analysts with minimal clicks is impressive, but the text-heavy interface lacks some of the intuitive threat event visualization options of competing solutions. In some instances, particularly investigations involving

multistage attack campaigns, findings are not as easy to understand as they could be. More support is also needed for assessing threats and posture specific to cloud environments.

While XDR customers can employ Sophos-built playbooks and pipelines with the standard license, the ability to create a custom-built workflow would require an additional license. Omdia believes most customers will eventually require this level of customization, hence there is an opportunity for licensing rationalization.

Omdia analysis

Despite remaining true to its SMB roots, for years Sophos has been carefully planning its move upmarket. And the many lessons the company has learned from successfully providing feature-rich, intuitive, and easy-to-use cybersecurity solutions to hundreds of thousands of SMBs are also bearing fruit with large enterprises.

For example, it has a unique account health monitoring capability that proactively informs administrators when configuration settings may be incorrect or overly permissive and provides remediation steps when these scenarios are encountered. Furthermore, its Security Heartbeat feature, which debuted in 2017, was one of the industry's first offerings that directly integrated endpoint and network security solutions—via a common interface and bidirectional exchange of real-time information—in order to respond automatically to threats. It was effectively XDR before XDR was even invented.

As noted, in Omdia's evaluation, Sophos was as good or better than its competitors in nearly all capabilities categories, and soundly routed competing solutions in the always-challenging area of threat response, as well as deployment/management and pricing and licensing. Indeed, all Sophos products, including XDR, are licensed either per-user (endpoint) or per-device (server), with tiered volume discounts—a far cry from the complex XDR licensing methodologies employed by its competitors.

With Comprehensive XDR, Sophos' moment to emerge as a top-tier enterprise cybersecurity vendor has finally arrived. Proving the point, nearly a third of its FY 2022 billings came from organizations with more than 1,000 employees.

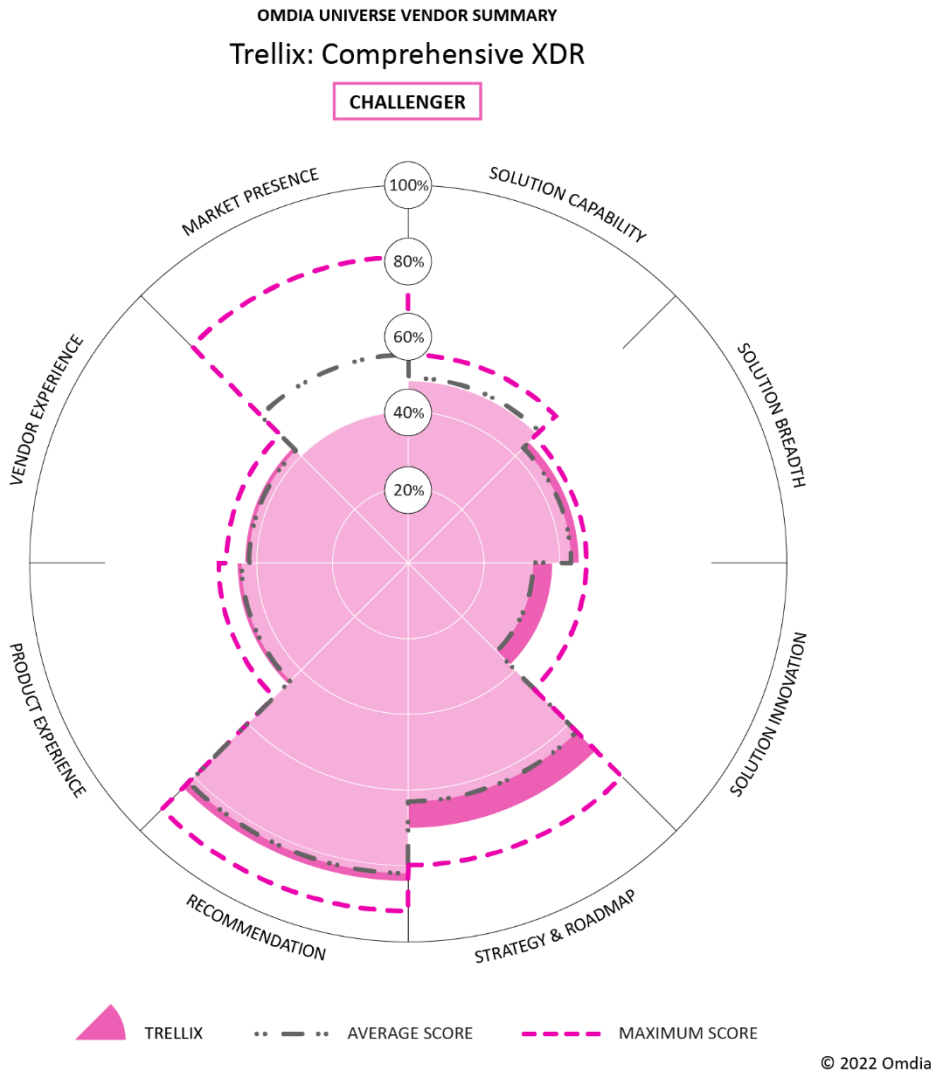
If the results of Omdia's Comprehensive XDR Omdia Universe are any indication, Sophos is only poised to continue its growth.

Trellix (Omdia recommendation: Challenger)

Table 4: Trellix solution profile

Product name(s)	Trellix XDR
Target market(s)	Global
Number of customers	2,000+
Key customers	Declined to provide

Figure 11: Omdia Universe ratings—Trellix



Source: Omdia

Trellix should appear on your shortlist if…

- A buyer wants the best of both worlds: an all-in-one platform with stout third-party integration.
- Analyst experience is a priority; specifically, visual ease of use with intuitive granularity of data.
- An aggressive, detailed long-term product roadmap is a key purchasing requirement.

Market position overview

Trellix may be a new name in enterprise cybersecurity, but its nascent Compressive XDR platform is leveraging a mature, proven solution set and it has all the pieces to be highly competitive.

Announced in January 2022, Trellix was formed through the combination of the former enterprise divisions of McAfee and FireEye. The Milpitas, California-based vendor inherited a massive security product portfolio spanning endpoint, network, cloud, email, data protection, and more.

Trellix is owned by private equity firm Symphony Technology Group (STG), which also owns sister company Skyhigh Security. Trellix has nearly 5,000 employees, more than 40,000 customers, and revenue (from the combined companies) close to $2bn, according to industry estimates. Omdia research indicates that its combined total XDR revenue in 2021 was $22.5m.

Technology details

The Trellix XDR platform consists of a core XDR engine that offers correlation, contextualization, and playbooks; discrete engines that cover specific IT estate regions (endpoint, network, cloud, and email, as well as data protection) with optional third-party data integration; a unified data lake that the individual engines feed data into; and XConsole, its upcoming unified console for managing investigation, response, and API-based integration.

Based largely on McAfee's heritage of industry-leading integration enablement, the Trellix XDR ecosystem already boasts an impressive 800+ unique solution integrations. The solution is supplemented by threat intelligence from Trellix Advanced Research Center Deployment options today are limited to on-premises and cloud-hosted; a cloud-native version is on the vendor's product roadmap.

Data collection: Trellix earned the top score among all entrants in data collection, due to the depth, breadth, and maturity of its solutions across essential CXDR IT estate regions. On the endpoint, it gathers data from Trellix ENS and EDR (formally McAfee MVISION and FireEye HX; a unified endpoint is scheduled for early 2023); on the network it can tap into Trellix Intrusion Prevention (formerly McAfee IPS) data center traffic, and Trellix Network Security (formerly FireEye NX) for egress traffic or advance threats, or the new Trellix Network Investigator, a dedicated NDR offering that leverages multiple solutions; in the cloud, Trellix offers API-based integration with all three major public cloud platforms—including Amazon Inspector EC2 and ECR vulnerability data—to assess posture, set benchmarks, and scan for anomalous activity. The solution natively collects data also from its email security and data protection solutions, and can optionally collect data from the McAfee ESM SIEM.

Telemetry and storage: Data is acquired through a mix of Trellix as well as third-party sensors (native clients), APIs, cloud services integrations, and evidence collectors. Its cloud-based data lake is

based on Snowflake but uses two separate data stores: Elastic search for "hot" data (7–14 days), and AWS S3 for "cold" storage (up to 13 months). Upon ingestion into the data store, data is normalized, indexed and then classified by event type, which in turn dictates how it is enriched with additional data attributes.

Threat detection: While machine learning capabilities exclusive to Trellix XDR are limited (ML is built into the discreet solutions in the IT estate regions), the solution bases its threat detection on rules-based detections, as well as optional behavioral baselining and threat intelligence. Heuristics are used to detect anomalies and threats such as stolen credentials and "time travel" scenarios. Detections are made by matching a given engine's findings against indicators such as return risk, severity, affected assets, path of the detection. Custom rules allow the ability to tune the detections for the customer environment.

Threat investigation: Trellix has designed its solution to meet the needs of four unique personas: incident analysts, threat hunters, solution partners, and managed security service providers. In 2023 Trellix plans the launch of XConsole, a single-pane-of-glass user experience for managing the TDIR lifecycle across the entire platform. XConsole is largely based on the former FireEye Helix security operations platform and the McAfee MVISION Insights threat analysis solution.

Alerts, including combined related events, are presented for investigation prioritized by severity, along with the reason for detection, correlated events, and mapping to the MITRE ATT&CK framework. Within the context of an event, related artifacts are presented visually, with those seen as most important highlighted. Analysts can drill down into any artifact's raw telemetry and atomic detections and automated investigation workflows can be configured using playbooks. Trellix offers one of the few CXDR solutions that supports contextual tips and guided questions to assist with data analysis, development of conclusions and identification of remediation options.

Threat response and resolution: At present, orchestrated and automated response actions rely on integration and use of Trellix Automated Response (TAR), formerly FireEye Security Orchestrator, a standalone SOAR solution (which falls outside of Omdia's definition of CXDR). TAR integration supports prebuilt playbooks, which can be used to implement custom incident response workflow automation between on-premises security appliances. After remediation, machine learning algorithms identify areas for improvement, such as tuning sensitivity in response to a behavior or particular IOC and sets these for review by a Trellix Advanced Research Center expert.

Strategy and roadmap

For the next 12–18 months, Trellix is focused on executing an ambitious product roadmap, which will bring to life what the company calls the Trellix XDR Platform: the combination of six core engines (endpoint, network, cloud, email, data, and third-party integrations) unified via a centralized data lake and the upcoming XConsole user experience with support from the company's research and engineering unit.

XConsole in particular presents a fascinating opportunity as Trellix intends for it to truly be a single interface offering multiple user personas, covering everything the company offers, including the upcoming revamp of its widely deployed McAfee ePO endpoint management solution.

Trellix believes that by integrating data exfiltration detection and prevention technology—Trellix DLP (formerly McAfee DLP)—as an integrated element of its XDR solution, not only will it provide customers with a "last line of defense" when sophisticated attacks go otherwise undetected, but it will also give Trellix a viable technical differentiator in the comprehensive XDR market segment.

Opportunities

As it brings together products from both McAfee and FireEye, despite the former companies' extensive focus on third-party integrations and its notable progress uniting their respective endpoint technologies, Omdia believes it has work to do to foster seamless integration among its own point solutions. For instance, the vendor only recently deployed single sign-on functionality across all its platforms. Thus, while users can transition from McAfee MVISION to FireEye Helix without multiple logins, to do so requires the use of a specially built app switcher, which offers little true integration between solutions, while the rest of the intra-solution integration work remains to be completed. Much of that capability will be enabled via the Trellix Event Fabric, an new software integration layer. Trellix Event Fabric will serve as a data ingestion conduit between Trellix XDR and its own data sources as well as third-party point solutions, eliminating scaling issues and allowing data to be easily correlated, contextualized, and alerted upon. The company says Trellix Event Fabric is a distinct approach from the former-McAfee OpenDXL security platform integration framework. Future plans for OpenDXL, one of the industry's most advanced cybersecurity integration platforms, remain unclear.

Today Trellix incident response playbooks must be custom-built, and while it has prebuilt many playbooks and made them available on its marketplace, the vendor has yet to enable customers to customize cloud-based playbooks but rather only on-premises ones. This means playbooks currently used for on-premises systems cannot yet be mapped to cloud computing assets, though this is due to be addressed in 1Q23.

Its pricing and licensing terms are a significant drawback for Trellix XDR buyers; at present, each Trellix XDR component must be purchased as part of up to six separate bundles. Trellix has an opportunity to introduce top-to-bottom improvements to its licensing model, emphasizing packages that fit both one-size-fits-all and highly customized buyer profiles as well as MSSPs.

Omdia analysis

Trellix has all the key technology components to build an industry-leading CXDR solution.

Omdia believes Trellix is right to focus its early efforts on bolstering point solution integration and quality of user experience, as those are critically important capabilities for XDR solutions. The early iteration of its solution already offers a compelling user experience, presenting highly granular data in a compelling, actionable way.

However, as it stands today, the solution lacks some of the finer points needed to compete as an all-in-one solution for the entire TDIR lifecycle. Its threat detection capabilities, while solid, aren't as advanced as some competitors; its threat response options still require too much manual integration and playbook development; and its pricing and licensing could be a deal-breaker for some.

Simply put, Trellix needs time. But not much. By the end of 2023, Omdia expects Trellix XDR to be able to hold its own against any XDR solution on the market.

Appendix

Further reading

Fundamentals of Comprehensive Extended Detection and Response (June 2022)

Fundamentals of XDR versus SIEM and SOAR: Understanding the Evolution of SecOps Architectures (March 2021)

Authors

Eric Parizo, Managing Principal Analyst, Security Operations Intelligence Service

Andrew Braunberg, Principal Analyst, Security Operations Intelligence Service

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com