IDC MarketScape

IDC MarketScape: Worldwide Extended Detection and Response Software 2025 Vendor Assessment

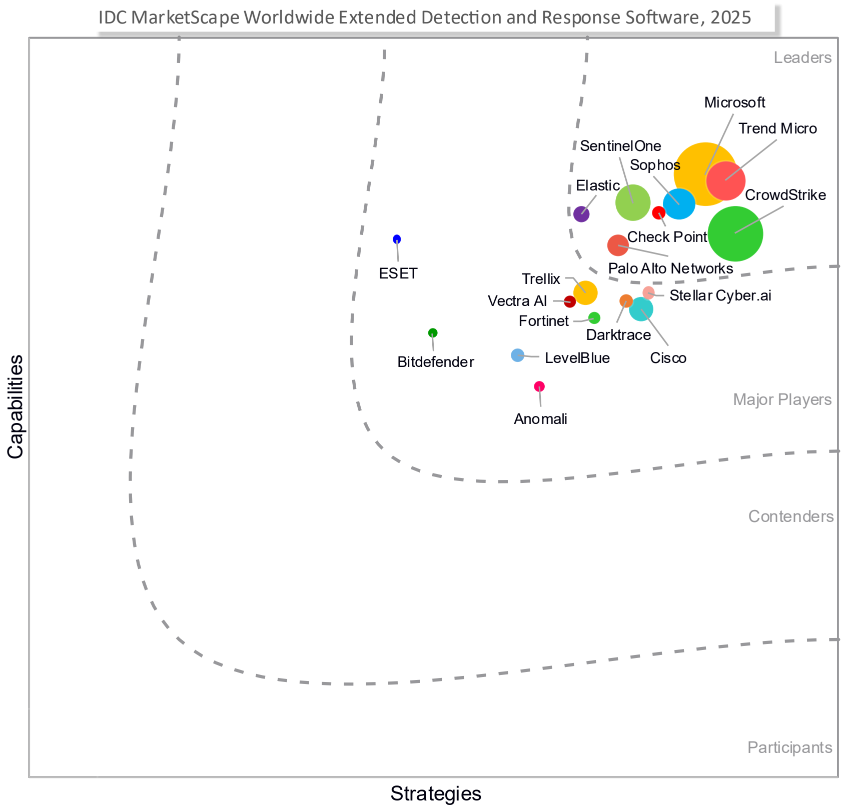
Christopher Kissel   Monika Soltysik

THIS EXCERPT FEATURES SOPHOS AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Extended Detection and Response Software Vendor Assessment



Source: IDC, 2025

September 2025, IDC #US52997325e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Extended Detection and Response 2025 Vendor Assessment (Doc # US52997325).

IDC OPINION

The concept of extended detection and response (XDR) started to gain traction in late 2017. This was a specific time in cybersecurity as user behavioral analytics (UBA) became an enhancement to machine learning. UBA had a profound effect on endpoint platforms and on network detection and response (NDR) concepts. UBA meant indicators of compromise (IoCs) aside from static malware signatures and explicit rules violations established in detection and response filters became possible. This also meant that far greater context about an alert was possible.

This history has a powerful impact on what XDR is and where it is going. At first, XDR was designed to reduce the number of alerts and provide the proper context for investigations. Now the expectation is to identify a campaign, create countermeasures, and respond quickly and appropriately. The types of activities an XDR solution is expected to monitor include:

- **Ransomware.** As one vendor puts it, ransomware starts slowly, imperceptibly, but then happens all at once. XDR solutions should be able to pick up on high-entropy events such as registration wipes, file name changes, and new egress ports opening.
- **Advanced persistent threats (APTs).** XDR should detect the subtle signals associated with APTs that traditional security systems may miss. In addition, an XDR solution should include early identification of abnormal behaviors, lateral movement, and privilege escalation spanning on-premises and cloud networks.
- **Identity-based attacks.** XDR should find sophisticated high-speed campaigns that start with account compromise and escalate to privileged access abuse to progress their attacks. Examples of identity-based attackers include Scattered Spider, Midnight Blizzard, Volt Typhoon, and Black Basta.
- **Living off the land (LOTL) attacks.** These occur when attackers can exploit legitimate tools and software present within the target's environment to conduct malicious activities, blending in with normal network activity and bypassing traditional security measures.

- **Cloud control plane attacks.** An adversary creates the opportunity to modify access and configuration — allowing them to inflict material damage. These attacks can occur across virtual machines, containers, and serverless infrastructure, leading to both data loss and impactful attacks.

XDR is at an inflection point. The adversary works at the speed of AI and businesses expand their IT profile horizontally for new ways to deliver applications and store data. XDR is changing with this. Strategies need to evolve to find indicators of compromise earlier, to offer immediate response and then permanent remediation, and then to ultimately determine the overall health of the network to not only solve the potential exploit/breach but also improve the network posture over time.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The following are how vendors were selected and what the "rules of the game" were:

- A vendor has to offer a commercial, do-it-yourself, XDR solution. Endpoint detection and response (EDR) vendors could get to an XDR solution by offering modules. However, other vendors offer an XDR solution that was used to augment EDR. Several managed detection and response (MDR) vendors obviously have platforms they use internally that collect telemetry, generate alerts, and start the response and remediation process. However, if these platforms were used only by that company and not commercially available, they were not considered for this study.
- The study only considered enterprise-licensed software and SaaS deployments. Hardware solutions have their place, but software solutions are the predominant form factor anyway.
- One could make the argument that security information and event management (SIEM) vendors could be included. In addition, IDC realizes that the XDR vendors are increasingly identifying themselves as next-generation (next-gen) SIEM. However, for this study, that which is rendered under SIEM should stay with SIEM.
- A company needed to do either $20 million in cloud-native XDR revenue or at least $100 million in detection and response revenue overall.
- IDC decided that the vendor should have global reach. In addition, we asked vendors to provide scenarios for midsize businesses through small enterprises (somewhere in the range of 1,500–10,000 employees) and then midsize enterprises to large enterprises (more than 10,000 employees).
- The XDR solution should have detection and response for on-premises as well as public cloud environments. IDC also placed an emphasis on an open XDR approach.

- Last, IDC only considered features and capabilities that were generally available (GA) as of July 4, 2025. In this era of agentic AI development, new capabilities are evolving every day. Given that it took time to edit and refine this study, some of the material may be dated.

ADVICE FOR TECHNOLOGY BUYERS

A key strength of the IDC MarketScape process is the integration of feedback from customer references provided by participating vendors. These firsthand perspectives offer actionable guidance for prospective buyers and highlight common challenges and opportunities in XDR adoption. Complementing this input, IDC recently conducted an XDR end-user survey, which provides additional validation of buyer perceptions. This section provides some of the impactful advice.

Disclaimer: The broad IDC survey data shall remain separate from this evaluation, which is grounded in vendor-provided and verified inputs.

Some of the impactful advice are:

- **Be transparent about total cost and deployment effort.** Budget and deployment complexity were the most frequently cited XDR challenges. It is important for suppliers to be upfront about what is included in the cost — licensing, onboarding, integration, and support — so customers do not encounter surprises later. Packaging deployment guidance helps reduce friction and sets realistic expectations from day one (see Figure 2).
- **Position XDR as a proactive defense platform — not just a detection layer**. Despite the acronym's emphasis on detection and response, buyers rank threat prevention and protection as the most important XDR use case (see Figure 3). Suppliers should emphasize how their platforms contribute to early-stage threat disruption — through capabilities like automated containment, policy enforcement, and integrated controls across endpoints, identity, and network.
- **Design for measurable, outcome-driven security performance**. XDR buyers most commonly assess effectiveness through detection accuracy, major incident prevention, and response metrics such as mean time to detect (MTTD) and mean time to respond (MTTR) along with risk-based prioritization (see Figure 4). Suppliers should build platforms that demonstrate tangible gains in these areas backed by built-in analytics and KPI reporting (e.g., dashboards that track MTTD/MTTR, alert conversion rates, risk reduction over time, and automated response actions tied to specific outcomes). Capabilities such as risk-based alert

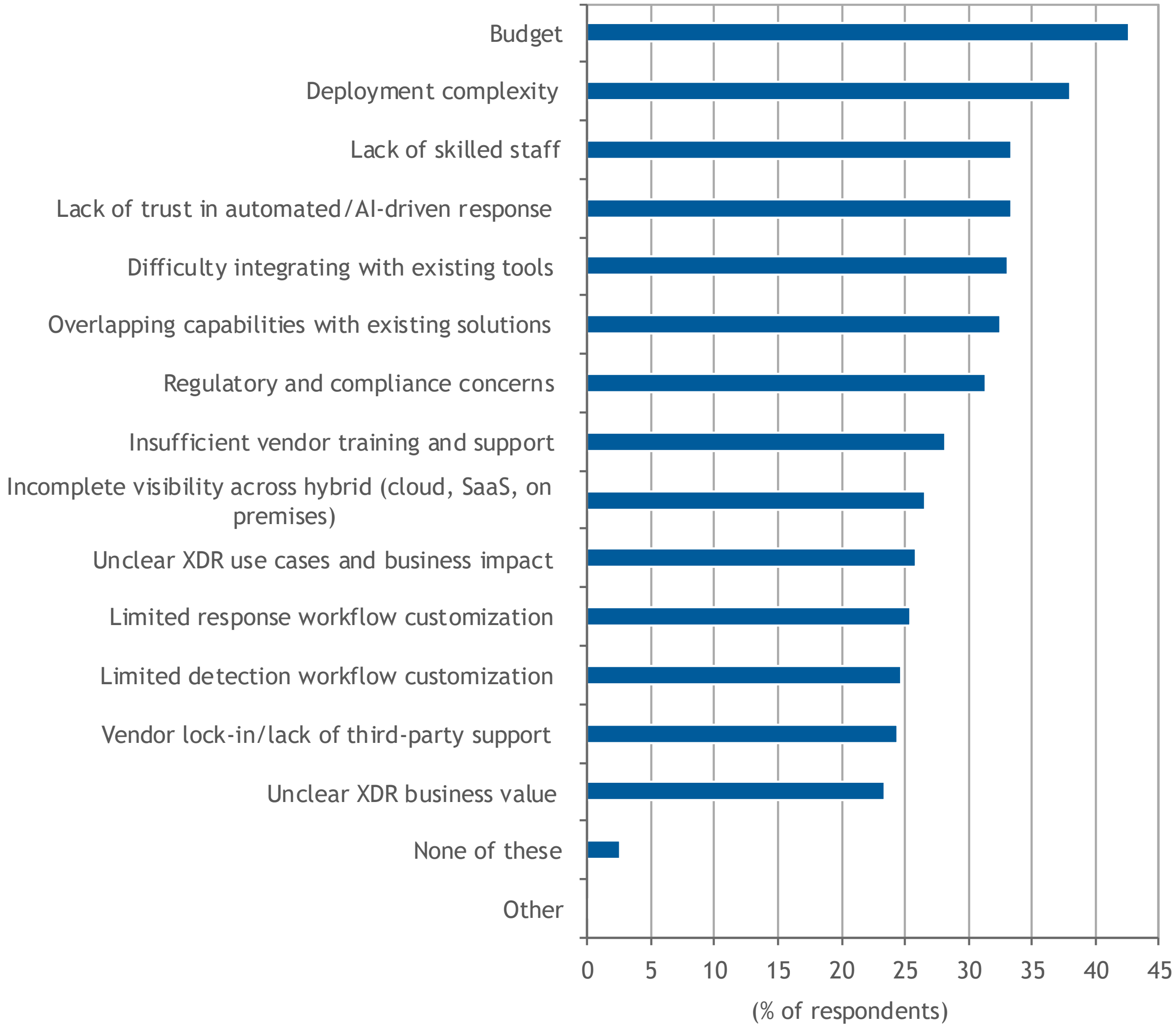
scoring, contextual correlation, preemptive containment, and workflow automation should be tied directly to reducing business impact. Vendors that position XDR as a performance-enhancing platform — rather than just a telemetry aggregator — will better align with how buyers define success.

- **Develop integrations that bridge detection and resolution.** Buyers rank integrations with network detection and response, IT service management (ITSM), firewalls (FWs), and threat intelligence (TI) platforms as the most important to XDR success (see Figure 5). Suppliers should prioritize bidirectional, context-aware integrations that go beyond data ingestion to support enrichment, automated response, and alignment with IT operations workflows. *Why?*
- **Note that operational connectivity is critical.** ITSM and security orchestration, automation, and response (SOAR) integrations reflect buyers' desire for XDR to align with incident response and ticketing workflows — not remain in a detection silo. Integrations with platforms like ServiceNow and Jira help teams take faster response actions and close the loop between security and IT operations.
- **Ensure that response is grounded in network visibility.** NDR and firewall integrations are foundational to understanding lateral movement, detecting covert activity, and enforcing containment. Buyers value XDR solutions that can act — not just observe — across key traffic and control points.
- **Expect enrichment to improve decision confidence.** Threat intelligence integration supports detection fidelity and faster triage. Buyers expect enrichment with reputation data; threat, tactics, and process (TTP) mappings; and threat campaign context to improve prioritization and reduce false positives.

FIGURE 2

Top Barriers to XDR Adoption

Q. What are the biggest challenges your organization faces in adopting extended detection and response?



n = 624

Base = all respondents

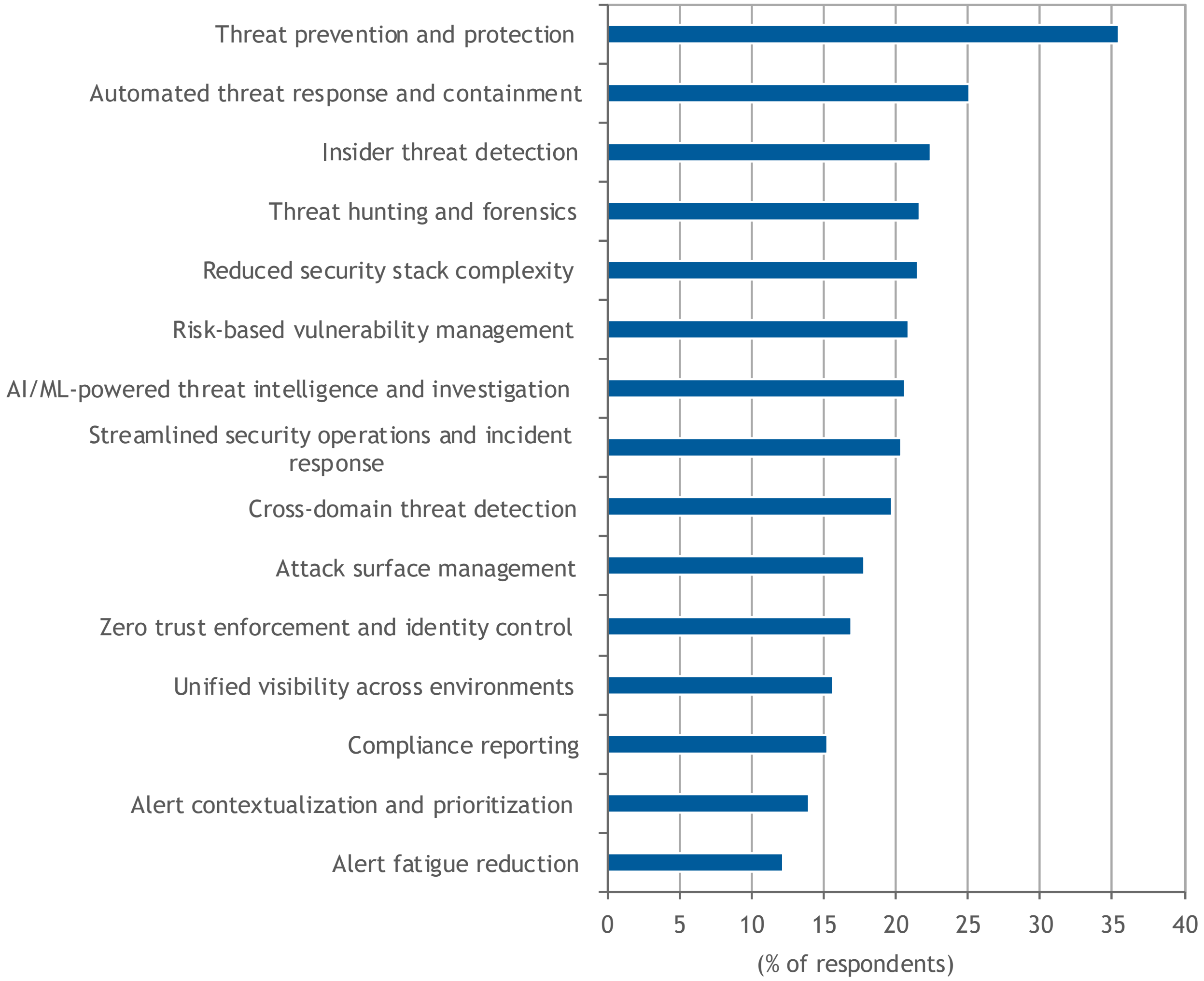
Note: Multiple responses were allowed.

Source: IDC's *End User XDR Perception — Cloud-Native XDR and Artificial Intelligence Security Analytics Survey*, June 2025

FIGURE 3

Most Important Use Cases for Extended Detection and Response Solution

Q. What are the most important use cases for your organization's extended detection and response solution?



n = 624

Base = all respondents

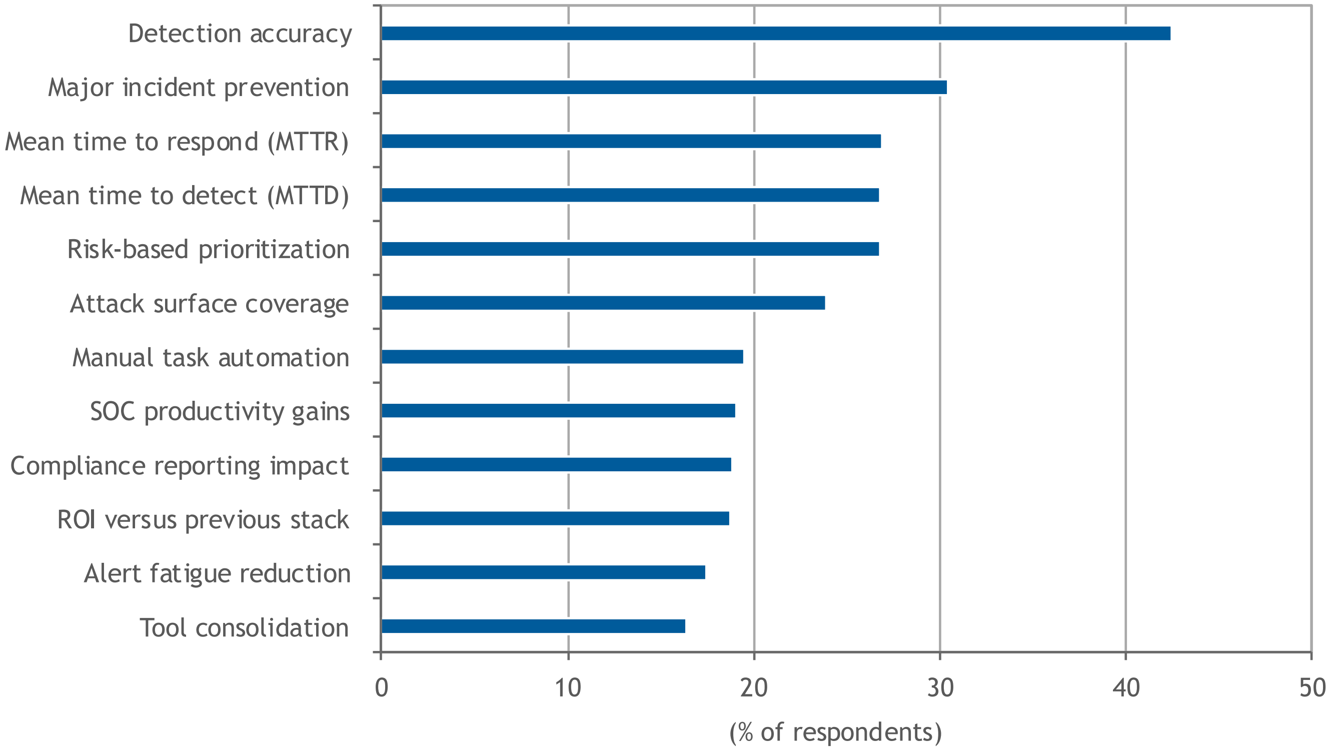
Note: Multiple responses were allowed.

Source: IDC's *End User XDR Perception — Cloud-Native XDR and Artificial Intelligence Security Analytics Survey*, June 2025

FIGURE 4

Design for Measurable, Outcome-Driven Security Performance

Q. How does your organization measure the effectiveness of your extended detection and response solution?



n = 624

Base = all respondents

Note: Multiple responses were allowed.

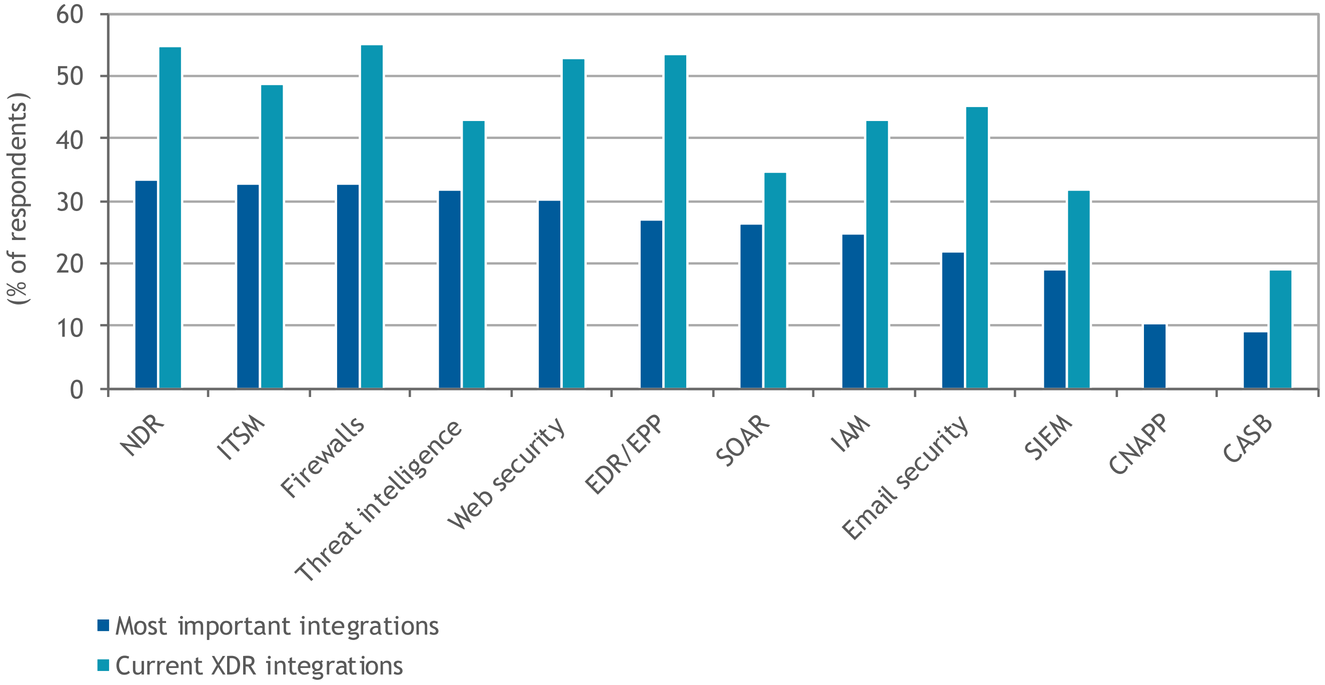
Source: IDC's *End User XDR Perception — Cloud-Native XDR and Artificial Intelligence Security Analytics Survey*, June 2025

FIGURE 5

Security Tools Integrations: Most Important Versus Current XDR Integrations

Q. *Which of the following security tool integrations are most important for your organization's extended detection and response solution?*

Q. *Which security tools does your current extended detection and response solutions integrate with?*



n = 624

Base = all respondents

Note: Multiple responses were allowed.

Source: IDC's *End User XDR Perception — Cloud-Native XDR and Artificial Intelligence Security Analytics Survey*, June 2025

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Sophos

Sophos is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide extended detection and response software.

In late October 2024, Sophos announced its plans to acquire Secureworks (see *Sophos Plans to Acquire Secureworks: The Bid for the Mid and Big Time,* IDC #IcUS52693524, October 2024), and the transaction was completed in February 2025. The reason this is relevant to this study is that Sophos is replacing the Secureworks endpoint EDR agent with Sophos XDR and integrating the Secureworks Taegis XDR platform, including its back end and user interface, into Sophos Central. IDC is evaluating the Sophos solution as it is offered today.

A brief summary of why Sophos acquired Secureworks helps explain Sophos' broader XDR and MDR strategies. First, Sophos has always had a primary focus on small and medium-sized businesses, while Secureworks generally focused on midsize through enterprise markets. The Secureworks Taegis XDR is a freestanding platform used in large businesses. In August 2024, Secureworks announced its ITDR solution, Taegis IDR, which scans an organization's environment for identity vulnerabilities and misconfigurations while providing dark web intelligence to detect compromised credentials — an example of a capability Sophos did not have. Last, Sophos calculated it would be ahead in terms of GenAI and soon-to-be agentic AI by combining forces with Secureworks data scientists and in-house capabilities than it would have been by developing on its own.

Key platforms considered in this profile are Sophos XDR, managed detection and response, extended data retention, ITDR, NDR, email security, and NGFW. Sophos and Secureworks have many integrations partners; Sophos has 350 bidirectional integrations. The degree to which Taegis XDR has been integrated, to our understanding, is fair to consider, but road map items, even if apparent, are not counted.

Strengths

Here is where IDC believes Sophos has notable capabilities in XDR:

- **Sophos is viewed favorably in terms of the protections it offers.** Key protection technologies included as standard features on the endpoint are host-based firewall and IDS/IPS, device control, DLP, antimalware scans, and encryption.
- **Sophos provides a continuous monitoring feature called Sophos Account Health Check.** Health Check enables customers running Sophos Endpoint and Sophos Server Protection to identify and address configuration issues with their Sophos-protected devices. Accessed through the Sophos Central platform, the Health Check performs checks across: vulnerabilities, identity posture, number of devices where protection is installed, tamper protection, policy settings, and exclusions (the number of devices not in any compliance). The anti-tamper

feature is especially compelling as it will provide protection even if an adversary has obtained admin permissions. Health Check also monitors configuration drift.

- **Colloquially known as "Shields Up," Sophos' Adaptive Attack Protection was introduced in 2023.** Adaptive Attack Protection automatically enforces certain protections if there is evidence of a "hands-on-keyboard attack." This approach minimizes the attacker's ability to act further, disrupts the attack, and provides time for security teams to respond. Examples of countermeasures include pushing any C2C IP or malicious domain detected to the Sophos firewall as part of a threat feed, monitoring file or registry name changes, forcing multifactor authentication, and isolating endpoints.
- **Sophos offers a various range of NDR detections on its platform.** Pertaining to NDR, the session risk analysis engine offers detections such as packet entropy, indication of a domain generation algorithm (DGA) created by a botnet, and precursors to specific attacks such as Cobalt Strike. Sophos also offers native detections for O365 and AD. In addition, Sophos NDR can see an anomaly if an end user initiates unauthorized access to an application.
- **The way Sophos uses AI/ML to find alerts is also interesting.** Not only are there fewer alerts, but the alerts are also prioritized. A 1-10 risk score is calculated, and severity of 6 or higher warrants further examination. To create probabilistic scoring, Sophos assigns a Producer Consumer Ratio (PCR) to identify upload/download activity of a flow. In addition, Sophos marks remote public IP range connections as "popular" or "unpopular" based on the entity of the customer's private IP device activity. The Cluster Severity Scoring engine then leverages this information when calculating the overall threat score.
- **Sophos has immediate response mechanisms to thwart ransomware.** CryptoGuard technology allows Sophos to locally recover end-user files and undo files and registry changes, a rollback feature. Sophos is also integrated with Veeam to offer data protection and recovery. Sophos X-labs threat intelligence has TTPs going back to 2011 if needed for additional investigation.
- **Sophos has its own data lake.** Data is labeled and normalized at the time of ingestion in the data lake. Sophos has a custom query language designed for fast, flexible threat hunting and investigation across endpoint, network, cloud, and third-party telemetry. It supports advanced filtering, time-based queries, powerful operators, and regex functions, making it accessible to analysts with varying levels of expertise. Note, if there is an indicator of compromise (a malicious IP, application log, malware signature, etc.), the IoC can be searched for *anywhere* on the data lake. To enable search, Sophos has sensors that it deploys in its data lake.

- **Sophos has multiple ingestion methods for cloud telemetry.** Syslog data collectors are supported in AWS, Azure, and GCP. In Azure, there is a direct ingestion from Event Hubs and log data can be pushed to blob storage. For AWS S3 Access Points, there is not a collector; however, there is continuous log collection at the source.

  The Sophos XDR offers comprehensive monitoring of Kubernetes environments through Cloud Workload Protection, enabling detection of malware, exploits, and anomalous behaviors in container workloads. Additional cloud protection includes real-time visibility into AWS, GCP, and Azure, and it has the Cloud Series Firewall to enforce policies for ingress/egress into cloud environments.
- **Incorporating Secureworks Taegis helps Sophos with identity detection and response.** Sophos has an Identity Risk Posture dashboard that charts users, groups, devices, and apps, which identifies the top risky users and provides an overall company identity risk score. Sophos Managed Risk pairs attack surface visibility and risk assessment with risk monitoring and threat response. Formal integrations with Entra ID and O365 add telemetry, which allows Sophos to track identities through various layers such as in the cloud, in email, or identity logs.

  Sophos XDR also supports a wide range of response actions to enable response actions that are specifically targeted at identity use cases such as resetting passwords, locking accounts, resetting MFA factors, resetting sessions, and disabling accounts across multiple IAM providers.
- **The Sophos ecosystem support for XDR is substantial.** In this case, this is meant as a dual meaning. First, Sophos has an enviable list of formal IT and security integrations. In firewalls alone, Barracuda, Check Point, Cisco, F5, Forcepoint, Fortinet, Juniper, Palo Alto Networks, SonicWall, Ubiquiti, and WatchGuard are already integrated, and the integration for SIEM, IAM, endpoint, web/email, NDR, threat intelligence, SOAR, and IT system management are similarly robust. To normalize logs, if a parser does not exist, an end user can customize one.

  Sophos boasts 25,000+ channel partners, 32,000+ MDR customers, 300,000+ endpoint customers, and 300,000+ firewall customers. Sophos products have been created with the managed security providers in mind. MSPs often fill the gap between local businesses that need cybersecurity and expertise that helps them find the right tooling and support.

Challenges

These are the challenges that IDC sees for Sophos in XDR:

- **Sophos has not gained much traction in the enterprise market.** This may be a chicken-and-egg argument where Sophos may have enterprise-scale products but missed a window in EDR, or it may be that its XDR approach is not scaling to enterprise or simply not resonating. The Secureworks acquisition over time may prove to be its gateway.

- **While Sophos has achieved several important global certifications, it does not monitor configuration drift.** This is a desired feature, and it would help clients return or reimage the device to its original state of innocence.
- **Sophos made its AI Assistant generally available in February 2025.** Sophos XDR has several GenAI capabilities integrated into it. However, most of the industry had a formal AI Assistant available to customers in mid or late 2024.

Consider Sophos When

Sophos has a contemporary approach to XDR. If a customer has an existing web/email platform, a specific next-generation firewall, or endpoint provider it uses, the Sophos XDR can accommodate its integration noting that Sophos-native capabilities in XDR are strong. The dashboards offer a comprehensive MITRE ATT&CK Alert Heatmap and different viewpoints based on personas are provided. A Sankey chart explains the alert and investigation flow. Sophos can also provide observability for mobile, OT, and IoT environments. Sophos offers a comprehensive set of automated responses.

Sophos appliances have an impressive list of certifications. Key certifications include CIS Security Controls, PCI DSS, HIPAA, GDPR, NIST Cybersecurity Framework, NIS/NIS 2 Directive, ISO/IEC 27001:2022, The Ohio Data Protection Act, and NIST SP800-171. Interestingly, Sophos does not have FedRAMP certification.

Sophos has an international presence, and its ecosystem is designed to empower businesses of all sizes and all types. Cybersecurity novices, intermediate users, and experts will gain value from the Sophos XDR platform.

APPENDIX

Reading an IDC MarketScape Graph

For this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here, and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed. IDC does not separate XDR revenue from EDR revenue if the product has the same SKU. To estimate XDR revenue, IDC used one-third of EDR/EPP revenue and/or any dedicated revenue reported as XDR.

Please keep in mind that IDC extended a request for information (RFI) in late March, asked for customer references and vendor demos in April through June and set a cutoff date of July 4, 2025, toward counting capabilities as generally available. Vendors were free to discuss road map items but if these were not GA, they did not count toward the formal scoring. (Note: The 18 vendors did have a chance to review content and make formal editing suggestions; as did the Vendors to Watch section.)

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

On how this research came about, in October 2024, IDC was almost certain it would create an XDR vendor assessment. IDC developed an XDR Survey Kit for vendors and then asked them their opinion of what XDR was and how we should develop the survey. Different syndicated research firms believe that XDR is exclusively an endpoint detection and response and endpoint protection platform providers with technology. In forming this study, EDR technology is wildly important to the fabric of XDR, however, the ability to find threats as they emerge in the cloud or on premises provides an opportunity for platforms/solutions that combine multiple sources of telemetry to chain alerts and find solid indicator of compromise. In addition, there is a certain pragmatism in this study. Vendors like Cisco and Darktrace are competing for the same dollars and clients that CrowdStrike and other EDR/EPP vendors try to win by expanding to an XDR solution.

In March 2025, the vendor list was further narrowed for formal inclusion into the study. In May 2025, IDC sent a survey to XDR end users in the United States and priority markets in Europe.

IDC asked vendors to provide a live demo session, provide two customer references, and fill out a formal request for information. Not every vendor was perfect, but the demands on the vendors are intense in this process. IDC could not be more thankful to the vendor community.

Market Definition

The definition for XDR is evolving. Concisely, IDC defines XDR as an API-enabled platform that ingests and correlates telemetry from various sources to detect cyberattacks.

As of now, the following features are found on an XDR stack:

- IDC never thought it would say this, but we could make the argument that the acronym should be pXDR (prevention and XDR). For XDR, IDC does not expect a comprehensive suite of vulnerability and exposure management capabilities. However, ASM and some detections based on policy or zero trust principles provide higher-quality alerts and help reduce the blast surface.
- The platform must have continuous visibility of endpoints through either a direct agent on the machine and a runtime executable or an OpenAPI connection to the platform for endpoint detection and response. The EDR is needed for the most rapid visibility possible, which is IOC of PowerShell commands, memory corruption, or performance issues that are not network related.
- The platform must include a log management backplane. EDR results must be aggregated and sent to the rest of the network through either SIEM and private cloud or an IaaS (public cloud) to match IoC across the hybrid network and then for forensic investigation.
- Becoming increasingly more important is search capability that extends into SIEM, various data lakes, and public cloud containers. While XDR vendors' search capabilities do not have to match that of SIEM, an XDR platform should be able to match and analyze what they see as either malware or compromised domains from a specific environment with what is on other environments across their entire digital estate.

- Security orchestration automation and response (SOAR) is necessarily included on the platform. The SOAR generates a workflow and advises or initiates ephemeral and permanent responses to incidents.
- The platform must provide contextual awareness including detection, containment, and recovery strategies. The platform must be able to describe what prompted an alert, what the blast radius is, and provide strategies on how to reduce the attack surface.
- User behavioral analytics is an essential part of the platform. UBA is designed to be self-learning and consistently wizening. UBA establishes statistical baselines for every entity within the network and the baseline relationships between devices within the network. UBA is one way to understand how devices are connected and provides the ability to reset devices back to the network if devices need reimaged.
- Network detection and response is a component piece. NDR is the set of technologies that look for user port anomaly, impossible travel and other IP and domain connectivity irregularities, evidence of C2C beaconing activity, unusual routing, and other internet session anomalies.
- Web/email is ingested as another way to correlate anomalies. Phishing remains an important access method for the adversary.
- External threat intelligence has become a valued feature of XDR. The proliferation of cybergangs and the soft layer between them and adversarial nation-states is necessitating that when the context is added to full packet collection or, more likely, metadata collection, there is a way to cross-reference the discovered adversarial tactics, techniques, and common knowledge (ATT&CK) against who most likely is the threat actor.
- Extensibility to hybrid architecture is universal. An XDR platform must include visibility for on-premises networks as well as for the leading public cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) and virtual private clouds (VPCs).
- For each detection capability, response is its necessary complement. An XDR solution should have immediate response and adaptive defenses that rise to the conditions caused by an exploit and against an active breach.
- Last, IDC believes an XDR solution should have two post-detection and response process mechanisms. First, an automation should occur that tells the IT/security team if a patch did get installed or a firewall rule was adopted. Second, the XDR solution should be able to tell if a security environment is getting safer and more efficient over time.

In this IDC MarketScape, consideration was given to specific capabilities around detection and response of use cases such as ransomware, phishing, and tools evasion. In addition, visibility and ingestion options that lead to detections from firewall logs, data loss prevention concepts, file-integrity management, or other ITSecOps platforms that could lead to better visibility, detection, or quicker responses were also considered in the scoring.

Market Analysis

Often cybersecurity improves when specific point products could make detections that were otherwise invisible. However, these point products often revealed the same insight. With point products such as web/email defense, NDR, EDR, and other types of defenses, the number of alerts themselves became problematic (and, of course, remain problematic).

For instance, an endpoint detection and response platform found that 30 servers have generated an alert. At this point, we do not know if this alert is based on temporary conditions such as a power fluctuation, a specific application, a type of OS or user group.

To better understand the alert, security teams would incorporate the perspective and context of NDR to help determine what type of threat is occurring. Threat intelligence could also be included to determine what the motivation of an attack is or at least what type of damage an exploit could cause. Therefore, XDR was conceived as a quick detection technology that could find IoC before formal processing in the SIEM (noting the concept of the SIEM will come up again).

This facile idea of XDR is reasonable, and it constitutes the core of what XDR is today — however, XDR was going to expand in two ways. The first area of expansion was the integration of other technologies into XDR. Web/email security is now considered an important part of XDR because web/email is still a point of ingress/egress for the adversary. Security orchestration automation and response capabilities are necessary for artifact collection and alert correlation capabilities. Certain inputs such as firewall logs are useful, but optional. The Market Definition subsection includes a comprehensive list of capabilities that an XDR platform/solution should have.

The second area of expansion is visibility into public clouds. Public cloud is how Amazon Web Services, Microsoft Azure, Google Cloud Platform, IBM Cloud, and Alibaba are referred to although these cloud service providers can also offer private data clouds. Public cloud hosts applications can be used for storage, host DevOps containers, and be used for virtual servers. Heterogeneous networks are common; most businesses use two or more public clouds. Businesses gain efficiency by using a combination of on-premises and public cloud resources; however, its attack surface becomes that much larger. The modern attacker knows this and can gain a foothold anywhere in each network and daisy-chain their way across different parts of the network. With time and persistence, an adversary, for instance, could find their way into an unexposed S3 bucket and advance to an on-premises directory.

As a technology platform, XDR has three challenges. The first is that it has to offer value that EDR, SOAR, and next-gen SIEM cannot. The second challenge is that it has to be scaled with the horizontal and vertical development of a business' network — if networks include more OT, IoT, and various cloud environments, the XDR has to create a visibility and detection and response plane. The last challenge is that XDR has to be the final guarantor that a remediation successfully took place and did in fact improve the hygiene of the network.

LEARN MORE

Related Research

- *How Does Agentic AI Adoption Vary by the Size of the Organization and Overall* (IDC #US53747025, August 2025)
- *Worldwide SOAR and Firewall Automation Forecast, 2025-2029: Automation at the Intersection of AI, Integration, and Zero Trust* (IDC #US52051225, August 2025)
- *Worldwide Network Detection and Response Forecast, 2025-2029: Providing Protection for the Network Proper and the Network Edges* (IDC #US52051025, July 2025)
- *Microsoft's SFI: Shedding the Old (Attack Surfaces) to Prepare for the New (Threats)* (IDC #lcUS53367525, May 2025)
- *Vishal Rao Will Lead Both Trellix and Skyhigh Security — Marking Yet Another Strategic Shift for These Companies* (IDC #US53213225, March 2025)
- *Microsoft Security Copilot Takes Its First Steps into Autonomy: AI Agents Are Both Boring and Appropriate* (IDC #lcUS53281425, March 2025)
- *Sophos Plans to Acquire Secureworks: The Bid for the Mid and Big Time* (IDC #lcUS52693524, October 2024)
- *North American Security Tools and Vendor Consolidation Study: NDR, SOAR, TI, and XDR* (IDC #US52303824, June 2024)
- *Elastic AI Assistant Shows What an AI Assistant Can Become* (IDC #US50211623, August 2023)

Synopsis

This IDC study discusses the concept of extended detection and response (XDR) that started to gain traction in late 2017. This was a specific time in cybersecurity as user behavioral analytics (UBA) became an enhancement to machine learning. UBA had a profound effect on endpoint platforms and on network detection and response (NDR) concepts. UBA meant indicators of compromise (IoC) aside from static malware signatures and explicit rules violations established in detection and response filters became possible.

XDR expanded in two different ways. The first area of expansion was the integration of other technologies into XDR. Web/email security is now considered an important part of XDR because web/email is still a point of ingress/egress for the adversary. Security orchestration, automation, and response (SOAR) capabilities are necessary for artifact collection and alert correlation capabilities. Certain inputs such as firewall logs are useful, but optional.

The second area of expansion is visibility into public cloud. Heterogeneous networks are common; most businesses use two or more public clouds. Businesses gain efficiency by using a combination of on-premises and public cloud resources; however, its attack surface becomes that much larger. The modern attacker knows this and can gain a foothold anywhere in each network and daisy-chain their way across different parts of the network.

This has a powerful impact on what XDR is and where it is going. At first, XDR was designed to reduce the number of alerts and provide the proper context for investigations. Now the expectation is to identify a campaign, create countermeasures, and respond quickly and appropriately.

"XDR gathers and correlates telemetry from multiple security appliances. However, EDR, NDR, and threat intelligence remain the staples of XDR," notes Chris Kissel, vice president, IDC's Security and Trust Division. "XDR though is called upon to find the first point of origin of a potential attack, determine what the best ephemeral reply and formal remediation is, and begin the process to make the network whole again. This is a tall order, but the promise of agentic AI should continue to improve all aspects of prevention, detection, and response in business networks."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice