ISSN: 2581-3404 (Online) IF: 5.86 (SJIF)
IJIRTM, Volume-10, Issue-6, November-2026

Extended Detection and Response (XDR): A Review of Concepts, Architectures, Capabilities, and Open Challenges

Jigyansh[1], Vikram Pawar[2], Dr. Shakti Arora[3]
Student, Department of Computer Science and Engineering (Cyber Security) [1,2]
Kurukshetra University, Kurukshetra, India[1,2,3]
Professor[3]

Abstract. *Since its emergence in the late 2010s, Extended Detection and Response (XDR) has been one of the most important categories in security operations. It offers the promise of unifying endpoint, network, identity, email, and cloud workload telemetry, correlating it into coherent incidents and enabling coordinated response. This paper covers the origins and definitions of XDR, its reference architecture, the native, open and hybrid deployment models, its relationship to EDR, SIEM, SOAR and MDR, the role of machine learning and agentic AI, and the main obstacles to adoption including data management cost, correlation quality, vendor lock-in and definitional ambiguity.*

Keywords: Extended Detection and Response, XDR, EDR, SIEM, SOAR, security operations, Agentic AI.

Introduction

Security operations centers (SOCs) have been accumulating point products for years: endpoint agents, network sensors, email gateways, identity tools, cloud security services. Each one creates its own alerts in its own format. Analysts are forced to hop between consoles to try and understand what happened, slowing down investigation and creating visibility gaps across the enterprise (see the ResearchGate paper "XDR: The Evolution of Endpoint Security Solutions").

This is what XDR came into being as a solution for. Analysts in the industry have called this technology-based solution a pre-built integration of multiple sources of security telemetry with analytics and responses (S&P Global 451 Research). As stated in the Gartner Market Guide, XDR "provides security incident detection and response" (Wikipedia, "Extended detection and response").

Interest was quite high but knowledge was low. According to a survey published by Dark Reading, only 24% of the participants stated that they had a very good understanding of XDR technology, while others gave definitions that were correct but rather vague. The article credits this lack of clarity to the lack of a standardized product. Another survey sponsored by a vendor showed that the participants could not agree on what XDR is made up of despite the high level of interest (OpenText, 2022).

This paper has four aims:

1) Clarify what XDR is and is not.
2) Describe the common architecture and its variants.
3) Review how AI and machine learning are used in XDR, including recent agentic approaches.
4) Identify the technical and organizational challenges that limit its effectiveness.

Background and Evolution

A. From antivirus to EDR

Endpoint Detection and Response (EDR) collects and correlates activity across endpoints, giving defenders host-level visibility and response actions such as isolation and remediation. It addressed the limits of signature-based antivirus but remains centered on the host.

B. From EDR to XDR

XDR has been presented as the future of EDR. The scope of detection, analysis, and remediation is extended from endpoints to networks, servers, cloud workloads, and other areas. The basic description is that EDR protects the endpoint while XDR protects the entire environment ("Understanding the Difference Between EDR, SIEM, SOAR, and XDR"). Typical sources of data used by XDR include identities, emails, and applications. For instance, Microsoft Defender XDR integrates data from endpoints, emails, identities, applications, and the cloud ("Understanding the Difference Between EDR, SIEM, SOAR, and XDR").

C. Why the category emerged

Three pressures are usually cited:

- Alert fatigue and tool sprawl. Analysts are flooded by alerts coming from isolated tools.
- Gaps in investigation capabilities. According to initial studies in the market, a significant number of businesses were unable to investigate some of the alerts, leaving the threat persistent (S&P Global 451 Research).
- Lack of staffing and expertise. Advanced implementations of SIEM and SOAR solutions require skill and effort that many teams don't have.

Reference Architecture

Although implementations differ, most XDR platforms share a layered structure (Fig. 1).

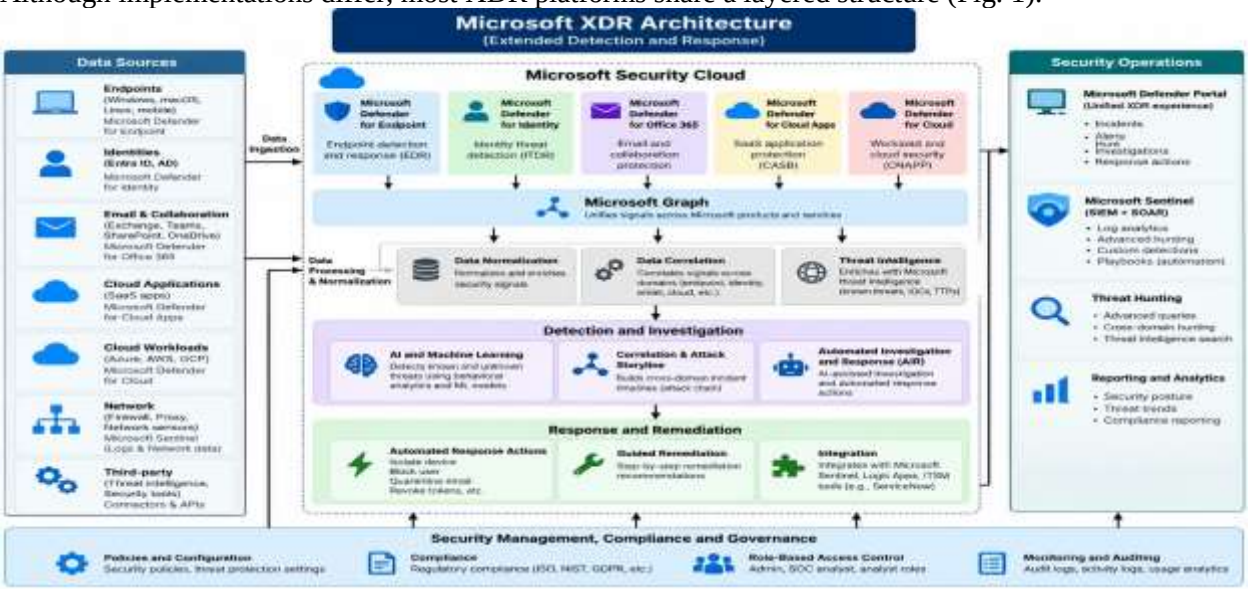


Fig. 1. Layered XDR reference architecture (Microsoft XDR example).

A. Native, open, and hybrid models

Vendor approaches in market research fall into three categories (Frost & Sullivan):

- Native (single-vendor) XDR integrates information from the vendor's security stack. It ensures a high integration level, an easy procurement process, and good data quality at the expense of flexibility.
- Open (multi-vendor) XDR serves as a layer of integration and analytics across diverse tools. The key task here is to normalize telemetry from various sources into a single data model. Such attempts as OCSF should be mentioned in this regard (Deepwatch).
- Hybrid XDR includes both categories, with a lower level of native integration and customer choice of sources.

The criteria that determine the choice of a model are the diversity of the tool portfolio, acceptance of lock-in, the level of SOC maturity, and the total cost of ownership including the costs of integration (Deepwatch). In view of the interest of the source company in the open approach, its recommendations should be taken as opinions.

XDR In Relation to Adjacent Technologies

Table I summarizes how XDR relates to EDR, NDR, SIEM, SOAR and MDR.

TABLE I: XDR IN RELATION TO ADJACENT TECHNOLOGIES

Technology	Primary role	Relationship to XDR
EDR	Endpoint detection and response	XDR expands this into other domains
NDR	Network traffic analysis	A common XDR telemetry source
SIEM	Log aggregation, compliance, long-term retention	Complementary; SIEM is good at log management, compliance, and retention, while XDR is focused on operational detection and response (Gruve)
SOAR	Playbook-driven automation across tools	XDR is referred to as "SOAR-lite", providing simple actions on connected tools (SentinelOne)
MDR / MXDR	Outsourced monitoring and response service	Provides XDR technology as a managed service

Several sources claim that XDR is not a complete replacement for SIEM or SOAR yet. One analysis claims that it does not have SIEM compliance features or SOAR orchestration capabilities (Expert Insights). SIEM or SOAR vendors claim the opposite — XDR automation only provides micro-automation outcomes (Swimlane), while some open XDR vendors claim that their platforms can replace a standalone SIEM for midmarket companies (Stellar Cyber). These arguments represent commercial interests and no independent comparison study was found within this review.

Managed XDR is a major adoption route. The 2022 OpenText survey found that many organizations were engaging managed providers, and it reported that outsourcing management and monitoring was an attractive way around perceived XDR complexity.

ANALYTICS: CORRELATION, MACHINE LEARNING, AND AGENTIC AI

A. Correlation

Correlation connects discrete events to stories of an attack. This concept, according to the Purdue CERIAS 2026 poster, entails transforming isolated reports of alerts into complete attack stories to enable analysts to view multi-stage attacks that might otherwise show up as dozens of unconnected alerts of low severity.

Correlation is what gives XDR its value, as it must provide analysts with actionable information from detections and correlations and not just a searchable repository of stored data (Stoner, MSSP Alert).

The GraphWeaver paper (arXiv:2406.01842) identifies large-scale correlation as a difficult problem and describes several challenges. They include handling false correlations, preventing over-correlation resulting in "black hole" incidents due to merging of uncorrelated alerts, and leveraging threat intelligence and domain knowledge for entity correlation such as IP addresses and files. This source is one of the scarce sources in this review that views XDR correlation as a research problem.

B. Machine learning

ML is explained by vendors and educational literature as being used in XDR to do behavioral baselining, anomaly detection, automated threat hunting, and predictive analytics by using supervised, unsupervised, and semi-supervised learning. The benefits claimed to be achieved from ML in XDR include reduced false positives and faster detection. The benefits claimed are usually backed up by product literature but not evaluation studies.

C. Rule-based limits

According to the whitepaper published by D3 Security, XDR correlation is mostly rule-based and associated with threat behaviors tied to MITRE ATT&CK, and thus reaches its peak in investigation. It is also noted that top-tier platforms scored well in MITRE ATT&CK Evaluations. This source further adds that cross-vendor correlation is never equal to native correlation in open XDR. Considering that the author sells autonomous SOC technology, this criticism must be taken into account.

D. Agentic AI

The literature from 2025 to 2026 treats agentic AI as the next level up from XDR:

- Industry predictions call for the transition of SOCs from human triage to human-in-the-loop AI solutions, where the analyst moves into supervision of AI (Cybersecurity Ventures, predictions 2026).
- Vendors speak about the incorporation of standalone SOAR into integrated open XDR platforms where agents are responsible for investigating threats and planning responses without the need for hand-written playbooks (Stellar Cyber).
- Academia is starting to catch up. In the poster at Purdue, an agentic pipeline is shown in parallel to Microsoft's managed XDR with subagents for correlation, analysis and rule tuning. It claims that the pipeline finds multi-day campaigns out of fragments created by the managed service in real enterprise alerts. This is a small-scale early example, yet it also shows that there are gaps in XDR correlation in practice.
- Skeptics point out that previous solutions labeled as "AI SOC" were still human-in-the-loop and that generative summarization is different from agents that take responsibility for solving the incident (as cited in the references).

Market and Adoption

Predictions made by market research vary significantly depending on the scope and the year of publication:

- MarketsandMarkets predicts growth from USD 10.98 billion in 2026 to USD 38.09 billion by 2031 (CAGR of 28.2%). Open or multi-vendor XDR is expected to have the highest growth rate (30.3% CAGR), whereas native XDR will take up the biggest market share. North America will be the market leader in 2026 with 36.9% of the market.
- A different prediction from MarketsandMarkets shows USD 1.7 billion in 2023 growing to USD 8.8 billion by 2028 (CAGR of 38.4%).
- The same company defines the market as consolidated, where Palo Alto Networks, Cisco, CrowdStrike, IBM, and Microsoft together own 50 to 60% of the market.

These forecasts should be considered indicative. They originate from commercial research whose methodology is not known, and even the categorization of XDR into types distinct from EDR, SIEM, and MDR is somewhat vague. The trends discussed include convergent security technologies, cloud-native solutions, SOAR integration, and increasing autonomy.

Challenges Aand Limitations

A. Data management and cost

Cost is an issue when it comes to ingesting, parsing, enriching, normalizing, archiving, and analyzing telemetry data of many types and cardinalities (SentinelOne). There is an argument that the issue facing adoption is not how high the goal of detection is set but rather the costs of scale, fragmentation, and retention of telemetry (NHIMG summary of SentinelOne). Consumption-based ingestion cost models make prediction very challenging (Fitgap, on Cortex Data Lake).

B. Vendor lock-in and coverage gaps

The majority of native XDR products are bound by their own technology stacks, which limits the amount of data that can be correlated and creates lock-in with expensive tools (eWEEK). Companies implementing native XDR in a heterogeneous environment run the risk of coverage holes and restricted future procurement (Deepwatch). Open XDR prevents lock-in but introduces integration challenges.

C. Correlation quality

Both under-correlation (fragmented incidents) and over-correlation (merged “black hole” incidents) have been identified as issues (GraphWeaver; Purdue CERIAS). Cross-vendor correlation tends to be described as less effective than single-vendor stack correlation.

D. Definitional ambiguity and overclaiming

The term is used broadly among security vendors, and buyers are faced with inconsistent terminology and overlapping statements (Hexnode). It is claimed that many solutions referred to as XDR only correlate a small portion of telemetry sources and provide an extended response only within their own ecosystem (Swimlane).

E. Operational maturity

XDR lowers but does not eliminate the necessity for skilled personnel. The amount of analyst work is proportional to the size of the detection surface, as stated in the critique from D3 Security, and tuning of rules and models continues to be an ongoing process (Gruve).

F. Evidence quality

The most important limitation of this review is that few independent, quantitative evaluations exist. Claims about reduced false positives and mean time to respond are mostly vendor-reported.

Evaluation Considerations for Practitioners

From the sources listed above, a good XDR evaluation should include the following:

1) Telemetry quality and coverage: what sources are natively ingested, and to what depth.
2) Integration depth: whether third-party data is first-class or bolted on.
3) Correlation quality: run real-life multistage tests, and measure both fragmentation and over-correlation of incidents.
4) Response ability: evaluate the ability to respond the way you would evaluate detection.
5) Total cost of ownership: include ingestion, retention, and integration costs, not just the license fee (Hexnode).
6) Relationship with SIEM: make sure that compliance and retention needs are covered as well.

Future Directions

- Standardized schemas (e.g., OCSF) to make open XDR cheaper.
- Benchmarks for the quality of correlation, e.g., public data sets for multi-staged incidents. GraphWeaver-type research for graph-based correlation could be a first step.
- Human-machine operations with explicit criteria for when agents can act without approval.
- Cost-sensitive telemetry strategy that decides what to keep hot, what to tier, and what to drop.
- Focus on identity and cloud because XDR now covers more than just endpoints.
- Safety and robustness of autonomous response with error handling when containment is automated incorrectly.

Conclusion

XDR solves the genuine practical problem of disconnected systems and excessive noise in alerting. Its basic concept of correlating telemetry from across domains to form incidents and reacting in concert is solid and well incorporated into the products of security's biggest players. The proof, however, is less compelling than the hype surrounding it. Definitions differ, low-quality correlation is one of the issues mentioned in studies, data costs and vendor lock-in are relevant considerations too, and independent testing is rare. The most dynamic area is integrating XDR with AI agents, which shows promise although the work is still in an early stage.

References

Many of the references below are vendor and/or market research publications. Such references are noted wherever this affects their interpretation. Each reference should be checked and replaced or supplemented with peer-reviewed sources prior to formal submission.

[1] "GraphWeaver: Billion-Scale Cybersecurity Incident Correlation," arXiv:2406.01842 (author list to be added). [Online]. Available: https://arxiv.org/pdf/2406.01842

[2] Cheng-Yun King Yang, Christina Zhang, Max Chen, and Dongyan Xu, "An Agentic AI Pipeline for Enterprise Alert Correlation," CERIAS 2026 Symposium poster, Purdue University. [Online]. Available: https://www.cerias.purdue.edu/symposium/index.php/posters/year/2026/MYO-JHO

[3] S&P Global Market Intelligence (451 Research), "The Rise of Extended Detection and Response." [Online]. Available: https://www.spglobal.com/content/dam/spglobal/mi/en/documents/general/the-rise-of-extended-detection-and-response.pdf
[4] "XDR: The Evolution of Endpoint Security Solutions: Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future," ResearchGate (authors and venue to be added). [Online]. Available: https://www.researchgate.net/publication/354190628_XDR_The_Evolution_of_Endpoint_Security_Solutions_-Superior_Extensibility_and_Analytics_to_Satisfy_the_Organizational_Needs_of_the_Future
[5] OpenText, "The 2022 State of Extended Detection and Response (XDR)" (vendor survey). [Online]. Available: https://www.opentext.com/assets/documents/en-US/pdf/opentext-sb-2022-xdr-survey-en.pdf
[6] Dark Reading, "The Realities of Extended Detection and Response (XDR) Technology." [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/the-realities-of-extended-detection-and-response-xdr-technology
[7] Wikipedia, "Extended detection and response" (as cited by Gartner, 2023 Market Guide for XDR). [Online]. Available: https://en.wikipedia.org/wiki/Extended_detection_and_response
[8] MarketsandMarkets, "Extended Detection and Response (XDR) Market" (market research). [Online]. Available: https://marketsandmarkets.com/ResearchInsight/extended-detection-response-market.asp.
[9] MarketsandMarkets, "Emerging Trends in the XDR Market." [Online]. Available: https://www.marketsandmarkets.com/ResearchInsight/emerging-trends-in-extended-detection-response-market.asp
[10] MarketsandMarkets press release via PR Newswire, "XDR Market worth $38.09 billion by 2031." [Online]. Available: https://www.webull.com/news/15679066021168128
[11] Frost & Sullivan, "Global Extended Detection and Response (XDR) Growth Opportunities." [Online]. Available: https://store.frost.com/global-extended-detection-and-response-xdr-growth-opportunities.html
[12] SentinelOne, "Understanding the Difference Between EDR, SIEM, SOAR, and XDR" (vendor). [Online]. Available: https://www.sentinelone.com/blog/understanding-the-difference-between-edr-siem-soar-and-xdr/
[13] Swimlane, "XDR vs SIEM vs SOAR" (vendor). [Online]. Available: https://swimlane.com/blog/xdr-vs-siem-vs-soar/
[14] Gruve, "XDR Correlation." [Online]. Available: https://gruve.ai/in/?p=995376
[15] Deepwatch, "Open XDR" (vendor glossary). [Online]. Available: https://www.deepwatch.com/glossary/open-xdr/
[16] SentinelOne, "The Rise of Big Data: Solving Today's Challenges with SentinelOne XDR" (vendor). [Online]. Available: https://sentinelone.com/?p=45846
[17] NHIMG, "XDR data management at scale is the real adoption bottleneck." [Online]. Available: https://nhimg.org/articles/xdr-data-management-at-scale-is-the-real-adoption-bottleneck/
[18] eWEEK, "Why XDR Has Emerged as an Important New Security Trend." [Online]. Available: https://www.eweek.com/security/why-xdr-has-emerged-as-an-important-new-security-trend/
[19] Fitgap, "Cortex Data Lake" product analysis. [Online]. Available: https://us.fitgap.com/products/cortex-data-lake

[20] B. Stoner, “Everything About XDR Is Around Correlations, Not Hype,” MSSP Alert (sponsored). [Online]. Available: https://www.msspalert.com/native/everything-about-xdr-is-around-correlations-not-hype
[21] D3 Security, “The XDR Ceiling: Why Extended Detection and Response Stops Short of the Autonomous SOC” (vendor). [Online]. Available: https://d3security.com/resources/xdr-ceiling-autonomous-soc/
[22] Verus Corp, “How XDR Leverages Machine Learning to Enhance Security.” [Online]. Available: https://veruscorp.com/?p=23691
[23] Fidelis Security, “Machine Learning in XDR: A Cybersecurity Breakthrough” (vendor). [Online]. Available: https://fidelissecurity.com/?p=34726
[24] Cybersecurity Ventures, “Cybersecurity Predictions for 2026.” [Online]. Available: https://cybersecurityventures.com/cybersecurity-predictions-for-2026/
[25] Stellar Cyber, “Best XDR Solutions for 2026” and “Best Security Automation Tools for 2026” (vendor). [Online]. Available: https://stellarcyber.ai/learn/xdr-solutions/
[26] Hexnode, “How to Evaluate an XDR Vendor for Your Security Stack.” [Online]. Available: https://www.hexnode.com/blogs/?p=42485.