The Rise of Extended Detection and Response

As the threat landscape continues to become increasingly sophisticated and resources are routinely constrained, security teams are finding it harder than ever to build and maintain efficient and effective security environments. Often using numerous incompatible tools that don't easily share context, teams frequently toggle between consoles trying to manually correlate massive amounts of data. At best, these results are inconsistent; sometimes catching threats (but often too late) or missing them entirely as analysts sort through volumes of unprioritized and potentially inaccurate alerts. Without the right technology, even the most talented security team may see compromised levels of detection and response.

The right tools prioritize alerts and propel teams to act on them with confidence. This confidence comes from the ability to gather context from every corner of their environment and consolidate into a single view that is easy to explore and provides a dashboard that facilitates the ability to remediate threats quickly.

Extended Detection and Response (XDR) platforms strive to provide context from disparate threat intelligence sources so that incident detection and response is based on correlated and actionable data.

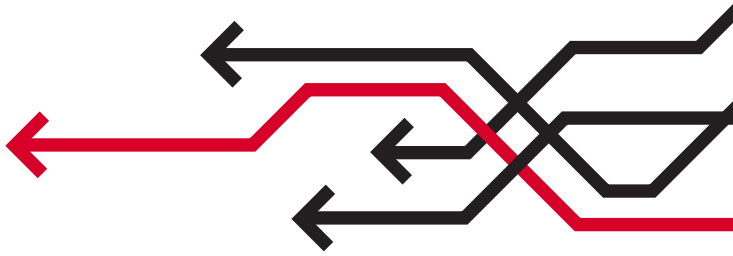
Only Cisco delivers on the promise of XDR today by unifying detection and response using what's already in a customer's environment so that threats can be detected across multiple vectors. Through Cisco's XDR platform approach, you can connect all of your telemetry and solutions seamlessly, rely on validated and correlated detections for better decision making, and accelerate response times.

Cisco's XDR solution is a unified detection and response approach with a built-in platform. It starts with our cloud-native platform, SecureX, which provides the central point for all integration. SecureX is built into all Cisco Security products, setting the foundation for our XDR approach by uniting our industry-leading Endpoint Detection and Response (Cisco Secure Endpoint) and Network Detection and Response (Cisco Secure Network Analytics) solutions.

Benefits with Cisco's XDR Approach

- Extends detection and response across security environments
- Deploys in any environment, regardless of vendor
- Normalizes and centralizes data efficiently
- Leverages machine learning and automation across the environment
- Facilitates proactive threat hunting and automated incident response

REPORT EXCERPT



Technology & Business Insight

Thought Leadership

June 2021

The Rise of Extended Detection and Response

Fernando Montenegro **Principal Research Analyst, Information Security**

Aaron Sherrill **Senior Research Analyst, Information Security**

Scott Crawford **Research Director, Security**

Extended detection and response (XDR) is a relatively new term for an approach to security operations aimed at empowering teams with the technology to detect threats across multiple vectors. XDR is gaining momentum with end users and vendors/providers and holds potential to be a disruptor for both groups.

The following is an excerpt from an independently published 451 Research report, "The Rise of Extended Detection and Response" released in June 2021.

To purchase the full report or to learn about additional 451 Research services, please visit https://451research.com/products or email 451sales451@spglobal.com.

451 Research

S&P Global
Market Intelligence

About the Authors

Fernando Montenegro

Principal Research Analyst, Information Security

Fernando is a Principal Research Analyst on the Information Security team at 451 Research, a part of S&P Global Market Intelligence. He is based out of Toronto, Canada. He has broad experience in security architecture for enterprise environments. He currently focuses on covering primarily the endpoint security and cloud security markets.

Aaron Sherrill

Senior Research Analyst, Information Security

Aaron Sherrill is a Senior Research Analyst for 451 Research, a part of S&P Global Market Intelligence, covering emerging trends, innovation and disruption in the Information Security channel with an emphasis on service providers.

Scott Crawford

Research Director, Security

Scott Crawford is Research Director for the Information Security Channel at 451 Research, a part of S&P Global Market Intelligence, where he leads coverage of emerging trends, innovation and disruption in the information security market. Scott is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Key Findings

- Customers indicate they continue to struggle with efficient security operations. On aggregate, only 54% indicate that they have a security operations center, while more than 90% indicate they can't investigate all the security alerts they receive on a typical day.
- Extended detection and response (XDR) rises as a potential approach to accelerate security operations outcomes – triage, investigations, incident response or threat hunting – while reducing efforts when compared with SIEM.
- Nearly 40 vendors are offering XDR capabilities aligned across three major themes: telemetry-centric, analytics-centric and services-centric.

Executive Summary

Introduction

Even before the COVID-19 pandemic, security teams – particularly those dealing with security operations workflows such as triage, investigations, incident response or threat hunting – were already dealing with ever-growing complexity in multiple dimensions. Modern attack patterns change, leveraging automation in combination with human actors to burrow deep within organizations. Technology platforms change with the rise of cloud-based environments and modern application development practices that emphasize shorter time to value. The broader penetration of IT services across the entire business brings more diverse initiatives, which are often being pursued in parallel by an increasing number of teams, each potentially using custom tooling that is exactly right for their jobs.

Amid all this, security operations teams struggle to make sense of multitudes of alerts, be it because they receive too many that end up being false positives or because the workflows they need to follow investigating the ones they do get are onerous and manual. Security operations is not an easy area to begin with and the increased demands don't make it any easier.

While analysts assigned to the specific tasks of triage, investigations or threat hunting may initially be looking at individual point products, the need to consolidate insight, analytics and response processes across security teams tends to lead toward security incident and event management (SIEM) systems for aggregating data from multiple sources. These systems, however, may not be designed to accommodate the nature of telemetry, analytics and processes arising from more modern techniques where visibility may be obtained from a variety of other sources beyond the logs that have long been the staple of SIEM.

Key industry vendors are positioning extended detection and response (XDR) as a new alternative to SIEM-centric architectures, or as a possible extension to SIEM investments. In either case, XDR purportedly provides operational benefits for customers with minimal effort. XDR is squarely aimed at security operations processes that have evolved beyond event centralization and triage. It often specifically targets investigations, incident response and threat hunting activities that draw analysts' attention out to the full reach of IT, wherever it may be found.

From the multiple conversations we've had on the topic, XDR is not clearly defined, often by design: For some it is the aggregation of data they already provide as independent products, sprinkled with additional insights derived from APIs, some machine-learning-enabled analytics, and a dash of automated responses. For others, it is a broader approach that provides efficiency gains in triage, investigations, incident response and threat hunting.

While definitions may vary depending on the source, we've settled on what we hope is a succinct, no-fluff definition for XDR:

Extended detection and response is a technology approach of providing pre-built integration of multiple security telemetry sources with analytics and response capabilities.

This report considers the factors influencing the development of XDR, makes considerations on composition and capabilities, highlights representative vendors and proposes aspects to consider as XDR evolves.

Methodology

This report includes observations on XDR trends derived from a combination of two key sources: numerous conversations and briefings with stakeholders – vendors and service providers both with and without specific product offerings or messaging around XDR, venture and investment professionals with interests in the space, and selected executive-level and technical-level practitioners at different organizations, among others – and the results from our various Voice of the Enterprise (VotE) surveys. The data is presented alongside our interpretation of these trends in the context of impact to different stakeholders and discussion of potential future challenges.

The report was also informed by custom research focused on XDR that the authors conducted in support of strategic advice provided to undisclosed stakeholders.

Reports such as this one represent a holistic perspective on key emerging markets in the enterprise IT space. These markets evolve quickly, though, so 451 Research offers additional services that provide critical marketplace updates. These updated reports and perspectives are presented on a daily basis via the company's core intelligence service, 451 Research Market Insight. Forward-looking M&A analysis and perspectives on strategic acquisitions and the liquidity environment for technology companies are also updated regularly via Market Insight, which is backed by the industry-leading 451 Research M&A KnowledgeBase.

Emerging technologies and markets are covered in 451 Research channels including Applied Infrastructure & DevOps; Cloud & Managed Services Transformation; Cloud Native; Customer Experience & Commerce; Data, AI & Analytics; Datacenter Services & Infrastructure; Information Security; Internet of Things; and Workforce Productivity & Collaboration.

Beyond that, 451 Research has a robust set of quantitative insights covered in products such as VotE, Voice of the Connected User Landscape, Voice of the Service Provider, Cloud Price Index, Market Monitor, the M&A KnowledgeBase and the Datacenter KnowledgeBase.

All of these 451 Research services, which are accessible via the web, provide critical and timely analysis specifically focused on the business of enterprise IT innovation.

For more information about 451 Research, please go to: www.451research.com.

This report cites data from the following 451 Research surveys:

- **Voice of the Enterprise: Information Security, Budgets & Outlook 2020** – This web-based survey was fielded during November and December 2019 among approximately 500 IT decision-makers and technology practitioners primarily based in North America.
- **Voice of the Enterprise: Information Security, Workloads & Key Projects 2020** – This web-based survey was fielded during March and April 2020 among approximately 500 IT decision-makers and technology practitioners primarily based in North America.
- **Voice of the Enterprise: Information Security, Organizational Dynamics 2020** – This web-based survey was fielded during June and July 2020 among approximately 450 IT decision-makers and technology practitioners primarily based in North America.
- **Voice of the Enterprise: Information Security, Vendor Evaluations 2020** – This web-based survey was fielded from August through November 2020 among approximately 400 IT decision-makers and technology practitioners primarily based in North America.

Table of Contents

2. Current Approaches to XDR

XDR provides threat detection and response capabilities that extend beyond the approach of single threat vector solutions such as EDR and NDR. XDR aggregates telemetry across the security stack, adding analytics and intelligence to interpret and correlate data and detect threats across the entire IT ecosystem.

With the usual caveats that categorization is seldom a clean-cut exercise and that some overlap is bound to occur, there's still a benefit to offering a segmentation of XDR offerings.

We are currently classifying vendors offering XDR in two distinct categories: product-centric vendors and services-centric vendors. The product-centric vendors are further segmented as 'telemetry-focused' or 'analytics-focused.'

Product-Centric, Telemetry-Focused

Favored by established security vendors, a product-centric, telemetry-focused approach seeks to unify different products and services from the same vendor into a single XDR 'platform,' sometimes complementing this with external data pulled via APIs.

The typical offering in this space will use the vendor's existing telemetry sources (endpoint, network, etc.), which are then complemented by a newer vendor-provided 'central analytics' capability of some sort to provide the user interface, integrations and more. This often means bringing in external data via APIs, with user identity data gathered from an identity provider being a common use case.

Having a unified stack from a single vendor can offer advantages, including tight integration of security tools, vendor consolidation, rapid XDR adoption and optimization of security technologies. However, because this approach requires significant dependence on a single provider, vendor lock-in is a potential drawback. To achieve the expected outcomes from XDR, security teams utilizing a product-centric, telemetry-focused XDR provider may find they need to rip and replace existing security controls and adopt a large portion of the vendor's proprietary tools and services.

This may not be immediately apparent in the early stages of XDR adoption as many organizations seek to upgrade to XDR with their current EDR provider to take advantage of adding points of telemetry that are missing from their security stack. However, gaining access to additional points of telemetry can mean sacrificing efficacy in certain areas if vendors have weaker product lines or gaps in their product portfolio. Although many product-centric XDR providers have aspirations to develop a more open approach to XDR, for now, a product-centric approach may be the best fit for organizations that have already built their security architecture around a single vendor or are shifting their security strategy and stack to a single integrated vendor.

Product-Centric, Analytics-Focused

The other product-centric approach is to focus on the 'analytics' side of the equation. Here, what the vendor is bringing to the table is its core 'central analytics' capability, which can then integrate with the existing security architecture and tools an organization has in place. This approach is more popular with newer market entrants that don't have a widely deployed customer base, choosing instead to count on the API integration with multiple data sources. As the market evolves, this is the approach that is more likely to be favored by existing SIEM vendors that choose to align themselves closer to XDR.

Analytics-focused XDR vendors tend to offer a broad catalog of pre-built, bi-directional integrations, providing security teams with visibility across a diverse set of security technologies and data sources and enabling automation that spans across tools from different vendors and platforms, often including cloud, identity, endpoint and network as key areas to support. In many cases, vendors are highlighting how their analytics capabilities include large amounts of machine learning (ML), scoring, threat intelligence and so on.

This analytics-centric approach is likely well-suited for organizations that have already invested in an array of security tools and, rather than make a choice of aligning to one strategic partner for security operations, prefer a best-in-class strategy of implementing different security technologies.

Services-Centric

A services-focused XDR approach can seem a bit like an oxymoron. There is often limited to no experience with the approach within a given security organization, so XDR requires teams to make significant investments in advanced security talent to cover 24/7 threat detection, investigation and response. A few vendors are promoting managed XDR as a new approach; however, MDR providers have offered XDR capabilities for several years, wrapped with managed services to help organizations scale and fill expertise gaps. Like XDR, MDR providers often take a product-centric or a telemetry-focused approach to their platform offerings.

A notable trend among MDR providers is the offering of their own core MDR platform without managed services, competing directly with emerging XDR technology providers. This may prove to be a competitive advantage for MDR providers in the XDR space. Offering an array of optional managed service levels to fit the unique needs of each organization, this strategy enables security teams to take an adaptive approach to threat detection and response. To counter this move by MDR providers, XDR vendors are increasingly partnering with MSSPs to deliver XDR as a managed service.

3. The Benefits and Drawbacks of XDR

Organizations are making significant investments in their cybersecurity programs. According to our VotE: Information Security, Budgets and Outlook 2020 survey, 90% of organizations are increasing security budgets by an average of 20% over the next 12 months. Those expectations may be underestimated, at least for the short term, as the global pandemic drove many enterprises to increase security spending to protect the explosion in remote workers and security incidents.

While larger security budgets will help to close some of the gaps organizations have in their security posture, many security teams are finding they are still struggling to implement the foundational capabilities needed to successfully employ detection and response tactics. However, by amplifying the scale, speed and scope in which organizations can detect and remediate attacks, XDR platform providers are aiming to help security teams address many of the ongoing obstacles to effective detection and response.

Expertise and Skills Shortages

Two of the most significant barriers to any security initiative are the lack of specialized expertise and the lack of available skilled resources. XDR aims to help organizations address both challenges.

By delivering data aggregation, automation, visibility, analytics and intelligence, XDR can be a force multiplier for security teams. Event triage, typically handled by tier one SOC analysts, tends to be one of the first areas to realize the benefits of implementing XDR benefiting from alert consolidation, contextualization and data enrichment. Streamlining and upscaling these activities can empower tier one analysts to achieve greater scale in the face of a growing volume of data while at the same time taking on more investigative activities typically handled by tier two and three analysts.

For tier two and three analysts, XDR can provide greater insights, intelligence and analysis on events, enabling the analysts to evaluate and prioritize threats to their specific environment and accelerate response actions. XDR also enables analysts to conduct broader and more efficient threat hunting activities and develop new threat intelligence to strengthen security policies and playbooks.

Automation and Orchestration

Although many XDR solutions only offer limited automation and orchestration capabilities or require security teams to integrate with third-party security automation and orchestration platforms, automation is a key benefit for XDR that is expanding and becoming increasingly native to XDR platforms. Automation enables security teams to perform at high velocity and with maximum efficiency amid an ever-expanding and complex IT ecosystem and an evolving threat landscape.

The automation and orchestration capabilities of XDR platforms hold the potential to optimize a large portion of security operations, including monitoring, management, detection, analysis, data enrichment, correlation and response. Providing end-to-end automation capabilities that span tools, processes and workflows, security platforms help alleviate the time needed to conduct mundane, repeatable tasks so more time can be focused on strategic and value-add initiatives. However, product-centric XDR providers may provide limited automation capabilities outside of their own technology stack.

The downside of a proliferation of automation tools is that disparate tools tend to exacerbate vendor and technology silos that may already be problematic for security and IT operations teams alike. SOAR is just one automation capability in the enterprise, and it is largely focused on security operations; others range from more general workflow and RPA tools to the automation typically seen in DevOps toolchains. For SIEM vendors and others that have acquired or embraced SOAR, however, this could be a point of potential cooperation and possible rationale for further integration of XDR with SIEM and SOAR strategies – for enterprises and, perhaps, acquirers alike.

Integrations

XDR can also alleviate the need for security teams to build and maintain integrations and connectors with security tools and data sources. Although most XDR providers offer an extensive set of APIs, most organizations lack the bandwidth and expertise to develop their own connectors, preferring vendors that offer out-of-the-box, bi-directional integrations. However, since no XDR platform natively integrates with every security tool available in the market, some custom integration will likely be required. Organizations will find that analytics- and services-focused XDR providers tend to integrate with a broad set of third-party security technologies while telemetry-centric XDR providers tightly integrate with their own proprietary security technologies, only offering limited integrations (typically only data ingestion) to third-party tools and data sources.

Continuous Improvement

ML holds great potential for XDR enabling security teams to scale operations and discover threats that would otherwise go undetected. ML's capacity and ability to correlate and decipher massive amounts of raw information make it an ideal fit for XDR. Contextualized, telemetry-based ML analytics can reduce false positives, prioritize alerts based on risk, and enable security teams to respond to threats faster and more efficiently. Although many XDR providers have started to leverage ML in their platforms and operations, they have yet to realize the full possibilities that ML-driven threat discovery and insight augmented with human intelligence and experience can deliver. Adaptive ML can enable organizations to continuously improve their threat detection and response capabilities and their overall security posture reducing risk to the enterprise.

Guidance and Recommendations

In addition to notifying security analysts of threats and indicators of compromise, many XDR platforms deliver prescriptive analysis, including guidance and recommendations for further investigation and response. While this analysis and guidance can help security teams contextualize threats and prioritize response efforts, it can be particularly valuable for lean security teams that may lack the in-depth expertise to determine the corrective actions needed to respond to events quickly and decisively.

Drawbacks

As with any security approach or technology, XDR has several risks, limitations and shortcomings that organizations should consider before committing to this strategy.

Today, most XDR providers tend to focus only on two or three domains and are often limited to detecting threats in certain environments (e.g., on-premises) and primarily from their own proprietary technologies (e.g., endpoint agents). In addition, XDR often requires organizations to make investments in other capabilities such as automation and orchestration, threat intelligence, SIEM, reporting, and developing integrations with workflow systems and security technologies not natively supported by the solution. This variability between XDR providers can make comparing and selecting the right platform difficult, forcing security teams to compromise and choose a specialized solution that may deliver the specific outcomes they are seeking.

When organizations have limited to no relevant expertise, XDR requires organizations to make significant investments in advanced security talent to cover 24/7 threat detection, investigation and response. Although XDR can be a force multiplier for organizations without a SOC or only staffing a lean security team, effective detection and response requires human insight and specialized expertise that many organizations lack.

XDR platforms often provide out-of-the-box use cases delivering pre-configured playbooks for response, preconfigured reports, and facilities to conduct threat hunting. However, many organizations may find that, due to available expertise, they are unable to effectively expand beyond the limited predefined capabilities of the XDR platform, reducing their ability to achieve the full capabilities the organization envisions for its security program. Considering the prevalence of product-centric XDR approaches, vendor lock-in is a strong possibility.

6. Conclusions

XDR emerged from a combination of increased demands from enterprises. The growing importance of proper stewardship in cybersecurity as technology expands – combined with the increased notoriety of security breaches – intersects with vendors that have expanded both capability and capacity for deploying more centralized analytics. The main classes of offerings that have emerged include what we're calling telemetry-centric or analytics-centric vendors, plus many managed security services providers that can also offer XDR services or technologies for customers.

We expect XDR to provide a meaningful alternative for organizations looking to focus on the pain points of integrating multiple security sources and applying analytics to derive better insights in security operations practices. Easier integrations may appeal to mid-sized organizations well positioned to benefit. Smaller organizations may gravitate toward managed services offerings that can include XDR, while larger organizations are more likely to embrace bespoke capabilities that accommodate their specific needs.

In terms of high-level considerations, the following applies:

- **Buyers need to consider needs and lock-in.** Organizations exploring XDR should view it as a possible avenue for obtaining some integration benefits in short order, particularly for simpler use cases. A key consideration, though, is that those gains on integration may come with a much deeper dependence on a specific vendor, which may be perfectly fine provided that the customer is coming at the opportunity with this understanding. As always, *caveat emptor.*
- **Telemetry-centric XDR vendors need to embrace third-party data.** Vendors with a focus on their own telemetry sources should consider maintaining and communicating a robust approach for incorporating third-party data. This includes having a manageable underlying data architecture for heterogeneous data but also maintaining a consistent and seamless user experience when incorporating external data, even from competitors in one or another telemetry source.
- **Analytics-centric XDR vendors must demonstrate superior benefits.** Vendors looking to provide 'independent' XDR via analytics should emphasize coverage of likely telemetry sources, ease of integration and tangible results from using an independent engine. They should clearly understand that their offering needs to provide sufficient benefits to overcome the general preference that customers have toward simplifying their vendor ecosystems, as demonstrated elsewhere in this report. They should be particularly mindful of how SIEM vendors may be able to accommodate XDR use cases by better integrating existing sources and providing user experience options optimized for security operations.
- **XDR vendors should have a managed offering.** For vendors ingrained in the model of transactional sales of security point products, adding managed services may seem scandalous. However, the reality is that technology alone is not going to solve the human resource and expertise shortage that will be prevalent for years to come. Offering varying degrees of managed services can ensure that platforms are configured and used correctly, enabling organizations to realize a quicker ROI on their investments. For the provider, a managed offering extends the opportunity for deeper insights and relationships with customers, and larger revenue streams.

- **Non-XDR vendors need to have XDR messages ready.** For security vendors not directly or currently involved in the XDR competition, they should understand how this dynamic may eventually touch their markets. Application security, data security and other areas are all candidates for feeding content into security operations practices that choose to leverage XDR. Each should have positioning ready to explain to customers what such a path might look like. SIEM vendors may have an opportunity to expand into the space by focusing on the pain points of easier integration of external sources and providing better workflows and experience for security operations.
- **Other interested parties need to consider nuances of XDR.** Those following the XDR space, including investors and entrepreneurs, should pay attention to the nuances between different approaches to XDR, as outlined in this report. There's also the context that, particularly in larger organizations, XDR conversations and competition is happening within the context of IT becoming an even more strategic partner, leading to conversations that move well beyond the SOC.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

With Cisco's XDR solution, customers get more value from their individual security products because of the superior telemetry capabilities within our solution. When a customer connects any security product to SecureX, telemetry from that product is automatically correlated with telemetry from more than 200 million natively integrated data inputs – more than any other vendor and including third party solutions. This process expedites the ability to turn data into intelligent insights that security teams can use to validate detected threats.

When security teams spend less time devoted to manual tasks like correlating alerts, they have time to focus on finding efficiencies and improving response time. Our XDR solution empowers your security teams to be more proactive by using our built-in workflows that offer automated solutions to machine-scale problems. This can radically reduce threat dwell times with retrospective security and playbook-driven automation.

The backbone of our XDR solution rests on the vast threat intelligence provided by Cisco Talos. Their broad visibility and comprehensive intelligence increases detection accuracy and strengthens alert fidelity and detection across all threat vectors.

While Cisco SecureX provides the critical tenets of XDR – detection, response, automation, coordination, and telemetry – it also delivers far more than just XDR. Because SecureX is not a singular product, but a platform, it is the mechanism for many elements of a security organization's maturity journey and positions your organization for security transformations beyond XDR.

Cisco's XDR Solution Highlights

- Reduces the dwell time and human-powered tasks involved with detecting, investigating, and remediating threats
- Empowers faster and more accurate decision making with less overhead and better precision with less error
- Maximizes efficiency by orchestrating and automating security tasks saves time and reduces cost
- Accelerates discovery of both known and unknown threats with high-fidelity alerting and proactive threat hunting
- Enriches insights from connected solutions for smarter investigations
- Delivers unrivaled contextual awareness and leverages the broadest telemetry base

How can Cisco's XDR platform approach elevate your security goals?

CISCO™