Innovation Insight for Extended Detection and Response

Published 19 March 2020 - ID G00718616 - 20 min read

By Analysts Peter Firstbrook, Craig Lawson

Extended detection and response describes a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components. Security and risk management leaders should consider the risks and advantages of an XDR solution.

Overview

Key Findings

- Security and risk management leaders are struggling with too many security tools from different vendors with little integration of data or incident response.
- Extended detection and response (XDR) products are beginning to have real value in improving security operations productivity with alert and incident correlation, as well as built-in automation.
- XDR products may be able to reduce the complexity of security configuration and incident response to provide a better security outcome than isolated best-of-breed components.
- XDR products have significant promise, but also carry risks such as vendor lock-in. The XDR market is immature and capabilities vary widely across products from different vendors.

Recommendations

SRM leaders looking to improve infrastructure security operations productivity and detection and response should:

- Work with stakeholders to determine if an XDR strategy is right for your organization based on staffing and productivity levels, level of federation of IT, risk tolerance, and security budget. Develop a gap analysis between your existing capabilities and those you’d want to have from an XDR solution.
- Conduct thorough product evaluation and testing to ensure outcomes meet the promises of this fledgling capability.

- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, including when and why exceptions might be permissible. Ensure that future security purchases and planned technology retirements are aligned with a long-term XDR architecture strategy.
- Outsource to a managed security service provider (MSSP) that can build an XDR substitute if it is likely to be beyond the skill sets of existing staff.

Analysis

Emerging XDR products consolidate multiple security products into a cohesive security incident detection and response platform for the mainstream market. XDR offerings are a natural evolution of endpoint detection and response (EDR) platforms, which have become a primary incident response tool for security teams. The primary value propositions of an XDR product are to improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple streams of telemetry, presenting options for multiple forms of detection and concurrently enabling multiple methods of response. Another benefit of XDR products is that they can provide what traditionally have been complex security operations capabilities, and make them more accessible to security teams that do not have the resources for more custom-made point solutions.

XDRs are similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools; however, XDRs are differentiated by the level of integration of their products at deployment, and the focus on threat detection and incident response use cases. While the SIEM market is mature, many organizations have not deployed SIEM tools, have failed or incomplete implementations, or only use SIEM for log storage and compliance. XDR products aim to solve the primary challenges with SIEM products, such as effective detection of and response to targeted attacks, including native support for behavior analysis, threat intelligence, behavior profiling and analytics.

SIEM vendors typically do not have the same level of threat detection and research analysis labs as XDR vendors. Moreover, while the SIEM market is now able to be delivered as SaaS, most XDR products are developed using new cloud-native architectures and services, making them an emerging alternative or complement to existing SIEM tools (see “Magic Quadrant for Security Information and Event Management”). However, XDRs are not a replacement for all SIEM use cases, such as generic log storage or compliance.

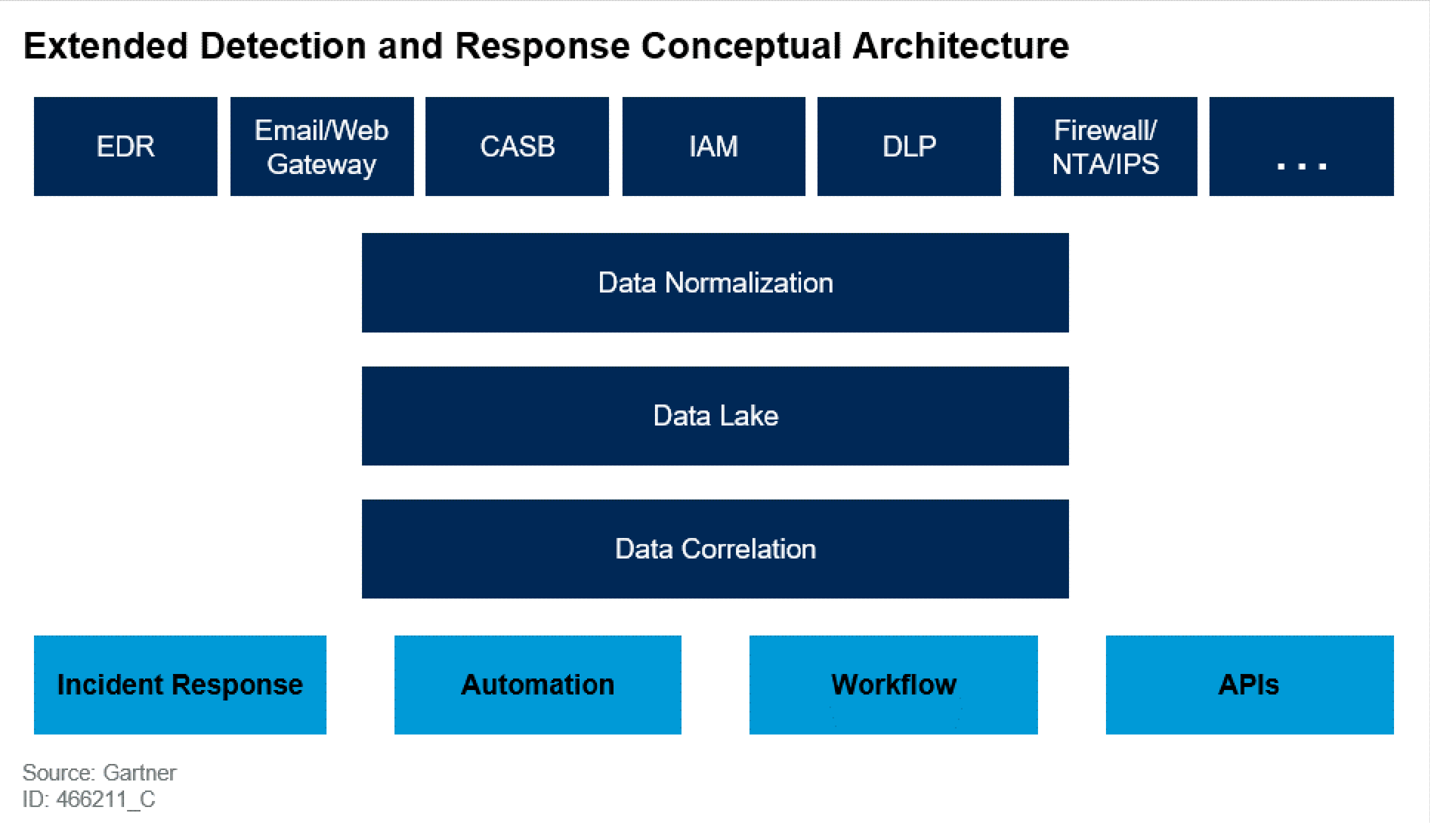
The three primary requirements of an XDR system are:

1. Centralization of normalized data, but primarily focusing on the XDR vendors’ ecosystem only
2. Correlation of security data and alerts into incidents

3. A centralized incident response capability that can change the state of individual security products as part of incident response or security policy setting

Initial XDR focus is primarily on protecting end users and the apps and data they consume (see Figure 1). However, the XDR concept can extend into data center protection, identity and access management, and secure access service edge product portfolios.

Figure 1. Extended Detection and Response Conceptual Architecture



Extended Detection and Response Conceptual Architecture

Source: Gartner
ID: 466211_C

Currently, XDR tools are primarily being marketed by security solution providers that have a portfolio of infrastructure protection products unified by their own SaaS-delivered XDR management. Being cloud-delivered, XDR also has the potential to benefit from novel analytics use cases. These XDR products are limited in scope to the vendors' own products and technology. Early XDR vendor candidates include Cisco, Fortinet, Fidelis Cybersecurity, McAfee, Microsoft, Palo Alto Networks, Trend Micro, Sophos, FireEye and Symantec. These vendors already have a proprietary understanding of the relationships in the underlying data, and can provide private APIs to enable automated actions more effectively than trying to integrate products from multiple vendors. A large appeal of these XDR products will be rapid time to value resulting from out-of-the box integration and pretuned detection mechanisms across products.

It may be possible for SIEM and SOAR tools and new entrants to claim XDR capability as the industry matures. For example, Hunters.AI is an early XDR product that integrates across multiple products.

However, the complexity of building a useful XDR for vendors that own all the components and can source the data natively illustrates the challenge independent vendors will face when integrating across multiple vendors. The reality today is that there are few common standards for data integration at this level, or extensive APIs that can automate across multiple vendors' products.

However, building an effective XDR is more challenging than it might seem. Lack of data collection, common data formats and APIs, as well as products built on legacy database structures, make it difficult to integrate security tools even within the same vendor's product portfolio. Development decisions in older products don't always scale or integrate well with cloud-native tools. Marketing hype can get ahead of the market before tools mature, and the vendors can fail to deliver.

Despite these challenges, and more listed below, the overall rewards of more efficient, effective security operations for the mainstream market make XDR a promising new approach to enterprise security. Two of the biggest challenges for all security organizations are hiring and retaining technically savvy security operations staff, and building a security operations capability that can confidently configure and maintain a defensive posture as well as provide a rapid detection and response capacity. Mainstream organizations are often overwhelmed by the intersectionality of these two problems.

The security market has been in a continual pendulum between best-of-breed component parts versus suite portfolios. As security products mature, best-of-breed product functionality tends to become features of broader platform products. Currently, many of the major component parts of security infrastructure protection are reaching feature maturity, and a number of vendors offer broad portfolios. Integrating them is a natural next step. Concurrently, cloud big data storage and analytics and machine learning capability are enabling more centralized approaches to security.

Best-of-breed security product buying has resulted in too many vendors and products with very little integration or coordination. Security alerts are often excessive, uncoordinated and too often go unattended. Configurations are not actively maintained or tested for effectiveness, and security products are too infrequently upgraded. The traditional integration point in most enterprises has been the SIEM tools, which are good at collecting logs, but rarely improve detection fidelity in most implementations, use contextual indicators to combine multiple alerts or provide full incident response capability. Organizations have a hard time developing SIEM playbooks and building deeper, richer integrations across a heterogeneous environment. Newer SOAR tools are designed to provide integration across multiple components, but are hobbled with a lack of available APIs, data merging issues and a workflow that is disconnected from the detection activity that can efficiently launch response activities.

XDR products are designed to alleviate these challenges. They consolidate multiple vendor-specific security products into a cohesive security incident detection and response platform that is accessible to the mainstream market without extensive integration efforts.

XDR products will appeal to pragmatic enterprise security buyers that do not have the resources to integrate a portfolio of best-of-breed security products into a SIEM or SOAR tool.

The core requirement of XDR systems is a centralized collection of historic and real-time event data in common data formats. Event data must be available for fast indexed searches for indefinite periods in scalable and high-performance storage. Another requirement is to use multiple detection techniques to combine weak signals from multiple products into strong evidence of malicious activity. In addition, XDRs are designed to enable a faster, more efficient response capability aided by automation. Finally, XDRs have the potential to improve the security posture by making it easier to maintain.

The primary advantages of XDR should be threefold:

1. Improve protection, detection and response capabilities.
2. Improve overall operational security staff productivity.
3. Lower total cost of ownership to create effective detection and response capability.

Ideally, XDRs can improve protection capability by:

- Sharing local threat intelligence immediately among component security products to provide efficient blocking of threats across all components. Also, leveraging externally acquired threat intelligence in multiple different detection methods (for example, network and endpoint).
- Combining weak signals from multiple components into stronger signals of malicious intent.
- Reducing missed alerts by correlating and confirming alerts automatically.
- Integrating relevant data for faster, more accurate alert triage.
- Providing centralized configuration and hardening capability with weighted guidance to help prioritize activities.

XDRs can potentially improve operational security staff productivity by:

- Converting a large stream of alerts into a much smaller number of incidents that are required to be manually investigated
- Providing integrated incident response options that have necessary context from all security components to resolve alerts quickly
- Providing response options that go beyond infrastructure control points (i.e., network and endpoints)

- Providing an automation capability for repetitive tasks
- Reducing training and upleveling Tier 1 support by providing a common management and workflow experience across security component parts
- Providing usable and high-quality detection content with small to no tuning required

Some XDRs are focused on integrating infrastructure security tools, such as combining network and endpoint security together. However, more advanced XDRs are focusing up the stack by integrating with identity, data protection and application access. These security services are closer to the business value of the incident. For example, incident response is enriched with the knowledge that endpoints have sensitive data or privileged access to critical IT or business applications.

Currently, emerging XDR products focus primarily on protecting against malicious attacks against endpoints, data and applications. As such, the predominant types of security services included in XDR systems commonly include:

- Endpoint protection platforms (EPPs) and endpoint detection and response (EDR) products
- Cloud access security brokers (CASBs)
- Secure web gateways (SWGs)
- Secure email gateways (SEGs)
- Network firewalls, network intrusion prevention systems (NIPS) and unified threat management products
- Identity and access management products
- Data loss prevention products
- User and entity behavior analytics
- Network traffic analysis
- Global threat intelligence

The XDR concept could extend into data center protection encompassing tools such as:

- Cloud workload protection platforms
- Cloud security posture management products
- Web application firewalls

Since the goal of XDR is improved detection accuracy and security operations center (SOC) productivity, integrating products that can contextualize and inform the incident response activity across common kill chains will be the initial goal. Combining security products that are not commonly involved in the same attack kill chain will have less value.

Definitions

XDR is a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed security components.

The three primary functions of an XDR system are:

1. To be a collection of common security products that are integrated out of the box
2. Centralization and normalization of data in a central repository for analysis and query
3. Improved detection sensitivity resulting from the contribution of multiple security products working in coordination
4. Correlated incident response capability that can change the state of individual security products as part of the recovery process

XDR is a SaaS-based, vendor-specific security incident response tool that natively integrates multiple security products into a cohesive security operations system that is contextualized by all licensed security components.

At a minimum, XDR tools require continuously updated intelligence about attacker tool tactics and techniques. They also need data normalization and other forms of preprocessing to enable analytics and correlations. They will typically also require extensive SaaS-based data storage, preferably in a graph database that is capable of connecting events that are not predefined. XDR tools tie together threat-facing security components, such as EPP/EDR, firewall, NIPS, SEG, CASB and SWG, into a cohesive security operations system.

Benefits and Uses

XDR is still an emerging product category; as such, the majority of benefits are still unproven.

Ideally, XDR vendors can deliver a unified portfolio of critical security functions that provide:

- More accurate detection and prevention capability
- Lower total cost of ownership driven by higher security operations productivity and lower acquisition costs
- Faster time to value (versus buyers integrating best-of-breed products)

- Security that is adaptable to changing infrastructure and application architecture
- Fewer blind spots
- Faster, more accurate and informed detections — i.e., alert correlation and full incident response data correlation
- Faster time to remediation — playbooks and operations integration — and automation
- Better visibility and searchability
- Prioritized hardening with product configuration and software vulnerability management as an integrated task across the portfolio, and not isolated siloed activities

Centralization and normalization of data improves detection by combining softer signals from more components to detect events that might otherwise be ignored. Detection across components can also detect tricky problems such as account takeover attacks, insider threats and detecting incidents in IoT/OT systems. Security can also be improved by enabling more rapid sharing of local IOC information among components to provide faster protection across all devices. For example, incident response can collect unique IOC information and disseminate it to all security components and simultaneously check historical data for similar events.

Ideally, this improved correlation, context and analytics will lead to reduced security alerts requiring human intervention by automating actions and providing stronger prevalidation capabilities. The benefit is that analysts spend more time on “incidents” and less time on a stream of “alerts” that often lack context. For example, network alerts can be confirmed or debunked by endpoint activity analysis. The total volume of alerts can be reduced by orders of magnitude by combining individual product alerts into systemwide incidents. For example, an attack that caused alerts on email, endpoint and network can be combined into a single incident. The analyst then has significantly more real-time “context” to be able to make a better decision, faster. XDR products also aim to improve security team productivity and uplevel the incident response capabilities of Level 1 SOC operators by consolidating and contextualizing all the evidence in an easy-to-understand management platform instead of propagating the age-old “context switching” problem of having to surf around between multiple consoles. Centralized data also enables faster query capabilities across multiple components. Like for SIEM, this will be a key benefit for capable XDR solutions. Being newer to the market, XDR has not just the promise, but also the reality of having APIs built in right from the start. This provides more opportunities for faster and partially automated incident response capabilities, and integrations with a wide range of other processes and systems such as SOAR, vulnerability management, ITSM and CMDB.

Adoption Rate

The development of XDR products is ongoing and few products are fully integrated yet. As a result, adoption of XDR is still primarily in beta and early trials for most products. Less than 5% of organizations have an XDR product strategy.

Risks

The emergence of XDR products is still in the development phase and there are numerous risks that can derail this new approach.

There's a basic problem with event management — new event sources and event volume are increasing faster than the technology to deal with them. Every increase in the sophistication of integration, detection, response and automation, can only partially compensate for the scale and complexity of the problem. While XDR may improve this situation, it is unlikely to solve it.

XDRs could lead to overreliance on a single vendor. XDRs may help improve security efficiency but may also lead to vendor lock-in, and potentially sacrifice functionality in component parts versus best-of-breed components.

XDR could improve efficiency, but in doing so, could sacrifice security efficacy as well. Just because a vendor is doing multiple things that are integrated doesn't mean it is necessarily doing it well. Efficacy will be a key metric for IT security leaders to pay attention to. You will not only have to answer the question of does it find things, but also is it actually finding things that your existing tooling is not.

Vendors are initially integrating mostly their own products, so may be missing critical integrations or component parts to make them effective. XDR may simply become a mechanism to try and lock in to a particular vendor without delivering the real benefits, and be a suite of point solutions versus a truly orchestrated whole. As a result, buyers need to be strategic in selecting an XDR provider.

There is only a small list of vendors that can truly offer an XDR approach. Many of the XDR products are immature and do not have full integration across all components. Most organizations do not have a complete portfolio of products from a single XDR vendor, or the budget to acquire them. Therefore, it will take three to five years for most organizations to realize the full value of an XDR product.

Indeed, if the pioneering XDR vendors deliver too little security or productivity value, or solution providers simply do not deliver on their roadmaps, or XDR products end up needing the same level of integration work as modern SIEM tools, then it is likely that XDR will die in the Trough of Disillusionment.

The large vendors that are capable of providing an XDR product often execute much slower than the best-of-breed startups in addressing new threats. To remain attractive, XDR solution providers must stay current with the latest technology, or make acquisitions and make it compelling for new vendors to integrate into their platform.

XDR vendors will have gaps in their portfolio of products that require point products that do not integrate with the XDR solution, creating blind spots. Most organizations already have blind spots so XDRs can add value even if they are not 100% integrated. However, leading XDR vendors will integrate with select partners to improve coverage.

The large multiple product vendors have the inside track on providing an out-of-the box XDR experience due to, in theory, their already owning many of the component parts. However, as more security products ship with APIs and information-sharing mechanisms, it is possible that independent startups, MSSPs or SIEM/SOAR solutions will be able to integrate best-of-breed components to deliver the same value as an XDR without the vendor lock-in. They will do this in innovative ways that can be simply categorized as “over the top” (OTT) capabilities. For example, SOAR solutions do some of this today by providing an abstraction layer over existing solutions. It is entirely feasible this model could be successful, especially if that startup delivers better analytics and storage, and can do so from the cloud.

It is highly possible that sales and go-to-market motion will fail to capture the correct buying audience, draining the vendor enthusiasm for XDR. It is clear that XDR buying cycles will be longer and more complicated than buying individual component parts. The average tenure of a CISO may be shorter than the time to implement a more strategic XDR component parts buying program. Moreover, a single acquisition can introduce new products in the mix before the XDR strategy is complete.

XDR strategy requires a high level of dependence on a single vendor. This raises multiple potential issues, including:

- Vendor lock-in
- Single point of failure
- The lack of diversity in threat intel and defensive techniques
- Vendor support or renewal issues increasing with vendor dependence
- Failure of the vendor to adapt to the changing threat or market landscape
- Buyers fearing higher strategic risk if they pick the wrong XDR product

The large XDR vendors likely have enough threat intelligence and a broad enough portfolio of security tools, each of which employs different detection and prevention techniques, that an XDR product can achieve an in-depth defense posture without the complexity of a multivendor strategy.

It is no secret that security domain experts want the latest and greatest tools on the market, even if they are not sure they need all the latest functionality. Very often, it is hard for CISOs to dispute the need for advanced features, making it hard to stick to strategic buying to gain more XDR functionality over time.

XDRs will not likely eliminate the need for log storage mechanisms to meet compliance or other needs.

Despite these risks, it is clear that the security market is ripe for consolidation, and XDR products will be appealing to more pragmatic organizations that are overwhelmed by security complexity and the lack of skilled security operations staff.

Evaluation Factors

XDR vendors will compete primarily on the range and quality of integrated security tools, the productivity gain of the SOC, and improvements in detection and prevention.

Other key capabilities will include:

- Quality of the component — security efficacy still matters
- Quantity of products that integrate into the XDR system, as more visibility is beneficial
- Depth of integration across component parts (for example, whether it is data-level integration only or deep configuration integration that allows the XDR system to change the state of component parts manually or automatically)
- Accuracy of correlation of alerts into incidents
- Use of advanced analytics such as UEBA to detect more sophisticated threats
- User interface and contextualization that enables faster remediation
- Quality of detection capability to detect more subtle attacks
- The range and depth of automation capability, including predefined playbooks and ability to customize automation
- The range of partners that can integrate into the XDR system out of the box
- Vendor execution on completing its roadmap and integrating new products and acquisitions into the XDR system
- The ability of the provider to offer advanced support, including a managed service offering and training
- Cloud-native service architecture

Buyers should focus on solutions that provide:

- Common data schema
- Common programming standard/framework, for both internally developed apps on the platforms and third parties to follow
- Rich set of APIs
- Enriched/correlated data from multiple sources supporting use cases such as threat hunting and advanced AI/analytics
- Detections that do not use endpoint agents/telemetry only
- Response actions that go beyond manipulation of the endpoint only
- Actions initiated in one tool and carried out in another
- Pivot between integrated tools within the same portal/UI
- Workflow for administrators using a portal and linked to automation
- Automation to initiate common tasks

SIEM and SOAR

The alternative to XDR is to use modern SaaS-based SIEM and SOAR that are optimized for the detect and respond use case (see "Magic Quadrant for Security Information and Event Management"). Another alternative is to use managed security services to provide an XDR-like experience. MSSPs do not offer services labeled specifically as XDR, but the primary value proposition of an MSSP is to assume the role that XDRs provide by doing the hard work of integration and alert correlation.

Recommendations

- Work with stakeholders to determine if an XDR strategy is right for your organization.
- Evaluate the XDR product capabilities and roadmap of incumbent and potential XDR providers.
- Develop an internal purchasing policy that is in line with your XDR strategy, including when and why exceptions might be permissible.
- Ensure that future security purchases are aligned with a long-term XDR integration strategy.
- Increase the importance of integration and automation in purchasing decisions.

Representative Providers

The following is a representative, but not exhaustive, list of potential future XDR vendors: Cisco, Fortinet, Fidelis Cybersecurity, McAfee, Microsoft, Palo Alto Networks, Symantec, Trend Micro, FireEye, Rapid7, and Sophos.

It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."