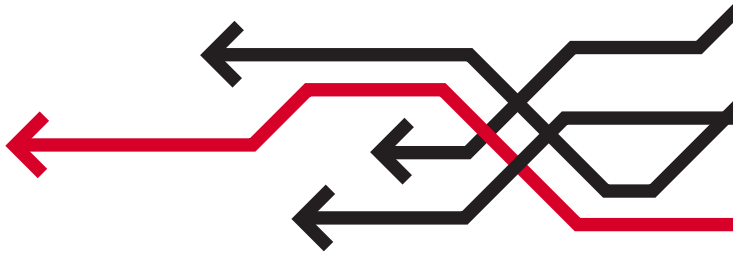


Technology & Business Insight

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.

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.

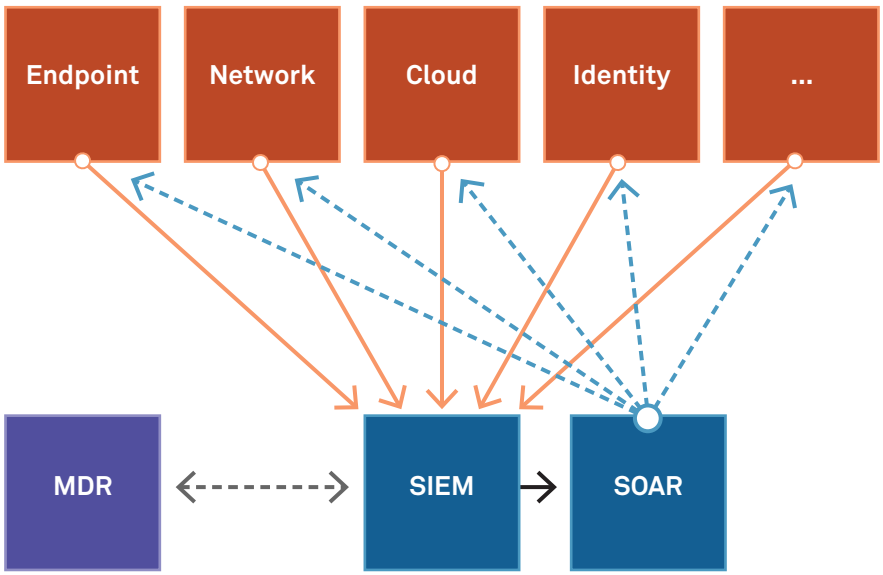
Table of Contents

1. Extended Detection and Response: Factors Shaping a Trend

Rethinking Security Operations Architecture

Before discussing XDR in more depth, it's useful to consider the traditional stack as it exists before XDR. Figure 1 illustrates key concepts.

Figure 1: Conceptual View of Traditional Stack, Pre-XDR



Source: 451 Research, 2021

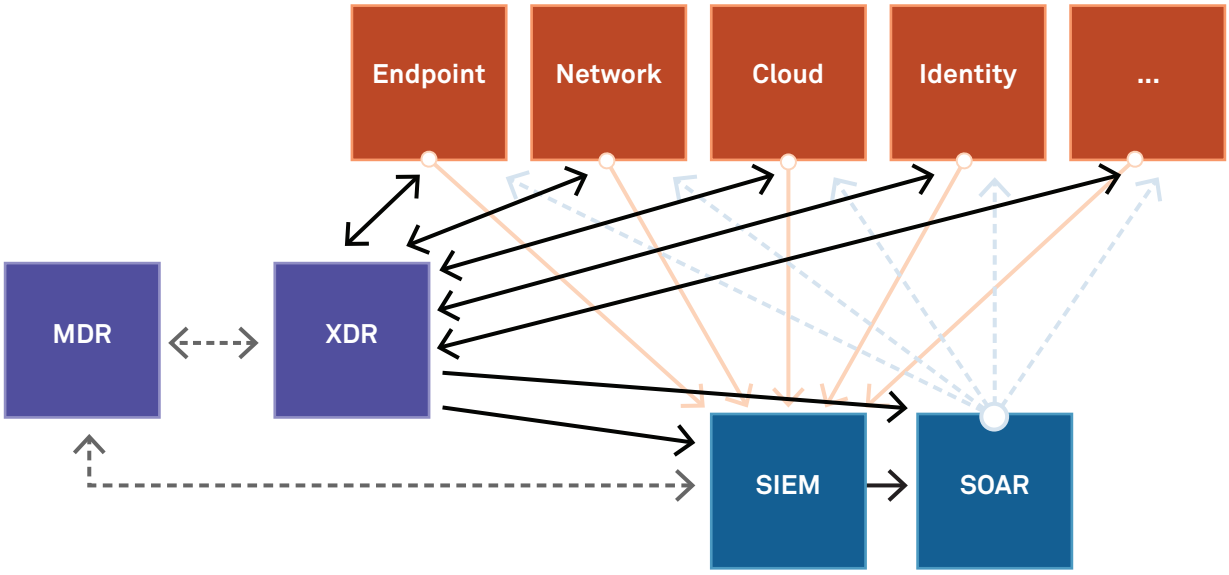
In broad terms, diverse sources of telemetry exist in the environment. These sources (endpoint, network, etc.) generate both 'generic' usage data as well as security-specific data such as alerts. This data is ideally set to feed centralized systems that perform log collection, management and analytics (depicted in the SIEM box). In some cases, an automation framework (security orchestration, automation and response [SOAR]) can initiate actions across the infrastructure, usually in response to events triggered by the SIEM or other workflow engines. Practitioners interact both with the telemetry sources for configuration or more in-depth searching and with the SIEM for searching, alerting, ad-hoc investigations and more.

In some scenarios, the SIEM (and likely other components in the infrastructure) may be managed by an outside service provider. Such an approach often includes a more complete slate of offerings beyond monitoring and initiating response to log inputs, however. From monitoring to investigation and response, and perhaps going even further toward threat containment or program guidance, these services approaches may be referred to as 'managed detection and response' (MDR).

There are both user-driven demand and vendor-driven supply considerations for why this current model may not be sufficient.

Starting over the past 24 months, but picking up steam since the start of the pandemic in early 2020, numerous vendors have pushed forward the XDR approach, which looks more like Figure 2.

Figure 2: High-Level XDR Approach



Source: 451 Research, 2021

Proponents of a more XDR-centric approach propose that data be either sent to a new XDR component or accessible from it. This may be done in parallel with an existing SIEM deployment or to supplement SIEM – but may also be done in preference to SIEM, if not outright exclusive of SIEM, for organizations so disposed. These proponents argue that the more XDR-centric approach is better suited to process the data from the telemetry sources for supporting typical security operations use cases, including analytics and automating responses.

The XDR component can also interact with existing SIEM and SOAR elements, which can retain their place in architecture albeit with differentiated usage for security use cases. In managed services scenarios, MDR providers can continue to support SIEM systems and others but can now also support the new XDR component.

What factors have driven this approach? We see both user demand considerations but also specific vendor-centric supply conditions that help explain the rise of XDR.

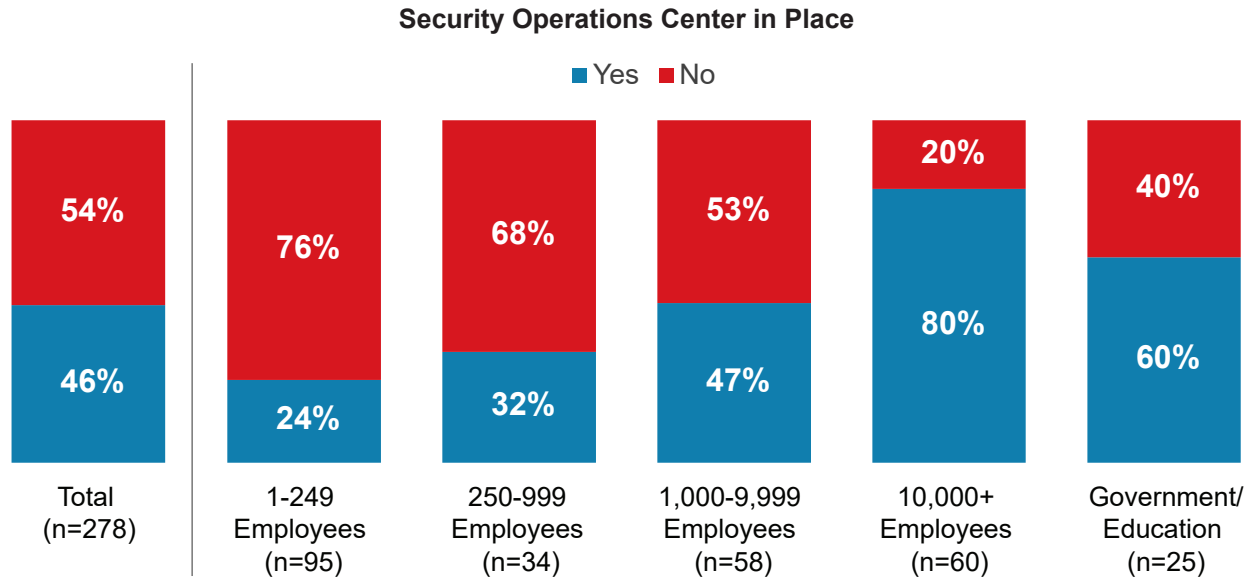
User/Demand-Side Factors for XDR Adoption

When considering what drives security operations teams or practitioners to weigh how they may incorporate something like XDR, the general theme is that teams are struggling to keep up with current and projected future demands.

Everyone Does 'Security Operations,' but Not Everyone Has Fully Managed 24/7 SOCs, or Even SOCs At All

The dearth of resources available to those practicing security operations manifests itself in many ways, including with organizations having wildly different capabilities in relation to a security operations center (SOC), which is often a key component of a mature security program. According to survey respondents, only approximately 54% of organizations have a formal SOC and numbers vary widely between organizations, often driven by their size (see Figure 3).

Figure 3: SOC Presence by Company Size



Q. A SOC is a facility where enterprise information systems (websites, applications, databases, datacenters, servers, networks, desktops and other endpoints) are monitored, assessed and defended. Does your organization have a security operations center (SOC) in place?
Base: All respondents (abbreviated fielding)

Note: Base sizes below n=30 should be interpreted anecdotally

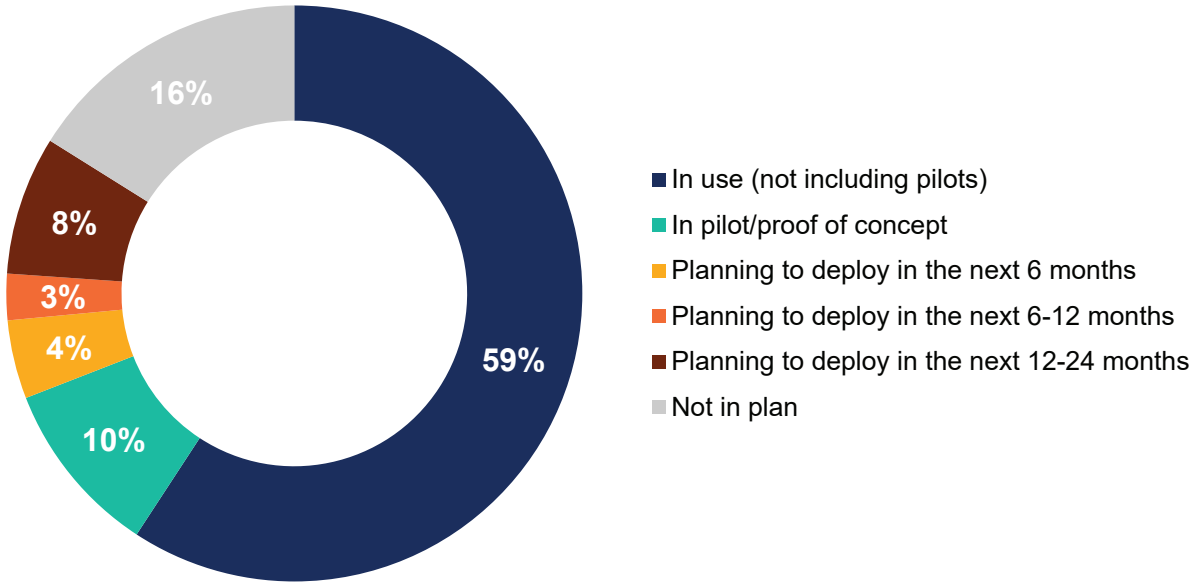
Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020

For those that do have SOCs in place, about a quarter of them are not operated 24/7/365. There's also a sizeable proportion of SOCs that are outsourced, as indicated by approximately 23% of respondents.

SIEMs Aren't Universal, Either

While the common pattern for security teams appears to be to collect data within their SIEMs, the picture that emerges is that a sizeable fraction of respondents indicate they don't have one at this point. Even under the best of circumstances, adding all the in-use, pilot and planning data shown in Figure 4, it will take another 24 months for SIEM coverage to cross the 80% penetration rate.

Figure 4: SIEM Adoption Is Far From Universal



Q. What is your organization's current implementation status for each of the following technologies? - Security information and event management (SIEM)

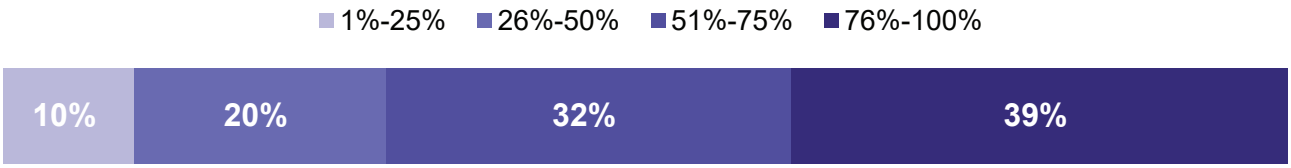
Base: All respondents (n=385)

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020

SIEM Collection and Analysis Is Apparently Incomplete

While it's common to highlight 'alert fatigue' and 'too many alerts' as significant issues for security operations teams, recent survey results give a different perspective. First, the survey response data shows that a sizeable proportion of respondents indicate that SIEM coverage is not uniformly broad. Only 39% indicate coverage of log-producing systems at or better than 76% (see Figure 5).

Figure 5: SIEM Data Collection Is Lagging



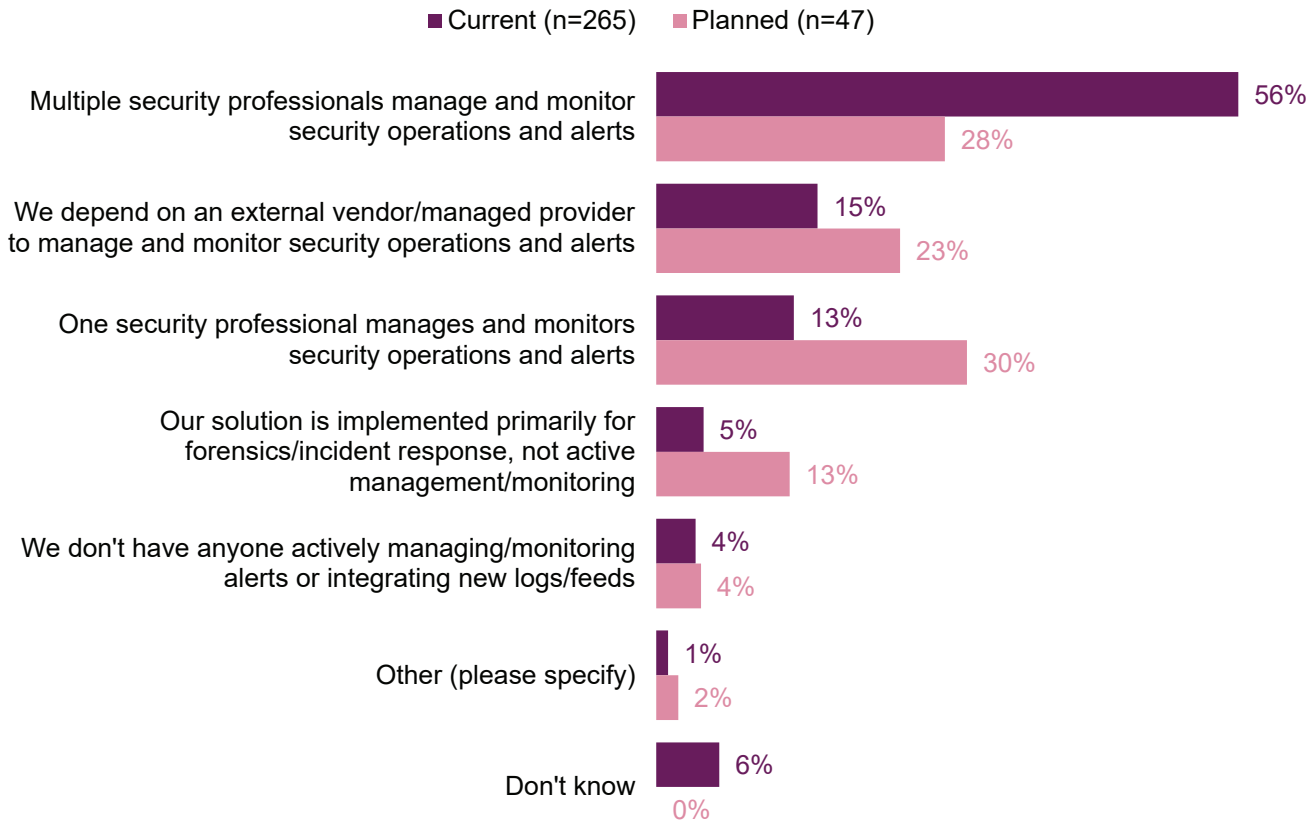
Q. What percentage of log producing systems within your organization are passing data to your SIEM/security analytics solution?
Base: Respondents currently using SIEM (n=225)
Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020

Second, according to the respondents to the survey, over 90% indicate they cannot investigate at least some of the alerts in a typical day, with nearly 30% indicating they can't process half or more of the incoming alerts. This, along with gaps in the nature and scope of telemetry, is the type of scenario that can allow attackers to persist in the environment for an extended period, making extracting them later that much more complicated and expensive.

Moving Forward, Even Fewer In-House Resources Dedicated to SIEM

Customers are also indicating that they appear to be making their security operations even leaner. The data in Figure 6 points to a scenario in which the set of practitioners that are planning to deploy SIEM in the next 6-24 months appear to expect their SIEM alerts will be managed, on aggregate, by a smaller team, by an external service provider, or even not at all, using SIEM only for forensic after-the-fact analysis.

Figure 6: Shifting Expectations on SIEM Usage



Q. Which of the following approaches best describes how your organization manages and monitors security operations and alerts for its SIEM/security analytics technology? Please select the option that most closely matches your organization's current approach.

Base: Respondents who currently use SIEM

Q. Which of the following approaches best describes how your organization plans to manage and monitor security operations and alerts for its SIEM/security analytics technology? Please select the option that most closely matches your organization's planned approach.

Base: Respondents planning to deploy SIEM in the next 6-24 months

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020

Supply-Side Factors for XDR Adoption

For those looking to get an understanding of the XDR landscape from a market perspective, looking at the 'supply' side of the equation is equally important.

The Rise of Cloud-Based Endpoint Management

It's interesting to note that many, if not all, of the relevant endpoint security vendors have added cloud-based back-end management for their customers over the past few years. For a variety of reasons, customers generally disliked the heavy lifting of having to manage the infrastructure to manage their endpoints, and vendors responded to that demand. What was innovative back in 2015 became more common in 2017 and commoditized in 2019.

With that management back end already available, the opportunity arose to not only manage the current software status and configuration of endpoints, but also ingest endpoint telemetry in a way that allowed for investigations even if the endpoints were unavailable. Now, a customer could go to a web interface and query endpoint data irrespective of the endpoint being connected, and in ways that enabled analysts to pivot from looking at one endpoint to looking at many.

We see some of these capabilities as the genesis of many vendors' XDR approaches: If the infrastructure is already there to manage endpoints and ingest endpoint telemetry, going from there to ingesting telemetry from other sources becomes a much easier conversation. Throw in some 'autonomous' independent search queries to find events of interest and there's an XDR offering in the making. Vendors also had an additional benefit with their cloud-based management/investigations offerings: By having access to customers' regular interactions with the platform, vendors can aggregate insights into usage patterns, future integrations and more.

The Richer Potential of a 'Pull' Versus a 'Push' Model

Historically, security operations teams have relied on inputs such as log messages collected by a SIEM. These are essentially text entries, each linear, if you will, in nature. That simplicity, however, makes pushing logs to a SIEM a straightforward matter. Logs are essentially text strings, and date back to the earliest days of log aggregation via syslog. Synthesis of findings may be simpler as well, traditionally based on what is often largely text correlation across entries. While this is fine for some workflows, there's some loss of contextual information as the data source (such as an endpoint detection and response [EDR] or firewall vendor, for example) translates its own insights from the signal it just processed into whatever common log format is being used.

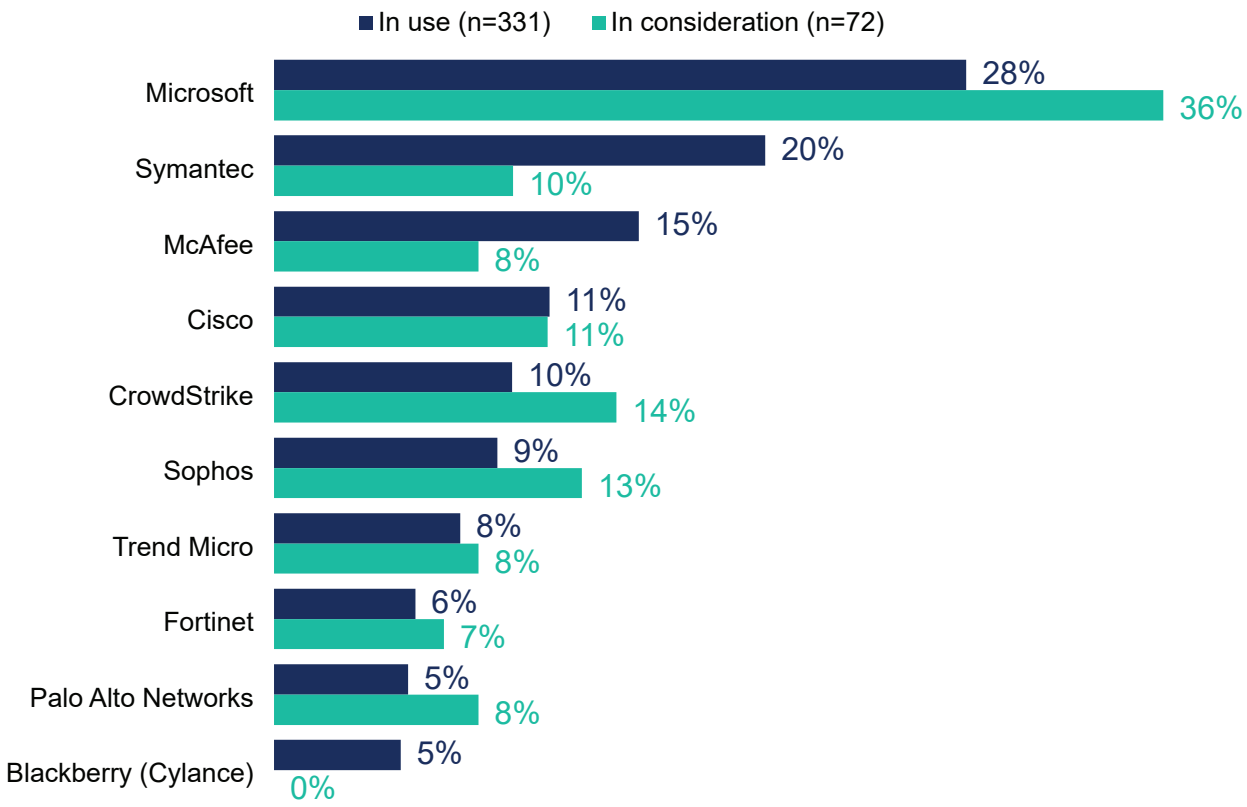
But log entries are only pushed to a SIEM if the monitored resource is programmed to generate them. With more modern approaches to telemetry, management systems may be able to reach out to targets and actively pull a wider variety of data rather than having it passively pushed to them. In the past, analysts often had to do such 'pulls' manually. If they desired to gain a detailed view of multiple aspects of an endpoint, for example, such as configuration, software complement or registry entries, they would have to reach out to a diagnostic tool installed on each such endpoint (which raises its own issues of secure access and connectivity).

With the flexibility of today's more modern approaches to cloud-based management, telemetry systems automate much of this collection of a variety of inputs across large numbers of targets, introducing the opportunity for a specialized engine that can retain some level of contextual insights from the original alerts. XDR can be such an engine.

The New Dynamics of Endpoint Security Competition Clamor for Something New

We see XDR as being closely aligned to endpoint security and in many ways a direct evolutionary step from endpoint-centric security operations that started with what was sometimes called 'next-gen' antivirus and endpoint protection platforms (EPP) and quickly incorporated EDR capabilities. As data from 451 Research's VotE: Information Security, Workloads & Key Projects 2020 shows, there's a market dynamic where a vendor refresh appears to be in motion when looking at endpoint security specifically (see Figure 7).

Figure 7: Signs of Generational Refresh in Endpoint Security



Q. Who are the main vendors your organization uses for endpoint security? Please select up to 2.
Base: Respondents currently using endpoint security technology (n=331)

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020

The nuance in this chart is that vendors need to react to two key trends:

- The surge in interest in Microsoft's endpoint security offering, which coincides with widespread popularity of Windows 10, which includes native anti-malware capabilities and additional telemetry.
- The opportunity that arises as customers indicate they're looking at alternatives to popular incumbents Symantec and McAfee.

When considering the data above, it's possible to see XDR as an approach that arises to extend (wordplay fully intended) the conversation beyond the endpoint alone.

A Deeper Relationship Is a Stickier Relationship

It's basic economics and sales management: It is cheaper to retain a customer than acquire a new one. With that in mind, vendors have a strong incentive to establish and deepen their presence within customers. On the customer side, customers know that the cost of switching can be an inhibitor in weighing new suppliers against incumbents.

For all the pain of changing endpoint software across tens of thousands of devices, it's relatively easier to do that if the endpoint software doesn't happen to be tightly integrated with additional sources such as network, email or the triage-investigation-response workflows that are the beating heart of security operations.

A good example of this kind of long-term presence is McAfee. The company's ePolicy Orchestrator is often mentioned anecdotally as a key component for many customers as it automated several aspects of security management, even incorporating support for third-party vendors.

Ideally, this is the kind of relationship that vendors are looking to develop with their customers as they propose XDR approaches.

SIEM Vendors Left the Door Open as They Chose To Evolve a Separate Way

For SIEM vendors, we saw a preference for providing more functionality on the response side of security operations workflows rather than investments in tighter integration with telemetry sources. With customers looking for help to make the insights derived from SIEMs actionable, adding more orchestration and automation capabilities was a natural adjacency. While the primary impetus behind many SOAR acquisitions may have been to enable both flexibility and consolidation in the implementation of an open-ended range of security functions, they also made sense as a way to accommodate the variety in endpoint sources and not pick favorites. The market saw significant movement among SIEM and non-SIEM vendors alike: Relevant transactions include Splunk acquiring Phantom, Palo Alto Networks picking up Demisto, Microsoft reaching for Hexadite, Rapid7 going for Kommand, and Sumo Logic taking on JASK and, most recently, DF Labs.

That said, this move toward automation alone was not universal, as some vendors with SIEM offerings did indeed go shopping for new telemetry sources. Elastic saw the opportunity to acquire Endgame, and Alert Logic picked up the assets from Barkly. The irony of trends that would widen a gulf between SIEM and XDR is that the use of technologies such as EDR in the SOC arose in part because analysts need richer insight in order to properly triage SIEM data and escalate alerts. When that data was not natively available to SOC teams via a SIEM deployment, it was obtainable by pivoting to alternate sources.

Multiple Data Sources To Help Security Teams

Before delving into current XDR approaches, it is beneficial to first get a broad understanding of some of the data sources that organizations have at their disposal for helping to contextualize security telemetry. This is relevant because many XDR vendors still only focus on a portion of these sources.

Endpoint Data

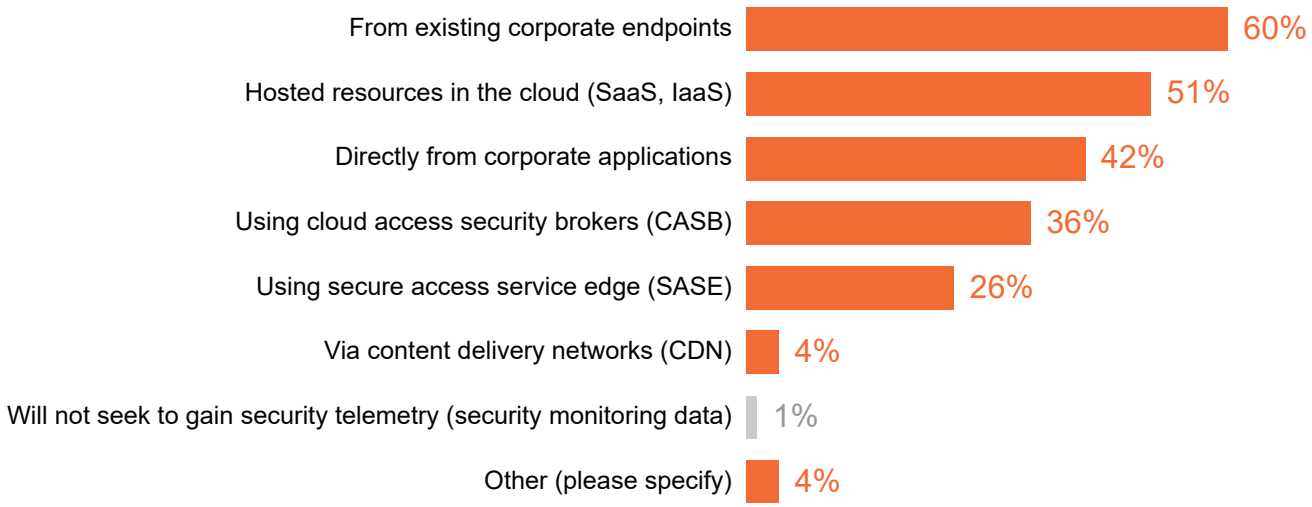
If there's one data source that could be considered primary for XDR, that must be endpoint data. Indeed, as we preview some of the later findings of this paper, endpoint shows up as the most common source reported by vendors. This is by design, as several factors have raised the prominence of the endpoint as a critical component in modern security operations.

Endpoints play multiple roles, with different levels of prominence if we're talking about end-user endpoints or server endpoints: They're the interface between end-user behavior and system activity, they're a prized foothold for adversaries looking for persistence during an attack and, in many cases, they may be the location of the actual attack objective itself.

Considering end-user-centric endpoints and their role in an attack campaign, endpoints are the source of rich telemetry from process activity as well as alert data from endpoint security tooling itself. Signals emanating from the endpoint include but are not limited to file and network access, registry access or manipulation, memory management, process start and stop activity, and much more. Endpoint security tooling can add some level of context to these, such as alerting on threats it prevented before execution or on unusual behaviors – processes spawning command shells, memory injection attempts, unusual file locations and more.

Naturally, because of the pandemic and workforce disruption, endpoints become more important as a source of telemetry. Data from 451 Research's VotE: Information Security, Organizational Dynamics 2020 study shows that organizations indicate they will look to corporate endpoints as a source of additional insight for any telemetry they lost because of the shift to remote work (see Figure 8).

Figure 8: Endpoint Security Provides Telemetry



Q. If remote working becomes more permanent, how you will your organization seek to gain security telemetry (security monitoring data)? Please select all that apply.

Base: Respondents whose organization is experiencing a loss of security telemetry (security monitoring data) as more employees work from home during the coronavirus (COVID-19) outbreak (n=73)

Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Server Endpoint Data

Server endpoints are often treated as regular endpoints. Much of the same telemetry is available from server endpoints, and our surveys indicate many customers use the same security tooling to secure both end-user and server endpoints. Still, there are some nuances worth calling out.

While end user devices are usually compromised by user action, servers may be compromised by vulnerabilities in whatever services or applications they may be hosting. It may be a flaw in a middleware component, an application-level issue that grants remote code execution, or another potential issue.

Not only are server workloads targets themselves, but given their persistence they make good launching points for additional reconnaissance, movement and exfiltration. A compromised web server, for example, may allow an attacker to persist via installation of a web shell and serve as a collection point for any data it wants to exfiltrate out of the organization.

Given the different nature of their workloads when compared to end-user devices, server workloads may have considerations on performance and availability. While modern application moves us closer to horizontal scale-out, not all servers can be quickly bounced.

In the context of XDR, differentiated data on server workloads may be a crucial element in multiple aspects. Servers are often a central point of interaction with some of the most sensitive content and functionality handled by an organization. This helps prioritize incidents and the investigation of both lateral movement and possible exfiltration.

Network Data

The network is the substrate that literally connects us all. As such, it can play a key role in XDR offerings.

Network traffic analysis can be particularly useful across multiple dimensions. Unexplained growth in traffic volume may be worth exploring. Use of new network protocols, particularly those associated with higher privilege or interactive activity such as SSH or RDP, may be indicative of compromise and lateral movement or reconnaissance.

Network data is also quite useful when handing unmanaged devices. There may be multiple reasons why a particular device does not have an endpoint agent, ranging from it not being a corporate-owned device to not being able to run a traditional endpoint agent, as is the case with many IoT devices, be they industrial devices or corporate support equipment. Here, network data provides a glimpse into how the unmanaged device is interacting with the rest of the environment.

A key issue for network traffic analysis remains the increased support for encryption at multiple layers of the stack and the growth in popularity of encryption methods that don't allow interception of traffic. Even then traffic analysis can be useful, or endpoint agents can provide insights as needed.

It's important to note that 451 Research's VotE: Information Security, Organizational Dynamics 2020 survey shows network security remains the most popular option chosen by respondents when asked about important skill sets for a security professional to have.

Cloud Infrastructure Data

With more organizations adopting cloud-based environments, XDR systems can greatly benefit from ingesting cloud infrastructure telemetry.

In the context of monitoring cloud IaaS, every provider offers a rich telemetry source to describe any structural changes to the environment – new virtual machines, new images or more. Vendors also offer ongoing telemetry from activity in that environment – flow logs, DNS request logs and more – as well as increasingly offering security-specific telemetry including threat detection, security findings and others. Use cases for such telemetry include not only detecting attacks against the multiple components that have been deployed to the cloud, but also against the very flexibility of cloud environments themselves: An attacker with the right credentials can affect significant costs to an organization by using those credentials to create new resources for their own purposes (mining cryptocurrency is a favorite, though not the only one).

There are some nuances to work through: While the data from each cloud provider's stream is mostly consistent within the framework of that provider, the data is quite different between providers and sometimes may show inconsistencies even within a single provider. This is particularly true for identity and access management (IAM) telemetry, which becomes even more important in cloud environments than it was on-premises.

Another aspect is that, according to our survey responses, most organizations are using hybrid and multicloud use cases. It falls on centralized teams such as security to oversee security operations in the multiple cloud and on-premises environments, somehow bridging the differences between each cloud provider. This is another use case that XDR may be able to address, particularly for scenarios where the scope extends beyond a single cloud provider.

User Identity Data

There are significant benefits to adding user identification and authentication data to security workflows. User identity can be used as a launch point to determine organizational hierarchy and function, which in turn can be an important element in triage: "the infected laptop belongs to someone who is in finance" or "the apparently compromised account belongs to someone in the privileged users group." Similarly, details about authentication events such as successful and failed logins, multi-factor authentication events and more can provide insights.

This data is generally available via easy-to-query systems such as Active Directory and increasingly in cloud-based systems such as Azure Active Directory and those provided by vendors such as Okta and Ping Identity. XDR offerings have started tying into these systems to extract this information.

User Behavior Data

The broad category of user behavior data covers elements such as browsing histories, including access to SaaS applications, insights derived from user entity and behavior analytics (UEBA) systems, and possibly application-level logging from selected applications.

This data can be useful particularly as teams investigate exfiltration and reconnaissance activities. As an example, it's likely more useful to understand that a specific user logged into the CRM application and downloaded 500 customer files, rather than the 5 or 6 they normally would, instead of focusing on the fact that endpoint *A* connected to server *X* and transferred 50MB over port *Y*.

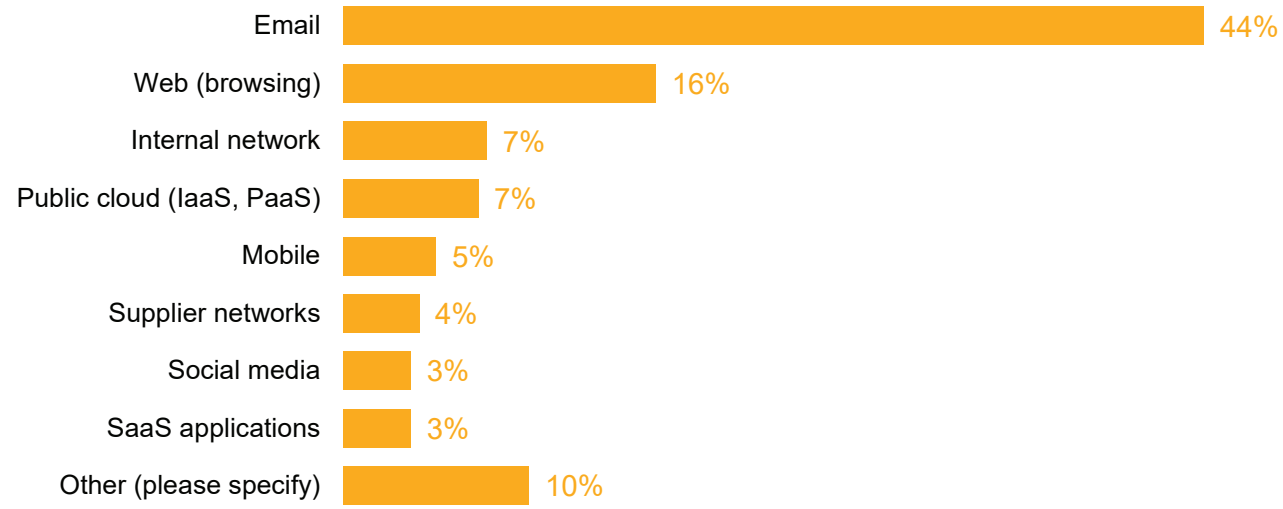
This analysis also extends to user interaction with remote sites, external site reputation, application installation activity and more. The linkage of information such as the department in which the user works may be even more meaningful if that endpoint connects to a site with a reputation as a source of malicious activity or content. A user in finance connecting with a source identified with cybercrime or fraud, or someone in a department responsible for IT functionality on which the business depends connecting with a source associated with ransomware, can do much to escalate containment and response.

Email Data

In the context of being an XDR data source, email data is key. This means not only email security data (emanating from email security vendors with reports of malicious attachments, suspicious senders or domains, etc.), but also regular email telemetry: which messages were sent to which users, who opened it and its disposition thereafter.

Figure 9, extracted from our Organizational Dynamics 2020 study, shows that respondents clearly see email as the vector representing the greatest security threat to the organization.

Figure 9: The Importance of Email



Q. When it comes to data security, which one of the following do you think poses the greatest security threat to your organization?
Base: All respondents (n=230)
Source: 451 Research's Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Why is email so important? For one thing, it's one of the primary intersections of people and technology. This makes it an excellent means for exploiting human behavior. Conceptually, email as a vector gives an attacker a direct connection to a human on the other end of the conversation. If a message is crafted just right – perhaps catching a victim in just the right frame of mind as well – it's quite likely that the user may indeed click through, open the attachment or malicious link and potentially execute content that kicks off further attack actions.

Email threats can include a variety of technical levels – from malware that executes, to phishing that tricks into disclosing passwords, to purely fraud-like emails such as business email compromise that aim to subvert without generating technical fingerprints. Because of its high value to the attacker, adversaries continue to invest in email attack sophistication – which, in turn, continues to drive threat detection and response in this domain.

In the context of XDR, email is particularly useful as investigators look to trace back the source of an attack, or if they want to quickly determine the 'blast radius' of a malicious email campaign. Therefore, both email security and regular email telemetry can and should be used in XDR deployments.

Threat Intelligence

Plenty has been said about how effective use of threat intelligence within a security program is much, much more than just uncritically pulling arbitrary lists of values from a feed to compare against local observations. Useful threat intelligence can help answer questions such as 'are there specific threat actor groups particularly active in relation to the organization, either directly or as part of a broader community?' It can also inform regarding the technical elements of attacks such as domains, IP addresses, email addresses and more that can be used for detections.

There's also a distinction to be made between threat intelligence that is generic in nature – aimed at describing broad threats – versus intelligence focused on an organization's specific sector or even the organization itself. Threat intelligence is also a useful byproduct of the organization's previous security operations activities and should be captured as such.

Given how threat intelligence can bring external and temporal insights into the organization, often mapping it to widely accepted ontologies such as the MITRE ATT&CK framework and related projects, it's widely accepted that threat intelligence can be useful in prioritizing and contextualizing security observations. As such, it is likely to be a key component of XDR offerings either natively or as an add-on.

Vulnerability Data

Having accurate vulnerability data about an asset, particularly in conjunction with additional business details, means being able to prioritize suspicious behavior from an endpoint based on whether the target is a highly secure bastion host or a poorly secured internal server, for example. Naturally, this can greatly aid in the response process as well, such as prioritizing fixes or isolating vulnerable components.

Many of the established vulnerability management vendors – Qualys, Rapid7, Tenable and others – have developed integration capabilities as well as native functionality that should easily fit with current or future XDR offerings.

Additional Security Sources

As an enumeration of the many segments beyond endpoint and network data that can contribute to XDR might suggest, there are potentially a number of additional sources that could be incorporated into XDR approaches to further assist in deriving context for any investigation or triage. The list of security tooling that can assist includes but is not limited to data loss prevention systems, breach detection systems (often based on use of deception techniques), insights from application security programs, results from security testing and more.

Business Context

While many technical alerts can be classified fairly straightforwardly as malicious activity (e.g., the proverbial "PowerShell process spawning from weirdly named binary in temporary directory"), not all indicators reveal themselves to be suspicious or important as easily. In those scenarios and others, failure to contextualize the technical alerts against the organization's business activities is potentially a missed opportunity.

Extracting and codifying business context in a way that can help security operations is much more art than science: there can be meaningful insights derived from HR systems, from corporate travel plans, from marketing initiatives, from recruiting drives, sales promotions and others, but the challenge in using that information in the context of security operations is doing an effective mapping and translation of those concepts into technical indicators.

The same business information used for context can also be used as potential blind spot detection. To what extent can a deeper understanding of the business context help the team better detect malicious activity? As a hypothetical, consider the tying of insight about international business expansion to new cloud presence in international locations as a possible example.

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.

4. Representative XDR Vendors

According to our research, there are currently upwards of 40 vendors aligning their offerings to XDR. The lists in Figures 10 and 11 present a representative sample of XDR offerings currently available or soon to be available, without making specific endorsements or quality assessments of vendors' offerings.

Figure 10: Representative XDR Vendors

Vendor	Description
Cisco Founded: 1984 HQ: San Jose, California CEO: Charles H. "Chuck" Robbins Ticker: CSCO Market Cap: $218bn	Cisco's XDR play combines endpoint visibility from Cisco Secure Endpoint with network detection and response via Cisco Secure Network Analytics, complemented with Umbrella threat visibility, Talos research and the company's overall portfolio of networking and security products. These assets have been brought together in SecureX, the company's recently introduced offering that combines visibility into all these products as well as selected partner integrations including cloud, email and more, with functionality for automating security investigation and response. SecureX allows customers to create custom dashboards and launch threat response investigations that fuse available information into a single view. Customers can then take response actions individually from the same interface or automate them as part of both customized and out-of-the-box playbooks.
Confluera Founded: 2018 HQ: Palo Alto, California CEO: John Morgan Total Funding: $30m	Confluera's approach to XDR revolves around its storyboarding technology, which stitches together various events and alerts to potentially identify and intercept attacks early in their life cycle. The cloud-based analytics engine, IQ Hub, ingests attack telemetry from its own detection technology as well as third-party sources. The company's integration framework ingests data from firewalls, Windows and Linux server workloads, containers, cloud logs, vulnerability management systems, and external threat intelligence. As a result of the analytics, Confluera provides different tools and capabilities including scoring and ranking, attack campaign narratives, and response actions.
CrowdStrike Founded: 2011 HQ: Sunnyvale, California CEO: George R. Kurtz Ticker: CRWD Market Cap: $38.5bn	As of late March 2021, CrowdStrike does not sell an explicit product offering for XDR but proposes that it has been able to solve for the same correlated event outcomes based on its cloud-native Falcon platform architecture. Originally focused on endpoint security use cases such as EPP and EDR, the company added support for vulnerability management, IT operations, zero trust assessment and enforcement, cloud security and more, backed by threat intelligence and managed services. CrowdStrike also highlights the CrowdStrike Store, which added integration for additional data sources, functionality and third-party vendors. CrowdStrike recently acquired data analytics and log management vendor Humio with the expectation to support data collection from additional sources, and to make that data available for XDR scenarios.
Cybereason Founded: 2012 HQ: Boston, Massachusetts CEO: Lior Div-Cohen Total Funding: $390.38m	Cybereason is an endpoint-centric vendor that has expanded on its core endpoint security offering to include XDR support. Cybereason's approach is centered on the concept of a 'Malop' (short for 'malicious operation'), which is how the company correlates disparate signals and alerts into an actionable attack story, including root cause and a proposed guided response. Originally focused on endpoint data, Cybereason's Malops now extends detection and response capabilities to cloud identity, workspace providers and network data, including Okta, Microsoft, AWS and Google. Cybereason indicated it will be adding integrations with additional cloud security vendors, along with protection for cloud workloads in Azure and Google.

Vendor	Description
Fortinet Founded: 2000 HQ: Sunnyvale, California CEO: Ken Xie Ticker: FTNT Market Cap: $30bn	Fortinet has been positioning its recently launched FortiXDR offering as a new extension that builds on its well-established Fortinet Fabric architecture. Fortinet has traditionally positioned the Fabric architecture as the common platform for its multiple offerings – network, endpoint, email, cloud, user behavior analytics, threat intelligence and more – as well as offerings from selected partners (via connectors). FortiXDR is expected to leverage this architecture by adding ML for investigation, use of deeper analytics methods, consolidation of security alerts, and increased automation support for faster responses.
Hunters Founded: 2018 HQ: Tel Aviv, Israel CEO: Uri May Total Funding: $20.4m	Hunters is one of the vendors pursuing an 'open XDR' approach. The company highlights that its cloud-based platform has integrations with key security vendors in endpoint security, cloud, network, identity and email, plus threat intelligence. Those sources then feed a data lake, which the company uses to build a proprietary knowledge graph that supports multiple security analytics capabilities. These capabilities include correlation, threat detection and investigation exercises that stitch up distinct signals into prioritized 'attack stories' that include context and incident information for timely and effective response. These are streamlined into response workflows, SOAR or ticketing systems. Hunters also offers optional threat hunting and incident response services.
McAfee Founded: 1987 HQ: San Jose, California CEO: Peter A. Leav Ticker: MCFE Market Cap: $3.5bn (Implied Market Cap: $9.3bn)	McAfee's approach to XDR centers on having an adaptive platform and that the combination of endpoint security and support from its network security products, threat intelligence insights, data-aware intelligence and integration capabilities meets customers' expectations of XDR. The company proposes that a combination of prioritization of threats, predictive assessment and prescriptive recommendations are required for efficient security operations. According to McAfee, XDR capabilities have been offered since late 2018 when it delivered EDR/SIEM integration, augmented by its MVISION Insights offering. McAfee is currently working on additional automation capabilities. The company proposes that as an established endpoint provider with an option to integrate non-McAfee products, it can provide customers a solid foundation on their XDR journey.
Microsoft Founded: 1975 HQ: Redmond, Washington CEO: Satya Nadella Ticker: MSFT Market Cap: $1.75 trillion	Microsoft's approach to XDR is to provide a set of capabilities spanning end-user and infrastructure environments. These capabilities include identities, endpoints, cloud applications, documents and email, virtual machines, databases, IoT, containers and cloud workloads. Microsoft delivers these in two experiences: Azure Defender for infrastructure environments and Microsoft 365 Defender for end-user environments. Complementing the XDR capabilities of the Defender products, Microsoft offers its Azure Sentinel SIEM, which supports ingesting data from different data sources including multicloud, multi-platform and third-party security products. Microsoft also highlights the role of analytics backed by ML capabilities to reduce alert fatigue and the TI capabilities of the Microsoft Graph, which is informed by Microsoft research and signals from Microsoft's set of cloud properties.
Palo Alto Networks Founded: 2005 HQ: Santa Clara, California CEO: Nikesh Arora Ticker: PANW Market Cap: $32bn	Palo Alto Networks has made XDR a key pillar of its overall security portfolio, alongside Strata (network security) and Prisma (cloud security) product lines. Cortex XDR stitches together security telemetry from data sources including network, endpoint, IAM and cloud infrastructure. The company has iterated on the technology it acquired from SecDO (for EDR) and LightCyber (UEBA) for its XDR platform. The company also emphasizes the role its broader threat intelligence and threat hunting services play in supporting XDR. The company has also teamed up with numerous service providers that have chosen Cortex XDR for their service offerings.

Vendor	Description
ReliaQuest Founded: 2007 HQ: Tampa, FL CEO: Brian Murphy Total Funding: $330m	Leveraging its unified threat detection, investigation and response platform GreyMatter, ReliaQuest announced its Open XDR approach in October 2020. The security tool-agnostic platform integrates disparate security technologies and data to provide unified, actionable visibility and insights across the entire IT environment. Utilizing a combination of technology, ML, analytics and human analysis, GreyMatter proactively identifies threats and eliminates noise, giving security teams situational awareness to orchestrate and automate response to threats in real time. The SaaS-based platform integrates the security tools enterprises have already deployed, ensuring that tools are properly implemented, configured and tuned to increase efficacy. The offering also includes an evolving library of pre-built playbooks, automated threat hunting packages, and attack simulations for continuous assurance and consistent outcomes.
Sophos Founded: 1985 HQ: Abingdon, United Kingdom CEO: Kris Hagerman	Expanding on its well-established Intercept X endpoint and server protection technologies, Sophos has recently released new XDR features and capabilities within the product line. In addition to data from endpoints and servers, Sophos' XDR enables organizations to ingest network data sources, including data from its XG Firewall and Cloud Optix products, to gain an in-depth picture of potential threats across the organization's IT ecosystem. The company plans to add additional data sources in the near future. For customers that need help with security operations, the company delivers XDR as a managed service through its Sophos Managed Threat Response (MTR) offering. The company is channel-focused, partnering with managed service providers to go to market and deliver enriched security services.
Stellar Cyber Founded: 2015 HQ: Santa Clara, CA CEO: Changming Liu Total Funding: $21.8m	Stellar Cyber's cloud-native Open XDR platform combines pervasive data collection, big data processing, advanced analytics with ML and automated response to deliver contextualized, normalized, enriched telemetry for detection, triage, investigation, hunting and response in a single intelligent platform. Utilizing sensors placed on networks, servers, containers, and physical and virtual hosts, the platform captures, correlates and analyzes data from a variety of sources, including network traffic, endpoints, logs, applications, user information and geo data. Telemetry data and the customer's existing cybersecurity tools are combined with threat intelligence and automatic correlation to increase alert fidelity, reduce false positives, prioritize alerts and increase detection efficacy. The platform offers an array of native automation and orchestration capabilities and provides several native security applications, including SIEM, NTA, automated threat hunting, UBA, asset management and threat intelligence platform. The company targets its platform for both enterprises and managed service providers.
Trend Micro Founded: 1988 HQ: Tokyo, Japan CEO: Eva Chen Ticker: Tokyo Stock Exchange: 4704 (OTC: TMICY) Market Cap: $7bn (780.9bn JPY)	Trend Micro has made XDR a key component of its portfolio, centered around the Trend Micro Vision One offering. Trend Micro Vision One consists of a SaaS offering that aggregates data from Trend Micro's other product families covering endpoint, email, server and cloud workloads, and network security. Customers then use a dedicate interface to search, detect, investigate and respond to threats by leveraging available data sources. The offering includes support for agent and policy management, integrations with external SIEM-SOAR systems via API, and risk-based insights including use of unsanctioned applications and prioritized lists of devices or users. Trend Micro also offers a managed services offering for managed XDR.

Vendor	Description
VMware Founded: 1998 HQ: Palo Alto, California CEO: Zane C. Rowe Ticker: VMW Market Cap: $63bn	VMware is offering some XDR capabilities now by combining distinct products and using the VMware Carbon Black Cloud Platform as the centerpiece. Carbon Black Cloud Endpoint Protection targets end-user devices and can also integrate with Workspace One, where customers can use additional scoring and playbooks to accelerate response based on user intelligence. Carbon Black Cloud Workload is for cloud workloads and integrates with vSphere. VMware also looks to soon include the ability to consider intelligence from the VMware NSX portfolio and more integrations with Lastline, CloudHealth, Tanzu and other properties. VMware indicates it will look at partners for functionality such as service management, SIEM and SOAR.

Source: 451 Research, 2021

With the caveat that this list is not fully comprehensive of all current or upcoming XDR vendors, additional names to consider are shown in Figure 11.

Figure 11: Additional Vendors With XDR offerings, Plans or Adjacencies

Vendor	Brief Description
Alert Logic	Although the company does not position its SaaS-based MDR platform as an XDR offering, it provides many of the capabilities of XDR wrapped with managed services.
AT&T	The company is looking to leverage its managed security services offerings and its AlienVault USM platform as a key component of its upcoming XDR strategy.
BitDefender	The company positions its GravityZone offering as having XDR capabilities, given the integration of data from endpoint, network and cloud sources.
BlackBerry	BlackBerry has indicated that it will soon support XDR, as it will offer a cloud-based version of its Optics EDR product.
Check Point	The company recently updated its portfolio and plans to emphasize its XDR capabilities, which are centered around its Infinity-Vision unified management offering.
Cynet	Has an integrated offering that includes functionality for endpoint security, network threat analytics, deception, user behavior analysis and managed services.
Elastic	Doesn't offer explicit XDR positioning but has integration between SIEM and its own endpoint security agent (Endgame acquisition).
eSentire	Utilizing its proprietary cloud-native XDR platform Atlas, eSentire delivers a broad portfolio of managed detection and response services.
Exabeam	The SIEM vendor has recently adopted XDR as an overarching message for its analytics, automation and response capabilities.
expel	The MDR provider offers a broad range of XDR capabilities wrapped with managed services.
Fidelis	With its Elevate XDR platform, the company offers integrated NDR, data loss prevention, deception and EDR in one unified solution.
FireEye	FireEye recently acquired Respond Software to build up a controls-agnostic approach with XDR capabilities, which it says will also work with other FireEye products including Helix.
Huntress Labs	The company focuses primarily on SMB end users via partners and has added network and cloud support to its SaaS-based managed offering as the basis for supporting XDR use cases.
IBM	IBM is not using explicit XDR messaging, but its Cloud Pak for Security offering shares some characteristics with other XDR vendors such as integration of multiple sources. IBM also has managed services offerings.
Kaspersky	The company does not have explicit XDR messaging, but has a suite of products that cover multiple data sources and can provide integrated approaches to SOC teams.

Vendor	Brief Description
Kognos	Kognos emerged from stealth in late 2020, launching with a technology-agnostic XDR platform. The platform, named Autonomous XDR Investigator, generates relationship graphs using data from EDR, NDR and SIEM products to model an overall attack campaign.
LogRhythm	The company recently acquired MistNet for its network-based threat hunting capabilities and has positioned its combination of SIEM, UEBA and network as XDR.
Qualys	The company recently indicated it is in the final stages of development of an XDR offering, which aims to provide correlation between Qualys sensors and external sources as well as support orchestration.
Rapid7	While marketed specifically as an XDR solution, the company offers a number of integrated products that achieve many of the same goals and outcomes as other XDR platforms.
SecBI	The company has an offering aimed at MSPs and MSSPs that supports integration with external third-party vendors, as well as support SecBI's autonomous investigation offering.
SecureWorks	Well known for its managed security services offerings, the company announced a productized version of its security platform earlier this year. The platform, Taegis XDR (previously Red Cloak TDR), is a cloud-native SaaS solution that combines analytics, data modeling and threat intelligence to detect threats.
SentinelOne	The endpoint-centric vendor recently acquired Scalyr to expand its XDR efforts and launched a marketplace for partner integrations.
Tanium	The endpoint-centric vendor has support for both security and operations use cases and has a partnership with Google to use Chronicle as a platform for XDR-like use cases.

Source: 451 Research, 2021

5. Looking Ahead

As XDR evolves (and organizations seek to gain broader and more robust telemetry), messaging and opportunities will continue to grow and extend beyond current providers. The topic is likely to capture more attention and drive much of the conversation as it relates to the evolution of security operations practices. Security technologies, vendors and service providers will need to develop and communicate their position and value-add to an XDR security approach.

XDR will look vastly different from today within a relatively short timeframe. The evolution will be rapid and the competition will be fierce as vendors and providers seek to gain market share, spurring innovation, differentiation and M&A activities on multiple fronts. Several traditional security product categories, such as SIEM and SOAR, run the risk of becoming less relevant as XDR approaches increasingly include automation, log ingestion and storage and analytics as part of their standard offerings. Conversely, however, entrenched capabilities such as SOAR platforms in which organizations may have invested considerable effort may discourage prospects from adding yet another automation tool simply because it's part of an XDR offering, instead presenting an opportunity for SOAR vendors to capitalize on XDR and add it to augment capability. For SIEM vendors and others that have embraced SOAR, it also provides an opportunity to consolidate XDR with their approach.

As vendors fine-tune their XDR offerings, we expect XDR to draw a portion of the interest currently aligned to SIEM regardless, particularly for scenarios where most of the insights can be derived from data that is feeding the XDR components. Additional SIEM use cases – including broader IT infrastructure monitoring, audit and compliance reporting, fraud detection and others – are unlikely to be incorporated into XDR at this point.

Security teams will seek to extend the capabilities of XDR to an increasingly growing and dynamic IT ecosystem. In the long term, product-centric approaches will likely give way to XDR providers that strategically combine telemetry-focused, analytics-focused and services-focused approaches. However, in the short term, given the heterogeneity of the client base, we expect all key XDR approaches – telemetry-centric, analytics-centric and services-centric – to find footing with at least a subset of customers. We expect several other vendors to increase alignment to XDR, even by the thinnest of threads. To the extent that any offering can detect threats (if not also enable some approach to response), 'XDR-washing' is quickly becoming a reality.

Endpoint security conversations (and sales opportunities) will be heavily influenced by XDR. With most large or established endpoint security vendors offering XDR capabilities, we expect XDR to be used as the differentiating factor by competitors. Ironically, as more competitors position XDR, it no longer becomes a differentiation. This can work in favor of both larger strategic vendors – which can then point to other aspects of their portfolios – as well as more focused endpoint security vendors that can find a shorter path to revenue compared to larger strategic sales.

XDR will likely follow several of the trends in the MDR space, adding an array of ancillary features and capabilities, including attack surface discovery/management, continuous automation security testing and validation, IoT and OT threat detection and response, security tool configuration and efficacy testing, and continuous risk scoring.

The impact on future investments will be interesting to watch. Enterprises will need to decide if they prefer security tools that conform to their XDR platform or favor XDR platforms that can support their choice of security tools and services. EDR and NDR providers will need to decide how they will adapt to an integrated XDR approach. Those that lack the capacity or desire to evolve may find a diminishing market for their single telemetry-focused solutions.

The impact on the services space will be disruptive as well. While many XDR providers are partnering with MSPs and MSSPs to empower them to deliver managed detection and response services, the lack of expertise and human resources within these providers may limit the expansion XDR vendors envision within this space. At the same time, XDR vendors will see increased competition from MDR providers that, in many cases, have more mature offerings and support a broader range of use cases in addition to offering a range of supportive managed services to help facilitate threat detection and response.

Vendors will need to watch the complexity of their data models. A key challenge when looking at XDR is just how the addition of new data sources will affect the overall product or service architecture and response. There are at least two dimensions to consider:

- **How complex does the data model get, and how quickly?** How does the data model account for how diverse sources treat identifiers in possibly incompatible ways? To use a simple example, any system that makes assumptions about an object being identified by an IP address will be challenged to interpret insights from one where IP addresses are fungible, such as modern containers/Kubernetes environments.
- **Does the 'curse of dimensionality' apply?** In ML, the 'curse of dimensionality' refers to the phenomenon where, as the number of dimensions being used in a particular model increases, the overall size of the multi-dimensional space increases but the actual number of observations does not. This leads to a scenario where individual observations become sparsely distributed, which in turn means that deriving statistically meaningful results requires exponentially more data.

Organizational security teams will need to be wary of distracting information. Particularly as they compete with others, vendors tend to include elaborate visual representations or seemingly quantitative scoring elements in their user interfaces, but those may not have the desired effect. Many security operations teams quickly dismiss overly complex visual representations, such as geographic maps that overlay current attack information. This is such a common phenomenon that the industry refers to these displays as 'pew-pew maps' with derision.

Similar concern starts to emerge as numerous vendors include variations of 'scoring' on their user interfaces, where the expectation is that customers will be able to use a numeric score to somehow gauge their progress in security operations or overall security health. The topic is fraught with danger in at least two ways. First, invariably the scoring systems proposed by vendors represent a simplistic understanding of technical elements that can easily be measured and fail to account for relevant information such as underlying asset distributions, asset values, potential impacts to the business, business seasonality trends and expansion/contraction of IT assets. And second, the relevance of metrics involved is not always clear. These are often unitless measurements that may be subjective or relative to some ill-defined parameter such as 'low,' 'medium' or 'high.' Without addressing these problems in more concrete ways, metrics such as these run the risk of burning through credibility capital faster than they can evolve.

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.

7. Further Reading

2021 Trends in Information Security, December 2020

Evolution of Managed Detection and Response Services, June 2020

As security use cases demand more analytics, CrowdStrike nabs Humio for its XDR offering, February 2021

SentinelOne suits up for XDR trend with Scalyr acquisition, February 2021

Endpoint Security Market Map 2020, December 2019

SASE, ZTNA and XDR: Three security trends catalyzed by the impact of 2020, August 2020

2021 Tech M&A Outlook: Information security, February 2021

Voice of the Enterprise: Information Security, Budgets and Outlook 2020

Voice of the Enterprise: Information Security, Organizational Dynamics 2020

Voice of the Enterprise: Information Security, Workloads & Key Projects 2020

Appendix – Selected M&A Transactions

The table below, extracted from 451 Research's M&A Knowledgebase, highlights the recency of XDR. Highlighted transactions refer specifically to XDR in their records. It's notable that many of the strategic acquirers made key purchases of endpoint security vendors and orchestration vendors in the past three years, which forms the basis of their XDR offerings.

Announced	Acquirer Name	Target Name	Sector	Total Deal Amount
14-May-21	Fidelis Cybersecurity Inc.	CloudPassage Inc.	Server protection SaaS	Undisclosed
25-Mar-21	Kroll LLC [Duff & Phelps] [Stone Point/Further Global/Permira]	Redscan	Managed detection & response	Undisclosed
18-Feb-21	CrowdStrike Holdings Inc. [NASDAQ:CRWD]	Humio Ltd.	Log management software & SaaS	$392,000,000
9-Feb-21	SentinelOne Inc.	Scalyr Inc.	Log management & analytics SaaS	$155,000,000
13-Jan-21	LogRhythm Inc. [Thoma Bravo]	MistNet	Cybersecurity SaaS	Undisclosed
19-Nov-20	FireEye Inc. [NASDAQ:FEYE]	Respond Software Inc.	Anti-malware security software	$186,000,000
13-Oct-20	BlueVoyant LLC	Managed Sentinel Inc.	Microsoft-based managed cybersecurity	Undisclosed
16-Sep-20	Avertium [Sunstone Partners]	NetBoundary Inc. [dba 1440 Security]	Managed security services	Undisclosed
25-Aug-20	Palo Alto Networks Inc.	The Crypsis Group [ZP Group]	Cybersecurity advisory services	$265,000,000
4-Jun-20	VMware Inc. [NYSE:VMW] [Dell EMC] [Dell Technologies Inc.]	Lastline Inc.	AI anti-malware software & SaaS	$160,000,000 *
20-May-20	Open Systems AG [EQT Partners]	Born in the Cloud Inc.	Managed security services	Undisclosed
13-May-20	VMware Inc. [NYSE:VMW] [Dell EMC] [Dell Technologies Inc.]	Octarine Inc.	Kubernetes application security SaaS	Undisclosed
28-Oct-19	Fortinet Inc. [NASDAQ:FTNT]	enSilo Inc.	Endpoint security SaaS & services	$20,000,000
22-Aug-19	VMware Inc. [NYSE:VMW] [Dell EMC] [Dell Technologies Inc.]	Carbon Black [fka Bit9] [NASDAQ: CBLK]	Endpoint & server security software	$2,100,000,000
5-Jun-19	Elastic NV [fka Elasticsearch] (NYSE: ESTC)	Endgame Inc. [fka Endgame Systems Inc.]	Endpoint security software & SaaS	$234,000,000
19-Feb-19	Palo Alto Networks Inc.	Demisto Inc.	Security orchestration software	$560,000,000
16-Nov-18	BlackBerry Ltd. [fka Research In Motion]	Cylance Inc.	AI-based security SaaS	$1,400,000,000
10-Apr-18	Palo Alto Networks Inc.	Secdo Ltd.	Endpoint security automation SaaS	$90,000,000 *

Announced	Acquirer Name	Target Name	Sector	Total Deal Amount
24-May-17	Microsoft Corporation	Hexadite	Automated cybersecurity SaaS	Undisclosed
30-Jun-15	Cisco Systems Inc.	OpenDNS	Network & BYOD security SaaS	$635,000,000
23-Jul-13	Cisco Systems Inc.	Sourcefire, Inc.	Intrusion detection & prevention & anti-malware	$2,700,000,000
15-Dec-03	Check Point Software Technologies Ltd.	Zone Labs, Inc.	Data security firewalls	$256,239,000

*451 Research estimate

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