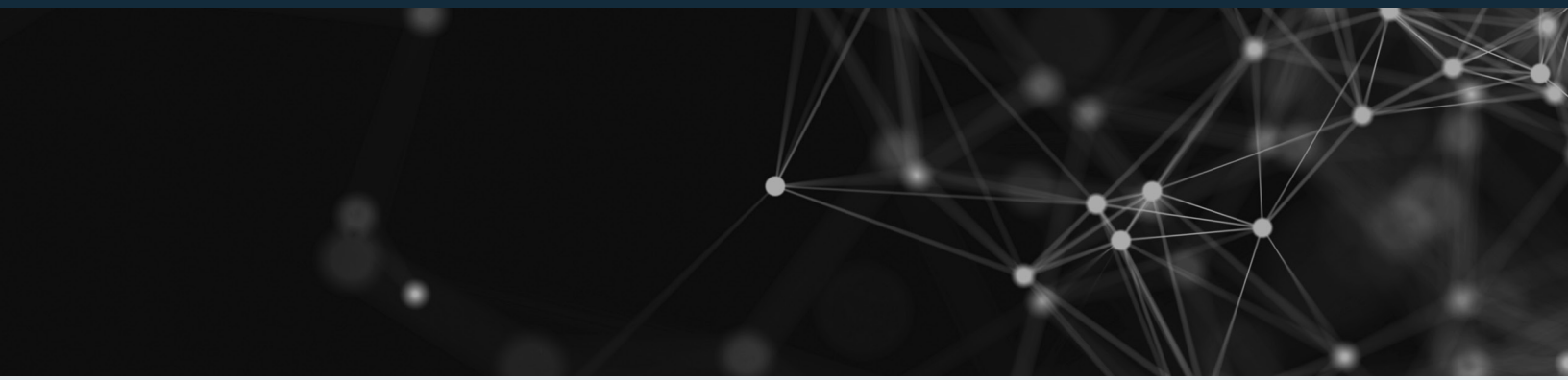


Foreword from Rapid7

Since the launch of Rapid7's cloud-native XDR, InsightIDR, six years ago our mission has remained constant: make it possible for ***any*** security team to achieve fast, sophisticated threat detection and response programs that scale with their business. While the "XDR" acronym may be new, the outcomes and approach have been aligned with our methodology around detection and response since the start.

InsightIDR provides the scale and contextualized insights that SOCs need to detect threats faster, respond smarter, and secure everywhere.

Simplify SecOps, elevate outcomes. Today's security analyst has to be a Renaissance player to be successful versus attackers. InsightIDR is cloud-native and SaaS-delivered to eliminate the distractions of months-to-years-long deployments and configurations. With a focus on flexibility, intuitive UI, and a highly contextualized view of the environment "out of the box," InsightIDR helps teams level-up resources and see value on day one.

Transform security as your business scales. InsightIDR provides a harmonious, correlated view of users, endpoints, network, cloud, and applications out-of-the-box. No more tab-hopping between disparate tools. Unlock the scale and extended visibility needed to keep up with digital transformation.

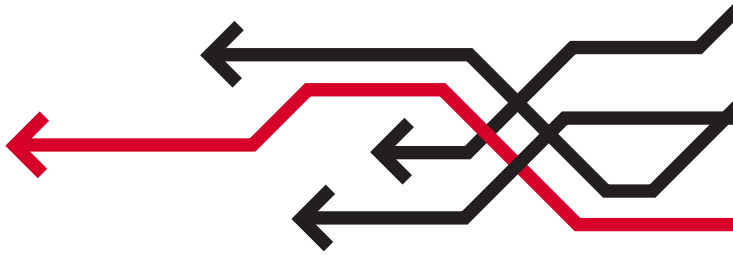
Trust your detections, immediately. InsightIDR takes a multi-layered detection approach, leveraging our knowledge of customer environments along with our internal and community-infused threat intelligence to fuel our attack surface mapping and detections library. This highly curated library is then expertly tested in the field by our industry-leading MDR SOC. The result is a robust collection of high-fidelity, relevant detections that teams can feel confident acting on.

Accelerate response, stay ahead of attackers. When your team is up against an attack every second matters. With detailed, correlated investigations in InsightIDR, teams have the full timeline of an attack and all relevant information they need in one place. With expert- and community-driven playbooks, and containment and automation built in, analysts are empowered to eliminate threats faster—before attackers can succeed.

With XDR from Rapid7, teams have the contextualized insights and streamlined SecOps they need to focus on what matters most.

To learn more about XDR, please enjoy this complimentary excerpt from 451 Research's report: The Rise of XDR.

REPORT EXCERPT



Technology & Business Insight

Thought Leadership

June 2021

The Rise of Extended Detection and Response

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

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

Scott Crawford **Research Director, Security**

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

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

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

451 Research

S&P Global
Market Intelligence

Table of Contents

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

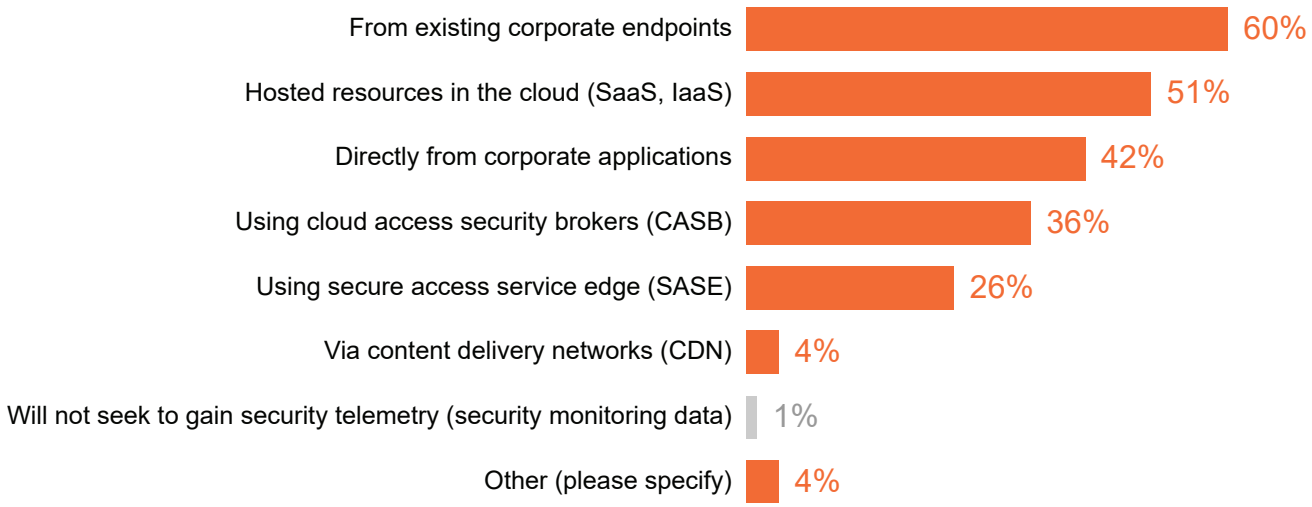
If there's one data source that could be considered primary for XDR, that must be endpoint data. Indeed, as we preview some of the later findings of this paper, endpoint shows up as the most common source reported by vendors. This is by design, as several factors have raised the prominence of the endpoint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

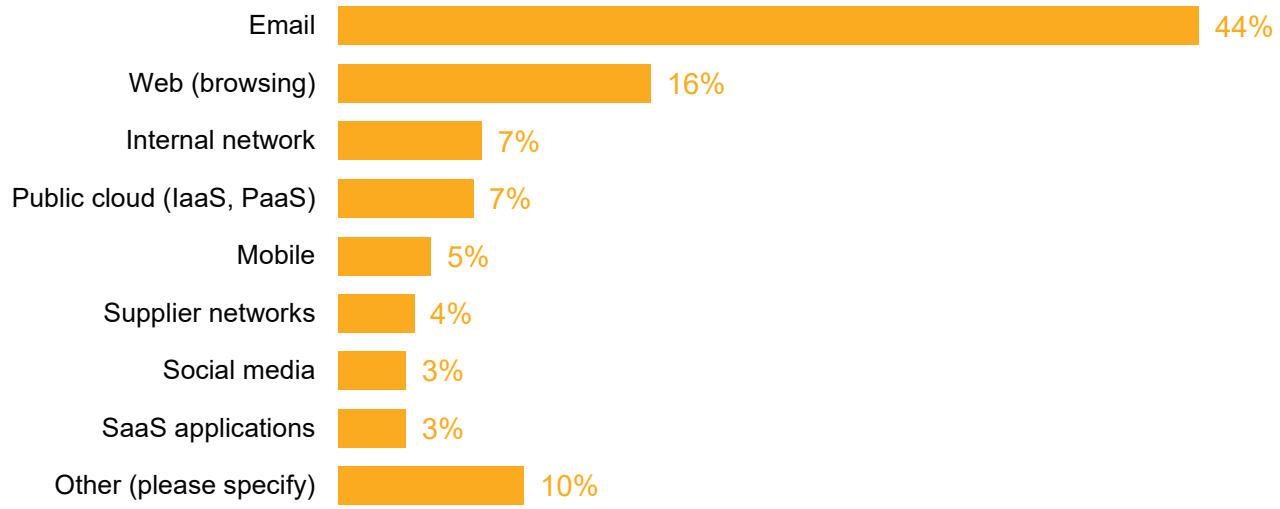
This analysis also extends to user interaction with remote sites, external site reputation, application installation activity and more. The linkage of information such as the department in which the user works may be even more meaningful if that endpoint connects to a site with a reputation as a source 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.

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.

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

Rapid7 simplifies cybersecurity with best-in-class solutions across vulnerability risk management, cloud security, and threat detection and response. Our cloud-delivered platform gives you the visibility and clarity to confidently drive business forward.

InsightIDR - Rapid7's cloud native, SaaS XDR - provides the scale and contextualized insights that SOCs need to detect threats faster, respond smarter, and secure everywhere. By simplifying SecOps and elevating outcomes, InsightIDR enables teams to focus on what matters most, and accelerate their security programs.

Learn more about Rapid7 and XDR here.