



ESG WHITE PAPER

The Future of XDR is Now!

By Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

August 2021

This ESG White Paper was commissioned by FireEye and is distributed under license from ESG.



Contents

Contents	2
Executive Summary	3
The State of Threat Detection and Response	3
Organizations Face a Multitude of Threat Detection and Response Impediments	5
What’s Needed for Threat Detection and Response	6
FireEye XDR.....	8
The Bigger Truth	9

Executive Summary

According to ESG research, many organizations plan to increase investments in threat detection and response this year.¹ Unfortunately, this is because current threat detection and response strategies aren't working well, so security operations center (SOC) teams need improvement across people, process, and technology.

Recognizing the myriad of issues with threat detection and response, security technology providers are pushing new technology solutions dubbed eXtended Detection and Response or XDR. These tools are designed to address many of today's technology issues with an integrated security architecture, advanced analytics, and simplified operations. Sounds great, but users remain confused about what XDR is and where to start.

Is XDR real? If so, what are the most important attributes of XDR? This white paper concludes:

- **Organizations have numerous threat detection and response objectives.** SOC teams are increasing spending because they have ambitious threat detection and response plans. ESG research indicates that organizations want to improve detection of advanced threats, increase process automation around remediation tasks, and improve incident response (IR) timing, amongst other priorities.
- **Threat detection and response impediments abound.** While SOC teams have numerous objectives, they face several historical vexing challenges, including increasing complexity, resource constraints, a growing/changing attack surface, and a dependence on independent point tools. These obstacles tend to increase adversary dwell time and can lead to costly cyber-attacks, data breaches, and devastating impacts to business operations.
- **XDR is an emerging solutions architecture.** In 2016, ESG defined a new type of integrated technology for security operations called a security operations and analytics platform architecture (SOAPA). Since no commercial SOAPA solutions were available, however, organizations needed to build their own, limiting SOAPA to those with strong security engineering and ample resources. In 2020, vendors started offering XDR, which was essentially a turnkey SOAPA solution. As XDR matures, it has the potential to act as a quantum improvement for threat detection and response.
- **Leading XDR solutions will feature five key attributes.** ESG believes that leading XDR solutions will provide coverage across major threat vectors, an "outside-in" view built on comprehensive threat intelligence integration, advanced cross-domain analytics, process automation, and central management.

The State of Threat Detection and Response

Threat detection and response remains a priority at most organizations. For example, ESG research indicates that 83% of organizations will increase spending on threat detection and response technologies, services, and personnel in the next 12 to 18 months. Furthermore, organizations have well-defined threat detection and response objectives including (see Figure 1):

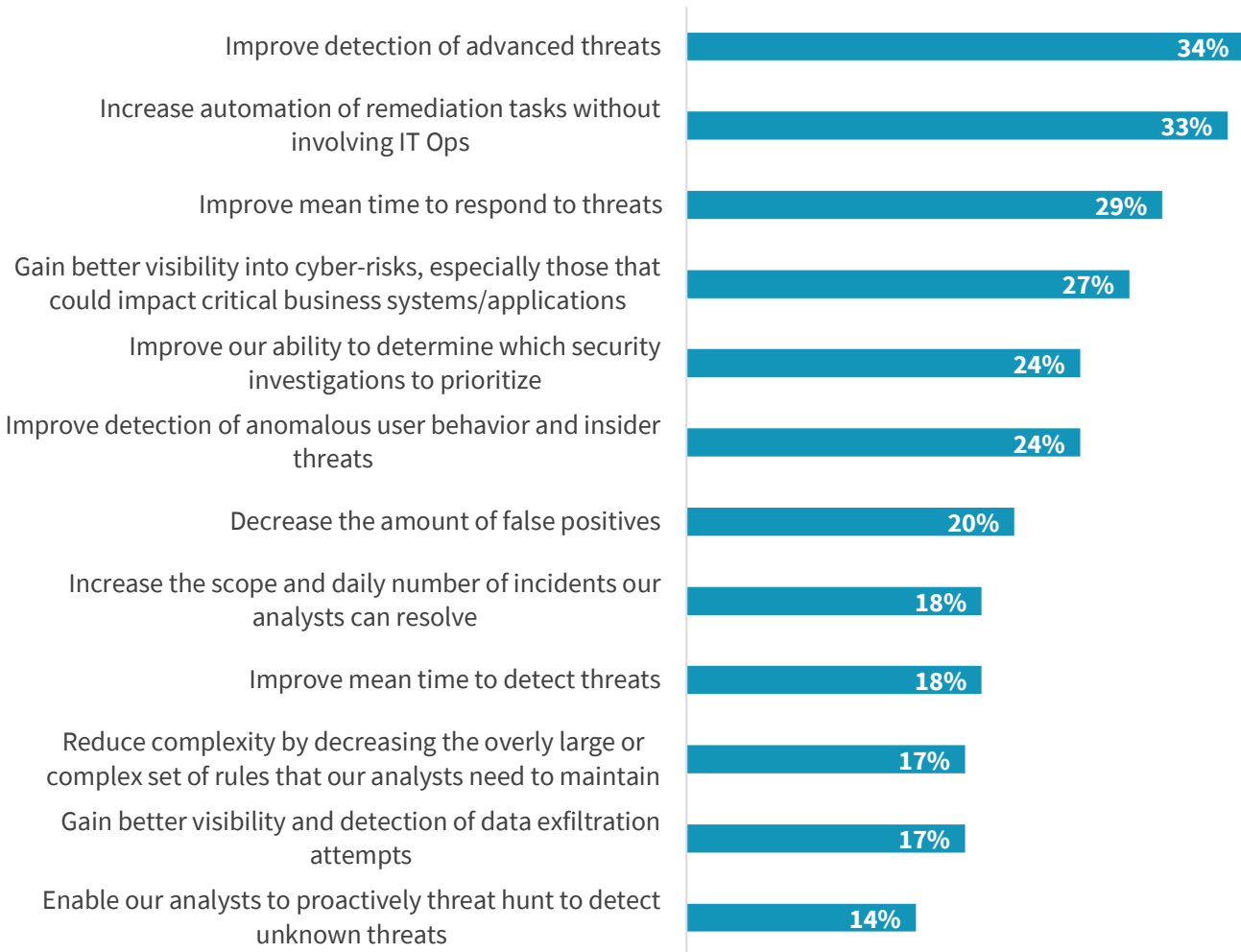
- **Improving the detection of advanced threats.** Organizations need to improve their ability to detect sophisticated multi-staged malicious campaigns like APTs, often described as "low and slow" attacks. This will require several advancements, including creating higher-fidelity security alerts, crafting cross-domain analytics, and integrating threat intelligence into security operations tools and processes. Many firms are using the MITRE ATT&CK framework as a guideline for advanced threat detection.

¹ Source: ESG Research Report, [The Impact of XDR in the Modern SOC](#), March 2021. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.

- **Increasing automation of remediation tasks.** Security operations have always relied on manual processes, leading to inefficiency and scalability problems. Recognizing these issues, CISOs want more process automation around remediation tasks without involving the IT operations team. When threat intelligence uncovers dangerous indicators of compromise (IoCs), security teams want a closed-loop process that automatically blocks malicious IP addresses, files, and domains at network perimeters, endpoints, cloud-based secure access service edge (SASE) tools, etc.
- **Improving mean time to respond to threats.** Closely aligned with automating remediation tasks, organizations want to accelerate their threat responses. To do so, SOC teams will have to improve all preliminary activities, including enriching and triaging alerts, conducting security investigations, prioritizing response actions, and working with IT operations on remediation. CISOs will need help from IT teams to accomplish these goals.

Figure 1. Threat Detection and Response Program Goals

When thinking about your organization’s overall threat detection and response program goals, what would you say are your top areas of focus for improving your organization’s overall security? (Percent of respondents, N=388, three responses accepted)



Source: Enterprise Strategy Group

It is also noteworthy that 27% of respondents say that they want to gain visibility into cyber-risks that could impact critical business systems. This could include misconfigurations, expired certificates, software vulnerabilities, and other issues that

may be easily exploited by sophisticated cyber-adversaries. Improved visibility of cyber-risk can help organizations better focus threat management activities.

Organizations Face a Multitude of Threat Detection and Response Impediments

Based on the data presented above, CISOs recognize that their threat detection and response programs need a lot of work, and they've set aggressive goals for improvement. While these objectives are admirable, SOC teams must overcome numerous challenges to achieve them. Threat detection and response programs remain constrained because of:

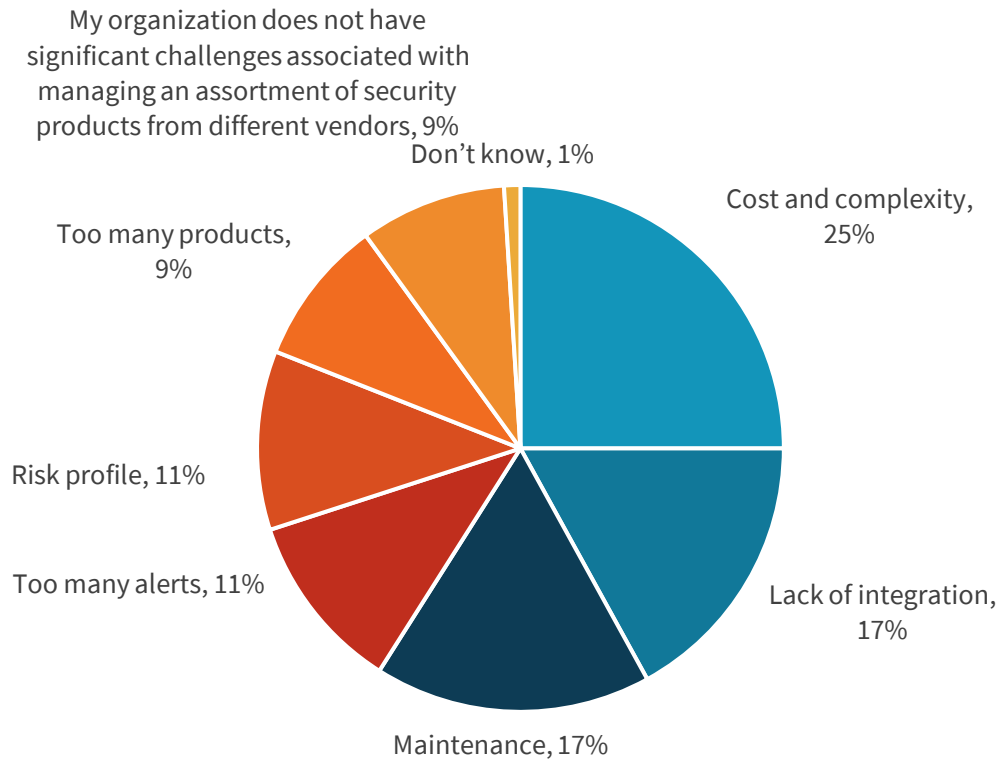
- **Increasing complexity.** Over the past few years, organizations have embraced SaaS, moved applications to cloud hosting on AWS, Azure, and others, developed cloud-native applications, and supported a growing army of remote workers and third parties. While many of these initiatives were in process, they were greatly accelerated in 2020 and 2021 in response to changing IT requirements driven by the global pandemic. Taken together, all these trends have produced a complex hybrid IT infrastructure and ever-growing and changing attack surface. To prevent, detect, and respond to threats, SOC analysts must have granular and continuous visibility into all assets and be able to identify and remediate problems rapidly as they arise—difficult tasks at best.
- **Resource constraints.** According to a recent cooperative research survey conducted by ESG and the Information Systems Security Association ([ISSA](#)), 57% of organizations claim they have been impacted by the global cybersecurity skills shortage, and 44% believe the skill shortage has gotten worse over the past few years. Ramifications of the skills shortage include an increasing workload on the cybersecurity staff, perpetually open job requisitions, and high rates of staff burnout.² While CISOs have bold threat detection and response plans, they may not have the internal skills or staff to meet the goals they set.
- **Changing threat landscape.** While most organizations have continually increased cybersecurity spending over the past few years, they remain ill-prepared for the sophisticated attacks that have become more commonplace. These incidents include the Kaseya Ransomware (July 2021), the Colonial Pipeline Ransomware (June 2021), the Microsoft Exchange Attack (March 2021), the Florida water system attack (February 2021), and the SolarWinds breach (December 2020). These incidents can carry high and unexpected costs. In April 2021, SolarWinds estimated that addressing the hack could cost the company \$18 million, while US federal government analysts claimed the total cost to the economy could exceed \$100 billion. Modern attacks are often conducted surreptitiously over weeks or months and are designed to circumvent security controls. Even well-resourced organizations are susceptible.
- **Point tools-based security controls and analytics.** Enterprise security infrastructure was developed organically with new controls and analytics added gradually over time. This patchwork approach has led to silos of security that carry multiple challenges to manage like cost and complexity, a lack of technical integration, cumbersome maintenance, and constant alert storms (see Figure 2). Ironically, despite all these disparate point tools, many organizations lack visibility into the right data sources necessary for analyzing security data and detecting true threats in real-time.

Much to CISOs' chagrin, existing security strategies and technologies are a mismatch for modern threats. Without changes, organizations lack the right controls for threat prevention and face increasing risk and disruptive security events. Clearly, organizations need new approaches for threat detection and response.

² Source: ESG Research Report, [The Life and Times of Cybersecurity Professionals 2021 Volume V](#), July 2021.

Figure 2. Top Organizational Challenges Between Networking and IT Security Teams

Which of the following represents the biggest challenge associated with managing an assortment of security products from different vendors? (Percent of respondents, N=388)



Source: Enterprise Strategy Group

What's Needed for Threat Detection and Response

Addressing today's sophisticated cyber-adversaries requires integrated defenses driven by timely and accurate threat intelligence. This demands an architectural approach to security operations that ESG refers to as a security operations and analytics platform architecture (SOAPA). In the past, organizations had to cobble SOAPA together on their own, but security technology vendors now offer their own SOAPA called eXtended Detection and Response or XDR. ESG defines XDR as:

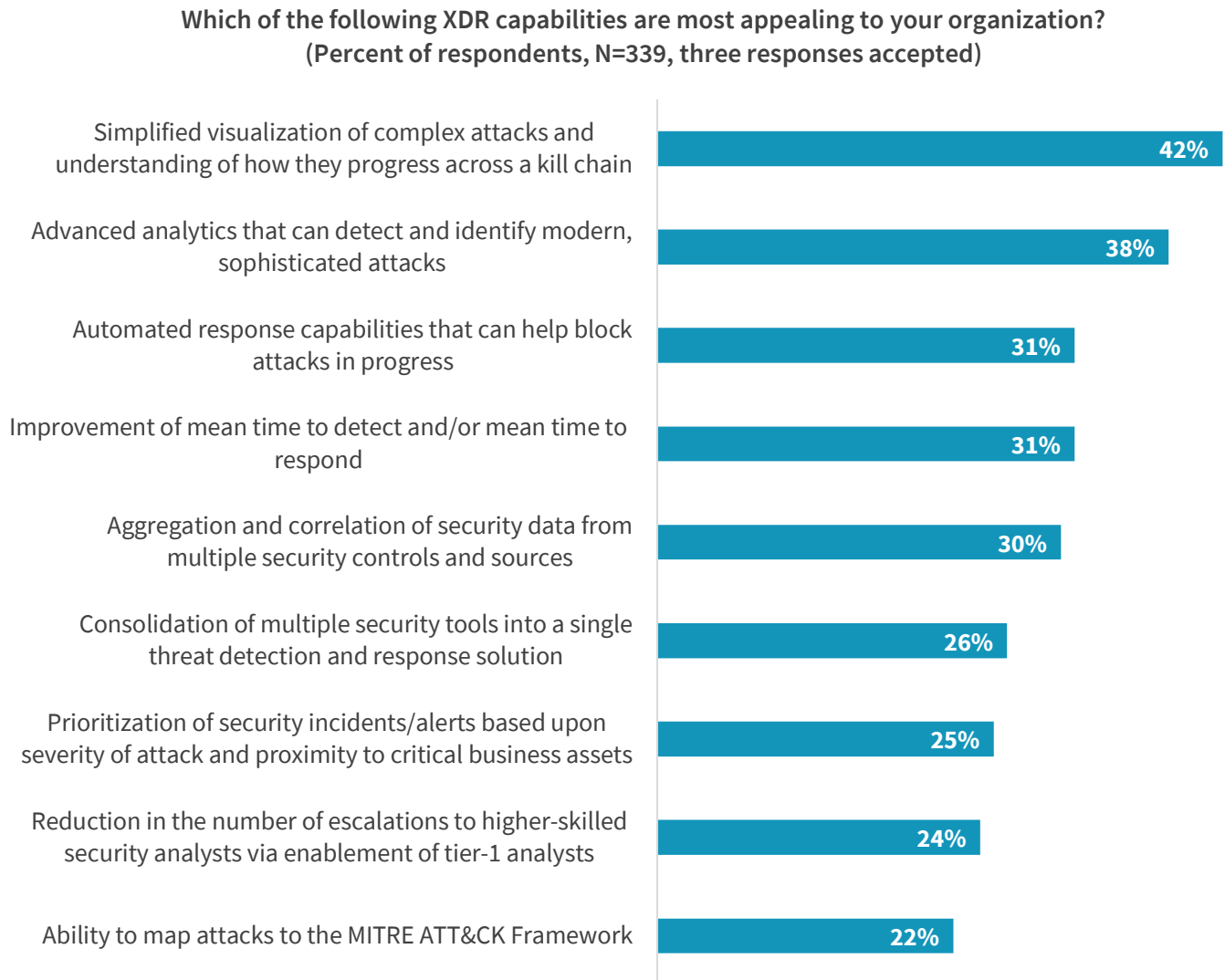
An integrated suite of security products spanning hybrid IT architectures, designed to interoperate and coordinate on threat prevention, detection, and response. XDR unifies control points, security telemetry, analytics, and operations into one enterprise system.

Like SOAPA, XDR integrates individual point tools into a common architecture. XDR uses each security control as a sensor and source of data; combines this data with threat intelligence; and then applies analytics algorithms to the data to detect anomalous, suspicious, or malicious incidents across an attack kill chain. Finally, XDR includes capabilities for process automation. In this way, XDR can address many of the challenges described above. Advanced analytics are especially beneficial, as they can help bolster the productivity of overworked SOC analysts by filtering noise and aggregating signals into high fidelity alerts. At the same time, process automation addresses the current dependence on manual processes.

As the research indicates, security professionals already recognize XDR’s potential for security operations improvement with (see Figure 3):

- **Strong prevention.** While few pundits include threat prevention as part of XDR, ESG believes leading XDR providers will offer strong threat prevention on endpoints, networks, email, web, and cloud-based workloads. Threat prevention in XDR is based on a combination of signatures, heuristics, threat intelligence integration, and advanced analytics algorithms. The goal here is to disrupt attacks early in the kill chain before they progress.

Figure 3. Most Appealing XDR Capabilities



Source: Enterprise Strategy Group

- **Simplified threat visualization.** Rather than view security status and alerts through multiple tools, SOC analysts want common visualization across multi-phased attacks, piecing together an end-to-end story. In this way, analysts can visualize the entire attack lifecycle, understand the breadth and depth of the attack, and then develop a comprehensive response plan. ESG data reinforces this desire, as 42% of respondents believe that XDR will be especially useful if it can simplify visualization of complex attacks across the attack surface. This visualization will

likely align with MITRE ATT&CK framework details about adversary tactics, techniques, and procedures (TTPs) as well as known campaigns by cyber-adversary groups.

- **Advanced analytics.** Today's threat detection and response is based on alert triage, prioritization, investigations, and remediation actions, but these are often manual processes based upon advanced skills. The ESG research indicates that security professionals want more help from their security technologies, as 38% of cybersecurity professionals want XDR solutions offering advanced analytics that use processing and analytics horsepower to detect and identify modern, sophisticated attacks. Ideally, XDR will replace today's domain-based analytics (i.e., endpoint security analytics, network security analytics, cloud security analytics, etc.) with cross-domain analytics that combine signals to produce higher-fidelity alerts supported by a detailed timeline of forensic evidence.
- **Automated response capabilities.** Once threats are detected, 31% of security teams want XDR to take automated responses to block attacks in progress—like quarantining a system, pushing new rules to security controls, or updating endpoint security signatures. Even experienced analysts want guided investigations or recommendations to help them with end-to-end remediation.

It is also worth noting that nearly one-third (31%) of respondents are looking for XDR to improve mean time to detect and mean time to respond to security incidents. This is especially important. On average, it takes an adversary days or weeks to gain a foothold on corporate networks, while it can take weeks to months for defenders to detect and respond to a system compromise. CISOs hope that XDR can help bridge this gap.

FireEye XDR

While many security vendors have adopted the XDR moniker for marketing purposes, FireEye is one of a few vendors offering a truly integrated XDR architecture capable of addressing enterprise threat detection and response requirements. FireEye XDR features:

- **A threat intelligence foundation.** Nearly one-third (31%) of organizations believe that integrating more external threat intelligence with internal security data collection and analysis would add significant value to their threat detection and response efforts. This aligns well with FireEye XDR, which is built on a foundation of threat intelligence data and a deep understanding of adversary behavior. FireEye uses its threat intelligence experience to include intelligence-led detections within its platform, using threat actor behavior triggers to take an “outside-in” approach to XDR.
- **Coverage across all major threat vectors.** Crafty cyber-adversaries typically penetrate corporate networks by spearphishing an employee or exploiting a software vulnerability. Once they establish a beachhead, they continue their attacks by moving laterally across networks, stealing credentials, exfiltrating data, or encrypting critical data sets. FireEye XDR can act as a countermeasure here with coverage across email, endpoints, network, and cloud workloads. Beyond its native capabilities, FireEye supplements its coverage by interoperating with third-party security technologies across identity and access management (IAM), messaging platforms, SOAR, etc.
- **An integrated and open architecture.** FireEye defines its XDR as a SaaS-based, security threat detection and incident response platform that natively integrates endpoint, network, email, cloud, and third-party security and cloud activity sources into a cohesive security operations system. FireEye provides this architecture by integrating its own products (i.e., email, endpoint, network, and cloud security) and enhancing its own products with more than 600 integrations across 70+ partners.

- **Analytics and knowledge for detection efficacy.** FireEye Endpoint Security was an early EDR offering built on advanced technology that detects known and unknown threats without using signatures and enables forensics and hunting for better response. Through its XDR offering, FireEye is extending these detection capabilities across domains for accurate threat detection spanning the entire kill chain.
- **A central management platform.** FireEye Helix has served as a central management hub for several years and now performs this same function for its XDR solution. SOC analysts can use Helix to anchor use cases like security investigations workflow, process automation/orchestration, event streaming/hunting, etc. Given these functions, it's likely that SOC analysts will eschew traditional "swivel chair" management across multiple security tools and use Helix instead to anchor most security operations management tasks.
- **Analyst experience.** FireEye put a lot of thought and development into the Helix UI/UX to provide SOC analysts, threat researchers, and incident responders with access to the data they need for timely and accurate analysis and decision making.

In aggregate, FireEye XDR checks off all the right requirements—threat intelligence integration, wide coverage, built-in analytics, an open architecture (with partner support), and a mature management platform. FireEye's deep security experience and pedigree also stand out from the crowded field. With all these attributes, CISOs looking for an enterprise-class XDR solution should assess how FireEye can help them address their needs.

The Bigger Truth

For most organizations, threat detection and response strategies based on point tools and manual processes are no longer adequate. XDR has the potential to address these weaknesses, but many infosec workers remain confused by industry hyperbole in this area. ESG research indicates that only 24% of cybersecurity professionals say they are very familiar with XDR.

ESG believes that successful XDR solutions will separate from the pack based on five attributes:

1. **Coverage.** Leading XDR solutions will span across endpoints, networks, cloud-based workloads, and critical applications (SaaS applications, email, etc.) and offer an open architecture for easy third-party technology integration.
2. **Threat intelligence affinity.** XDR solutions must provide timely and detailed threat intelligence and do so in the context of security alerts and an organization's infrastructure, industry, location, etc.
3. **Analytics.** XDR solutions must provide accurate cross-domain analytics to detect cyber-attacks across a kill chain.
4. **Automation.** XDR must help automate processes in areas like threat investigations, IR, and risk mitigation.
5. **Security operations utilization.** XDR must provide visibility and a common UI for different SOC analyst roles and use cases.

FireEye is one of few vendors that can meet all five requirements today, and the company has an aggressive roadmap for future XDR enhancements. As such, FireEye deserves a spot on a CISO's XDR short list.


All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188