Enterprise Strategy Group™
by TechTarget

WHITE PAPER

Why XDR Matters

(The Real Reasons) Why Security Leaders Care

By Dave Gruber, Principal Analyst
Enterprise Strategy Group

October 2023

This Enterprise Strategy Group White Paper was commissioned by Cisco Systems and is distributed under license from TechTarget, Inc.

Contents

Introduction

Modern cybersecurity programs require a combination of proactive and reactive security strategies that are capable of protecting operating infrastructure within the realm of agreed-upon risk tolerance levels. In support of key business objectives, the rapid adoption of cloud and SaaS-based applications, together with a more diverse and distributed device environment and the rise of remote and hybrid work, has expanded the attack surface, all of which challenge even the most mature security programs to keep up. Research from TechTarget's Enterprise Strategy Group shows that monitoring security across a growing and changing attack surface and spending too much time on high priority and emergency issues and not enough time on strategy and process improvement were the two most common security operations challenges.[1]

Further exacerbating this situation is the growing number of fragmented and often isolated security tools in use, together with the ongoing cybersecurity skills shortage, resulting in visibility challenges and an increase in the number of reactive and firefighting activities.

As threats have become more sophisticated and have involved multiple attack vectors, the industry has seen massive interest, investment, and adoption of solutions that can detect and facilitate rapid response to these more-sophisticated attacks. The extended detection and response (XDR) movement was born from this need, aggregating, correlating, and analyzing signals from all aspects of infrastructure to detect and stop attacks earlier.

Mega-trends and XDR

The XDR megatrend has influenced virtually every security solution provider to participate in some way in the XDR movement, as security strategies require more comprehensive visibility and speed to shut down threats before they cause damage.

The XDR megatrend has influenced virtually every security solution provider to participate in some way in the XDR movement, as security strategies require more comprehensive visibility and speed to shut down threats before they cause damage. AI and machine learning are deeply imbedded in most XDR solutions, with new levels of generative AI capabilities being added to further accelerate investigations and remediation. Beyond the hype, is XDR really helping security teams improve security outcomes?

Still rapidly evolving, XDR is contributing to security outcomes that may be surprising. This paper will provide an outcome-based perspective on what organizations should know about how XDR is contributing to broader security program objectives and where XDR has the potential to accelerate key strategies that can increase the security posture of the organization.

The Lifecycle of Security Megatrends and Why They Matter

Over the lifetime of the cybersecurity industry, we've seen plenty of big ideas emerge that have had a profound impact on modern security strategies. Some are born from advancements outside of the security industry and are then reapplied to security use cases. Frequently, many of these big ideas converge with other innovations, resulting in more comprehensive, scalable approaches supporting a broad set of environments and use cases.

Most megatrends evolve and mature rapidly as people experiment and investigate to understand their potential. Hype quickly turns to reality as experimentation uncovers gaps and opportunities to grow, expand, and mature concepts. As megatrends gain further adoption, they also gain momentum, which results in a further acceleration of capabilities, application, and use cases. Technology partnerships and alliances help providers close gaps and

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022. All Enterprise Strategy Group research references and charts in this white paper are from this research report.

assemble more comprehensive offerings that can accelerate additional positive outcomes. Zero trust, SASE, XDR, and generative AI all follow this pattern, each currently at a different point in its lifecycle.

The XDR Movement

The XDR movement is one such megatrend that has evolved substantially since its inception. XDR was born from the recognition that prior approaches to detection and response automation were unable to provide security analysts the ability to keep up with the rapidly expanding and changing attack surface, together with an increasingly more complex threat landscape. More than half of respondents to an Enterprise Strategy Group research report that their current tools struggling to detect and investigate advance threats is a challenge driving their organization's interest and investment in XDR solutions. This has resulted in frustrated security team members, extended attack dwell times, missed attacks, and, for many, cyber attacks that succeeded and damaged operating infrastructure.

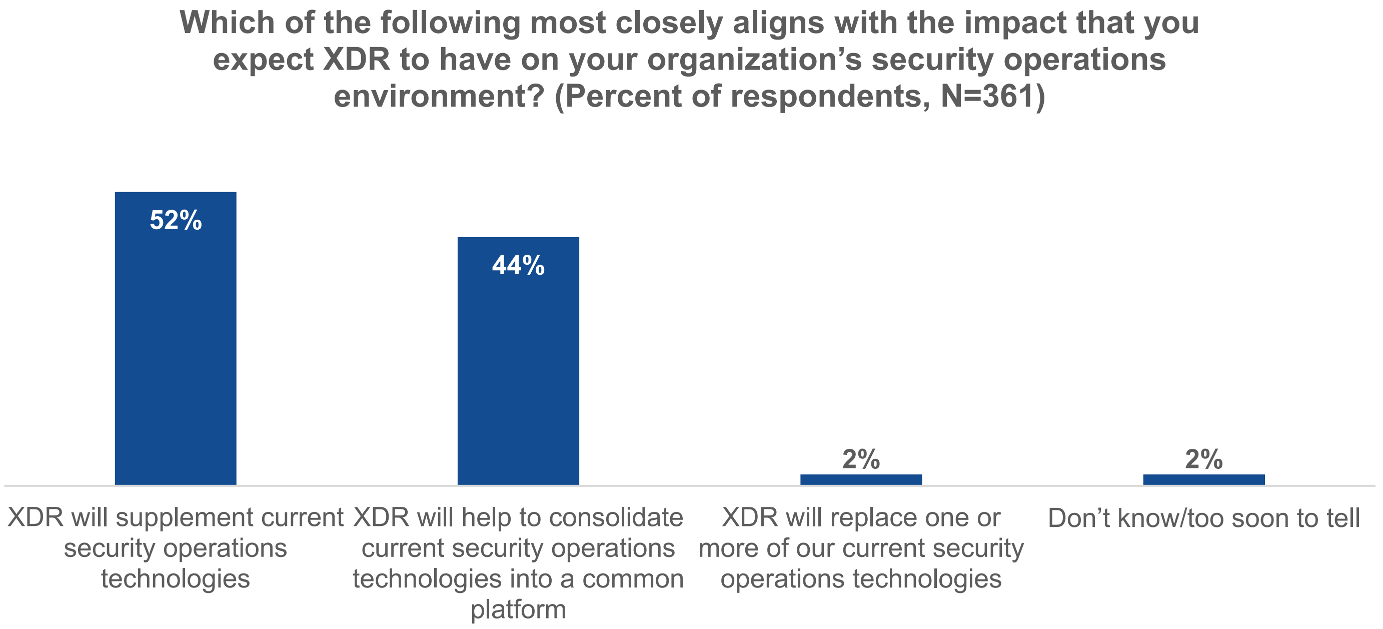
The XDR Movement

XDR set out to modernize detection and response automation, re-energizing SecOps teams to detect and mitigate complex threats more efficiently and effectively.

XDR set out to modernize detection and response automation, re-energizing SecOps teams to detect and mitigate advance threats more efficiently and effectively. The research also reports that nearly two-thirds of organizations have already deployed an XDR solution.

Profoundly influencing the rapid evolution of XDR were prior innovations, including endpoint detection and response (EDR), network detection and response (NDR), security information and event management (SIEM), and security orchestration, automation, and response (SOAR) solutions. These earlier, more siloed approaches laid the groundwork for what we see today as XDR. And while many organizations are leveraging XDR solutions to consolidate two or more of these earlier solutions, for many, XDR will supplement current security operations tools.

Figure 1. XDR Will Consolidate Tech for Many and Supplement for Others



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Support for Key Security Program Strategies

Building and managing an effective security program requires developing strategies to protect the organization against cyber-risk while supporting key growth and regulatory compliance objectives. An effective security program supports many objectives, including:

1. **Exposure management**, which identifies vulnerabilities and areas of exposure that present risk to the operation. An effective security program should help organizations answer the following exposure management-related questions:
   - What is our organization's risk tolerance? Is it different in different areas of the operation?
   - What is the scope of our risk perspective? Where are we exposed? Internally? Externally? Are there areas of potential cyber-risk that we are not effectively managing (e.g., supply chain, partners, third-party SaaS applications, etc.)?
   - Are we capable of assessing, understanding, and prioritizing vulnerabilities and exposure in all aspects of our infrastructure?
   - Do we understand the types and specific threats that are most likely to impact our operation?
2. **Visibility** to monitor the security of the operation. An effective security program should help organizations answer the following visibility-related questions:
   - Do we have continuous visibility and controls across the entire estate that align with our risk profile and critical operational elements?
   - Can we see and understand when we are under attack, and can we recognize when an attack poses a significant risk to the operation?
   - Can we correlate threat activity across all vectors and tools deployed to understand the scope of an attack? Are we leveraging advancements on AI and machine learning to correlate signals and identify threats?
3. **Response** to contain the threats that matter most. An effective security program should help organizations answer the following response-related questions:
   - Can we readily determine which threats present the biggest risk to the overall operation? Are we prioritizing remediation to address these threats first?
   - How fast can we understand and contain the full scope of a threat?
   - Are we leveraging automation to respond to routine tasks?
   - Is the operation confidently prepared to respond to a significant cyber attack?
4. **Remediation** to close gaps and prevent future risk. An effective security program should help organizations answer the following remediation-related questions:
   - Are we capable of identifying root cause and entry vectors of attacks?
   - How long does it take to close identified gaps or exposure so we can prevent future attacks that attempt to leverage them?
5. **Compliance**, which ensures regulatory requirements are met. An effective security program should help organizations answer the following compliance-related questions:
   - Do we have the right security processes and controls in place to meet our regulatory requirements? Can we prove it?

Effective Security Programs

Building and managing an effect security program requires developing strategies to protect the operation against cyber-risk while supporting key growth and regulatory compliance objectives.

- Are we operating at levels that enable us to meet cyber insurance requirements?

6. **Operational excellence** for continuous program improvement. An effective security program should help organizations answer the following operational excellence questions:
   - Do we understand our current security posture? Can we quantifiably measure improvement?
   - How well are we supporting the growth and health of our team members? Does our team have the skills, tools, and support it needs to succeed? How do we know?
   - How well are our security architecture and solution investments supporting our need to keep our costs and complexity under control through continuous convergence and consolidation?

XDR Is Positively Impacting Security Outcomes

XDR is contributing in many ways to the improvement of security program objectives. According to Enterprise Strategy Group research, when asked what are or likely would be the highest priorities for organizations when considering use cases for XDR, respondents most commonly reported that their organizations were prioritizing an XDR solution that could help prioritize alerts based on risk, improve the detection of advance threats, offer more efficient threat or forensic investigations, act as a layered addition to existing threat detection tools in order to identify advance or more complex threats, reinforce security controls and prevent future similar attacks, and consolidate disparate tools into a common, simplified threat detection and response architecture.

More than just a detection and response operational tool, XDR solutions are helping organizations gain new levels of visibility into risk and threats, detect and mitigate advance threats, and improve operational efficiency and analyst retention, resulting in improved overall security posture and program scalability. XDR solution investments are contributing to multiple security program objectives, including:

More Than Detection and Response

More than just a detection and response operational tool, XDR solutions are helping organizations gain new levels of visibility into risk and threats, detect and mitigate advance threats, and improve operational efficiency and analyst retention, resulting in improved overall security posture and program scalability.

- Tools consolidation.
- Earlier detection, mitigation, and remediation of advance threats.
- Increased visibility into program gaps and areas of risk, aligned with the evolving threat landscape.
- Exposure and risk-based approach prioritization.
- Staffing efficiency, increased throughput, and employee retention enabled by automation, AI, and refined user experience.
- Improved data and tools integration and collaboration.
- Response readiness and effectiveness.

85% of respondents to Enterprise Strategy Group research reporting investments in XDR solutions or services, and 83% of these have reported making significant or good progress on the effectiveness of their security program over the prior 12 months. Reported improvements include better efficiency, fewer breaches or compromises, better attack surface coverage, and improved MTTD/MTTR.

Introducing Cisco XDR

Cisco Systems has massively invested in building a broad cybersecurity product and services portfolio over the past several years, making it one of only a small number of security platform providers. Anchored in a deep history of delivering market-leading network solutions, Cisco security offerings now cover cloud, network, endpoint, email, identity, data, and security operations solutions. Underlying this portfolio is Talos, an industry-leading threat intelligence service fueling the entire portfolio.

Cisco XDR, built on top of the Cisco Security Cloud platform, is a relatively late entrant to the XDR movement. One of the advantages to late entrants is their ability to learn from the growth of the rest of the industry, enabling late entrants to emerge with strong, scalable architecture and capabilities that meet or exceed the industry leaders. Cisco is well positioned to accomplish this and has launched a strong initial XDR offering, together with deep data and platform integrations across the broad Cisco security portfolio, ecosystem, and select third-party solutions.

Cisco XDR is available as part of the Cisco Breach Protection Suite, protecting endpoint, network, email, and cloud within a single offering. Cisco XDR is also available separately and as a managed service.

Conclusion

The rapidly changing threat landscape, together with an increasingly diverse and distributed attack surface, is challenging even the most mature security teams to keep up. Incident response programs need help across all five phases: preparation, investigation, containment, eradication, and post incident analysis. More integrated, automated security solutions that can provide security teams with enough leverage to defend existing infrastructure while supporting new business initiatives are needed.

Megatrends including XDR are critical innovations that are helping security leaders strengthen and grow their programs. More than just another tool, XDR investments are contributing to many program objectives, underlined by their ability to strengthen overall security posture while increasing team throughput.

Enterprise Strategy Group recommends that security leaders take the time to explore how and why XDR solutions from security platform providers such as Cisco Systems can strengthen security outcomes, improve the overall scalability of security programs, and help consolidate security tools to reduce cost and complexity.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com

www.esg-global.com