Kaspersky Next XDR Expert

Whitepaper

kaspersky

Game-changer, or an itch looking for a scratch?

Who is XDR for?

XDR is for organizations with a mature security posture, needing a single platform to give them a complete and coherent picture of what's happening throughout their infrastructure.

XDR: Extended Detection and Response

It's the acronym on many peoples' lips, but like all relatively young technologies, not everybody knows exactly what it is or what it can do for their business. One thing's for sure — XDR involves a strategic shift from reactivity to proactivity, because 'wait and see' doesn't wash in cybersecurity. The smart money is on viewing XDR as a strategy rather than just a product.

So is XDR just the latest tech-itch looking for a scratch, or a potential game-changer? The itches are certainly there, from the global skills shortage, overworked IT security staff, and a threat landscape that never stands still, to alert overload, disparate tools, weak threat intelligence and the expanding attack surface. IDC says XDR will be "a disruptive force, impacting sales of SIEM, EDR, SOAR, network intelligence and threat analytics platforms, as well as providers of external threat intelligence"[1], and Forrester believes that differentiated XDR technology "will supersede endpoint detection and response (EDR) in the short term and usurp SIEM in the long run"[2].

XDR will be a disruptive force — IDC

More devices, more applications, more network traffic, more data, more threats...

Who is XDR for — and what challenges can it resolve?

XDR is for organizations with a mature security posture, needing a single platform to give them a complete and coherent picture of what's happening throughout their infrastructure.

The cybersecurity challenges these organizations face are consistent and well-established. ESG Research surveyed IT and cybersecurity professionals[3] at organizations with 100 or more employees, over 80% in enterprises, across multiple verticals. Here are some of the key findings:

Difficulties keeping up with the operational requirements of SOC technologies

Managing security operations is more difficult now than at any time in the previous two years, due to difficulties keeping up with the operational needs of SOC technologies — scalability in the data pipeline, load balancing processing engines, adding storage capacity, etc.

[1] Source: IDC, Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now? 2022

[2] Source: Forrester, Extended Detection and Response (XDR) — A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

[3] Source: ESG Research Report, SOC Modernization and the Role of XDR, 2022

The growing and constantly changing attack surface and the threat landscape overall

More devices, more applications, more network traffic, more data, more threats. The threat landscape doesn't stand still, and cyberthreats evolve relentlessly in volume and complexity as new tools proliferate. At the same time, the barrier to entry for hackers is lower than ever, with low-skilled buyers of cheap packaged threats on the dark web on the one side of the spectrum, and highly skilled, patient hackers building complex attacks on the other. And don't forget insider threats and supply chain vulnerabilities.

The high number of manual processes required to manage security

There's more security data to be collected and processed, and processing it manually is inefficient and ineffective. This creates a perfect storm that impacts scalability, results on an over-reliance on direct human involvement, and degrades the efficacy of dealing with threats in general.

An inability to develop detection rules

An inability to develop detection rules, fine-tune security controls and identify and deal with threats quickly and efficiently, due to a lack of time, resources and skills. Organizations don't always have the right skills or staff to keep up with security analytics and operations. Which leads us straight to the next pain...

The very real global skills shortage

Despite the global cybersecurity workforce being at an all-time high of 4.7 million professionals, there's still a 3.4 million gap that needs to be filled — but isn't being filled. This gap is growing twice as fast as the workforce, with a 26.2% year-on-year surge.[4]

[4] Source: (ISC)², Cybersecurity Workforce Study, 2022

Existing tools often struggle

to detect and investigate advanced threats, yet specialized skills are needed to use and manage them.

Tools not fit for purpose

When the tools themselves become part of the problem, something has to give. Existing tools often struggle to detect and investigate advanced threats, yet specialized skills are still required to use and manage them. Research[5] shows that current tools are frequently ineffective at correlating alerts, and IT security staff struggle with multiple disconnected, disparate tools handling disparate data. This is inefficient, cumbersome, messy and expensive. Another challenge is that current tools don't scale to deal with the expanding attack surface, and there are big gaps in cloud detection and response capabilities.[6]

Is it any wonder your CISO looks stressed?

The good news is that improving SecOps is a priority, and is funded — 88% of organizations will spend more this year, 66% say that tools consolidation is a priority, and modern applications development and deployment has increased velocity, requiring new skills.[7]

88%

of organizations will spend more this year on improving SecOps

66%

say that tools consolidation is a priority

What XDR does

Here's how XDR can hit these challenges on the head.

XDR detects advanced threats better

XDR's threat detection capabilities span endpoints, networks, and cloud environments. It uses machine learning algorithms and behavioral analytics to identify sophisticated threats, including malware, ransomware, and advanced persistent threats (APTs).

Automated response and remediation actions

XDR automates response and remediation actions, enabling organizations to contain threats quickly and minimize any potential damage. It can automatically quarantine or isolate compromised endpoints, block malicious activities, and remediate vulnerabilities, reducing manual effort and response time.

Integrates with endpoint protection tools

Integration with EPP is a key issue, and XDR leverages rich endpoint telemetry and behavioral analytics to provide deep insights into endpoint activities. It employs advanced machine learning algorithms to identify suspicious behavior and indicators of attacks (IOAs), facilitating early detection of sophisticated threats.

[5] Source: ESG Research Report, SOC Modernization and the Role of XDR, May 2022

[6] Source: ESG Research Report, SOC Modernization and the Role of XDR, 2022

[7] Source: ESG Research Report, SOC Modernization and the Role of XDR, May 2022

Where XDR fits into the EDR, MDR, SOAR and SIEM ecosystem

The clue is in the X — extended. XDR extends the capabilities offered by EDR to proactively detect complex threats across multiple infrastructure levels, and automatically respond to and counter these threats.

An integrated approach is key

By integrating multiple tools and security applications, and monitoring data on endpoints, networks, clouds, web servers, mail servers and more, XDR does more to detect and eliminate threats while at the same time simplifying information security management by automating cross-product interaction.

Forrester believes that in most cases, XDR won't outright replace security analytics platforms, noting that "XDR is on a journey, and [we] expect that over the next five years, security analytics platforms and XDR will collide".

SIEM has use cases beyond threat detection, and SOAR's customizability is useful, but when it comes to detecting and responding to threats, the advanced analytics of XDR's enhanced protection are second to none.

Delivers real-time visibility

XDR provides real-time visibility into your organization's security posture. It collects and analyzes data from various sources, such as endpoints, servers, firewalls, and cloud platforms, to deliver comprehensive insights into ongoing threats and suspicious activities into single console. This makes it truly proactive — proactive threat hunting and faster incident response. An holistic view helps security teams identify suspicious activities and potential security incidents more efficiently.

Contextualizes data and threat intelligence

When it leverages high quality threat intelligence and a comprehensive threat intelligence database, XDR provides highly useful contextual information about threats and attackers. This enriched threat intelligence simplifies investigation alerts and incident handling, and helps security teams understand the tactics, techniques, and motivations of threat actors, facilitating more effective incident response and proactive defense measures.

Enables streamlined security ops

Properly integrated, the best solutions will slot into your current infrastructure effortlessly to deliver the best results from automation, and give full visibility and awareness without having to replace third-party security solutions already in use. And don't forget that by providing a comprehensive view of security incidents and user behavior, integration supports compliance.

Clearly, XDR can deliver what it says on the tin: control, stability and that all-important edge. But not all XDR offerings are created equal... How do you choose the one that's right for you?

5 key things to consider when comparing XDR vendors and solutions

Here's how XDR can hit these challenges on the head.

1

There is a direct link between the quality of an XDR solution and the synergy between the vendor's EPP and EDR

An EDR solution for advanced detection and response to sophisticated cyberthreats at endpoint level is a key element of XDR. At the same time, EDR needs a robust Endpoint Protection Platform (EPP) to automatically sift out huge numbers of mass threats. It's important to look carefully at the endpoint protection features, and check that there is support for all kinds of endpoints — PCs, laptops, virtual machines, mobile devices, and various operating systems.

2

Up-to-date threat intelligence and a complete view of cybercriminals' tactics and techniques are essential to counter cyberthreats

It's not rocket science — any XDR solution worth its salt will offer both of these capabilities, together with additional context to improve and speed-up incident investigation and response.

3

Integration with third-party solutions is more sustainable and cost-effective

How well an XDR solution integrates with third-parties is another absolutely critical issue, because interoperability makes the purchase a more sustainable investment from the start. An XDR solution that offers numerous and genuine integration options will collect more data sources and deliver a more complete picture of what's happening in your infrastructure.

4

Independent reviews, global recognition and independent test results matter

When you're investing in something as important to your business as cybersecurity, don't overlook independent assessments. Ask for the results of independent tests. Check about international recognition from the likes of Forrester, IDC and others. Are the solutions implemented globally? Ask for case studies.

5

Is your investment futureproofed?

Technology doesn't stand still, and especially for something like XDR, which is still a relatively young technology, you should find out what a vendor's roadmap looks like for ongoing development.

Why Kaspersky

Most tested. Most awarded. Kaspersky protection.

Kaspersky is an established global cybersecurity company with a strong track record of security expertise. We've been protecting organizations around the world for over 25 years and have received countless awards and accolades for our products and services. Between 2013 and 2022, Kaspersky products:

587

achieved 587 first places

685

achieved top-three finishes

827

participated in 827 independent tests and reviews

In 2023, Kaspersky was named the Leader in the XDR solutions market by leading global technology research and advisory firm ISG. ISG defines 'leaders' as having a comprehensive product and service offering and represent innovative strength and competitive stability.

Learn more

Kaspersky Extended Detection and Response

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture