SWIMLANE TURBINE

White Paper

The Force Multiplier for XDR

Unlock the promise of XDR with low-code automation that unifies visibility and actionability at the point of inception

The security industry has developed an exhausting habit of trying to solve all problems with a new acronym, and extended detection and response (XDR) is the latest hype. At the end of the day, it does not matter if the solution is named XDR; security information and event management (SIEM); security orchestration, automation and response (SOAR); endpoint detection and response (EDR); or whatever other alphabet soup name is given to a category. What matters most is that technology can solve the organization's most urgent and pervasive problems.

Based on responses from a recent Forrester survey[1], the top problems that enterprises are allocating resources to solve fall into four areas:

1. **Global security talent shortage:** XDR promises to detect and respond to alerts across the SOC, which minimizes alert fatigue and staff burnout.
2. **Reducing complexity across the security environment:** By extending detection across disjointed tech stacks, XDR aggregates data for more detection and easier monitoring
3. **Keeping pace with the changing nature of threats:** Security leaders know that threats continue to grow more frequent and more severe, so XDR responds to more threats faster by extending detection across more than just endpoints.
4. **Quantifying business value:** Speeding up detection and response improves performance and security metrics, something XDR helps to accomplish.

This paper shares perspective on several legacy and emerging technology categories that aim to solve some or all of these problems. The goal of this analysis is to help cut through the marketing buzz so that security leaders can find the solution that is best suited for solving their top challenges. After all, instead focus on the capabilities needed to deliver the desired outcomes:

- **Action at the point of inception**
- **Integrate with any API in your environment**
- **Automation that is based on human logic and user-experience**

The Promise & Pitfalls of XDR

XDR was born out of the hope for a better way to deliver the outcomes that security leaders have traditionally looked to solve with their EDR platform or through their security operations center (SOC). The problem with EDR tools is the amount of expertise and monitoring resources required to adopt them. The pitfall of legacy SOC tools like SIEM and SOAR have historically been more costly and complicated than many organizations can manage. XDR vendors have perpetuated the hype by positioning their offering as a way to get higher alert efficacy with fewer false positives.

[1] Forrester Infographic: Global Security Budgets in 2022, December 10th 2021

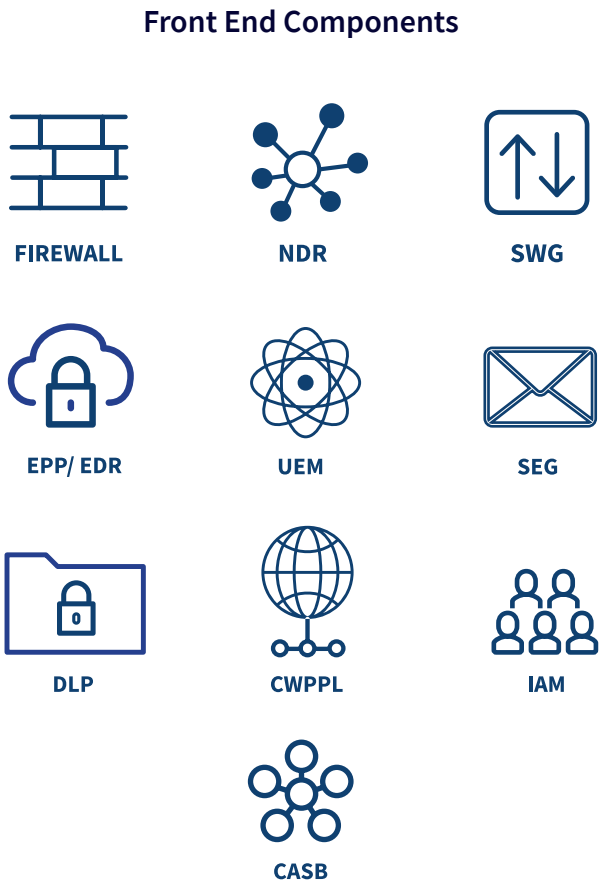
These sets of products claim to be less dependent on resources, like hiring more analysts, while also claiming to save on costs traditionally associated with SIEM tools and the required data retention that accompanies those tools. Simply put, security leaders strive for a solution that will enable their teams to effectively stop breaches, without the dependency on hiring more people, and they need the ability to quantify the outcomes the security program accomplishes. XDR promises to deliver a centralized management hub and simplified visualizations for complex attacks, and while this concept is undoubtedly intriguing, the solution has pitfalls.

XDR Turned Up The Noise

As their name implies, EDR solutions are exceptional at detecting activity on the endpoint, but they are notorious for having a poor signal-to-noise ratio. For EDR customers, this means that finding the relevant alert and actioning on it in near-real-time is a challenging task. As a result, "The biggest barrier to adoption of EDR tools remains the skills requirement to operate them and the increased total costs, particularly as later adopters deploy EDR. On average, EDR capabilities will add an extra 37% to initial costs, and adoption of EDR must be accompanied by investment in training to be effective."[2] A desire for "next-gen EDR" – a solution that promises higher fidelity – contributes to the allure of XDR.

In the current reality, XDR only perpetuates the problem because it combines detection from multiple sources, like a subset of firewalls, EDR, data loss prevention (DLP), network detection and response (NDR), unified endpoint management (UEM), cloud workload protection platforms (CWPP), cloud access security brokers (CASB), secure web gateways (SWG), secure email gateways (SEG), or identity access management (IAM) into a single platform without ever actually improving the signal-to-noise ratio from each detection tool.

While this telemetry consolidation sounds like nirvana, the reality is that XDR providers today only offer a limited sub-set of these detection sources today. This forces customers to sacrifice visibility due to vendor limitations like their endpoint agents or integrated systems. In contrast, next-generation low-code security automation fully delivers on the promise of XDR by integrating with all of these sources, effectively extending visibility and response to all corners of a customer environment in a fully environment-agnostic way.



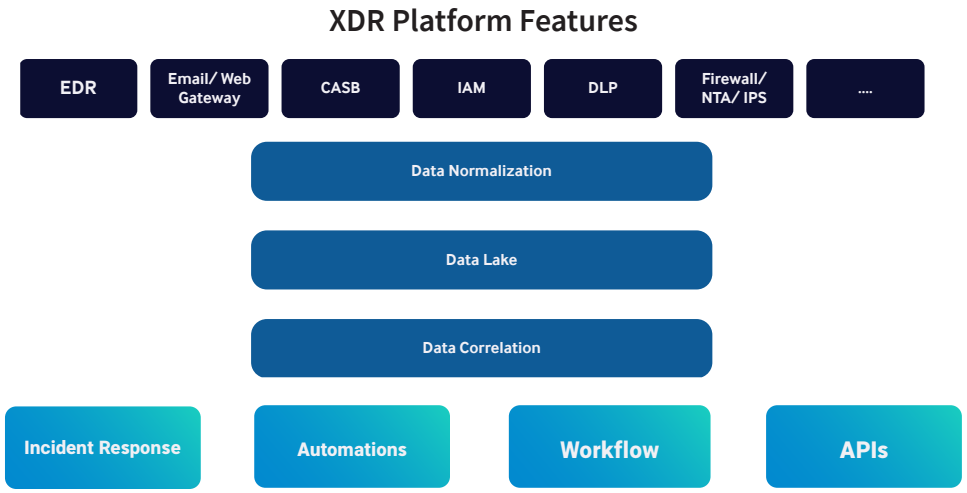
XDR platforms offer a handful of front-end telemetry sources, but most who claim to be XDR only offer a limited sub-set of these sources. In contrast, low-code security automation integrates with all hard-to-reach telemetry sources and expands actionability beyond the closed XDR ecosystem.

[2] *Gartner®, Magic Quadrant™ for Endpoint Protection Platforms, Paul Webber, Peter Firstbrook, Rob Smith, Mark Harris, Prateek Bhajanka (March 15, 2022). GARTNER and MAGIC QUADRANT are a registered trademark and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission.*

Extended Detection = Extended Human Monitoring

This integrated platform approach is XDR's way of breaking down technology silos for a wider view of data aggregation and response. The pitfall is that without first solving the signal-to-noise ratio problem, extended detection only extends the dependency on human monitoring, contributing to the already prevalent problem of alert fatigue. If the goal is to increase the security team's productivity and decrease false positive alerts, then the XDR solutions available today are not delivering on this promise.

To overcome this pitfall, nearly all XDR implementations today are accompanied by a managed services offering. While managed services can be useful for some organizations, the need for XDR vendors to supplement their technology with a service offering highlights the technology's immaturity when it comes to incident response, automation, workflows, and APIs. This is where Swimlane excels.



While XDR vendors have been racing to differentiate front-end features, many have simply checked the box when it comes to delivering backend XDR features like APIs, incident response, automation and workflows. This approach is not good enough. To unlock the promise of XDR, security teams really need low-code security automation.

XDR Underdelivers on the Promise of Extended Response

While XDR tools claim to expand the detection of events across the SOC, this is not what modern SOCs are missing. ***What's actually missing is a tool that helps security leaders respond to threats the instant they occur – not after detection, data aggregation, and manual response.***

Without case management extended response is impossible. Most XDR providers today lack robust case management capabilities to support incident response. In order to enable extended response, customers need flexible APIs and automation that can go beyond limited data and ingestion sources. Workflows must be defined and automated based on their business needs not by technology constraints. When it comes to these back-end capabilities of XDR, current vendors are merely scratching the surface of what's needed in order to deliver business outcomes.

In order to speed time to value, reduce mean-time-to-resolution (MTTR) and mean-time-to-detect (MTTD), overcome the skills shortage, and make security professionals more efficient, what organizations really need is next-generation low-code security automation. Swimlane's approach to automation is the force multiplier needed to make these outcomes a reality and deliver on the promise of XDR.

THE PITFALLS OF XDR

- It has a poor signal-to-noise ratio
- It requires even more monitoring than EDR
- It does not extend response

Event Management of Shelfware?

As the name implies, SIEM was created to help security professionals manage security events. At its core, it should make incident response faster and easier. The truth is, SIEM vendors never truly got around to the "EM" part of their namesake. That's why many have acquired SOAR companies to supplement this feature set.

Unfortunately, early adopters have found that this bundled SIEM and SOAR platform approach is not working. That's why many customers, like the world's largest organizations in finance, technology, government, and consulting are making the switch to purpose-built low-code security automation. And all it takes is a quick Reddit binge to see that other security professionals are wondering if XDR can be a replacement for their SIEM.

The truth is, it can't be. Like it or not, SIEM is still a very necessary part of a security tech stack for the benefits it provides for big data analytics, compliance and audit requirements. Instead of throwing the baby out with the bathwater, it's time to rethink the relationship between your SIEM and SOAR, so that you increase response speed, simplify processes, improve analyst experience, and ultimately gain a more holistic view of the value derived from security operations.

Consider the Impact of the Data Aggregation Lifecycle

SOAR first hit the market as an attempt to save security teams time by automating and orchestrating the alert response process. However, most SOAR technologies today are built in a way that is dependent on underlying infrastructure, like a SIEM platform, to get an alert. This lengthy alert process often looks like this:

1. an endpoint agent on a workstation must generate an alert
2. send it to the centralized manager for the EDR product
3. then log data is sent to and processed by the SIEM
4. which then runs analytics, creates an event, and finally then sends that alert to the SOAR for response.

In examples like this, where the alert has high-fidelity, the SIEM does not add the enrichment necessary for enabling action. As a result, the SIEM data aggregation lifecycle slows mean-time-to-respond (MTTR) and increases dwell time. Unlike traditional SOAR platforms, next-generation low-code security automation solutions are not dependent on SIEM. This architecture enables security leaders to rethink their data analytics strategy, and shift the response action earlier in the attack lifecycle.

A Cybersecurity System of Record

Most, if not all, security professionals agree that the notion of a "single pane of glass" is marketing fluff at best, but many may think of their SIEM as a system of record. SIEM is a great system for logging and preserving machine data needed for analytics, compliance and audit purposes, but it does not factor in the human element of security. XDR claims it will deliver a centralized management hub and simplified visualizations for complex attacks, but major security-forward organizations like Sony, Lumen, Sagicor and Toshiba already know that a solution exists.

Swimlane's low-code security automation platform combines human and machine data to deliver a system of record for not only the SOC, but all of security. While an XDR platform offers a selection of front-end detection capabilities like firewall, EDR, DLP, NDR, CASB and more, Swimlane's ability to integrate with any data source enables it to respond to any detected threat - regardless of the source. This means that customers gain actionable visibility into their entire security environment, without having to make compromises by deploying the detection tools that are only supported by the XDR vendor.

With Swimlane, all extended detection and response actions are captured through case management, reporting and dashboard features. The platform's low-code approach makes it easy for security teams to create custom visuals to highlight their KPIs, ROI and risk posture maturity.

Low-Code Security Automation: The Force Multiplier for Detection and Response

Swimlane Turbine provides security teams with a force multiplier that delivers on the promise of XDR, without time-consuming and burdensome pitfalls. This next-generation security automation technology accomplishes this by enabling security teams to re-focus their SIEM strategy on incident response and finding attacks that require analytics or correlation across big data sets. Security teams who make this shift from a detection-centric strategy to action-centric strategy will be more successful at identifying sophisticated attackers in near-real-time.

Benefits of Low-Code Automation

Stop threats at the point of inception

With Swimlane customers dramatically reduce their response times. One customer reported cutting their MTTR by 50%.

Overcome the security talent gap shortage

Increase staff capacity by 50%. A fortune 100 Swimlane customer saves $160,000 every month in labor costs by eliminating 3700 hours of work with automation.

Unify complex environments, disconnected teams and processes

Global organizations, like Lumen, reach 70% automation levels shortly after integrating Siwmlane into their infrastructure.

Quantify the business value of security through a system of record

A fortune 100 Swimlane customer saves $900k a year with Swimlane. Their biggest savings come from outside the SOC use cases.

What our Customers Say

LUMEN®

"Swimlane has become an essential core component of our SOC. It's part and parcel of our SOC operations today, and I would say that it's almost impossible to do without Swimlane."

– Wai Kit Cheah, Director of Security Practice at Lumen Technologies

Softcat

"With Swimlane, we didn't have to try and fit our outcome into a preconceived box that had already been developed. Swimlane allowed us to build something that worked for us and how we operate"

– Matt Helling, Head of Cyber Security at Softcat

SWIMLANE

Corporate Headquarters
363 Centennial Pkwy Suite 210
Louisville, CO 80027
1-844-SWIMLANE
swimlane.com

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. For more information, visit swimlane.com or join the conversation on LinkedIn, Twitter and YouTube.