cynet

Why Autonomous XDR is going to Replace NGAV/EDR

A guide for small security teams that need an efficient and affordable breach protection solution

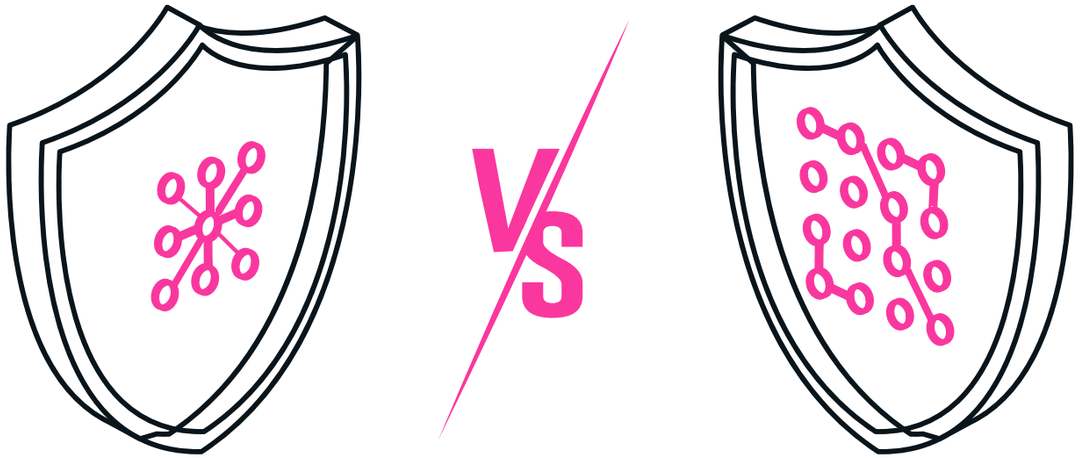
NGAV/EDR vs. Autonomous XDR

While the pairing of NGAV and Endpoint Detection and Response (EDR) has become a common endpoint security combination, it falls short on bringing full prevention and detection capabilities. It has become clear that to receive full visibility and response capabilities, more data and intelligence across the organizational environment is required.

Extended Detection and Response (XDR) technology efficiently solves this breach detection gap. The Autonomous XDR platform takes XDR a step further and provides the necessary automation to assess the scope of attack across the entire environment, fully contain the threat, and remediate all components of the attack.

Effectively detecting a threat in the organizational environment and then analyzing the attack to full remediation, a challenge that once took days to months, is reduced to mere minutes with Autonomous XDR.

There's more to the Autonomous XDR and small security teams are rapidly adopting this technology to replace their NGAV/EDR combo. Here's why.



cynet

The case for NGAV/EDR

The “assume breach” mentality is a mindset that has not only been adopted by security teams, but it is already well-understood by the organization’s executives, board members and other stakeholders. This mentality gave rise to the now-common combination of NGAV and EDR. The first is used to prevent the known ”bads” from entering and the latter to detect threats on the endpoint as quickly as possible in order to contain the threat before further damage is done.

The endpoint approach has its strengths:

Prevention – both file analysis and process monitoring make endpoint protection an efficient prevention tool against zero day malware, exploits, scripts and Macros.

Detection – commodity hacking tools such as Mimikatz, Powersploit and others generate memory patterns that are easily detectable.

Investigation – the endpoint agent continuously monitors and records logon activities, internal and external communications and process executions, providing rich investigation context.

Operation – NGAV/EDR can easily replace all traditional anti-virus as all anti-virus functionalities are a small subset of the NGAV/EDR offering.

Unfortunately, the NGAV/EDR combination suffers from the following weaknesses:

Limitations and Blindspots – NGAV/EDR cannot reliably distinguish between the legitimate use of admin tools, such as PSexec.exe, Powershell, WMI, etc. and their malicious abuse by attackers performing reconnaissance, credential theft and lateral movement, resulting in a high rate of false positives. NGAV/EDR are blind to any malicious activity that doesn’t entail a distinct process behavior change including a multitude of commonly used attack vectors (ARP Spoofing, DNS Responder, lateral movement, tunneling attacks, etc.)

Remediation - Cyber attacks have a cross environment impact on endpoints, user accounts and network traffic, and recovery processes must address all of them. While NGAV/EDR can isolate and join endpoints, they have zero capabilities across users and network traffic.

Operation - Efficient operation of NGAV/EDR alerts requires highly skilled security staff which is practically out of reach for most to all organizations.

Deployment - Many NGAV/EDR agents are hard to deploy and clash with existing software on the endpoint. Typically, NGAV/EDR projects result in at least 20% undeployed endpoints.

cynet

The irony of tacking on more security solutions to NGAV/EDR

To receive the necessary visibility across the environment and to properly analyze, prioritize and respond to the multiple alerts, security teams have found themselves complementing their NGAV/EDR combination with further technologies such as User Behavior Analytics Rules (UBA Ruls), Network Detection Rules, Deception and more.

Beyond the detection security stack, security teams have found themselves needing to manually consolidate, normalize, and correlate the threats simply to assess the attack and then to respond to the threat across the environment.

Building such a stack requires budget, time and skills, which is out of reach for most organizations.

Ironically, instead of gaining more security, security teams - especially small ones - are finding that building such a stack becomes nearly useless due to the complexity of operating, managing and maintaining it.

cynet

The case for Autonomous XDR

The advent of XDR brings a sigh of relief to security teams that need more visibility but not at the expense of more budget, headcount or complexity.

An XDR platform overcomes the NGAV/EDR shortcoming by providing more accurate, effective and automated prevention, detection and response The XDR platform natively integrates multiple security technologies - NGAV, EDR, UBA Rules, Network Detection Rules and deception - into a single wholesome solution.

The Autonomous XDR provides automated remediation – immediate scoping, full threat analysis and threat containment - without the need for human intervention.

Comprehensive attack prevention and detection

The various detection technologies - at a minimum NGAV, EDR, UBA Rules, Network Detection Rules and deception - are integrated within a single, unified environment.

Alerts are already consolidated within a single platform, normalized and correlated. This eliminates the need to build a security stack of various solutions to receive more accurate and efficient alerts and reduces the manual alert analysis price tag that comes with the NGAV/EDR combo.

Response at the highest levels of automation

An XDR platform further addresses the need for speed and elimination of manual activities and burdensome alert analysis by automating response activities.

XDR automation capabilities run the gamut - from basic automated remediation on a single endpoint to automated investigation with extended remediation across the environment.

It is true that basic automated remediation on a single endpoint is available in nearly all EDR solutions. In this case, automated remediation mainly includes activities such as quarantining a suspicious file before it executes, killing a malicious process, isolating an infected device, and other rudimentary endpoint-centric remediation actions.

Taking it a step further, XDR solutions provide additional automation such as basic automation remediation on multiple endpoints - something that not all EDR platforms offer. This includes the ability to search for a threat identified on one endpoint on other endpoints across the environment and take appropriate remediation actions.

As the levels of automation increase, they are unlikely to be found in EDR platforms and are offered only by XDR solutions. The highest level of automation, which is only offered by Autonomous XDR, takes automated threat investigation beyond
responding to a single threat at hand to helping determine if the detected threat is only one part of a larger attack, and if so, uncover and remediate related attack components. This allows security teams to achieve threat scoping and remediation in just minutes.

cynet

Affordable MDR services

Many of the EDR and XDR providers also offer Managed Detection and Response (MDR) services.

Those offered by the EDR providers typically use specialized and in-house tools to build and operate the security stack that the security teams would've liked, and do the required analysis on that security stack. This makes their offering costly, putting resource-constrained teams again in a dilemma as to security versus budget.

MDR services that extend to XDR actually use the very same XDR platform used by their clients as it provides them with the necessary visibility and automation they require, thus reducing the costs to their clients.

Operational simplicity

Naturally, the security stack that accompanies the NGAV/EDR is cumbersome to deploy due to clashing agents and integrations (even when all components come from the same vendor!).

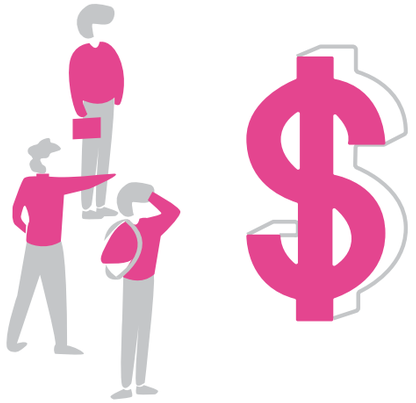
Since the XDR natively integrates all the solutions, it is easy and quick to deploy, providing immediate value.

Affordable for all security teams regardless of size

Building and operating the security stack needed to close the gap over NGAV/ EDR is costly. Direct costs sky rocket as each product is purchased separately and indirect costs, which involve operating and maintaining the stack, bill up quickly, as do the intangible costs such as team burnout.

The XDR platform makes the security stack an affordable alternative as the technologies are already within that single platform and threat analysis is done automatically - removing those indirect and intangible costs.

Some Autonomous XDR providers also offer their MDR services free of charge, further making their solution highly affordable to security teams of all sizes and skill sets.



cynet

The NGAV/EDR Stack or Autonomous XDR?

No business today expects that a single tool or technology will prevent all threats from penetrating the organization. However, businesses expect to keep operations going - regardless of security - and it's the security team's role today to minimize risk and contain damage as quickly as possible. These have become key parameters in measuring the success of the team.

Small security teams have recognized that the NGAV/EDR combination cannot reach the high levels of detection accuracy and response speed required to ensure that business operations run smoothly in case of an attack without investing in complementing technologies and headcount.

The alternative, Autonomous XDR, provides the necessary visibility and response capabilities security teams need. They receive this without overstretching budget, human resources or hard-to-find expertise. With NGAV/EDR integrated within the XDR, as a component of the platform together with more detection technologies, as well as fully automated threat response and MDR services - why would anyone want to go down the NGAV/EDR route again?

cynet

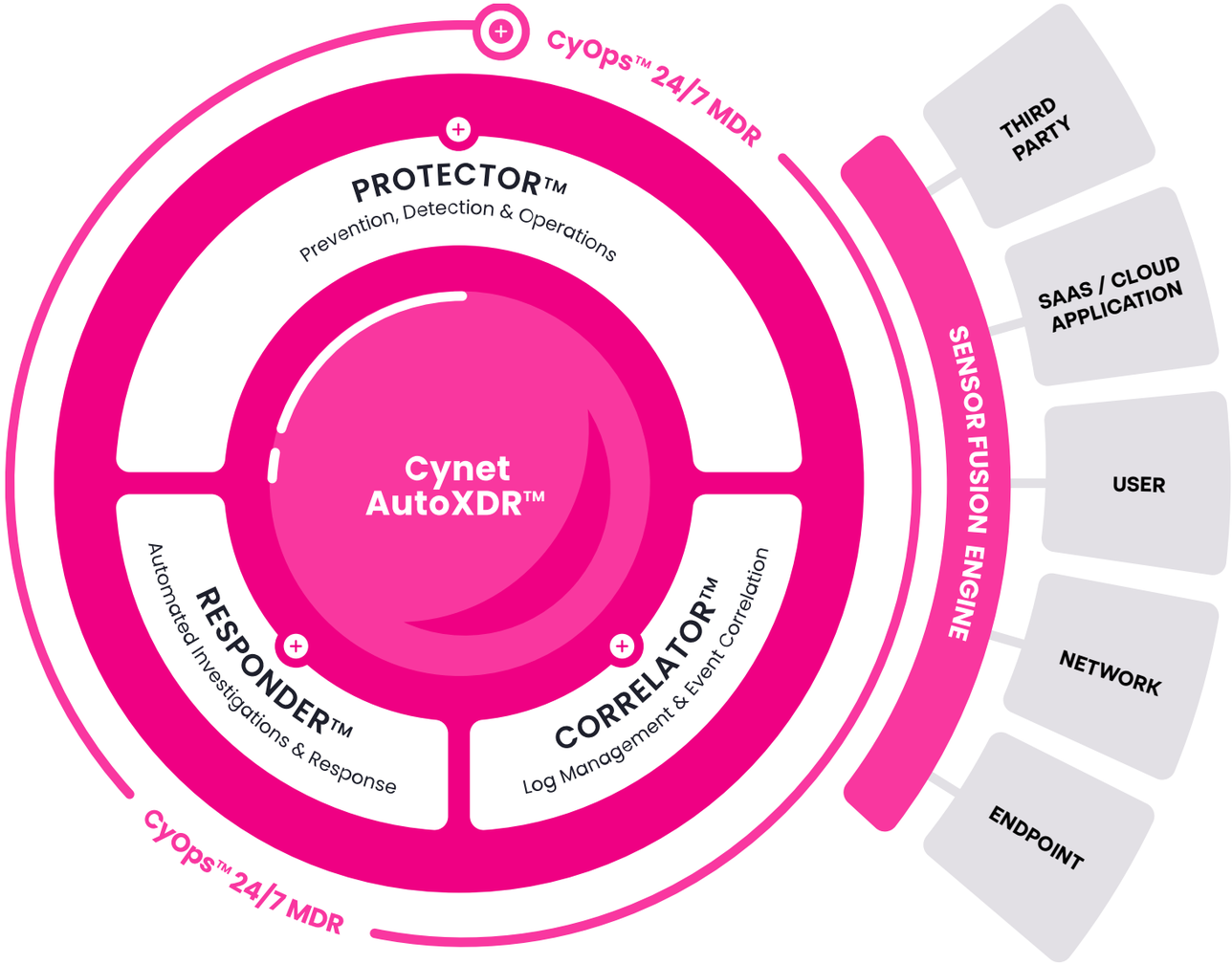
ABOUT US

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.



	NGAV/EDR	Autonomous XDR
Prevention and detection technologies	NGAV EDR	At a minimum: • NGAV • EDR • Network Detection Rules • UBA Rules • Deception
Alert accuracy and efficiency	Low Requires complementing technologies to reduce false positives, deduce the significance of the alert and eliminate alert fatigue due to multiple alerts for the same incident.	High Reduced number of false positives, incident view as opposed to list of alerts shows the full picture with its associated alerts, higher rate of validated alerts.
Response automation offerings	Remediation automation on the endpoint. Some also provide remediation automation on multiple endpoints.	All levels of response automation, already built-in: • Automated remediation on the endpoint • Automation remediation on multiple endpoints • Extended automated remediation across environment • Extended remediation playbooks across environment • Automated investigation with extended remediation across environment
MDR services pricing	High	Low **Cynet offers 24*7 MDR services included in their offering at no extra cost.**
Deployment complexity	High	Low **Cynet's 360 XDR deploys up to 5000 hosts per hour.**
Operational complexity	High	Low
Cost	High	Low