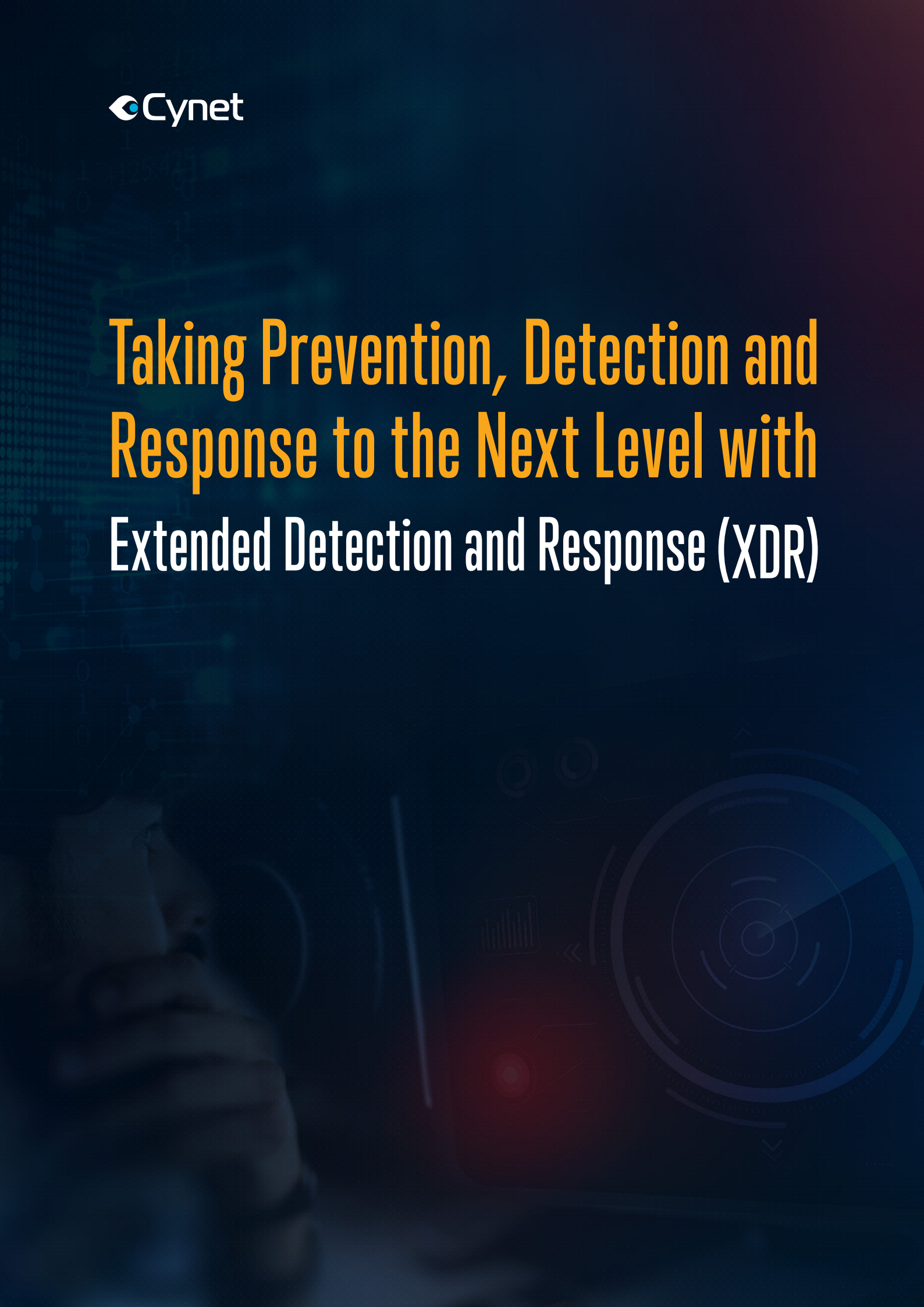
Cynet

Taking Prevention, Detection and Response to the Next Level with Extended Detection and Response (XDR)



Seeing the Forest Through the Trees: Reducing the Complexity of Cybersecurity

Increased Budgets ≠ Increased Performance

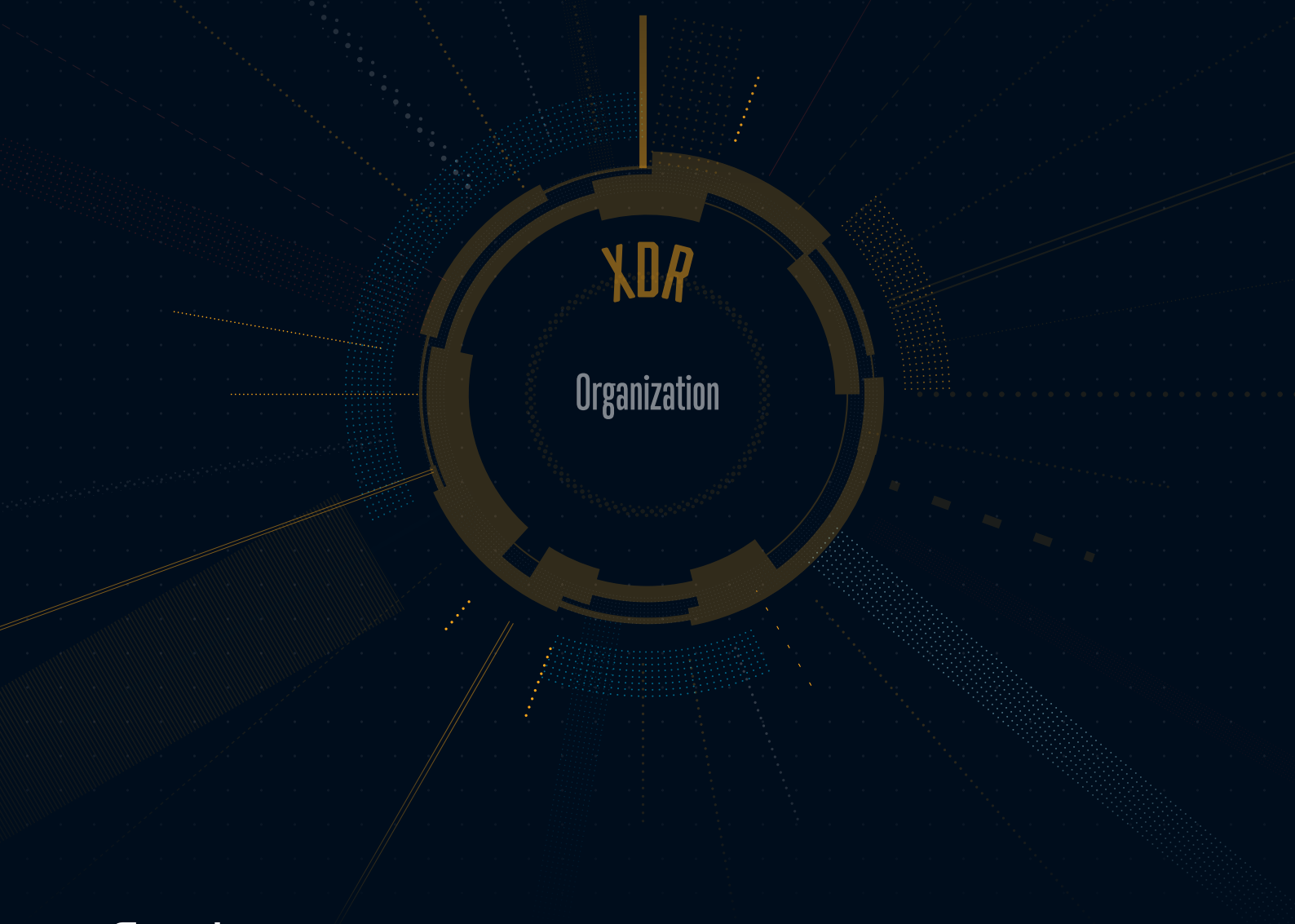
Security professionals are inundated with potentially thousands of alerts per day that are generated by the growing number of security solutions. Investigating and connecting individual alerts can take days. Seeing the proverbial forest through the trees is an ongoing struggle. And, once threats are discovered, the time required to understand the breadth of the attack and ultimately remediate the threat is now measured in months. IBM's Cost of a Data Breach Report 2019 found the mean time to identify a malicious attack is 230 days and then the mean time to contain the attack is 84 days. This is why cyber breach incidents continue to increase despite increased cybersecurity investments.

Smaller Organizations Suffer Most

Smaller organizations also suffer from runaway cybersecurity complexity, but many simply cannot afford the wide array of security solutions needed to provide visibility into impending threats across their environments. Moreover, the cybersecurity stack has become so complex and unwieldy that the skillset required to maintain and operate the solutions is beyond the grasp of all but the largest global organizations.

Seeing the Forest

A new class of security tools is emerging that promises to greatly improve the effectiveness and efficiency of threat detection and response. Gartner defined a new solution category that aggregates and correlates telemetry from multiple detection controls and then synthesizes and automates response actions - Extended Detection and Response (XDR).



The Challenge with Threat Protection: More Point Solutions Miss the Point

Businesses typically deploy multiple prevention and detection technologies to defend points of entry and movement, such as endpoints, networks, users and data. While these tools generally do a fine job preventing and detecting the vast majority of cyberattacks, they continue to miss the edge cases – the sneaky attacks that squeak through the cracks of point solutions. Visibility across the environment and understanding the context of security data and alerts is the first step to solving the complexity problem.

Endpoint Protection is Not Enough

Many organizations have turned to Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP) and Next Generation Anti-Virus (NGAV) solutions for enhanced protection beyond the commonly used Anti-Virus (AV) platforms. The EDR/EPP/NGAV solutions have proven highly valuable in preventing and detecting many forms of endpoint attacks. However, the cybercriminals are finding ways to bypass these endpoint-centric approaches with increasingly stealthy attacks. Confirmed breach levels have continued to rise despite massive investments in cybersecurity solutions and resources.

The Need for Unified Detection

Based on the "dwell time" cited in the above-mentioned IBM study, the real challenge in security today is finding the threats that bypassed first line defenses as quickly as possible. Something that may seem innocuous by one security solution suddenly becomes cause for concern when intelligently paired with information from other security solutions. Consolidating prevention and detection technologies into a single solution can coordinate threat signals to paint a more accurate picture of the attack landscape.

The Need for Automated Response

Another important step for simplifying security lies in automating response actions to address the real threats identified through better visibility and context. Security teams today spend significant time investigating false positive alerts. Confirmed threats then require access to multiple controls through multiple consoles and presentation schema for investigating the full breadth of the attack. Remediating threats also requires a far too much effort to plan and coordinate corrective actions across multiple security systems. Security teams are simply overwhelmed by operating and maintaining too many point solutions.

XDR: A New Approach to Threat Detection and Response

XDR helps security teams by consolidating and rationalizing alerts into actionable incidents and automating investigation and response actions. The primary requirements of an XDR platform are threat visibility, incident orientation, and response automation.

Broad Threat Visibility and Protection

Broad visibility across the primary prevention and detection components that provide the most pertinent threat telemetry forms the basis of XDR. Combining signals from these components provides the context required to detect stealthy (and otherwise undetectable) attacks while providing far greater detection accuracy (and thereby slashing false positives). Because the components included are part of a single platform, data and alert information can be easily normalized and combined; a feat that is highly difficult when trying to coordinate multiple vendor point solutions.

Deciding which prevention and detection components should be included in the XDR platform is critical. While some suggest including a very broad range of detection and security tools, focusing on tools that cover the primary attack vectors should be prioritized. At a minimum, XDR tools should include signals from the following key components:

NGAV

Next Generation AntiVirus for basic endpoint malware prevention and detection.

UEBA

User and Entity Behavioral Analytics (to detect anomalous user behaviors).

EPP/EDR

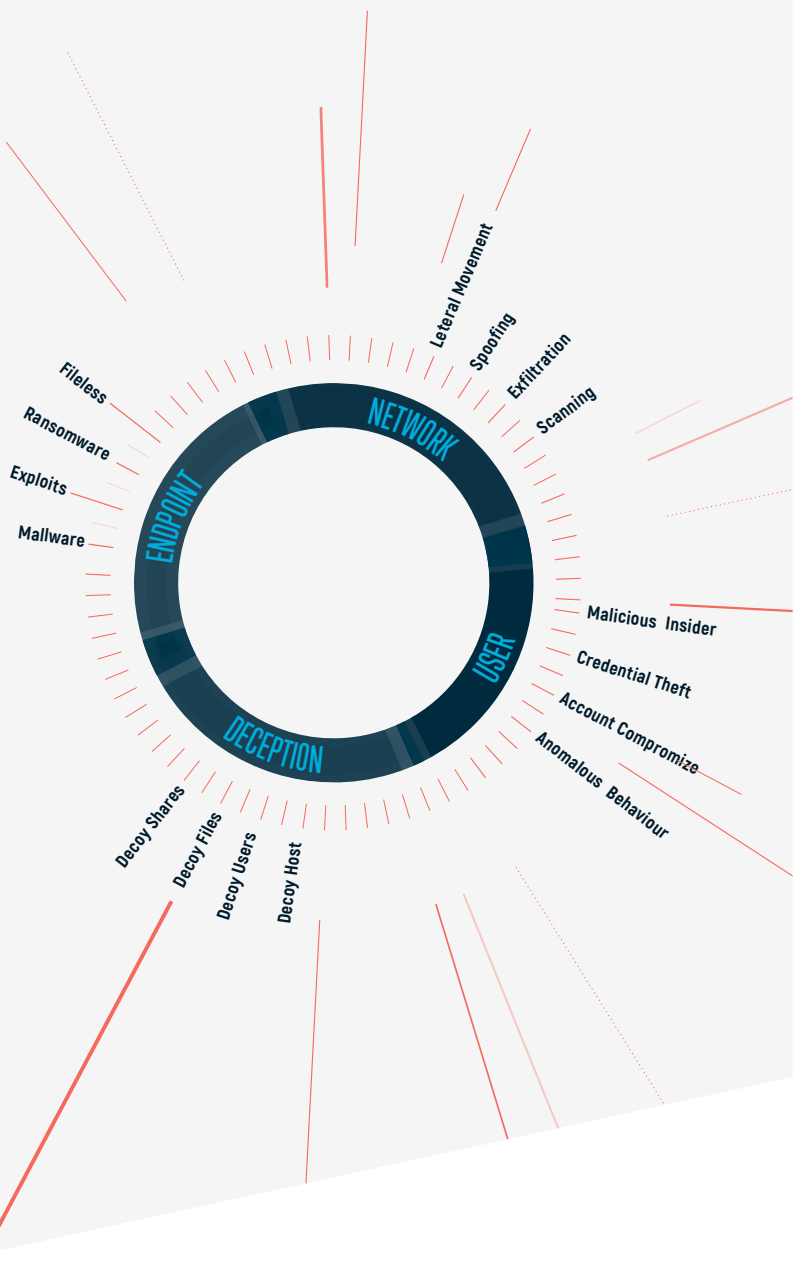
Endpoint Protection Platform/ Endpoint Detection and Response for more advanced endpoint protection, detection and response.

NTA

Network Traffic Analysis for malicious activity on your network.

Combined, the signals from these solution categories provide the broad visibility required to detect the vast majority of attacks across the cyber kill chain. Other data may supplement this core set, but these components have been shown to provide the best value. For example, signals from Deception technologies that trick successful intruders into exposing their presence before damage can be done can provide highly valuable signals to an XDR platform.

It's also recommended that as many components as possible are native to the platform. This ensures that all signals are properly normalized and weighted and that all features and policies can be managed from a single interface. It also eliminates the time and effort required to integrate and continuously maintain tools from multiple vendors.



Incident Orientation

Centralizing the signals from multiple detection tools allows XDR platforms to combine alerts and data into incidents. XDR platforms can Intelligently combine seemingly benign signals from multiple sources to uncover threats that were not detected by any single source. The platform can also determine if alerts should be combined and escalated into holistic incidents or dismissed as false positives.

The formation of holistic incidents provides far more context to response actions than individual alerts. Incidents include all pertinent alerts and information related to an attack to accelerate investigation, decision and response actions. Presenting threats in a unified incident view is far more efficient than toggling between multiple systems to (hopefully) gather the same intelligence. In this way, XDR platforms resemble SIEM tools, but the data and capabilities are native to the XDR platform.

Response Automation

After formulating a security incident, along with all associated details and context, XDR platforms also provide response capabilities to quickly and automatically prevent or minimize damage. Response actions begin with investigation, potentially automatically collecting information associated with the incident, determining the root cause and analyzing the impact of the threat. For example, some XDR tools might automatically list running processes associated with an alert, query a windows registry, collect environmental variables or run an automated script, among others.

While much attention has been paid to the detection part of XDR, the response capabilities of the platform can allow organizations to instantly react to real threats while minimizing the burden on their security teams. Most XDR tools provide some level of automated remediation actions, such as deleting malicious files, quarantining infected endpoints or killing rogue processes. More advanced XDR platforms expand remediation across the environment and automate more complex response actions that chain various remediation actions into a single flow that runs automatically when a predefined alert is triggered.

Many large organizations are turning to Security Orchestration, Automation and Response (SOAR) technology to collect threat-related data from multiple sources and then automate responses to real threats across multiple security controls. However, successfully operationalizing SOAR is highly complex and requires a significant management burden, lending it to only the largest enterprises. XDR platforms, with multiple security controls natively built in, have the potential to provide SOAR-like capabilities without the heavy lifting required for a full SOAR solution.

The Benefits of XDR

XDR provides a holistic platform that unifies multiple control points to coordinate threat prevention, detection and response. This approach improves detection accuracy while dramatically reducing the complexity and overhead required for comprehensive threat protection.

Accuracy

XDR platforms provide a broader view of incoming threats by natively combining prevention and detection controls from the meaningful attack vectors. This holistic view enables XDR platforms to automatically separate real alerts from noise, as well as uncover subtle threat clues that may have gone unnoticed with siloed detection tools. The visibility and intelligence provided by XDR platforms leads to unprecedented threat detection accuracy.

Efficiency

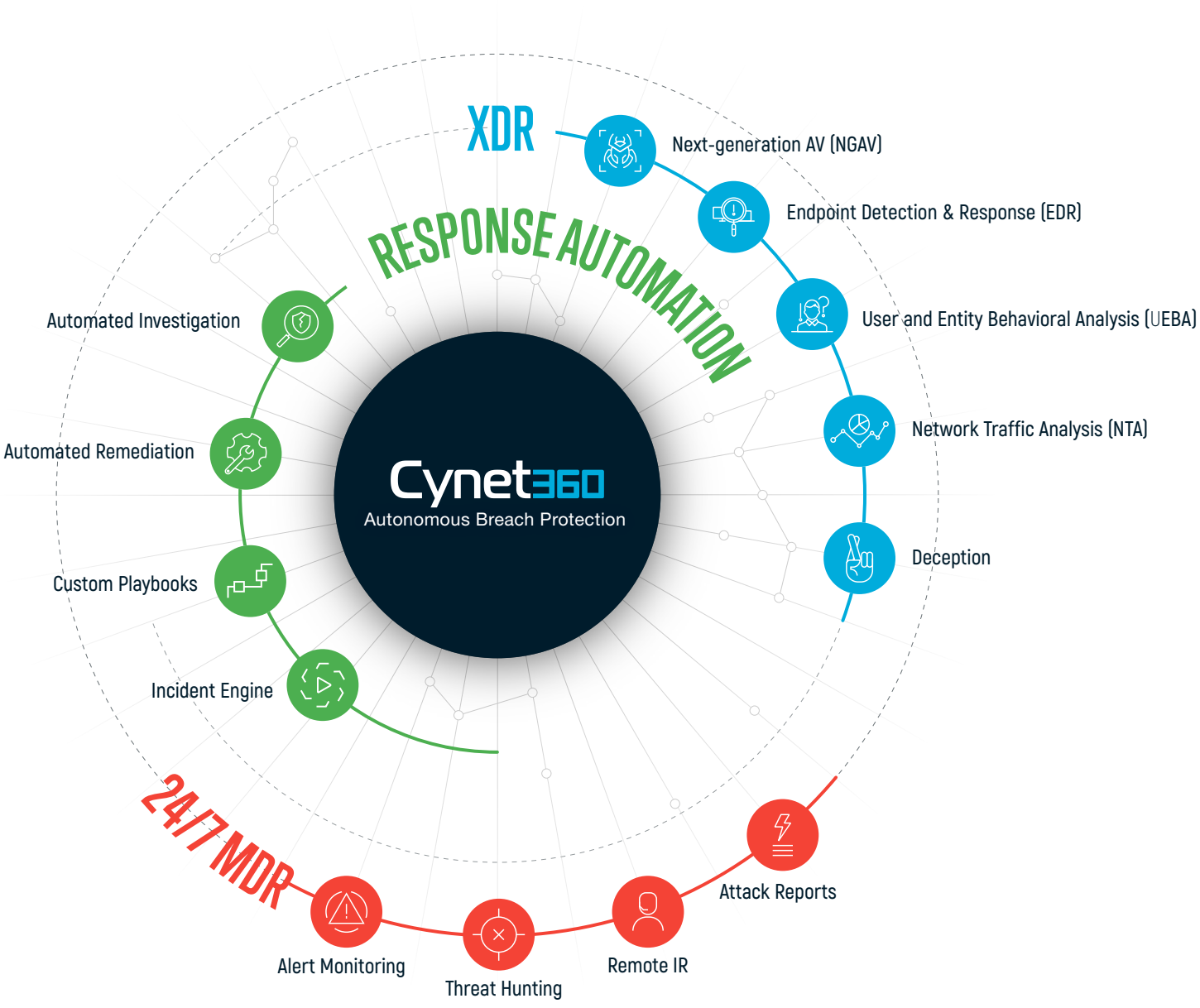
Security teams spend far less time chasing after false positive alerts with XDR platforms. Many real threats are automatically remediated with no manual intervention required. Confirmed incidents are either automatically investigated and remediated or accompanied by rich data and context to shorten manual investinvestigation and response actions. The time required to integrate, maintain and operate disparate vendor systems is eliminated. With much of the organization's threat detection and response on auto-drive, the security staff can focus on other pressing issues rather than ongoing alert-chasing.

Cost Reduction

Consolidating multiple security products into a single XDR platform provides significant cost savings, both in terms of direct vendor costs and internal support costs. Smaller companies without the full array of prevention and detection controls automatically gain broad and deep threat coverage with the purchase of a single XDR solution. Reducing a large volume of alerts into fewer meaningful incidents along with automating response actions reduces the time security teams would otherwise spend on these tasks.

Cynet 360: A Full XDR and Response Automation Platform Complemented by 24/7 MDR Services

XDR provides a holistic platform that unifies multiple control points to coordinate threat prevention, detection and response. This approach improves detection accuracy while dramatically reducing the complexity and overhead required for comprehensive threat protection.



Cynet Is Setting the Standard for XDR Platforms

Full Threat Visibility

By combining signals from endpoint, network and user controls, Cynet XDR has full visibility across your environment. The detection power achieved by natively combining signals and data from multiple sources simply cannot be matched by siloed, point protection solutions. Even the most stealthy attacks are fully exposed with pinpoint accuracy by Cynet XDR.

Complete Prevention and Detection

Cynet XDR provides multiple, integrated prevention technologies to block standard and advanced attacks across your environment. Deception technology is also built into Cynet XDR to entice cybercriminals that have successfully penetrated your network into exposing themselves before damage is done.

Incident Engine

The Cynet Incident Engine automates the entire response workflow, including automating investigation to reveal root cause and full impact of the identified threat and a wide set of remediation actions across hosts, process, files, users and network traffic. Fully automating the response workflow provides relief to overworked security teams that do not have the bandwidth, or expertise, to fully investigate and respond to every alert.

Response Automation

Cynet XDR provides fully automated response tools for cross-environment investigation and remediation. Investigations are fully automated - first determining the root cause and then analyzing the full breadth and impact of the threat. Using pre-built and custom remediation tools, Cynet XDR accelerates and optimizes incident response workflows, equipping security teams with a full remediation arsenal without ever needing to shift from the Cynet console.

Managed Detection and Response

Cynet XDR extends and improves your security resources with a team of world-class cybersecurity experts – CyOps. The CyOps team continuously monitors your environment 24/7 to ensure any attacks are uncovered, provide ad-hoc threat investigations and forensic analysis, and guide you through any necessary remediation steps. Moreover, CyOps 24/7 Managed Detection and Response is automatically included in the Cynet XDR platform – at no additional cost. While other providers charge exorbitant fees for this type of service, you won't pay a penny extra with Cynet.