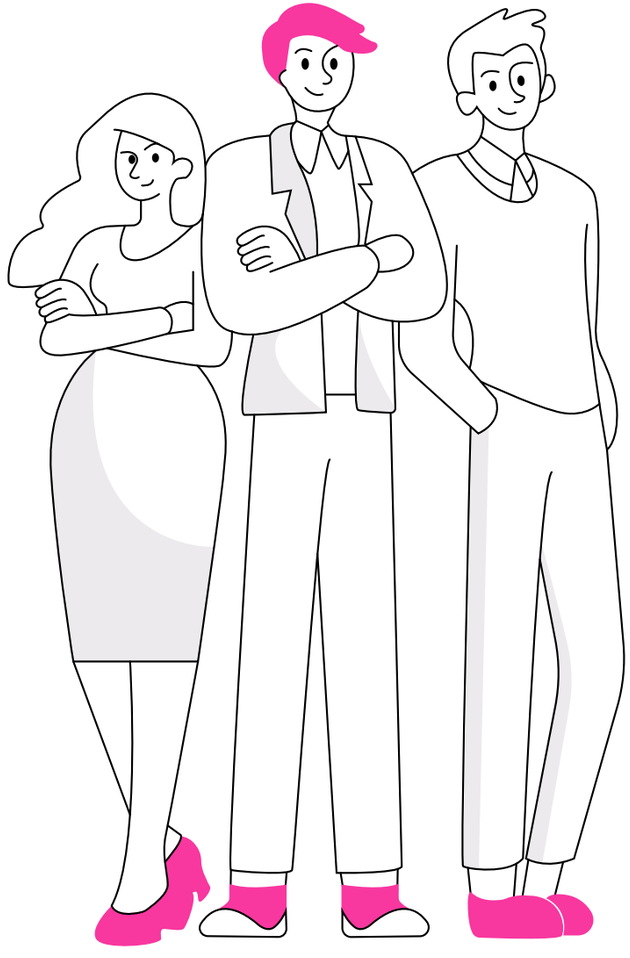
cynet

Comprehensive, Easy Cybersecurity for Lean IT Security Teams Starts with

Extended Detection and Response (XDR)



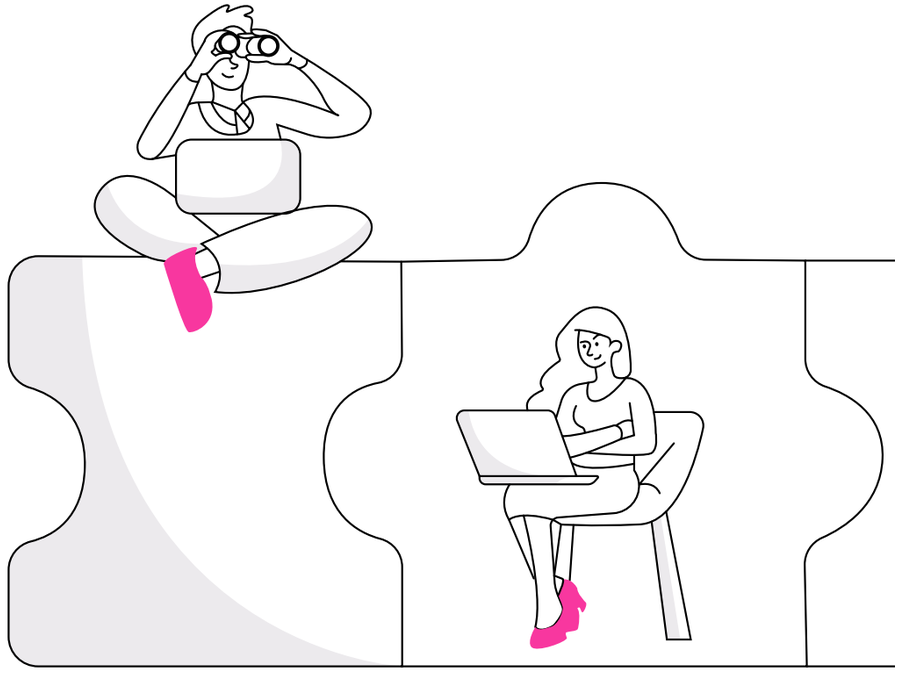
Contents

The Need for Full Protection, Visibility and Instant Response:
Cybersecurity for Lean IT Security Teams

Effective cybersecurity comes down to an organization's ability to see and eliminate all threats. This includes:

- Preventing threats before they infiltrate IT systems.
- Detecting the threats that do make their way into the environment.
- Determining if a detected threat is part of a larger attack.
- Containing and eradicating all threats and attack components.

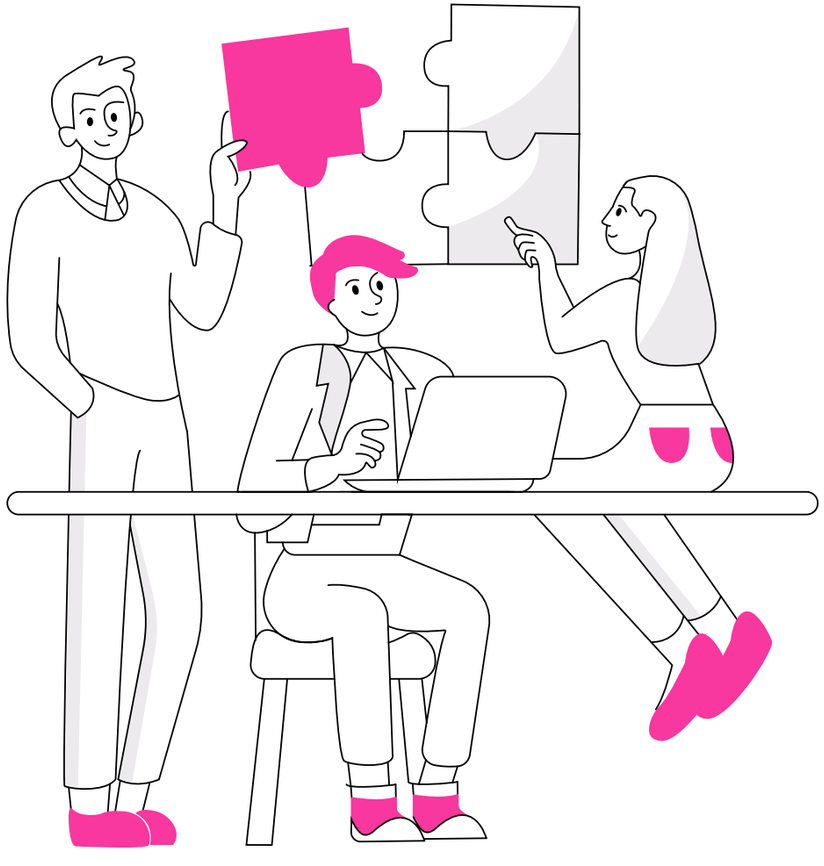
Therefore, cybersecurity technology must detect and react to threats in an instant.



The Challenge:
Effective Cybersecurity Requires Big Budgets and Big Teams

Implementing a solution that instantly detects and reacts to all threats is easy to say but difficult and expensive to accomplish. Most organizations cannot afford the wide array of security solutions needed to detect and stop advanced threats across their environments. They lack the full visibility required to detect all threats and the automation needed to respond quickly and completely. Missing, too, are the people and expertise required to manage their cybersecurity technology and fully address all security issues.

The realization that cybersecurity technology must be more effective while also being more integrated, automated, and intuitive is driving XDR.



XDR: A New Approach to Cybersecurity

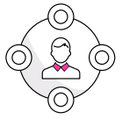
As a new cybersecurity category, XDR has been described differently by industry analysts and security vendors. Because most analysts and vendors focus on serving massive enterprises, their approach to XDR is skewed to the needs of these constituents. These companies tend to already have multiple prevention and detection technologies, as well as additional integrations like Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) solutions, in place.

But these organizations struggle with sufficiently integrating and orchestrating these technologies. Most XDR solutions focus on integrating and orchestrating the technology stack that already exists within these large global enterprises to improve real-time threat detection and response and reduce “panes of glass.”

Companies outside of the Fortune 500, conversely, cannot afford the vast array of cybersecurity solutions required to protect against advancing threats and lack the staff and expertise to build, operate, and maintain a complex, multi-product security stack. For these companies, an XDR solution that was purposely built for small security teams can provide the key technologies required to monitor the entire environment and the response automation necessary to react to threats and attacks — all on a single, natively-built platform.

Rather than being forced to acquire and integrate a multitude of security products, XDR can provide all the necessary protection capabilities out-of-the-box.

An XDR solution purposefully built for lean security teams has four key characteristics: it’s **comprehensive, intuitive, automated**, and fully **supported**.

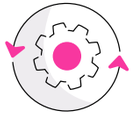


Comprehensive

The core characteristic of an XDR platform that supports lean security teams is comprehensiveness — providing an extensive set of native tools and capabilities that are pre-integrated out-of-the-box. Rather than forcing companies to research, purchase, install, integrate, and maintain a broad set of cybersecurity solutions from multiple vendors, XDR can provide the most important tools necessary on a single platform.

Intuitive

Most cybersecurity solutions designed for large enterprises provide an extensive set of features and configuration settings — making the tools highly complex to operate. The complexity only gets worse when several of these tools must be configured and operated by a lean security team. By natively building all capabilities into a single platform, XDR solutions become much easier to master.



Automated

Because most companies don't have the luxury of a large, expert security team, they are overwhelmed by an unending stream of time-consuming manual tasks. One of the drivers for XDR was to extend the response automation capabilities found in EDR technologies. Lean security teams, in particular, benefit from automation to both perform important functions that may be beyond their expertise and those that are routine and extremely time consuming.

Supported

Lean security teams do not have the bandwidth or expertise of their large enterprise counterparts. XDR vendors can provide extensive support capabilities to supplement the technology platform and act as an extension of their client security team. This support can and should go beyond help operating the platform to assist with technical questions, alert interpretation, response strategy, and any other security-related questions their clients may have. A comprehensive technology solution, like XDR, should also provide full support to be considered a complete solution for lean security teams.

The Core Capabilities of XDR for Lean Security Teams

XDR helps security teams by extending threat visibility across the environment and automating investigation and response actions. The primary requirements of an XDR platform are **threat visibility**, **alert correlation**, and **response automation**.

Broad Threat Visibility and Protection

XDR is based on broad visibility across the primary prevention and detection components that provide the most pertinent threat telemetry. Although many organizations with lean security teams have turned to Next Generation Anti-Virus (NGAV) and Endpoint Detection and Response (EDR) solutions, cybercriminals are successfully bypassing these endpoint-centric approaches with increasingly stealthy attacks. Confirmed breach levels have continued to rise despite massive investments in cybersecurity solutions and resources.

Deciding which prevention and detection components should be included in the XDR platform is critical. Platforms with components that cover the primary attack vectors, providing layered security protection, should be prioritized. Consider the following features when investigating XDR platforms.

- **NGAV/EPP** - Next Generation AntiVirus/ Endpoint Protection Platform, for basic endpoint malware prevention and detection and endpoint control
- **EDR** - Endpoint Detection and Response, for more advanced endpoint protection, detection, and response)
- **NTA** - Network Traffic Analytics, for malicious activity on your network
- **UBA** - User Behavioral Analytics, to detect anomalous user behaviors
- **SSPM & CSPM** – SaaS Security Posture Management & Cloud Security Posture Management, to reduce the risk introduced by SaaS and Cloud misconfigurations

The signals from these solution categories provide the broad visibility required to detect the vast majority of attacks across the cyber kill chain. These components, which may be supplemented by other data, have been shown to provide the best value. For example, signals from Deception technologies can trick successful intruders into exposing their presence before damage is done, providing highly valuable signals for an XDR platform.

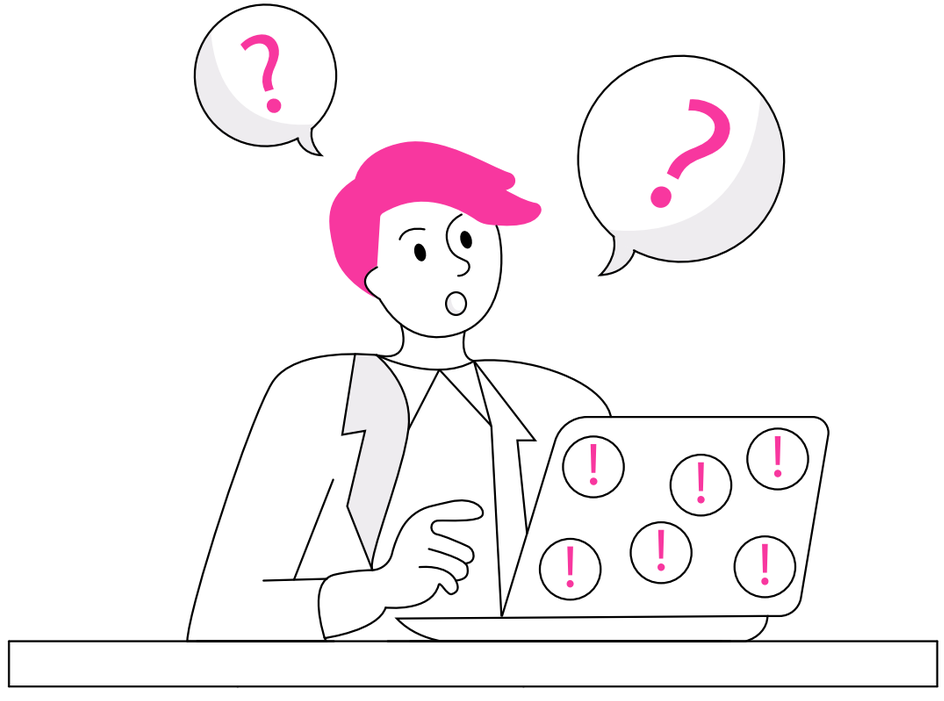
Because most companies with lean security teams cannot afford to acquire, integrate, and maintain multiple prevention and detection tools, XDR solutions built for lean security teams can provide an affordable and logical route to layered protection. For example, including Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) capabilities natively within the XDR platform provides critical security capabilities that resource-constrained teams might otherwise find unattainable.

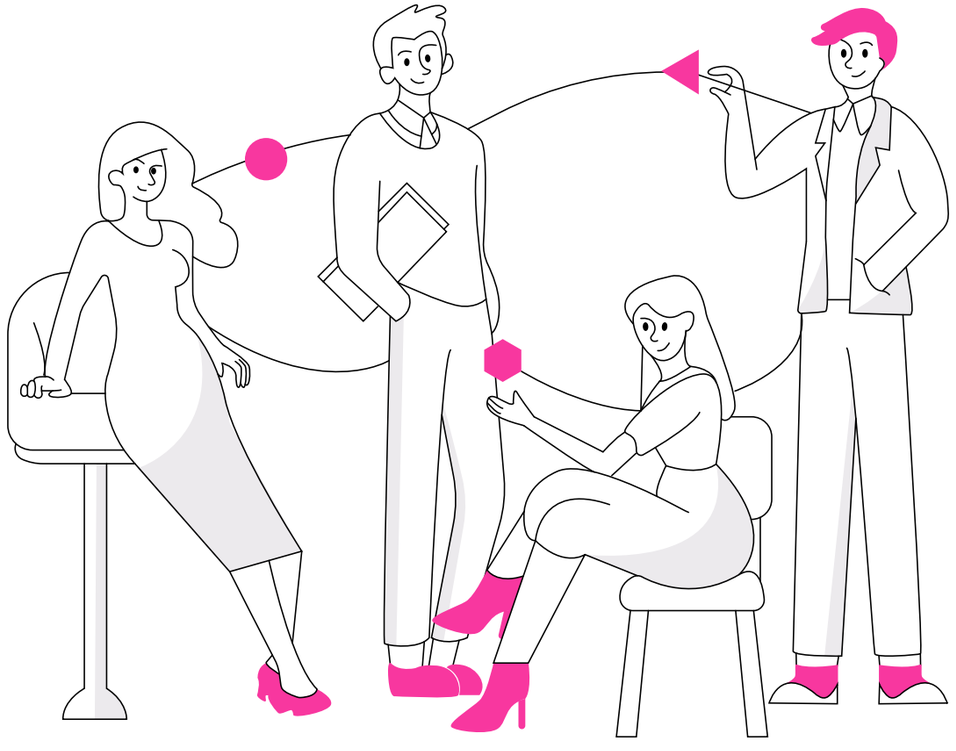
Alert and Data Correlation

The real challenge in security today is to find threats that bypass first line defenses as quickly as possible. Something that may seem harmless to one security solution suddenly becomes cause for concern when intelligently paired with information from other security solutions.

Combining signals from multiple points of telemetry provides the context required to detect stealthy (and otherwise undetectable) attacks while providing far greater detection accuracy (and thereby slashing false positives). When all prevention and detection components are part of a single platform, data and alert information can be easily normalized and combined; a difficult feat when trying to coordinate multiple vendor point solutions.

Combining signals into incidents provides far more context for response actions than individual alerts can detail. An incident view includes all pertinent alerts and information related to an attack to accelerate investigation, decision, and response actions. This also provides a significant time-savings over 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

Security teams today spend far too much time investigating alerts. Once threats are confirmed, an investigation of the full breadth of the attack requires access to multiple controls through multiple consoles and presentation schema. Remediating threats also requires a significant effort to plan and coordinate corrective actions across multiple security systems. Security teams are simply overwhelmed by operating and maintaining too many point solutions.

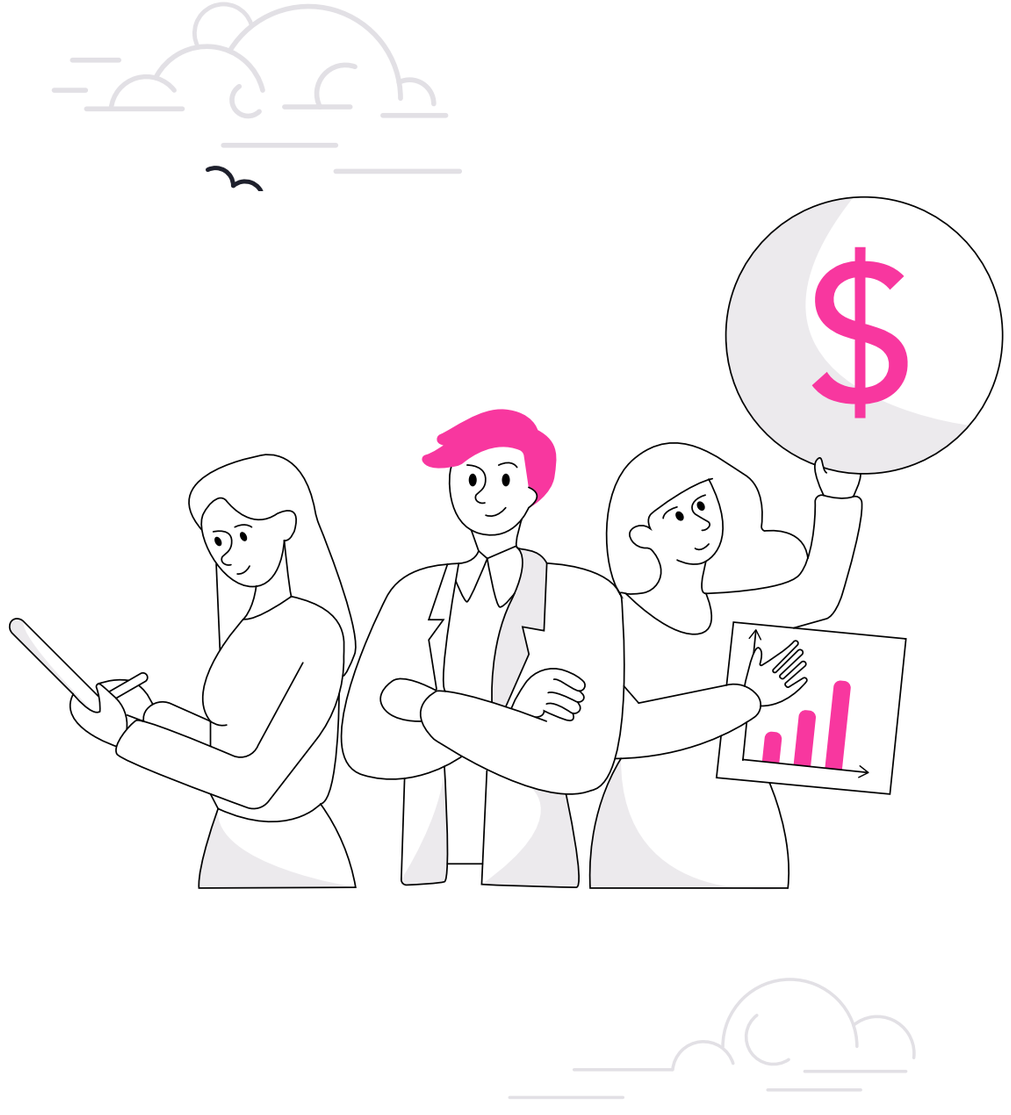
XDR platforms provide response capabilities to quickly and automatically prevent or minimize damage. Response actions begin with investigation, potentially automatically collecting information associated with the incident, determining the root cause, and analyzing the impact of the threat. For example,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

While a lot of 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 infrastructure and automate more complex response actions that chain various remediation actions into a single flow that automatically runs 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, reserving it for only the largest of 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 for Lean Security Teams

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.

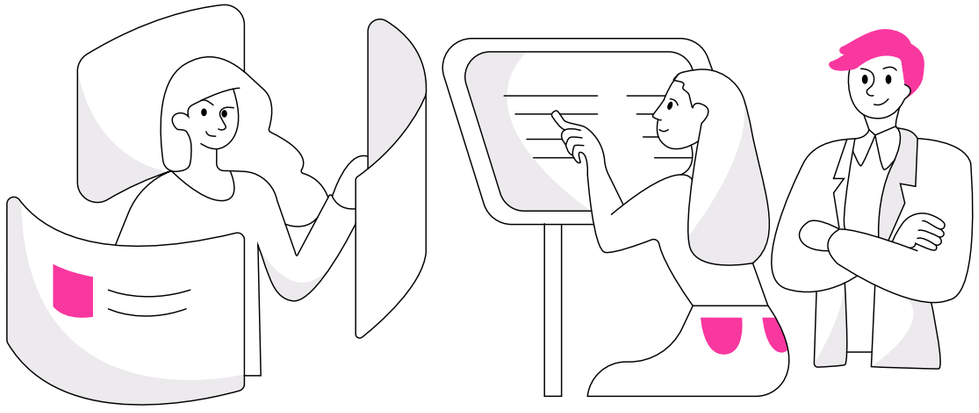


Accuracy

XDR platforms provide a broader view of incoming threats by natively combining prevention and detection controls from the most 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 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 investigation 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

Consolidation of 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.

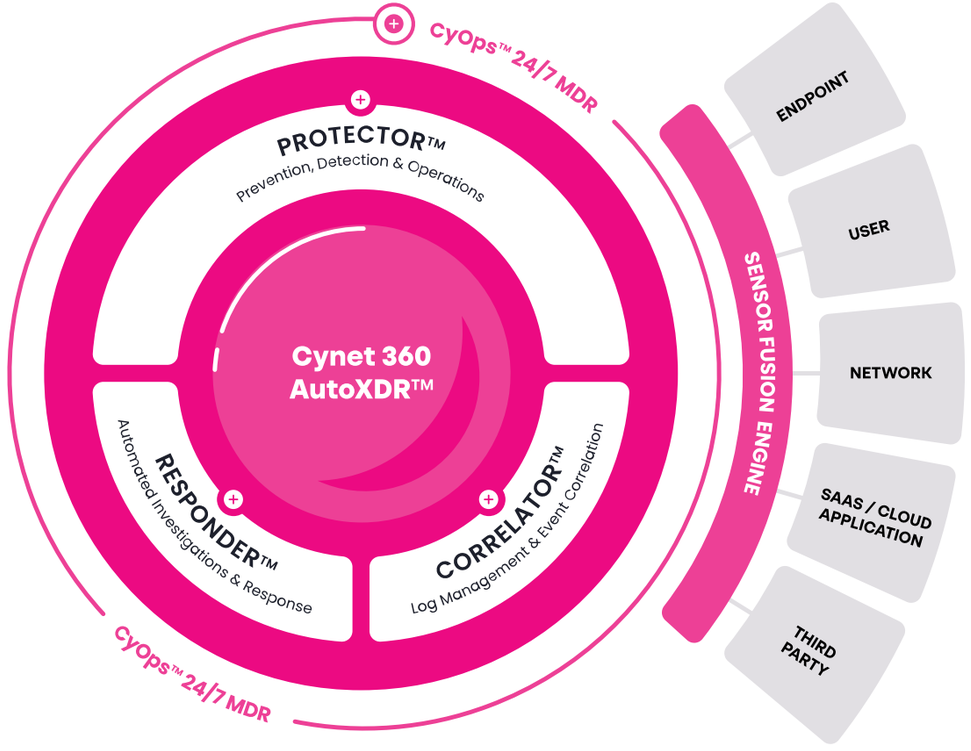
Simplicity

Cynet's natively automated, end-to-end platform eliminates the complexity of managing multiple disjointed security tools. Cynet enables a new era of cybersecurity with a platform that is fast to deploy and easy to use while providing comprehensive and effective threat protection. As Leonardo Da Vinci said, "simplicity is the ultimate sophistication." Cynet has done the heavy lifting to integrate the important protections you need on a single, affordable, intuitive XDR platform.

Cynet 360 AutoXDR™: A Natively Automated, End-to-End XDR Platform for Lean IT Security Teams, Complemented by 24/7 MDR Services

While the XDR category is new, Cynet pioneered the concept of XDR before the term was even invented. Along with deep experience and mature, vetted XDR capabilities, Cynet 360 AutoXDR™ provides the most extensive automated remediation capabilities available from any XDR provider. Moreover, Cynet provides an expert team of cybersecurity experts to augment and guide your team 24 hours a day, 7 days a week — included with the Cynet 360 AutoXDR™ platform.

Cynet 360 AutoXDR™ was purpose-built for lean security teams that need an "all in one" solution that's easy to use, highly effective, and affordable. With multiple security capabilities, an extensive set of automated response actions, and a 24/7 MDR service included at no extra cost, Cynet 360 AutoXDR™ provides the most effective total cost of ownership (TCO) possible for lean security teams.



Cynet Is Setting the Standard for XDR for Lean Security Teams

Full Threat Visibility:

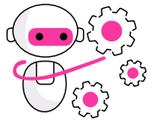
By combining signals from endpoint, network, and user controls, Cynet enables full visibility across your environment. The detection power achieved by natively combining signals and data from multiple sources simply cannot be matched by siloed point protection solutions. Even the stealthiest attacks are fully exposed with pinpoint accuracy by Cynet 360 AutoXDR™.

Complete Prevention and Detection:

Cynet's platform integrates multiple prevention technologies to block standard and advanced attacks across your environment. Deception technology is also built into Cynet 360 AutoXDR™ to entice cybercriminals that have successfully penetrated your network into exposing themselves before damage is done.

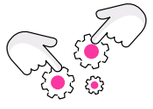
Alert Correlation:

Combining signals from multiple detection sources allows Cynet's platform to group related alerts and data into actionable incidents, leading to more accurate alerts. Analysts experience less alert fatigue and no longer need to toggle between multiple systems to gather threat intelligence.



Response Automation:

Cynet provides fully automated response tools for cross-environment investigation and remediation. Investigations are fully automated — the root cause is determined, then the threat's full breadth and impact are analyzed. Using pre-built and custom remediation tools, Cynet 360 AutoXDR™ 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 360 AuotXDR™ 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 360 AutoXDR™ platform — at no additional cost. While other providers charge exorbitant fees for this type of service, you won't pay a penny extra.

About Cynet

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, SSPM, and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Learn More