RANSOMWARE PREVENTION, DETECTION AND REMEDIATION

CYNET STOPS RANSOMWARE BEFORE IT STOPS YOU

The rising ransomware threat

Ransomware is a type of malware that threatens to publish the victim's data and/or perpetually block access to it unless a ransom is paid. Some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse. More advanced ransomware uses a technique called cryptoviral extortion, in which it encrypts the victim's files to make them inaccessible and demands a ransom payment to decrypt them.

Stopping ransomware in its tracks

The Cynet XDR platform provides a layered approach to ransomware protection with extended visibility and protection across endpoints, networks and users. This uniquely allows Cynet to immediately detect ransomware at the beginning of its cycle. With the ability to automatically respond, Cynet can stop the process before files or drives are encrypted.

Key Benefits

Natively Layered Protections

Cynet XDR includes integrated NGAV, EDR, NDR, UEBA and Deception technologies out of the box.

Automated Response Actions

Cynet can automate a wide range of remediation actions at the first hint of ransomware.

Real-time Protection

Specifically designed to prevent and detect advanced ransomware threats.

Single Click Away

One click on 'engage CyOps' in the Cynet Dashboard app to get a security analyst on the line.

100% Proactive

Continuously hunting for critical and evasive threats in your environment.

Extended Prevention and Detection

Cynet utilizes machine learning malware detection that leverages rich data across millions of malware samples and continually improves as new malware evolves. Beyond Cynet's protections that scan files at rest and non-executable files, Cynet additionally employs several real-time protection mechanisms specifically designed to prevent and detect ransomware, including:

Real-time Memory Protection

Detect and block memory strings which are associated with ransomware so even unknown/obfuscated ransomware is exposed upon execution.

Critical Component Filtering

Protect the OS password vault so ransomware cannot harvest credentials and spread across the network.

Real-time File Filtering

Detect and prevent unapproved apps from writing to various file types, preventing access to important company assets.

Deception Technology

Place decoy files and hosts in various locations, especially those that ransomware typically tries to access, to detect the presence of ransomware.

Automated Investigation and Remediation

Quickly uncovering and fully remediating all components of a ransomware attack ensures that the entire scope of the attack is contained and no hidden components are left lingering in your environment. Cynet automated response capabilities ensure ransomware attacks are immediately detected, blocked and eradicated, including:

Automated Incident Engine

Automatically launches an investigation following high risk alerts to uncover the root cause and full extent of the attack and can then automatically apply all required remediation actions across the environment.

Extended Remediation

Cynet XDR provides the widest range of automated remediation actions across endpoints, networks and users.

Custom Remediation

Beyond the built-in remediation capabilities, Cynet enables you to build your own custom remediations leveraging custom scripts and commands for more complex remediation actions unique to your environment.

Automated Remediation Playbooks

Combines multiple remediation actions together in response to specific threats. Playbooks can be automatically invoked when the threat is detected or triggered manually, depending on what the organization prefers.

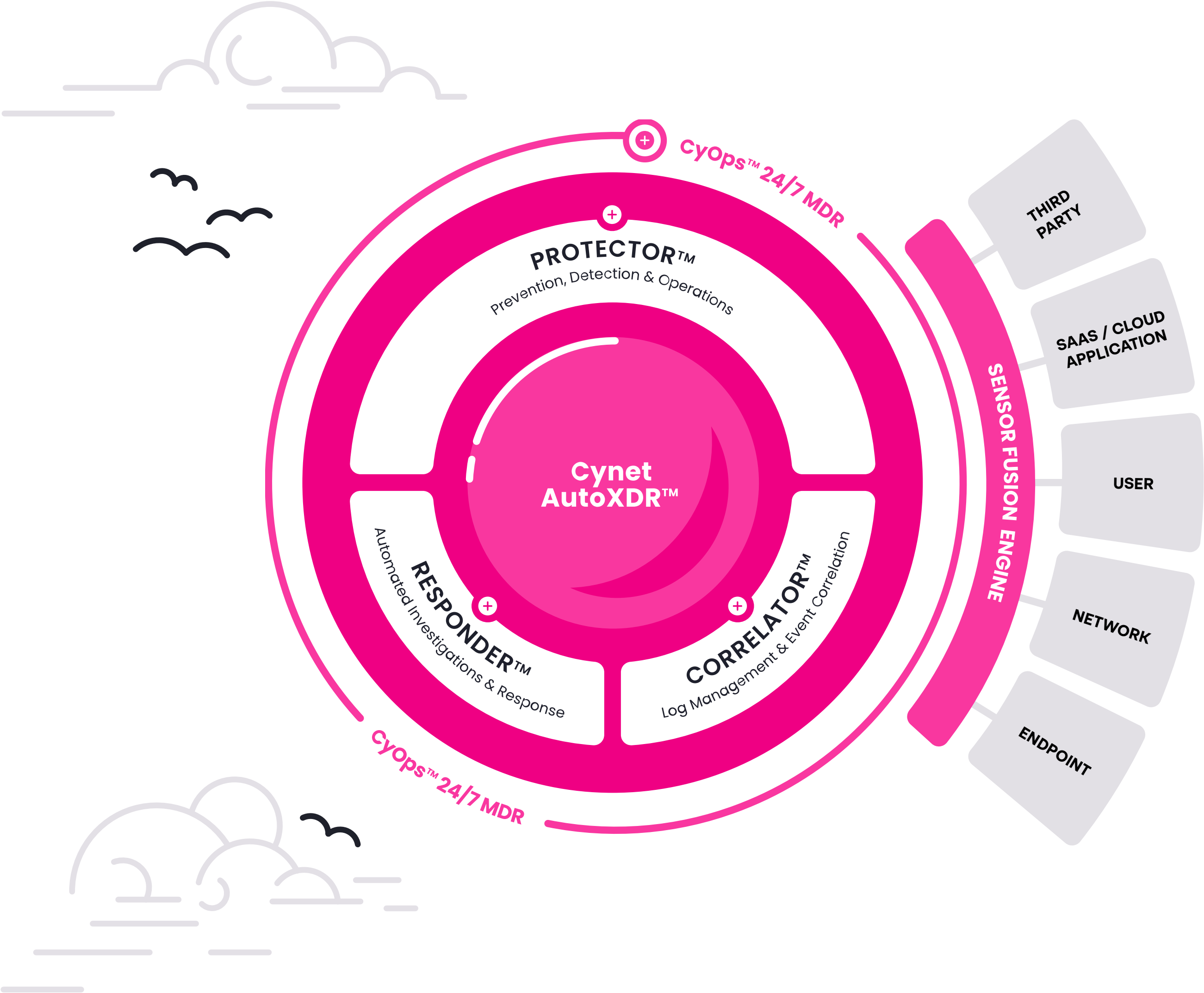
24x7 Proactive MDR Service

Cynet's 24x7 MDR service continuously monitors your environment to ensure nothing is overlooked and any hint of ransomware is immediately investigated and resolved. Cynet's world-class cybersecurity team, CyOps, expert oversight and advice is available to all Cynet clients at no additional cost. CyOps researchers are continuously analyzing the newest ransomware techniques, developing protection mechanisms, and educating clients on best protection practices.

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.

LEARN MORE