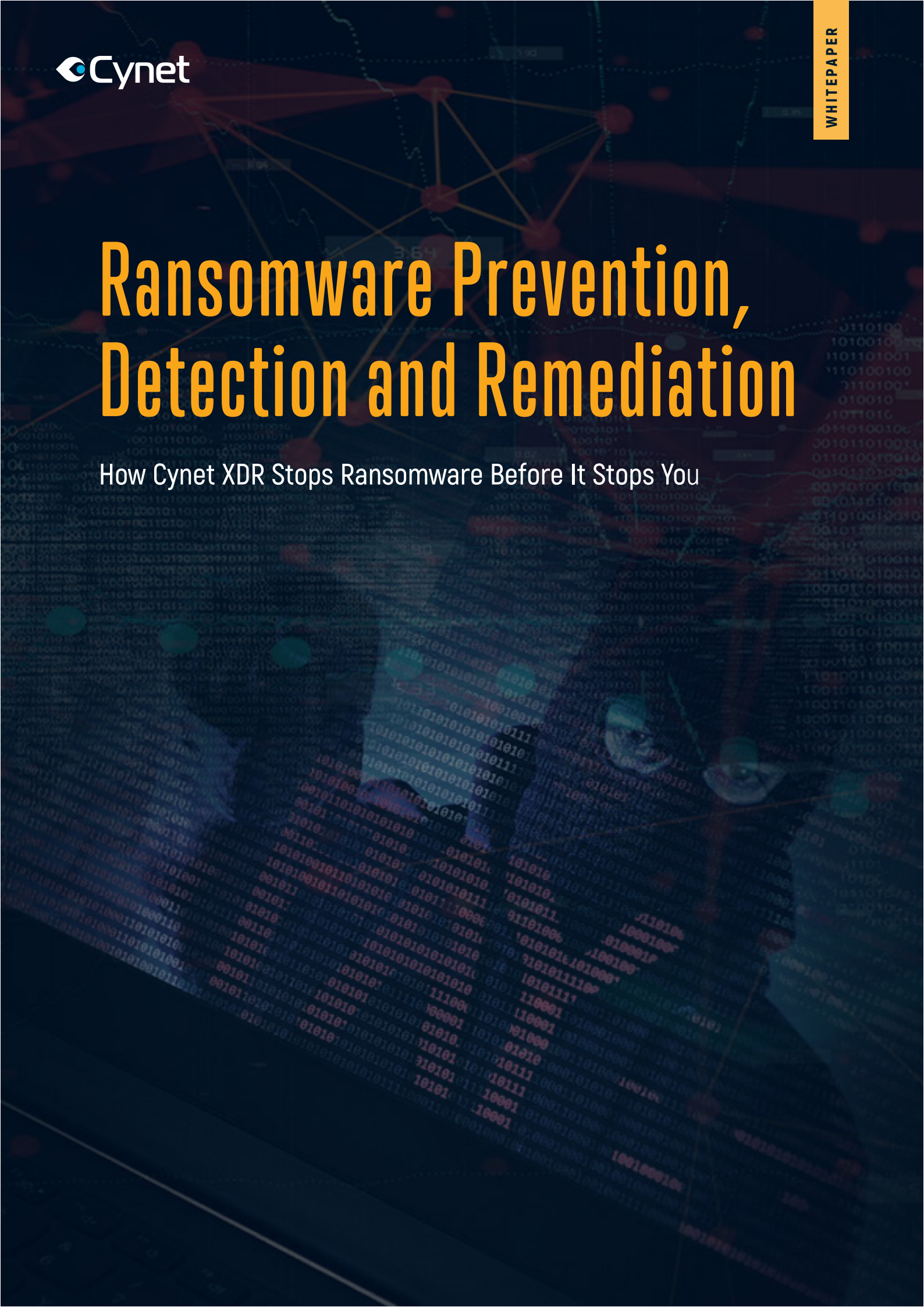
Cynet

WHITEPAPER

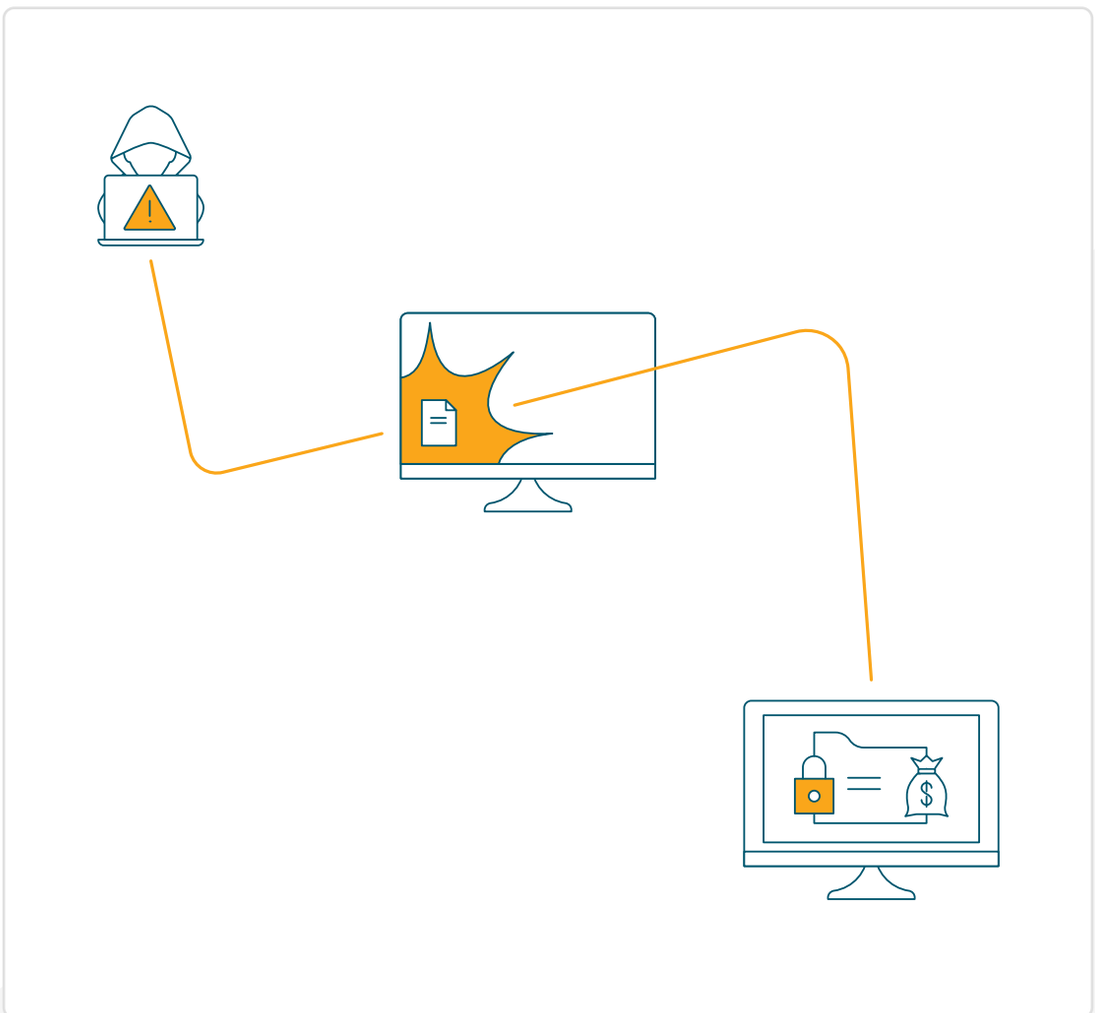
Ransomware Prevention, Detection and Remediation

How Cynet XDR Stops Ransomware Before It Stops You



Overview

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.



Cynet XDR Prevents Ransomware

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 its ability to automatically respond, it can stop the process before files or drives are encrypted.

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. Cynet AI capabilities are based on the in-depth knowledge of our cybersecurity researchers and, as such, adapt to new ransomware techniques rapidly and effectively. Cynet's AI can scan suspicious files and classify them according to their nature. 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.

Real-time Memory Protection

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

Examples:

- Identify encryption attempt behavior
- Attempt to delete shadow copies
- Attempt to inject to legit processes such as wmic.exe or other legitimate OS processes
- Identify SSDeep-based processes loading into memory

Critical Component Filtering

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

Examples:

- Protecting the hard drive Master Boot Record
- Protecting sensitive registry locations

Real-time File Filtering

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

Examples:

- Only MS Office apps allowed to write to or change .docx files
- Sensitive files custom access only by specific business application
- Alerting based on abnormal file access by unique applications

Deception Technology

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

Examples:

- Detect ransomware access and exfiltration using decoy files
- Detect ransomware lateral movement using decoy connections
- Detect mass delete / change files

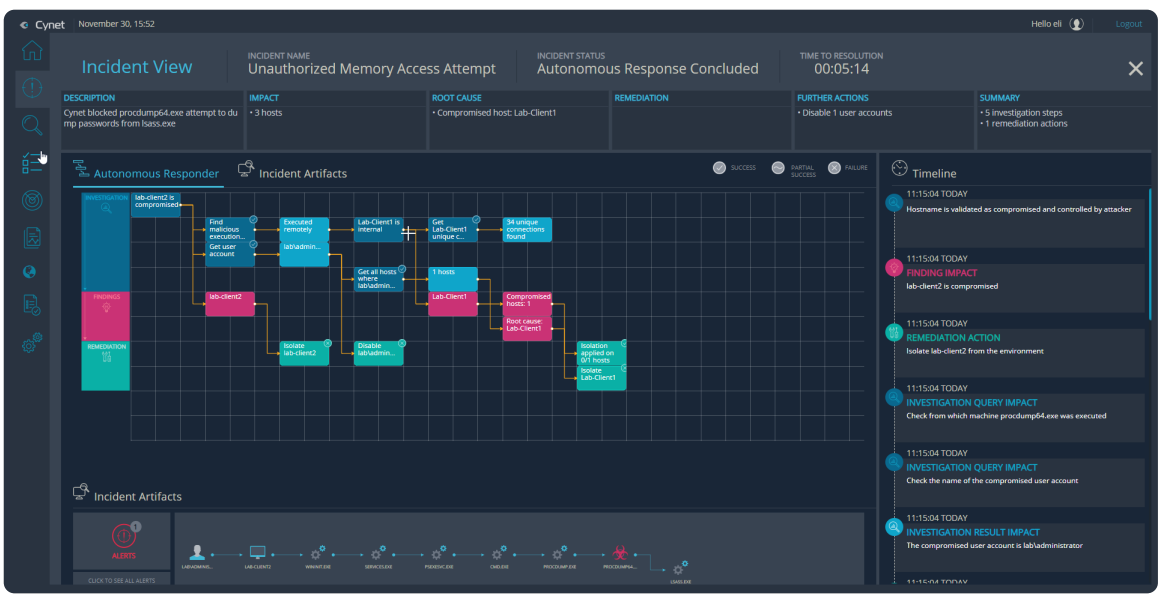
Automated Investigation and Remediation

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.

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. Remediating an identified threat may provide temporary relief, but until all components of the attack are discovered and fully remediated can you be assured you are safe.

In the example below, Cynet detected that a legitimate windows process was attempting to access stored credentials. Simply killing this process would block this attempt and resolve the alert, but does not fully expose and remediate the attack. The Incident Engine investigates the alert and immediately finds that the host is compromised and isolates the machine. Further investigation determines the root cause to be a different compromised internal machine that is attempting to move laterally through the environment. Cynet isolates that machine and disables the administrative account responsible. These actions halt the attack and provide important data for the security team to further respond to this incident.



Example showing investigation and remediation steps in the Cynet Incident Engine

Extended Remediation

Cynet XDR provides the widest range of automated remediation actions across endpoints, networks and users. Cynet includes remediations for every detection mechanism in the platform. Multiple remediation actions across the environment are often necessary to eliminate all traces of an attack. Cynet XDR can take necessary remediation across files, hosts, networks and users from a single pane of glass.

Remediation examples:

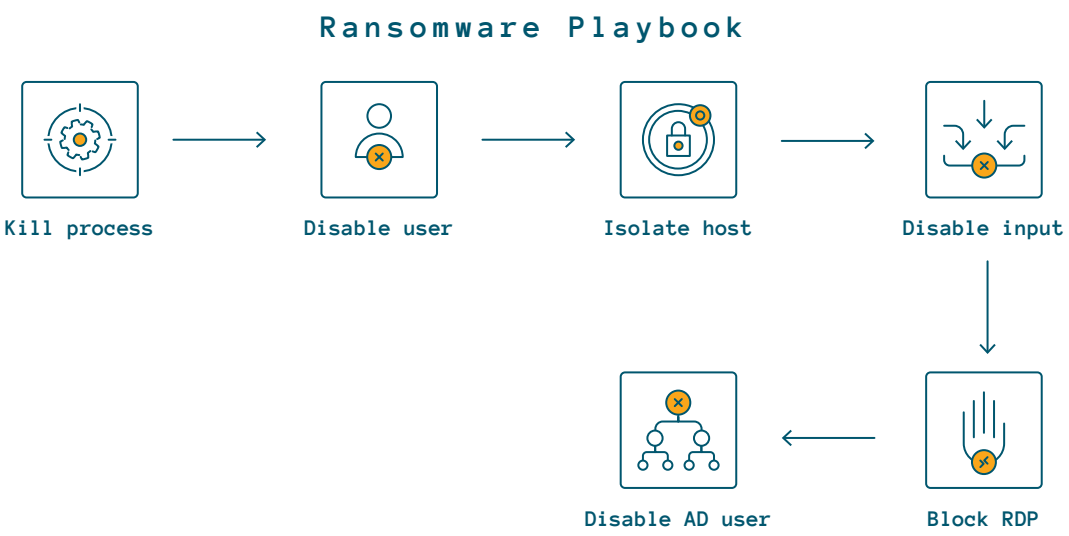
File	Host	Network	User
• Restart	• Isolate	• Block Traffic	• Disable/enable
• Change IP	• Run Command	• Clear DNS Cache	• Reset Password
• Delete/Disable Service	• Run Script		
	• Delete		
	• Quarantine		
	• Kill Process		

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. You can also automate the actions taken to remediate a specific threat to create a custom remediation.

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. Clients can leverage pre-built remediation playbooks provided in the Cynet platform or easily build fully customized playbooks to suit their particular needs. Additionally, Cynet is always available to create remediation playbooks upon request.



Example of an automated ransomware playbook

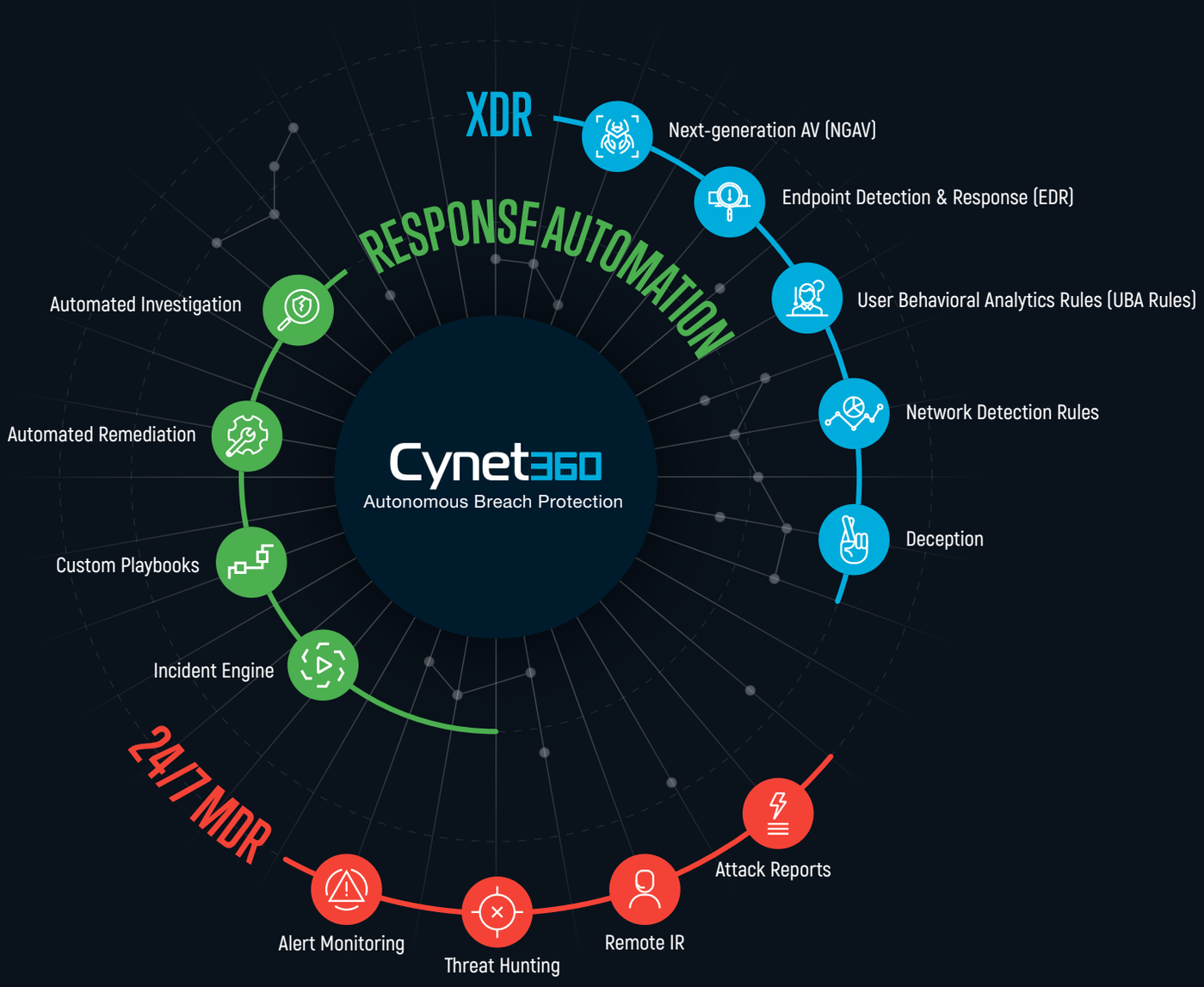
24x7 Proactive MDR Service

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 Cynet

Cynet XDR provides a single, unified platform to prevent, detect, investigate and fully remediate the broad range of attack vectors. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

LEARN MORE



Cynet