Solution Brief

Cynet 360 AutoXDR™ Platform Support

CMMC Compliance

Companies that work along the DoD supply chain must now meet the standards of the Cybersecurity Maturity Model Certification (CMMC). Unless companies meet a certified level of cybersecurity from a certified assessor, they may be ineligible to participate in DoD contracts. Cynet can help meet the standards required for several of the most challenging CMMC domains.

Overview

The Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC) to ensure contractors have implemented best practices around cybersecurity. The CMMC model provides a broad set of requirements that must be implemented by all DoD suppliers and the maturity level claimed must be validated by an independent certified examiner to be eligible for DoD contract awards.

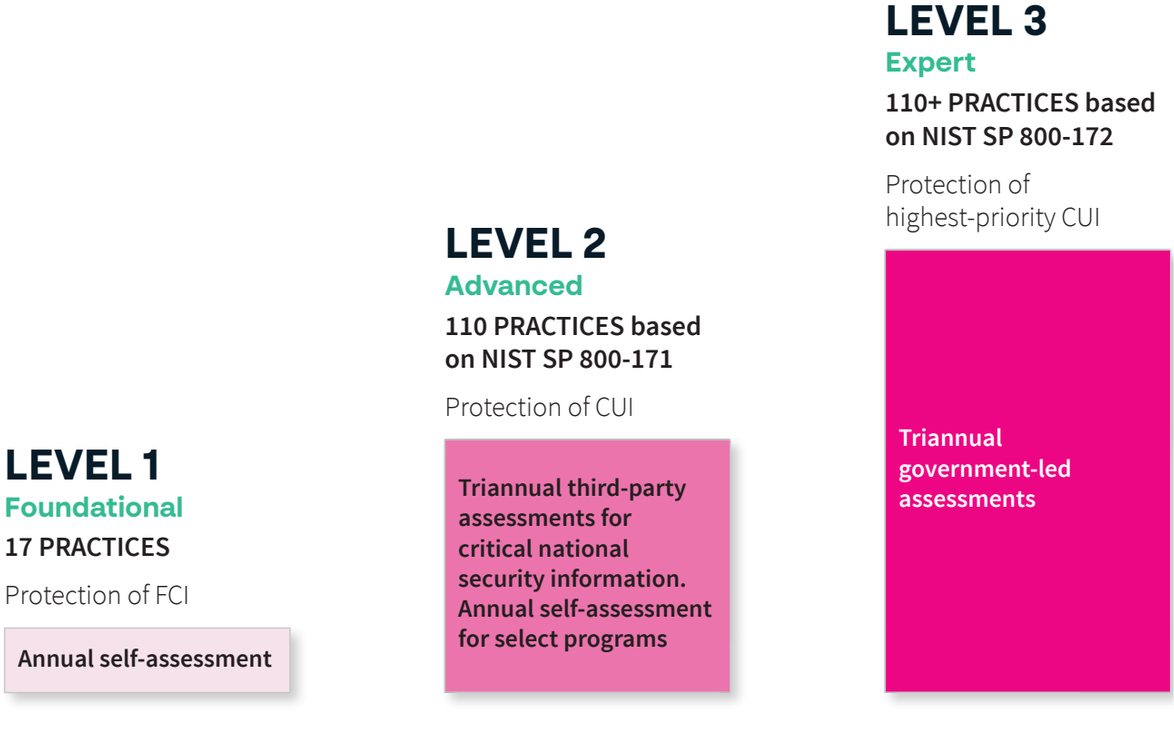
There are three tiered certification levels established by CMMC 2.0, each reflecting an organization's maturity attained in cybersecurity processes and practices across 14 domains. The maturity levels range from "Foundational" to "Expert." Level 1 applies to organizations that only protect federal contract information (FCI), while Levels 2-3 deal with protecting controlled unclassified information (CUI) .

While CMMC 2.0 does not take effect until mid-2023, it is anticipated that the bulk of DoD contracts will require compliance with Level 2, "Advanced." A smaller proportion of companies will target Level 3, depending on the contracts desired.

Achieving CMMC Compliance

The CMMC requirements include a mix of standards focused on people and processes, as well as a lesser amount of cybersecurity technologies that must be implemented and maintained.

While some of the 300,000+ DoD contractors have the resources and expertise to fully meet their CMMC requirements using in-house resources, many will require help from outside providers. Contractors may need help with defining policies and procedures, documentation, cybersecurity technologies or ongoing monitoring and reporting.



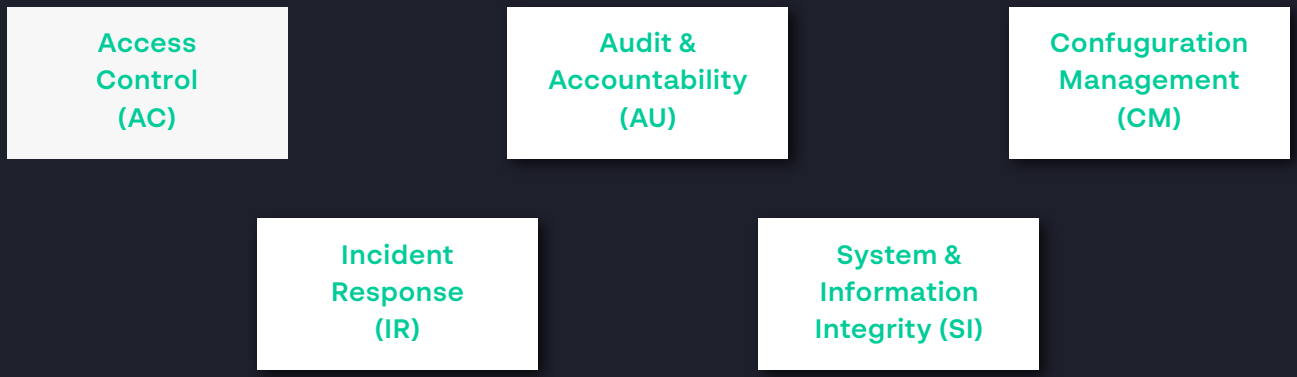
CMMC Model 2.0

How Cynet Helps

Cynet provides a sophisticated threat prevention and detection platform that can automatically assess and remediate even the most sophisticated cyber attacks.

The Cynet 360 AutoXDR platform deploys in hours, immediately providing insights and protections across your IT environment. Cynet's comprehensive 24x7 MDR service is also available to help protect customer environments. The combination of controls and full response automation, along with our MDR service, provides an extensive set of cybersecurity capabilities for meeting CMMC requirements.

Cynet can help you address several security requirements across five different CMMC domains, including:



CMMC Domains Supported by Cynet

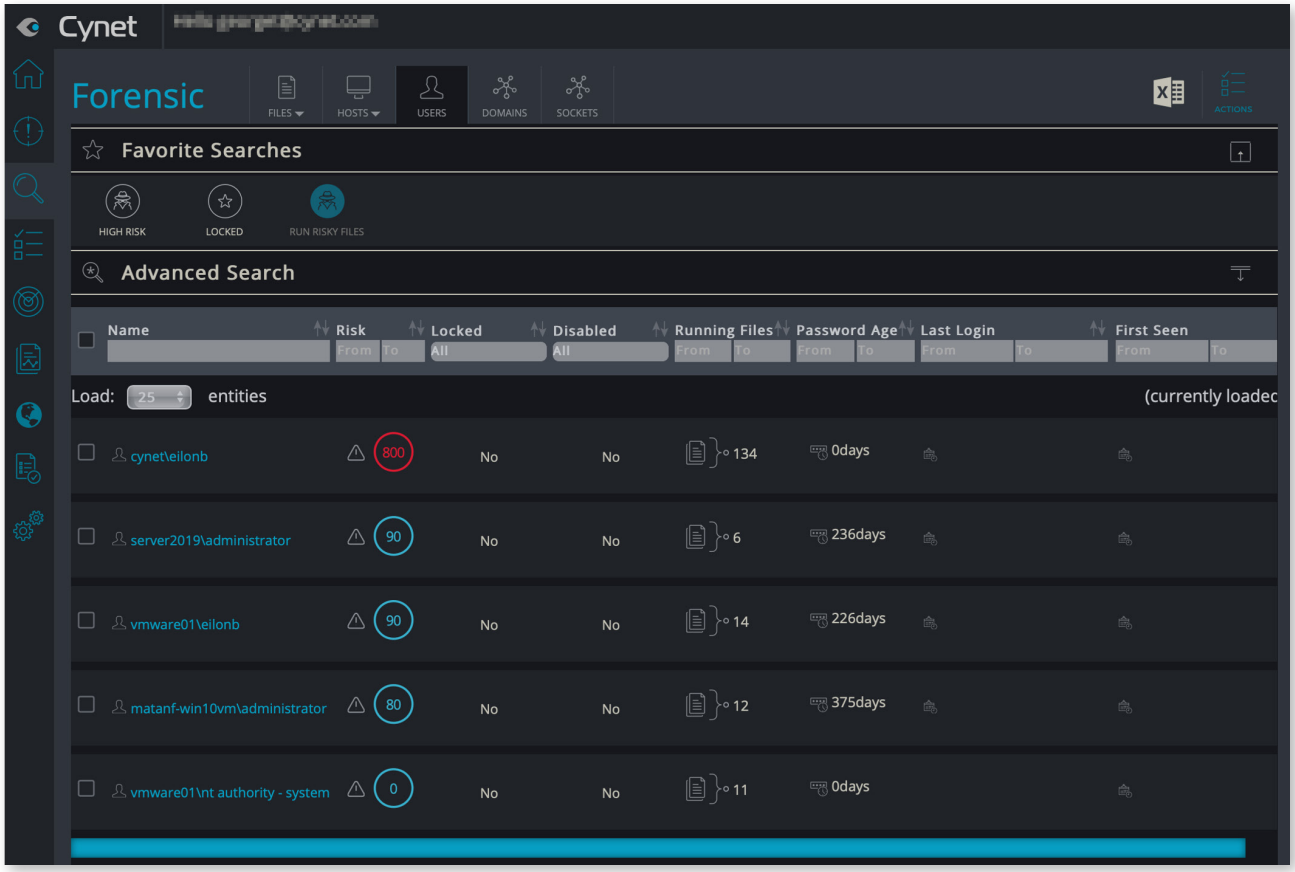
CMMC Domains and Practices

The CMMC defines a number of practices required for each of fourteen domains. These domains span a variety of security areas, ranging from physical security to training to incident response.

See below for details about how Cynet supports practices in five of the CMMC domains. This information will be updated once the details of CMMC 2.0 are formally published.

Access Control (AC)

Cynet 360 AutoXDR provides supplemental support practice **AC 1.001** by continuously collecting and analyzing all account management and network access/authentication logs. Cynet correlation rules provide alerting on account authentication failures. Cynet User and Entity Behavioral Analytics Rules (UEBA Rules) profiles user activity and alerts upon anomalies that are indicative of malicious presence. Cynet investigations, reports, and logs provide evidence of account access/authentication activity.

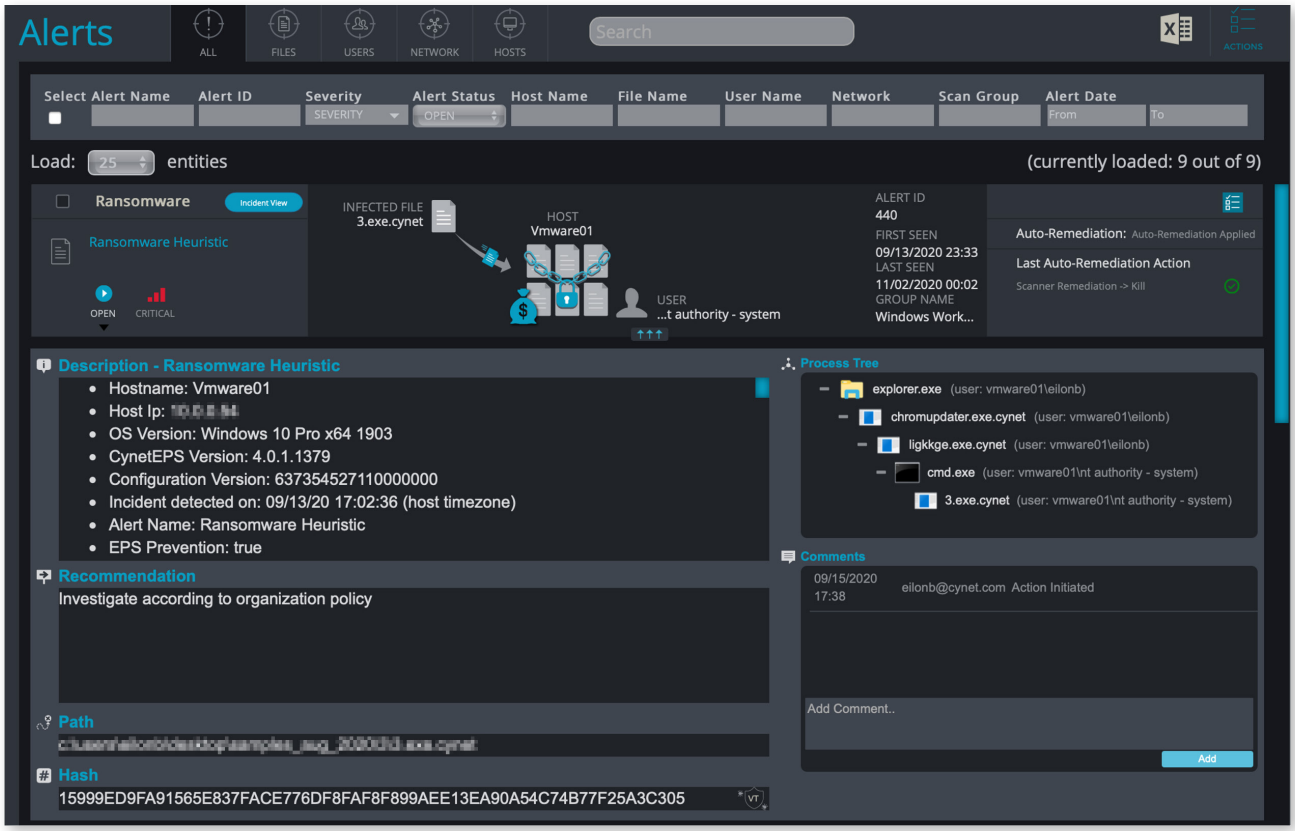


Search results for users that ran risky files in Cynet's Forensics view

Audit and Accountability (AU)

Cynet 360 AutoXDR detects threats across hosts, users, files and networks. It also uses deception technology to lure attackers into exposing their presence in your environment. Cynet collects, analyzes and retains successful & failed logins, software download, password changes and multiple other activities within the environment according to data privacy requirements (learn more here), providing unmatched clarity and context into current and historic events, supporting practice **AU 3.045**. And, Cynet easily integrates with SIEM platforms to support the efforts to consolidate audit information into a central repository if desired, per practice **AU 3.048**.

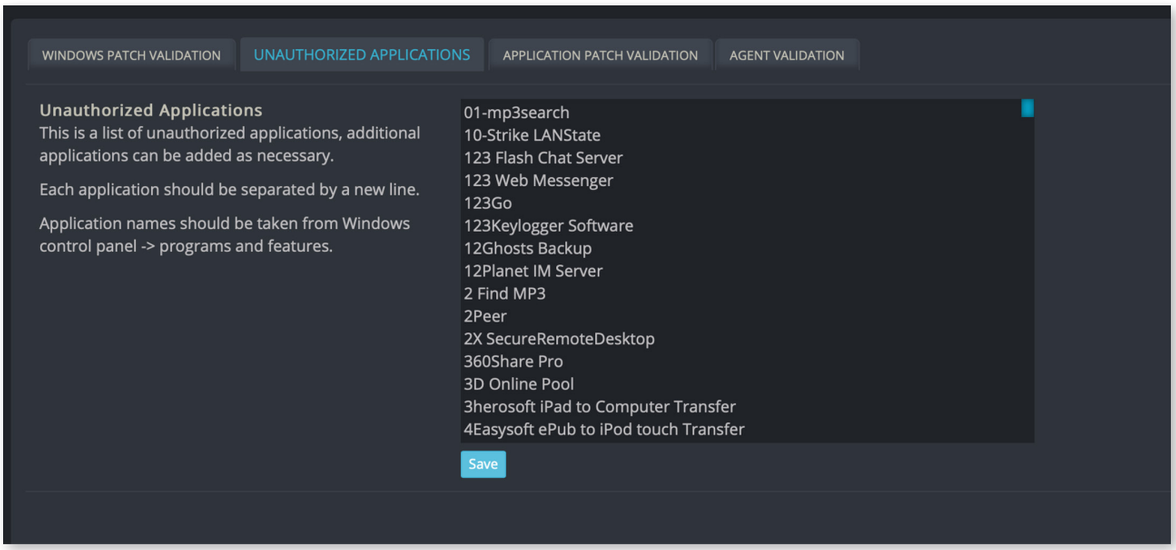
Cynet rich forensic data can be used to investigate and respond to indicators of unlawful, unauthorized, suspicious, or unusual activity across the environment as required in **AU 3.051**. Cynet Automated Response capabilities can instantly implement remediation actions in response to identifying critical indicators of fraud and/or organizationally defined suspicious activity, as defined in **AU 4.053.**



Example of Cynet Alerts screen with detailed information regarding the threat

Configuration Management (CM)

Blacklisting and whitelisting is supported in the Cynet platform to block or allow access to data, applications or ports based on predefined lists. Blacklists blocks access while whitelists block anything that isn't approved for access. Cynet blacklisting and whitelisting capabilities support **CM 3.069** and **CM 4.073** requirements.



Sample menu for configuring unauthorized applications in Cynet platform settings

Incident Response (IR)

Cynet provides supplemental support for practice requirements **IR 2.092** and **IR 2.093** by collecting and analyzing all cybersecurity events from Cynet attack protection technologies: NGAV, EDR, UEBA Rules, NDR and Deception, and providing notifications to assigned personnel.

Cynet correlation rules provide alerting on cybersecurity events while automated investigations, reports, and forensics provide evidence behind cybersecurity events, supporting practice **IR 2.094.**

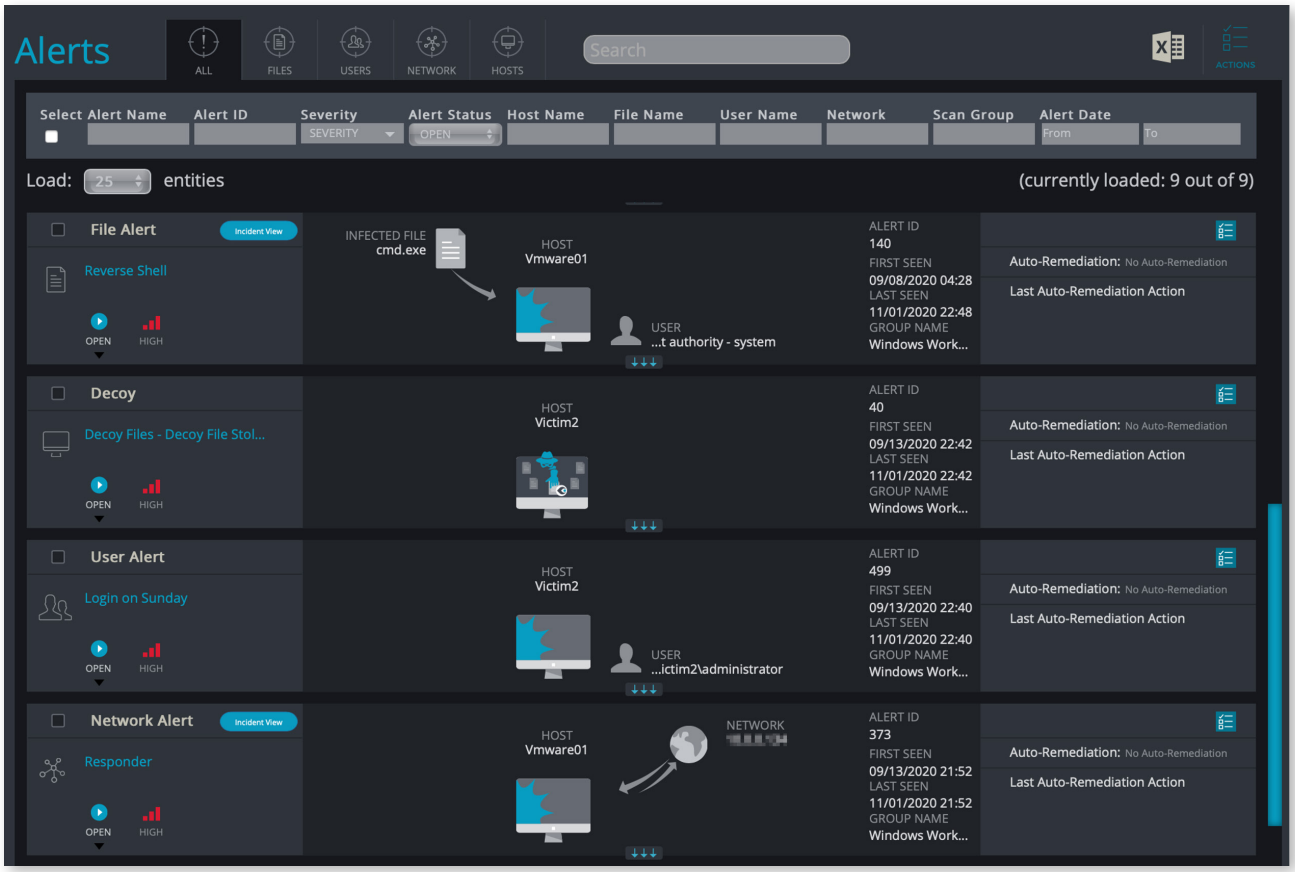
Cynet natively provides incident response tools for cross-environment remediation: infected hosts, compromised user accounts, malicious processes and attacker-controlled network traffic. Cynet provides an extensive set of remediation tools which can be implemented manually, or automatically triggered based on the organization's preferences to help clients meet the requirement of **IR 2.096.**

Cynet's extensive forensic tools assist clients with determining the root cause of an event. Further, the Cynet Incident Engine automatically launches a full investigation following certain high risk events to determine the root cause and scope of an attack. These capabilities support the requirements of **IR 2.097** and **IR 5.102.**

Example Incident View showing full investigation and remediation workflow

System and Information Integrity (SI)

Cynet provides direct support of practice **SI 2.214** and **SI 2.216** by providing continuous monitoring, analysis, and reporting of network, physical access and other events indicative of malicious cyber activities. Periodic and real-time scans of files from external sources can be performed to support practice **SI 1.213.** Cynet 360 AutoXDR prevents and detects threats using the combined power of NGAV, EDR, NDR, UEBA Rules and Deception technologies that monitor individuals and system behaviors for malicious code and anomalous behaviors as required in **SI 1.211, SI 5.222** and **SI 5.223**. Threat indicators derived from the client organization, third party sources and other Cynet clients are used to continuously update Cynet's defenses and inform threat hunting activities as required in practices **SI 1.212** and **SI 4.221.**



Cynet Alert view showing a sample of alerts across files, decoys, users and network

Conclusion

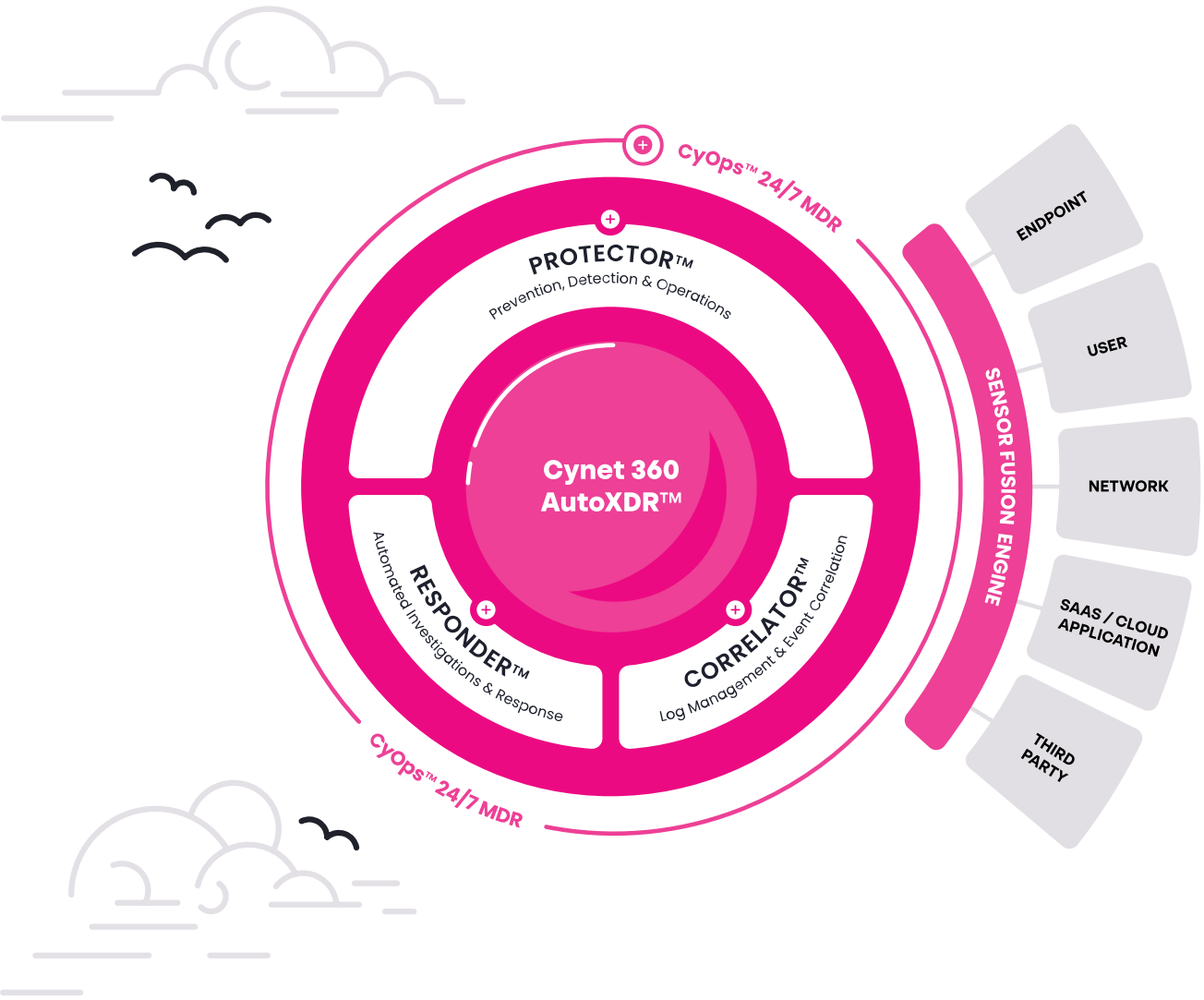
Beyond compliance with CMMC requirements, Cynet 360 AutoXDR provides a single, unified platform to automatically prevent, detect, investigate and fully remediate the broad range of attack vectors faced by DoD suppliers. Visibility across endpoint, network and user activities, plus the power of deception provides the broadest and deepest protection against all threats.

Cynet 360 AutoXDR is the only solution that triggers an automated investigation following each endpoint, user, or network alert, fully disclosing its root cause and scope and applying all the required remediation activities to fully eliminate the threat. Cynet also provides a broad set of automated and highly customizable remediation actions to address threats according to your preferences.

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, SSPM 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

Summary of CMMC practices supported by Cynet

Practice	Description
AC 1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AU 3.045	Review and update logged events.
AU 3.048	Collect audit information (e.g., logs) into one or more central repositories.
AU 3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
AU 4.053	Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.
CM 3.069	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
CM 4.073	Employ application whitelisting and an application vetting process for systems identified by the organization.
IR 2.092	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
IR 2.093	Detect and report events.
IR 2.094	Analyze and triage events to support event resolution and incident declaration.
IR 2.096	Develop and implement responses to declared incidents according to pre-defined procedures.
IR 2.097	Perform root cause analysis on incidents to determine underlying causes.
IR 5.102	Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.
SI 1.211	Provide protection from malicious code at appropriate locations within organizational information systems.
SI 1.212	Update malicious code protection mechanisms when new releases are available.
SI 1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
SI 2.214	Monitor system security alerts and advisories and take action in response.
SI 2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
SI 4.221	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.
SI 5.222	Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.
SI 5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.