Cynet

CYNET 360 PLATFORM SUPPORT FOR HIPAA REQUIREMENTS

EXECUTIVE SUMMARY

HIPAA provides requirements and guidelines for maintaining the security and privacy of individually identifiable health information, and the Cynet 360 platform collects activity data and provides protection against threats to the implementing organization.

Some of the specifications in HIPAA are policy/process requirements are entirely the implementing organization's responsibility, while others apply to a technology platform that handles or interacts with any personally identifiable information. The features available in the Cynet 360 Platform can be utilized by the implementing organization to partially or fully satisfy the specifications in the requirement.

Cynet 360 platform provides HIPAA compliance in the following groups:

Risk Management

Vulnerability assessment and ranking, as well as proactive risk scoring for hosts, user accounts, executed files and network domains/sockets.

Protection from Malicious Software

Multilayered endpoint protection: signature-based Antivirus + Next-Gen Antivirus that includes AI-based static analysis, behavioral analysis, memory monitoring and comprehensive threat intelligence feeds.

Log-in Monitoring

Monitoring of all attempted logins.

Integrity

Enforcement of File Integrity Monitoring (FIM) policy.

Response and Reporting

Array of attack detection technologies: EDR, Network Analytics, User Behavior Analytics (UBA) and Deception.

Audit Controls

Collection of all activity logs across the environment: host, account logins, data access, Windows events and firewall/proxy logs.

Notification

Supplemental support via Cynet 360, detailed threat prevention/detection and alert reporting.

HIPAA REQUIREMENTS

HIPAA Requirement	Testing Requirements	Comments
§ 164.306 (A)	Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.	• The Cynet 360 Platform provides detection, prevention, monitoring, and search capabilities to defend against sophisticated threats and adversaries. • The Cynet agent on each endpoint autonomously prevents and detects threats targeting users, the network, files and hosts. • The Cynet server correlates events and activities across the protected environment to detect malicious presence and activities. • The Cynet 360 platform provides anti-virus capabilities for protection against known threats. • The Cynet 360 Platform uses machine learning-based predictive models to prevent unknown malware (a.k.a. 'zero day').
§ 164.308 (a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	• Cynet 360 platform provides vulnerability assessment and ranking capabilities. • Cynet 360 platform assigns a risk score to any host, user account, executed file and network domain/socket in order to proactively identify risk and reduce the attack surface.
§ 164.308 (a)(5)(ii)(B)	Procedures to guard against malicious software host/network IPS, unified threat management, network anomaly detection, patch management, firmware management, host/network IDS, OS access controls (least-privileged user), content filtering.	• The Cynet 360 platform provides Network Analytics to detect anomalies in network traffic. • The Cynet 360 agent applies strict whitelisting to processes requesting access to critical OS resources. • The Cynet 360 platform employs a User Behavior Analytics (UBA) technology alerting upon any anomalous login activity.

HIPAA Requirement	Testing Requirements	Comments
§ 164.308 (a)(5)(ii)(C)	Implement procedures for monitoring log-in attempts and reporting discrepancies.	• The Cynet 360 agent continuously gathers event data (primarily focused on process execution) for the host and transfers it to the Cynet Server. • Log-in attempts can be inferred by associating the logged in users with process executions.
§ 164.308 (a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	• Cynet 360 EDR provides detailed information on detected activity, matched patterns, impacted hosts, severity level, and resolution status. • Cynet 360 UI provides search capabilities to identify and collect relevant information during an investigation and to track incidents. • Cynet 360 provides capabilities to block threats based on specific thresholds, hashes, IP addresses, and other Indicators of Compromise (IOC).
§ 164.312 (b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	• The Cynet 360 agent continuously gathers event data (process execution, user account logins, network traffic and user-defined Windows events) for the host and transfers it to Cynet server. Additionally, the Cynet server ingests firewall/proxy logs. • The collected data is available for review via the Cynet UI. Which provides capabilities to execute custom queries to examine collected activities.
§ 164.312 (c)(1)	Policies and procedures to safeguard PHI unauthorized alteration.	• Cynet 360 supports enforcement of File Integrity Monitoring policies based on user definitions.
§ 164.316 (b)(2)(i, ii)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	• Cynet 360 retains authentication, file access, network, security and incident breach notification logs for an unlimited period of time. • Cynet makes documentation of these logs available to any individuals per the organization's choice.

HIPAA Requirement	Testing Requirements	Comments
§ 164.404 (b)	(1) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Cynet 360 supplements this requirement with the following capabilities: • Cynet 360 has the capability to detect known and new attacks. • Cynet 360 UI provides capabilities to identify, investigate, and track incidents. • Cynet 360 enables the organization to identify the source, the method, and the scope of the breach in a timely manner.