How Cynet 360 Can Help Your Organization Be HIPAA Compliant

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law which was passed in 1996. It provides regulations and guidelines for maintaining the security and privacy of protected health information (PHI). The standards within the law require organizations with PHI to ensure that physical, network, and process security measures are implemented.

Cynet 360 is a comprehensive security platform that was designed to provide organizations with the necessary means to protect their environment from modern security threats and attacks. Because Cynet 360 is a security platform, it is able to be extremely versatile and beneficial to organizations striving to be HIPAA compliant. Cynet 360 provides malware prevention capabilities, incident response and remediation, automated risk calculation, visibility throughout the environment, the ability to report on all of these, and more.

The following mapping summary explains the HIPAA standard requirements, and how Cynet 360 can help with each standard requirement and make your organization HIPAA compliant:

HIPAA Standard	Standard Description	How Cynet 360 Addresses Standard Requirements
164.306(a)	• Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. • Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. • Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. • Ensure compliance with this subpart by its workforce.	Cynet 360 addresses these general HIPAA requirements through multiple feature sets. It can protect information systems within the corporate network from today's modern threats and attacks. It can provide data integrity by ensuring one of these advanced threats, Ransomware, does not improperly alter or destroy PHI data.
164.308(a)(1)(ii)(A)	**Risk Analysis**: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Cynet 360 can help organizations identify potential risks in the environment through its risk level calculations for every monitored object (files, users, hosts, and network traffic). Risk levels are calculated through the analysis of behavioral indicators collected from the information systems in the environment.

HIPAA Standard	Standard Description	How Cynet 360 Addresses Standard Requirements
164.308(a)(1)(ii)(B)	**Risk Management**: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).	Cynet 360 can help organizations reduce security risks by providing (A) Visibility of high risk objects in the environment, determined through automated behavioral analysis (B) Prevention and remediation capabilities for threats (C) Reporting of all security risks (D) A comprehensive security platform which can be integrated with other security systems to protect information systems.
164.308(a)(1)(ii)(D)	**Information System Activity Review**: Implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports.	Cynet 360 can contribute to organizations' access control and review procedures by providing the ability to review security activity within the environment. This includes auditing of user access and reporting on advanced security threat detections.
164.308(a)(5)(ii)(B)	**Protection from Malicious Software**: Implement procedures for guarding, detecting, and reporting malicious software.	Cynet 360 provides protection for organizations by providing detection, prevention, and reporting of malicious software within the environment.
164.308(a)(5)(ii)(C)	**Login Monitoring**: Implement procedures for monitoring login attempts and reporting discrepancies.	Cynet 360 can monitor login attempts on information systems and can provide user behavior analysis based on login behavior. Alerting and reporting capabilities can be used to examine discrepancies or anomalous behavior.
164.308(a)(5)(ii)(D)	**Password Management:** Implement procedures for creating, changing, and safeguarding passwords.	Cynet 360 can help organizations monitor and report on the password age of user login accounts.
164.308(a)(6)(ii)	**Response & Reporting**: 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 provides security teams the capabilities to effectively respond to a security incident by providing several remediation capabilities to mitigate advanced threats. Automated response capabilities empower security teams to effectively mitigate threats rather than allowing them to dwell. Forensic reporting capabilities provide security teams the ability to document incidents and the responses taken.

HIPAA Standard	Standard Description	How Cynet 360 Addresses Standard Requirements
164.312(b)	**Audit Controls**: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Cynet 360 is able to record user activity on systems which may contain protected health information and provide IT and Security professionals the ability to examine all recorded activity. Cynet 360 can also collect and retain logs from various systems in the environment regarding audit logging.
164.312(c)(1)	**Data Integrity:** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Cynet 360 is able to protect organizations from improper alteration or destruction of PHI data through its detection and prevention of advanced threats such as Ransomware. Through Cynet's Ransomware Heuristic Detection capabilities, new and old variants of Ransomware can be stopped before any data is encrypted or altered.
164.312(e)(2)(i)	**Integrity Controls:** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection, until disposed of.	
164.316(b)(2)(i)	**Time Limit:** 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 was in effect, whichever is later.	According to most HIPAA interpretations, it is mandatory to retain audit logs for a period of 6-years. Cynet 360 is able to collect and retain audit logs from the environment as specified in 164.213(b). In addition to this, Cynet 360 is able to retain these logs for any given period of time.