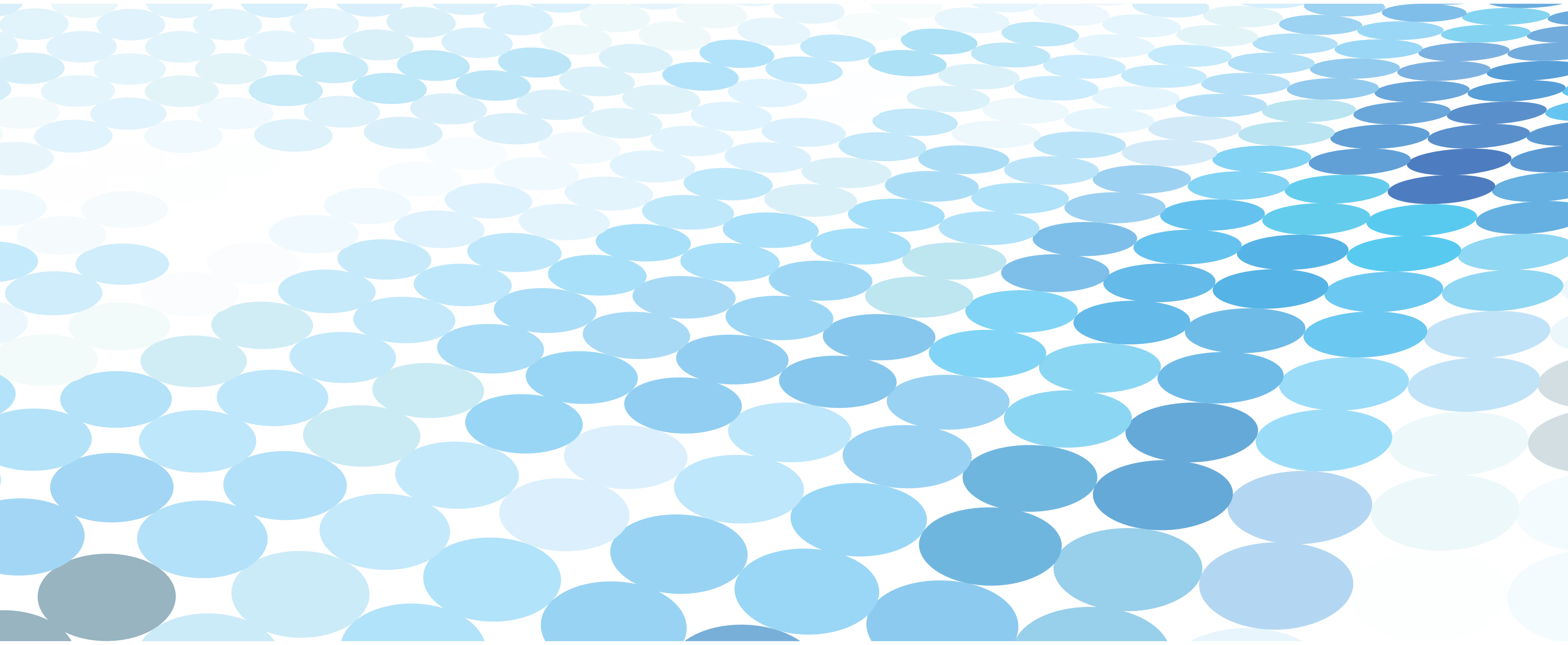
Carbon Black.



Carbon Black for Compliance

HIPAA Mapping Summary

Section	Standard	Implementation Specification
		R = Required
		A = Addressable
			How Carbon Black Helps

		Administrative Safeguards	
164.308(a)(1)	Security Management Process	Risk Analysis (R)	**Carbon Black File Analysis and Vulnerability Management Solution** Carbon Black Protection can assign trust and threat ratings for all software in your environment giving you a real-time feed of new and existing file reputations in order to filter out compelling data. Views can be filtered on risk weight or any other metric contained within Carbon Black Threat Intel such as prevalence, key vulnerability, publisher, threat, trust and more. Cb Protection will be able to build a trust base around any desired threat level, therefore eliminating the risk posed by those potential vulnerabilities by simply blocking them from execution if the risk is deemed too high.
		Risk Management (R)	**Cb Protection File Analysis and Vulnerability Management** Cb Protection allows enterprises to set trusted software rules and proactively block the execution of any software that is not preapproved to run. Cb Protection there is no scanning, no signatures updates, and no intermittent risk assessment around patching. Untrusted software is continuously blocked without the burden of keeping signature files up to date. Cb Protection also provides real-time file monitoring to protect your critical configuration files from unauthorized change while allowing companies to view their risk exposure at any time.
		Sanction Policy (R)	With the control that Cb Protection introduces to at the application level, sanctions in the way of higher enforcement and unapproved software can be imposed on any sector of the workforce if it's deemed that they have failed to comply with the security policies and procedures.

		Information System Activity Review (R)	Cb Protection provides a real time inventory of all file assets installed on an endpoint; users can centrally identify the presence or absence of vendor-supplied security patches. This real time business intelligence allows the review of event activity in numerous perspectives, such as: • Track and automatically reconcile and validate changes against enterprise change management system requests. • Maintain archive version of configuration files for easy rollback. • Track changes to all systems and software and automatically reconcile with approved change requests. • Track changes by users to provide evidence of separation of duties across environments.
164.308(a)(3)	Workforce Security	Authorization and/or Supervision (A)	Cb Protection centrally managed policies automatically identify trusted software in your enterprise and prevent anything else from running.
		Workforce Clearance Procedure (A)	IT and cloud driven approvals with trust policies for software "pushed" to end-users. These dynamic policies are aligned with IT-confirmed trusted sources, such as software publishers, internal software repositories, software delivery and patch- management solutions. This allows trusted software to run with minimal or no administrative effort.
		Termination Procedure (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
164.308(a)(4)	Information Access Management	Isolating Healthcare Clearinghouse Functions (R)	N/A — must be done in a manual fashion as it pertains to business manual functions within the organization.
		Access Authorization (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.

		Access Establishment and Modification (A)	**Cb Protection Access and Modification Control** Cb Protection helps organizations ensure that only trusted applications and devices are allowed to run on their devices. IT can set controls to ban portable storage devices from reading, writing and executing—even down to a specific serial number, preventing accidental or malicious information leakage. In addition, Cb Protection's device control policies and trusted software lists ensure that only authorized personnel are allowed to copy data to portable storage devices, which controls the distribution, storage, accessibility, and portability of confidential information.
164.308(a)(5)	Security Awareness and Training	Security Reminders (A)	**Cb Protection Policy Awareness and Enforcement** Cb Protection notification controls and customizable notification messages are delivered to end users when attempting to contravene security policy. This will both enforce policy and educate users on policy guidelines.
		Protection from Malicious Software (A)	**Cb Protection Enterprise Application Control and Trust-Based Detection** Cb Protection detects and stops advanced threats and malware that evade traditional security solutions. This approach combines three key technologies: a real-time sensor that monitors and records all activity on every server, endpoint, and fixed-function device; policy-driven application control and whitelisting that enables organizations to specify the software they trust and automatically prevent everything else from executing; and the largest cloud-driven software reputation service that provides trust ratings for the world's software. This combination gives organizations immediate visibility into the software running in their enterprises; real-time detection and protection against cyber threats; and the richest set of forensics information for incident response. The Carbon Black Security Platform provides you with a set of Advanced Threat Indicators (ATI) that look for (potential) threats within servers and endpoints. ATIs are based on advanced indicators of compromise that look at not only static, but also real-time and time-based event information to identify suspicious files and activities. Carbon Black Enterprise Response is uniquely able to identify threats before they are able to compromise your environment, as well as those that may be in progress or those that may have run in the past.

		Log-in Monitoring (A)	**Cb Protection Policy Awareness and Enforcement** Cb Protection notification controls and customizable notification messages are delivered to end users when attempting to contravene security policy. This will both enforce policy and educate users on policy guidelines.
		Password Management (A)	**Cb Protection Policy Awareness and Enforcement** Cb Protection notification controls and customizable notification messages are delivered to end users when attempting to contravene security policy. This will both enforce policy and educate users on policy guidelines.
164.308(a)(6)	Security Incident Procedures	Response and Reporting (R)	**Cb Protection security events and Incident Reporting** Real-time software tracking enables comparisons against approved configurations to visually identify users or systems that are high risk, out of compliance, or are likely to generate frequent support calls. Both drift against baselines and forensic audit reporting is available to dissect the full spectrum of any event.
164.308(a)(7)	Contingency Plan	Data Backup Plan (R)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
		Disaster Recovery Plan (R)	**Cb Protection Policy Awareness and Enforcement** Cb Protection notification controls and customizable notification messages are delivered to end users to facilitate the distribution of the Disaster Recovery Plan and security policy. This will both enforce policy and educate users on policy guidelines.
		Emergency Mode Operation Plan (R)	**Cb Protection Policy Awareness and Enforcement** Cb Protection notification controls and customizable notification messages are delivered to end users to facilitate the distribution of the Emergency Mode Operation Plan and security policy. This will both enforce policy and educate users on policy guidelines.

164.308(a)(8)	Evaluation		**Cb Protection Policy Assessment and Validation** Cb Protection has solutions and services that can help assess the compliance stance for HIPAA and or can assist in providing pre-compliance information to and external evaluator or independent assessor.
164.308(b)(1)	Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement (R)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
		Physical Safeguards	
164.310(a)(1)	Facility Access Controls	Contingency Operations (A)	This is a physical access security control. **Cb Protection Security Policy Awareness and Enforcement** The enforcement mechanism can be used to ensure the consumption of the policy around the control and audit the successful dissemination of the plan to the stakeholders.
		Access Control and Validation Procedures	**Carbon Black Device and File Asset Control** Carbon Black lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
164.310(b)	Workstation Use	(A)	**Cb Protection File Integrity Control** Cb Protection's continuous, real-time file monitoring protects your critical configuration files from unauthorized change to meet file integrity monitoring and audit trail rules. Cb Protection blocks unauthorized activities, and ensures that only authorized processes can write to log data files. **Cb Protection Policy Enforcement and Thresholds** Cb Protection's centrally managed policies automatically identify trusted software in your enterprise and prevent anything else from running. Policies can be set for individuals or groups and approval thresholds established in order to ensure compliance across workstations.

164.310(c)	Workstation Security	(R)	Control user and machine rights and machine access **Cb Protection Policy Enforcement and Thresholds** Cb Protection helps organizations ensure that only trusted applications and devices are allowed to run on their workstation devices. IT can set controls to ban portable storage devices from reading, writing and executing—even down to a specific serial number, preventing accidental or malicious information leakage. In addition, Cb Protection's device control policies and trusted software lists ensure that only authorized personnel are allowed to copy data to portable storage devices, which controls the distribution, storage, accessibility, and portability of confidential information.
164.310(d)(1)	Device and Media Controls	Disposal (R)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
		Media Reuse (R)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
		Accountability (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
		Data Backup and Storage (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.

Technical Safeguards

164.312(a)(1)	Access Control	Unique User Identification (R)	**Cb Protection Policy Enforcement and Thresholds** Cb Protection can inherit user privileges and set policies and enforcement levels based on existing MS Active Directory and other directory servers. This allows synchronization between organizational standards for user identification and controls user approvals based on policies.
164.312(b)	Audit Controls		**Cb Protection Asset Monitoring and File Analysis** Cb Protection can assigns trust and threat ratings for all software in your environment giving you a real-time feed of new and existing file reputations in order to filter out compelling data. Views can be filtered on risk weight or any other metric contained within Cb Threat Intel such as prevalence, key vulnerability, publisher, threat, trust and more. The ability to assign trust ratings to the file inventory aligns with the required audit controls to apply ranks and measure to any possible or known vulnerability. This ensures a more concise pre-compliance audit process. Cb Protection will be able to build a trust base around any desired threat level, therefore eliminating the risk posed by those potential vulnerabilities by simply blocking them from execution if the deemed risk is too high. This is particularly important since remediation of any discovered or known vulnerabilities is a required audit control.
164.312(c)(1)	Integrity	Mechanism to Authenticate Electronic Protected Health Information (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
164.312(d)	Person or Entity Authentication		**Cb Protection Policy Enforcement and Thresholds** Cb Protection can inherit user privileges and set policies and enforcement levels based on existing MS Active Directory and other directory servers. This allows synchronization between organizational standards for user identification and controls user approvals based on policies.

164.312(e)(1)	Transmission Security	Integrity Controls (A)	**Cb Protection File Integrity Control** Cb Protection's continuous, real-time file monitoring protects your critical configuration files from unauthorized change to meet file integrity monitoring and audit trail rules. Cb Protection blocks unauthorized user and process activities, and it ensures that only authorized processes can write or access authorized files.
		Encryption (A)	**Cb Protection Device and File Asset Control** Cb Protection lets you enforce read, write and execute policies for both data and software on USB keys and other such removable media. Devices can be banned or approved by specific device type or by specific device by serial number. This allows full control and audit on all events related to the movement and use of data throughout the enterprise.
Policies and Procedure and Documentation Requirements			
164.316(a)	Policies and Procedures		**Cb Protection Security Policy Awareness and Enforcement** Cb Protection can assist the enterprise by facilitating and automating much of the policies and procedures associated with HIPAA Compliance. Cb Protection can step outside of the standard functional specifications and assist the organization with distributing and colleting everything required to ensure and enforce the adherence to security policies, but also put mechanisms in place to both inform and educate the end user community on those establish policies. By adding visibility and control through policy to the endpoints, Cb Protection's templates will ensure that the end users are directed at both acknowledging and reviewing the corporate security and compliance policy, but also provide the audit measure and data that the policy has been consumed. By utilizing the Cb Protection notification window and education templates, users across the organization can be informed and directed to the appropriate security awareness tutorials. These awareness templates can be presented within the notification window upon login to the corporate assets, or can be automatically re-directed to Cb Protection's Security Awareness training templates appropriate and catered to the enterprise.

Carbon Black.