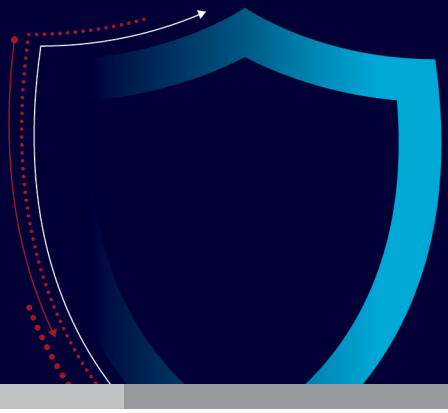
WHITE PAPER

Carbon Black. by Broadcom

Carbon Black® App Control

PCI DSS 4.0 Mapping



Compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements helps organizations ensure data security. The following table examines how Carbon Black® App Control maps to specific PCI DSS requirements.

PCI DSS Requirement		How Carbon Black App Control Helps
2.2.4	Only necessary services, protocols, daemons and functions are enabled, and all unnecessary functionality is removed or disabled.	The App Control policy-driven security approach enforces this on all desired endpoints, only allowing approved software to execute. This ensures only approved services and software are allowed to run, according to the policy established for each endpoint.
2.2.5	If any insecure services, protocols or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols or daemons.	App Control catalogs all software in the environment and can help document the software present on each system.
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per requirement 5.2.3 that concludes the system components are not at risk from malware.	App Control is a direct control for this requirement, enabling customers to remove traditional antivirus without the need to undergo the compensating control process.
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks or contains all known types of malware.	App Control offers a unique solution to protect your system from malware. In addition to protecting against just known malware, App Control only allows trusted processes to execute.
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	By the very nature of the App Control solution (a default deny posture), signature packs for known malware are not necessary. However, App Control can provide software reputation that is delivered automatically from the cloud.
5.3.2	The anti-malware solution(s) performs periodic scans and active or realtime scans, or performs continuous behavioral analysis of systems or processes.	App Control can retrieve updated reputations from the cloud, but the default deny security posture does not require the use of reputation.
5.3.3	For removable electronic media, the antimalware solution(s) performs automatic scans of when the media is inserted, connected or logically mounted, or performs continuous behavioral analysis of systems or processes when the media is inserted, connected or logically mounted.	App Control offers device control to prevent removable devices from running in your environment.
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with requirement 10.5.1.	App Control provides event logs that track activity within your environment, exportable in several different formats.
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented and authorized by management on a case-by-case basis for a limited time period.	App Control includes tamper protection, which prevents the product from being disabled without the appropriate permissions.

PCI DSS Requirement		How Carbon Black App Control Helps
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example, operating systems and databases) are covered.	App Control can assist with this requirement by providing a mechanism to map the catalog of software in the environment with the catalog of vulnerable software in the National Vulnerability Database (NVD). This aids with the ability of customers to query for vulnerable software.
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	App Control aids in cataloging custom software by providing an inventory of all the software in an environment.
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • The reason for, and description of, the change. • Documentation of the security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • Testing all updates for bespoke and custom software changes for compliance with requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	App Control can help with tracking and enforcing change in the environment by leveraging its ability to enforce file integrity controls.
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	Change and drift from a baseline file system can be monitored from within App Control. Additionally, file integrity control and/or monitoring features can support this by preventing and tracking change.
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	App Control manages access for users to execute and modify files based on roles and policy. This can be integrated with Active Directory to leverage existing organizational structure and access rules to enforce policy.
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • The least privileges necessary to perform job responsibilities.	App Control can provide access to execute and modify files based on roles and policy.
7.2.3	Required privileges are approved by authorized personnel.	App Control provides role-based access controls to limit the ability to assign privileges to other users to execute and modify files.
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications or processes that specifically require their use.	Leveraging App Control, only users with the appropriate security policy can run applications that are assigned to them or that business group.
7.3.x	Access to system components and data is managed via an access control system(s).	Access to business processes (applications) can be defined and controlled by App Control.
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	App Control can be configured to allow data to be written to only specific removable devices.
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.	App Control can maintain an event log of all writes to external devices.
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	App Control can collect execution of applications within the environment and send that data to external logging tools.

PCI DSS Requirement		How Carbon Black App Control Helps
10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource or service (for example, name and protocol).	App Control logs required data to identify attempts to access/launch components within the environment.
10.3.1	Read access to audit log files is limited to those with a job-related need.	App Control controls access to these events within the product using role-based access control (RBAC).
10.3.2	Audit log files are protected to prevent modifications by individuals.	App Control encrypts logs.
10.3.4	File integrity monitoring (FIM) or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	App Control can be used to meet this requirement but can also be configured to prevent audit logs from being changed except by specific processes.
10.7.1	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • Intrusion detection systems/intrusion prevention systems (IDS/IPS). • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	App Control can alert when systems covering anti-malware and FIM are out of policy.
11.3.1	Internal vulnerability scans are performed as follows: • Scans are performed at least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • The scan tool is kept up to date with the latest vulnerability information. • Scans are performed by qualified personnel, and organizational independence of the tester exists.	App Control can assist with this requirement by providing a mechanism to map the catalog of software in the environment with the catalog of vulnerable software in the NVD. This aids with the ability of customers to query for vulnerable software.
11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	App Control can assist by allowing customers to block vulnerable software from executing and deleting that software.
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions and deletions) of critical files. • To perform critical file comparisons at least once weekly.	App Control can be used for file integrity monitoring/file integrity control requirements, and to track drift within an environment.

For more information, visit the Carbon Black App Control product page.