DATASHEET

NIST Special Publication 800-53

Security and Privacy Controls for Federal Information Systems and Organizations Mapping for Carbon Black

BACKGROUND

The National Institute of Standards and Technology (NIST) released its fourth revision of the Security and Privacy Controls publication as of January 22nd, 2015. NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to establish a unified information security framework for the federal government and related organizations. In this document the mapping between the family class grouping of NIST specifications and the Carbon Black Security Platform shows how the compliance and security objectives are met for a federal security framework.

NIST PUBLICATION: MANAGING THE RISK TO ORGANIZATIONAL MISSIONS/BUSINESS FUNCTIONS

"The security controls in NIST Special Publication 800-53 are designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Compliance is not about adhering to static checklists or generating unnecessary FISMA reporting paperwork. Rather, compliance necessitates organizations executing due diligence with regard to information security and risk management. Information security due diligence includes using all appropriate information as part of an organization-wide risk management program to effectively use the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in organizational security plans meet the mission and business requirements of organizations. Using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation. Employing effective risk-based processes, procedures, and technologies will help ensure that all federal information systems and organizations have the necessary resilience to support ongoing federal responsibilities, critical infrastructure applications, and continuity of government." More information.

INTRODUCTION

Carbon Black has created this publication for those companies utilizing, or looking to utilize, the NIST 800-53 framework. The table below walks through each class as it pertains to our product offerings and provides evidence of how we can solve your compliance needs with real-time seamless reporting and audit capabilities. Carbon Black gives you these essential controls while helping you maintain operational effectiveness and compliance. Carbon Black Enterprise Protection, our always-on real-time vulnerability and threat analysis solution ensures policy enforcement by only allowing approved and compliant processes to run in your environment. Carbon Black Enterprise Response, our incident response solution, allows you to trace the entire timeline of an event and take key remediation steps within a fraction of the time of typical forensics and imaging software. You can now detect, respond, and act instantly to any threats and malicious activity. These capabilities not only ensure compliance and IT audit controls but provide greater security and a proactive approach to preventing advanced threats and responding in real time. The below table is a guide to each NIST control and the related Carbon Black offering.

Carbon Black.

FAMILY	IDENTIFIER	CARBON BLACK SECURITY PLATFORM MAPPING
Access Control	**AC – 4** Information Flow Enforcement **AC – 17** Remote Access **AC – 19** Access Control for Remote Devices **AC – 21** Information Sharing **AC – 23** Data mining Protection **AC – 25** Reference Monitor	High enforcement policies that create bans on any unauthorized access to sensitive information based on user access policy. When users log into a system running Cb Protection, they are restricted by policy to run only preapproved applications. All other applications are restricted from use, based on policy and the user's need to know. Application accounts are monitored in the Cb Protection console along with user information and associated IP addresses. Privileged accesses can be monitored by trust policy implemented from mapping rules to AD. The Cb Protection connector allows for you to integrate into next-gen firewalls and other networking solutions. Also built in are device visibility/control capabilities like remote devices, which provide business solutions that comply with network controls. Cb Protection also integrates with the leading network security providers such as Check Point, Fidelis, FireEye and Palo Alto Networks.
Awareness and Training	**AT – 1** Security Awareness and Training Policy and Procedures	Companies should prioritize those mission critical roles to the business and its security; identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy via the Cb Protection sensor on in scope systems, and develop organizational planning, training, and awareness programs.
Audit and Accountability	**AU – 1** Audit and Accountability Policy and Procedures **AU – 2** Audit Events **AU – 3** Content of Audit Records **AU – 4** Audit Storage Capacity **AU – 5** Response to Audit Processing Failures **AU – 6** Audit Review, Analysis, and Reporting **AU – 7** Audit Reduction and Report Generation **AU – 8** Time Stamps **AU – 9** Protection of Audit Information **AU – 10** Non-repudiation **AU – 11** Audit Record Retention **AU – 12** Audit Generation **AU – 13** Monitoring for Information Disclosure **AU – 14** Session Audit	Cb Protection provides logging and unauthorized access tracking, giving a complete and detailed audit trail of every event across the security ecosystem. Policy is being enforced on all in scope systems with up-to-date real time reporting and detection alerts. Cb Protection limits the scope for auditing and reporting focus by customizing the content and log maintenance and reporting on what's important for your compliance objectives. Cb Response's visibility, detection and incident response are "always-on", allowing the ability to proactively monitor system and file components and maintain audit trails of associated events. The lightweight sensor continuously monitors and records every endpoint in the enterprise, building and storing audit trails for system and file components. Cb Response's unmatched detection and response capabilities enable users to collect and retain the precise data points that are needed during an investigation including records of execution, file system modifications, registry modifications, network connections, and a copy of every unique binary executed on an enterprise machine. Most importantly, Cb Response's collects and retains the relationship among each of these data types, giving you the power to understand behaviors, not just individual events.

FAMILY	IDENTIFIER	CARBON BLACK SECURITY PLATFORM MAPPING
Certification, Accreditation, and Security Assessments	**CA – 1** Security Assessment and Authorization Policies and Procedures **CA – 2** Security Assessments **CA –7** Continuous Monitoring **CA – 8** Pen Testing **CA – 9** Internal System Connections	Carbon Black Threat Intel, combined with internal IT approvals of established policies, enables organizations to apply real-time, proactive threat and trust measurements to the asset inventory, discover potential risky files and enforce policy-based control on all endpoints. Cb Protection's asset reporting applies threat and trust ratings to every file within the infrastructure, providing immediate low-friction analysis and risk ranking of any potential file vulnerability discovered. You can discover and get alerts on any potentially compelling or suspicious file activity with Cb Protection's advanced threat analysis report as well as its continuous always - on monitoring. Cb Response's visibility and detection, combined with Cb Protection's console alerts will narrow the scope of events when going through a penetration test exercise. You can shorten response time significantly while being able to see the entire timeline of a security event and provide remediation steps. You will also be able to alleviate the number of steps in penetration tests and enhance testing benefits by showing vulnerabilities in real time. With Cb Threat Intel, Cb Response can automate and apply comprehensive threat intelligence from a combination of public, custom, third-party, and proprietary providers. This intelligence, combined with Cb Response's continuously recorded endpoint visibility, reduces alert fatigue, accelerates threat discovery and instantly classifies attacks.
Configuration Management	**CM – 1** Configuration Management Policy and Procedures **CM – 2** Baseline Configuration **CM – 3** Configuration Change Control **CM – 4** Security Impact Analysis **CM – 5** Access Restrictions for Change **CM – 6** Configuration Settings **CM – 7** Least Functionality **CM – 8** Information System Component Inventory **CM – 10** Software Usage Restrictions **CM – 11** User-Installed Software	Cb Protection detects advanced threats in real time without signatures, while providing visibility into what's running on every endpoint and server. Cb Enterprise Protection can enforce the enterprise trust policy on all endpoints and reduce scope by controlling and blocking unauthorized change, as well as by monitoring and detecting anomalies and compelling events as they happen to ensure the desired endpoint configuration is kept in check. Security compliance checks include verification of the relevant baseline configuration. Cb Response's threat intelligence and capabilities can assist in keeping endpoint configurations in check by finding vulnerable applications in the enterprise. Cb Response is "always on," and can tell you if the vulnerable application has ever been seen, when it was last seen, and on which computers. Cb Response can also create an alert whenever a vulnerable application is executed within the environment. This makes it easy to identify the existence of any vulnerable application, without scanning, providing a much greater detection rate in a shorter amount of time. Cb Response's alerting features ensure real time notice the instant the enterprise becomes vulnerable or drifts outside of the system configurations. Cb Response utilizes feeds from US CERT's National Vulnerability Database, providing intelligence on and checking the current list of vulnerable software by CVE to identify and track the presence of vulnerable applications within the enterprise.
Identification and Authentication	**IA-3** Device Identification and Authentication	The Cb Protection agent, once deployed, crawls through your system devices, systems, files, and processes at the hash level, providing visibility on where your critical assets reside and to what changes is occurring. Cb Protection only allows those devices to run that are approved by your trust policy. Unauthorized devices will be banned from extracting and modifying data.

FAMILY	IDENTIFIER	CARBON BLACK SECURITY PLATFORM MAPPING
Incident Response	**IR – 1** Incident Response Policy and Procedures **IR – 4** Incident Handling **IR – 5** Incident Monitoring **IR – 6** Incident Reporting **IR – 7** Incident Response Assistance **IR – 9** Information Spillage Response	Cb Response's threat protection is always-on, allowing it to actively monitor system and file components, and maintain audit trails of associated events. The lightweight sensor continuously monitors and records every endpoint in the enterprise, and storing audit trails for system and file components. Cb Response provides the ability to "rewind the tape" to view the full spectrum of an event. Since Cb Response is always recording, even if the indicator of compromise (IOC), anomaly, or suspicious activity has long since passed, Cb Response will provide all the related activity to immediately determine what process caused the activity, and any other activity it performed. With Cb Response's dashboards, security teams now gain instant insight into key endpoint and incident response performance indicators across their entire environment. This enables organizations to understand and articulate the state of their endpoint detection and response capabilities. With Cb Response's endpoint isolation and live response, responders can immediately disrupt active intrusions by isolating one or multiple endpoints from the network, perform remote live investigations, terminate ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to both observe and "touch" endpoints to take immediate action during an investigation—even while the endpoint remains isolated from the rest of the network.
Maintenance	**MA – 1** System Maintenance Policy and Procedures **MA – 2** Controlled Maintenance **MA – 3** Maintenance Tools **MA – 4** Nonlocal Maintenance **MA – 6** Timely Maintenance	Cb Protection's version control and application control policies inform customers of all the incidents of software running on their endpoints and servers, along with the vulnerabilities and trust ratings of each version. Cb Response can function very similar to a patch management solution, providing immediate intelligence on how many systems have successfully been updated and which are still pending. Cb Response can quickly identify computers that are not up to date with the patch policy. A standard feature within Cb Response is to record and retain critical data, identifying precisely what happened and where. The utilizing of a Cb Response watch list for vulnerable or dated applications allows for identification and notification once they appear within the network.
Media Protection	**MP-1** Media Protection Policy and Procedures **MP-2** Media Access	Cb Protection's device control and policy settings can enforce and monitor access to systems and restrict access to portable storage devices that could potentially store sensitive information. Cb Protection's device control policies ensure that only authorized staff is allowed to copy sensitive data to portable storage devices.
Risk Assessment	**RA – 1** Risk Assessment Policy and Procedures **RA – 3** Risk Assessment **RA – 5** Vulnerability Scanning	Cb Threat Intel, combined with internal IT approvals of established policies, enables organizations to apply real time, proactive threatand trust/reputation measurements to the asset inventory to discover potential risky files and enforce policy based control on all endpoints. Using real-time vulnerability rankings and threat intelligence informs your IT Administration with up-to-date risk rankings of all files and system components.

FAMILY	IDENTIFIER	CARBON BLACK SECURITY PLATFORM MAPPING
System and Services Acquisition	**SA – 3** System Development Life Cycle **SA – 4** Acquisition Process **SA – 5** Information System Documentation **SA – 8** Security Engineering Principles **SA – 12** Supply Chain Protection **SA – 13** Trustworthiness **SA – 14** Criticality Analysis **SA – 18** Tamper Resistance and Detection **SA – 19** Component Authenticity **SA – 22** Unsupported System Components	Cb Protection controls the execution of software and ensures that systems are prevented from drifting from their desired state. Software and configuration drift can be closely monitored within the Cb Protection console so you can measure any compliance risk at any time. Cb Protection tracks changes to system configurations as well as the removal of applications, utilities and drivers. It also bans outdated components from running based on new trust policy rules. Cb Protection is the only solution that continuously monitors and records all activity on endpoints and servers. While antivirus software can easily be deactivated on client endpoints, Cb Protection cannot be disabled due to the built-in tamper protection. Cb Protection is a compensating control for unsupported system components that have reached end of life and which are no longer supported by patch updates from the publisher.
System and Communications Protection	**SC – 1** System and Communications Protection Policy and Procedures **SC – 3** Security Function Isolation **SC – 4** Information in Shared Resources **SC – 5** Denial of Service Protection **SC – 8** Transmission Confidentiality and Integrity **SC – 28** Protection of Information at Rest **SC – 34** Non-Modifiable Executable Programs	Cb Response's real-time endpoint sensor delivers always on visibility and automates the tedious and time consuming data acquisition process by continuously recording and maintaining the relationships of every critical action on every machine, including a copy of every executed binary, all registry modifications, all file modifications, all file executions, and all network connections. All of these can easily be transferred into meaningful reporting through extraction or using a connector to a SIEM. Cb Response's remediation capabilities allow for a compromised endpoint to be isolated. Alerts can be triggered when compromise or compelling events happen. Restricted functions can protect your data at rest from allowing access or modifications.
System and Information Integrity	**SI – 1** System and Information Integrity Policy and Procedures **SI – 2** Flaw Remediation **SI – 3** Malicious Code Protection **SI – 4** Information System Monitoring **SI – 5** Security Alerts, Advisories, and Directives **SI – 6** Security Function Verification **SI – 7** Software, Firmware, and Information Integrity **SI – 8** Spam Protection **SI – 10** Information Input Validation **SI – 11** Error Handling **SI – 14** Non-Persistence **SI – 15** Information Output Filtering **SI – 16** Memory Protection	Cb Protection achieves information integrity and monitoring controls that are based on policy, and includes discovering file assets across an enterprise, enforcing controls, as well as reporting and auditing to ensure policy compliance. Cb Protection ensures secure configuration of devices using file-integrity and registry controls. Cb Protection sets controls on the ability to read/write/execute software on portable storage devices, preventing information leakage and accidental loss of sensitive, confidential information. Flaw remediation is achieved by your organization's security assessments using Cb Protection's continuous monitoring and Cb Response's incident response capabilities. Cb Response uses a Common Vulnerabilities and Exposures (CVE) database, which can be used to identify and remediate flaws discovered in organizational information systems.

Carbon Black.

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 30 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its newly introduced big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

1100 Winter Street, Waltham, MA 02451 USA P 617.393.7400 F 617.393.7499 www.carbonblack.com