Carbon Black.

Aligning with the **Critical Security Controls** to Achieve Quick Security Wins

BACKGROUND

The Council on CyberSecurity's Critical Security Controls for Effective Cyber Defense provide guidance on easy wins for prioritizing security processes that are most effective against the latest advanced threats, such as malware and other malicious targeted attacks. The main emphasis of the controls is on standardization and automation that not only maximize security but enhance the operational effectiveness of your IT Administration. The 20 Critical Security Controls are derived from frameworks such as the National Institute of Standards and Technology (NIST) SP 800-53.

INTRODUCTION

Carbon Black Security Solutions provide essential controls while helping you ensure operational effectiveness and compliance. CB Protection's always-on real-time vulnerability and threat analysis capabilities ensure policy enforcement by only allowing approved and compliant processes to run in your environment. CB Response allows you to trace the entire timeline of an event and take key remediation steps within a fraction of the time typical forensics and imaging software can.

This document will walk you through how the Carbon Black Security Solutions map to 18 of the SANS top 20 critical controls that will allow your organization to continuously maintain a strong security posture.

CONTROL 1:

Inventory of Authorized and Unauthorized Devices

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

The CB Protection agent, once deployed, crawls through your system devices, systems, files, and processes at the hash level, providing real time visibility on where your critical assets reside and to what changes are 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.

CONTROL 1 QUICK WINS

- Deploy an automated asset inventory discovery tool
- Using a Dynamic Host Configuration Protocol with an asset inventory tool
- Monitor an automate new asset inventory

CONTROL 2:

Inventory of Authorized and Unauthorized Software

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

CB Protection is a dynamic application whitelisting solution that applies policy to execution. CB Protection enables enterprises to specify trusted software rules to proactively block the execution of any software that is not pre-approved to run. With CB Protection there is no scanning, no signature updates, and no need to install security patches based on the operating system vendor's schedule. Untrusted software is continuously blocked without the burden of keeping signature files up to date.

CB Protection provides instant visibility into the enterprise exposing what applications are being used on all endpoints and servers as well as what versions are running on which machines. CB Protection has built in File Integrity Monitoring and File Integrity Control. CB Protection provides mappings and templates for file integrity control to enable monitoring and reporting on your Control Policies.

CB Protection has automatic real time assessment of all processes being run in your environment. File Integrity rules are created at the hash level to maintain accuracy of critical files. Once an unauthorized process tries to execute, alerts are generated to notify administration and global bans can be created to eliminate execution across the enterprise. CB Protection provides templates for common rules that help to automate and expedite the process of: identifying asset types; determining what activities to deny by policy; and specifying which users, systems or processes may modify critical files.

CONTROL 2 QUICK WINS

- Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.
- Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
- Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system.

CONTROL 3.

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CB Protection baseline drift reporting can establish a benchmark on your endpoints and servers while visually graphing them in a timeline. CB Protection establishes need-to-run policies based on approved applications and accesses. Using feeds from the Carbon Black Predictive Security Cloud (PSC) you can see the trust level rankings for all versions of software running in your environment. If an outdated version is found, or a vulnerability is identified, a correlated trust level will indicate whether you should update or deny old versions of software.

Change management is achieved by only allowing trusted change to occur. All change is recorded and monitored, and compliance is met with automated reporting on all change modifications. With continuous recording of all changes and policy enforcement built in to only authorize approved change, you no longer have to perform periodic scans and compare images. Any changes will be reported and no untrusted modifications can run.

CONTROL 3 QUICK WINS

- Establish and ensure the use of standard secure configurations of your operating systems.
- Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise.
- Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible.

CONTROL 4.

Continuous Vulnerability Assessment and Remediation

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

CB Protection is an always-on, continuous threat and vulnerability assessment tool. Other scan-based approaches can miss zero day attacks and leave your endpoints and servers vulnerable in the off time between scans. CB PSC provides trust ratings for new and not yet approved software. These ratings give you the ability to build custom detection events, prioritize investigations, and define threat prevention policies.

CB Response shows you a timeline view of all processes and child processes. You no longer have to dig through logs to identify the initiation of an attack. Both products provide instant alerts anytime a rule has been violated or a ban has taken place.

The CB Protection console provides real time vulnerability analysis of all critical machines that the agents are deployed on. Only users with authorized access to the console will be able to see the vulnerability assessments.

The Carbon Black Predictive Security Cloud utilizes feeds from US CERT's National Vulnerability Database that checks the current list of vulnerable software by CVE providing intelligence to help identify and track the presence of vulnerable applications within the enterprise.

CONTROL 4 QUICK WINS

- Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities.
- Correlate event logs with information from vulnerability scans
- Perform vulnerability scanning with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.
- Subscribe to vulnerability intelligence services to stay aware of emerging exposures, and use the information gained to update the organization's vulnerability scanning activities on at least a monthly basis.

CONTROL 5.

Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CB Protection has customizable audit logs of admin logins and associated approved access rules monitoring. Your trust policy can be mapped to Active Directory so only approved admin accounts can manage their
own consoles.

CONTROL 5 QUICK WINS

- Minimize administrative privileges and only use administrative accounts when they are required.
- Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.

CONTROL 6.

Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CB Response 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. This includes copies of every executed binary, all registry modifications, all file modifications, all file executions, and all network connections.

All of these recordings can be easily transferred into meaningful reporting through extraction or using a connector to a SIEM via its RESTful API.

CONTROL 6 QUICK WINS

- Include at least two synchronized time sources (i.e., Network Time Protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent, and are set to UTC (Coordinate Universal Time).
- Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction
- Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals.
- Develop a log retention policy to make sure that the logs are kept for a sufficient period of time.
- Have security personnel and/or system administrators run
biweekly reports that identify anomalies in logs.

CONTROL 8.

Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CB Protection is the only solution that continuously monitors and records all activity on endpoints and servers. Solutions like antivirus software can often be easily deactivated on client endpoints. CB Protection has extensive built-in tamper protection, and is virtually impossible to counteract and disable.

With CB Response you can create custom log reports and alerts for any malware related events. CB Response will show instant visibility into any malware related event providing the entire timeline from start to finish including child processes.

CB Predictive Security Cloud is cloud-based and, when combined with internal IT approvals of established policies, enables organizations to apply real-time, proactive threat and trust/reputation measurements to the asset inventory; discover potential risky files; and enforce policy-based control on all endpoints.

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.

CONTROL 8 QUICK WINS

- Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality.
- Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines.
- Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.
- Limit use of external devices to those that have an approved, documented business need. Monitor for use and attempted use of external devices.

CONTROL 9.

Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CB Protection controls the execution of software and prevents systems from drifting outside of their desired state. Software and configuration drift can be closely monitored within the CB Protection console so you can measure 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 trust policy rules.

CONTROL 9 QUICK WINS

- Ensure that only ports, protocols, and services with validated business needs are running on each system.
- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
- Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization’s approved baseline is discovered, an alert should be generated and reviewed.

CONTROL 11.

Secure Configurations for Network Devices

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CB Protection can track inventory and reporting of all connections made via inbound and outbound traffic on all endpoints and servers, and ban unauthorized network connections made to specified machines and Active Directory groups. With the CB Protection baseline drift reporting you can also manage and track system configurations.

CB Protection prevents unauthorized modification of critical system files and content files while ensuring only authorized processes can write to critical system files and content files. This allows you to filter out and block unauthorized change.

CONTROL 11 QUICK WINS

- Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.

CONTROL 12.

Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

In today’s threat landscape boundaries are becoming blurred between internal and external networks. CB Protection can alert you of unapproved connections while integrating with all your network perimeter devices. This Quick win is based on the multilayer or defense-in-depth strategy for boundary defense.

CONTROL 12 QUICK WINS

- Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists).
- On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

CONTROL 13.

Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CB Protection helps to prevent data exfiltration based on built-in policy, which includes discovering file assets across an enterprise, enforcing controls, reporting and auditing to ensure policy compliance.

CB Protection ensures secure configuration of devices using file integrity and registry controls. CB Protection tests controls on the ability to read/write/execute software on portable storage devices, preventing information leakage and accidental loss of sensitive, confidential information.

CONTROL 13 QUICK WINS

- Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
- Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
- Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.

CONTROL 14.

Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CB Protection offers “default-deny” high enforcement policies that create bans on any unauthorized access to sensitive information. When users log into a system running CB Protection, they are restricted by policy to run only pre-approved applications. All other applications are restricted from use, based on policy and the user’s need to know.

CONTROL 14 QUICK WINS

- Segment the network based on the label or classification level of the information stored on the servers.
- Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.

CONTROL 15.

Wireless Access Control

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

The CB Protection connector allows you to integrate with next generation firewalls and other networking solutions. Device control capabilities are also built in to provide business solutions that comply with network controls.

CB Protection also integrates with the leading network security providers such as Check Point, Fidelis and Palo Alto Networks.

CONTROL 15 QUICK WINS

- Ensure that each wireless device connected to the network matches an authorized configuration and security profile. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
- Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.

CONTROL 16.

Account Monitoring and Control

Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

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 Active Directory.

CONTROL 16 QUICK WINS

- Review all system accounts and disable any account that cannot be associated with a business process and owner.
- Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.
- Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

CONTROL 17.

Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical 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, organizational planning, training, and awareness programs.

CB Protection notifies end users and company personnel of updated and recent security policy changes while maintaining a full audit record of acknowledgment and compliance. CB Protection provides you with branded templates for training and testing of security policy.

CONTROL 17 QUICK WINS

- Perform gap analysis to see which skills employees' need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
- Deliver training to fill the skills gap and implement an online security awareness program.

CONTROL 18.

Application Software Security

Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses.

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.

Much like a patch management solution, CB Response can provide 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. Using a CB Response watch list for vulnerable or dated applications provides users notifications once they appear within the network. Vulnerable or dated applications will be identified immediately within the environment as soon as they appear.

CONTROL 18 QUICK WINS

- For all acquired application software, check that the version you are using is still supported by the vendor.

CONTROL 19.

Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CB Response's always-on threat protection allows for the ability to actively monitor system and file components proactively 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 provides incident response management, as it lets you "rewind the tape" to view the full spectrum of an event.

Since CB Response is always recording so even if the indicators of compromise (IOC), anomaly, or suspicious activity have long since passed, CB Response will provide all the related activity to immediately determine what process caused the event, and any other processes it performed.

CONTROL 19 QUICK WINS

- Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
- Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
- Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team.

CONTROL 20.

Penetration Tests and Red Team Exercises

Test the overall strength of an organization’s defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

CB Response’s incident response functionality combined with CB Protection’s console alerts will narrow the scope of events when going through a penetration test exercise. You can drastically reduce your response down to a fraction of the time normally spent investigating and event. While investigating, CB Response provides the entire timeline of a security event with associated remediation steps. This reduces the number of steps required for penetration testing and enhances both white box and black box analysis by showing vulnerabilities in real time.

CONTROL 20 QUICK WINS

- Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.
- Any user or system accounts used to perform penetration testing, should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.

Carbon Black.

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

Carbon Black (NASDAQ: CBLK) is a leader in endpoint security dedicated to keeping the world safe from cyberattacks. The company's big data and analytics platform, the CB Predictive Security Cloud (PSC), consolidates endpoint security and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behavior patterns, enabling customers to detect, respond to and stop emerging attacks. More than 5,000 global customers, including 34 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use Carbon Black's technology in more than 500 breach investigations per year.