DATA SHEET

Advanced Threat Protection: Carbon Black Enterprise Protection Server Security

At A Glance

Your servers, whether physical or virtual, hold your company's IP are the target of Advanced Threats.

Carbon Black Enterprise Response provides a new generation of server security using a trust-based security model that will protect your servers, in real time, from internal and external threats.

> *"Gartner recommends using 'whitelisting' approaches for critical servers whenever possible" to "go beyond simple signature or pattern detection."*
>
> Focus on the how, not the who, of Advanced Targeted Threats Like Flame
>
> *-John Pescatore, vice president and distinguished analyst, Gartner.*

What if you could…

- Protect your organization's sensitive information within the data center from advanced threats?
- Continuously monitor, control, and report on changes to critical configuration files in real time?
- Eliminate costly and time-consuming re-imaging?
- Lower the administrative effort of your server security solution?

Business Challenge

Your servers, whether physical or virtual, hold your organization's intellectual property and are the target of advanced threats. Attackers - such as nation states, cyber criminals and hacktivists - are skilled, organized and well-funded. And they are after every valuable piece of data they can get their hands on, including but not limited to intellectual property, military data, and financial information. If yours was to become yet another name on the growing list of companies that has been breached, the damage to your bottom line, and your brand, could be irreversible.

A challenge unique to servers is that following an incident, they cannot be returned to a useable state as quickly or easily as desktop systems. Remediation and recovery is extremely difficult, disruptive, and costly and can affect the availability of revenue-generating applications and services.

Cb Enterprise Protection Solution

Cb Enterprise Protection is the leader in advanced threat protection for endpoints and servers and is the only solution that continuously monitors all activity on these machines to prevent advanced attacks from occurring in the first place. While organizations have traditionally relied on blacklisting technologies such as anti-virus, these solutions are no longer adequate to protect against today's advanced threats. Today's attackers are well skilled at altering known malware to make it undetectable by most traditional defenses.

Cb Enterprise Protection's proactive approach to security enables organizations to prevent malicious software from infecting protected machines. Cb Enterprise Protection's policy-based approach enables IT teams to take an inventory of all software applications running in their environments, decide which software is trusted and should be permitted to run, and block all other software and executable files by default. Cb Enterprise Protection also provides real-time visibility into all software changes, both authorized and unauthorized, so that administrators can be immediately alerted to suspicious activity. The Cb Enterprise Protection Platform is optimized for both physical servers and virtual machines, and it offers the lowest administrative effort of any application control solution.

CARBON BLACK
ARM YOUR ENDPOINTS

"Default-Deny" Policies Secure Your Highest Risk Assets

Define trusted software that is permitted to run and deny everything by default. No more malware, zero-day threats, viruses, or unauthorized software.

The machines within your data center store a variety of highly sensitive information. From your servers that hold intellectual property to your domain controllers that hold the "keys to the kingdom," you need to know where your most-sensitive data lives and take actionable steps to apply the strongest forms of protection. One of the most effective ways to protect this data is to enforce application control on the machines that store this sensitive information.

During a typical advanced attack, malicious parties breach the organization, do reconnaissance to locate the most valuable data, and install malicious software to facilitate the exfiltration of that data. Often times this malware easily bypasses traditional security defenses. However, Cb Enterprise Protection tools and policies can be used to simply prevent this malicious, unknown software from executing, and thereby prevent the data loss.

- **Real-time software inventory.** Cb Enterprise Protection enables administrators to pull a real-time inventory of all software that currently exists in their environment. This software inventory provides information on what software is running and exactly where it is located.
- **Policy-driven approach.** Based on the software inventory, your security team can determine which software should be permitted to be run, which software should be banned and which requires further analysis. Based on this risk-assessment, security teams can set policies within Cb Enterprise Protection to automatically ban, permit or analyze software and files as they attempt to execute on your protected servers.
- **Default-deny policies.** For machines that store your highest risk assets, "default-deny" policies provide the strongest form of security. With default-deny policies, security teams are able to prevent all untrusted software from running. This approach allows known, trusted software to run normally while automatically protecting organizations from known malware, unknown malware, unauthorized software and zero-day threats.

Monitor File Integrity and Registry Changes to Improve Security and Compliance

Detect, in real time, unauthorized change that may represent an attack on your servers.

When software-driven breach methods fail, sophisticated attackers on a targeted mission may pivot their efforts to users – but not just any users. If an attacker is able to compromise a privileged user's credentials, the attack will become even more difficult to detect.
To remove this blind spot, Cb Enterprise Protection provides real-time monitoring of all activity that occurs on protected servers. Thanks to this increased visibility, security teams can easily look for abnormal changes to files, software and registries, which could be signs of an advanced attack.

- **File Integrity Monitoring and Control.** Cb Enterprise Protection provides continuous, real-time monitoring of your critical configuration files and can alert your security teams to unauthorized or suspicious changes. This capability helps organizations improve their security postures as well as meet file integrity monitoring and audit trail rules.
- **Registry protection**. Cb Enterprise Protection enables you to write rules to automatically report any changes to specific registry keys.
- **Baseline drift.** Baseline drift reporting enables you to easily identity anomalous software and system changes. Cb Enterprise Protection tracks software and system changes in real-time and compares these against a baseline of what is "normal" within your environment. By comparing these changes against what is known to be normal, security teams can gain visibility into anomalous activity that could potentially signal an attack is underway.

"By locking down kiosks and servers with Cb Enterprise Protection (formerly Bit9), we are able to protect our brand name while enforcing compliance and eliminating risk of security vulnerabilities."

— VP Information Systems, National Retail Chain

Consistently Apply Security Policies to Physical and Virtual Machines Alike

Carbon Black Enterprise Protection is the only application control solution optimized for virtualized environments.

- **Real-Time Protection:** Cb Enterprise Protection is the first application control solution optimized for virtualized desktops and servers, including terminal services, VDI and both persistent and non-persistent implementations. Cb Enterprise Protection helps customers protect their investments in virtualization by providing real-time advanced threat protection without the overhead of scanning or I/O storms.
- **Terminal services:** Cb Enterprise Protection records all activity on protected servers and endpoints, and as a result, it is able to associate security events with user accounts on shared work stations. When multiple users are sharing the same operating environment, events and notifications are associated with the appropriate user.
- **Baseline image templates:** Cb Enterprise Protection is optimized to support the use of cloned images and non-persistence in your virtual environment. Images created from a master image are not put through the standard initialization process, eliminating CPU and network utilization for increased performance and efficiency.

Improve Server Operations

The Cb Enterprise Protection Platform helps organizations reduce the administrative effort associated with server security by enforcing strong application control without interfering with normal systems maintenance

- **"High-enforcement" application control.** Cb Enterprise Protection policy-based approach to security enables organizations to operate their servers in "high enforcement" mode. In this mode of application control, security teams define the software that they would like to run on their machines, which in turn bans everything else. By only permitting known, trusted and approved software to run, security teams are able to dramatically reduce the threat surface, prevent malware and zero-day attacks, and eliminate the need to re-image these machines due to compromise.
- **Seamless updates for trusted software.** Applications and software that are approved to run in high-enforcement mode can be configured to update without requiring changes to application control policies. Policies can be set to automatically trust pre-defined software publishers, internal software repositories, and software delivery and patch management solutions.
- **Enhanced device control.** Prevent data leakage and unintentional or intentional direct loading of malware by limiting the use of portable storage devices to an authorized set, type or even to a specific serial number.
- **Centrally manage security policies for servers and endpoints.** Carbon Black System Console is the central repository for policy management and system administration. The adaptable administrative console provides comprehensive visibility into agent management, reporting, software exception alerting, system components and removable storage media on managed servers.

Case Study

International Communications Company Locks down its Domain Controllers

Customer Challenge

An international communications company needed to lock down 225 domain controllers to ensure that thieves could not use social engineering and malware to exploit perimeter machines and penetrate inward. The company was in the process of evaluating solutions when a breach occurred.

Cb Enterprise Protection Solution

Cb Enterprise Protection Professional Services team created an approach to protect the company's critical infrastructure immediately, with a phased rollout to other components. Cb Enterprise Protection was quickly deployed to stop all unauthorized software, utilities, drivers and tools until IT could approve, investigate and if need be delete them. Cb Enterprise Protection solution prevents zero-day attacks, malware and other malicious activity by only allowing trusted software to install and execute on the domain controllers and nothing else.

Results

The ease of deploying Cb Enterprise Protection has allowed the company to enact a high enforcement policy among its domain controllers a month ahead of schedule. The company has safeguarded its intellectual property by stopping zero-day and other attacks with unrecognized signatures. The solution has enabled IT to centrally manage multi-server and multi-site domain controller environments. In addition, Cb Enterprise Protection works in tandem with other security tools allowing the organization to enforce a comprehensive, in-depth defense.

Building a Security Strategy: Start with your Domain Controllers

Your domain controllers sit at the epicenter of your enterprise serving as the gatekeeper for user and administrator access as well as your company's intellectual property. Domain controllers contain the "keys to the kingdom" and if successfully compromised, will give attackers access to virtually every other repository of IP within the organization. If that weren't enough, the costs and disruptions stemming from remediating attacks on domain controllers can be overwhelming.

Therefore, in building a server security strategy, it is important to develop a security plan that is built out in phases, protecting your critical domain controllers first—then extending protection outward as your enterprise policy, priorities and resources dictate.

About Carbon Black

Carbon Black leads a new era of endpoint security by enabling organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals from IR firms, MSSPs and enterprises to shift the balance of power back to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Carbon Black has been named #1 in endpoint protection, incident response, and market share. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to: Disrupt. Defend. Unite.

20160226 RKB

CARBON
BLACK
ARM YOUR ENDPOINTS

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