DATA SHEET

Cb PROTECTION

The market-leading application control solution

Cb Protection is the industry's most trusted and proven automated application control solution for endpoint security. Utilizing a combination of cloud reputation services, IT-based trust policies, and multiple sources of threat intelligence, Cb Protection ensures only trusted and approved software is allowed to execute on your regulatory-mandated highly-sensitive and targeted systems. More than 1,800 organizations globally rely on Cb Protection.

Traditional endpoint security methods have failed to protect high-valued and targeted business systems. Hundreds of millions of financial records, personal identifiable information (PII), credit card accounts, emails, and passwords have been stolen, costing consumers and enterprises billions. The market for stolen data is only growing, motivating cybercriminals to attack any system that stores and processes valuable information, including laptops, desktops, data centers, fixed-function devices, industrial control systems, medical devices, and financial exchanges.

Fig. 1: Cb Protection Visibility dashboard

Antivirus (AV) technology has put an unnecessary load on processing resources while only slightly reducing the risk of attacks. The value does not equal the effort. Today's enterprises, both large and small, need the best possible control over systems containing IP, PII, and other sensitive data.

LOCK DOWN ENDPOINTS AND SYSTEMS AND PREVENT UNWANTED CHANGE

Cb Protection is the industry's only automated application control solution that provides zero-touch whitelisting capabilities through policy-driven approvals. Approvals of new and updated software are done based on trust. Policy-based trust can be driven by IT and through the cloud. The combination of both an IT-driven policy and a dynamic cloud-based trust policy allows you to whitelist without a list, lessening the administrative effort required by IT while also minimizing user interruption.

IT-DRIVEN TRUST

IT-driven trust is defined by the software that IT deploys within the organization. By definition, this software is trusted and would therefore be allowed to run. An IT-driven trust scenario includes the ability to automate trust for things such as patch management, software repositories, self-updating applications, trusted users or publishers, software distribution systems, and IT Help Desk.

BENEFITS

- Stop attacks by allowing only approved software to run
- Automate software approvals and updates via IT and cloud-driven policies
- Prevent unwanted change to system configuration at the kernel and user mode levels
- Power device control and file integrity monitoring and control (FIM/FIC) capabilities
- Meet IT risk and audit controls across major regulatory mandates
- Replace inadequate security controls and consolidate endpoint agents
- Streamline regulatory and IT audit processes
- Increase efficiency of IT resources
- Eliminate unplanned downtime of critical systems

USE CASES

- Corporate desktops, laptops, and tablets
- Point-of-sale terminals
- ATM machines
- Industrial Control Systems (SCADA)
- Medical devices
- Domain controllers
- Financial trading platforms
- Email and web application servers
- VDI environments
- Card data environments (CDE)
- Unsupported systems
- Data centers
- Fixed-function

SUPPORTED PLATFORMS

CLOUD-DRIVEN TRUST

A common issue that arises in dynamic organizations is the need for users to download and run software without having to go through a formal process and wait for IT to approve and install the software. Cb Protection utilizes the Cb Collective Defense Cloud as another reference point when considering trust. This means Cb Protection can be configured to allow software downloaded by the user to run with no administrative effort including 'grey' files. Grey files are those files that haven't been assessed yet. The name comes from their status as neither whitelisted or blacklisted. Cb Protection enables users to define the trust threshold for grey files and then define actions based on the trust value for that file.

CB COLLECTIVE DEFENSE CLOUD & THREAT INTELLIGENCE

Threat intelligence refers to the ability to determine the trust value for a given file. Cloud integration is a key component of modern threat intelligence. The real-time nature of the cloud, coupled with advanced and automated detonation, means that Cb Protection can determine the disposition and trust value for a file as needed. Cb Protection includes file detonation along with threat reputation scores. By analyzing these sources of information, new intelligence can be applied immediately.

ACHIEVE CONTINUOUS COMPLIANCE

The control policies within Cb Protection provide a simple way to determine: which assets are in-scope for a particular standard; what software is required on those devices; who can make changes to the software and files on those devices. Once in place, control policies automatically enforce the appropriate compliance standards and provide auditable logs for evidence of compliance. If an executable is not on a controlled list of pre-approved software, it will not run. Total coverage with Cb Protection nearly eliminates the pre-compliance auditing process, dramatically reduces your attack surface by leveraging policies such file integrity monitoring and control (FIM/FIC), and accelerates your ability to meet and continuously comply with numerous regulatory standards and frameworks, such as PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, NIST 800-53, and more.

CONSOLIDATE SECURITY AGENTS

Cb Protection simplifies the complexity of endpoint security management and closes all your security gaps by reducing the amount of agents required on your devices to just one light weight and complete agent. By eliminating the need for performance degrading solutions like AV, FIM/FIC, ABM, RSD, DLP, and HIPS, you will cut costs, free up resources, and optimize endpoint security and performance.

OPEN INTEGRATION AND APIS

Cb Protection integrates with Security Information and Event Management Systems (SIEMS), log management systems, software delivery, patch management, and IT ticketing systems utilizing prebuilt connectors and open APIs to minimize the need for customization.

AUTOMATION

Cb Protection automates the approvals of new software, file analysis, lockdown, file upload, and so on — all are common workflows for application control administrators. Automation means that users enjoy rapid response while the organization reduces administrative costs and maximizes its return on investment for all elements of its security stack.

ABOUT CARBON BLACK

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

CARBON BLACK
ARM YOUR ENDPOINTS

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