SOLUTION BRIEF

Financial Services Security and Compliance

BENEFIT STATEMENTS

- Reduce your time to detect and resolve incidents.
- Integrate with your existing security.
- Detect and prevent unauthorized processes from executing.
- Extend the value of and protect EOL systems such as Windows XP, Windows Server 2003 and others.
- Exceed regulatory compliance requirements and align with advanced cyber-security frameworks.
- Disrupt attackers by locking down fixed-function devices (POS, ATM), end-user workstations, critical servers, and PCI environments.
- Flexible threat management controls to fit your security posture without disrupting business operations.
- Live attack response.

Disrupt attacker behavior and root out threats to protect corporate and customer data, while improving system uptime and enterprise compliance

OVERVIEW

The high value of corporate and customer data transmitted and stored by financial institutions, along with the vulnerabilities introduced by third-party vendor relationships, call for a sophisticated security strategy. A prolonged disruption can mean millions of dollars in lost productivity and permanent reputational damage. The financial services industry has been recognized for its advanced approaches to security, but the threat remains real as nation-states and cyber criminals continue to develop and deploy new attack techniques.

Carbon Black's Next-Generation Endpoint Security solutions disrupt the advanced cyber attacks targeting financial institutions at the first sign of compromise, preventing data breaches without impacting transactional or organizational efficiency. With Carbon Black you can align your cyber-security strategy with the latest guidance and frameworks from the FFIEC, SEC, FDIC and others, helping you ensure a secure and compliant operating environment.

92% of financial institutions are implementing/have implemented a risk-based security framework

[Source: PWC, The Global State of Information Security® Survey 2016, *http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-financial-services.pdf*]

Top 5 Cyber Risk is the top concern among financial industry leaders, with a record **46%** of citing it as the single biggest risk to the broader economy and **80%** citing it as a top five risk.

[Source: Depository Trust & Clearing Corporation's 2015 Systemic Risk Barometer survey]

4X Financial institutions are attacked **four times as often** as organizations in other industries

[Source: CSO, *http://www.csoonline.com/article/2938767/advanced-persistent-threats/report-banks-get-attacked-four-times-more-than-other-industries.html*]

Carbon Black enables financial institutions to identify and disrupt advanced attacks before they cause damage. Cb Protection helps you lock down fixed-function devices (POS, ATM), end-user workstations, critical servers, and PCI environments. Carbon Black Enterprise Response enables you to root out the sources of compromise and prevent them from recurring, freeing up the security team to focus on other priorities.

Carbon Black.

The FFIEC Cybersecurity Assessment Tool, introduced in July 2015, helps financial institutions identify their risks and determine their cyber-security preparedness. Banks can use the assessment tool's inherent risk profile to categorize their risk from areas of most concern to least. Once their inherent risks are identified they can rank their cyber-security maturity level from having the bare baseline of security essentials to being proactive and innovative.

Download Understanding the FFIEC Cybersecurity Assessment Tool

Security for the Extended Operational Environment

By preventing any unauthorized process from running on your endpoints and servers, Cb Protection stops malware from exfiltrating corporate and customer data. Carbon Black's real-time approach to detection, prevention and response does not slow down transactional or administrative systems.

Cybersecurity Framework Alignment

Carbon Black's Next-Generation Endpoint Security platform helps you align with the most advanced cyber-security frameworks, such as the CIS Critical Security Controls, FFIEC CAT and NIST 800-53, to ensure coverage of the latest techniques.

United Community of Experts

Carbon Black's customers, whether they share threat intelligence or not, benefit from the collective expertise and shared knowledge of 10,000 security professionals from large enterprises, small companies, IR firms and MSSPs.

Third-party Validated Controls for PCI DSS

Coalfire, an industry-leading QSA and charter member of the PCI Council, has validated Cb Protection against several PCI DSS requirements. No other endpoint security solution has achieved such validation.

Extended Value of Legacy Infrastructure

Using application control to block unapproved processes from executing, Cb Protection helps you keep unsupported and legacy operating systems in place, while maintaining a secure—and compliant—posture.

CARBON BLACK MAKES IT EASY TO COMPLY WITH REGULATORY REQUIREMENTS FOR DATA COLLECTION, ANALYSIS, REPORTING, ARCHIVAL AND RETRIEVAL.

SOX Compliance Control	Carbon Black Capability
Section 105: Investigations and Disciplinary Proceedings Endpoint Liability: People	
Section 105 requires that the Boards of any firm involved in an investigation or a disciplinary action keep all documents and information related to the action "confidential and privileged as an evidentiary matter." Sanctions can be imposed for failure to reasonably supervise any associated person with regard to auditing or quality control standards.	**Prevent data leakage** — Cb Protection's device control feature, which prevents users from copying data to unauthorized devices (for example, to keep it off unencrypted devices). Carbon Black traces each binary and process step throughout the entire security event. All file changes and modifications are recorded and with whom made them for audit records. **Audit data transfer** — Cb Protection's built-in auditing capabilities also provide visibility to any files copied to a personal storage device to ensure quality control. **Block unauthorized software** — Application whitelisting ensures that no malicious software, including keyloggers, spyware, or custom-built Trojan viruses, are able to run on a PC and steal confidential data. **Audit trail integrity** — Carbon Black will provide evidence of any change that has occurred and what happened. Playing the full replay from start to finish with no forensics wait time or obligation of dealing with the chain of command when removing hard drives.

SOX Compliance Control	Carbon Black Capability
Section 302: Corporate Responsibility for Financial Reports Endpoint Liability: Cyber-Infrastructure	
Section 302 requires significant workflow management to assure that financial officers who sign annual and quarterly financial statements can attest to the accuracy of the information in those reports. Changes in the reporting systems and their controls must be tracked and reported in addition to the data.	**Identify and block software changes** — Cb Protection's software tracking system identifies any new software that appears on a |system, including patches, updates, installations, downloaded files, malicious software, and more. Any time a new software file is written to disk, Bitg creates an audit entry identifying the software and, when configured with a lockdown policy, prevents it from running. **Audit for change control** in this manner, financial reporting systems can not only be audited for change control, but also prevented from running unauthorized software. Carbon Black visually displays all change records allowing full visibility into file integrity and file monitoring reporting.
Section 404: Management Assessment of Internal Controls Endpoint Liability: People, Processes	
Section 404 requires management to attest to the effectiveness of their internal controls, which in turn implies that processes used to develop, manage, and report on information systems are consistent and accurate.	**Audit and enforce internal controls** — Using Cb Protection managers can narrow their scope on compliance audits and save time with automated reporting showing your organizations policy enforcement on all in scope assets while maintaining full audit trails. **Block unauthorized software and data leakage** — Cb Protection prevents unauthorized users from accessing or using software that violates your control policies, or from transferring data to personal storage devices. Built-in audit trails track every software application run or file transferred to or from a personal storage device.
Section 409: Real-time Issuer Disclosures Endpoint Liability: Cyber-Infrastructure, Processes	
Section 409 requires firms to disclose—in a timely manner— information that pertains to material changes in operations. As most systems that would capture or create this information (ranging from ERP and GL to BI and data mining) are under the control of IT, compliance relies heavily on IT.	**Ensure system availability** — Cb Protection prevents unauthorized or malicious software from running on critical systems. This ensures the availability of those systems. **Audit changes to critical systems** — With Cb Protection's automatically generated audit trails, all changes to critical systems can be detected and monitored to enforce policy and smooth operation. Carbon Black will display the entire timeline of a compelling event narrowing your response time in seconds. You are able to be the first responder in the event of a security incident. You can now isolate an infected system and keep the attack from spreading.

SUMMARY

Carbon Black provides the most advanced Next-Generation Endpoint Security platform available to help financial institutions prevent advanced attacks and identify threats in their environment, without impacting operations. The Carbon Black Security Platform enables security teams to disrupt attacker behavior, optimize efficiency and productivity, and align with advanced cyber-security frameworks.

Carbon Black.

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable 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 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

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