Carbon Black.

SOLUTION BRIEF

Healthcare Security & Compliance Solution

Protect Patient's Data & Reduce Liability with Endpoint Threat Prevention, Detection & Response

KEY TAKEAWAYS

- Governance, unsupported software and control processes are the biggest gaps in stopping attacks. You need your endpoints to be security sensors, not weak links.
- Deploy a proactive security strategy across all of your back-office, on- and off-network endpoints and servers.
- Go beyond simple file encryption by future-proofing your ransomware defenses.

Overview

Healthcare providers and insurers are responsible for protecting electronic protected health information (ePHI) and other patient data regardless of how it's transmitted, where it resides or how authorized users access it. Fail to do so, and the effects can be devastating: loss of highly confidential and sensitive information; financial penalties and damaged trust and credibility. To add to these security concerns, healthcare organizations also are required to maintain HIPAA — and perhaps even PCI — compliance. This is particularly tricky with systems that reach end-of life (EOL). Without support like patching and critical updates, the enterprise will be vulnerable to malware attacks and potential "zero-day forever" scenarios.

Without Visibility Endpoints Are Blind Spots and Vulnerable

Accepting the inevitability of compromise is the first step in protecting your systems. Anti-virus or scan-based security measures are no longer sufficient. The reality is that healthcare organizations need a security solution that will deliver full real-time advanced threat protection that has continuous endpoint visibility at its foundation. Without this type of solution, the organization is blind to many sophisticated malware and non-malware attacks, like ransomware meant to steal patient information, extort large amounts of money, or something even more nefarious.

Stop Ransomware Before It Starts

Many industry associations and security advisors in the healthcare industry preach education of end-users above all else because employees can be the biggest deterrent to hackers getting in.

While it is important to add an employee training program to your security strategy, the reality is even the most educated end users, which never click on email attachments, and practice good security procedures can become victims of sophisticated exploits, through drive-bys and other exploit kits.

The best way to stop malware like Locky, TorrentLocker, and other ransomware variants is to implement a security system that continuously, centrally records all endpoint activity and stops untrusted code from executing on endpoints.

Stop Malware Attacks and Non-malware Attacks with the Carbon Black Security and Compliance

Secure ePHI by closing the security gaps that are being exploited by targeted attacks and unknown malware. Built on a proactive, trust-based security approach, Carbon Black provides visibility, detection, response and protection for servers and endpoints. It also automates and manages many regulatory requirements listed in HIPAA/HITECH and PCI. The result is a focused security and compliance program that aligns resources and budgets with threats and risk, to secure a positive patient experience and prove Meaningful Use.

Transform Weak Links into Security Sensors

Carbon Black provides IT security teams with comprehensive and effective application control by monitoring and recording all activity on endpoints and servers to detect and stop cyber threats that evade traditional defenses. The solution takes a policy-driven approach that enables you to easily determine and catalogue the software you trust.

Healthcare enterprises have a diverse population of endpoints and servers from traditional business systems to medical devices that scan a patient's personal, financial and health information. This data travels throughout the healthcare network through a number of different endpoints. With three different policy-driven enforcement levels, you choose what level of enforcement will be most effective based on the type of endpoint or server you are protecting.

For example, XP may be running on workstations used by clinical staff, imaging modalities and other critical devices or terminals. These devices are typically connected via the network to the EHR/EMR and, therefore, can't just be disconnected. This leaves you facing a full hardware upgrade and/or upgrading the legacy applications running on the XP systems. These systems require a "set it and forget it" security approach. Deploying Carbon Black's lightweight agent and setting a high enforcement policy, locks down the system without disrupting performance. It also provides evidence for audits by offering full, detailed compliance reports.

Cb Protection

Cb Protection leverages a comprehensive, aggregated advanced threat intelligence network that combines leading software reputation, threat indicator and attack classification services to provide some of the most accurate threat insight. Cb Protection offers Carbon Black's unique threat intelligence and industry-leading third-party intelligence sources to empower you to optimize and improve your prevention, detection, response and recovery capabilities.

- Threat Indicator Service for detection of malicious behaviors and compromise
- Reputation Service for trust ratings of known-good, known-bad and unproven software and domains
- Attack Classification Service for third-party attack context and attribution

USE CASE: TOP PEDIATRIC HOSPITAL

Following breaches, the hospital's IT and security team deploys a new generation of endpoint security against advanced threats.

SUMMARY

One of the top three pediatric medical centers in the United States, this hospital serves patients from around the world who need treatment for rare diseases or complex surgical procedures. Following two security breaches, the hospital's CISO realized that his incumbent security solutions were insufficient to protect the facility against advanced threats. He also wanted to integrate his endpoint and network security. Like any medical organization, the hospital also needed to ensure that it complied with HIPAA requirements for securing patient records. That's why the hospital chose to deploy Cb Protection for FireEye.

CHALLENGE

Just as the hospital was about to deploy Mandiant's endpoint solution in its security stack, they decided to take another look at what Cb Protection could do. During the review process, the team became convinced that the solution offered a true next generation of endpoint security that was especially well suited for the critical needs of the hospital. They also wanted to ensure that their endpoint and network security solutions would work together seamlessly to eliminate blind spots and false positive alarms.

During its extensive evaluation of Cb Protection, the hospital was hit by CryptoLocker, one of the most sophisticated ransomware attacks ever seen. Once the Cb team showed how effectively it could stop such an attack, the process quickly moved from "we need to do more testing" to "how fast can we deploy Cb Protection?"

THE CARBON BLACK SOLUTION

The hospital deployed Cb Protection for Windows and Mac on its thousands of endpoints and saw immediate results as the Cb Protection sensors began monitoring and recording all activity on every machine. In addition, the hospital integrated its endpoint and network security by deploying Cb Protection for FireEye.

RESULTS

Carbon Black's advanced threat protection capabilities have successfully prevented further breaches at the hospital including a repeat of the CryptoLocker attack.

Discovered by Carbon Black, PowerWare - Healthcare's newest security threat

The Carbon Black Threat Research Team discovered a new family of ransomware, which they dubbed "PowerWare," through an unnamed healthcare client whom first brought the suspicious email to the company's attention. "PowerWare" targets organizations via Microsoft Word and PowerShell. PowerShell is the scripting language inherent to Microsoft operating systems. "PowerWare" is a new instance of ransomware utilizing native tools, such as PowerShell on operating systems.

"Traditional" ransomware variants typically install new malicious files on the system, which, in some instances, can be easier to detect. "PowerWare" asks PowerShell, a core utility of current Windows systems, to do the dirty work. By leveraging PowerShell, this ransomware attempts to avoid writing new files to disk and tries to blend in with more legitimate computer activity.

Deceptively simple in code, "PowerWare" is a novel approach to ransomware, reflecting a growing trend of malware authors thinking outside the box in delivering ransomware.

Secure Unsupported or Unpatched Software with a Positive Security Approach

There are a number of reasons why healthcare organizations continue to use aging or unsupported software; budget, system integration requirements, business priorities, etc. As a result you have limited threat intelligence and situational awareness to fend off APTs. What's more, the inability to address this issue creates a bigger gap due to the inability to keep up with the ever-increasing attack surface and the threats of never before seen attacks. These constraints make securing the environment difficult and can often cause compliance violations.

Carbon Black can lock down all in-scope endpoints and extend the security window to protect endpoints well past OS EOL deadlines and allow updates or upgrades to be scheduled when convenient. You get visibility to ensure that vulnerabilities are identified in real time and the entire system remains in a dynamic state.

Carbon Black's positive security is a model based on known, 'good' applications that are pre-approved to run. Every rule added to a positive security model increases what is known and allowed, while untrusted processes are blocked from executing. Positive security software is designed to secure all systems, including hardening out-of-date systems, such as XP — so anything that is not known will not run, preventing zero-day exploits and targeted attacks.

Cb Protection and Cb Response

Cb Protection and Cb Response run across Windows, Mac and Linux machines to keep all endpoints and servers secure, whether on or off network, dramatically reducing an organization's attack surface. Together they go beyond basic security with advanced file integrity monitoring and control capabilities, enabling organizations to maintain continuous compliance with PCI-DSS, HIPAA/HITECH, SOX/GLBA, NERC CIP, NIST 800-53, and other regulations and frameworks.

Because your end user endpoints and critical infrastructure servers have very different requirements and prevention needs, Carbon Black provides flexible prevention options to ensure the right balance between organizational culture and risk posture. Regardless of the level of enforcement you choose, Carbon Black is always recording endpoint activity and base image drift, providing unprecedented visibility into your endpoints.

Carbon Black makes it easy to comply with regulatory requirements for data collection, analysis, reporting, archival and retrieval.

ENDPOINT LIABILITY

PROCESS RELATED

- Monitor, secure systems/assets across business security and supply chain
- Keeping compliant in all things cyber security on and off network

BEHAVIORAL

- Personal convenience over procedure
- Privileged users
- Third-party service providers and contractors
- Insider accounts hacked

TECHNOLOGICAL

- Unpatched systems
- Old operating systems and applications bugs
- System misconfiguration
- Internet of Things

Compliance Control	Compliance Goals	Carbon Black Capabilities	Endpoint Liability	HIPAA	PCI
Compliance Risk Analysis and Measurement	• A repeatable process for identifying, categorizing and measuring risk across corporate assets • Provide evidence of compliance and communication of policies	• Create automatic application baselines • Automatic risk ranking and trust ratings • Continuous assessment, enforcement and audit		Administrative Safeguards 164.308 (a)(1) 164.308 (a)(8)	Build and Maintain a Secure Network and Systems PCI 2.2, PCI 2.4
				Physical Safeguards 164.310 (b)(1)	Maintain a Vulnerability Management Program PCI 5.1. PCI 6.1, PCI 6.
					Implement Strong Access Control Measures PCI 7.2
				Technical Safeguards 164.312 (b)(1)	Regularly Monitor and Test Networks PCI 10.6
Configuration Change Monitoring and Chain of Custody	• Protect critical information from exposure • Prevent unauthorized changes to control files, including configuration and log files • Establish an audit-able chain of custody for all control file changes • Real-time monitoring and recording of all critical files	• Enforcing configuration control policies for compliance • Control policies recognize legitimate and malicious changes • Near real-time monitoring of your environment		Administrative Safeguards 164.308 (a)(6)	Build and Maintain a Secure Network and Systems PCI 2.2, PCI 2.4
				Physical Safeguards 164.310(b)(1)	Maintain a Vulnerability Management Program PCI 6.4.5
					Regularly Monitor and Test Networks PCI 10.2, PCI 10.3, 10.5, 11.5a, 11.5b
Device & USB	• Prevent unauthorized portable devices from accessing information in the protected environment • Prevent protected information from being removed or disclosed via portable devices • Prevent the installation of unapproved software or malware from removable devices	• Prevent data loss • Granular and flexible device and port control • Evidence for audits		Administrative Safeguards 164.308 (a)(3), 164.308(b)(1), 164.310 (a)(1), Physical Safeguards 164.312(a)(1)	Implement Strong Access Control Measures PCI 7.1, 9
				Physical Safeguards 164.310 (d)(1), 164.312 (c)(1)	Maintain an Information Security Policy 12.3

Compliance Control	Compliance Goals	Carbon Black Capabilities	Endpoint Liability			HIPAA	PCI
File Integrity Monitoring and Control	• Detect changes to critical files, including configuration and log files • Real time monitoring and recording of all critical files	• Prevent unauthorized changes to critical files • Standard and custom rules • Evidence and artifacts for auditors • Correlated and contextual logging for SIEMs					Build and Maintain a Secure Network and Systems PCI 2.2
						Administrative Safeguards 164.308 (a)(3) Technical Safeguards 164.312(e)(2)(i)	Implement Strong Access Control Measures PCI 7.1
						Administrative Safeguards 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C) Technical Safeguards 164.312 (c)(1), 164.312 (e)(1)	Regularly Monitor and Test Networks PCI 10.5.5
Malware Prevention and Continuous Compliance Visibility	• Block all malicious software • Address threat from zero-day attacks • Provide evidence that controls map to corporate policies	• Blocks UNKNOWN malware • Flexible control policies for users • Documented control with audit-ready reports				Administrative Safeguards 164.308(a)(5)(ii)(B)	Maintain a Vulnerability Management Program PCI 5.1, PCI 5.2, PCI 5.3
Security Policy Awareness, Enforcement and Audit	• Demonstrate that compliance policy awareness plans are in place, enforced and audited • Provide evidence that policies have been communicated to employees/stakeholders	• Ongoing policy awareness and enforcement • Positive device control • Policy exception requests and logging • Evidence-based compliance				Administrative Safeguards 164.308(a)(5)(ii)(A)	Maintain a Vulnerability Management Program PCI 5.4
						Administrative Safeguards 164.308(a)(4) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D) Technical Safeguards 164.312(d)	
						Technical Safeguards 164.312(b)	Regularly Monitor and Test Networks PCI 10.7, 10.8, 11.5.1 Maintain an Information Security Policy PCI 12.1, 12.1.1, 12.3

Summary

More than ever, cybercriminals are targeting healthcare enterprises using a new breed of advanced threats in order to steal and exploit patients' personal and financial information. You understand these security challenges, but remain unable to adequately protect these systems due to a continued reliance on legacy antivirus solutions, aging software, and human error. And while the aftereffects of a data breach are worrisome in their own right, you also grapple with how a security breach will affect ongoing compliance with HIPAA requirements. At Carbon Black, our mission is to provide healthcare organizations a solution that will allow them to close these gaps by controlling change, blocking advanced threats, and securing patients' personal and financial information to significantly minimize attack surfaces and comply with key HIPAA and PCI requirements.

Threat detection and response in seconds

- Always have the information to instantly detect and respond top an attack.
- Real-time, "always-on" monitoring and recording means never wait for a sweep, poll or scan.
- See the entire "kill chain" of any attack and stop it in its tracks with innovative visualization technology.

Multiple, customizable, signature-less forms of prevention

- Only Carbon Black can customize for each group of machines and users.
- Mix and match different levels of Default-Deny—the best known form of prevention.
- You are in control of the level and type of protection you deploy

Automated alert analysis and threat remediation

- Prioritize alerts with real-time endpoint data, and investigate incidents from days to minutes.
- Locate every instance of a suspicious file across endpoints and services and enfoprce security policies to stop an attack and prevent it from happening again.
- Quickly determine risk of files arriving on your endpoints and servers—both automatically and on-demand.

Protect all end users and servers, including remote and offline

- Deploy Carbon Black on all of your endpoints and lower your risk profile by expanding protection to even remote and disconnected users.
- Real-time sensor watches and rercords everything while the endpoint is disconnected to maintain a full history.
- Runs on Windows, Mac, and Linux machines.

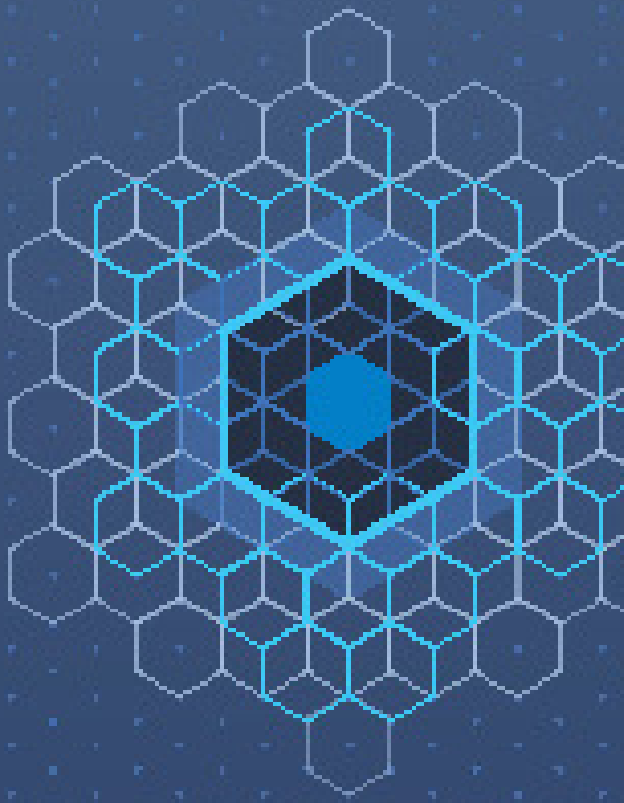
Integrates seamlessly into your environment

- Use endpoint data any way you want with open APIs.
- Integrate and correlate with network security products, analytics, SIEM solutions, and even home-grown tools.

Global ransomware damage costs are predicted to exceed $5 billion in 2017. That's up from $325 million in 2015—a 15X increase in two years, and expected to worsen.

Ransomware attacks on healthcare organizations—the No. 1 cyber-attacked industry—will quadruple by 2020.

-CSO Business Report, Oct. 17, 2017



Carbon Black.

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

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.

 Rev.2_171102