DATA SHEET

Integrating Carbon Black Enterprise Protection with FireEye

Together, Carbon Black and FireEye provide customers with unprecedented protection against advanced threats and malware

Key Benefits

Reduce operational effort

Filter non-actionable alerts discovered on the network through endpoint correlation and isolate the root cause of malware discovered on systems.

Accelerate incident response time

Immediate visibility of all infected systems for malware discovered on the network.

Improve security

Protect against advanced attacks designed to evade traditional security technologies. Enjoy the highest level of security for systems both within and outside of your perimeter.

Delivering Immediate Malware Alert Prioritization and Accelerated Incident Response

Together Carbon Black and FireEye deliver a first-of-its kind integration of network security with Cb Enterprise Protection trust-based real-time endpoint and server security solution. When FireEye detects malware on the network, Cb Enterprise Protection automatically confirms the location, scope and severity of the threat on your endpoints and servers, which accelerates incident response and remediation. With this integration, security analysts can filter out non-actionable events and prioritize high-impact alerts for rapid incident response, locate every instance of malware across their endpoints and servers, prevent future attacks through automated security policy updates, and use FireEye to automaticallyanalyze all files arriving on endpoints and servers to determine their risk. The Cb Enterprise Protection for FireEye will reduce the overall operational effort of managing network and system security, accelerate incident response time and improve your organization's overall security posture.

Carbon Black Enterprise Protection

The Cb Enterprise Protection continuously monitors and records all activity on servers and endpoints to detect and stop cyberthreats that evade traditional security defenses.

Cb Enterprise Protection

- The industry's **only real-time endpoint sensor and recorder** that provides real-time and historical data for every server and endpoint. You'll have a central repository of real-time data available at your fingertips without any scanning or polling
- **Policy-driven trust-based security** allows you to define the software you trust in your environment and deny everything else by default.
- A complete **inventory of files** that exist in your environment so you can instantly retrieve files from any endpoint or server at any time to submit to FireEye's detonation engine.

The FireEye Threat Prevention Platform (TPP)

The FireEye TPP stops advanced targeted attacks across web, email, file-based threat vectors. The FireEye security platform offers integrated, multi-vector protection utilizing stateful attack analysis to stop all stages of an advanced attack.

Each of FireEye's products features the Multi-Vector Virtual Execution (MVX) engine that provides state-of-the-art, signature-less file analysis using patented, proprietary virtual machines. The The FireEye TPP builds a 360-degree, stage-by-stage analysis of an advanced attack, from system exploitation to data exfiltration, in order to most effectively stop would-be APT attackers.

CARBON BLACK
ARM YOUR ENDPOINTS

This powerful combination of endpoint/server and network security solves four key security challenges:

Prioritize: I am receiving FireEye alerts, how do I prioritize them?"
Cb Enterprise Protection automatically correlates FireEye alerts with Carbon Black's real-time endpoint sensor and recorder data to determine which alerts are actionable and prioritize them based on the number of systems infected. Quickly decide if an alert requires escalation.

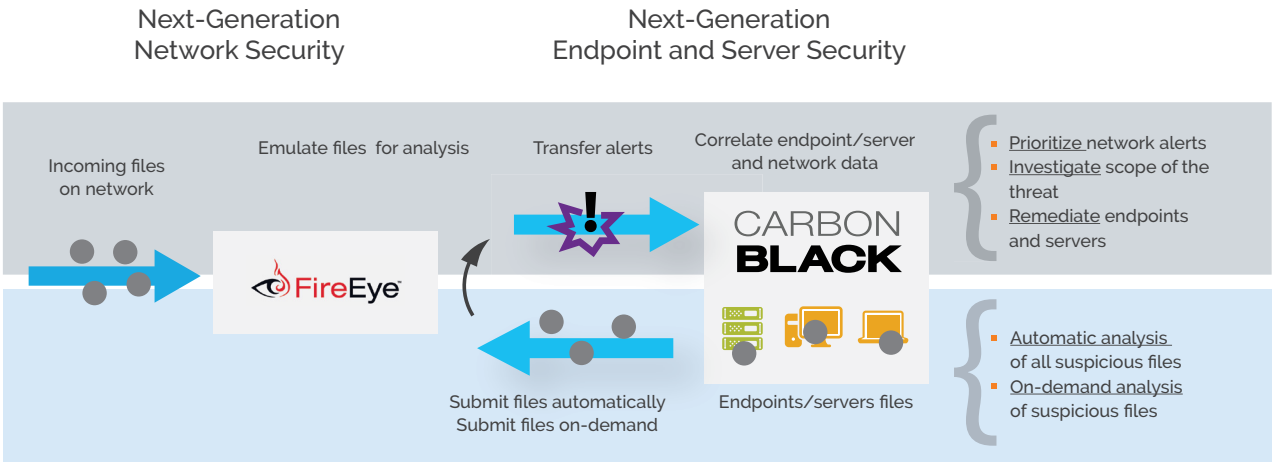
Investigate: "Is there a real threat and what is the scope?"
Locate every instance of a suspicious file across your endpoints and servers to accelerate incident response. Find out where a file landed, if it executed, how many machines it is affecting, and if you need to take further action.

Remediate: "How do I stop the attack and prevent it from happening again?"
Automatically enforce endpoint and server security policies based on FireEye alerts. Immediately stop malicious software from spreading throughout your enterprise and prevent it from affecting your machines again.

Analyze: Automatic Analysis: "When files arrive on my endpoints and servers how do I know which ones are malicious and need to be stopped?"
Use Cb Enterprise Protection to automatically submit all new files arriving on your endpoints and servers to FireEye's detonation engine to quickly determine the risk of each file and whether it needs to be stopped. Use criteria-driven rules to automatically determine which files to submit.

On-Demand Analysis: "I have suspicious files on my endpoints, how do I quickly assess their risk?"
Use Cb Enterprise Protection to retrieve any file from any endpoint or server and submit it to FireEye's detonation engine to analyze the file and to determine its risk.

"When I receive a user request to run unknown software, how do I know if it is safe?"
Use Cb Enterprise Protection to retrieve any file from any endpoint or server to submit to FireEye's detonation engine to make educated decisions about software approval management.



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.

CARBON BLACK
ARM YOUR ENDPOINTS

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