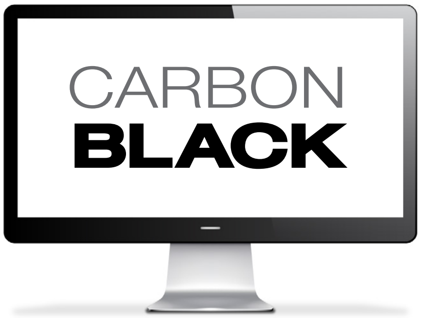
DATA SHEET

Carbon Black

First and only solution with continuous endpoint recording, live response & attack recovery

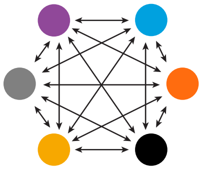


Carbon Black is the first and only endpoint threat detection and response platform that enables SOC and IR teams to prepare for a breach through continuous endpoint recording, customized detection, live response, remediation, and rapid attack recovery with threat banning. Carbon Black makes advanced threats easier to see and faster to stop by empowering SOC and IR teams to arm their endpoints against the most advanced and targeted attacks. Top IR firms and MSSPs have made Carbon Black a core component of their detection and response services.

65%
of data breaches
happened on endpoints[1]

52%
of incident responders
lack necessary endpoint visibility[2]

$737, 473
average cost
for crisis services[3]



Continuous monitoring & recording for gapless endpoint visibility

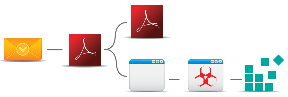
Carbon Black reduces the cost, complexity and time of traditional incident response by replacing reactive "after-the-fact" manual data acquisition with proactive continuous monitoring and recording of all activity on endpoints and servers—dramatically decreasing the dwell time of targeted attacks. Carbon Black provides the most complete and gapless enterprise visibility in the industry, by covering all major operating systems (Windows, Mac OS X, and Linux).

Open & extensible platform for integrated best-of-breed detection & response

Built entirely on open APIs, Carbon Black delivers an unmatched ability for responders to both "pull in" capabilities from other security solutions and threat intelligence as well as expose and "push out" the data captured by Carbon Black and its full feature set to third-party or homegrown security products. This delivers unparalleled security operations development capabilities to integrate with and build on top of Carbon Black for best-of-breed detection and response tailored for your organization.

Watchlists for real-time customized detection techniques that go beyond signatures

Through Carbon Black watchlists, responders can build robust and actionable detection by leveraging the combination of its continuous endpoint recording and instant, aggregated threat intelligence—delivered from the Bit9 + Carbon Black Threat Intelligence Cloud. This enables responders to reduce alert fatigue by receiving and designing advanced threat detection optimized for their organization.



Recorded history for instant root cause investigations

Carbon Black delivers an unmatched ability to instantly understand root cause—through a gapless recorded history and visualization of the entire attack kill chain—to respond and recover at the moment of discovery. This enables responders to immediately "roll back the tape" to identify root cause. This empowers security operations personnel to also learn from their investigations to improve future processes, procedures and security.

Bit9 + CARBON BLACK

Sensor Features

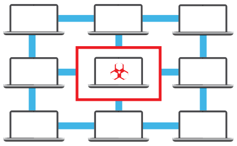
- CPU usage less than 1%
- RAM usage 20MB
- Network bandwidth 50 bytes per second on average
- Man-in-the-middle protection through bi-directional SSL authentication with server
- Centralized management, storage and control

Use Cases

- Breach preparation
- Malware detection
- Incident response
- Endpoint isolation
- Threat hunting
- Live response
- Threat banning
- Remediation

Supported Platforms

> "Carbon Black changes the dynamic of incident response."
>
> — *Digital Forensics Expert*



One-click endpoint isolation for immediate threat containment

Responders can instantly contain active intrusions remotely by isolating one or multiple endpoints from communicating with the network. By still maintaining an active connection with the Carbon Black server—even while isolated—IR teams can perform more conclusive and surgical investigations on or off the network.

Live response for endpoint threat inspection, termination & remediation

With live response, responders can understand the current state of an endpoint, perform remote live investigations, intervene with ongoing attacks, and instantly remediate endpoint threats. This enables incident responders to "look" and "touch" endpoints to take immediate action during an investigation—even while the endpoint remains isolated from the rest of the network.

Endpoint threat banning for instant attack disruption & recovery

With endpoint threat banning in Carbon Black, responders can instantly stop, contain and disrupt advanced threats as well as block the future execution of similar attacks. This expands Carbon Black's ability—along with its leading endpoint threat isolation and live response capabilities—to recover from advanced threats faster than any endpoint threat detection and response solution on the market.

Microsoft Enhanced Mitigation Experience Toolkit (EMET) Integration for improved detection & kill chain analysis

Carbon Black is the only endpoint threat detection and response solution that integrates with Microsoft's Enhanced Mitigation Experience Toolkit (EMET). This enables responders to correlate blocked exploitation attempts—from Microsoft EMET—with Carbon Black's collective intelligence to show key aspects of the attack both before and after the event. This empowers responders to optimize and improve their detection, investigations and patch management efforts by understanding the full kill chain of every exploitation attempt at the moment of compromise.

KPI dashboards for instant endpoint insight

With Carbon Black's dashboards, security teams gain instant insight into key endpoint and incident response performance indicators across their entire environment. This enables organizations to understand and articulate the state of their endpoint detection and response capabilities.

1: 2014 Verizon Data Breach Investigations Report

2: A SANS Survey, Incident Response: How to Fight Back, Alissa Torres, August 2014

3: NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims: A Study of Actual Claim Payo

ABOUT BIT9 + CARBON BLACK

Bit9 + Carbon Black provides the most complete solution against advanced threats that target organizations' endpoints and servers, making it easier to see—and immediately stop—those threats. The company enables organizations to arm their endpoints by combining continuous, real-time visibility into what's happening on every computer; real-time signature-less threat detection; incident response that combines a recorded history with live remediation; and prevention that is proactive and customizable. More than 1,000 organizations worldwide—from Fortune 100 companies to small enterprises—use Bit9 + Carbon Black to increase security, reduce operational costs and improve compliance. Leading managed security service providers (MSSP) and incident response (IR) companies have made Bit9 + Carbon Black a core component of their detection and response services.

20150327

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

SANS BEST OF 2014 WINNER IN End Point Protection

P 617.393.7400 F 617.393.7499 **www.bit9.com**