CARBON
BLACK

PARTNER SALES GUIDE
Zero-Gap Endpoint Protection

Partner Portal

The portal is where you'll find everything you need to sell Carbon Black.

Visit partners.carbonblack.com
- » Deal Registration
- » SPIF Portal
- » Sales Territory maps
- » Sales training, collateral, sales presentations, battle cards, marketing kits and other resources.

Contact Us

If you have questions don't hesitate to contact your CAM or sales rep, email us at channels@carbonblack.com, or call 855-525-2480.

Cb **DEFENSE**

Cb Defense is our powerful, light-weight next generation AV solution. Using a combination of endpoint and cloud-based technologies, Cb Defense stops more attacks than other NGAV products. Its analytic approach inspects files and identifies malicious behavior to block both malware and increasingly common malware-less attacks. Once malware is blocked, Cb Defense gives you full visibility into how the attack happened, if it was successful, if it's anywhere else in the enterprise, plus many more important answers.

Core Benefits

» Prevents attacks that evade traditional endpoint security
» Lightweight and non-disruptive
» Eliminate legacy anti-virus

| 1 | **Deploys in 15 Minutes** | 2 | **No Impact to Users** | 3 | **Windows MAC** | 4 | **CPU - <1% DISK - <1% NET - 3.5 Mb/d** |

Cb DEFENSE CASE STUDY

Social Media Enterprise Gains Visibility Without Sacrificing Speed

Problem

» Needed to improve their security posture with easy prevention

» Could not slow down their developer-heavy, dynamic organization

» Saw advanced threats target their organization regularly

Outcome

» Seamlessly integrated Cb Defense into their systems

» Saw no impact to productivity on developer machines

» Scalable and lightweight on Windows and Mac

» Gained visibility into endpoints

» Have had 0 breaches

Cb **PROTECTION**

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 regulatory-mandated highly-sensitive and targeted systems. More than 1,800 organizations globally rely on Cb Protection.

Core Benefits
» Stop attacks by allowing only approved software to run
» Automate software approvals via IT and cloud-driven policies
» Enterprise ready

HIGH:
Default Deny

MEDIUM:
Prompt User

LOW:
Execute & Track

Cb PROTECTION CASE STUDY

Healthcare Organization Ends Ransomware Attacks

Problem

» Needed protection against ransomware, specifically CryptoLocker

» Cb provided visibility that Cylance & CrowdStrike couldn't

Outcome

» Company was getting hit with CryptoLocker & other ransomware variants

» They had some issues with their critical infrastructure getting hit

» Evaluated Cylance and CrowdStrike in a POC

» Both claimed they could stop ransomware but couldn't show how

» CSO chose Carbon Black because of prevention & visibility

» Cb stopped the ransomware and showed how it was stopped

» Customer has had zero breaches since deployment

Cb **RESPONSE**

Cb Response is the most precise IR and threat hunting solution. All threat activity is captured and centralized so you can hunt threats in real time, visualize the complete kill chain, and then respond and remediate quickly. Investigations are accelerated because information you need is always available – even if you're breached after hours.

Core Benefits

» Complete endpoint visibility

» Reduced IT involvement

» Conclusive understanding of the attack

Cb RESPONSE CASE STUDY

Manufacturing Conglomerate Turns to
Carbon Black after AV Continues to Fail

Problem

» AV failed with 600+ compromises

» IT was working around the clock to remediate

Outcome

» 6 watch-lists through Cb Response did 90% of their detection

» Detected events in near real-time instead of 6-8 hours

» Accelerated root cause identification by 75%

Cb Defense Competitive Matrix

Yes 🟢 No 🔴 Limited 🟠

		CARBON BLACK	CYLANCE	CROWDSTRIKE	SentinelOne
STOP ATTACKS	Malware	🟢	🟢	🟠	🟠
	Malware-less & file-less	🟢	🟠	🟠	🟠
	Exploit Prevention	🟠	🟠	🟠	🟠
	Offline Protection	🟢	🟢	🟠	🟠
SEE THREATS	Investigate Discovered Attacks	🟢	🔴	🟢	🟢
	Behavioral Threat Analytics	🟢	🔴	🟢	🟢
	Threat Source / Root Cause	🟢	🔴	🟢	🟠
CLOSE GAPS	Kill Files and Processes	🟢	🔴	🔴	🟢
	Isolate Machine	🟢	🔴	🟢	🟢
	Rollback	🔴	🔴	🔴	🟠
LIGHTWEIGHT & EASY	Deploys in 15 Minutes	🟢	🟢	🟢	🟠
	<1% CPU, <1% Disk	🟢	🟢	🟢	🟢
	Minimal Administration	🟢	🟢	🟢	🟢

Cb Protection Competitive Matrix

Yes 🟢 No 🔴 Limited 🟠

		CARBON BLACK	McAfee	Lumension	Bromium
LOCK DOWN ENDPOINTS & SYSTEMS	Desktops, Laptops, Servers	🟢	🟢	🟢	🔴
	POS, ATM, SCADA, Fixed-Function	🟢	🟠	🟢	🔴
	"Dial-Up" Lock down Levels	🟢	🟠	🟢	🔴
PREVENT UNWANTED CHANGE	Integrated FIM	🟢	🔴	🟠	🔴
	Integrated Device Control	🟢	🟢	🟢	🟢
	Complete Change MGMT	🟠	🟠	🟠	🔴
	AV / HIPS Replacement	🟢	🔴	🟢	🟢
ACHIEVE CONTINUOUS COMPLIANCE	Continuous Recording	🟢	🔴	🔴	🔴
	Remote Investigation	🟢	🔴	🟢	🟢
	Auditor Attestation	🟢	🔴	🔴	🔴
	Regulatory Controls	🟢	🟢	🟢	🔴
LOW-TOUCH WHITELISTING	Automate Software Approval	🟢	🟠	🟠	🟠
	IT & Cloud-Driven Trust	🟢	🟢	🔴	🔴
	Process Isolation	🟠	🔴	🔴	🟢
	Network Detonation	🟢	🔴	🔴	🔴

Cb Response Competitive Matrix

Yes 🟢   No 🔴   Limited 🟠

		CARBON BLACK	CROWDSTRIKE	SentinelOne	TANIUM
CAPTURE ALL THREAT ACTIVITY	Continuous Recording of All Data	🟢	🟢	🔴	🟠
	Centralized Storage of All Data	🟢	🟠	🔴	🔴
	File, Registry, Network	🟢	🟢	🟢	🟢
HUNTS THREATS IN REAL TIME	10-Second Query Response Time	🟢	🟢	🔴	🟠
	Easy Threat Scope Investigation	🟢	🟠	🟠	🟠
	Integrated 3rd-Party Threat Intel	🟢	🟠	🟠	🔴
	Direct Query of Endpoint	🟠	🟠	🟠	🟢
	Community Detection	🟢	🔴	🔴	🔴
VISUALIZE THE ATTACK KILL-CHAIN	Expert-Level Technical Detail	🟢	🟢	🟢	🔴
	Dynamic Process Tree Visualization	🟢	🔴	🔴	🔴
	Full, Console-based Remediation	🟢	🔴	🟠	🔴
RESPOND & REMEDIATE	Malicious File Banning	🟢	🔴	🟠	🔴
	Attack Isolation	🟢	🔴	🟢	🟢
	Rollback	🟢	🟢	🟢	🟢
	Network Detonation	🔴	🔴	🟠	🟠

Next-Gen Endpoint Protection Simplified

Every organization has diverse requirements for keeping their endpoints protected against attacks, and the marketplace is a crowded space with no silver bullet. You may be wondering how to help your customers navigate through the solutions available in order to create the best security stack for their business - this grid can help.

Below are four important tools for a strong security posture and the point vendors that provide them.

Next-Gen AV	Endpoint Detection & Response	Application Control	Remediation
Carbon Black	Carbon Black	Carbon Black	Guidance
Cylance	SentinalOne	Microsoft	Mandiant
SentinalOne	Tanium	Bromium	
Palo Alto	Palo Alto		
CrowdStrike	CrowdStrike		
FireEye	FireEye		
FireAMP	FireAMP		

Identifying Opportunities

	Cb Defense	Cb Response	Cb Protection
Primary Market	**NGAV** mass market needing better security quick	**IR and Threat Hunting** high-performing SOC/IR teams	**Application Control** lock down endpoints, servers, fixed function devices
Key Use Cases	**AV Replacement** Advanced threat prevention Threat detection & response	**Incident Response** Threat hunting Customizable detection Complete visibility	**Lock down/ Whitelisting** PCI / compliance Server security Fixed Function / POS security OS EOL projects
Deployment Options	**SaaS**, MSSP	**SaaS**, on-prem, or MSSP	**On-prem** or MSSP

Integration is Easy with Carbon Black

Open API, Automation and Orchestration

NETWORK SECURITY

BLUE COAT · Check Point SOFTWARE TECHNOLOGIES LTD. · DAMBALLA · CYPHORT · FIDELIS CYBERSECURITY

FireEye · Infoblox CONTROL YOUR NETWORK · lastline · paloalto NETWORKS

SIEM & ANALYTICS

CLICK SECURITY · exabeam · hp · IBM · LogRhythm · RSA SECURITY · splunk>

THREAT INTELLIGENCE

BrightPoint SECURITY · DAMBALLA · NIST · iSIGHTPARTNERS · Microsoft

THREAT CONNECT · THREATQUOTIENT · THREATSTREAM · Tor