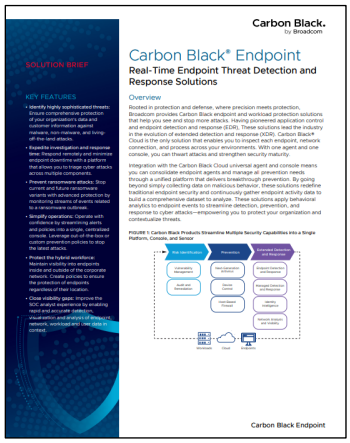
Carbon Black.
by Broadcom

carahsoft.



Carbon Black Endpoint

Real-Time Endpoint Threat Detection and Response Solutions

Thank you for downloading this Broadcom Solution Brief. Carahsoft is the distributor for Broadcom Cybersecurity solutions available via Illinois Public Higher Education Cooperative (IPHEC), North Carolina Endpoint Protection Contract 208M, Educational Software Solutions and Services – OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring Broadcom's solutions, please check out the following resources and information:

For additional resources:
carah.io/BroadcomResources

For upcoming events:
carah.io/BroadcomEvents

For additional Carbon Black solutions:
carah.io/CBSolutions

For additional Cybersecurity solutions:
carah.io/CybersecuritySolutions

To set up a meeting:
Broadcom@carahsoft.com
(571) 662-3260

To purchase, check out the contract vehicles available for procurement:
carah.io/BroadcomContracts

For more information, contact Carahsoft or our reseller partners:
Broadcom@carahsoft.com | 571-662-3260

Carbon Black.
by Broadcom

SOLUTION BRIEF

Carbon Black® Endpoint

Real-Time Endpoint Threat Detection and Response Solutions

KEY FEATURES

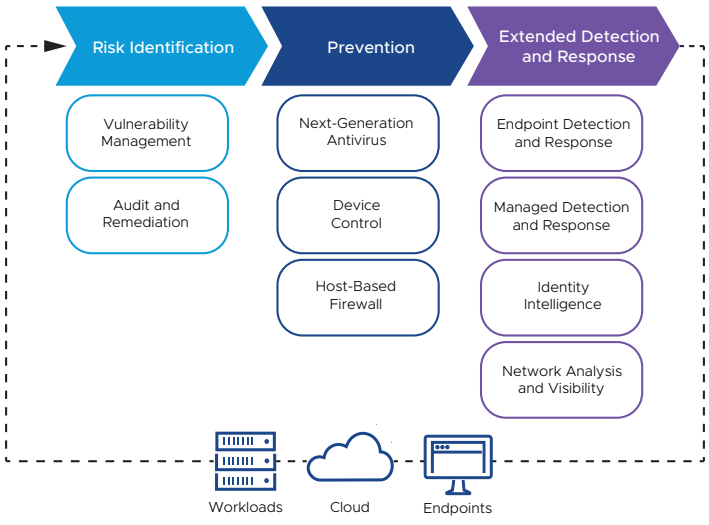
- **Identify highly sophisticated threats:** Ensure comprehensive protection of your organization's data and customer information against malware, non-malware, and living-off-the-land attacks.
- **Expedite investigation and response time:** Respond remotely and minimize endpoint downtime with a platform that allows you to triage cyber attacks across multiple components.
- **Prevent ransomware attacks:** Stop current and future ransomware variants with advanced protection by monitoring streams of events related to a ransomware outbreak.
- **Simplify operations:** Operate with confidence by streamlining alerts and policies into a single, centralized console. Leverage out-of-the-box or custom prevention policies to stop the latest attacks.
- **Protect the hybrid workforce:** Maintain visibility into endpoints inside and outside of the corporate network. Create policies to ensure the protection of endpoints regardless of their location.
- **Close visibility gaps:** Improve the SOC analyst experience by enabling rapid and accurate detection, visualization and analysis of endpoint, network, workload and user data in context.

Overview

Rooted in protection and defense, where precision meets protection, Broadcom provides Carbon Black endpoint and workload protection solutions that help you see and stop more attacks. Having pioneered application control and endpoint detection and response (EDR), These solutions lead the industry in the evolution of extended detection and response (XDR). Carbon Black® Cloud is the only solution that enables you to inspect each endpoint, network connection, and process across your environments. With one agent and one console, you can thwart attacks and strengthen security maturity.

Integration with the Carbon Black Cloud universal agent and console means you can consolidate endpoint agents and manage all prevention needs through a unified platform that delivers breakthrough prevention. By going beyond simply collecting data on malicious behavior, these solutions redefine traditional endpoint security and continuously gather endpoint activity data to build a comprehensive dataset to analyze. These solutions apply behavioral analytics to endpoint events to streamline detection, prevention, and response to cyber attacks—empowering you to protect your organization and contextualize threats.

FIGURE 1: Carbon Black Products Streamline Multiple Security Capabilities into a Single Platform, Console, and Sensor



APPLICATIONS

- **Ransomware protection:** Lure all types of ransomware into a trap with advanced prevention capabilities.
- **Enterprise AV replacement:** Centralize prevention capabilities.
- **Dwell time reduction:** Accelerate detection and response.
- **Threat hunting:** Make it harder for adversaries to hide.
- **Industry requirements and compliance:** Meet industry requirements and prove security control assurance.

Risk Identification

Vulnerability Management

Vulnerability management provides risk-prioritized visibility and context into the vulnerabilities present on endpoints and workloads. Security teams can make quick and confident decisions and harden systems to effectively increase security posture and thwart the most critical vulnerabilities in their environments.

Audit and Remediation

Audit and remediation provides real-time device assessment and remediation, giving teams faster, easier access to audit and change the system state of endpoints. Make quick and confident decisions to harden systems and improve security posture.

Prevention

Next-Generation Antivirus

Next-generation antivirus (NGAV) and behavioral EDR solutions protect against the full spectrum of modern cyber attacks. Using the universal agent and console, these solutions apply behavioral analytics to endpoint events to streamline detection, prevention, and response to cyber attacks.

Host-Based Firewall

Enable security operations center (SOC) teams to further consolidate legacy security stacks by eliminating legacy endpoint solutions. Host-based Firewall replaces legacy firewall solutions with a lightweight, rule-based solution that's easy to manage and scale. Govern network behaviors of applications across endpoints in your environment.

Device Control

Device control helps provide the insights and granular control required to enable safe USB device use. Protect against external and internal threats across your organization.

Extended Detection and Response

Managed Detection and Response

Gain essential visibility into attacks with managed detection and response, built directly on the Carbon Black Cloud platform. A world-class team of security experts monitor and analyze data in Carbon Black Cloud by using advanced ML and algorithmic toolsets and recommend policy changes needed to remediate threats.

Enterprise EDR

This advanced threat hunting and containment solution delivers continuous visibility for top SOC and incident response (IR) teams. Enterprise EDR empowers teams to respond and remediate in real time, stopping active attacks and repairing damage quickly.

Network Analysis and Visibility

Visualize and analyze network data in context using Carbon Black Cloud. With native network telemetry, XDR includes continuous capture and analysis of network fingerprints, flow, TLS data, and application protocol data. Additionally, IDS observations instantly identify malicious network behaviors without opening a case, switching consoles, or changed context.

Identity Intelligence

Identity intelligence, also known as authentication events, provides insight into the activity of user accounts for context, correlation and analysis. Get insights on log on, logoff events, account changes, privilege escalation, and how local domain accounts are being used on the network.

Open APIs and Third-Party Integrations

Broadcom has an extensive ecosystem of strategic partners. As a member of the XDR Alliance, these products deliver out-of-the-box integrations with industry-leading vendors across domains, including Splunk, ServiceNow, Proofpoint, and IBM. These pre-built integrations and open APIs extend the value of your endpoint protection platform to the rest of your tools and enrich existing workflows.

Helps Fix Security Blind Spots

Carbon Black solutions empower top security teams to fix the security blind spots they face today. Specific directed attacks are now the cyber-crime norm, and no business is exempt. There's increasing cyber-insurance scrutiny, and government regulations continue to get stricter. In this context, security teams can no longer rely on general security platforms alone. Rather, teams must be empowered with deeper visibility and more control to tailor response to their unique environment. With Carbon Black solutions, security teams have unprecedented ability to see directed attacks, contain potential impact, change policies with no user interruption, prevent repeat incidents, and measure what they stopped.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

CB-Endpoint-SB100 December 17, 2024