Carbon Black.
by Broadcom

SOLUTION BRIEF

AT A GLANCE

- Neutralize known and unknown threats by combining static and behavioral detections
- Eliminate analyst fatigue with automated responses to suspicious behavior
- Proactively prevent threats by extending your endpoint visibility

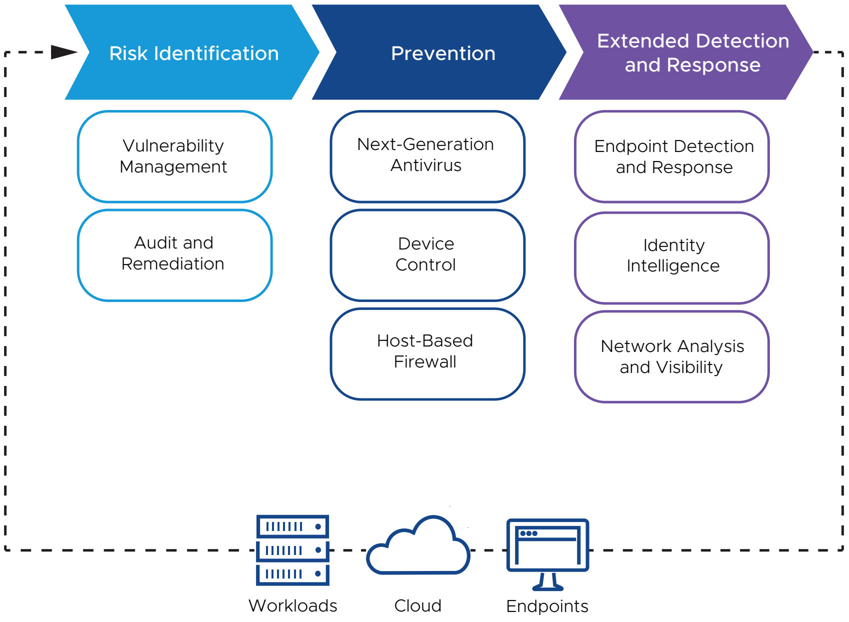
Carbon Black Endpoint

Real-time endpoint protection, detection and response solution

Rooted in protection and defense – where precision meets protection Carbon Black® is a leader in endpoint and workload protection that helps you see and stop more attacks. Having pioneered application control and endpoint detection and response (EDR), 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, Carbon Black 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 cyberattacks—empowering you to protect your organization and contextualize threats.

FIGURE 1: Carbon Black streamlines multiple security capabilities into a single platform, console and sensor.



48%

increase in reported ransomware attacks in 2023.[1]

68%

of security chiefs fear a "material cyberattack" on their organization in the next 12 months.[2]

95%

of ransomware incidents result in a loss between $1 and $2.25 million.[3]

Risk identification

Vulnerability management

Carbon Black Cloud 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.

Live Query

Carbon Black Cloud Live Query 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 cyberattacks. Using the Carbon Black Cloud universal agent and console, these solutions apply behavioral analytics to endpoint events to streamline detection, prevention, and response to cyberattacks.

Host-based firewall

Enable security operations center (SOC) teams to further consolidate legacy security stacks by eliminating legacy endpoint solutions. Carbon Black™ Cloud 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.

> "Our time to value was almost instantaneous. I'm spending less time tracking down false positives and spending more time triaging and acting on threats."
>
> **Jeremy Wilkins, Security Technology Administrator, OFS**

[1] Thales Group. "2023 Thales Data Threat Report." April 2023.

[2] Proofpoint. "2023 Voice of the CISO." May 2023.

[3] Verizon. "2023 Data Breach Investigations Report." June 2023.

Extended detection and response

Enterprise EDR

This advanced threat hunting and containment solution delivers continuous visibility for top SOC and incident response (IR) teams. Carbon Black 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, Carbon Black eNDR™ 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

Carbon Black has an extensive ecosystem of strategic partners. As a member of the XDR Alliance, Carbon Black delivers 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. Carbon Black also powers products and services globally for top incident response, channel, and OEM partners.

Use Cases

- 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.

Carbon Black Cloud by the numbers[4]

427%

ROI over three years

$2.3M

cost savings from faster investigation and remediation

75%

reduction in mean time to resolution (MTTR)

40%

risk reduction of a large-scale security breach

[4] A commissioned study conducted by Forrester Consulting on behalf of Carbon Black. “The Total Economic Impact™ Of Carbon Black Cloud.” December 2023.

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 cyberattacks 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.

Carbon Black Helps Fix Your Security Blindspots

Carbon Black empowers top security teams to fix the security blindspots they face today. Specific directed attacks are now the cybercrime 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, 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.

Carbon Black.
by Broadcom

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