Carbon Black.
by Broadcom

Product Brief

Carbon Black® App Control

Positive Security Model Permits Only Trusted Software

Key Features

- Application Control
- File Integrity Monitoring and Control
- Device Control
- Memory Protection
- Registry Protection
- Application Catalog Inventory
- Common Platform Enumeration (CPE)
- Rapid Configurations
- Content-Based Inspection
- Process Hollowing Protection

Benefits

- Stop malware, ransomware, and next-gen attacks
- Reduce unplanned downtime across critical infrastructure
- Consolidate endpoint agents
- Prevent unauthorized changes to system configurations
- Streamline IT audits and satisfy controls across major regulatory mandates
- Protect legacy systems running on end-of-life (EOL) operating systems
- Gain total visibility to identify all software running in critical environments
- Prevent unauthorized data writes and exfiltration to unsanctioned devices

Overview

Today's cyber threats move faster than ever. Financially motivated actors and nation-states leverage AI to move laterally in under 48 minutes, driving average breach costs in financial services past $6M. Meanwhile, security teams face severe talent shortages, alert fatigue, and tool sprawl that creates dangerous visibility silos. These blind spots force a reactive posture—leaving teams unable to contain sophisticated threats like ransomware (now 44% of breaches) before damage occurs.

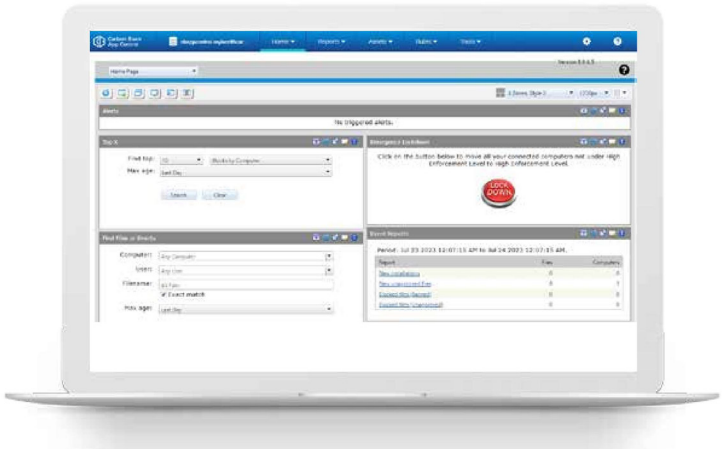
Organizations cannot afford the downtime, lost productivity, or reputational damage that follows a breach. As attacks become more frequent and targeted, one question remains: How can teams best protect modern servers and endpoints?

Security relies on two core models: positive and negative. Negative security detects and blocks known-bad activity, offering a proven baseline defense against established viruses, worms, and signatures. But sophisticated, modern attacks are designed to bypass these traditional controls. The negative security model isn't bad—it's essential. But on its own, it isn't enough.

A positive security model identifies software with a verified level of trust, allowing access only to approved resources. Under this model, unknown software is untrusted by default and must be explicitly vetted before execution. By design, the classic positive security model permits only known-good applications and activities.

Carbon Black® App Control uses a positive security model to protect critical systems across on-premises, private cloud, and public cloud environments. This prevents unauthorized changes and ensures continuous regulatory compliance.

Figure 1: Prevent Unauthorized System Changes with Carbon Black App Control



Use Cases

- Lock down systems on-premises, in private clouds, or in public clouds
- Secure fixed-function devices
- Protect EOL operating systems
- Secure air-gapped systems

Platform Support

Sensor support:

- Windows XP, Server, Embedded/POS, ARM64
- macOS
- Linux:
  - Red Hat Enterprise Linux (RHEL)
  - Oracle Linux (RHCK)

A Holistic Approach to Positive Security

Carbon Black App Control delivers a holistic positive security model through the following core capabilities:

- Application Control: Uses allowlisting and denylisting to enforce granular rules on how applications execute and interact with system resources.
- File Integrity Monitoring and Control (FIM/FIC): Tracks alterations to sensitive files, registry keys, and host operating system folders. FIM alerts on unauthorized changes, while FIC actively blocks them.
- Device Control: Regulates data transfers to and from external media, such as USB drives. Granular access rules allow organizations to permit or restrict device connections based on specific users, groups, or schedules.
- Memory Protection: Enforces strict memory access boundaries—preventing malicious processes from reading or injecting code into unauthorized memory space.
- Registry Protection: Locks down system-critical Windows registry keys against tampering. By reporting or blocking unauthorized modifications, it prevents attackers from establishing persistence or corrupting essential OS configurations.

Flexible Deployment

As organizations migrate workloads to the cloud, legacy and specialized systems often become vulnerable blind spots. Many enterprises still rely on critical infrastructure running on air-gapped servers, proprietary software, or end-of-life (EOL) operating systems.

Carbon Black App Control provides a unified positive security approach across all these environments—whether deployed in an on-premises data center, Amazon Web Services (AWS), Microsoft Azure, or hosted private clouds.

A cloud-only security solution cannot adequately protect:

- Air-gapped systems completely isolated from the public internet
- Fixed-function devices such as ATMs, point-of-sale (POS) terminals, kiosks, and medical machinery
- Legacy and EOL operating systems including Windows XP, Windows Server 2003, and Windows Server 2008
- Mission-critical servers running proprietary applications and high-value data

Trusted Content Approval

Carbon Black App Control avoids the overhead of manually maintaining hash allowlists, which quickly become outdated. Instead, it employs a trust-based approach comprising multiple automated mechanisms to approve clean software without friction. This makes establishing a positive security posture seamless and sustainable:

- IT and Cloud-Driven Trust: Leverages pre-approved trusted directories alongside real-time cloud threat intelligence and reputation scores.
- Trusted Publishers: Allows organizations to automatically trust signed software from reputable vendors (such as Microsoft, Google, or Adobe).
- Custom Rules: Provides granular control to approve files based on path, process, user, or publisher attributes.
- External Integrations: Automatically routes unknown files for static or dynamic analysis, then approves or bans them based on results using event rules.

Summary

Carbon Black App Control locks down your environment, prevents unauthorized changes, and ensures continuous compliance with regulatory mandates. By enforcing a default-deny positive security model, it protects critical systems against sophisticated threats that evade traditional defenses.

Rather than relying on rigid, easily outdated hash lists, Carbon Black App Control automates software approvals using cloud-driven intelligence, trusted publishers, custom policy rules, and integrated file analysis.

The result is complete control over your critical infrastructure—giving security teams true peace of mind.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CB-AppControl-PB101 July 23, 2026