Carbon Black.

WHITEPAPER

Moving Endpoint Security to the Predictive Cloud

Endpoint Security Is Broken

Traditional antivirus (AV) vendors aren't keeping up with today's threats. They don't protect against unknown attacks until it's too late, forcing security teams to scramble for new products every time a new wave of attacks hits. This reactive approach has resulted in too many tools on the endpoint that don't work together — stretching security professionals to their breaking point.

Meanwhile, endpoints cluttered with resource-hogging agents hinder productivity to the point where frustrated end users take matters into their own hands by uninstalling antivirus, leaving their device vulnerable to even the most common malware.

This situation won't be fixed with legacy products and the outdated architecture on which they run. A whole new approach to endpoint security is required, built on big data and real-time analytics in the cloud.

WHERE LEGACY ENDPOINT SECURITY FALLS SHORT

Limited to known attacks

Legacy antivirus suites rely primarily on malware signatures and behavioral rules to detect attacks. These reactive technologies only work for known, executable-based threats; attackers easily work around them.

Unprepared for new threats

Attackers are getting more sophisticated, incorporating government-leaked exploits, fileless techniques, and "living off the land" attacks that use the operating system itself for malicious purposes. Legacy antivirus rarely detects or stops these tactics.

Complex to manage

The typical antivirus suite contains at least five independent technologies (signatures, firewall, host IPS, device control, app control, etc.) that admins must keep up to date. Unfortunately, these policies are so complex that they are often misconfigured, rendering them useless.

Provides no information

When a security solution detects a threat, it should provide information to help you stop that threat from happening again. Yet legacy antivirus was never built with this in mind. As a result, regularly exploited security gaps never get fixed.

The Future of Endpoint Security is the Cloud

SECURITY MEETS BIG DATA

Technology has certainly empowered the adversary, across far more attack surfaces than just endpoints alone. In fact, many other security disciplines have been forced to adapt to increasingly sophisticated attacks — and when they do, they all turn to the same foundation: big data.

The analogy is as simple as moving from a lock on a door to a video surveillance system, but we see it manifest in many different ways. Consider these examples:

Credit Card Fraud Detection
Instead of relying on the cardholder to check his or her bill, credit card companies use big data to detect fraud through large-scale analysis of every transaction in real-time.

Online Authentication
Passwords are vulnerable, and two-factor authentication is obtrusive. That's why some websites now validate identity by analyzing users' behaviors and matching them to a usage profile.

Spam Filtering
Web-based spam filtering systems look across billions of messages and metadata to find spam and spammers.

Security systems that capture, centralize, and analyze data are far more effective than those that perform a spot check at a single point in time. In short, the better your data, the better your protection.

IT'S TIME FOR ENDPOINT SECURITY TO CATCH UP

For too long, endpoint security has followed the antiquated "point-in-time" security model: if the executable doesn't match a known malware signature, let it run.

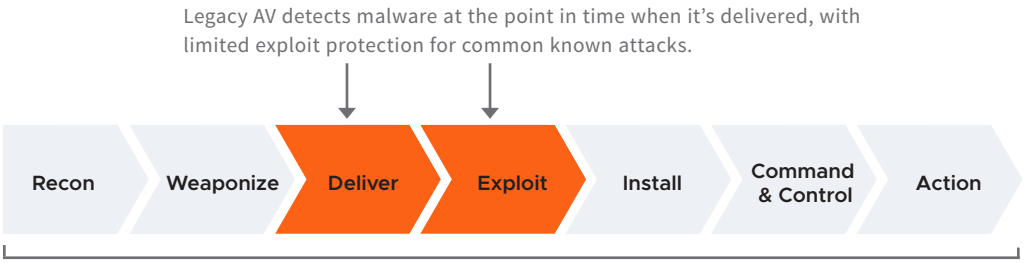
It's now time for endpoint security to move to a new model built on big data in the cloud. Only by applying the unlimited processing power and scale of the cloud to the endpoint security problem can we keep up with — and even predict — the threats coming our way.

The Cloud Is Predictive: Better Security

The key flaw in antivirus is the assumption that if it finds malware, it has stopped the threat. In fact, that is not at all the case. Malware is just one piece of the attack — and not always a necessary one.

This rudimentary view of how attacks work is too reactive to be successful in today's fast-changing threat landscape. In the days it takes to define and deploy a signature, the damage has already been done.

Consider what's possible with the cloud. The cloud can monitor an endpoint's behavior, looking at both normal and abnormal activity, and compare that activity to vast stores of data from other endpoints. By analyzing these event streams across all endpoints under management through a process known as **streaming analytics**, the cloud creates a global threat monitoring system, allowing it to detect and predict attacks — even if they've never been seen before.



Attackers leverage the entire kill chain to execute an attack – when malware gets blocked, they find a way around and keep going.

This is only possible if the endpoint solution does not filter data before going to the cloud. Many endpoint solutions only send data related to threats they've detected. **Unfiltered data collection**, on the other hand, gives the cloud the opportunity to analyze data it otherwise wouldn't, enabling the detection of unknown threats hiding in what looks like normal event streams.

Each **endpoint** in an organization generates anywhere between **10,000 and 40,000** individual **events** on a **daily basis**.

The cloud delivers **faster, more accurate protection**:

Threat Prediction

Discovers new threats through unfiltered data collection and streaming analytics

Global Threat Monitoring

Every endpoint under management becomes part of a worldwide threat monitoring system

Real-time Intelligence

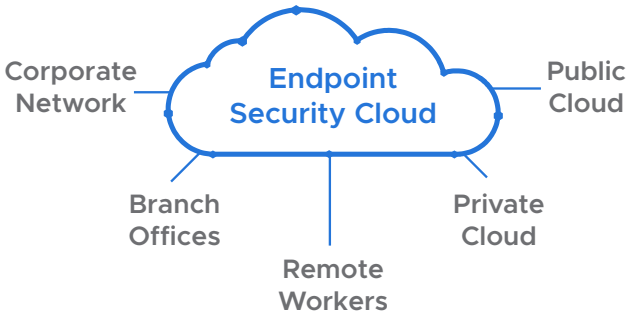
Shares detections, trends, and key threat intel across all endpoints within seconds

The Cloud Is Easy: Simplified Operations

The cloud has been a transformative force across many disciplines within IT, and **security is no different**.

Infrastructure is inherently costly to manage, but what makes it even more challenging for security professionals is the impact that lapses in proper maintenance can have on security effectiveness. The threat landscape is changing so quickly that a security system left unpatched, misconfigured, or without the latest enhancements creates substantial risk.

Running endpoint security natively in the cloud greatly simplifies its operation, resulting in a number of benefits.



First, managing the system becomes much, much easier. All the costs and complexity related to infrastructure management disappear — storage, operating systems, hotfixes, VPNs — meaning you can deploy faster and spend money your where it counts.

This has an especially big impact when it comes to systems outside the corporate network. It's notoriously difficult to keep antivirus running smoothly in branch offices and among the mobile workforce. When managed from the cloud, these systems are treated no differently than those at the main office, equipped with the same high level of protection no matter where in the world they are.

Perhaps most importantly, the cloud keeps your security system up to date. Whether simple definitions of new threats or entirely novel detection algorithms for advanced attacks, the cloud takes the burden of these updates off the shoulders of the admins, deploying new enhancements automatically and regularly.

The cloud delivers a **simplified operational experience**:

No Infrastructure

Eliminates the need for on-premise hardware, saving time, money, and effort

Easy for Mobile Workforce

Keeps every endpoint protected, even when not connected to the corporate network

Automatic Updates

Delivers the latest security enhancements regularly, without requiring significant IT effort

Choosing the Right Cloud

In an attempt to take advantage of the clear benefits that come with cloud computing, many traditional endpoint security vendors have begun offering cloud versions of their solutions. However, not all security clouds are built the same.

In fact, most cloud-based antivirus options available today are retrofit solutions that have simply migrated their on premises products to vendor-managed servers. Under the covers, they still operate with the same outdated technologies that only protect against malware threats after they have been discovered. Customers are left with weak protection in a rapidly accelerating threat landscape.

On the other hand, a cloud built on bi-directional communication with endpoints, where endpoint data is sent to a cloud-based big data and real-time analytics engine, transforms the endpoint environment into a global threat monitoring system. The cloud is predictive, able to discover threats never seen before and provide protection from sophisticated attacks to every endpoint under management.

When evaluating your next endpoint security solution, the following table will help you determine if the cloud solution you are looking at will deliver on the full promise of cloud computing for security.

HOW TO CHOOSE THE RIGHT CLOUD

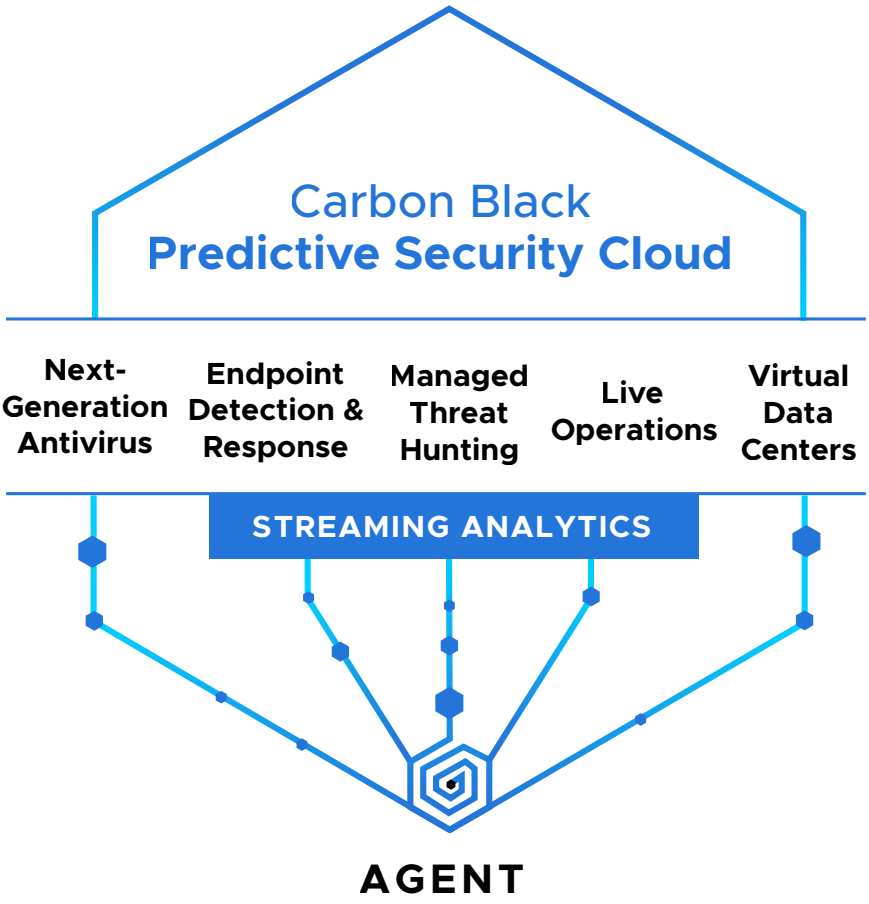
	Traditional AV (Retrofit Cloud)	Next-Gen Endpoint Security (Big Data Cloud)
Threat Detection	**Malware Only** Focuses on executable-based threats.	**Malware and Fileless** Detects executable-based threats as well as advanced attacks that don't use malware.
Endpoint Communications	**Broadcast** "Black-box" threat information is broadcast one-way to endpoints, with no data collected from them.	**Bi-directional** Threat data is exchanged back and forth between endpoints and the cloud, creating a global threat monitoring system.
Data Collection	**None** Endpoint data is not sent to the cloud, leaving users with no context about security events.	**Unfiltered** Endpoint telemetry is sent to the cloud, providing a complete contextual picture for investigation and remediation.
Security Posture	**Reactive** Protects against known threats and limited attack behaviors.	**Predictive** Discovers new threats never seen before and protects against them.
Updates	**Manual and Delayed** The customer is responsible for applying updates, keeping policies configured correctly, and deploying new defense techniques when they are available.	**Automatic and Real Time** Every endpoint benefits from new defense techniques and algorithms deployed natively in the cloud, along with easy, lightweight agent updates.

Introducing the Cb Predictive Security Cloud

The Cb Predictive Security Cloud (PSC) is a converged endpoint protection platform delivering next-generation security services through the cloud.

Built with big data and real-time analytics at its core, the Cb Predictive Security Cloud is transforming endpoint security through the power of the cloud. Through a single lightweight agent and a single console, customers can activate a variety of endpoint security services to meet a broad set of security needs.

The best data yields the best protection. That's why the PSC collects unfiltered data from endpoints — only in that unfiltered data can you find threats that other solutions miss. By applying streaming analytics to that data, consisting of behavioral analytics, machine learning, reputational scoring, and more, the PSC is able to predict threats never seen before.



Every Carbon Black product leverages this same unfiltered data set and streaming analytics architecture to deliver next-generation protection from advanced attacks:

Cb Response — Threat hunting for SOCs and IR teams

Cb Defense — Next-gen AV + EDR to replace AV

Cb Defense for VMware — Next-gen AV + EDR optimized for virtual data centers

Cb ThreatSight — 24x7 managed threat hunting

Cb Protection — Application control for servers and critical systems

The Best Data Yields the Best Protection

BETTER SECURITY

Cb Defense, a native PSC service, delivers converged prevention, detection, and response through unique streaming prevention technology that stops both malware and fileless attacks, including specialized protection from ransomware, script-based attacks, PowerShell attacks, and living-off-the-land attacks.

Cb Defense for VMware delivers the same powerful capabilities, optimized for application-centric virtual data centers. Finally, with 24x7 coverage from expert threat hunters, the Cb ThreatSight managed service helps you stay on top of your environment to identify threats and prevent breaches.

SIMPLIFIED OPERATIONS

The PSC solves one of endpoint security's most frustrating challenges — complexity — through a single, lightweight agent. Deployment is simple, and once deployed you can activate any service on the PSC without additional technology.

The PSC presents a unified workflow across all services, making it easy to use and easy to configure. Finally, as the cloud is enhanced with updated detection algorithms and entirely new services, you'll always stay up-to-date with the latest protection.

UNIFIED ECOSYSTEM

The most effective security strategy requires integration across all facets of the security stack, incorporating as much data as possible to identify advanced threats and protect against them.

The Cb Predictive Security Cloud supports an open API framework that, with the support of active communities for both security developers and security practitioners, makes its data easily accessible for every security solution to use.

Conclusion

In an industry solely focused on staying a step ahead of the adversary, the reactive signature-based approach of traditional antivirus has long outlived its shelf life. Organizations need to shift their endpoint security away from this outdated technology to cloud solutions built on big data and real-time analytics.

The Cb Predictive Security Cloud makes next-generation security possible in a way that no other single solution is currently able to do.

- Better protection through unfiltered data collection and streaming analytics to predict and prevent emerging threats
- Simplified operations through a single, lightweight agent that supports a variety of innovative endpoint security services
- A unified ecosystem that enables integration across the security stack, supported by active developer and practitioner communities

Now is the time for your organization to begin assessing its endpoint security strategy and to plan the move to a cloud-based solution, built on big data and analytics, ushering in the next-generation of protection.

To see the power of the Cb Predictive Security Cloud first hand, sign up to **attend a live demo of Cb Defense** — our cloud-native solution for next-generation AV and endpoint detection and response.

Carbon Black.

Carbon Black is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 30 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its newly introduced big data and analytics cloud platform - the Cb Predictive Security Cloud - Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.

For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

www.carbonblack.com