Carbon Black.

Getting More from Less

Simplifying Endpoint Security With a Cloud Delivered Platform

Introduction

IT and security professionals know that the threat landscape is dynamic. Everyday, attackers are getting smarter and coming up with new techniques to avoid detection. With non-malware and in-memory attacks now making up 70% of breaches[1], traditional antivirus (AV) is no longer enough to keep systems safe. In fact, less than a third of organizations believe traditional AV can stop the advanced ransomware attacks that are so prevalent today[2].

To combat this increased risk, many organizations are adding more products onto their existing security stack, increasing the cost and complexity of their environments. Today, 48% of businesses are using more than 25 different discrete or point security tools to manage, investigate and respond to security threats[3]. Unfortunately, this complexity doesn't correlate with efficacy for several reasons.

1. **TOO MANY SILOS**
   It's not enough to have a variety of solutions if they don't have the capability to work together. Organizations are working with data, systems and consoles that all operate in isolation. In the event of an investigation, professionals must work with disparate datasets from multiple security solutions. This is an arduous and time-consuming task that ultimately doesn't give enough insight into the context around the incident.

2. **COMPLICATED MANAGEMENT**
   Having a variety of systems and products is a burden to IT and security professionals. It's unnecessarily complex, and requires a great deal of training. In fact, over 50% of organizations that deploy 50+ security solutions define their security orchestration as "very challenging" and, because of this, nearly half (49%) of legitimate alerts are not remediated[4]. This translates into significant risk to the organization because people are spending less time on what really matters.

3. **ENDPOINT PERFORMANCE IMPACT**
   Running multiple systems is taxing to endpoints. The more agents that are added to them, the slower they become. Antivirus scans and other protection models require excessive processing power and, if an issue does occur, the limited visibility provided by these systems creates a huge productivity drain — especially if machines need to be reimaged. Some users will simply turn off their endpoint security altogether — a situation that at best puts them in noncompliance and, at worst, opens the door for a major breach.

[1] Data Breach Investigations, Verizon, 2018
[2] The State of Endpoint Security Risk, Ponemon Institute, 2017
[3] Cybersecurity Operations Challenges and Strategies, ESG Research, 2018
[4] Annual Cybersecurity Report, Cisco, 2018

Most IT and security teams struggle to hire enough qualified security personnel. Only 30% of organizations rate the skill level of their security staff as more than adequate5. Additionally, professionals that run multiple, siloed solutions often spread their limited personnel too thin to be effective. With a marketplace this scarce, skilled resources need to be highly focused on core security activities, not burdened with trying to piece information together from a variety of disparate systems.

Further contributing to these staffing challenges, IT and security teams have different mandates. Too frequently, these professionals are caught up in a backand-forth around the trade-offs of adding a new security tool. IT professionals are focused on the performance of machines and the productivity of end users, while security professionals are worried about having the right information and control to stop attacks and keep data safe. When security wants to add a new tool that requires a new agent to be deployed, IT will often push back, requiring the security team to either replace an existing agent or spend time making a strong case around the value the new product will provide to the company. This type of negotiation can turn into a political dispute between departments that ultimately negatively impacts both of their primary roles.

THE BOTTOM LINE IS THIS:
IT AND SECURITY PROFESSIONALS WANT TO DO MORE, BUT THEY ARE LIMITED BY PERSONNEL, RESOURCES AND THE IMPACT THAT ADDING MORE TOOLS AND AGENTS WILL HAVE ON THEIR ENDPOINTS.

Organizations need a simpler more flexible solution — one that can remove the friction between IT and security uniting all the teams in a company with a common source of truth. They need a solution that is easy to set up and use flexible enough to support a wide range of endpoint security services customizable enough to fit the specific needs of each organization and easy to expand and grow with their needs and security maturity without adding additional agents deployment or training.

[5] Cybersecurity Operations Challenges and Strategies, ESG Research, 2018

CB Predictive Security Cloud®

Consolidated Endpoint Security, Simplified

At Carbon Black we understand the current state of endpoint security and have built a solution that is uniquely positioned to meet today's needs. The CB Predictive Security Cloud (PSC) is an endpoint protection platform that consolidates security in the cloud making it easy to prevent investigate remediate and hunt for threats. Instead of needing to deploy a variety of products each with their own setups configurations and policies the PSC delivers multiple security capabilities through a common cloud-delivered platform that shares one sensor one console and one dataset. As requirements change adding new services is fast and easy eliminating the need for additional CapEx investment or the need to deploy new agents.

The platform is built on a comprehensive endpoint dataset that can be used and shared across tools and services — whether provided by Carbon Black or other vendors. This creates a single source of truth and adds context to security across the board. Additionally the PSC was constructed with the understanding that security needs grow and change as the threat landscape evolves. Because of this the platform supports the addition of new or custom solutions over time.

"ONE OF OUR GOALS WAS TO CONSOLIDATE OUR SECURITY PRODUCTS. WHAT CARBON BLACK WAS ABLE TO DO WAS BRING MULTIPLE SYSTEMS INTO ONE. THE FACT THAT IT'S KEEPING UP WITH THE LATEST THREATS OUT THERE REALLY MADE IT A DIFFERENTIATOR FROM THE OTHER SOLUTIONS WE LOOKED AT."

– WILLIAM BOCASH IT MANAGER | STONEWALL KITCHEN

Our Differentiator:
Behavioral Analytics

A Surveillance Camera on the Endpoint.

At Carbon Black, we focus on understanding attackers' behavior patterns, enabling us to detect and stop never-before-seen attacks in real time. How can a fileless attack be prevented without understanding the way it was executed? How can something previously unseen be recognized with only historical attack data? In order to provide the best security, it's important to understand how attackers operate. This is why behavioral analysis is at the foundation of everything we do.

To enable this analysis, we collect comprehensive endpoint data. Rich data — and the deep visibility it provides — is the foundation of strong endpoint security.

The CB Predictive Security Cloud platform is unique. Most endpoint security solutions begin recording data only when they determine an activity is suspect. This approach often misses earlier activities that are essential to determining root cause. When a problem arises, whether it's with endpoint security or IT hygiene, it's difficult to rapidly investigate the issue, or gain insight into new attack patterns. In contrast, the PSC continuously looks at endpoint activity, regardless of if it seems good or bad, and analyzes the behaviors. This gives security professionals the context and confidence they need to defend their systems.

Carbon Black has spent the better part of a decade developing and refining the ability to reliably collect, cost-effectively analyze and securely store massive amounts of data, without disrupting the network. Leveraging the power of the cloud, we are able to analyze more than 200 terabytes of endpoint data and over 500 billion security events on a daily basis — that's 13 times the number of iMessages processed and 150 times the number of Google searches in the same period. These powerful analytics give power to the many endpoint security services offered on the PSC.

200
TERABYTES
OF ENDPOINT DATA ARE ANALYZED IN THE CLOUD

500
BILLION
SECURITY EVENTS ARE ANALYZED DAILY

THAT IS

13X
THE NUMBER OF IMESSAGES PROCESSED

150X
THE NUMBER OF GOOGLE SEARCHES IN THE SAME PERIOD

Our Differentiator:
Superior Protection

Stop More Attacks, Take Back Control Over Endpoints and Worry Less.

Our unique approach provides a advantage when it comes to protecting endpoints. By analyzing attackers' behavior patterns the PSC can stop attacks whether they've been seen before or not and gives visibility into how these attacks evolved over time. This visibility allows us to detect new forms of attack constantly evolve our security defenses and deliver customizable control of security posture to our customers. In this way organizations can futureproof themselves from adversaries who are constantly evolving their methods.

We achieve this by applying streaming analytics to all of our endpoint data. Streaming analytics is derived from event stream processing a technique that has been implemented for years across multiple industries — from credit card fraud detection to high frequency trading. By focusing on streams of activity as opposed to point-in-time detections the PSC can recognize when a series of actions that have taken place over time is suspicious. The PSC stops both malware and non-malware attacks including attacks that leverage known good software to do malicious things. For example an attack leveraging a command interpreter like PowerShell to find and encrypt all files on disk could be run entirely remotely without a file bypassing any form of signaturebased prevention. However the process running the commands would still exhibit behavioral patterns similar to ransomware which would be detected by streaming analytics and stopped. The PSC uncovers threats patterns and indicators invisible to traditional and machine learning antivirus by looking upstream to the root cause of attacks and then applying this knowledge to better predict future ones.

The PSC offers out-of-the-box protection for those who want to "set it and forget it" but also provides the option for highly customizable policies. This lets organizations disrupt future attacks by specifically addressing gaps or blind spots. IT and security professionals can create custom control policies for individual work groups in their environment control update frequency and define exactly what types of processes are or are not allowed to run and how untrusted execution is handled. For example unknown applications could be denied operation entirely or could be allowed to run but not allowed to make any network connections or invoke command interpreters. This level of granular control ensures that professionals who need specific control of their machines can have it while still stopping advanced attacks. When protecting endpoints it is important to acknowledge that there are many ways to gather threat intelligence and to utilize all available sources. More than 75 of the world's leading incident response vendors use Carbon Black to investigate breaches daily providing insights into the most recent attacks. Carbon Black's dedicated Threat Analysis Unit (TAU) leverages these insights and further investigates current attack trends ensuring our analytics are up to date at all times evolving to protect against emerging attacks. On top of this our customers have access to a user community of more than 17000 security experts allowing members to interact with one another and learn about the latest insights and intelligence.

Our Differentiator:
Actionable Visibility

Cut Down the Guesswork and Close Security Gaps, Fast.

The PSC makes it possible to identify emerging threats prioritize the most critical attacks and provide detailed visibility into the attack chain to help professionals rapidly understand investigate and remediate attacks. While siloed tool sets can make it difficult to fully understand what is happening on endpoints — forcing professionals to piece together the necessary information from multiple places — the PSC gives a comprehensive picture of what occurred in the past and what is happening now. With the power of comprehensive IT and security professionals have deep visibility into the state of their endpoints — eliminating gaps and blind spots accelerating investigations and remediation and leading to a significant reduction in dwell time.

This visibility is beneficial to all security professionals but offers specific value to threat hunters and incident responders who need quick and clear access to data to investigate proactively hunt for and remediate threats. Our approach allows investigations that often take days or weeks to be completed in just minutes. The sophisticated detection capabilities combine custom and cloud-delivered threat intel automated watchlists and integrations with the rest of the security stack to efficiently scale hunting across the enterprise.

The PSC's quick and agile search zoom process trees and timelines give a comprehensive understanding of how an attack was executed. It's easy to uncover exactly where an attacker went and what they did as well as the root cause in minutes to quickly address gaps in defenses. With remote investigation and remediation of any endpoint from anywhere security professionals can reduce IT involvement eliminating unnecessary reimaging and support tickets.

To augment and supplement the operating system event data that the platform is continuously collecting the PSC offers tools to gather additional information that cannot and should not be collected on a continuous basis. Real-time endpoint query and remediation capabilities enable professionals to ask questions of all endpoints and take action to remediate in real time. This power to create custom queries provides visibility into precise details about the current state of all endpoints — on and off the network. Professionals can then respond to this information by isolating infected systems to prevent lateral movement creating a remote secure shell to any endpoint collecting and storing additional forensics data for post-incident investigation or running scripts for full remediation.

Administrators also have the option to run queries against specific groups of devices and even individual devices. This enables the user to start broadly and then get more and more granular targeting only those machines that are important to that specific investigation or audit.

Having the tools to quickly gather all of the information needed to fully understand an attack and being able to take immediate action remotely helps professionals reduce dwell time and minimize risk in their environment.

Our Differentiator:
Simplified Operations

Eliminate Multi-vendor Complexity and Agent Fatigue.

While most endpoint security programs require multiple siloed systems that burden end users and complicate management the PSC provides a single consolidated platform supporting multiple endpoint security needs. Although some AV vendors have begun to use cloud-based consoles they aren't taking full advantage of the cloud for security analysis and operations. Additionally other vendors call themselves a "platform" but actually operate as a suite of separate products. Unlike these solutions the PSC delivers multiple services using a single lightweight sensor enabling organizations to consolidate security products. A centralized unified console provides professionals access to numerous capabilities and the complete dataset.

The PSC makes it easy to deploy multiple security services without compromising endpoint performance. There is no need to purchase or stand up on-site infrastructure and our out-of-the-box policies are easily customized to fit any environment. Additionally when an organization decides that it is time to expand their security capabilities they can seamlessly add new features without new infrastructure sensors or deployment costs.

The PSC automatically adapts to new attacks so endpoints remain protected without requiring manual updates. Gone is the burden of constantly distributing large signature updates. Our automatic protection against the latest most advanced threats gives organizations access to new and updated features as soon as they are released.

Strengthen Security Posture.

When security tools can work together they provide more visibility more context and ultimately better overall protection. Unlike traditional solutions that exist in silos the PSC is an extensible platform built on open APIs elegantly integrating with the rest of a company's security stack.

Pre-built integrations are available for many industry-leading solution providers such as IBM VMware Splunk LogRhythm ForeScout and more. This shared visibility drives a common understanding of issues across security and IT teams decreasing friction and simplifying workflows. Security and IT professionals can extract more value from their data by adding context that other solutions lack. Access to unfiltered data speeds up investigation and analysis leading to identification and remediation of more attacks.

For example the bidirectional integration with VMware AppDefense leverages the PSC's unfiltered data to identify specific behaviors that indicate attempted lateral movement in the datacenter and automatically blocks the attack while invoking AppDefense remediation actions such as snapshot shut down or suspend an affected VM from a single console. It makes it easy to understand what applications a virtual server supports within the Carbon Black console and provides important context — with IT data flowing into the security console automatically.

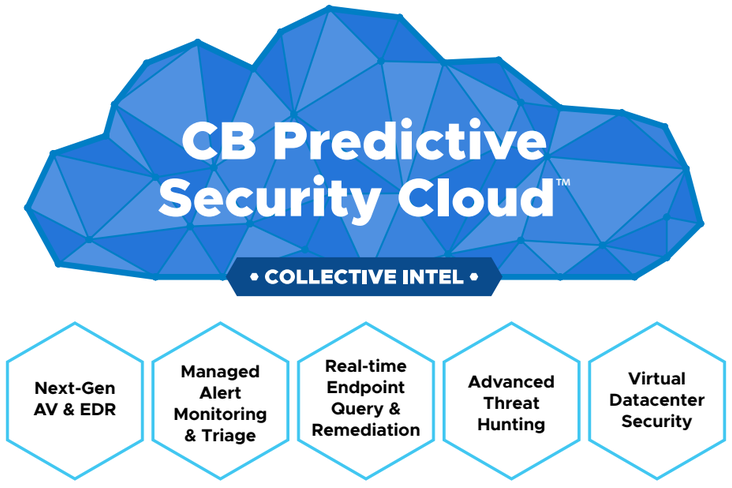
Similarly the tight integration with IBM QRadar allows administrators to leverage industry-leading NGAV (next-gen antivirus) and EDR (endpoint detection and response) solutions to see detect and act upon endpoint activity from directly within the QRadar console. When necessary security analysts are able to immediately remediate at the point of compromise from the QRadar console streamlining workflows and speeding response.

Beyond integrations data collected from the endpoint can be exported quickly out of the core PSC data pipeline for use with customer-specific integrations and custom processing. Open APIs further allow organizations to build custom dashboards for integrated management and reporting and create new workflows that support and enhance their security programs. When security tools are operationally unified an organization's overall security posture can improve dramatically reducing dwell time and risk.

"[CARBON BLACK] PROVIDES US A SINGLE CONSOLE...(MAKING IT EASIER) TO MANAGE AND CONSOLIDATE EVERYTHING IN ONE PLACE...REMOTELY WE CAN CHECK THE USER SYSTEM AND PERFORM INVESTIGATIONS WHICH WILL ACTUALLY HELP US ANALYZE DIRECTLY ON THE ENDPOINT AND WE CAN TAKE IMMEDIATE ACTION AT THE SAME TIME"

– HAARIS FAIZAN CYBERSOC | SENIOR SECURITY ENGINEER | ST. GOBAIN

Services Delivered Through the PSC



NGAV + EDR

Carbon Black's NGAV and EDR solution uses streaming analytics to uncover malicious behavior and stop known and unknown attack before they compromise systems.

Carbon Black offers powerful flexible prevention that is able to stop malware ransomware and non-malware attacks. It prevents these attacks automatically whether the endpoint is online or offline from anywhere in the world and is able to keep up with the always-changing threat landscape to block emerging neverbefore- seen attacks that other solutions may miss.

Carbon Black's industry-leading detection and response capabilities reveal threat activity in real time so organizations can respond to any type of attack as soon as it's identified. The root cause of an attack can be uncovered in minutes through visualizations that show every stage of the attack with easy-to-follow attack chain details. CB Defense lets administrators immediately triage alerts by isolating endpoints blacklisting applications or terminating processes. Professionals can secure shell into any endpoint on or off the network to perform full investigations and recommendations remotely.

Alert Prioritization and Triage

Carbon Black's alert prioritization and triage service provides customers with a world-class professional team of Carbon Black security experts who work side by side with organizations that need more resources to validate and prioritize alerts, uncover new threats and accelerate investigations.

Carbon Black's US-based experts analyze, validate and prioritize alerts from Carbon Black, helping to ensure that companies don't miss the threats that matter. The service provides additional, human-generated context to alerts, such as connecting alerts caused by the same root cause, to help streamline investigations and resolve security issues. Carbon Black threat experts proactively identify trends by monitoring threat activity across millions of endpoints, providing advice on widespread attacks and retroactively detecting and confirming emerging threats based on iterative discovery techniques. Monthly reports summarize alert data, turning a month's worth of unfiltered data into actionable recommendations that help security professionals see the bigger picture and continually improve efficacy.

Advanced Threat Hunting and IR

Carbon Black's advanced threat hunting and incident response solution delivers unfiltered visibility for top security operations centers and IR professionals.

Investigations that typically take days or weeks can be completed in just minutes. Carbon Black correlates and visualizes comprehensive information about endpoint events, giving IT and security professionals greater visibility into their environments. The solution's sophisticated detection enables IOC (indicators of compromise) monitoring with your choice of threat intel, including your own custom feeds. This solution extends the automated TTP (tactics, techniques and procedures) recognition in Carbon Black's NGAV and EDR solution with deep investigation data and tools to help not only understand current attacks, but also longer term attack patterns. With threat hunting on the PSC, professionals have the power to respond and remediate in real time, stopping active attacks and repairing damage quickly.

Real-time Query and Remediation

Carbon Black's real-time query and remediation solution enables organizations to ask questions of all endpoints and take action to instantly remediate issues. Carbon Black extends core functionality of the widely adopted open source osquery project providing visibility into precise details about the current state of all endpoints

enabling security and IT teams to make quick confident decisions to reduce risk.

Carbon Black gives administrators visibility into the most precise details about the current state of all endpoints. It automates operational reporting on patch levels and assesses IT hygiene. When combined with Carbon Black's threat hunting capabilities live query and response provides an unprecedented level of visibility to speed investigation and threat hunting.

Securing the Virtualized Datacenter

Carbon Black's virtual data center security solution is a cloud-delivered purpose-built security solution for protecting applications deployed in the virtualized datacenter. Jointly architected with VMware the solution seamlessly integrates with VMware AppDefense combining least-privilege application control from the hypervisor with application-informed behavioral threat detection and EDR. This unique combination delivers superior protection from advanced threats without compromising availability and performance.

Conclusion

The CB Predictive Security Cloud leverages unfiltered data across all of its security products to provide customers with:

- **Superior Protection** — using predictive modeling and streaming analytics tostay ahead of sophisticated threats.
- **Actionable Visibility** — accelerating investigations allowing professionals torespond confidently to threats using a comprehensive picture of past andpresent events.
- **Simplified Operations** — consolidating multiple capabilities in the cloud usinga single endpoint agent console and dataset.
- **Platform Extensibility** — leveraging pre-built integrations and open APIs toshare data across the security stack and extract greater value.

5,000+
CUSTOMERS

1,100+
EMPLOYEES

1/3
OF THE FORTUNE 100

140+
PRODUCT INTEGRATIONS

BlueCross BlueShield Association · COX COMMUNICATIONS · PHILIPS · DRAFTKINGS · kordia · Mercy MEDICAL CENTER · Motors Management Corp · MLB · medibank PRIVATE · D|A DAVIDSON INVESTMENT BANKING · Nasdaq · SAMSUNG · Adobe · EVERNOTE · Lithium · PeoplesBank A passion for what is possible™

Carbon Black.

ABOUT CARBON BLACK

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the CB Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. 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) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe.

1100 WINTER STREET, WALTHAM, MA 02451, USA • P 617.393.7400 • F 617.393.7499 • WWW.CARBONBLACK.COM