WHITE PAPER–AUGUST 2020

Getting More from Less

Simplifying endpoint security With a cloud-delivered platform

vmware® Carbon Black

Table of contents

Introduction

IT and security professionals know that the threat landscape is dynamic. Every day, attackers are getting smarter and coming up with new techniques to avoid detection. With non-malware and in-memory attacks now making up 72 percent of breaches,[1] traditional antivirus (AV) is no longer enough to keep systems safe. In fact, less than one-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, 60 percent of enterprise organizations are using at least 25 different cybersecurity 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, more than 50 percent of organizations that deploy more than 50 security solutions define their security orchestration as "very challenging" and, because of this, nearly half (49 percent) 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 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.

Most IT and security teams struggle to hire enough qualified security personnel. 32 percent of cybersecurity professionals believe their organization is taking the necessary actions to address the impact of the ongoing cybersecurity skills shortage.[5] 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 back-and-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

[1] Verizon. "2019 Data Breach Investigations Report." May 2019.

[2] Ponemon Institute. "The 2017 State of Endpoint Security Risk." November 2017.

[3] ESG Brief, Security Infrastructure and Market Changes in Progress, August 2020.

[4] Cisco. "2018 Annual Cybersecurity Report." February 2018.

[5] ESG Research Report, The Life and Times of Cybersecurity Professionals 2020, June 2020.

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.

> “One of our goals was to consolidate our security products. What VMware 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

VMware Carbon Black Cloud

Consolidated endpoint security, simplified

At VMware, we understand the current state of endpoint security and have built a solution that is uniquely positioned to meet today’s needs.

VMware Carbon Black Cloud™ is a cloud native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lightweight agent and an easy-to-use console. Instead of needing to deploy a variety of products each with their own setups, configurations and policies, this solution delivers multiple security capabilities through a common cloud-delivered platform that shares one sensor, one cloud 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 VMware or other vendors. This creates a single source of truth and adds context to security across the board. This platform was constructed with the understanding that security needs grow and change as the threat landscape evolves.

Our differentiator: Behavioral analytics

A surveillance camera on the endpoint

At VMware, 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? 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.

VMware Carbon Black Cloud 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, this platform continuously looks at endpoint activity, regardless of if it seems good or bad, and analyzes the behaviors. This gives

200 terabytes of endpoint data are analyzed in the cloud. That is 13 times the number of iMessages processed.

500 billion security events are analyzed daily. That is 150 times the number of google searches in the same period.

security professionals the context and confidence they need to defend their systems.

VMware 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 more than 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 cloud native platform.

Our differentiator: Superior protection

Stop more attacks, take back control over endpoints and worry less

Our unique approach provides an advantage when it comes to protecting endpoints. By analyzing attackers' behavior patterns, VMware Carbon Black Cloud 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 future-proof themselves from adversaries who are constantly evolving their methods.

We achieve this by applying machine learning and behavioral models to analyze endpoint data and uncover malicious activity to stop all types of attacks before they reach critical systems. 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 ongoing behavioral analysis as opposed to point-in-time detections, the platform can recognize when a series of actions that have taken place over time is suspicious. The platform 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 such as PowerShell to find and encrypt all files on disk could be run entirely remotely without a file bypassing any form of signature-based prevention. However, the process running the commands would still exhibit behavioral patterns similar to ransomware, which would be detected and stopped. The platform threats, 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.

VMware Carbon Black Cloud offers out-of-the-box protection (for those who want to set it and forget it) and 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 VMware Carbon Black to investigate breaches daily, providing insights into the most recent attacks. The dedicated VMware Carbon Black Threat Analysis Unit leverages these insights and further investigates current attack trends, ensuring our analytics are up to date at all times and evolving to protect against emerging attacks. On top of this, our customers have access to a user community of more than 30,000 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

VMware Carbon Black Cloud 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—our platform gives a comprehensive picture of what occurred in the past and what is happening now. With the power of comprehensive IT, 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, and 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 platform's quick and agile search/zoom process, with trees and timelines, gives 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 it is continuously collecting, the platform offers tools to gather additional information that cannot and should not be collected on a continuous basis. Real-time audit and remediation capabilities make it faster and easier for security and IT teams to assess and change system state to harden their environment against the most relevant threats. This power to create custom queries provides visibility into precise details about the current state of all devices and workloads—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 granular by targeting only those machines 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.

> "[VMware 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

Our differentiator: Simplified operations

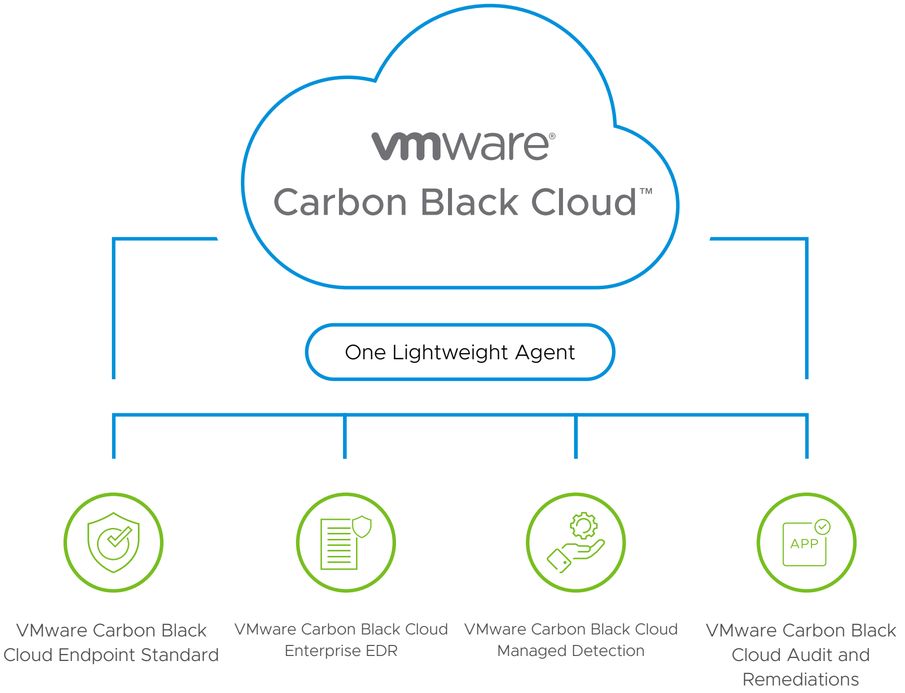
vmware
Carbon Black Cloud™
One Lightweight Agent
APP
VMware Carbon Black Cloud Endpoint Standard
VMware Carbon Black Cloud Enterprise EDR
VMware Carbon Black Cloud Managed Detection
VMware Carbon Black Cloud Audit and Remediations

FIGURE 1: VMware Carbon Black Cloud product diagram.

Eliminate multi-vendor complexity and agent fatigue

While most endpoint security programs require multiple siloed systems that burden end users and complicate management, VMware Carbon Black Cloud 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, our cloud native platform 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.

This platform makes it easy to deploy multiple security services without compromising endpoint performance. There is no need to purchase or stand up onsite 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.

VMware Carbon Black Cloud 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, our platform 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, 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 tight integration with IBM QRadar allows administrators to leverage industry-leading next-generation antivirus (NGAV) and endpoint detection and response (EDR) solutions to see, detect and act on 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 platform's 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.

Services delivered through VMware Carbon Black Cloud

NGAV and behavioral EDR

The VMware Carbon Black NGAV and behavioral EDR solution uses machine learning and behavioral models to analyze endpoint data and uncover malicious activity to stop all types of attacks before they reach critical systems.

VMware 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 never-before-seen attacks that other solutions may miss. VMware'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. VMware Carbon Black Cloud Endpoint™ Standard lets administrators immediately triage alerts by isolating endpoints, denylisting applications or terminating processes. Professionals can secure shell into any endpoint on or off the network to perform full investigations and recommendations remotely.

Alert monitoring and triage

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

The VMware U.S.-based experts analyze, validate and prioritize alerts from VMware Carbon Black Cloud, 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. VMware 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.

LEARN MORE

To set up a personalized demo or try it free in your organization, visit *carbonblack.com/request-a-demo*.

For more information or to purchase VMware Carbon Black products, please call 855-525-2489 in the U.S. or +44-118-908-2374 in EMEA, email *contact@carbonblack.com* or visit *carbonblack.com/products/vmware-carbon-black-cloud*.

Enterprise EDR

VMware Carbon Black® Cloud Enterprise EDR,™ our threat hunting and incident response (IR) solution, delivers continuous visibility for top security operations centers and IR professionals.

Investigations that typically take days or weeks can be completed in just minutes. Carbon Black Cloud Enterprise EDR correlates and visualizes comprehensive information about endpoint events, giving IT and security professionals greater visibility into their environments. The solution's sophisticated detection enables indicators of compromise (IoC) monitoring with your choice of threat intel, including your own custom feeds. This solution extends the automated recognition of tactics, techniques and procedures (TTPs) in Carbon Black Cloud Endpoint Standard with deep investigation data and tools to help understand current attacks as well as longer-term attack patterns. With threat hunting on the VMware Carbon Black Cloud, professionals have the power to respond and remediate in real time, stopping active attacks and repairing damage quickly.

Audit and remediation

VMware Carbon Black® Cloud Audit and Remediation,™ our real-time assessment and remediation solution, enables security and IT teams to assess and change system state to harden their environment against the most relevant threats. This allows teams to effortlessly benchmark their devices, workloads and containers against industry standards or regulations from a single console to help minimize risk and simplify operational reporting across the entire fleet.

Carbon Black Cloud Audit and Remediation 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 the VMware threat hunting capabilities, Carbon Black Cloud Audit and Remediation provides an unprecedented level of visibility to speed investigation and threat hunting.

Conclusion

VMware Carbon Black Cloud leverages unfiltered data across all of its security products to provide customers with:

- Superior protection, usingpredictive modeling and streaming analytics to stay ahead of sophisticated threats
- Actionable visibility, accelerating investigations and allowing professionals to respond confidently to threats using a comprehensive picture of past and present events
- Simplified operations, consolidating multiple capabilities in the cloud using a single endpoint agent console and dataset
- Platform extensibility, leveraging pre-built integrations and open APIs to share data across the security stack and extract greater value

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com

Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware and Carbon Black are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMWCB-WP-GMFL-R1-03 08/20