WHITE PAPER–JULY 2020

Top Three Essential Endpoint Security Integration Use Cases

vmware® Carbon Black

Table of contents

According to Verizon's Data Breach Investigation Report, 56 percent of breaches took months or longer for IT security teams to discover.[1]

Dwell Time = Amount of time threat actors operate undetected in an environment.

Introduction

Despite technological innovations and investment in the cybersecurity industry, enterprises lack the resources needed to detect and disrupt threats quickly. Many enterprise IT and security teams are understaffed, most are working from home, and they struggle to keep up with newly sophisticated attacks against a largely distributed remote workforce.

Most cyberattacks aren't discovered until months after initial access. Many reasons for this exist, but the most significant driver for long (and increasing) dwell times remains the lack of a unified perspective into all that attackers are doing at each stage of an attack. From this unified perspective. IT security teams can coordinate fast and precise countermeasures to detect and disrupt threats before they gain footholds and start to impact operations.

Whether corporate-owned or personally-owned, endpoints are on the front lines of this cyber battlefield. And since most end users aren't warriors, we rely on endpoint security platforms to do all the heavy lifting.

Spotting and stopping malicious activity before it impacts productivity or puts essential data or services at risk is now more difficult. And because most enterprises already use dozens of security technologies, endpoint security platforms must easily integrate with existing tools and processes, use an open architecture with a growing and well-established partner ecosystem, along with well-documented, publicly available APIs. A supportive and vibrant user community is also a critical success factor.

VMware Carbon Black Cloud™ offers all of these essential capabilities so your team is fully prepared for the cyber threats. As part of VMware's intrinsic security approach, VMware Carbon Black Cloud consolidates multiple endpoint security capabilities to help you operate faster and more effectively. This guide outlines the most common endpoint security integration use cases, and how to set up seamless workflows between VMware Carbon Black Cloud, VMware Workspace One®, and leading products from vendors such as IBM, Splunk, Lastline, VMRay, and more.

Integration process: three phases

Considering that the average enterprise works with 80 cybersecurity vendors,[2] knowing how easy it is to integrate your next cyber security technology investment becomes critical.

While integration details may vary based on the vendors involved, using this three-tiered "Ingest-Enrich-Act" process framework can help you map out each integration.

1. **Ingestion:** Event data is ingested into the integrated workflow. For example, the event data may involve a security policy, endpoint activity or behavior, or threat intelligence artifact or indicator. After initial processing, the data may require enrichment or validation from a local or external source. If not, it skips to step 3.

[1] Verizon "2020 Data Breach Investigations Report" 2020

[2] Help Net Security. "Are there too many cybersecurity companies?" March 30, 2018

THE POWER OF COMMUNITY DEFENSES

Cyber attackers collaborate with each other on a daily basis. On the dark web in underground forums, they share bragging rights as well as TTPs on how to target their next victim. Enterprises are well-served to do the same. More than 30,000 security professionals have joined VMware Carbon Black's User Exchange (UEX) to share best practices, lessons learned, and threat intelligence to improve their company's security posture and help collectively combat threats.

According to VMware research,[3] 82 percent of surveyed financial institutions said cybercriminals have become more sophisticated and more stealthy using highly targeted social engineering attacks and advanced TTPs to remain under cover. By exploiting weaknesses in people, processes and technology, they gain a foothold and persist in the network, transferring funds and exfiltrating sensitive data–all without setting off alarms.

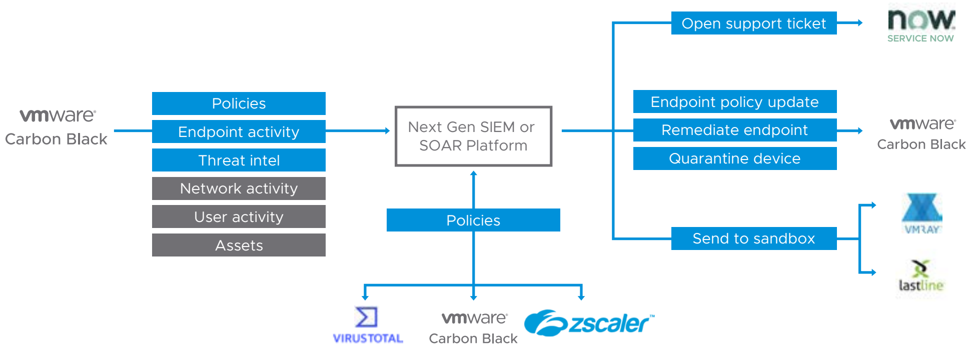


FIGURE 1: Three phases of integration process.

2. **Enrichment:** The original event data is validated and enriched via calls to external data sources (e.g. VirusTotal), and then repackaged for further analysis and action. By the way, if the original event data is a false positive (or deemed irrelevant, inaccurate, or unnecessary), the workflow can end without any need for human intervention.
3. **Action:** The validated event data now triggers an action either on the VMware Carbon Black Cloud or on the integrated technology's platform, or both. For example, the action may include opening a service ticket in ServiceNow for further investigation. Or, the workflow could include sending malware to a sandbox, quarantining the endpoint and resolving the issue, as well as opening and updating a ticket in ServiceNow.

The use cases: why they're essential

Two capabilities are essential to reduce an attacker's dwell time: 1) the ability to detect stealthy threats quickly and 2) a well-orchestrated and streamlined response workflow. That's why endpoint security integrations are perhaps the most critical success factors for global enterprises.

Integrations between your endpoint security platform and the other monitoring and enforcement tools in your arsenal improve your defenses in these key ways:

1. Optimizes monitoring and detection efforts: An enriched data set inherently improves efficiency and increases the accuracy of the analysis
2. Orchestrates and automates response: Harmonize security policy across enforcement points while also accelerating a targeted response to incidents as they arise
3. Enables highly distributed teams to respond quickly: Attackers are constantly innovating and adapting; well-integrated workflows empower disparate teams to work together better in combating adaptive attacks at scale

We recommend implementing the following endpoint security integrations to accelerate incident response efforts across the enterprise:

- SIEM Integration for Accurate and Actionable Threat Detection
- SOAR Integration for Automated and Orchestrated Defenses
- Next Generation Network Security Integration for Threat Disruption at Scale

[3] VMware Carbon Black. Modern Bank Hesists report.

Endpoint security use case 1:

SIEM integration – accurate and actionable threat detection

What it does: Integrating your SIEM with your EDR and NGAV platform will enhance and automate your alert verification process, arm your threat hunters at scale, and convert threat detection into immediate action.

Why you need it: The fact that it usually takes months for enterprises to detect an attacker's presence on their network is the wake-up call you need to establish and invest in your threat hunting program. Whether it's too many alerts for analysts to discern the signal from the noise or an attacker's ability to operate under the radar (or likely both), a tight integration between your SIEM and your endpoint security platform is the cure for these chronic ailments.

How it works: The most common setup is to have our event forwarder automatically deliver endpoint event data to an Amazon S3 bucket (or other public cloud instance). On a set schedule, the SIEM then pulls the data from the S3 bucket to start the normalization and correlation process. Next, the SIEM analysis engine normalizes the raw data to its own schema, or develops a new schema to store, analyze, and correlate the data.

At this point, some SIEM platforms will trigger an additional data enrichment process. If supported, the SIEM platform sends a request for more information from the VMware Carbon Black Cloud. These enrichment requests are wide-ranging and could be simple things like a file hash, registry setting or something more involved, such as what the parent process was that spawned a particular process, what other processes were running at the time, and so on.

The SIEM generates an alert which includes all of the raw endpoint artifacts, the enriched data, and associated priority level—all without the need to manually collect the information from the endpoint itself. For SIEMs that support it, VMware Carbon Black Cloud can also take remediation actions based on an alert, enabling actionable defenses across your entire endpoint environment.

Where to use it: Threat Hunting Programs

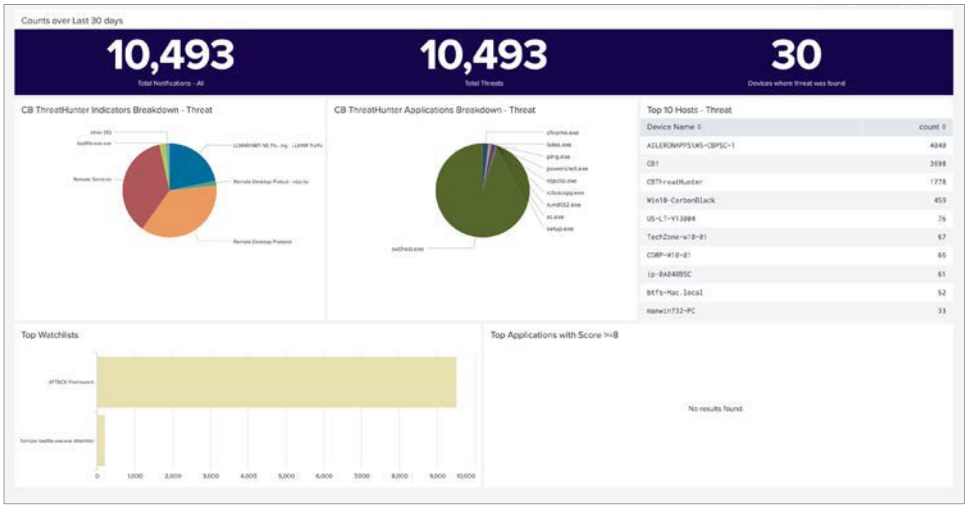
Let's face an ugly truth. The intruder is well past the gate. They are already inside your network, and living off the land, installed on any number of your endpoints.

Your next move is critical. You need to find them and contain them. Threat hunting is the best way to turn the tables on the intruders, and your defense starts with a VMware Carbon Black Cloud-SIEM integration. Thanks to open integration, you'll have timely, highly detailed, and accurate data—across 1500 endpoint data points—to prioritize the most critical alerts, hunt down adversaries, and make the best decisions on how to implement effective countermeasures.

Rather than struggling with too many alerts to respond to, your SIEM will pinpoint which alerts are truly critical, and provide detailed endpoint data not available from any other platform.

NEXT GEN SIEM PARTNER SPOTLIGHT

SIEM solutions have been a staple of enterprise security for decades, giving SOC teams a better understanding of user, network, and app activity, and pinpointing any threats that may pose risks to an organization. Next-Gen SIEM vendors like Exabeam and Sumologic take it a step further. By adding in User and Entity Behavior Analytics (UEBA) and SOAR capabilities to their platforms, these VMware Carbon Black Cloud integration partners maximize SOC team efforts, by prioritizing events that pose the biggest risks to an organization, and making them truly actionable. *Learn more*.



Counts over Last 30 days

10,493 Total Notifications - All

10,493 Total Threats

30 Devices where threat was found

CB ThreatHunter Indicators Breakdown - Threat

other (10)
LLMNR/NBT-NS Po...ing - LLMNR Traffic
Remote Services
Remote Desktop Protoc - rdpclip
Remote Desktop Protocol

CB ThreatHunter Applications Breakdown - Threat

Top 10 Hosts - Threat

Device Name	count
AILERONAPPS\WS-CBPSC-1	4040
CB1	3598
CBThreatHunter	1778
Win10-CarbonBlack	459
US-LT-Y13004	76
TechZone-w10-01	67
CORP-W10-01	65
ip-0A0400SC	61
btfs-Mac.local	52
manwin732-PC	33

Top Watchlists

Top Applications with Score >=8

No results found.

FIGURE 2: Carbon Black Cloud Enterprise EDR App for Splunk.

Learn more about threat hunting: *How to Create a Scalable and Repeatable Threat Hunting Program | VMware*

Learn more from some of our SIEM integration partners:

- IBM QRadar App Listing: *IBM Security App Exchange - Carbon Black Cloud App for IBM QRadar*
- Splunk App Listing: *CB ThreatHunter App for Splunk*

Endpoint security use case 2:

SOAR integration – automated and orchestrated defenses

What it does: Integrating your endpoint security technology with your SOAR platform enables standardized and orchestrated incident response workflows so teams can consistently resolve issues faster and contain threats more effectively. Additionally, integrating VMware Carbon Black Cloud endpoint data alongside other security data adds rich context and telemetry to each security event and investigation.

Why you need it: Cyberattacks have increasingly become more difficult to identify as well as contain and disrupt, making it nearly impossible for defenders to scale their efforts in response. To meet this escalating onslaught, two things are essential: real-time visibility into and across enterprise infrastructure (clouds, networks, apps, and endpoints), and the ability to orchestrate countermeasures at enterprise scale. A tight integration between your endpoint security technology and your SOAR platform is an essential ingredient.

How it works: Many SOAR platforms like Splunk Phantom and IBM Resilient offer pre-built playbooks and actions, so you're not starting from scratch. These pre-built playbooks can be easily repurposed and customized depending upon your unique requirements. Additionally, VMware Carbon Black Cloud supports a number of apps within these partner ecosystems to quickly enable and integrate our core capabilities into the SOAR platform: EDR, NGAV, Audit and Remediation or all of the above.

Our open APIs and developer tools can streamline the integration process between your

SOAR and the VMware Carbon Black Cloud platform. These include our Event and Alert Forwarder, Live Query and Response APIs, and our Enterprise EDR Feed Management API. All of our APIs and developer tools are publicly available and posted on our Developer website at *https://developer.carbonblack.com/getting-started/*.

The endpoint data collected by VMware Carbon Black Cloud is detailed and voluminous, allowing SOC teams to implement automated workflows with precision and highly granular enforcement actions. For example, you can choose precisely what happens when a specific IoC is discovered or an endpoint behaves in a certain way rather than relying on an enforcement action that is overly burdensome, unnecessary, or is based on a false positive.

Plus, our SOAR integration supports bi-directional information flow so you can use our APIs to update endpoint policies across the enterprise based on a SOAR alert, threat intelligence indicator or other aspect of an integrated workflow. For example, in the process of responding to an alert, the team may discover that a threat indicator is a false positive, in which case you can use our APIs to update the NGAV policy on all of your endpoints at the same time.

Where to use it: Automate Remediations based on MITRE ATT&CK Matrix

MITRE's ATT&CK database[4] provides enterprise SOC teams with a roadmap for how the most damaging cyberattacks happen and how to disrupt them. Recognizing that attackers do most of their work while living-off-the-land, using the matrix to build automated workflows helps enterprises hunt down attackers where they live, and disrupt attacks more effectively than other approaches. To facilitate this process, VMware Carbon Black has built MITRE ATT&CK TIDs into our platform alongside our own proprietary TTP tags.

By integrating VMware Carbon Black Cloud into your SOAR platform, you can use our MITRE ATT&CK TIDs to build playbooks aligned to MITRE's 12 attacker tactics and 314 techniques. Many of our SOAR technology partners support this approach including Splunk Phantom, IBM Resilient, Demisto, Siemplify, ThreatConnect, and Swimlane.

If you're new to VMware Carbon Black Cloud, find our apps in the Splunk and IBM marketplaces below:

- **Splunk Phantom App Listing:** *https://my.phantom.us/4.6/apps/?search=Carbon%20Black%20ThreatHunter*
- **IBM Resilient App Listing:** *https://exchange.xforce.ibmcloud.com/hub/extension/eb7463ce6fa67ce6ca3fd1e2f3d3d46a*

Endpoint security use case 3:

Next-gen network security integration for threat disruption at scale

What it Does: Network security is undergoing a radical evolution, thanks to global enterprise digital transformation initiatives, the rise of the cloud, and the dissolution of the enterprise perimeter. Since most users, apps, and the data they access are no longer housed in the data center, network security inspection, analysis, and policy enforcement need to be done elsewhere.

Technologies like Sandbox/Binary Detonation tools, CASB, and Next-Gen Secure Web Gateways remain essential capabilities, yet where and how they're deployed may evolve in the near future. As a new network security model, SASE, or Secure Access Service Edge, shows promise in terms of redesigning network security so the inspection is performed in the cloud, closer to the edge (the user, entity or endpoint).

[4] For more information, please see https://attack.mitre.org.

In the meantime, integrating these network security technologies with VMware Carbon Black Cloud delivers advanced threat analysis you can deploy at scale, particularly for unknown and malicious threats.

Why you need it: Since it takes most software vendors an average of 59 days to patch an unpublished yet newly discovered vulnerability,[5] it's imperative that enterprise security teams identify and disarm exploits for these vulnerabilities as soon as possible. Plus, in some cases, the malware we examine on an endpoint is purpose-built to prevent local analysis, making integrations with our next generation network security vendors an invaluable service.

Integrating VMware Carbon Black Cloud with Sandbox/Binary Detonation technologies enables bi-directional threat intelligence sharing so teams can make quick, accurate, and safe decisions on whether to allow or block a particular executable. Additionally, integrating our platform with Next-Gen Secure Web Gateways (NG SWGs) and Cloud Access Security Brokers (CASB) adds additional layers of protection against zero-day exploits, unknown attacks, and other nefarious behavior that may otherwise be undetectable by either technology on its own.

Whichever integration option you choose, you'll reap the following benefits:

- Enhanced visibility: See threats across cloud workloads and endpoints
- Collective threat analysis: Share threat intelligence between cloud and endpoint
- Closed-loop remediation: Combat cloud threats by coordinating with endpoints
- Dynamic protection: Adapt access controls based on endpoint security posture
- Future-proof security: Support and enable SASE architecture evolution

How it works: Since next generation network security architectures are still evolving, there are a variety of different approaches for how an integrated workflow can work between VMware Carbon Black Cloud and our cloud-native next generation network security partners. We've outlined three scenarios below, which include our technology partners NetSkope, Zscaler, and *LastLine*.

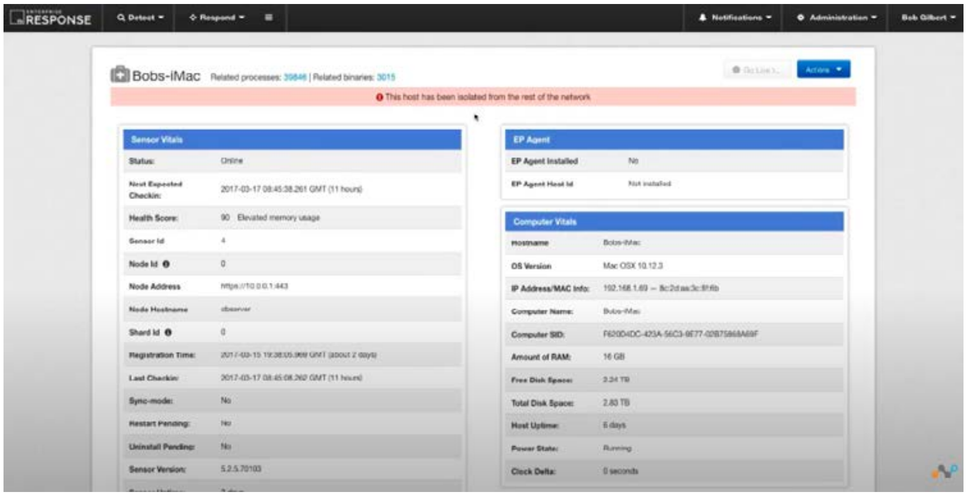
Please note: Our partner ecosystem is vast; we support integrations with many other vendors in this space (including support for on-premiseds deployments). Developing your custom integration with the VMware Carbon Black Cloud can be streamlined using the Binary Analysis SDK, Live Query and Response APIs and the Unified Binary Store APIs.[6]

"Inside out" threat protection

Threat intelligence sharing is a key success factor when determining whether an endpoint, a file, or an activity pattern poses a threat to your network, endpoints, or apps. One of VMware Carbon Black's key partners, Netskope Cloud Threat Exchange ingests, curates, and shares threat data in real-time so its technology partners benefit from the bi-directional exchange of IoCs, artifacts, attacker TIDs, TTPs, and other valuable intelligence.

[5] Business 2 Community. "Zero-Day Vulnerability: The Unknown Threats to Your Data." Dave Wallen. June 8, 2020

[6] Find more information here: https://developer.carbonblack.com



Bobs-iMac Related processes: 39846 | Related binaries: 3015

This host has been isolated from the rest of the network

Sensor Vitals	
Status:	Online
Next Expected Checkin:	2017-03-17 08:45:38.261 GMT (11 hours)
Health Score:	90 Elevated memory usage
Sensor Id	4
Node Id	0
Node Address	https://10.0.0.1:443
Node Hostname	cbserver
Shard Id	0
Registration Time:	2017-03-15 19:38:05.969 GMT (about 2 days)
Last Checkin:	2017-03-17 08:45:08.262 GMT (11 hours)
Sync-mode:	No
Restart Pending:	No
Uninstall Pending:	No
Sensor Version:	5.2.5.70103

EP Agent	
EP Agent Installed	No
EP Agent Host Id	Not installed

Computer Vitals	
Hostname	Bobs-iMac
OS Version	Mac OSX 10.12.3
IP Address/MAC Info:	192.168.1.69 -- 8c:2d:aa:3c:8f:6b
Computer Name:	Bobs-iMac
Computer SID:	F620D4DC-423A-56C3-9E77-02B75868A69F
Amount of RAM:	16 GB
Free Disk Space:	2.24 TB
Total Disk Space:	2.80 TB
Host Uptime:	6 days
Power State:	Running
Clock Delta:	0 seconds

FIGURE 3: VMware Carbon Black® EDR™.

By ingesting all of the rich and detailed endpoint data VMware Carbon Black Cloud captures, NetSkope can better identify malicious files and behavior and block it at a network level. Putting the endpoint at the center of your security ecosystem in this way reflects the new SASE reality… protecting against threats at the edge (aka inside) and moving those protections out into the network at scale. This kind of "inside out" security innovation is the best way to scale to meet the current onslaught and exponential increase of cyber threats.

Device posture and sandboxing: allow vs. warning

Responsible for securing more than 400 of the Forbes Global 2000 companies, our cloud-native technology partner Zscaler offers one of the industry's first SASE platforms designed for enterprise scalability and performance. Integrating VMware Carbon Black Cloud with the Zscaler Cloud Security Platform offers the ability to sandbox any malware that VMware Carbon Black Cloud may not yet identify as malicious. If malicious, Zscaler will automatically isolate the endpoint.

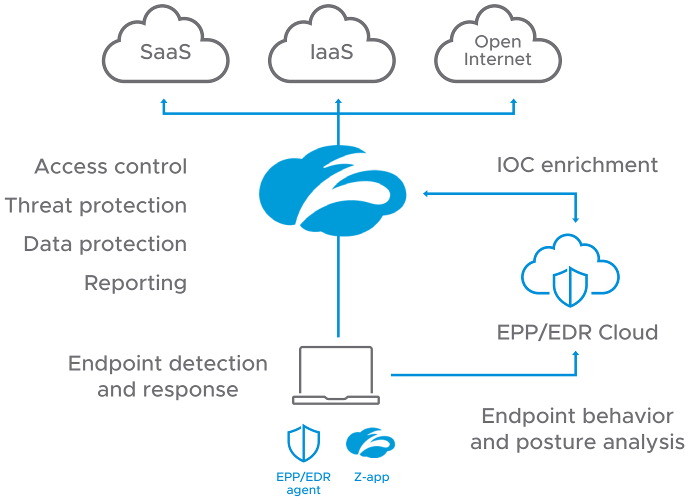
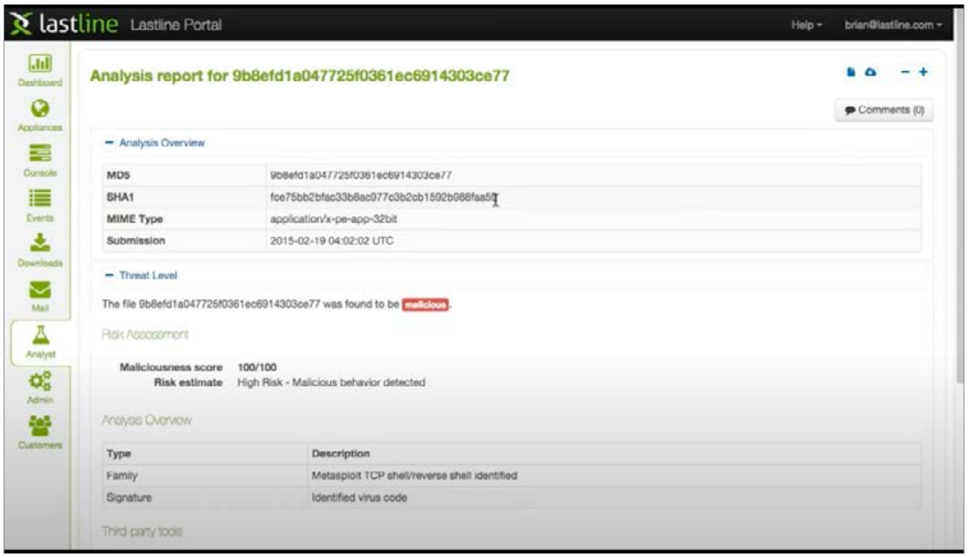


FIGURE 4: Integrated process connecting Zscaler and VMware Carbon Black.

Additionally, the Zscaler platform can also block a user’s request based on their device’s security posture, and whether or not the VMware Carbon Black Cloud agent is installed. If the agent is not installed, the user is presented a warning that explains why the app request or URL was blocked. If the agent is installed, the request is allowed—secured by the endpoint security policy and Zscaler’s ability to enforce network security controls.



Analysis report for 9b8efd1a047725f0361ec6914303ce77

– Analysis Overview

MD5	9b8efd1a047725f0361ec6914303ce77
SHA1	fce75bb2bfac33b8ac077c3b2cb1592b088faa50
MIME Type	application/x-pe-app-32bit
Submission	2015-02-19 04:02:02 UTC

– Threat Level

The file 9b8efd1a047725f0361ec6914303ce77 was found to be malicious.

Risk Assessment

Maliciousness score	100/100
Risk estimate	High Risk - Malicious behavior detected

Analysis Overview

Type	Description
Family	Metasploit TCP shell/reverse shell identified
Signature	Identified virus code

Third-party tools

FIGURE 5: Lastline Portal.

Device posture and sandboxing: threatfeed report and block

Another premier VMware Carbon Black Cloud partner, the Lastline Defender Network Detection and Response (NDR) platform detects and contains sophisticated threats before they impact operations. By integrating VMware Carbon Black Cloud with Lastline’s platform, customers can pull potentially malicious binaries into Lastline’s sandbox to detonate and analyze before they’re downloaded.

After examination, Lastline delivers a ThreatFeed report on each piece of code analyzed, enabling VMware Carbon Black Cloud to look for it in the future, along with adding malicious files to blocklists so all of our customers reap the protection benefits at once.

Where to use it: protection against zero day attacks and unknown threats
Each of the above integrations enhances and extends an enterprise's ability to detect unknown malware and zero day attacks. Since Zero Day exploits are extremely costly for cyber criminals to use (and can only be used once before they're discovered), they aren't deployed as much as broad-based attacks against more widely known vulnerabilities.

Still, the right zero-day exploit delivered at the right time could put a global enterprise at risk for data theft, brand damage, corporate espionage, and more. According to a recent article published by Motherboard, hackers are selling two zero day exploits attacking Zoom users (one for MacOs, and one for Windows) priced at $500K.[7] Since most employees are working from home these days, exploiting these particular vulnerabilities now could have huge downstream effects for many global organizations.

Integrating VMware Carbon Black Cloud with these network security platforms offers bidirectional threat intelligence sharing to detect and disrupt these zero day attacks and other unknown threats, before impact. Whether it's a watering hole attack infecting your website visitors or fears over the next Zero Day Wednesday cycle, integrations like these enable you to disrupt these advanced threats at scale.

Summary / next steps

No enterprise security technology can exist in a vacuum. To provide value, each investment in your security arsenal should be easily and quickly integrated into your existing process and workflows. Security success is directly proportional to the ease with which new technology can be weaved into your current security operations, workflows, and technological infrastructure.

VMware Carbon Black supports more than 100 integrations with best-of-breed technology partners. Additionally, we're one of the few companies to offer publicly available and well-documented APIs, developer tools, and a vibrant user community.

The following checklist can help you choose the right endpoint security solution for your enterprise.

[7] VICE. "Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000" Lorenzo Franceschi-Bicchierai. April 15, 2020.

Checklist: questions to ask endpoint security vendors

1. How many agents does your endpoint security platform require?
○ 1 ○ 2 ○ 3 ○ 4 or more

2. How much CPU on average does your agent consume on each endpoint?
○ 0-1% ○ 1-5% ○ 5-10% ○ 10%+ ○ I don't know, we don't measure it

3. How large is your agent's footprint?
○ < 3MB ____ 4MB-10MB ____11MB-25MB ____ >25MB ____Not sure

4. Does the agent operate at the kernel level or in userspace?
○ Kernel-level ○ Userspace ○ Not sure

5. How many integrations do you currently support with other security vendors?
○ 0-25 ○ 26-50 ○ 51-75 ○ 75-100 ○ more than 100

6. Which OSes does your endpoint security platform support?
○ Windows ○ OSX ○ Linux (RedHat, CentOS, Ubuntu)
○ Legacy versions of Windows (e.g. XP, Server 2003, etc.)
○ Legacy versions of Linux (e.g. RedHat/CentOS 5)
○ Variants such as 32- and 64-bit

Which of the following functions does your endpoint security platform support? (select all that apply)
○ EDR ○ NGAV ○ Threat Hunting ○ File Integrity Monitoring
○ Audit and Remediation ○ Live Query ○ Secure Remote Access

Which of the following prevention mechanisms is possible with your endpoint security platform?
○ Cloud-based Machine Learning ○ Local Machine Learning
○ Cloud-based Behavioral Analysis ○ Local Behavioral Analysis
○ Signature-based

7. What type of endpoint activity do you collect and analyze? (select all that apply)
○ Process starts, stops, and cross-process injection ○ Network connections
○ File modifications ○ Registry changes
○ Binary / executable / application metadata and full content
○ Memory content and structures

8. Where can I find APIs, tools, and documentation on the following integrations? (select all that apply)
○ Github ○ Our website
○ We don't offer any public APIs or tools, call Tech Support

LEARN MORE

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

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.

For more information, email *contact@carbonblack.com* or visit *carbonblack.com/epp-cloud.*

Which of the following integration types are already supported in the field?
○ SIEM ○ SOAR ○ Sandbox/Binary Detonation Tool
○ Next-Gen SWG ○ CASB

9. Can all collected endpoint data be retrieved from the solution via an API?
○ Yes ○ No ○ Not sure

10. What is the solution's false positive rate? ____________
False negative rate? ____________

11. Does the solution offer automated response features such as the below? (select all that apply)
○ Isolating an endpoint from the network
○ Killing threatening processes / applications
○ Deleting applications, files, registry keys, etc.
○ Locking a user account or forcing a password reset
○ Re-imaging to a known good state

Does the solution allow for response regardless of the endpoint's location/corporate network connectivity?
○ Yes ○ No ○ Not sure

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