Next-Gen Protection for the Endpoint: SANS Review of Carbon Black Cb Defense

In today’s threat landscape, organizations wanting to shore up their defenses need endpoint tools that not only detect, alert and prevent malware and malware-less attacks, but also provide defenders a road map of the systems and pathways attackers took advantage of. Our review shows that Carbon Black’s Cb Defense does all this and more with a high degree of intelligence and analytics. Utilizing a cloud-based delivery system, it makes informed decisions on subtle user and system behaviors that we wouldn’t otherwise see...
How does malware end up on a computer? Once it gets there, what does it do? How do you detect it if the malware is custom-written or simply slightly altered so that it doesn’t match any known signatures? What if an attacker doesn’t use any malware but instead misuses known, trusted applications that already exist on a computer—programs such as Adobe Flash or even a part of the operating system such as a command prompt or PowerShell? Some new PowerShell attacks can be launched over an encrypted communication channel and pivot to other computers within an organization without ever adding any files to the file system.

These attack types are already proliferating, and traditional antivirus is blind to the subtle actions indicating an attack in progress. In the SANS 2017 Endpoint Security Survey, 74 percent of respondents said they had traced compromises to browser-based attacks, and 62 percent blamed social engineering (through phishing).

In today’s threat landscape, organizations wanting to shore up their defenses need endpoint tools that not only detect, alert and prevent malware and malware-less attacks, but also provide defenders a road map of the systems and pathways attackers took advantage of.

Our review shows that Carbon Black’s Cb Defense does all this and more with a high degree of intelligence and analytics. Utilizing a cloud-based delivery system, it makes informed decisions on subtle user and system behaviors that we wouldn’t otherwise see with traditional antivirus tools.

Importantly, it saved us time: Manual correlation and false positives are among the top 10 time-consuming tasks IT professionals hate, according to a recent article in Dark Reading. Rather than toggling between separate security systems, traffic logs and so on, we used a single cloud interface—through drill-down and pivot—to determine whether a threat was a false positive or real.

Overall, the product performed well and gave us visibility into the non-malware attacks we launched against it, including PowerShell attacks, changes in hash values, and running an illicit Nmap program. Some of these we even tried to whitelist, but Cb Defense detected and blocked us based on other malicious indicators that our actions with these tools were creating. The cloud-based dashboard provides a quick overview, which helped us quickly see what was happening on the network, what vectors the attacks took (email, web, app store, etc.), known versus unknown malware detected, information about non-malware attacks detected and more.

---

**Key Differentiators**

Cb Defense integrates next-generation antivirus with endpoint detection and response to monitor all events happening on an endpoint (workstation, laptop or server), based on preset and customized policies. Key capabilities include:

- Prevention of commodity malware, malware variants and file-less attacks
- Intelligent detection and response based on subtle behaviors and actions
- Intelligence; Cb Defense was difficult to trick into accepting whitelisted malicious applications
- Nimbleness; when something suspicious is detected, Cb Defense can perform multiple actions based on preset policy:
  - Report and stop the attack
  - Report and isolate
  - Report only
  - Provide an attack road map, helping operators build a case explaining how it happened
- Easy drill-down and pivot in support of investigations and remediation
- Learning; new attack information is used for future protection
- Ability to work online or offline
- Light agent on the endpoint

---

Cb Defense is a cloud-based security platform, with a lightweight sensor that runs on an endpoint to monitor what is happening in real time. Having security, threat, whitelisting, intelligence, threat hunting and other pertinent data hosted on Carbon Black’s platform is a real advantage. So, too, is the combined knowledge of Carbon Black’s 3,000 customers, which is leveraged to share new attack information across the Carbon Black customer base.

Setup and Installation

SANS reviewed Cb Defense with a mix of computers and virtual machines running both Windows and macOS, some in the lab and some at remote locations to test the ability of Cb Defense to monitor and protect computers that are not on the local network.

There are two options to install: Download the Carbon Black MSI (Microsoft Installer) package from the company’s website and push it out to workstations on the network, or send workstation users an email message with a link for them to download and install the agent. The push option should work well in a normal office environment as part of a login script or group policy. The email option is good for remote users.

Once the agent is installed on an endpoint, it examines the local hard drive to inventory the applications installed on that computer. For this review, we primarily used the default policy for Windows computers and the Advanced Mac Workstation policy for Macs.

Alerts and Permissions

Cb Defense defaults to posting alerts on the dashboard. For high-level alerts, it can also send out an email notification to specified administrators. We found that most alerts were earning a level of 3 through 5, so we set the email alert threshold to 7. See Figure 1.
Cb Defense policies include settings to monitor known applications, unknown applications or specific applications we selected and added into policy. There are two sections of the policy that relate to applications: “Blocking and Isolation,” which includes the options of “Deny Operation” or “Terminate Process,” and “Permissions,” where options are “Allow” or “Allow and Log.” Figure 2 shows some of the operations that Cb Defense will flag.

![Figure 2. Operations Monitored by Cb Defense](image_url)

The default policies were preset for current and older critical threats and worked well. For example, the default policy for blocking files that attempt to extract passwords using `pwdump3.exe`, a well-known program, were automatically enforced when we attempted that attack method on our mock network.

**Protecting Even When Policies Are Changed**

In another case, we mimicked the way attackers typically use a whitelisted program to get around defenses. In this case, we used a whitelisted program, `powershell.exe`. Since `powershell.exe` is part of the Windows OS, it is not considered malicious, and traditional antivirus would not catch these behaviors if PowerShell were being used maliciously.

**TAKEAWAY:**
Modern-day attackers use trusted applications and administrative tools such as PowerShell to get around traditional defenses.
We used PowerShell as an attacker would, such as querying the operating system for credentials. Cb Defense, which takes in a lot of factors to determine whether or not an application is acting maliciously, didn’t allow these actions to execute in our environment. In Figure 3, you can see `powershell.exe` was set up as a “TRUSTED_WHITE_LIST” application, but PowerShell was making calls that were sufficiently suspicious to flag a priority 7 alert. This thwarted the attack by blocking access to additional information about accounts that could be used to penetrate deeper into the system.

In another example, we added an “Allow and Log” rule (to the Permissions section of the policy) so we could whitelist Netcat3 (`nc.exe`), which is an open-source utility often used by attackers to create backdoors for trafficking commands and sensitive data. We chose “Allow and Log” over simply “Log” so we could track Netcat operation. While we wanted to use Netcat legitimately, since attackers also use it, logging activity is good practice.

We tried the same thing on the Mac using Cb Defense’s Advanced Mac Workstation policy to alert if an application tries to scrape memory, inject code or modify the memory of an existing process, which it did. These activities on the Mac were alerted but not blocked.

---

Both the Windows and Mac policies did a good job of logging activity and stopping malware per policies. While threats are advancing, stopping known bad malware is still a critical function for organizations looking to replace their traditional antivirus solution. For example, Figure 4 shows that the CoinThief malware, designed to steal digital currency, was stopped.

Figure 4. Malicious File Logged and Blocked
Dashboards and Reports

The Cb Defense dashboard is accessed through a web portal that gives a brief status report on recent activity, what attacks have been detected, the attack vector (web, email, app store, etc.), and the health of the monitored devices, as seen in Figure 5.

![Figure 5. Status Report Shown on the Cb Defense Dashboard](image)

The dashboard doesn't auto-refresh with new behavior data, but running a keepalive plug-in causes the page to automatically reload and update with the latest data—saving the security operations center staff the trouble of having to log back in every 60 minutes to keep the behavior data current.
Easy Drill-Down

From the dashboard, we could click on any of the items to drill down for more detail. For example, Figure 6 shows one day’s worth of “Known Malware” detected.

The malware in this case is `pwdump3 .exe`, a relatively old piece of software used to extract user credentials from a system. This screen also shows `pwdump3` started to run but was killed, along with the time that happened, the computer it happened on, and the registered email address of the user.

Clicking on the small arrow to the left of this report gave us more detail, as seen in Figure 7.
Finding the Source

Every alert is accompanied by a set of three icons, shown below the words “Take Action” in Figure 7. From left to right, these icons are Attack Visualization, Investigate and a dropdown menu to dismiss the alert or view notification history. Clicking the Attack Visualization icon shows the full-picture view of the attack’s origin and activities. See Figure 8.

As you can see, the malware was invoked by Windows Explorer, which is shown accessing multiple files. Specifically note the “read memory” line between pwdump and Explorer. It shows the attack attempting to inject code into `explorer.exe`. The action was automatically denied when `pwdump3.exe` was identified as known malware.
Taking Action

The tool also provides an external means of confirming whether or not a blocking action is warranted. The “Take Action” dropdown menu button allows you to whitelist the application, blacklist it, delete it or request an upload from the infected computer to the sensor. It also includes the option to open a browser to other resources on the Internet to get more context.

As seen in Figure 9, the victim computer (cfdisk-PC) downloaded malware when using the Chrome browser to connect to a web server in the test lab. The malware was blocked from execution.

That’s a quick overview of Cb Defense. The solution collects a lot of valuable information, and dashboards enable easy pivot through the attack information. Overall, the product provides more details about what happened for investigation and remediation than would be possible with simple antivirus, an IDS or a combination of those tools.

In the next section, we will detail our attacks against Cb Defense and how well it stood up to them.
When we ran samples of malware and loaded them onto the hard drive, Cb Defense detected and terminated the processes immediately, per our policy. (Our policy was set up so that when malware arrives on the drive, it logs an alert, and when the malware attempts to run, the process is terminated.) It did so with strong visualization capabilities and easy, intuitive pivot screens. Figure 10 shows the “Attack Visualization” screen for a piece of malware (XSLCmd) that was detected on a MacBook.

This showed that the malware had not been allowed to run. We selected the “Delete Application” option from the Take Action dropdown menu, and the file was deleted in under two minutes, which was the next time the MacBook checked in. (Sometimes this can take up to 10 minutes, depending on the check-in cycle.)
Netcat Backdoor

Netcat is an open-source penetration testing tool used by network administrators, pen testers and attackers that allows a variety of traffic to be transported—or concatenated—over a network interface (hence the name). It is also commonly used as an attack tool to deliver a malicious shell (Linux or macOS X shell or Windows command prompt) to another computer over an Internet connection.

Because there is no actual malware involved, and because it is a legitimate application, this type of attack is easily hidden on the network. Cb Defense ably detected our Netcat activity, setting up a listener on a Linux host as an attacker, and then using one of our Windows computers as the victim connecting to it. This demonstrates how Cb Defense understands and blocks common attack techniques without needing to rely solely on the reputation of the software being executed. See Figure 11.
When we tried to set up the connection, it was automatically blocked by Cb Defense, which issued a report we could drill down into.

**Changing the Hash Value**

In another attack, we tried to thwart the Netcat detection by changing the name and hash of the executable. To do that, we initially appended text to the file (``echo "abc" >> nc.exe``), but that was blocked. We then copied text to the end of a new file (``copy /B nc.exe + "abc" test2.exe``) and got a functional copy of Netcat with a different name, size and hash. We used that new executable to attempt to establish a backdoor connection, and it was also blocked (see Figure 12).

The intelligence and analytics behind Cb Defense were able to detect the functionality, actions and behaviors of our `Test2.exe` program, even though it was no longer a “KNOWN_MALWARE” match because we had changed the hash.
Blacklisting

When we added the Netcat hash to the blacklist, the running Netcat backdoor (nc) was immediately terminated. Further attempts to start nc on the laptop failed, with an “Operation not permitted” message, as shown in Figure 13.

Overall, Cb Defense did a good job blocking known malware and specifically blacklisted files on both the Windows and macOS platforms.

Hiding in PowerShell

PowerShell is used by administrators to manage computers on the network. It can also be used by attackers to take over an endpoint without detection. Because it is part of the Windows operating system, PowerShell won’t trip any antivirus signature alerts. Our question was whether Cb Defense would ignore PowerShell attacks, because PowerShell is fundamentally a whitelisted application.
We first tried to get a list of plain-text keys of wireless connections. We opened a command prompt and started PowerShell, executing the command `netsh.exe wlan show profiles name=* key=clear`. Figure 14 shows that our malicious program attempted to run but failed.

![Figure 14. Failed PowerShell Event in Cb Defense](image)

That report also shows who the user was, the IP address and the command line that was executed. And it shows that the parent process involved in the attack was PowerShell.
Credential Extraction

We also tried to extract credentials using a combination of PowerShell and Mimikatz, a security research tool that is sometimes abused by attackers for malicious credential scraping. We started by loading the attack in memory without ever installing Mimikatz on the local hard drive (of a standalone Windows workstation and a workstation that was joined to a domain). Cb Defense blocked the connections and gave them a high alert priority, shown in bright red in Figure 15.

This attack visualization enabled us to see that PowerShell was launched from the command prompt (cmd.exe) and that it used a memory injection attack against lsass.exe. We could also see that it communicated with two external hosts. This information is critical in blocking future attempts at this attack, going way beyond blacklisting and reputational data such as malicious host IP addresses. It also detects and blocks based on the individual actions that attackers take using tools such as PowerShell and Mimikatz, and what series of actions should and should not be allowed.

Figure 15. A Cb Defense Alert on a Mimikatz/PowerShell-Based Attack

---

Tactics, Techniques and Procedures

The TTP (Tactics, Techniques and Procedures) section of the dashboard (Figure 16) showed us the trajectory of this attack: scraping RAM, reading security data and modifying processes.

These are processes that most legitimate software does not do, but when the combination of activities occurs, the behaviors trigger alerts in Cb Defense’s console. In this case, this attack earned a priority of 7, which is pretty serious. However, if you aren’t sure, you can click on the file to find out.

To avoid getting bombarded with alerts while testing, we had set priority 7 as the threshold for receiving email notifications. The notification we were sent on this attempt to extract domain credentials included a brief overview that was helpful and not overly wordy: “The application **powershell.exe** read memory from a system security process (**lsass.exe**). This may have included user credential or password information. A Deny Policy Action was applied.”
It also included specifics: the user, the target’s value, the device, the threat score and some TTP information. In this case, the application was PowerShell, and the indicators were:

- Modify Memory Protection
- Modify Process RAM Scraping
- Policy Deny Packed Code
- Network Access
- Enumerate Processes
- Active Client
- Read Security Data

**Visualization: Attack Kill Chain**

One way to visualize the progress of an attacker within a network is to look at the kill chain, a concept originated in the military as a framework for defining the phases of an attack so that attacks can be identified before they succeed (see Figure 17).

The dashboard below summarizes the attacks Cb Defense stopped and at which stage in the kill chain each attack was when it was stopped.

---

The alert from Cb Defense was an example of what Windows security expert Randy Franklin Smith calls good-guy code watching out for bad-guy code.5

---

This reinforces the unique approach Cb Defense takes to detecting and blocking attacks; instead of relying only on detecting malware in the install/run stage like most antivirus products, Cb Defense can be used to block attacks at any stage of the kill chain.

Previously, as shown in Figure 16, we attempted an instance of recon, triggered by Nmap being used for a port scan. At the other end of the chain, “Execute Goal” was triggered by PowerShell being used to extract user credentials on Windows computers. It also detected a reverse shell being used on Windows and Mac computers to launch internal port scans and other internal attacks from the compromised endpoints.

Given the short window of time in which administrators have to respond to attacks in progress, we find Cb Defense to be a useful tool for detecting malicious actions hidden under the guise of approved applications. Reports provide full-spectrum visibility into the details of the attack, which gives investigators a road map to follow and assists with remediation.

---

5 About Randy Franklin Smith, [www.ultimatewindowssecurity.com/about/rfs.aspx](http://www.ultimatewindowssecurity.com/about/rfs.aspx)
Dealing with malicious attacks against computer endpoints is a constantly shifting battle. The bad guys come up with new attack methods that fly beneath our traditional antivirus protections, and we need accurate visibility into these threats so we can protect against them.

Attacks that place executable files on a computer’s hard drive could be spotted by traditional antivirus tools.

But when attacks leverage programs that already exist on the endpoint, defenders have to detect subtle signs of suspicious activity, connect the dots and get full visibility into the actions that make up an attack. Some recent attacks don’t even use malware; by using software that is built into the Windows operating system, they don’t leave remnants on the file system for antivirus signatures to detect and remove.

Cb Defense did a good job detecting and blocking suspicious activity such as scraping memory in an attempt to harvest user credentials or launching applications that would be used to spread the attack, as well as sending out notifications when critical thresholds of suspicious activity were reached.

Cb Defense’s integrated endpoint detection and response and next-generation antivirus work together for better detection and visibility into threats, enabling fast remediation based on policies, as well as providing future protection against new behaviors that are analyzed and determined to be malicious.

We also appreciated that it allowed us to set our own thresholds for blocking and email alerts, with the ability to update policy as needed—all from a single, cloud-based console.

Using the cloud to process and disseminate endpoint threat information will become increasingly important to organizations looking to streamline their security operations and reduce stress on their staff.
**About the Author**

**Jerry Shenk** currently serves as a senior analyst for the SANS Institute and is senior security analyst for Windstream Communications, working out of the company’s Ephrata, Pennsylvania, location. Since 1984, he has consulted with companies and financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans networks of all sizes, from small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds six GIAC certifications—all completed with honors—and five with Gold certifications: GCIA, GCIH, GCFW, GSNA, GPEN and GCFA. He also holds the CISSP certification.

**Sponsor**

*SANS would like to thank this paper’s sponsor:*

**Carbon Black.**
<table>
<thead>
<tr>
<th>SANS Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Dallas 2019</td>
<td>Dallas, TX US</td>
<td>Feb 18, 2019 - Feb 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2019</td>
<td>Tokyo, JP</td>
<td>Feb 18, 2019 - Mar 02, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich February 2019</td>
<td>Zurich, CH</td>
<td>Feb 18, 2019 - Feb 23, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2019</td>
<td>Bangalore, IN</td>
<td>Mar 04, 2019 - Mar 09, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS St. Louis 2019</td>
<td>St. Louis, MO US</td>
<td>Mar 11, 2019 - Mar 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2019</td>
<td>Orlando, FL US</td>
<td>Apr 01, 2019 - Apr 08, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2019</td>
<td>London, GB</td>
<td>Apr 08, 2019 - Apr 13, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 Stuttgart February 2019</td>
<td>OnlineDE</td>
<td>Feb 04, 2019 - Feb 09, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s Only US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>