Hunt Like a Pro: A Threat Hunting Guide
In a recent SANS survey, a resounding 82 percent of companies said they anticipate loss or theft of data resulting from an unsecured internet-connected device or application. By preparing for the inevitable breach, rather than expecting that it will always be prevented, enterprises can deliver a better security posture and set the foundation for their team to proactively hunt for threats. With that said, many organizations still focus on — and prioritize — the wrong protection techniques across their environment. Despite the fact that corporate endpoints such as servers and user devices made up the top five assets involved in breaches last year according to Verizon, many enterprises still focus only on securing their network. Today, an increasingly mobile workforce and the explosion of enterprise data and applications in the cloud have expanded the attack surface beyond the traditional network perimeter. In short, the endpoint is the new perimeter.

However, even if an enterprise is focusing on its endpoints, it typically prioritizes detection capabilities over data collection. This makes it difficult to expand detection beyond the moment of compromise and accelerate the discovery of the most sophisticated threats. Additionally, most attackers take minutes to compromise an enterprise. When they do, an advanced attacker can escalate their privileges and establish persistence in a given environment. If acquired, the attacker can essentially “live off the land” by using trusted tools to move in and out of an organization, as well as exfiltrate data. This whitepaper will explore why 91 percent of organizations reported improvements in the speed and accuracy of response due to their threat hunting practices, and will outline the capabilities and best practices necessary to proactively and efficiently hunt for threats across your enterprise, ultimately tilting the advantage from the attacker back to the defender.
Non-malware attacks are on the rise. Only 30% of attacks use malware.\(^7\)

77% of organizations said endpoint data was critical for conducting proactive threat hunts.\(^9\)

**THREAT HUNTING DEFINED**

Threat hunting is a proactive process that looks for abnormal activity. Threat hunters search for anomalies on servers and other endpoints to glean evidence of intrusion, including legitimate programs performing in unusual ways. With non-malware attacks on the rise, the threat hunting process is becoming critical for enterprise security. According to Verizon’s 2018 Data Breach Report, only 30 percent of attacks actually use file-based malware, meaning traditional antivirus (AV) and perimeter defense solutions cannot address many of these new threats.\(^6\) Most enterprises recognize it is no longer a matter of if they will be compromised, but when. As a result, many businesses are looking for a detection and response solution that not only answers the question: “Is this behavior happening in my environment right now?” but also, “Has this ever happened before?” To do so, they need tools that not only detect and respond to threats, but can proactively hunt them as well. To hunt for threats, enterprises need tools that can accelerate their threat discovery to identify a potential compromise before it’s too late.

**EXISTING CHALLENGES AND SOLUTIONS**

Many enterprises overload on detection capabilities from network security and/or threat intelligence providers. Although these capabilities can be useful, they are still only a fraction of your overall security stack. The majority of respondents (77 percent) in a recent SANS survey said that endpoint data was critical for conducting proactive threat hunts.\(^8\) If you are only deploying scan-based technologies on the endpoint, or rely on a tool that filters out information not known to be malicious yet, you are leaving gaps in your data collection coverage, and losing the full context of any attack. This is particularly dangerous considering that newer, more advanced techniques often exploit trusted software. When preparing to hunt for threats, ensuring that your endpoint security tools can continuously collect all the critical data necessary to conduct immediate and conclusive threat discovery is indispensable. Combing through logs and SIEM data for indicators of compromise (IOCs) can be tedious, time
consuming and expensive. By proactively capturing and storing all unfiltered endpoint activity, whether known to be bad or not, enterprises can instantly leverage a comprehensive historical record of their environment for effective threat hunting.

**THREAT HUNTING ON THE VMWARE CARBON BLACK CLOUD**

After years of leading the industry with Carbon Black EDR, our endpoint detection and response solution formerly known as CB Response, VMware Carbon Black has introduced the next generation of threat hunting and incident response (IR) on the VMware Carbon Black Cloud with the release of Enterprise EDR.

Enterprise EDR, formerly CB ThreatHunter, takes all the capabilities of Carbon Black EDR, together with powerful new enhancements, enabling customers to prevent, detect, respond to, predict and now, hunt threats from a single cloud platform. Carbon Black EDR on the Carbon Black Cloud delivers best-of-breed threat hunting and incident response functionality from the same agent and console as our NGAV, EDR and real-time query solutions, allowing teams to consolidate multiple point products with one converged cloud platform.

Leveraging the power of the Carbon Black Cloud, Enterprise EDR automates the enterprise-wide activity collection process, continuously recording all endpoint activity, much like an always-on surveillance camera. The result is comprehensive endpoint visibility that retains the recorded relationships of every file execution, file modification, registry modification, network connection and executed binary in an environment. Together with insights delivered via the Carbon Black Cloud, organizations can efficiently classify threats to accelerate their threat hunt.
LEVERAGING COMPREHENSIVE THREAT INTELLIGENCE

With Enterprise EDR, enterprises benefit from a holistic approach to threat hunting by layering a variety of custom and out-of-the-box threat intelligence feeds, delivered via the Carbon Black Cloud, over the continuously recorded endpoint data. This enables organizations to classify threats based on software reputation, network communication, open-source malware tracking, community-sourced threat intelligence, malicious domains, custom intel and the latest curated intelligence from the Carbon Black Threat Analysis Unit (TAU).

With its in-depth process search, Enterprise EDR empowers security teams to uncover threats based on threat intelligence feeds, or by searching across all attack processes captured by its unfiltered data collection. Utilizing Enterprise EDR’s unique watchlist capabilities, any process search run in the Carbon Black Cloud console can easily be saved as a watchlist to deliver ongoing automated detection and response.
98% of breaches, attackers take minutes or less to compromise systems.\textsuperscript{10}

**EXPAND DETECTION BEYOND THE MOMENT OF COMPROMISE**

Today, compromises are measured in minutes whereas the speed of response is measured in days or months.\textsuperscript{11} Enterprises the world over are realizing that to close the gap, they need to evolve their security operations from being a largely reactive unit (waiting for alerts that indicate a threat) to being proactively on the hunt for new attacks that have evaded detection. Many enterprises have trouble discovering advanced threats quickly because they rely exclusively on the limited detection capabilities of legacy antivirus solutions, or EDR tools with secret “black box” analysis that arbitrarily filters out activity it believes to be benign. The figure below demonstrates how AV signatures will only ever be effective at discovering opportunistic attackers. Opportunistic attackers find value in scale. Their objective is to compromise as many endpoints as possible since it is likely that a signature will be developed shortly after the attack is first used. The advanced attacker, who only targets a few specific, high-value assets needed to accomplish the mission, can stealthily remain below the detection threshold. The attacker can therefore spend a significant amount of time within a compromised network without registering a signature, if one registers at all.

Once inside, an advanced attacker will move laterally to more critical systems in an attempt to escalate their privileges and access sensitive data. If the attacker succeeds, he or she can come and go as they please within a given enterprise and evade future detection by “living off the land,” leveraging built-in trusted software...
to reduce the number of new executables and the amount of change they introduce into the environment. By proactively deploying unfiltered data collection to track an attacker’s every move, enterprises can hunt across their adversary’s entire attack chain, whether it’s happening now or a month ago.

The example above illustrates the shortcomings of endpoint visibility provided by most security solutions. If a new, zero-day attack is unfolding in your environment, working with anything less than unfiltered data means previously unknown malicious behavior will not be recorded. With Enterprise EDR, new threat intelligence from the Carbon Black Cloud can be applied to both real-time and historical detection. Threat hunters can effectively hunt through time and not only determine if their environment is currently at risk to a new threat, they can go one step further and definitively answer the question, “Has this threat ever existed in my environment?”
In a recent survey, 88 percent of organizations reported reductions in dwell time (infection to detection) as a direct result of their threat hunting practices. Enterprise EDR offers powerful and comprehensive threat hunting and incident response (IR) in the cloud. It enables security operations centers (SOCs) and IR teams to quickly and accurately hunt for anomalies. Enterprise EDR continuously records and centrally stores comprehensive threat activity enabling security teams to hunt for threats in real time, visualize a complete, interactive attack kill chain and quickly respond to and remediate the threat.

The following screenshots illustrate a typical threat hunting scenario. Let’s say, for example, you read the latest Verizon Data Breach Investigations Report that says 30% of phishing messages are opened by targeted users and 12% of those users click on the malicious attachment or link. You decide you want to begin hunting for this type of activity. With Enterprise EDR you can instantly search across all endpoints and processes with a simple search. In this case, we want to see what other processes have been spawned as child processes of our email client.

“The combination of rapidly searchable, unfiltered endpoint data for advanced threat hunting, combined with an array of prevention and response capabilities built-in to one endpoint sensor is a significant step forward. Enterprise EDR further enhances our ability to deliver rapid incident detection and response to our global customers.”

— Marc Brawner | Principal, Cyber Risk | Kroll
When analyzing this binary on the process analysis page, Enterprise EDR displays a variety of information to put the activity into context. You immediately see that Outlook spawned Excel, which seems rather normal. But digging in a little deeper, you notice it was spawned with Microsoft’s Dynamic Data Exchange (DDE) enabled, a common attacker technique. More obviously however, it looks like Excel spawned PowerShell. Although Microsoft’s PowerShell is preinstalled on nearly all Microsoft systems and is considered trusted software, seeing it launched via Excel is highly anomalous and definitely suspicious.

When you run your search, one result on the list seems particularly suspicious. To dive in further, you click on this particular binary to open up Enterprise EDR’s process analysis view.
Taking a closer look at this instance of PowerShell, we see all kinds of indications that this is malicious activity. Not only has PowerShell been initiated in a suspicious way, but we see it has made a network connection and the commands associated with the process clearly indicate an effort to obfuscate what is actually being run. The attacker has even encoded commands in Base64 to further obfuscate the malicious activity to evade legacy antivirus and other traditional means of detection.

Below the process analysis view, we can filter the activity to only show file modifications associated with this instance of PowerShell. Here we can easily see when and where file modifications were made, as well as relevant file hashes. Among the file modifications listed, we see that PowerShell has written a suspicious batch file to disk.
Looking further into the process tree of this attack reveals these trusted applications are being used to execute the files that PowerShell wrote. Although each of these binaries might be trusted or signed, executing in this way with encoded commands is clearly an indicator of a malicious attack.

Now that you have reason to believe this behavior is malicious, you can instantly isolate the endpoint from your network (allowing only a secure connection to the Carbon Black Cloud) and begin your remediation process directly from the console. We can also leverage Live Response to establish a secure connection for killing processes, perform a memory dump, or push down another IR tool.

CLOSING THE LOOP

Your threat hunt will not unmask evil every time, but when you do uncover malicious activity, Enterprise EDR makes it easy to ensure you never fall victim to the same attacker tactics, techniques and procedures (TTPs) twice. You can save the search queries you used in your threat hunt as automated watchlists, which going forward, will automatically detect the patterns of malicious activity you uncovered. This allows you to hunt once manually and then automate that hunt going forward, forcing the attacker to completely rethink their technique, not just change their IP address.
Enterprise EDR makes it easy to save a search as a watchlist to help harden your defenses against that behavior in the future. Watchlists provide ongoing detection even after you’ve completed your hunt, automatically triggering alerts and containment actions for similar malicious behavior based on both historical and real-time activity. This eliminates the need to manually address the same security holes over and over by leveraging time-saving automation.

“The watchlist component is a valuable tool in which our staff can craft custom events, sequences, or procedures which indicate bad behavior on the system.”

— Kevin Kraft | IT Director | Bowman & Company LLP
JOIN A GLOBAL COMMUNITY OF EXPERTS

As the latest variant of the global Petya cyberattack made waves, paralyzing numerous organizations across the globe, VMware Carbon Black’s Threat Analysis Unit worked through the night with over 100 VMware Carbon Black customers, actively analyzing and sharing new insights and indicators of compromise in our online community. Hour by hour and hash by hash, our community of over 27,000 security professionals absorbed all the latest intel available as seasoned experts weighed in for the benefit of the entire community.

Access to the User Exchange Community is included for all VMware Carbon Black customers. As new threats and indicators are posted, the VMware Carbon Black Threat Analysis Unit scours and curates all the shared threat data and reinfuses the intelligence back into the Carbon Black Cloud to ensure that all customers, no matter which products they use, can benefit from what other customers see and learn. In addition, the Threat Analysis Unit regularly posts Threat Intelligence Notifications (TAU-TINs) to inform customers about existing and new threat detection/prevention capabilities for new, emerging threats across VMware Carbon Black’s products.

“The analysis & IOCs provided by security experts in Carbon Black’s global community were most helpful... All IOCs were pre-banned across endpoints prior to infection.”

— Caleb Cromun  |  System Engineer  |  Samaritan Ministries
Conclusion

With the number of advanced attacks increasing every day, and most going undiscovered by traditional AV or detection and response tools, hunting for threats in a sea of noise can be a laborious task. To combat this, enterprises must:

JOIN A GLOBAL COMMUNITY OF EXPERTS
Organizations need to continuously record all endpoint activity to be able to fully scope and remediate an attack, whether it occurred today or a month ago.

LEVERAGE COMPREHENSIVE THREAT INTELLIGENCE
Alongside continuous data collection, enterprises must possess the capability to layer threat intelligence and reputation over the data they collect to instantly classify and prioritize threats, accelerating the threat discovery process.

EXPAND DETECTION BEYOND THE MOMENT OF COMPROMISE
Businesses should deploy solutions that can hunt both past and present threats based off of a continuously recorded history, not just from individual events from a single point in time.

Organizations need to continue to make the endpoint a priority when it comes to information security. When proactively hunting for threats, enterprises need a solution that allows them to hunt across one comprehensive set of data, not just the handful of IP addresses and hashes. Enterprise EDR on the Carbon Black Cloud delivers a powerful solution to hunt for threats, accelerate threat discovery, respond in seconds and proactively prepare businesses for a breach.
To schedule a live demo or obtain more information on how Enterprise EDR protects financial institutions, contact a Carbon Black sales representative today!

Send us an email at: contact@carbonblack.com
Give us a call at: (855) 525-2489