Enterprises face an uphill battle when it comes to protecting their endpoints and defending against the myriad of aggressive, targeted and sophisticated cyberattacks they face on a daily basis. Environments are diverse, dynamic and increasingly remote. With thousands and thousands of endpoints comprised of varying operating systems and purposes, and often handling sensitive company information completely off the corporate network, globally-defined solutions like legacy antivirus (AV) are more cumbersome than their worth.

Advances in cloud and communications technology have paved the way for a mobile workforce; free from the corporate network, these end users can access all the critical assets and data they need to accomplish their jobs without stepping foot on the protected corporate network. They work from home or public venues, accessing cloud-hosted solutions from their laptops and phones with ease. This has eroded the network perimeter and placed the onus square on the backs of endpoints to protect the business’s most valuable information from cybercriminals.

Additionally, advances on the side of cybercriminals have elevated and streamlined the use of hacking techniques that completely bypass legacy and even some more modern antivirus products. Malware is used only half the time to breach a network, and even then it is likely tailor-made to infect that specific target; legacy antivirus by nature only detects and prevents known malware. In either case, endpoints are blind to these techniques, which in turn leaves security teams unable to respond effectively, if at all.

However, managing multiple point solutions designed to address specific issues on the endpoint is also untenable given the oft over-worked, understaffed security teams that support even the largest enterprise. Simply put, stopping attacks before they reach their destructive ends is difficult to do with traditional technologies and approaches, and the experiences of enterprises around the globe are exponentially more difficult given the vast number of endpoints, limited visibility and stretched priorities.
Enterprises need a comprehensive security strategy that addresses the reality of protecting endpoints at scale from advanced targeted attacks; stop as much as possible, but be prepared to address the threats that do get through by enabling security teams to respond to attacks in progress as quickly as possible.

In order to stop attacks in progress, shutting them down before they carry out their malicious ends, enterprises need to invest in emerging endpoint security platforms like next-generation antivirus (NGAV) that incorporate endpoint detection and response (EDR). However, they must ensure the platform is enterprise-ready, able to withstand the scalability demands and administrative requirements inherent to large organizations.

This whitepaper intended to help enterprises assess their current capabilities and guide their upcoming discussions about NGAV + EDR solutions. In particular, it focuses on three primary aspects of NGAV + EDR:

**Prevention**
It must be able to stop all types of malicious behaviors effectively.

**Investigation and Response**
It must support real-time response capabilities that can quarantine and remediate infected endpoints remotely.

**Enterprise Operations**
It must easily scale to support massive, dynamic environments with granular policy needs.
Due to the increased opportunity for financial gain, cyber criminals invest significant time and resources into creating advanced attacks to target enterprises.

According to a recently published report from Sophos, 70% of malware is designed for a single organization. These targeted samples cannot be stopped by legacy AV products that maintain signature databases of known, in-the-wild samples. Plus, most malware attacks employ obfuscation techniques that allow them to run in memory, evading more advanced anti-malware and machine-learning platforms focused on assessing new files that are dropped on an endpoint.

This doesn’t even account for the fact that for the past two years over half of breaches were caused by non-malware attacks. These attacks use sophisticated techniques that evade traditional defenses completely, and, as they require more knowledge of the environment for success, the attackers generally have a higher investment in the attack and therefore adjust and pivot where needed to maintain persistence until they reach their objectives.

**QUESTIONS TO ASK YOURSELF**

- What percentage of attempted cyberattacks resulted in a successful infection?
- How confident are you that your existing endpoint security can detect and prevent all types of attack?
- What is your biggest concern when it comes to preventing unknown, zero-day or non-malware-based attacks?
In response to this, when evaluating NGAV, enterprises should ensure that the platform:

1. Has capabilities to detect and prevent non-malware techniques; not just capabilities like static or dynamic analysis that only address file-based attacks.
2. Can detect malicious behavior from unknown sources; those that do not have reputation or have not been seen in the wild.
3. Can address new and emerging threats (like ransomware) that experience rapid innovation and implement new techniques faster than signature-based approaches can be deployed.

Unlike other solutions that focus on blocking commodity malware, Cb Defense mitigates risk of a breach caused by advanced and targeted threats that enterprises face on a daily basis:

- Blocks custom-built threats targeted at enterprises
- Prevents sophisticated non-malware attacks that bypass tradition AV
- Enables you to future-proof your ransomware defenses

**KEY FEATURE**

**Streaming Prevention**

Cb Defense’s prevention technology was built and tested against emerging threats and targeted attacks that are critically important to high-profile enterprises. It analyzes events and how they connect (event streams) to uncover malicious behavior as it unfolds.
Fast Investigation & Response

During a response scenario, every minute counts. The longer it takes to address an issue the more risk your business faces.

COMPROMISES ARE MEASURED IN MINUTES OR LESS 98% OF THE TIME. ²

Visibility is the foundation of investigation and response. Without a full picture of everything that’s happening and has happened, response teams are at a significant disadvantage to address threats at their core. Since compromises are measured in a matter of minutes, response teams need to be able to go from a detection of a potential indicator of attack to root cause analysis in nearly the same amount of time if the negative effects of the breach are to be mitigated. To achieve that level of speed, you need the right data and the ability to analyze and prioritize it quickly and efficiently.

After an incident has been discovered, new risks emerge; unscheduled downtime of systems and people can cost the business greatly, and resources dedicated to reimaging can pull away from other critical IT activities. This is a function of the dated separation between IT operations and security; it unnecessarily gets more groups involved to perform time-intensive tasks related to fixing endpoints targeted in an attack.

QUESTIONS TO ASK YOURSELF

+ What would you say is your average response time to a security incident (from point of detection to point of resolution)?
+ In a typical month how many machines are re-imaged as a result of a security incident?
+ How confident are you that your security team can easily search for relevant information about infected endpoints during an investigation?
In response to this, when evaluating NGAV, enterprises should ensure that the platform:

1. Provides contextual analysis based on a complete dataset of endpoint events to remove time-intensive forensic activities and fast-track root cause analysis.
2. Contains native capabilities to quarantine infected machines and address their issues remotely.
3. Supports intuitive search functions that help responders find the right information quickly and effectively.

**Cb Defense** provides administrators with faster ways to investigate and remediate attacks in progress, eliminating uncertainty and reducing downtime:

- Faster, more precise investigations to reduce exposure
- Real-time remediation of any endpoint from a central console
- Get end users back to work quickly without calling IT

**KEY FEATURES**

**Live Response**
**Cb Defense** enables responders to establish a secure remote shell into any system to get information, perform memory dumps, or run scripts for full remediation in minutes whether or not they are on your corporate network.

**Enhanced Search**
**Cb Defense** allows your team to search based on key-value categories with auto-populated search suggestions, making it very easy to run more advanced and specific searches to quickly find the information you are looking for.
Enterprises face a shortage of skilled security professionals, and security teams spend too much time gathering the information they need, limiting the time available to perform true security analysis.

According to National Initiative for Cybersecurity Education (NICE), a program of NIST, there are currently 350K open positions in cybersecurity, up 67% from 2015. Despite promising salaries and job security, enterprises struggle to fill these positions. As a result, security teams are looking increasingly at how to automate day-to-day tasks, integrate products and leverage cloud-based platforms to enhance the capabilities throughout their security stack.

To fill these gaps, enterprises need to focus on how to infuse automation and integration into two critical aspects of their security team’s core responsibilities: administration and investigation. Increasing their capabilities with better, contextual data and more powerful prevention and response technologies means they can work quickly and with high precision, while increasing their efficiency with cloud-based platforms that support open APIs for integration and automation make data-sharing easy and free up time to tackle high-priority tasks that require human involvement.

Administration and management are as essential a function as security efficacy; this can be overlooked by enterprises eager to reduce their attack surface with burgeoning technologies.

Questions to Ask Yourself:

- What percentage of your security stack is cloud-based?
- How would you describe the level of automation across your security stack?
- In a typical week, how much time is spent by skilled security professionals doing administrative and data management tasks?
In response to this, when evaluating NGAV, enterprises should ensure that the platform:

1. Supports secure, native integrations with IT and Endpoint management systems to automate tasks like enrollment, policy assignment and deactivation.
2. Supports an open API framework that can easily integrate throughout the security stack, including support for API calls that both pull data and execute actions.
3. Provides intelligent, contextual analysis of endpoint behaviors and malicious activities to empower the entire security team to act rather than relying on in-house, expert analysis to drive action.

The intelligence, integration and automation capabilities in **Cb Defense** boost the productivity of everyone on your security team:

- Hands-free management of devices and policies at enterprise scale
- Automation of remediation tasks for speed and reliability
- Integration with your existing security stack to share data wherever it’s needed

**KEY FEATURES**

**Deploy with Ease**
Mass sensor management allows you to automatically assign endpoint policies based on Active Directory, IP, Machine Name, or OS.

**Auto-Update Your Defenses**
Automatically adapts to brand new attacks, so your endpoint remain protected without requiring manual updates.

**Integrate and Automate**
APIs allow for integration with the rest of your security and IT stack to share endpoint context and automate operational tasks across your existing toolset.
So What Now?

The questions in this assessment are meant to help you drive your initial conversations about NGAV + EDR. Bring them to a product demo, presentation or your weekly team meeting - wherever you are at in your evaluation process. Our hope is that, armed with the right information and questions to ask, you'll be able to get to the topics that are most important to you and your organization.

You can also reach out to us directly if you have any questions or would like to see how Carbon Black’s NGAV + EDR solution, Cb Defense, can help you achieve better prevention, faster response and efficient operations at scale.

[Contact details]

1. Sophos.
3. National Initiative for Cybersecurity Education (NICE), a program of NIST.
Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,300 global customers, including 35 of the Fortune 100, trust Carbon Black to keep their organizations safe. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.

Copyright 2018 | Carbon Black and Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and other jurisdictions