




Carbon Black.

Streaming Prevention in Cb Defense

Stop malware and non-malware attacks that
bypass machine-learning AV and traditional AV





OVERVIEW

Over the past three years, cyberattackers have gained the upper hand. In a defensive industry largely dominated by preventing malware, modern attackers have developed a robust suite of tactics and techniques to penetrate systems and steal data without using malware at all.

Using these tactics, adversaries can reach deep into an organization's systems and pull out virtually any information they seek. These non-malware attacks have quickly become extremely dangerous and prevalent, as they have been weaponized and deployed on a global scale.

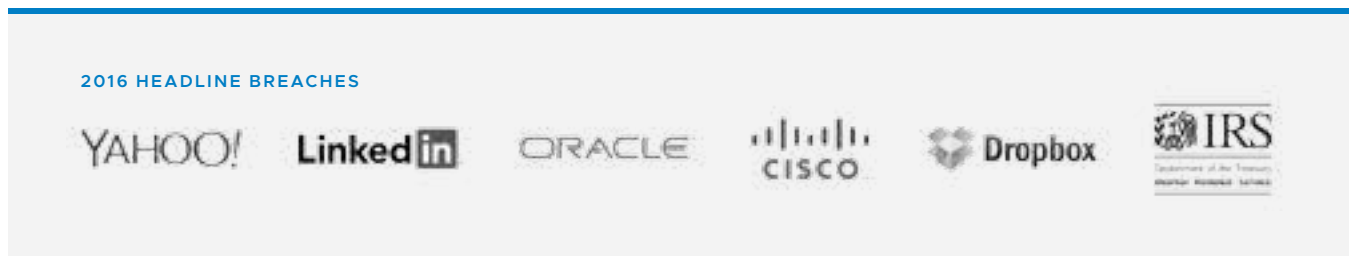
Despite this, many organizations are still defending themselves with machine-learning antivirus (AV) or traditional AV, which only stop malware—addressing only a small part of the problem.

Meanwhile, attackers continue to deploy undetectable non-malware threats any time they please.

It's time for a different approach to endpoint security: one that focuses on and stops all forms of cyberattacks, not just malware.

Non-Malware Attacks and Ransomware on the Rise

Breaches used to be a problem that only the largest, most cash-rich organizations needed to deal with. Unfortunately, that is no longer the case. Businesses of all sizes and in every part of the world are now targets for the mass-market attacker. In fact, almost half of all businesses in the U.S. have been hit by ransomware.



What’s on the horizon is even scarier: non-malware attacks that gain control of computers by using trusted, native operating system tools, such as PowerShell, and exploit running applications, such as browsers. Attackers “live off the land” without downloading any malicious software. These attacks pose a bigger risk than malware attacks because they are undetectable by machine-learning AV or traditional AV and, as a result, cause more damage.



of organizations were targeted by a non-malware attack in 2016



of breaches don't use malware

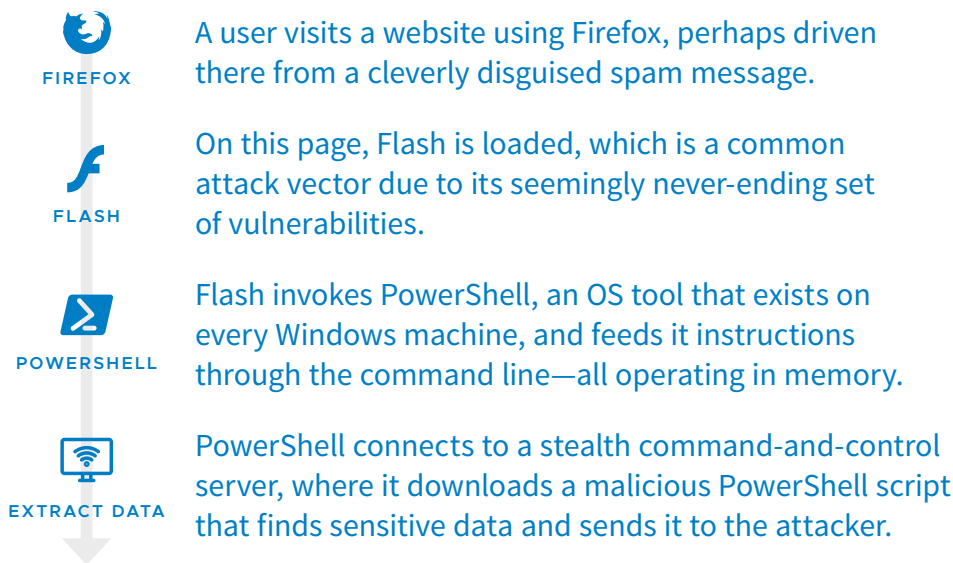


organizations can expect to be targeted by a non-malware attack in the next 90 days

This rise in non-malware attacks should make everyone question why the endpoint security industry is singularly focused on detecting malware. At Carbon Black, we see the bigger picture.

Non-Malware Attacks Bypass Machine-Learning AV and Traditional AV

Non-malware attacks leverage a robust suite of tactics and techniques to penetrate systems and steal data without using malware at all. They have grown in prevalence in recent years as attackers have developed ways to launch these attacks on a large scale.



This attack never downloads any malware. As a result, traditional AV or machine-learning AV will not even see the attack, let alone stop it. These protective technologies are designed to only identify threats at a single point in time when a file is written to disk. Since they only look at the attributes of an executable file, they are completely blind in the face of attacks where no files are involved.

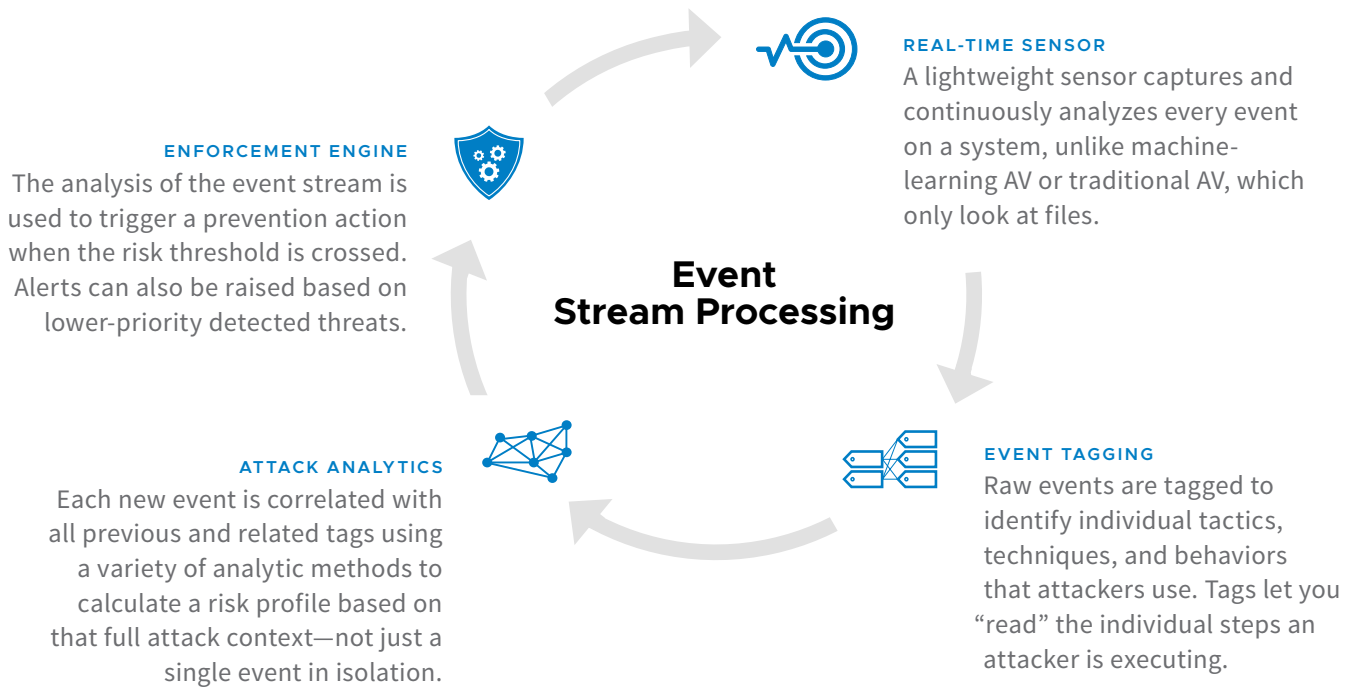
For attacks that still involve malware, machine-learning AV and traditional AV fail when files do not look like malware they have seen before. By only looking for malware, these products ignore the overall context of the attack, dramatically reducing their effectiveness.

Think about it: A website spawns PowerShell, downloads a script, and automatically tries to execute it. That sequence of activities should never happen. By zooming out and looking at the full scope of the activity, it becomes crystal clear that the stream of events outlined above is an attack that should be stopped.

Streaming Prevention: Breakthrough Prevention That Stops All Forms of Attacks

For decades, the foundation of the AV industry has been malware prevention, from the earliest signature-based methods to modern, machine-learning-AV products. Clearly, just stopping malware is not sufficient.

This is why Carbon Black developed streaming prevention, a breakthrough endpoint security technology that applies a fundamentally different approach to preventing cyberattacks. Streaming prevention is designed to stop all types of attacks, not just malware, making it uniquely suited to address the growing realities of today’s threat landscape.






EVENT STREAM PROCESSING

What Is Event Stream Processing?

Event Stream Processing identifies meaningful patterns within streams of data. It takes into account cause-and-effect, timing, and relationships among events. It has transformed many industries: algorithmic trading, fraud detection, telecom, and more. Carbon Black is the first to bring event stream processing to endpoint security.

Streaming prevention is a foundational part of the Cb Defense Next-Gen Antivirus (NGAV) solution. Cb Defense stops not just commodity or zero-day malware, but also non-malware attacks including macros, scripts, memory attacks, and the malicious use of good software, such as PowerShell.



Head to Head: What Provides Better Security?

THE APPROACH

Streaming Prevention is a breakthrough prevention technology designed to stop all forms of cyberattacks, not just malware, by analyzing the full scope and context of every attack.

THE TECHNOLOGY

Event Stream Processing applies advanced analytics to all attack data— processes, applications, network, and files— even as the attack moves across processes and through memory.

Machine-Learning AV uses statistical analysis to determine if an executable file is malicious, replacing antivirus signatures with a sophisticated mathematical model.

Static Analysis applies machine-learning algorithms at a single point in time (when a file is written to disk) without evaluating additional context from the attack.

RESULTS

- ✓ **Prevents Malware and Non-Malware**
Sees the entire attack sequence, whether it contains malware or not
- ✓ **Difficult to Bypass**
Monitors the tactics attackers use to carry out an attack and shuts them down
- ✓ **Pre-Delivery, Pre-Execution, Mid-Execution**
Detects and prevents attacks at any stage of execution by continuously monitoring dynamic behavior
- ✓ **High Confidence**
Analysis of the entire attack stream means prevention and detection decisions are made with very low false positives
- ✓ **Detection and Response**
Fully converged prevention, detection, and response
- ✓ **Visibility**
Complete visibility into full attack including root cause
- ✓ **Analytics**
In-cloud and on-device, continuously updated
- ✓ **Ease of Use**
Lightweight and easy for all attacks

- ✗ **Only Prevents Malware**
Blind to attacks that do not utilize malware, such as PowerShell and script-based attacks
- ✗ **Easily Bypassed**
Attackers have an endless supply of malware and proven tools for bypassing machine-learning AV
- ✗ **Pre-Execution Only**
Point-in-time technology that has only one chance to catch malware
- ✗ **High False Positives**
Often mistakes acceptable software for malware, due to all-or-nothing, low-confidence decision-making
- ✗ **Detection and Response**
Detection and response is separate from prevention
- ✗ **Visibility**
No visibility into where malware came from
- ✗ **Analytics**
On-device only, updated rarely
- ✓ **Ease of Use**
Lightweight and easy for malware only

 See for yourself at ngav.carbonblack.com

Face Off Against the Attacker

THE ATTACKER

Non-Malware PowerShell Attack

Possible uses: data theft, ransomware

In this attack, a rogue Flash app exploits a remote code execution vulnerability to launch PowerShell, which establishes covert control and steals data. This is a hallmark non-malware attack where the objective is achieved by “living off the land” and using tools native to the operating system.

Packed Malware

Possible uses: credential theft, keylogging

By using customized “packers,” which obfuscate software through compression and other algorithms, malware authors can hide their software in plain sight. None of the file contents or attributes look the same as the original malware, and the malware only reveals itself once it is run.

Commodity Malware

Possible uses: botnets, adware, rootkits, spambots

Commodity malware is found “in the wild” and analyzed by threat researchers who produce signatures that identify it. The sheer scale and speed needed to push signatures to endpoints is what makes traditional AV so problematic, plus it takes time to develop a signature when new malware is discovered.

STREAMING PREVENTION

Streaming Prevention detects a series of suspicious events, including Flash modifying the registry, spawning a shell, which downloads a script. This is obviously an attack.

 **Attack Stopped**

Streaming Prevention is continuously monitoring events at every stage of the attack. Packers that get past static analysis trigger suspicious activity as soon as they are unpacked, which streaming prevention detects.

 **Attack Stopped**

Streaming Prevention stops commodity malware before it executes, just like any other antivirus solution, making it a great fit for companies looking to replace traditional antivirus.

 **Attack Stopped**

MACHINE-LEARNING AV

Because there is no software downloaded, machine-learning AV does not see or stop this attack.

 **Attack Succeeds**

Packers hide any identifiable fingerprints of the file, rendering the static analysis that machine-learning AV relies on useless. To compensate, machine-learning AV may block anything that appears to be packed, resulting in high false positives.

 **Attack Succeeds or High False Positives**

Malware attacks are what machine-learning AV was designed to stop, replacing signature-based AV with a more sophisticated mathematical model.

 **Attack Stopped**



The Only Next-Gen Antivirus with Streaming Prevention

Cb Defense is designed to automatically detect and prevent both malware and non-malware attacks. Cb Defense provides customers with a fundamentally different approach to endpoint security by addressing all forms of cyberattacks, not just malware.

With lightweight deployment and low-touch management, Cb Defense protects endpoints against commodity malware and goes above and beyond traditional AV in the following ways:

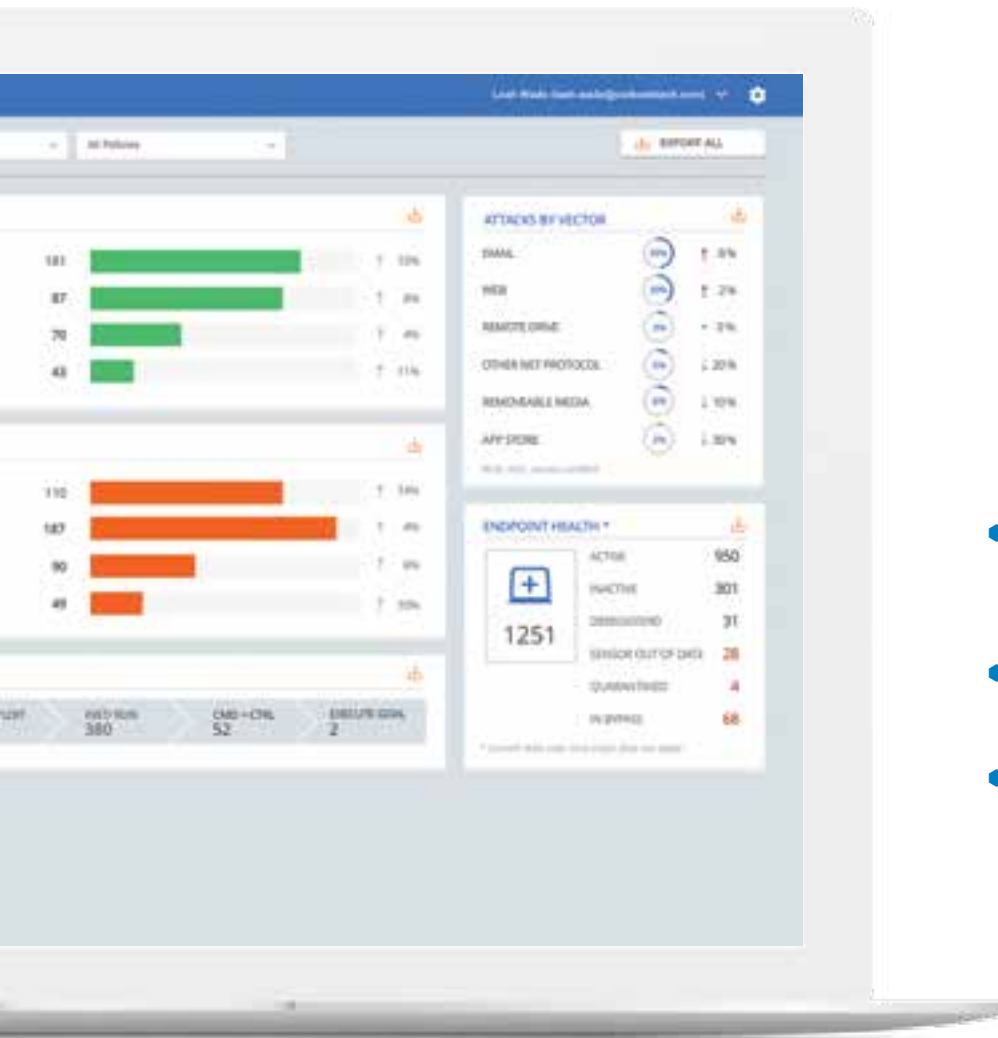
Cb Defense stops non-malware attacks, in addition to preventing malware

It contains fully integrated detection and response capabilities that reveal threat activity in real time

It provides visibility into the full context of the attack, along with root cause

Stop the Most Attacks with Streaming Prevention

Streaming Prevention goes beyond machine-learning AV to stop all types of attacks before they compromise your system.



97% of organizations were targeted by a non-malware attack in 2016

- Stop all types of attacks, including malware, ransomware, zero-days, and non-malware attacks.
- Prevent attacks automatically: online and offline.
- Customize security policies to optimize protection for each asset group.

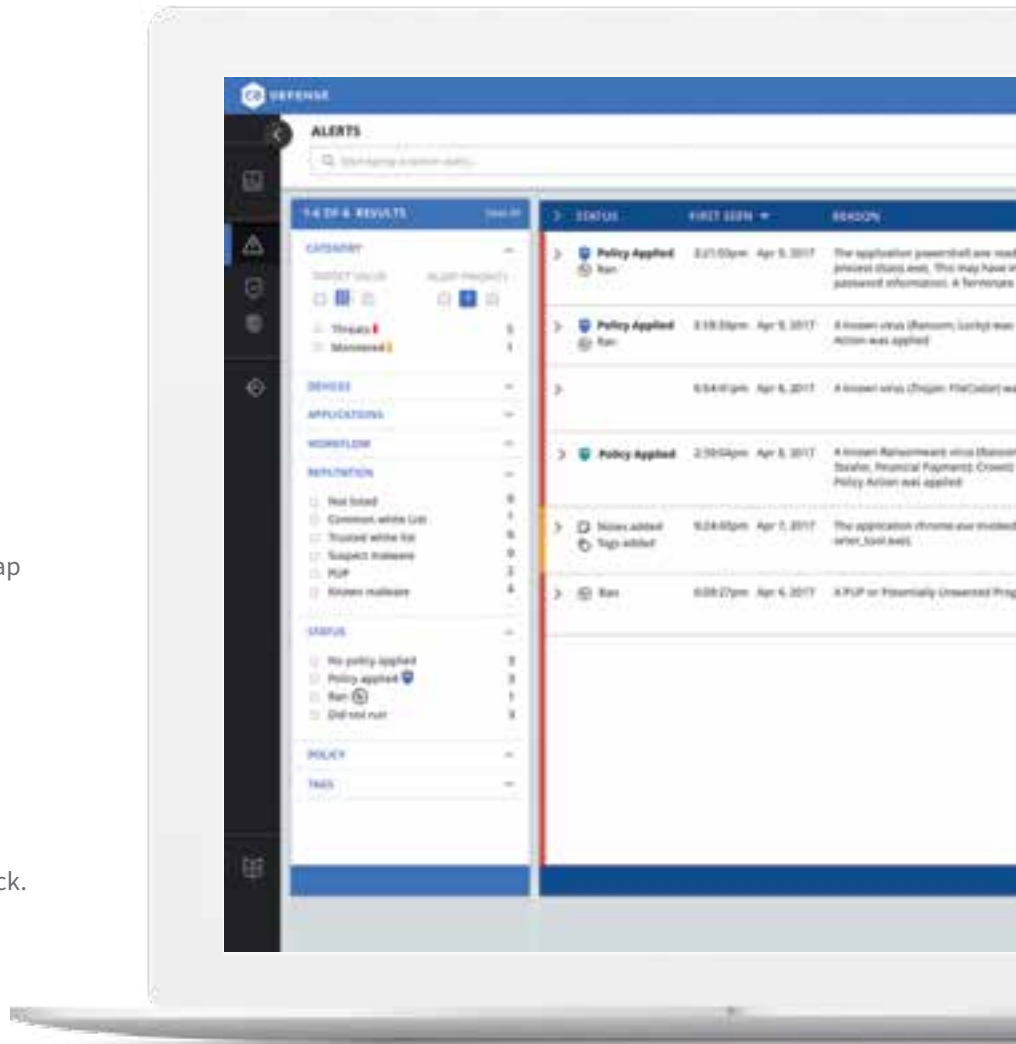
See Every Threat with Market-Leading Detection and Response

Our market-leading detection and response capabilities reveal threat activity in real time so you can respond to any type of attack immediately.



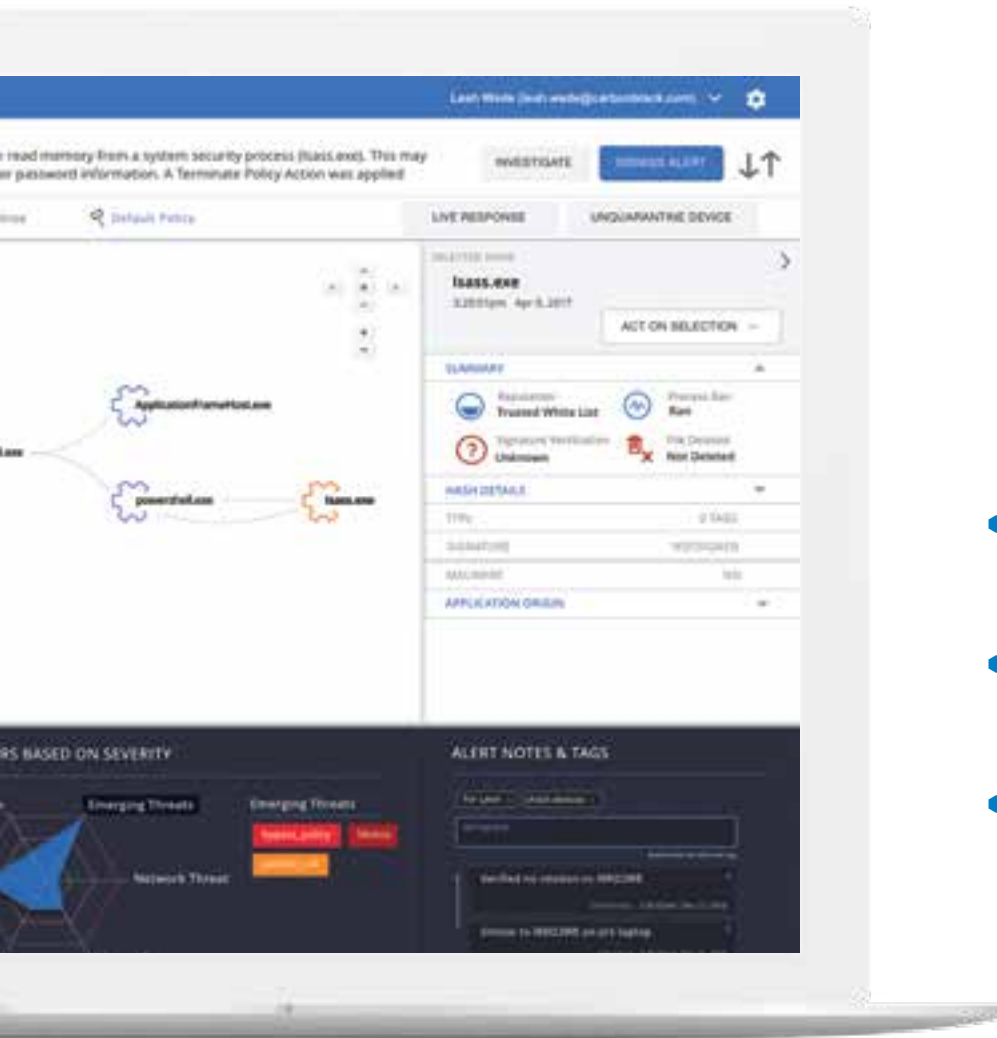
of breaches don't use malware

- Continuous and centralized data recording in the cloud provides zero-gap endpoint visibility.
- Easily visualize the attack chain to hunt down attackers and see exactly what they are trying to do.
- Automated threat hunting algorithms powered by infinite cloud resources keep you one step ahead of every attack.



Compromise Nothing: Lightweight and Easy

Take back control quickly with a single agent—a simple, cloud console with virtually no impact to end users.



organizations can expect to be targeted by a non-malware attack in the next 90 days

- Feel nothing: 15 minutes or less to deploy and requires less than 1% CPU and disk space from each endpoint
- Unobtrusive single agent never interferes with regular operations, keeping your users happy and productive
- Finally feel in control with effective endpoint security that balances total visibility, automated prevention, and user impact



Implement SANS Best Practices for NGAV

Cb Defense is the first and only product to follow the best practices and recommendations for replacing traditional AV with NGAV as described in the SANS Guide *“Out with the Old, In with the New: Replacing Traditional Antivirus.”*

If you are thinking about deploying NGAV in your organization, this Evaluator’s Guide from SANS is a great place to start for a full set of NGAV product requirements as well as a step-by-step methodology for conducting the evaluation.



This guide can be downloaded at
carbonblack.com/files/sans-evaluators-guide-to-ngav/

Carbon Black.

1100 Winter Street, Waltham, MA 02451 USA

P 617.393.7400 F 617.393.7499

carbonblack.com

© 2017 Carbon Black

Ver. 17_0510

Carbon Black is the leading provider of next-gen endpoint security. Carbon Black's Next-Gen Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, "Streaming Prevention," to instantly see and stop cyberattacks before they execute. Cb Defense uniquely combines breakthrough prevention with market-leading detection and response into a single, lightweight agent delivered through the cloud. With more than 7 million endpoints under management, Carbon Black has more than 2,500 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.



Work smarter.

At Insight, we'll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more

