CARBON BLACK

BEYOND THE HYPE

SECURITY EXPERTS WEIGH IN ON ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND NON-MALWARE ATTACKS

In Carbon Black's latest report, 410 security researchers were interviewed to provide insight on the cybersecurity landscape in 2017

SUMMARY

Non-malware attacks, **artificial intelligence** (AI), and **machine learning** (ML) have emerged as the topics du jour in cybersecurity.

AI and ML's roles in preventing cyberattacks have been met with both hope and skepticism. They have been marketed as game-changing technologies though doubts still persist, especially when used in siloes. Their emergence is due largely to the climbing number of breaches, increased prevalence of non-malware attacks, and the waning efficacy of legacy antivirus (AV).

For businesses, cutting through the noise is no easy task.

For an accurate assessment of the cybersecurity landscape in 2017, Carbon Black turned to the experts. For this research, Carbon Black interviewed 410 leading security researchers in an effort to gauge how non-malware attacks, AI and ML are currently perceived.

The interviews point to some interesting trends. Among them:

» Non-malware attacks are considered more threatening than malware-based attacks.

» Non-malware attacks are increasingly leveraging native system tools, such as WMI and PowerShell, to conduct nefarious actions.

» Confidence levels in legacy AV's ability to prevent non-malware attacks are low.

» AI is considered by most security researchers to be in its nascent stages and not yet able to replace human decision making in cybersecurity.

» Researchers say ML-driven security solutions can be bypassed by attackers.

» Cybersecurity talent, resourcing and trust in executives continue to be top challenges plaguing many businesses.

INTERVIEW HIGHLIGHTS

NON-MALWARE ATTACKS

» Nearly two thirds (64%) of security researchers said they've **seen an increase in non-malware attacks since the beginning of 2016**.

» The vast majority (93%) of security researchers said **non-malware attacks pose more of a business risk than commodity malware attacks**.

» Among the most common types of non-malware attacks researches reported seeing were: **remote logins** (55%), **WMI-based attacks** (41%), **in-memory attacks** (39%), **PowerShell-based attacks** (34%), and **attacks leveraging Office macros** (31%).

» Two thirds of security researchers said they were **not confident legacy AV could protect an organization from non-malware attacks**, such as those seen in the recent WikiLeaks CIA data dump.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

» Three quarters (74%) of researchers said **AI-driven cybersecurity solutions are still flawed**.

» 70% of security researchers said **attackers can bypass ML-driven security technologies**; and nearly one-third (30%) said **ML-driven security solutions are easy to bypass**.

» 87% of security researchers said it will be **longer than three years before they trust AI** to lead cybersecurity decisions.

OTHER INDUSTRY TRENDS

» **Executive teams expressed a 16% higher confidence level** in their security solutions compared to the employees who use that software day-to-day.

» Attackers are primarily targeting **customer data** (62%), **corporate IP** (53%), **service disruption** (51%), **credentials** (42%), and **financial data** (41%).

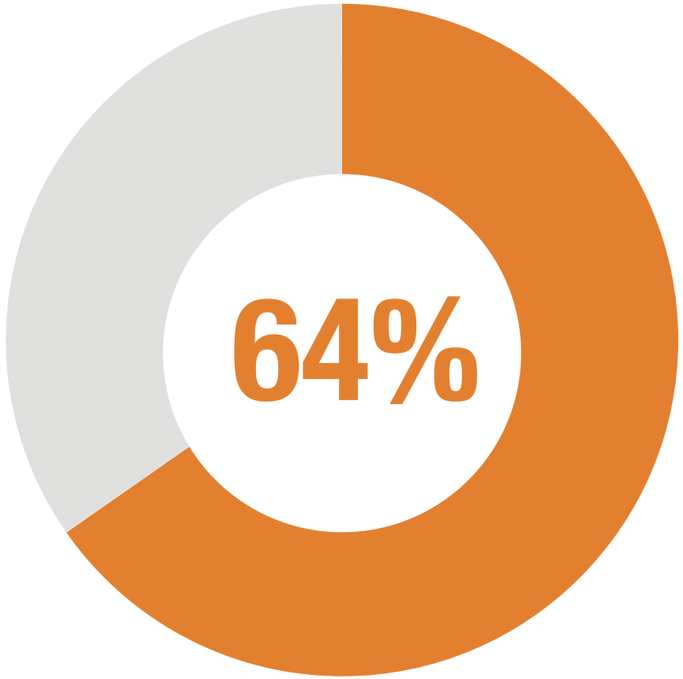
RESEARCHERS WEIGH IN ON NON-MALWARE ATTACKS

Non-malware attacks have become as ubiquitous as ever. Nearly every Carbon Black customer was **targeted by a non-malware attack in 2016**. Additionally, more than half of breaches are now the result of non-malware attacks, according to the Verizon Data Breach Investigations Report (DBIR).

A non-malware attack is one in which an attacker **uses existing software**, allowed applications and authorized protocols to carry out malicious activities. Non-malware attacks are capable of gaining control of computers without downloading any malicious files, hence the name. Non-malware attacks are also referred to as fileless, memory-based or "living-off-the-land" attacks. Because non-malware attacks are fileless, they more easily bypass traditional AV protection and ML-based AV, which typically stop attacks based on files rather than behaviors.

With non-malware attacks, an attacker is able to infiltrate, take control and carry out objectives by taking advantage of vulnerable software, insecure configurations, or humans.

Attackers will also use successful exploits to gain access to web browsers, Office-suite applications, native operating system tools (think **PowerShell** or Windows Management Instrumentation – WMI) and other applications that grant the attacker a level of execution freedom. These native tools grant users exceptional rights and privileges to carry out the most basic commands across a network that lead to valuable data.



OF SECURITY RESEARCHERS REPORT AN **INCREASE IN NON-MALWARE ATTACKS** SINCE THE BEGINNING OF 2016.

Our research found that nearly two thirds (64%) of security researchers said they've seen an increase in non-malware attacks since the beginning of 2016 and the vast majority (93%) said non-malware attacks pose more of a business risk than commodity malware attacks.

Almost all of the researchers (96%) said being able to prevent non-malware attacks would improve their organization's security posture. Among researchers, confidence is waning that legacy AV can protect an organization against these attacks. Two thirds of security researchers said they were not confident legacy AV could protect an organization from non-malware attacks.

MOST COMMON TYPES OF **NON-MALWARE ATTACKS**

According to researchers, the most common types of non-malware attacks reported were

62%
CUSTOMER DATA

53%
CORPORATE IP

51%
SERVICE DISRUPTION

42%
CREDENTIALS

41%
FINANCIAL DATA

NOTABLE NON-MALWARE ATTACKS

2015

August

Macros embedded in MS Office files

PowerShell being launched via macros embedded in MS Office files (xls, doc, ppt, etc.)

2016

April

Squiblydoo

Designed to bypass application whitelisting software by utilizing tools that are built into the operating system by default.

March

PowerWare Ransomware

Family of ransomware targeting organizations via Microsoft Word and PowerShell.

June

Democratic National Committee (DNC)

Non-malware tactics to influence 2016 U.S. Presidential campaign.

December

Instances of severe non-malware attacks grew throughout the year

Over a 90-day period, about one-third of organizations encounter at least one severe, non-malware attack.

2017

March

Wikileaks Unveiling of “RickyBobby”

The initial Rickybobby infection occurs via a PowerShell script that downloads and dynamically executes .NET DLLs in memory. There is no disk footprint during attack execution and the injection is entirely memory-based.

March

Non-malware attack leveraging Excel, PowerShell and Domain Name System (DNS)

Malicious Excel document was used to create a PowerShell script, which then used the Domain Name System (DNS) to communicate with an Internet Command and Control (C2) server.

IN THEIR OWN WORDS

Expected Evolution of Non-Malware Attacks

Several interviews pointed to some interesting trends researchers expect to see in 2017 and beyond when it comes to non-malware attacks:

Proactive and targeted manner

"Non-malware attacks will become so widespread and target even the smallest business that users will become familiar with them. Most users seem to be familiar with the idea that their computer or network may have accidentally become infected with a virus, but rarely consider a person who is actually attacking them in a more proactive and targeted manner."

Poisoning local WiFi networks

"PowerShell and WMI attacks will increase dramatically. Waterhole attacks, such as poisoning local WiFi networks where computer access can be compromised, will rise and attacks on blockchain technology will increase significantly."

Be proactive, not reactive

"I believe that more sophisticated non-malware attacks and malware variants that are ransom-based will emerge [in 2017.] The best way to address these is to stay one step ahead of the attackers and learn about new security threats and stay on top of security constantly. Be proactive, not reactive."

CREATIVITY SEEN WITH NON-MALWARE ATTACKS

Researchers reported that once in the system, attackers posed as internal employees to either send emails from the corporate address, social engineer the IT team, and takeover hardware, among other activities.

Additional, creative, non-malware tactics researchers reported included:

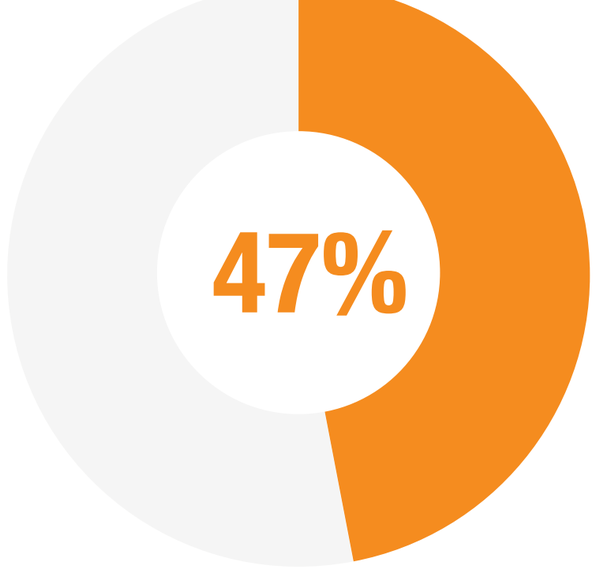
- **Attacks attempting to affect satellite transmission**
- **Attackers trying to impersonate the CSO while attempting to access the corporate IP**
- **Attacks spoofing login systems to appear authentic, allowed login information to be immediately uploaded to the attacker**
- **Attacks sending email from HR employees asking for personal details to be updated to internal systems**
- **Hiding inside of PowerShell**

LACK OF VISIBILITY FROM LEGACY AV SOLUTIONS

While non-malware attacks continue to take center stage, commodity malware is still a major problem for many organizations. Almost half (47%) of breaches are caused by malware, according to the Verizon DBIR.

Researchers reported a lack of visibility from their legacy AV solutions.

When they were asked: "Did your legacy AV miss any malware in 2016?" nearly half (47%) said their AV solution missed malware or they weren't sure if it had missed any malware during the year.



OF SECURITY RESEARCHERS REPORTED A **LACK OF VISIBILITY** WITH THEIR LEGACY AV SOLUTION

IN THEIR OWN WORDS

Combatting Non-Malware Attacks

When asked, "What is your organization doing to bolster security measures against non-malware attacks?" top answers included employee awareness training, turning to next-generation antivirus (NGAV), increased focused on patching, and limiting / locking down personal device usage as needed.

Telltale signs of an attack

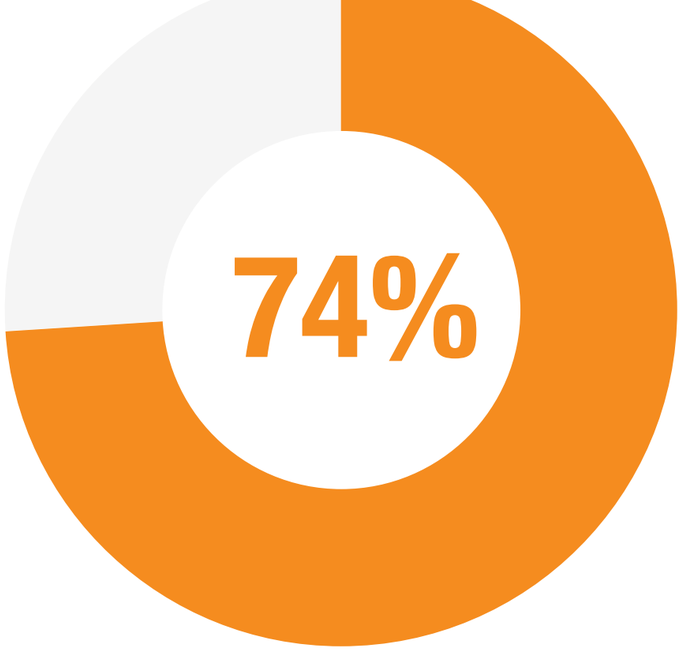
To combat non-malware attacks, one researcher suggested: "Do more than just monitor files. It is critical that processes are also monitored. If you look at the command line and see what PowerShell is being used for, if the context doesn't make sense, then investigate. Moreover, if you look at the command line and see text that looks like it is unrecognizable or random instead of just English, that also is a red flag. You can also look at the execution of the script. If a PowerShell script starts to run, it could be a red flag if it is exhibiting unusual behavior. For instance, if it is trying to access an inordinate amount of files very quickly or trying to communicate outside of your network then these are some telltale signs of an attack."

AI-DRIVEN SECURITY SOLUTIONS ARE STILL NASCENT

The global deficit of qualified cybersecurity talent and the waning efficacy of legacy AV are both major issues facing today's businesses. As a result, some organizations are turning to AI-driven security solutions to parse through data, identify threats and augment human decision making.

Attackers, too, are leveraging AI automation to launch attacks. For some, information security is being perceived as a "machine vs. machine" battle. And, while the future for AI-driven security may look bright, the majority of security researchers are not ready to give the machines all the power just yet, according our research.

Three quarters (74%) of respondents said that AI-driven security solutions are flawed. When considering the biggest risk associated with using AI-driven security solutions, security researchers cited: high false positive rates, too much reliance on humans to make security decisions, slower security operations and "easy for attackers to bypass."



OF SECURITY RESEARCHERS SAID THAT

AI-DRIVEN SECURITY SOLUTIONS ARE FLAWED

The maturity of AI-based security solutions appears to be a big concern for security researchers when it comes to giving computers more power. The vast majority of security researchers **(87%) said it will be longer than three years before they trust AI to lead cybersecurity decisions.**

As a result, only 13% of these researchers indicated they will look to implement AI-driven cybersecurity solutions at their organizations over that time period.

RECOMMENDATIONS FOR INCORPORATING AI IN CYBER SECURITY

AI technology can be useful in helping humans parse through significant amounts of data. What once took days or weeks can be done by AI in a matter of minutes or hours. That's certainly a good thing.

A key element of AI to consider, though, is that it is programmed and trained by humans and, much like humans, can be defeated. AI-driven security will only work as well as it's been taught to.

This leaves many organizations in an interesting position. Do they place their full trust in AI-driven security technologies? According to our research, the vast majority of security researchers are unwilling to do that.

While AI is being used to effectively highlight non-obvious relationships in data sets, it still appears to be in its nascent stages.

As a result, AI can be a component to modern information security programs, but should be used primarily to assist and augment human decision making.

Based on how security researchers perceive current AI-driven security solutions, cybersecurity is still very much a "human vs. human" battle, even with the increased levels of automation seen on both the offensive and defensive sides of the battlefield.

BIGGEST RISKS ASSOCIATED WITH USING **AI-DRIVEN** SECURITY SOLUTIONS

- too much **reliance on humans** to make security decisions
- high **false positive** rates
- **slower** security operations
- **"easy for attacker to bypass"**

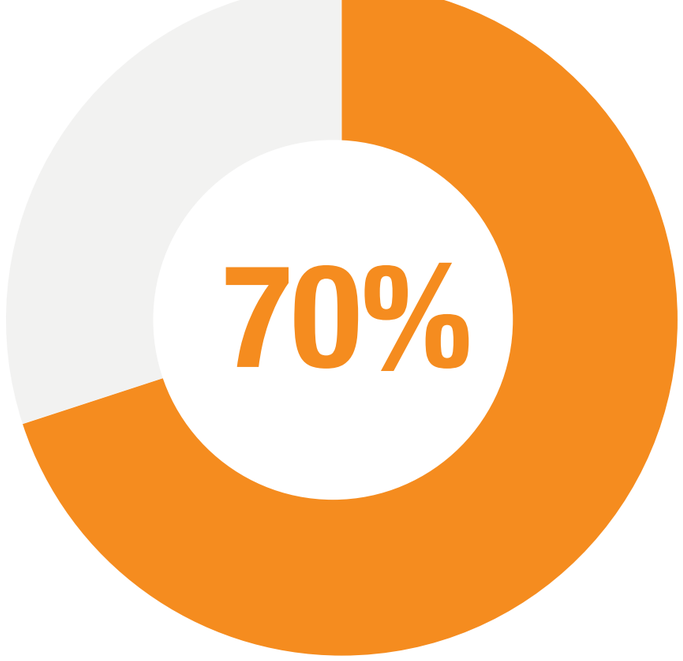
BIGGEST BENEFITS ASSOCIATED WITH USING **AI-DRIVEN** SECURITY SOLUTIONS

- **Highlight non-obvious** relationships in big data
- Augment **human decision** making
- **Potential time savings**
- Learn company **security preferences**

BYPASSING ML-DRIVEN SECURITY SOLUTIONS

As a branch of artificial intelligence (AI), machine learning (ML) has garnered significant interest in the current market. Similar to AI-driven security, ML can certainly be an effective component to a security solution. However, organizations may be putting themselves at risk if ML is the primary security element, according to our research.

According to our survey, 70% of researchers said they feel **attackers are able to bypass ML-driven security solutions** with nearly one-third (30%) saying it is "easy" to do so.



OF RESEARCHERS SAY ATTACKERS

ARE ABLE TO BYPASS ML-DRIVEN SECURITY SOLUTIONS

RECOMMENDATIONS FOR INCORPORATING ML IN CYBERSECURITY

We are not reading these responses as an indictment on ML as a technology. In fact, we feel quite the opposite. ML is a critical component to next-generation endpoint security technologies.

The fault with ML exists in how much emphasis organizations may be placing on it and how they are using it. Static, analysis-based approaches relying exclusively on files have historically been popular, but they have not proven sufficient for reliably detecting new attacks. Rather, the most resilient ML approaches involve dynamic analysis - evaluating programs based on the actions they take.

Any reasonable ML approach to endpoint security is going to face the problem of obtaining training data at scale. If you're looking at files, you'll need a lot of files. If you're looking at behavior, you're going to need a lot of behavior. Unfortunately, obtaining many examples of real attacks as they happen isn't always feasible.

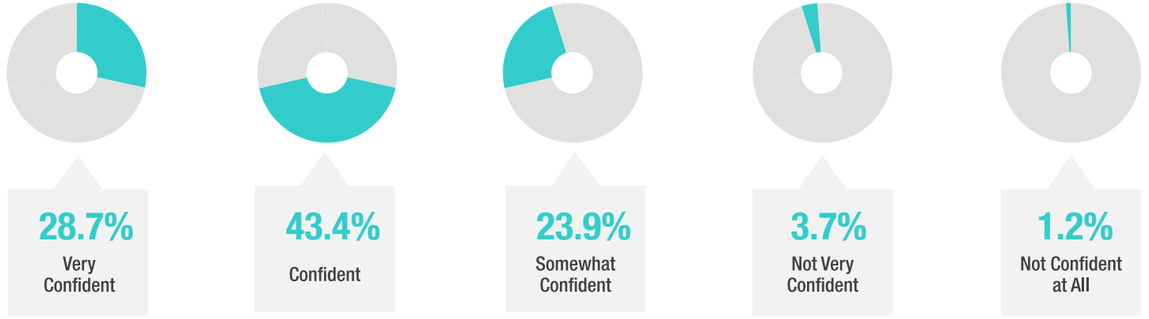
Our recommendation is to use: a massive body of baseline data, a torrent of detonation data, and statistics and comparisons among behaviors for validation. Collectively, these approaches will give you a powerful set of tools to generate patterns of malicious behavior.

Security technologies should be founded on big data collection, make use of automation wherever effective and efficient, and, most importantly, empower humans to make better decisions. In turn, these humans can better train ML-driven solutions to be more effective. ML-driven security solutions exist in a similar bucket as AI - they are promising components though nascent in their current form. They should not yet be relied upon as the sole technology in cybersecurity programs.

CHALLENGES CONTINUING TO PLAGUE MODERN SECURITY PROGRAMS

Talent and resourcing continue to be top challenges plaguing the security industry. According to our research, a disconnect between executive and ground-level employees persists. **Only 28% of researchers said they are "very confident" that their executive teams have a good handle on cybersecurity** at their organization.

That confidence discrepancy is reflected in perceived efficacy of security solutions. Executive teams also expressed a 16% higher confidence level in their security solutions compared to the employees who use that software day-to-day.



WHAT **DATA** ATTACKERS ARE LOOKING FOR

According to researchers, attackers are primarily targeting:

62% CUSTOMER DATA

53% CORPORATE IP

51% SERVICE DISRUPTION

42% CREDENTIALS

41% FINANCIAL DATA

CONCLUSION

The scope of today's cyberattacks is vast and, often, overwhelming. Malware and non-malware attacks continue to target businesses in every vertical. Many of these businesses are understaffed and buried by a flood by security alerts. As a result, businesses have considered using security solutions that promise better security via extensive automation - essentially making cybersecurity a "machine vs. machine" battle.

Based on interviews with more than 400 leading security researchers, it's clear that these promises are currently limited by nascent technologies.

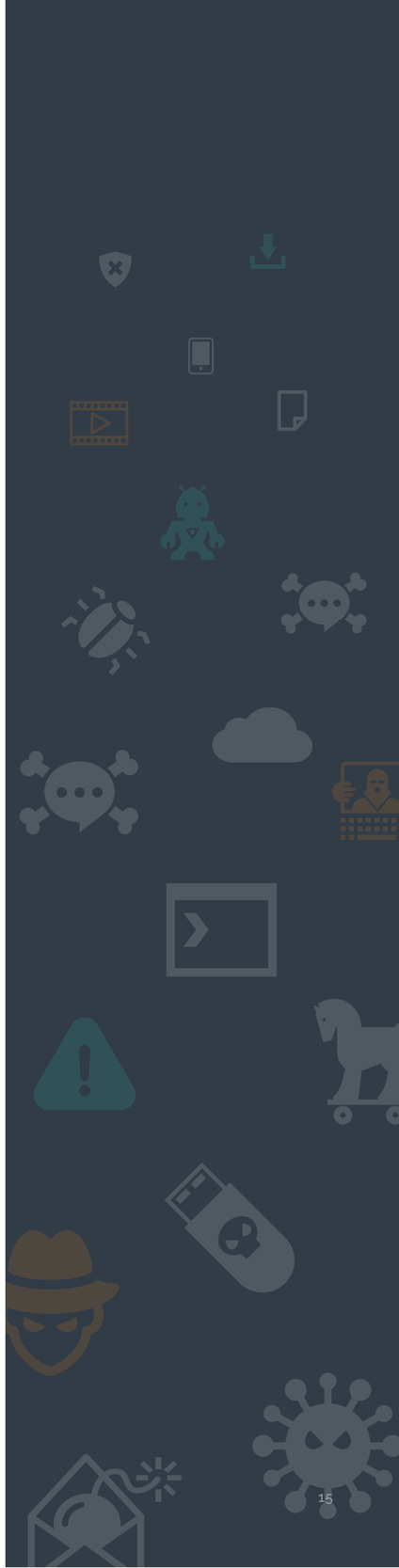
While AI and ML-driven security solutions can exist as effective components to cybersecurity programs, they should not yet be exclusively relied upon as sole protections. Similarly, while confidence remains stable in legacy AV in preventing malware-based attacks, confidence is clearly waning in legacy AV's efficacy in stopping the more threatening non-malware attacks. The responses to several AV-related questions appear to support a prevailing sentiment in the market - many organizations are ready to replace ineffective, legacy AV solutions.

According to a majority of security researchers, cybersecurity will continue to be, at least for the next five years, a battle of "human vs. human," where AI and ML can be used to augment and empower human reasoning, not replace it.

Additionally, the increased ubiquity of non-malware attacks is an issue the organizations should look to address in earnest in 2017 and beyond.

METHODOLOGY

For this report, Carbon Black interviewed 410 security researchers in late December 2016 and early January 2017. Two screening questions determined eligibility. Participants were required to work as researchers in IT, engineering or security operations in one of the following roles for at least one year: security engineer/analyst; security executive (CISO, CSO); security director; incident responder; security consultant; security operations center (SOC) analyst); security data scientist; pen-tester; or threat researcher. Participants currently employed by security vendors were disqualified from participating.



CARBON BLACK

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

www.carbonblack.com

Ver. 17_0327

ABOUT CARBON BLACK

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black's Next-Generation Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, streaming prevention, to instantly see and stop cyberattacks. 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.