

Carbon Black Innovations Set Industry Standard for Next-Generation Antivirus With Streaming Ransomware Prevention and Live Response

Submitted by: C8 Consulting
Monday, 11 September 2017

Latest release of Cb Defense uniquely protects businesses from fast-evolving ransomware threats while providing proven capability to accelerate and simplify security operations

Reading, UK. – 11th September 2017 – Carbon Black, the leader in next-generation endpoint security, today announced the Q3 2017 release of Cb Defense, the company's next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution.

Powered by "Streaming Ransomware Prevention" technology, Cb Defense is the market's first NGAV plus EDR solution to protect organisations from ransomware by detecting and preventing against fileless attacks or unknown tactics. The latest version of Cb Defense also incorporates Carbon Black's popular "Live Response" capability from Cb Response, leveraged by 1,700 enterprise customers globally. With Live Response, enterprises can remediate an attack within minutes and immediately quarantine an endpoint to limit damage, fix the issue, and restore service.

"After conducting an extensive evaluation of anti-malware solutions, Samsung found that only Cb Defense could stop all the attacks we threw its way," said Steven Lentz, CSO at Samsung Research America. "The ransomware threatscape will continue to evolve and the technology in the latest release of Cb Defense is exactly what enterprises need to maintain business continuity in the face of today's biggest cyber threats."

Streaming Ransomware Prevention

The newest release of Cb Defense uses "Streaming Ransomware Prevention," expanding on Carbon Black's breakthrough "Streaming Prevention" technology. This innovation leverages event-stream processing, the same technology that revolutionised algorithmic day-trading, to continuously update risk profiles based on a stream of computer activity. When multiple, potentially malicious events occur in a cluster, Cb Defense blocks the attack, whether file-based or fileless. By building upon an event-stream model, rather than the file-based signature approach used by ineffective legacy antivirus solutions, Cb Defense is able to:

- Detect and prevent ransomware attacks, even if the attack uses an unknown file or no file at all.
- Work online or offline, protecting systems from the most dangerous ransomware, even if they are disconnected from the corporate network or the cloud.
- Enable smooth operations with virtually no performance impact for end-users.
- Provide no additional resource burden to constrained security and IT teams.

"Ransomware has quickly evolved to become one of the most threatening attack methods used by modern cybercriminals," said Patrick Morley, Carbon Black's president and chief executive officer. "With the Q3 2017 release of Cb Defense, Carbon Black empowers enterprises to leverage the full power of our cloud scalable architecture and streaming prevention, equipping security teams with the ability to

detect, prevent and respond to evolving attacks.”

Bringing Live Response to Cb Defense

The latest version of Cb Defense incorporates Carbon Black’s popular “Live Response” capability from Cb Response. With this functionality, security professionals have a centralised, high-powered remediation console empowering them to respond to attacks in progress within minutes, minimising business impact. Live Response has become a mission-critical capability for Carbon Black customers and now as a part of Cb Defense.

With “Live Response,” Cb Defense helps organisations take full control during the most critical moments of an attack. Competing legacy solutions simply inform businesses about security issues, and often require other systems or people to resolve them. “Live Response” in Cb Defense benefits organisations by:

- Giving security teams one interface to quarantine as well as remediate an endpoint and then restore service.
- Providing easy access to any endpoint for gathering information, extracting memory dumps, and running scripts for full remediation in minutes.

Third-Party Validates Carbon Black Ransomware Technology

“Carbon Black Cb Defense was able to block all attacks, from both in-the-wild Ransomware and POC tool attacks, stopping traditional executables or fileless,” said Sveta Miladinov, CEO of security research firm MRG-Effitas, which tested the latest release. “Whether the ransomware tries to encrypt files or the boot sector, Cb Defense provided exceptional protection.”

Recently, Cb Defense won an Edison Award for innovation in cybersecurity and was named “Best Advanced Persistent Threat (APT) Protection Solution” by SC Magazine Awards Europe 2017. During a recent test, Cb Defense received a 5-star overall rating from SC Media.

“Ransomware continues to be a significant cyber security challenge enterprises face today,” said Jon Oltsik, senior principal analyst at the Enterprise Strategy Group. “With this new release, Carbon Black can help resource-constrained organisations address ransomware quickly and effectively.”

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 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 9 million endpoints under management, Carbon Black has more than 3,000 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.