The Situation

Today’s businesses face a unique set of security challenges that traditional endpoint security can’t solve. The reality is that 70% of attacks today are fileless or Living off the Land (LotL) attacks which traditional AV can’t even detect, let alone stop. Cybercriminals are getting smarter—investing significant time and resources into creating advanced attacks to target businesses.

Organizations need security that is reliable, protecting against the full spectrum of today’s attacks, and that can withstand scalability demands and administrative requirements.

Carbon Black’s Cloud-Native Endpoint Protection Platform (EPP)

Carbon Black offers organizations of all sizes the tools they need to keep their systems safe from both known and unknown attacks—using a single agent and an easy to use console. It is lightweight, and easy to deploy on tens of thousands or even hundreds of thousands of endpoints.
Establish Protection from Emerging Attacks
With the potential attack surface growing and evolving quickly, you need to be able to stop as much as possible. This means leveraging a variety of technologies from whitelisting to streaming analytics to behavioral prevention.

Carbon Black’s EPP collects and centralizes massive amounts of data in real time and analyzes attackers’ behavior patterns to detect and stop never-seen-before attacks. Leveraging the power of the cloud, it analyzes more than 500B events per day across millions of global endpoints, helping you stay ahead of emerging attacks.

Increase Endpoint Visibility
With the growing sophistication of attacks, it’s imperative to understand how threats are entering your environment, and what they are doing once they’re there.

Carbon Black’s EPP empowers you to accelerate investigations and respond confidently to threats. Easy to digest attack chain visualizations—powered by real-time endpoint data—make it simple to see what has happened, and is happening on your machines. A comprehensive understanding of your systems also allows you to proactively find vulnerabilities in your environment before an attacker does.

Deploy Endpoint Detection and Response (EDR)
Traditional antivirus solutions provide organizations with preventive protection—which can’t protect from the full spectrum of attacks. Specifically, traditional AV is architected to look for indicators of compromise (IOC) associated with malware only. Fileless attacks are a blindspot for such solutions.

Carbon Black’s EPP provides a more comprehensive solution that includes behavior intelligence, which is compulsory to detect living-off-the-land, fileless attacks. With this in place, security teams can continually collect, record, and store endpoint data, providing them with surveillance-like visibility that can be used to investigate a past incident or proactively hunt for threats.

Integrate Your Security Controls
Without an integrated defense strategy, companies can’t achieve their strongest security. Organizations depend on multiple security products and when these products work together, they gain efficiency and speed.

Carbon Black’s EPP offers open APIs which are used by more than 100 leading security product and service vendors to deliver seamlessly integrated solutions. These open APIs enable partners and customers the flexibility to custom-build their security stack with integrated solutions that amplify the investments they’ve made in Carbon Black and other security solutions.

To learn more about how Carbon Black can help secure your organization, contact us.