The Situation

In today’s world, it’s no longer a matter of if you’ll face a cyberattack, but when. To combat this, threat hunting has emerged as an essential process for organizations to preempt destructive attacks. With threat hunting, you are proactively seeking out malicious activity instead of waiting for alerts to roll in. The people defending your organization are your best chance at staying a step ahead of your adversaries. While it may seem aggressive to work on the “assumption of breach,” the reality is that attackers may be inside a network for days, weeks and even months on end, executing attacks without any automated defense detecting their presence. Threat hunting uncovers these attacks by seeking out covert indicators of compromise (IOCs) so attacks can be mitigated before the adversary can achieve their objectives.

How to Stay Ahead

VMware Carbon Black Cloud™

VMware 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. The solution is lightweight, and easy to deploy on tens of thousands or even hundreds of thousands of endpoints.
With VMware Carbon Black you can:

**Know Your Environment**
Centralized access to endpoint telemetry means that security professionals have all the information they need to hunt threats in real-time as well as conduct in-depth investigations after a compromise has occurred.

**Visualize the Attack Chain**
Intuitive attack chain visualization to make identifying root cause fast and easy. With access to the complete activity record of every endpoint—even if it’s offline—you can see what happened at every stage of an attack. Analysts can quickly jump through each stage of an attack to gain insight into the attacker’s behavior, close security gaps, and learn from every new attack technique to avoid falling victim to the same attack twice.

**Remediate in Real-Time**
With Live Response, you can respond and remediate in real-time, stopping active attacks and repairing damage quickly. Create a secure connection to infected hosts to pull or push files, kill processes, perform memory dumps and quickly remediate from anywhere in the world.

**Leverage Cloud-Native Threat Intel and Custom Watchlists**
Consolidate threat intelligence by integrating third-party and proprietary feeds allowing you to detect attacks others have seen. Create custom watchlists to automate repetitive hunts.

**Automate via Integrations & Open APIs**
VMware Carbon Black offers a robust partner ecosystem, out-of-the-box integrations, and an open platform that allows security teams to integrate their endpoint protection platform into existing stacks.

The average total cost of a breach is $3.86 million, and breaches that take over 30 days to contain can cost companies an extra $1 million.

91% of organizations reported improvements in speed and accuracy of response as a direct result of their threat hunting practices.

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