The Situation

Your endpoints no longer exist in the safe confines of your corporate network—they are in the wild, exposed to new threats every day. This means that you need to accept the very real possibility that intruders have already compromised your systems, regardless of your security posture. On average, it takes organizations more than 7 months to detect a malicious attack and another 81 days to contain it. And the average cost of a breach lasting more than 30 days is $4.86 million, which means that every second counts.

To combat this, Security has evolved from being largely reactive (waiting for alerts to roll in) to proactive—you must constantly be on the hunt for new attacks that evaded detection. A highly efficient security operations center (SOC) enables its skilled defenders to harness both advanced automation and human insight to combat the ubiquitous threat of cybercrime. An intelligence-driven operation can hunt for zero-day threats before an incident has occurred.

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**
Investigations that typically take days or weeks can be completed in just minutes. VMware Carbon Black works with your current SIEM and many other elements of your security stack to ensure every system event is recorded and readily available for you to visualize when an investigation is necessary. At a glance, analysts have instant access to your SOC’s key performance indicators. With access to the complete activity record of every endpoint—even if it’s offline—you can confidently see what happened on your endpoints at any given moment.

**Remediate in Real-Time**
Respond and remediate the attack within minutes, without having to manually aggregate and sift through relevant raw data post-incident. With Live Response, you can safely isolate an infected host and then obtain direct access to that endpoint to continue your response. This enables IR professionals to pull or push files, run commands, and perform memory dumps, all from within a single console.

**Proactively Threat Hunt**
Explore your environment, discover threats missed by outdated detection methods, and reduce attack dwell time. VMware Carbon Black lets you consolidate threat intelligence by integrating third-party and proprietary feeds allowing you to detect attacks others just saw today. Validate your hunting hypotheses and create automated watchlists to generate custom alerts for suspicious patterns they identify.

**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.

To learn more about how Carbon Black can help secure your organization, [contact us.](mailto:sales@vmwarecarbonblack.com)