A New Approach to Workload Protection for the Modern Data Center

Stop attacks on production workloads in private cloud environments

Key Highlights

- VMware Carbon Black Workload provides a unique one-two punch for stopping threats to production workloads inside the software defined data center:
- Shrink the attack surface by enforcing known good application behavior
- Use behavioral threat detection on workloads to disrupt attacks that abuse trusted processes.

Overview

As applications become more distributed and dynamic, they become more difficult to secure. Traditional security solutions are not flexible enough to keep up as applications change over time, leading to breakdowns in security and increasing the risk of a breach.

In addition, siloed information and disparate tools disrupt security remediation and slow incident response, allowing attackers to dwell within the data center undetected. Traditional endpoint security solutions, such as signature-based antivirus, are outdated and ineffective in virtualized environments, and hurt system performance.

Attacks in the Data Center Require a New Approach

Attacks in the data center use different methodologies than end-user attacks. In turn, the threat model for server workloads is very different from a traditional endpoint. The majority of attacks in the data center involve an attacker manipulating the executables, processes, and operating system of the asset itself. They modify the OS, introduce new executables, leverage trusted system processes to move across the data center, and abuse those processes to aid data exfiltration. Modern workloads must be accessible to a distributed team of administrators, giving attackers more avenues than ever to breach and move throughout the data center undetected.

Identifying these threats requires a deep understanding of both intended application behavior and attacker behavior, something that traditional endpoint security products don't possess.

Solution

As a solution, VMware Carbon Black Workload provides a unique one-two punch for stopping threats to critical applications and server workloads inside the software defined data center:

1. Shrink the attack surface by enforcing known good application behavior
2. Use behavioral threat detection on workloads to disrupt attacks that abuse trusted processes

Enforcing Known Good

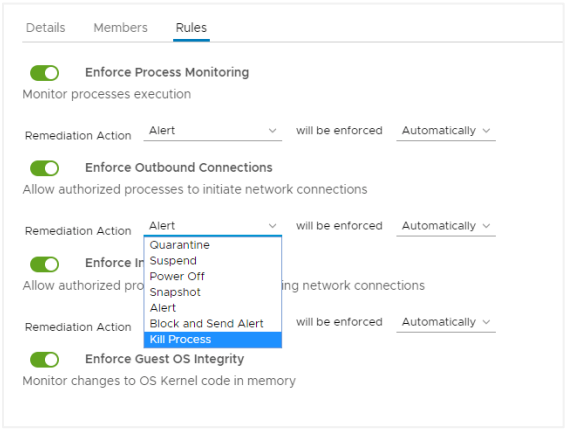
By leveraging VMware's unique understanding of how applications normally behave, Carbon Black Workload is the first to know when changes are made. This contextual intelligence removes the guesswork in determining which changes to processes, executables, and operating systems are legitimate and which indicate real threats.

Detecting Unknown Threats and Advanced Attacks

Any attack that isn't prevented by locking down the workload's behavior is picked up by adaptive prevention – an advanced combination of prevention techniques that include both machine learning and behavioral analysis, to correlate multiple events over time and reveal attacker behavior. By monitoring the activity within server workloads, the solution can detect previously unknown threats and sophisticated attacks. Continuous behavioral analysis highlights all anomalous activity, preventing attackers from leveraging trusted system processes to move laterally through the data center.

Automated, Orchestrated Response

Once an attack is identified, the solution provides numerous options for containment and remediation. Files can be deleted, processes can be terminated, actions can be denied, network communications blocked, and virtual machine-level actions can be taken (snapshot, suspend, quarantine, power off). Additionally, the solution provides an API framework that can be leveraged by orchestration platforms to automate common incident response and containment activities. Organizations can build custom playbooks on top of these APIs, depending on the type of attack encountered.



Differentiation

Combining a hypervisor-based, least privileged model with behavioral analytics delivers the most robust security available for workloads in the modern data center.

What makes this solution unique is the workload visibility and change control afforded by embedding the solution directly into the virtualization layer. By leveraging the vSphere hypervisor, security operations is given a crystal clear understanding of which application is at risk when an alert triggers while monitoring all activity taken by running processes. Furthermore, the SOC has precise control over the response, allowing them to minimize business impact while eradicating the threat.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.