vmware® PARTNER NETWORK

REDEFINING SECURITY IN THE SOFTWARE DEFINED DATA CENTER

Stop attacks on critical applications in virtualized data center and cloud environments

Overview

As applications have become more distributed and more dynamic, they have become more difficult to secure. Traditional security solutions are not flexible enough to keep up with applications as they change over time, leading to breakdowns in security. Additionally, traditional endpoint security solutions are focused on preventing the infiltration step of the kill chain, but threats inside the data center are well past this step -- busy propagating or extracting information from the environment.

Attacks in the Data Center Require a New Approach

Attacks in the data center use different methodologies than end-user attacks. The majority of attacks against data center endpoints hinge on an attacker manipulating the executables, processes, and operating system of the endpoint, itself. They inject new code into application binaries. They introduce new executables. They modify processes for communicating to new things — like their own command and control servers or to other endpoints to spread their malware.

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

Solution

Together, VMware AppDefense and Cb Defense for VMware provide a unique one-two punch for stopping application threats inside the virtualized data center.

- Shrink the attack surface by enforcing known good application behavior
- Use behavioral threat detection to detect and prevent advanced attacks.

Enforcing Known Good

By leveraging the power of the virtual infrastructure, the solution has an authoritative understanding of how data center endpoints are meant to behave and is the first to know when changes are made. This contextual intelligence removes the guess work involved in determining which application changes and network traffic anomalies associated with processes, executables, and operating systems are legitimate and which indicate real threats.

KEY HIGHLIGHTS

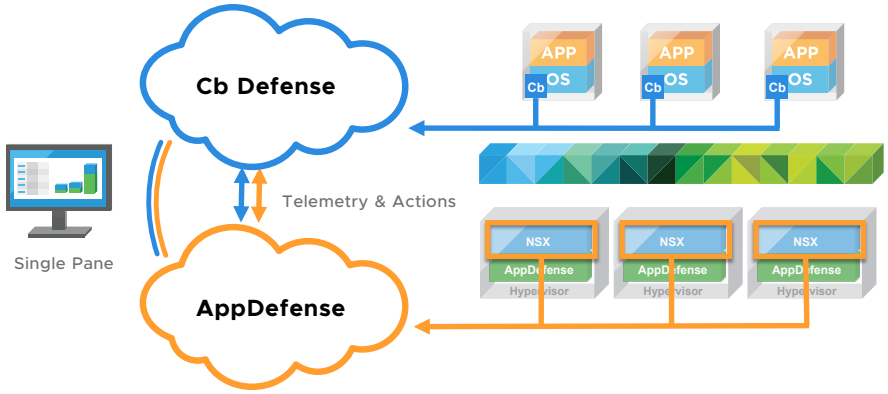
- Attacks on data center endpoints have the power to take down critical applications, steal sensitive data, and disrupt the integrity and availability of a company's information structure.
- Stopping attacks requires a deep understanding of both intended application behavior and threat behavior, something that traditional endpoint security products don't possess.
- Combining a hypervisor-based, least privileged model with application-informed behavioral analytics delivers the most robust security available for the virtualized data center.

Detecting Unknown Threats

Any threat that isn't prevented by locking down the application's behavior, is picked up by Streaming Prevention – a next-gen threat detection technology that uses event stream processing to correlate multiple events over time, indicating the presence of a threat.

Automated, Orchestrated Response

Once a threat is identified, the solution again leverages the virtual infrastructure, itself to deliver a library of responses, ranging from suspending or snapshotting a VM, to quarantining the compromised machine and performing forensic analysis.



Differentiation

Combining a hypervisor-based, least privileged model with application-informed behavioral analytics delivers the most robust security available for the virtualized data center.

What makes this solution unique is the application visibility and 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 is triggered. Furthermore, the SOC has precise control over the response, allowing them to minimize business impact, while still eradicating the threat.

For more information on Redefining Security in the Software Defined Data Center visit, http://www.carbonblack.com/vmware or contact your Carbon Black representative.

vmware® | Carbon Black.

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