SOLUTION OVERVIEW

APPDEFENSE

Deployment Cycle Overview

AT A GLANCE

VMware AppDefense™ can be deployed easily in just four weeks. The deployment should be monitored by the organization’s Security Operations Center (SOC) with intimate knowledge of the application to be protected.

LEARN HOW TO:

- Establish Scopes, Services, and VMs
- Protect Your Application
- Tune Behaviors

AppDefense

Overview

VMware AppDefense is a data center endpoint security product that protects applications running in virtualized environments. Rather than chasing after threats, AppDefense understands an application's natural state and behavior, then monitors for changes to that natural state that indicate a threat. When a threat is detected, AppDefense automatically responds.

This Guide

Use this guide as a best practices reference for the AppDefense deployment cycle. This guide will cover the week-to-week processes for introducing AppDefense to your environment and ensuring that the software clearly understands your environment.

Prerequisites

VMware AppDefense requires four pre-requisites for the operating system. Please be sure your system meets these minimum prerequisites:

- VMware vSphere Hypervisor (ESXi) 6.5
- VMware Tools
- Microsoft: Windows 2016, 2012R2, 2012, 2008R2 (Hardware Level HDW 13), Linux: CentOS 7.1, 7.2, 7.3, 7.4, RHEL 7.0, 7.3, 7.4

Week 1: Establishing Scopes, Services, and VMs

The first step is the physical deployment of AppDefense. This covers appliance install, host install (UI), and guest install (VMware Tools). AppDefense can also be integrated with NSX to help with quarantining malicious connections and with VRA and puppet to help with automating scopes and services. This step should take approximately 90 minutes.

The next step is to create **scopes**, which can be thought of as datacenter applications (i.e., Active Directory). Any VMs that support the application should be included in this scope. The key here is to understand the application and which VMs lie within that application. Within each scope, you can add different **services**, which are tiers or roles that allow you to take specific actions against certain connections based on the tier of service within the scope (i.e., application, web, DB). For example, you may want to set different permissions for AD-Internal vs. AD-External. You may not AD-Internal to have the same inbound and outbound connections as AD-External. Setting up scopes and services should take approximately 30 minutes. Once you have established your scopes, you should put each scope into learning mode.

Week 2: Discovering Behaviors

Once the scope is in learning mode, AppDefense starts to learn the **behaviors** of the application. Behaviors are the processes or connections into and out of the application. During this time, no action is needed as AppDefense is learning the environment automatically.

Weeks 3-4: Protecting Your Application

Once AppDefense is not discovering any new behaviors, the next couple of weeks will require some manual verification of AppDefense's learning. You will verify behaviors within each scope, put the scope into protected mode, and designate remediation actions.

- **Verify behaviors**: AppDefense has verified behaviors during its discovery process using features like machine learning for anomalous behavior, upgrade auto detection, etc. However, you will need to verify behaviors that are not automatically verified and still unknown. Some scopes will need to be in learning mode for longer periods of time depending on number of behaviors, VMs, etc.
- **Put the scope into protected mode**: Once you have verified all remaining behaviors and the scopes are confirmed, put the scope into protected mode.
- **Remediation:** In protected mode, you will automatically receive alerts from AppDefense. You can customize these alerts based on criticality, type, etc. You can also specify the remediation action for each type of alert (block, shut down, suspend, snapshot, etc.).

Weeks 4-5: Tuning Behaviors

Once scopes are in protected mode, you should continue to tune and refine the behaviors within each scope. Repeat the steps for Week 3 to ensure that behaviors are properly verified. Continue to monitor the behaviors and scopes in protected mode.

Key Takeaways & Next Steps

When deploying AppDefense, please refer to this guide as a best practice guide – though some steps and scenarios will be different in each environment. Immediate actions to start the deployment process include: 1) establishing a deployment plan for updating the AppDefense hardware so that your environment meets all minimum prerequisites and 2) preparing a scope creation plan which requires understanding your applications and VMs.

LEARN MORE

For more information on VMware AppDefense, visit http://www.vmware.com/appdefense and test drive the product in our Hands-on Lab. You can find more information on installation and operations in the VMware AppDefense documentation.

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