AppDefense Getting Started

VMware AppDefense

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

AppDefense Getting Started

The *AppDefense Getting Started* provides complete overview of VMware AppDefense™ and information about how to sign up for VMware AppDefense™, use and configure AppDefense to secure applications.

The information includes step-by-step instructions to use AppDefense Service (SaaS), and suggested best practices.

Intended Audience

This information is intended for anyone who wants to sign up for AppDefense Service and use AppDefense. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. This manual assumes familiarity with VMware vSphere ®, including VMware ESXi ™, vCenter Server, vSphere Client, and VMware Tools ™.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

AppDefense Overview

1

AppDefense is a data center endpoint security product that protects applications running in a virtualized environment.

AppDefense builds a known good state for your applications and then detects and responds to deviations from that state. This approach is effective because attackers almost always perform operations that fall outside the typical behavior of the application, such as downloading toolkits, running new code, connecting to command and control systems, and so on. AppDefense provides foundational elements of cloud workload protection, such as system integrity, application control, and memory monitoring.

AppDefense provides these features by leveraging the hypervisor to monitor the behavior of the application running in the virtual machine (operating system kernel, process behavior, and network connections). AppDefense manages VMs as members of an application scope and service, which allows it to have a richer understanding of an application's behavior in the data center, not just individual machine behavior.

This authoritative understanding of the application's intended state is built from integrations into the continuous integration and delivery (CI/CD) pipeline with a comprehensive discovery mode. Automating this creation phase is critical to the efficacy of the solution. AppDefense allows you to orchestrate ahead of time and automatically trigger the response when it detects a given threat.

AppDefense uses vSphere and if installed NSX Data Center for vSphere, to act in response to a detected threat. For instance, you can take a snapshot of the compromised virtual machine for forensic analysis later using vSphere, then quarantine the virtual machine using NSX.

This chapter includes the following topics:

Installation Overview

AppDefense is a data center endpoint security product that protects applications running in a virtualized environment. AppDefense is installed in vSphere from which AppDefense continuously monitors the data center endpoints.

When you install AppDefense, an on-premises AppDefense Appliance OVF/OVA template deploys an AppDefense Appliance, and connects to the vCenter Server through a registration process. AppDefense Appliance then collects the inventory from the vCenter Server and register a UI extension in the vSphere Client. You can then install AppDefense Host Module on ESXi host and AppDefense Guest Module on the virtual machines where your application workloads are running.

You can install AppDefense in the following ways.

- With AppDefense Plug-In
- With AppDefense Service

Install With AppDefense Plug-In

AppDefense plug-in is available with the vSphere Platinum edition. When you add the license key for the Platinum edition, AppDefense appears in the left navigation pane of the vSphere Client. You can now install and use the AppDefense plug-in to protect your application and ensure endpoint security.

For AppDefense plug-in to work, vCenter Server must be 6.7 U1 and above and the ESXi host must be 6.5 U1 and above. The AppDefense plug-in is supported only in the HTML5 version of the vSphere Client. For details, refer to *System Requirements for AppDefense*.

When you install AppDefense with AppDefense plug-in, you can access AppDefense from the vSphere Client. AppDefense appears in the left navigation pane, and in the **Shortcuts** menu of the vSphere Client.

When you install AppDefense, an OVF/OVA template deploys an on-premises AppDefense Appliance which connects to the vCenter Server through a registration process. After the registration is complete, AppDefense Appliance installs the AppDefense plug-in and collects inventory from the vCenter Server.

You can then install AppDefense Host Module on the on ESXi host and AppDefense Guest Module on the virtual machines where your application workloads are running with one-click install process.

You can install AppDefense even when you do not have access to Internet. The offline and online connectivity modes of the AppDefense Appliance can help you to install AppDefense plug-in even without subscribing to theAppDefense Service (SaaS).

You can view and monitor your processes from the VMs **Monitor** tab or the AppDefense Dashboard. You can see the analysis and the reputation for all the processes that AppDefense monitors.

When subscribed to the AppDefense Service (SaaS), you can seamlessly navigate to the AppDefense Manager and create a scope, service, and take the necessary remediation action.

Install With AppDefense Service

When you install AppDefense, an OVF/OVA template deploys an on-premises AppDefense Appliance, and connects to the vCenter Server through a registration process. AppDefense Appliance then collects the inventory from the vCenter Server. You can then install AppDefense Host Module on ESXi host and AppDefense Guest Module on the virtual machines where your application workloads are running.

You cannot install AppDefense with offline and online connectivity modes of the AppDefense Appliance. You must install AppDefense with the SaaS connectivity mode and must subscribe to the AppDefense Service (SaaS).

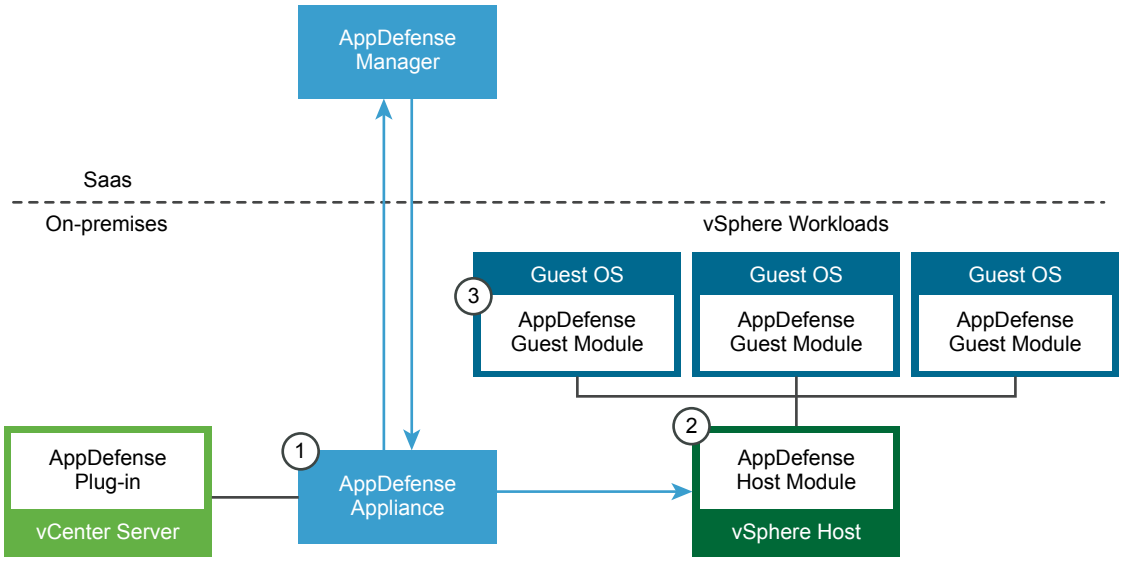
You cannot navigate to the AppDefense Manager from the vSphere Client.

For AppDefense to work, vCenter Server must be 6.5 and above and the ESXi host must be 6.5 U1 and above. For details, refer to *System Requirements for AppDefense*.

AppDefense Components

This section describes the architecture and primary components of the AppDefense platform.

AppDefense Architecture



AppDefense Manager

The AppDefense Manager is a multi-tenant cloud service that delivers the complete AppDefense feature set. You can use the AppDefense Manager to define the intended behavior and protection rules of your applications and then monitor security events and alerts in real time. In addition to management capabilities, the AppDefense Manager provides process reputation services, machine learning capabilities, and other additional visibility features for your environment. If you are using the AppDefense Plug-in, adding the features available in the Manager is optional. For more information, see AppDefense Appliance *Connectivity Modes*.

AppDefense Plug-in

The AppDefense Plug-in provides improved life cycle management and real-time visibility directly in the vCenter Server. With the plug-in, you can configure your connection to the AppDefense Manager with three different connectivity modes. In offline mode, the AppDefense plug-in offers a fully on-premise operating mode with a limited set of functionality. In the connected modes (online and SaaS), the plug-in retrieves process reputation and behavior analysis information from the AppDefense Manager. For more information, see AppDefense Appliance *Connectivity Modes*.

On-Premises AppDefense Appliance

AppDefense Appliance is an on-premises based control point for ingress and egress of data from and to the AppDefense Manager. It brokers connections to the VMware management components like vCenter Server and makes outbound connections to the AppDefense Manager.

AppDefense Host Module

The AppDefense Host Module is a standard VMware Integration Bundle (VIB) that is deployed on the ESXi host in order to support AppDefense. The Host Module enables virtual machines (VMs) on that host to deploy and run AppDefense. For Windows environments, the Host Module also monitors and ensures the integrity of the Guest Module installed on the VM.

AppDefense Guest Module

The AppDefense Guest Module is also required on each VM, delivered with VMware Tools ™ (Windows-only) or a one-click installation. The Guest Module collects guest context from the VM and communicates directly with the AppDefense Host Module.

vCenter Server

vCenter Server is used to gather inventory data on the customer’s site. This inventory data is used for the security scope assignment, guest readiness (based on OS information), and guest to the host assignment. AppDefense can also use vCenter Server to perform remediation actions in response to security events, such as suspending a guest.

NSX Data Center for vSphere (Optional Component)

NSX can be optionally used as an extra, optional remediation channel for AppDefense. If any of the protection rules are violated, NSX can be used to automatically or manually quarantine the machines.

vRealize Automation (Optional Component)

vRealize Automation can be optionally used to capture the application context at provisioning time from the Application blueprint.

AppDefense Components at a Glance

Table 1-1. AppDefense Components

AppDefense Components	Description
AppDefense Manager	Delivers the complete AppDefense feature set. No installation is required. You must sign up for a VMware AppDefense Service.
AppDefense Plug-in	AppDefense plug-in is available with the vSphere Platinum license. When you install AppDefense with plug-in, you can access AppDefense from the vSphere Client.
AppDefense Appliance	AppDefense Appliance is installed on-premises in the management cluster.
AppDefense Host Module	Host module is deployed on theESXi host.
AppDefense Guest Module	Guest module is deployed on one or more hosts where your application workloads are running.

System Requirements For AppDefense

Before you install or upgrade AppDefense, consider your network configuration and resources. You can install one AppDefense Appliance per vCenter Server.

Note The scale limit for the virtual machine (VM) with AppDefense installed is 1000 VMs. AppDefense supports up to 200 hosts, with maximum of 50 VMs per host.

Table 1-2. Required Components

Product/Component	Description	Supported Version
VMware vCenter Server	Used to manage the ESXi infrastructure. You can install AppDefense plug-in for Platinum edition.	6.7 U1 and above The AppDefense plug-in is supported only in the HTML5 version of the vSphere Client.
VMware vCenter Server	Used to manage the ESXi infrastructure. You can install AppDefense without plug-in from AppDefense Service.	6.5.x
VMware ESXi	Hypervisor where virtual infrastructure is spawned.	6.5 U1 and above

Table 1-2. Required Components (Continued)

Product/Component	Description	Supported Version
VMware Tools	Guest Virtual Machine needs VMware Tools installed. AppDefense Guest Module is bundled with latest VMware Tools.	Recommended is latest 10.3.5 version. Supported 10.3.2 and above
VMware NSX Data Center for vSphere (optional)	To leverage the network virtualization, integrate with NSX and use for remediation actions.	6.3 and above
VMware vRealize Automation (optional)	Provisioning system to manage a deployment of the application.	7.2
Windows Guest Operating System		■ Windows Server 2008 R2 x64 ■ Windows Server 2012 x64 ■ Windows Server 2012 R2 x64 ■ Windows Server 2016 x64 **Note** Windows guest operating system with Virtualization-based security (VBS) feature enabled is NOT supported.
Linux Guest Operating System		■ CentOS - 7.1,7.2,7.3, 7.4 (x86_64) ■ RHEL - 7.0, 7.3, 7.4 (x86_64) ■ Ubuntu - 14.04, 16.04 (x86_64) ■ SUSE - 11.4, 12.2, 12.3 (x86_64)
Supported Browsers		Internet Explorer 11 or Microsoft Edge, Google Chrome

Hardware Requirements

Before you install or upgrade AppDefense, your system hardware must meet the following requirements. You can install one AppDefense Appliance per vCenter Server.

AppDefense Appliance Hardware Requirements

AppDefense Appliance	Requirements
Memory	24 GB
Disk Space	186 GB
vCPU	16 vCPU

AppDefense Host Module Hardware Requirements

AppDefense Host Module	Requirements
Memory	Minimum 256 MB
Disk Space	15 MB

AppDefense Guest Module Hardware Requirements for Windows System

AppDefense Guest Module Windows	Requirements
Memory	512 MB
Disk Space	20 MB (Driver and Service binaries)
vCPU	1 vCPU 4 vCPU for In-Memory Process Forensics (IMPF) service

AppDefense Guest Module Hardware Requirements for Linux System

AppDefense Guest Module Linux	Requirements
Memory	1 GB
Disk Space	5 MB
vCPU	1 vCPU

Special Hardware Requirement

Component	Requirements
ESXi host	Make sure that the *cpuHwMmuSupported* flag is **`true`** for the physical CPU.

Key Concepts

The common AppDefense concepts that are used in the documentation and user interface.

Scope A Scope in AppDefense is the foundational component that establishes what the intended state and specific allowed behaviors of an application should be.

	A Security Scope defines the relevant configuration elements to protect an application and its constituent workloads. These configuration elements are like a *blueprint* or a *birth certificate* for the application. It contains a description, member workloads, rules, and behaviors.
Service	A service is a tier or a role within a scope. Typically, homegrown applications have three services (Application, Web, and Database), but scopes can include more than three services (file server, print server, compliance server, and so on).
Member	A member is a virtual machine (VM) within a service. Members (or VMs) in a service must have an identical operating system (means within a service, all the VMs must be homogeneous – either all Microsoft or all Linux).
Provisioning Events	AppDefense can tie into provisioning systems such as vRealize Automation or Puppet to define appropriate and allowed behaviors.
Behaviors	Behaviors are the ports, processes, or connections into and out of the application.
Discovery Mode	When you set up your scopes and services, AppDefense automatically enters into discovery mode. Discovery mode is when AppDefense creates a list of allowed behaviors to build a *blueprint* or a *birth certificate* of the natural state of the application. This mode helps AppDefense to understand how the application must function so that AppDefense can identify malicious or unintended behaviors. The orange color represents the VMs that are either in discovery mode or under protection.
Protected Mode	You can put your scope (application) into protected mode when AppDefense is learning no new behaviors, or you are comfortable with the number of behaviors it has learned. However, it is best practice to keep AppDefense in discovery mode for at least 14 days before moving to protected mode.

Sign up for VMware AppDefense Service (SaaS) 2

You must verify that you satisfy the system requirements before signing up. Though AppDefense is delivered as a Software as a Service (SaaS) solution, it requires some on-premises components to be installed.

This chapter includes the following topics:

Sign up for VMware AppDefense Service

When you sign up for a VMware AppDefense Service, or when someone invites you to join a service, you receive an email invitation containing a link that you can use to sign up.

You can request to sign up for VMware AppDefense at https://cloud.vmware.com/appdefense. You sign up for VMware AppDefense with your VMware ID or you can skip VMware ID and use your business ID.

VMware sets up your organization and user name within the AppDefense Manager. After the setup is done, you receive an invitation to join the AppDefense Service.

Procedure

1 Click the **Confirm my account** link in your invitation mail.

Note If you do not receive the invitation email, contact the VMware AppDefense support team at *appdefense_support@vmware.com*.

You are redirected to the AppDefense sign-in page.

If you are not redirected to the VMware AppDefense page, go to https://appdefense.vmware.com.

2 Log in to VMware AppDefense by entering the following parameters.

Parameter	Description
Select your region	Select either **US**, **UK**, **DE**, or **AU**. By default, **US** region is selected.
Email	Enter email ID on which you received the invitation.

Parameter	Description
Password	Enter your own password.
Organization	Select your organization from the drop-down menu.

3 Click **Sign In**.

The **Dashboard** page of the AppDefense Manager appears as your default homepage.

You can log in to AppDefense Manager based on your region. For example:

Region	URL
US	https://appdefense.vmware.com
UK	https://uk.appdefense.vmware.com
Frankfurt	https://de.appdefense.vmware.com
Sydney	https://au.appdefense.vmware.com

What to do next

Install AppDefense.

Sign Out of AppDefense Service

Sign out of VMware AppDefense Service when you have completed your tasks.

Procedure

1 At the bottom of the left navigation pane, click the setting () icon.

2 Click **Sign Out**.

You are logged out without disconnecting from the service.

Installing AppDefense

3

You can install AppDefense in the following ways.

- With AppDefense Plug-In: For details, refer to *AppDefense Plug-In Guide*.
- With AppDefense Service (Without Plug-in): For details, refer to *Installing AppDefense Guide*.

Using AppDefense Manager

4

AppDefense is a security product for protecting your organizations applications by understanding and analyzing the natural state of the application within the guest virtual machine, establishing the normal operational behavior (intended state) and identifying malicious behaviors. AppDefense constantly measures the future state of the applications against the intended state and control or remediate the behavior when a non-conformance is detected. A key component of AppDefense is creating and maintaining scopes and services for each application.

AppDefense provides four basic functions:

- **Application control**: AppDefense provides application control by establishing a Scope. A Scope is nothing but an intended state. A Scope in AppDefense is the foundational component that establishes what the intended state and specific allowed behaviors of an application or virtual machine (VM) in the data center. Scope also defines a set of allowed behaviors that the application performs normally. Scope is derived from analyzing normal application behaviors, and can even take definitions from integrated applications such as Puppet.
- **Process analysis**: Once AppDefense has established the known state and allowed behaviors for the application, AppDefense constantly monitors the applications, analyzing and looking for suspicious behaviors.
- **Anomaly detection**: AppDefense detects an anomaly in the behavior based on the defined scope. If an application usually receives traffic from one port, attempting communication to another, different port can signal an anomaly that might indicate a threat or attack.
- **Response and remediation**: When an anomalous event occurs and the application's behaviors deviate from the known state, AppDefense responds to potential threats by reporting/alerting, isolating the application, or shutting it down completely. AppDefense includes an orchestration capability that can remediate threats in real time with no administrator oversight.

This chapter includes the following topics:

AppDefense Modes

After you install and configure AppDefense as described in *Installing AppDefense*, you can start using AppDefense to measure the future state of the application against the intended state and control or remediate the behavior when a non-conformance is detected. A key component of AppDefense is creating and maintaining scopes and services for each application.

AppDefense Modes

AppDefense has the following modes of operation:

- **Discovery Mode**: Guest virtual machine on which you have installed and configured AppDefense Guest Module must spend at least a week (7–14 days) in the **Discovery Mode** to learn the specifics and also use IP Address and Port wildcard when a process exhibits many variations in behavior.

After you create scopes and services, AppDefense enters Discovery Mode automatically. The system dynamically populates allowed behaviors based on a runtime view of the application over a period of time. During this time, all relevant activity is recorded as the application is functioning. The learning period for a workload or application must be at least a week (7–14 days). This information is later applied to the Protected Mode.

- **Protected Mode**: In Protected Mode, AppDefense enforces a least privilege posture (default deny) on the managed virtual machines. That means that any observed behavior that is not part of the machines profile throws an alarm.

AppDefense Scope

When you first log in, you are presented with a list of **Security Scopes**. A Security Scope defines the relevant configuration elements to protect an application and its constituent workloads. These configuration elements are like a *blueprint* or a *birth certificate* for the application. It contains a description, member workloads, rules, and behaviors. Security Scopes are a grouping of data center assets (VMs, Containers, and so on) that make up an application or a regulatory scope.

You can send Security Scope information to AppDefense by the following ways:

- **Provisioning Events**: Integrate and provision an application with AppDefense, such as vRealize Automation or Puppet to define appropriate and allowed behaviors.
- **Create Scope**: Manually create Scope. You can define a scope, begin learning behavior, and enforce rules.

To know more about creating a workflow, refer to Securing Applications Using AppDefense.

Securing Applications Using AppDefense

You can define a scope, begin learning behavior, and enforce rules using AppDefense Manager.

Prerequisites

You have access to AppDefense Manager.

Procedure

1 Log in to the AppDefense Manager.

The AppDefense Manager Dashboard appears. You can see the overall coverage data, alarms, available scopes, and provisioned events. You can click VMwareAppDefense to go back to Dashboard from any screen.

2 Perform the following tasks:

Workflow/Task	Description
Create a Scope.	If you have integrated and provisioned an application with AppDefense such as vRealize Automation or Puppet Enterprise, you can view the created scope. You can manually create a scope as well. To create a Scope: 1 To add a scope, in the left navigation pane, next to **Scopes**, click +. 2 In **Scope Name**, enter some identifying information about the application, and then click **Create**. The scope is created and appears in the Dashboard under the **Scope in discovery** panel. By default, the created scope is in the Discovery Mode. You can filter scopes by name or by mode (Protected or Discovery).
Create a Service.	A Service is made up of one or more VMs that perform a function within an application. *App Server*, or a *DB Cluster* are examples of a service. All VMs within a service are expected to be homogeneous and have the exact same allowed behavior/rules. Therefore, all behavior and rules are defined at the Service level. To create a Service: 1 Go to the created Scope, and click **Add Service**. 2 Provide the service details. Enter **Service Name**. 3 Select **Service Type** from the list. For example, *App Server*, or a *Web Server*. 4 Enter description for the service, and click **Next**. 5 Add members by selecting required virtual machine from the list. The selected VMs are VMs that you are protecting. Click **Next**. 6 In the **Allowed Behavior** section, do not add any allowed behaviors right now. In the Discovery Mode, system learns the behavior.
Learn the behavior.	AppDefense now tracks the activity on the members in each service under the **Behavior** tab. To create or edit a behavior: 1 From the left navigation pane, filter and click the created scope. 2 Select the required service. 3 Go to the **Behavior** tab. 4 To view new learned behaviors, refresh the AppDefense Manager. 5 To edit the behavior, click the required behavior and then click **Edit**. Leave a scope in the Discovery Mode for at least 7–14 days.

Workflow/Task	Description
Verify and protect.	Once the allowed behaviors learning is satisfactory, you can move the scope and all services within the scope to the Protected Mode. The **Verify and Protect** button moves the scope to the Protected Mode. To move a scope to the Protected Mode: 1 From the left navigation pane, filter and click the created scope. 2 To add the selected scope to the Protected Mode, click the **Verify and Protect** button at the top of the page. 3 A confirmation dialog box appears. Click **Verify and Protect**. This action marks the *golden image* of the application state and begins locking down the behavior. After moving to Protected Mode, rules are applied. You can view the applied rule under the **Rules** tab, and any violations generates an alarm. After the scopes are in the Protected Mode, continue tuning and refining the behaviors within each scope. To ensure that behaviors are properly verified, repeat the steps. Continue to monitor the behaviors and scopes in the Protected Mode.
Configure Rules.	You can configure which rules are enabled for a service and what must be the desired remediation action. By default, all rules are enabled and the remediation action is just to **Alert**. You can edit the rule. To edit the rule: 1 From the left navigation pane, filter and click the created scope. 2 Select the required service. 3 Go to the **Rules** tab. Click the **More options** (⋮) icon, and then click **Edit service**. 4 Click the **Rules** tab. 5 Select the required remediation action and required enforcement type as Automatic or Manual. 6 Click **Update**.
Detect and respond.	Alarm for the scope appears at the top of the page. All alarms appear under **Alarms** in the left navigation pane. All alarms are refreshed when you navigate to any tab. To view and respond to an alarm: 1 From the left navigation pane, click **Alarms**. All alarms are listed. 2 Click the required alarm. Detailed view of the alarm appears. 3 Select the required alarm ID, and perform the required action: a Clear Alarms: The selected alarm is cleared from the list and the alarm is not displayed later . b Allow Behavior: The selected alarm is added to the allowed behavior. c Remediation Action: Select the remediation action such as, quarantine, suspend, snapshot, or power off the VM. **Note** Quarantine remediation is available only when NSX is deployed and configured. 4 Click **Confirm**.

3 Continue to monitor alarms and modify behaviors and rules as required.