Cisco AMP Private Cloud Virtual Appliance

Product Overview

If your organization has high privacy requirements that restrict the use of a public cloud, the Cisco® Advanced Malware Protection (AMP) Private Cloud Virtual Appliance is an on-premises option. It delivers comprehensive advanced malware protection using big data analytics, continuous analysis, and security intelligence stored locally. The Cisco AMP Private Cloud Virtual Appliance not only satisfies stringent privacy mandates, but also provides network and endpoint protection across the enterprise, comprehensive advanced malware protection without compromising capabilities, and scalability for even the largest global organizations.

The Private Cloud Approach

To defend against today's advanced malware and targeted attacks, you need a solution that goes beyond point-in-time detection to provide comprehensive protection for your organization before, during, and after an attack. Cisco AMP delivers this protection through a set of capabilities that allow you to achieve unmatched visibility, control, and remediation throughout your environment. These capabilities - such as the use of big data and advanced analytics to detect, track, analyze, control, and block advanced malware outbreaks enterprisewide - are best delivered in the cloud. But privacy policies and heavy regulations can limit the use of a public cloud as a means to combat sophisticated threats. The Cisco AMP Private Cloud Virtual Appliance allows organizations in industries, markets, or regions with strict privacy mandates to have an effective, highly secure alternative to the public cloud.

The Cisco AMP Private Cloud Virtual Appliance delivers comprehensive advanced malware protection using big data analytics, policies, detections, and protections stored locally on premises. If the solution discovers an unknown suspicious file, it will interact with our intelligence database, the Cisco Collective Security Intelligence (CSI) public cloud, for file disposition lookup. It will send only anonymized Secure Hash Algorithm 256 (SHA256) information, and then update the AMP Private Cloud and implement retrospective security.

This solution:

- **Helps ensure privacy through a self-contained virtual machine:** The Cisco AMP Private Cloud Virtual Appliance and management system is a single on-premises solution that you install on your own hardware.
- **Delivers network and endpoint protection:** The Cisco AMP Private Cloud Virtual Appliance connects to endpoints through Cisco AMP for Endpoints connectors and directly to AMP for Networks for protection against network malware.
- **Includes many of the same capabilities as the public version:** Much like Cisco's Collective Security Intelligence cloud, the Cisco AMP Private Cloud Virtual Appliance facilitates centralized management through the AMP for Endpoints console. It provides support for custom policies and detections, file trajectory and root cause analysis, reporting, disposition cache, and device-identifiable information. File analysis using Cisco's cloud-based sandbox is currently available only on the public version; AMP Private Cloud customers will receive an account as part of their license if they are required to do file analysis.
- **Scales to meet expanding needs:** Each Private Cloud instance supports up to 10,000 connectors, and multiple Cisco AMP Private Cloud Virtual Appliances can be added to the environment.

Figure 1 illustrates how the solution protects your data, and Table 1 provides a list of its benefits compared with those of the Cisco Collective Security Intelligence Public Cloud.

Figure 1. Cisco AMP Private Cloud Virtual Appliance

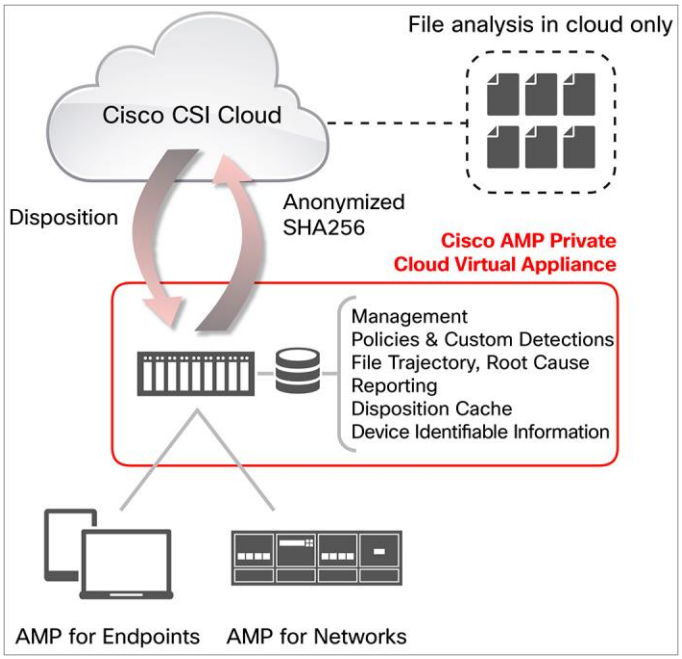

Table 1. Features Comparison

Capability	Cisco AMP Private Cloud Virtual Appliance	Cisco Collective Security Intelligence Public Cloud
File and device trajectory	Yes	Yes
Threat root cause	Yes	Yes
(Local) cloud indications of compromise and alerting	Yes	Yes
Simple and advanced custom detections	Yes	Yes
Cloud lookups, retrospective alerting	Yes	Yes
File analysis, file properties, scheduled scans	-	Yes

System Requirements

The minimum requirements to run this virtual machine instance are outlined in Table 2.

Table 2. Software Requirements

AMP Private Cloud	• VMware Workstation 9 or later: dual-core processor,4 GB RAM, 75 GB free disk space • VMware Fusion 5 or later: dual-core processor, 4 GB RAM, 75 GB free disk space • VMware vSphere ESX 5 or later: dual-core processor, 4 GB RAM, 75 GB free disk space
Connectors	• Microsoft Windows XP with Service Pack 3 or later • Microsoft Windows Vista with Service Pack 2 or later • Microsoft Windows 7 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Mac OSX 10.7 and later • AMP for Networks (v5.4 or later)

Platform Support and Compatibility

The Cisco AMP Private Cloud Virtual Appliance includes the virtual appliance itself and relevant AMP subscriptions.

Warranty Information

Find warranty information on the Cisco.com Product Warranties page.

Ordering Information

To place an order, visit the Cisco Ordering Home Page, contact your Cisco sales representative, or call us at 800 553-6387.

For More Information

For more information, please visit the following link:

- AMP Private Cloud Virtual Appliance

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-733180-00 11/14