Cisco Advanced Malware Protection Virtual Private Cloud Appliance

Organizations with stringent privacy requirements that restrict the use of a public cloud can take advantage of our on-premises, air-gapped solution.

Product Overview

The Cisco® Advanced Malware Protection (AMP) Virtual Private Cloud Appliance is an on-premises, air-gapped private cloud deployment of Cisco AMP for Networks or Cisco AMP for Endpoints technology.[1] It delivers advanced malware protection using static analysis, malware analysis (sandboxing), continuous monitoring of all file activity, and security intelligence stored locally. The virtual appliance not only satisfies stringent privacy mandates, but also provides network and endpoint protection across the enterprise, comprehensive advanced malware protection without compromising your 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 gives you exceptional 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 enterprise wide-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 AMP Virtual Private Cloud Appliance gives organizations in industries, markets, or regions with strict privacy mandates 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. When the solution discovers an unknown suspicious file, it interacts with our intelligence database, the Cisco AMP threat intelligence public cloud, for file disposition lookup. It sends only anonymized Secure Hash Algorithm 256 (SHA-256) information, and then updates the AMP Virtual Private Cloud Appliance and implements retrospective security.

This solution:

- **Helps ensure privacy through a self-contained virtual machine:** The virtual appliance and its management system is a single on-premises solution that you install on your own hardware.
- **Delivers network and endpoint protection:** It connects to endpoints through AMP for Endpoints connectors and directly to AMP for Networks for protection against network malware.

[1] AMP for Endpoints and AMP for Networks deployments use the public AMP cloud for disposition lookups and threat intelligence. On the other hand, the AMP Virtual Private Cloud Appliance is an on-premises private cloud.

- **Includes many of the same capabilities as the public version:** Much like our public cloud, the Cisco AMP Virtual Private Cloud Appliance facilitates centralized management for the AMP for Endpoints private cloud deployment through the AMP for Endpoints console. Firepower Management Center is the management console for the AMP for Networks private cloud deployment. Both consoles provide support for custom policies and detections, trajectory and root cause analysis, reporting, disposition cache, file analysis, and device-identifiable information.
- **Scales to meet expanding needs:** Each private cloud instance supports up to 10,000 connectors, and multiple appliances can be added to the environment.

Deployment Modes

The Cisco AMP Virtual Private Cloud Appliance supports two deployment modes: “cloud proxy mode” and “air gap mode”.

In the cloud-proxy mode:

- An Internet connection is needed to complete disposition lookups.
- All traffic from endpoint connectors is to the private cloud, but disposition lookup is subsequently performed between the private cloud and the AMP public cloud.
- The SHA-256 hash of the file being inspected is the only data sent to the public AMP cloud from the AMP Virtual Private Cloud Appliance.
- Content and software updates can be retrieved automatically from the AMP cloud directly to the AMP Virtual Private Cloud Appliance.

In the air gap mode:

- No internet connection is needed to complete disposition lookups.
- All traffic is between the connectors and the appliance only.
- Disposition queries are handled by the private device.
  - A local virtual instance called “Protect DB” contains all the dispositions and threat intelligence required for full functionality and protection.

In the air gap mode, threat intelligence updates work as follows:

- Content and software updates are retrieved separately from the AMP Virtual Private Cloud Appliance.
- A provided tool called “amp-sync” is used to download and sync software and content updates for the AMP Virtual Private Cloud Appliance from the AMP public cloud.
- A dedicated host server (“update host”) is required to run amp-sync and build update packages.
  - The update host requires Internet access to retrieve updates.
  - The minimum requirement for the update host is CentOS 6.6.
  - The update package (ISO file) built by amp-sync is transferred from the update host and mounted on the virtual appliance. The update process can then be initiated and completed from the administrative console.

- The initial update is large (about 85 Gb), because the Protect DB initial snapshot needs to be synced and a local file repository is built. Subsequent updates are smaller as they patch the local repository.
- It can take three hours or longer for the Protect DB import to be completed on the initial installation.
- Updates are created daily. These include Protect DB, Tetra definition, and other threat intelligence updates (DFC, SE, etc.)
- The Protect DB snapshot is refreshed weekly, reducing the number of updates that are required for a fresh installation.

Figures 1 and 2 illustrate how each deployment mode operates.

Figure 1. Cloud Proxy Mode

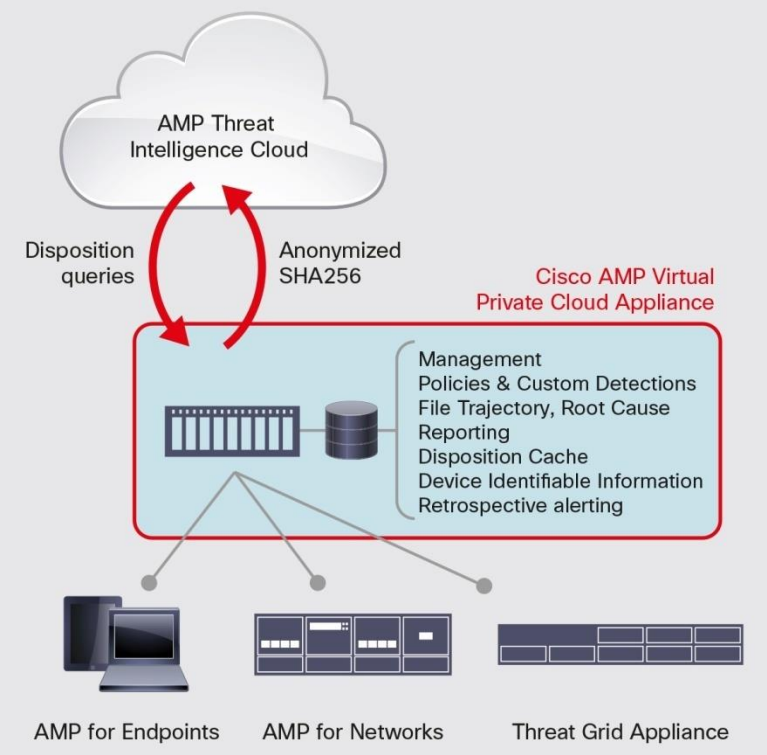

Figure 2. Air Gap Mode

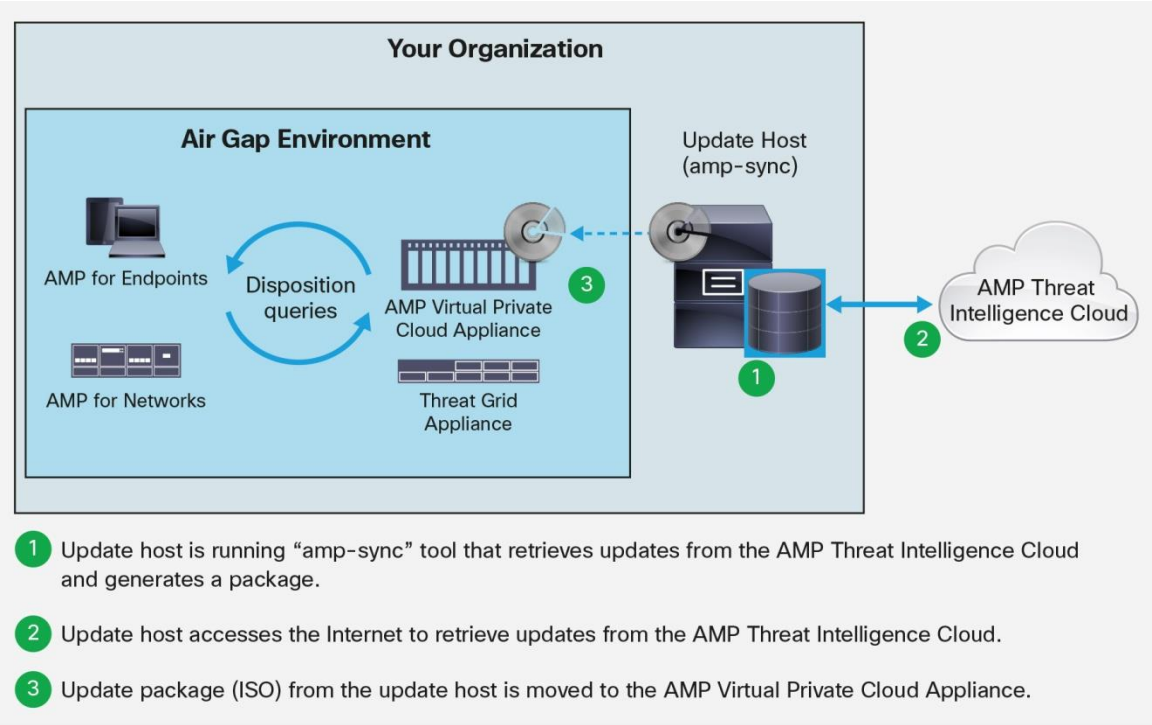

Table 1 provides a comparison of the private and public cloud deployments of AMP.

Table 1. Comparison of AMP Private and Public Cloud Deployments

Capability	Cisco AMP Virtual Private Cloud Appliance	Cisco AMP Public Cloud Deployment	Additional Information
Device and file trajectory	Yes	Yes	Trajectory tracks file propagation over time, on individual devices and throughout your environment, in order to achieve visibility and reduce the time required to scope a malware breach.
Threat root cause	Yes	Yes	Understand where malware came from and how it got in.
Cloud-based indications of compromise (IOCs)	Yes	Yes	IoCs are file and telemetry events correlated and prioritized as potential active breaches. AMP automatically correlates multisource security event data, such as intrusion and malware events, to connect events to larger, coordinated attacks and prioritize high-risk events.
Retrospective Alerting	Yes	Yes	Retrospective security is the ability to look back in time and trace processes, file activities, and communications in order to understand the full extent of an infection, establish root causes, and perform remediation. Alerts are sent when a file disposition changes after extended analysis, giving you awareness of and visibility into malware that evades initial defenses.
Simple custom detections	Yes	Yes	Simple hash-based 1-to-1 detection signatures.
Advanced custom detections	Yes (Windows only)	Yes	Advanced signature support.
Malware analysis	Yes	Yes	Powered by Threat Grid, File Analysis is available as an on premises appliance. It provides static and dynamic analysis of unknown files to identify if a file is malicious, and if so, why.

Capability	Cisco AMP Virtual Private Cloud Appliance	Cisco AMP Public Cloud Deployment	Additional Information
Cloud disposition lookups	Cloud proxy mode: Yes Air-gapped mode: No	Yes	While the AMP Private Cloud Virtual Appliance is in air-gapped mode, it does not connect directly to the internet to retrieve dispositions from the cloud. However, dispositions are retrieved from the same robust repository of threat intelligence (which is instead manually synced and contained within the air-gapped environment).
SPERO detection engine	Yes	Yes	SPERO is machine learning technology.
ETHOS detection engine	No	Yes	ETHOS catches families of malware through use of “fuzzy hashes” as a way to counter malware evasion aided by “bit-twiddling”.
TETRA detection engine	Yes	Yes	Offline detection engine.
Role-based access control (RBAC)	Yes	Yes	Regulate access and permission to perform specific tasks within AMP based on roles of individual users.
Endpoint indications of compromise (IOCs)	Yes	Yes	Ability to author and deploy OpenIOC format rules for endpoint scanning.
Vulnerable software detection	Yes	Yes	Alerts administrator to the presence of vulnerable software on endpoints that could serve as an attack vector for malware.
Managed connectors	10K limit per private cloud appliance	Unlimited	For the AMP Virtual Private Cloud Appliance, more than 10,000 connectors will require an additional appliance, and currently each instance needs to be managed separately.
Firepower Management Center integration	As of FMC 6.1	Yes	Management console for the AMP for Networks deployment through the AMP Virtual Private Cloud Appliance.
Data privacy	Yes	Yes	The AMP Virtual Private Cloud Appliance in cloud proxy mode only sends SHA-256 hashes to the AMP public cloud. In air-gapped mode, no data is sent to the AMP public cloud. An AMP public cloud deployment requires other file metadata to be sent but no personally identifiable information.

System Requirements

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

Table 2. Software Requirements

AMP Private Cloud 2.0	• VMware ESX 5 or later; unofficial support for VMware Fusion 6, Workstation 9 and later • Cloud-proxy mode: 32 GB RAM, 8 CPU Cores (2 CPUs with 4 cores each recommended), 238 GB minimum free disk space • Air-gap mode: 128 GB RAM, 8 CPU Cores (2 CPUs with 4 cores each recommended), 1 TB minimum 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 to 10.9 • AMP for Networks (v5.4 or later)

Platform Support and Compatibility

The AMP Virtual Private Cloud Appliance includes the virtual appliance itself and relevant AMP and Threat Grid 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. View the Ordering Guide to receive detailed instructions on how to order the Cisco AMP Virtual Private Cloud Appliance for your organization.

Cisco Capital

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. Learn more here.

For More Information

For more information, please visit the Cisco AMP Virtual Private Cloud Appliance webpage.

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 C78-733180-04 05/16