Cisco Advanced Malware Protection Private Cloud Appliance

Contents

An on-premises, air-gapped solution for organizations with stringent privacy requirements that restrict the use of a public cloud.

Product Overview

The Cisco® Advanced Malware Protection (AMP) Private Cloud Appliance is an on-premises, private cloud deployment capable of supporting Cisco AMP for Networks, AMP for Email, AMP for Web Security, and AMP for Endpoints. It delivers threat protection using file reputation, malware analysis, continuous monitoring of all file activity, and security intelligence stored locally. The appliance satisfies stringent privacy mandates without compromising the ability to leverage the power of collective security intelligence and provides network and endpoint protection across small and large enterprises.

Stop Advanced Threats

Stopping threats before they cause damage is ideal. But what do you do when that doesn't happen? How long does it take you to respond? Someone will ask "Are we safe from this attack?" and want an answer as soon as possible. The question then becomes, how fast can you get an accurate response?

On average, it takes about 200 days to detect a breach in an organization. Responding to a large-scale event means sifting through stacks of disparate data from multiple sources and tools, scoping the impact, and finally eliminating the threat, all of which costs valuable time. AMP for Endpoints eliminates the guess work, drastically reducing the time it takes to hunt for threats from days or months down to just a matter of hours.

Cisco's private cloud appliance does the heavy lifting for you, so you can take back control of your time. With automated protection, continuous monitoring, and analysis that provides retrospective security, AMP prevents attacks to your network before they start — and accelerates incident investigation and response to the stealthiest 1% of threats.

How We Do It

The Cisco AMP Private Cloud Appliance delivers comprehensive threat protection, with all information stored locally on-premises. When the solution discovers an unknown suspicious file, it interacts with our intelligence database for file disposition lookup. If configured in Proxy Mode, the appliance sends only anonymized Secure Hash Algorithm 256 (SHA-256) information to the public AMP cloud. If using the physical appliance and configured in air-gap mode, the appliance will perform the file disposition lookup locally on the appliance and does not send the SHA-256 to the public AMP cloud.

This solution:

- **Helps ensure privacy through a self-contained physical or virtual appliance:** The appliance and its management system are a single on-premises solution.
- **Delivers network and endpoint protection:** It connects to endpoints through AMP for Endpoints connectors and directly to AMP for Networks on Cisco Firepower® Next-Generation Firewall and Next-Generation Intrusion Prevention System (NGFW/NGIPS) for protection against network malware. The solution also supports Cisco Email Security Appliances (ESA) and Cisco Web Security Appliances (WSA).
- **Provides a single console for management:** Much like our public cloud, the Cisco AMP Private Cloud Appliance facilitates centralized management for supported integrated products. For example, custom policies and detections, file and device trajectory, root cause analysis, reporting, disposition cache, file analysis, and device-identifiable information are maintained through the AMP for Endpoints console.
- **Scales to meet expanding needs:** Each private cloud instance supports up to 10,000 connectors on the virtual appliance and 100,000 connectors on the physical appliance. In addition, multiple appliances (Firepower Management Center [FMC], ESA, WSA) can be added to the environment.

Deployment Modes

The Cisco AMP Private Cloud Appliance supports two deployment modes: "cloud proxy mode" and "air-gap mode."

In the cloud proxy mode:

- It is supported on both the virtual and physical appliance.
- 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 Private Cloud Appliance.
- Content and software updates can be retrieved automatically from the AMP cloud directly to the AMP Private Cloud Appliance.

In the air-gap mode:

- It is supported only on the physical appliance.
- 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 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 Private Cloud Appliance.
- A provided tool called "amp-sync" is used to download and sync software and content updates for the AMP 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, an ISO disk image, built by amp-sync is transferred from the update host and mounted on the appliance. The update process can then be initiated and completed from the administrative console.
- Updates are created daily. These include the collective security intelligence database, anti-virus definitions, and other threat intelligence updates.
- In special air-gap deployments where the appliance can access the AMP public cloud, it is possible to pull updates directly from the AMP public cloud to the appliance without the need of an intermediary step to download content on one server and transfer it to the appliance as you would in a true air-gap environment.

Figures 1 and 2 illustrate how each deployment mode operates.

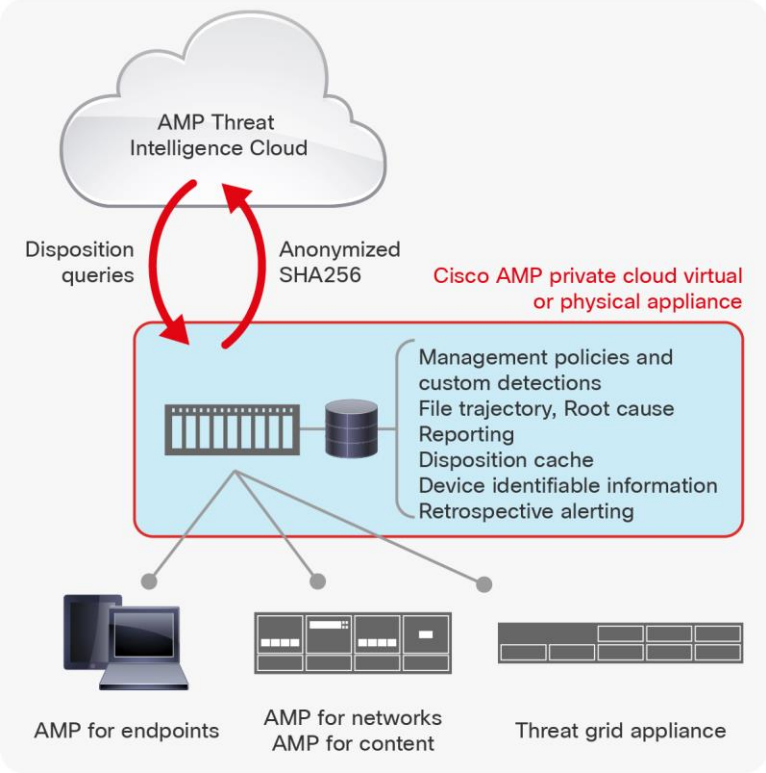

Figure 1.
Cloud proxy Mode

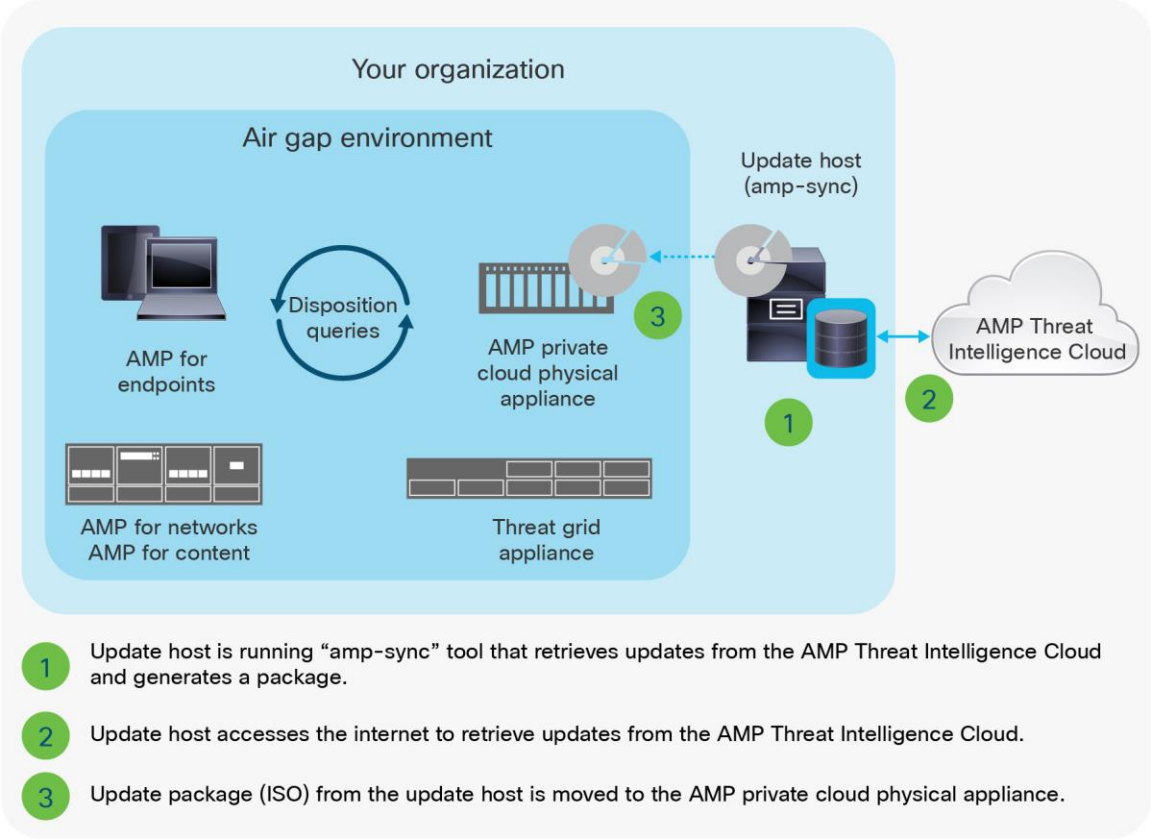

Figure 2.
Air-gap mode

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 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.

Capability	Cisco AMP Private Cloud Appliance	Cisco AMP Public Cloud Deployment	Additional Information
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 Cisco Threat Grid (TG), 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.
Cloud disposition lookups	Cloud proxy mode: Yes Air-gap 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).
Machine learning detection engine	Yes	Yes	Dedicate detection engine trained by algorithms to predictively identify malicious files and activity based on the attributes of known threats.
Polymorphic detection engine	No	Yes	This engine catches families of malware through use of "fuzzy hashes" as a way to counter malware evasion aided by "bit-twiddling."
Anti-virus engine	Yes	Yes	Signature-based 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.

Capability	Cisco AMP Private Cloud Appliance	Cisco AMP Public Cloud Deployment	Additional Information
Managed connectors	10,000 limit per virtual private cloud appliance; 100,000 limit per physical private cloud appliance	Unlimited	Where multiple appliances are used, each appliance 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.

Table 2 compares the two appliance options.

Table 2. Comparison of Virtual and Physical Appliance Options

	AMP Private Cloud Appliance PC3000	AMP Private Cloud Virtual Appliance
Form factor	2RU physical appliance	VMware virtual machine
Supports FMC, TG, ESA, WSA	Yes	Yes
Number of supported connectors	100,000	10,000
Support air-gap deployments	Yes	No

Product Specification

The Cisco AMP Private Cloud Appliance is available in two deployment options, a VMware OVA virtual appliance and a physical appliance.

The minimum requirements to run the virtual machine instance are outlined in Table 3.

Table 3. Virtual Appliance Software Requirements

Software	System Requirements
AMP Private Cloud Virtual Appliance 3.0	• VMware ESX 5 or later • Cloud-proxy mode (only): 64 GB RAM, 8 CPU cores (2 CPUs with 4 cores each recommended), 1 TB minimum free disk space on VMware datastore ◦ Type of drives: SSD required ◦ RAID Type: One RAID 10 group (striped mirror) ◦ Minimum VMware datastore size: 1 TB ◦ Minimum datastore random reads for the RAID 10 group (4K): 60K IOPS ◦ Minimum datastore random writes for the RAID 10 group (4K): 30K IOPS
AMP for Endpoints Connectors	• Microsoft Windows 7 • Microsoft Windows 8 and 8.1 • Microsoft Windows 10

Software	System Requirements
	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 and 2012 R2 • Microsoft Windows Server 2016 • Apple macOS 10.7 • Redhat Enterprise Linux (RHEL)/CentOS 6.8 and 6.9 • Redhat Enterprise Linux (RHEL)/CentOS 7.3 and 7.4

The physical appliance product specification is outlined in Table 4.

Table 4. Physical Appliance Product Specification

AMP Private Cloud 3000 (PC3000) Physical Appliance	Specifications
Form factor	2 Rack Unit (RU)
Dimensions	3.4 x 16.9 x 29.8 in. (H x W x D)
Network interface	2 x 1 GB Copper + SFP+
CIMC interface	1 GB Copper
Power options	770W AC

Ordering Information

To place an order for a Cisco AMP Private Cloud appliance, visit the Cisco ordering homepage. Table 5 provides ordering information.

Table 5. Ordering Information

AMP Private Cloud Physical Appliance and Subscription	
Part number	**Product description**
AMPPC-3000-K9	Cisco AMP Private Cloud Appliance - 3000 Model
L-AMP-PC-K9=	Cisco AMP Private Cloud, Content License available for 1, 3, and 5 years (L-AMP-PC-1Y, L-AMP-PC-3Y, L-AMP-PC-5Y)

AMP Private Cloud Virtual Appliance and Subscription	
Part number	**Product description**
FP-AMP-CLOUD-BUN	Cisco AMPv Private Cloud SW and Service Subscription Bundle. Use this bundle for convenience of ordering. The following PIDs are included in this bundle.
FP-AMP-CLOUD=	Cisco AMPv Private Cloud Service Subscription available for 1, 3, and 5 years (FP-AMP-CLOUD-1Y, FP-AMP-CLOUD -3Y, FP-AMP-CLOUD -5Y).
FP-AMP-CLOUD-SW	Cisco AMP Private Cloud Virtual Appliance.

Cisco Services

At Cisco, we're committed to minimizing our customers' TCO, and we offer a wide range of services programs to accelerate customer success. Our innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services helps you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Some of the key benefits of Cisco Services are:

- Mitigating risks by enabling proactive or expedited problem resolution.
- Lowering TCO by taking advantage of Cisco expertise and knowledge for advisory, implementation, and on-going optimization.
- Minimizing network downtime.
- Supplementing your existing support staff so they can focus on additional productive activities.

Cisco Smart Net Total Care

All Cisco Smart Net Total Care® service levels are available for Cisco AMP Private Cloud Appliance. The Smart Net Total Care (SmartNet) service helps customers resolve network problems quickly with direct, anytime access to Cisco experts, self-help support tools, and rapid hardware replacement.

Learn more about SmartNet and Cisco Security Services.

Warranty Information

Find warranty information on the product warranties webpage.

Ordering Information

To place an order, visit the Cisco ordering webpage, contact your Cisco sales representative, or call us at +1 800 553 6387. View the ordering guide to receive detailed instructions on how to order the Cisco AMP Private Cloud Appliance for your organization.

Cisco Capital

Flexible Payment Solutions to Help You Achieve Your Objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate

growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For More Information

For more information, please visit the Cisco AMP 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 **https://www.cisco.com/go/offices**.

Printed in USAs

C78-742267-00 04/19