Data Sheet

Cisco Advanced Malware Protection Virtual Private Cloud Appliance

퍼블릭 클라우드의 사용을 제한하는 엄격한 개인정보 보호 요건을 요구하는 기업의 경우 Cisco의 온프레미스 에어갭(air-gap) 솔루션을 이용할 수 있습니다.

제품 개요

Cisco® AMP(Advanced Malware Protection) Virtual Private Cloud Appliance는 Cisco AMP for Networks 또는 Cisco AMP for Endpoints 기술을 온프레미스 에어갭(air-gap) 프라이빗 클라우드로 구축한 솔루션입니다.[1] 정적 분석, 악성코드 분석(샌드박싱), 모든 파일 활동에 대한 지속적인 모니터링, 로컬에 저장되는 보안 인텔리전스를 사용하여 지능형 악성코드를 차단합니다. 이 가상 어플라이언스는 엄격한 개인정보 보호 요건을 충족할 뿐 아니라 전사적인 네트워크 및 엔드포인트 보호, 기능 저하 없는 포괄적인 지능형 악성코드 차단, 최대 규모의 글로벌 기업도 수용할 수 있는 확장성까지 제공합니다.

프라이빗 클라우드 방식

오늘날 지능형 악성코드 및 표적 공격으로부터 방어하기 위해서는 특정 시점 탐지에 머무르지 않고 공격 전, 중, 후에 전방위적으로 포괄적인 차단을 할 수 있는 솔루션이 필요합니다. Cisco AMP는 해당 환경 전반에 걸쳐 뛰어난 가시성, 제어력, 치료 등 여러 기능을 통해 이러한 보호를 실현합니다. 빅데이터 및 고급 분석을 사용하여 전사적으로 지능형 악성코드를 탐지, 추적, 분석, 제어, 차단하는 것과 같은 기능은 클라우드에서 가장 효과적으로 제공됩니다. 그러나 개인 정보 보호 정책 및 엄격한 규제 때문에 퍼블릭 클라우드의 사용이 교묘한 위협을 차단하기 위한 수단으로 제한 될 수 있습니다. AMP Virtual Private Cloud Appliance는 개인정보 보호 요건이 엄격한 산업, 시장, 지역의 기업에 퍼블릭 클라우드의 효과적이고 매우 안전한 대안을 제공합니다.

Cisco AMP Private Cloud Virtual Appliance는 온프레미스 로컬 환경에 저장된 빅데이터 분석, 정책, 탐지, 보호 기능을 사용해 포괄적인 지능형 악성코드 차단을 제공합니다. 솔루션이 알려지지 않은 의심스러운 파일을 발견한 경우, Cisco의 인텔리전스 데이터베이스인 Cisco AMP 위협 인텔리전스 퍼블릭 클라우드와 상호 작용하여 파일 속성을 조사합니다. 이 솔루션에서는 익명화된 SHA256(Secure Hash Algorithm 256) 정보만 보낸 다음 AMP Virtual Private Cloud Appliance를 업데이트하고 회귀적 보안을 실행합니다.

솔루션의 특징:

[1] AMP for Endpoints 및 AMP for Networks 구축 작업에서는 속성 조사 및 위협 인텔리전스에 퍼블릭 AMP 클라우드를 사용합니다. 반면에 AMP Virtual Private Cloud Appliance 는 온프레미스 프라이빗 클라우드입니다.

- **자족형 가상 머신을 통해 개인정보 보호 지원:** 가상 어플라이언스와 관리 시스템은 사용자의 자체 하드웨어에 설치하는 단일 온프레미스 솔루션입니다.
- **네트워크 및 엔드포인트 보호 제공:** 이 솔루션은 AMP for Endpoints 커넥터를 통해 엔드포인트에 연결하고 AMP for Networks에 직접 연결하여 네트워크 악성코드를 차단합니다.
- **퍼블릭 버전과 동일하게 다양한 기능 포함:** Cisco 퍼블릭 클라우드와 비슷하게 Cisco AMP Virtual Private Cloud Appliance는 AMP for Endpoints 콘솔을 통해 AMP for Endpoints 프라이빗 클라우드 구축의 중앙 집중식 관리를 활성화합니다. Firepower Management Center는 AMP for Networks 프라이빗 클라우드 구축을 위한 관리 콘솔입니다. 두 콘솔 모두 맞춤형 정책 및 탐지, 경로 추적 및 근본 원인 분석, 보고, 성향 캐시, 파일 분석, 디바이스 식별 가능 정보를 지원합니다.
- **늘어나는 요구사항을 해결할 수 있는 확장성:** 각 프라이빗 클라우드 인스턴스는 최대 10,000개의 커넥터를 지원하며, 여러 개의 어플라이언스를 환경에 추가할 수 있습니다.

구축 모드

Cisco AMP Virtual Private Cloud Appliance는 "Cloud Proxy Mode(클라우드 프록시 모드)" 및 "Air Gap mode(Air Gap 모드)"라는 두 가지 구축 모드가 지원됩니다.

Cloud-Proxy mode(클라우드 프록시 모드)의 경우:

- 성향 조사를 완료하는 데 인터넷 연결이 필요합니다.
- 엔드포인트 커넥터의 모든 트래픽은 프라이빗 클라우드로 향하지만, 성향 조사는 프라이빗 클라우드와 AMP 퍼블릭 클라우드 사이에서 이후에 수행됩니다.
- 검사되는 파일의 SHA-256 해시는 AMP Virtual Private Cloud Appliance에서 퍼블릭 AMP 클라우드에 전송되는 유일한 데이터입니다.
- AMP 클라우드에서 AMP Virtual Private Cloud Appliance로 직접 콘텐츠 및 소프트웨어 업데이트를 자동으로 검색할 수 있습니다.

Air Gap mode(Air Gap 모드)의 경우:

- 성향 조사를 완료하는 데 인터넷 연결이 필요하지 않습니다.
- 모든 트래픽은 커넥터와 어플라이언스 사이에만 존재합니다.
- 상태 쿼리는 프라이빗 디바이스에서 처리됩니다.
  - "Protect DB"라는 로컬 가상 인스턴스에는 전체 기능 및 보호에 필요한 성향 및 위협 인텔리전스가 포함되어 있습니다.

Air Gap mode(Air Gap 모드)에서 위협 인텔리전스 업데이트는 다음과 같이 실행됩니다.

- AMP Virtual Private Cloud Appliance에서 콘텐츠 및 소프트웨어 업데이트가 개별적으로 검색됩니다.
- "amp-sync"라는 제공된 툴을 사용하여 AMP 퍼블릭 클라우드에서 AMP Virtual Private Cloud Appliance에 대한 소프트웨어 및 콘텐츠 업데이트를 다운로드하고 동기화합니다.
- amp-sync를 실행하고 업데이트 패키지를 구축하려면 전용 호스트 서버("update host")가 필요합니다.
  - update host를 사용하여 업데이트를 검색하려면 인터넷 액세스가 필요합니다.

- update host의 최소 요건은 CentOS 6.6입니다.
- amp-sync로 구축된 업데이트 패키지 파일(ISO 파일)이 update host에서 전송되어 가상 어플라이언스에 마운트됩니다. 그다음, 관리 콘솔에서 업데이트 프로세스를 시작하고 완료할 수 있습니다.

- Protect DB 초기 스냅샷을 동기화하고 로컬 파일 저장소가 구축되므로, 초기 업데이트는 용량이 큽니다(약 85Gb). 후속 업데이트에서는 로컬 저장소 패치가 적용되므로 그보다 용량이 작습니다.
- 초기 설치 시 Protect DB 가져오기를 완료하기까지 3시간 이상이 소요될 수 있습니다.
- 업데이트는 매일 생성됩니다. 여기에는 Protect DB, Tetra 정의, 기타 위협 인텔리전스 업데이트(DFC, SE 등)가 포함됩니다.
- Protect DB 스냅샷은 매주 새로고침되므로, 신규 설치에 필요한 업데이트 수가 줄어듭니다.

그림 1과 2에는 각 구축 모드가 실행되는 방식이 그림으로 설명되어 있습니다.

그림 1. Cloud Proxy Mode(클라우드 프록시 모드)

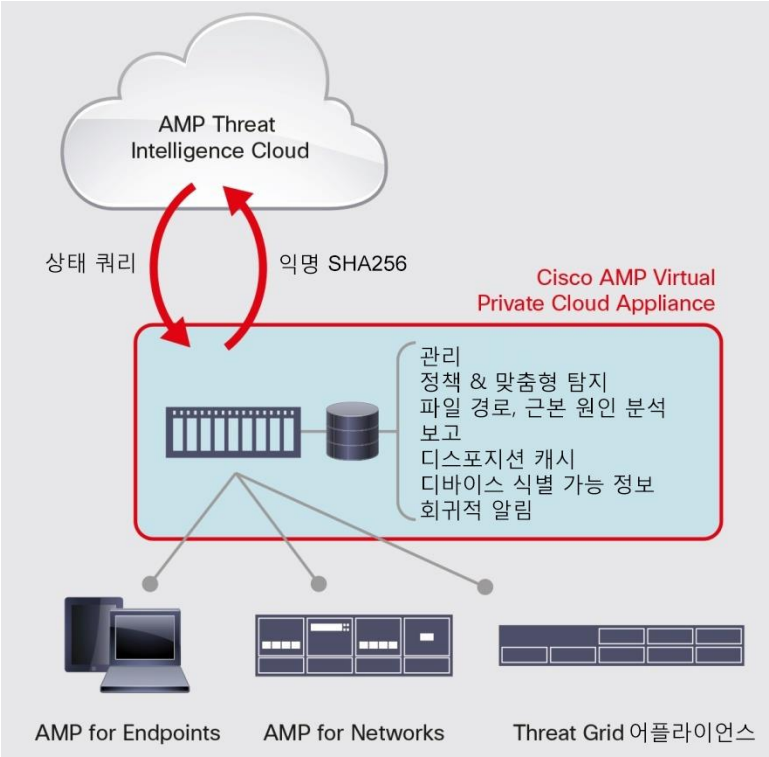
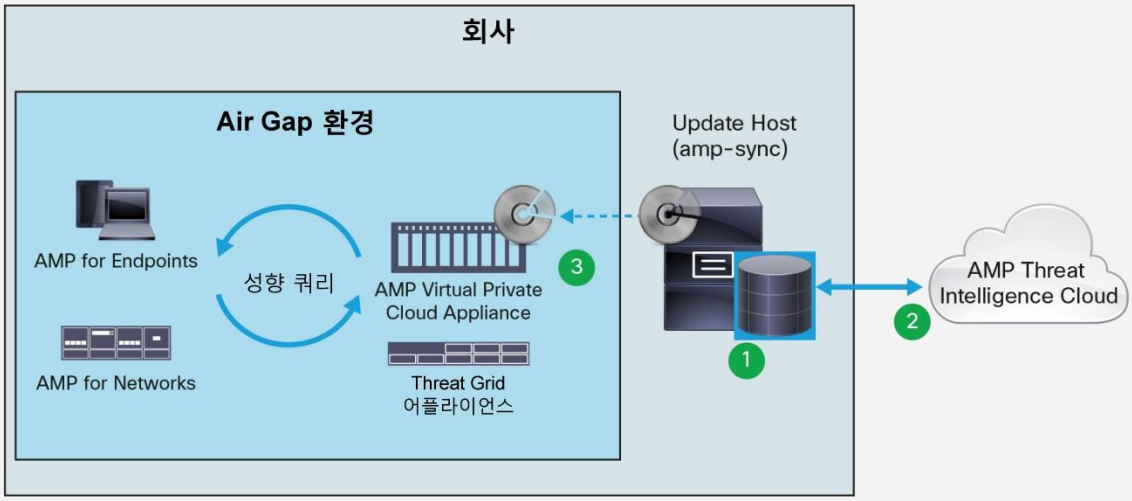


그림 2. Air Gap Mode(Air Gap 모드)



1 Update Host는 AMP Threat Intelligence Cloud에서 업데이트를 검색하고 패키지를 생성하는 "amp-sync" 툴을 실행 중입니다.

2 Update Host는 인터넷에 액세스하여 AMP Threat Intelligence Cloud에서 업데이트를 검색합니다.

3 Update Host의 업데이트 패키지(ISO)가 AMP Virtual Private Cloud Appliance로 이동합니다.

표 1에서는 AMP의 프라이빗 클라우드 구축과 퍼블릭 클라우드 구축을 비교하여 설명합니다.

표 1. AMP 프라이빗 클라우드 구축과 퍼블릭 클라우드 구축 비교

기능	Cisco AMP Virtual Private Cloud Appliance	Cisco AMP 퍼블릭 클라우드 구축	추가 정보
디바이스 및 파일 전파 흔적 분석	예	예	경로 추적 기능은 가시성을 확보하는 한편 악성코드 침입 범위를 파악하는 시간을 줄이기 위해 개별 디바이스에서, 그리고 전체 환경에서 오랜 시간 동안 파일 전파 경로를 추적합니다.
위협 근본 원인	예	예	악성코드의 출처 및 유입된 경위를 파악합니다.
클라우드 기반 보안 침해 지표(IOC)	예	예	IoC는 상관관계 분석을 통해 잠재적으로 유효한 침해로 우선 순위가 지정된 파일 및 텔레메트리 이벤트입니다. AMP에서는 여러 소스의 보안 이벤트 데이터(예: 침입, 악성코드 이벤트)를 대상으로 그 상관관계를 자동으로 파악하여 해당 이벤트를 더 큰 규모의 연계 공격에 연결하고 고위험 이벤트의 우선 순위를 지정할 수 있도록 합니다.
회귀적 알림	예	예	회귀적 보안이란 과거의 시점으로 돌아가 각종 프로세스, 파일의 활동, 통신을 추적하여 감염 사실을 종합적으로 파악하고 근본 원인을 규명한 다음 위협 요소를 제거하는 것을 의미합니다. 장기간의 분석 후에 파일 성향이 변경되면 알림이 전송되므로 관리자는 초기 방어를 우회하는 악성코드를 인지하고 가시화할 수 있습니다.

기능	Cisco AMP Virtual Private Cloud Appliance	Cisco AMP 퍼블릭 클라우드 구축	추가 정보
간단한 맞춤형 탐지	예	예	간단한 해시 기반의 1대 1 탐지 시그니처입니다.
고급 맞춤형 탐지	예(Windows 전용)	예	고급 시그니처를 지원합니다.
악성코드 분석	예	예	Threat Grid에 기반하여, File Analysis(파일 분석) 기능이 온프레미스 어플라이언스로 제공됩니다. 이 기능은 알 수 없는 파일의 고정 및 동적 분석을 수행하여 파일이 악성인지 확인하고, 양성일 경우 그 이유를 밝힙니다.
클라우드 성향 조사	Cloud Proxy Mode(클라우드 프록시 모드): 예 Air-Gapped Mode(Air-Gapped 모드): 아니요	예	AMP Private Cloud Virtual Appliance는 Air-Gapped Mode(Air-Gapped 모드)이지만, 클라우드에서 성향을 검색하기 위해 인터넷에 직접 연결하지 않습니다. 그러나 그와 동일한 강력한 위협 인텔리전스 저장소에서 성향을 검색합니다. 이 저장소는 대신 수동으로 동기화되며 Air-Gapped 환경에 포함됩니다.
SPERO 탐지 엔진	예	예	SPERO는 머신 학습 기술입니다.
ETHOS 탐지 엔진	아니요	예	ETHOS는 "비트 조작"에 기반한 악성코드 우회에 대응하기 위한 방법으로 "퍼지 해시"를 사용하여 악성코드군을 포착합니다.
TETRA 탐지 엔진	예	예	오프라인 탐지 엔진입니다.
역할 기반 액세스 제어(RBAC)	예	예	개별 사용자의 역할에 따라 AMP 내에서 특정 작업을 수행할 수 있는 액세스 및 권한을 규제합니다.
엔드포인트 IOC(보안 침해 지표)	예	예	엔드포인트 검사에 대한 OpenIOC 형식 규칙을 작성하고 구축할 수 있는 기능입니다.
취약한 소프트웨어 탐지	예	예	엔드포인트에 악성코드의 공격 벡터 역할을 할 수 있는 취약한 소프트웨어가 있다는 사실을 관리자에게 알립니다.
관리되는 커넥터	프라이빗 클라우드 어플라이언스당 10,000개로 제한	무제한	AMP Virtual Private Cloud Appliance의 경우 10,000개 이상의 커넥터에 추가 어플라이언스가 필요하며, 현재 각 인스턴스는 개별적으로 관리해야 합니다.
Firepower Management Center 통합	FMC 6.1부터	예	AMP Virtual Private Cloud Appliance를 통한 AMP for Networks 구축을 지원하는 관리 콘솔입니다.
데이터 프라이버시	예	예	Cloud Proxy Mode(클라우드 프록시 모드)의 AMP Virtual Private Cloud Appliance는 SHA-256 해시만 AMP 퍼블릭 클라우드에 전송합니다. Air-Gapped Mode(Air-Gapped 모드)에서는 AMP 퍼블릭 클라우드에 데이터가 전송되지 않습니다. AMP 퍼블릭 클라우드 구축을 위해서는 개인적으로 식별 가능한 정보를 제외한 기타 파일 메타데이터를 전송해야 합니다.

시스템 요구 사항

이 가상 시스템 인스턴스를 실행하기 위한 최소 요구 사항이 표 2에 나와 있습니다.

표 2. 소프트웨어 요구 사항

AMP Private Cloud 2.0	• VMware ESX 5 이상: 비공식적으로 VMware Fusion 6, Workstation 9 이상 지원 • Cloud-Proxy Mode(클라우드 프록시 모드): 32GB RAM, CPU 코어 8개(코어 4개당 CPU 2개 권장), 최소 여유 디스크 공간 238GB • Air-Gap Mode(Air-Gap 모드): 128GB RAM, CPU 코어 8개(코어 4개당 CPU 2개 권장), 최소 여유 디스크 공간 1TB
커넥터	• Microsoft Windows XP 서비스 팩 3 이상 • Microsoft Windows Vista 서비스 팩 2 이상 • Microsoft Windows 7 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Mac OSX 10.7~10.9 • AMP for Networks(v5.4 이상)

플랫폼 지원 및 호환성

AMP Virtual Private Cloud Appliance에는 가상 어플라이언스 자체와 관련 AMP 및 Threat Grid 서브스크립션이 포함됩니다.

보증 정보

보증 정보는 Cisco.com의 제품 보증 페이지에서 확인하십시오.

주문 정보

주문하려면 Cisco 주문 홈 페이지를 방문하거나 Cisco 세일즈 담당자에게 문의하거나 800 553-6387로 전화하십시오. 귀사에서 Cisco AMP Virtual Private Cloud Appliance를 주문하는 방법에 대한 자세한 지침을 제공받으려면 주문 설명서를 참조하십시오.

Cisco Capital

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 자세한 내용은 여기에서 확인하십시오.

추가 정보

자세한 내용은 Cisco AMP Virtual Private Cloud Appliance 웹 페이지를 참조하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA

C78-733180-04 12/16