



Cisco Advanced Malware Protection

실제 환경을 위한 침입 차단, 탐지, 대응 및 복원

이점

- 최전선 방어를 강화할 수 있는 최고 수준의 글로벌 위협 인텔리전스 확보
- 보안 침해의 최초 위치와 범위를 심층 파악하는 가시화 기능
- 악성코드에 대한 신속한 탐지, 대응, 복원 기능
- 많은 비용이 드는 재감염 및 복원 상황의 발생 방지
- 어디서나 제공되는 보호 - 네트워크, 엔드포인트, 모바일 디바이스, 이메일, 웹(공격 전, 공격 중, 공격 후)

오늘날의 지능형 악성코드는 잘 드러나지 않고 집요하며 기존의 방어 체계를 우회할 수 있습니다. 기존의 보안 기술은 위협을 빠르게 탐지 및 제거하여 피해를 방지하는 데 필수적인 가시성과 제어 능력을 제공하지 못합니다. 따라서 보안 팀은 각종 공격으로부터 조직을 방어하는 데 어려움을 겪고 있습니다.

조직은 공격에 노출되어 있으며 보안 침해 사고가 잇달아 뉴스 헤드라인을 장식하고 있습니다. 오늘날 해커들은 글로벌 커뮤니티를 만들어 활동하면서 지능형 악성코드를 양산해 다양한 공격 경로로 각 조직에 침투시키고 있습니다. 다면적인 표적 공격은 최고 수준의 특정 시점 탐지 톨마저도 우회할 수

있습니다. 이러한 톨은 트래픽과 파일이 네트워크에 진입하는 시점부터 면밀한 검사를 시도하지만 초기 탐지를 어떻게든 우회하는 위협까지 가시화하기는 어렵습니다. 따라서 보안 전문가들은 잠재적 보안 침해의 범위를 가늠할 수 없게 되고 악성코드로 인해 심각한 피해를 입기 전에 신속한 대응으로 악성코드를 막는 데 실패하게 됩니다.

Cisco® AMP(Advanced Malware Protection)는 지능형 악성코드 문제의 전체 라이프사이클을 다룰 수 있는 보안 솔루션입니다. 이 솔루션은 보안 침해 방지 기능과 더불어 1차 방어선을 우회하는 위협도 신속하게 탐지, 억제, 치료할 수 있도록 지원하는 가시성과 제어 기능을 제공합니다. 이 모든 기능을 비용 효율적으로 이용할 수 있고 운영 효율성에도 영향을 주지 않습니다.

제품 개요

AMP는 인텔리전스 기반의 통합 엔터프라이즈급 지능형 악성코드 분석 및 차단 솔루션입니다. 이 솔루션으로 공격 전, 공격 중, 공격 후에 걸친 공격의 전 범위에서 조직을 포괄적으로 보호할 수 있습니다.

- **공격 전**, AMP에서는 Cisco의 Collective Security intelligence, Talos Security Intelligence and Research Group, AMP Threat Grid의 위협 인텔리전스 피드 등의 글로벌 위협 인텔리전스를 활용하여 방어를 강화하고 이미 알려져 있거나 새롭게 대두되는 위협에 대비해 보호를 수행합니다.

- 공격 중에는 이러한 인텔리전스와 함께 잘 알려진 파일 시그니처 및 Cisco AMP Threat Grid의 동적 악성코드 분석 기술을 결합하여 정책 위반 파일 유형, 취약점 공격 시도, 네트워크에 침투하려는 악성 파일 등을 식별하고 차단합니다.
- 공격 후 또는 파일이 최초로 검사된 후에는 특정 시점 탐지 기능 수준을 넘어 모든 파일 활동과 트래픽을 지속적으로 모니터링하고 분석합니다. 이 과정에서는 파일의 성향에 관계없이 악의적인 동작의 가능성을 나타내는 모든 징후를 검색합니다. AMP에서는 알 수 없는 상태의 파일 또는 "양호"한 상태였던 파일의 행동에 이상이 나타나기 시작하면 즉시 탐지하여 보안 팀에 IoC(Indications of Compromise: 보안침해지표)와 함께 알립니다. 그런 다음 악성코드의 출처, 감염된 시스템, 악성코드의 행동을 확인할 수 있는 가시성을 제공합니다. 또한 침입이 발견되면 빠르게 대응하여 단 몇 번의 클릭만으로 복원할 수 있는 제어 기능도 제공합니다. 따라서 보안 팀에서는 신속하게 공격을 탐지하고, 침해 범위를 파악하고, 시스템 손상 이전에 악성코드를 격리하는 데 필요한 심층적인 가시성과 제어 기능을 확보합니다.

글로벌 위협 인텔리전스 및 동적 악성코드 분석

AMP는 뛰어난 수준의 보안 인텔리전스 및 동적 악성코드 분석을 기반으로 구축되었습니다. Cisco Collective Security Intelligence 에코시스템, Talos Security Intelligence and Research Group, AMP Threat Grid 위협 인텔리전스 피드는 업계 최고 수준의 실시간 위협 인텔리전스 및 빅 데이터 분석의 집합입니다. 이 데이터는 클라우드에서 AMP 클라이언트로 전달되므로 보안 팀에서는 최신 위협 인텔리전스를 확보해 각종 위협을 사전에 효과적으로 방어할 수 있습니다. 조직에서는 다음과 같은 이점을 얻을 수 있습니다.

- 매일 150만 개 악성코드 샘플 수신
- 전 세계 160만 개의 센서
- 일일 100테라바이트(TB)의 데이터
- 130억개의 웹 요청
- 엔지니어, 기술자, 연구원으로 구성된 글로벌 팀
- 24시간 운영

AMP는 이 강력하고 풍부한 상황별 정보에 대한 파일, 행동, 텔레메트리 데이터, 활동의 상관관계를 분석하여 악성코드를 신속하게 탐지해낼 수 있습니다. 보안 팀은 AMP의 자동화된 분석을 사용하여 침입을 검색할 때 시간을 절약할 수 있고 최신 위협 인텔리전스를 상시 확보하여 정교한 공격을 신속히 파악하고, 우선 순위를 지정하고, 차단할 수 있습니다.

또한 Cisco의 Threat Grid 기술은 AMP에 통합되므로 다음과 같은 이점도 제공합니다.

- 표준 형식으로 제공되는 고도로 정확하면서도 풍부한 상황 기반 인텔리전스 피드와 기존 보안 기술과의 원활한 통합 구현
- 560개 이상의 행동 지표를 바탕으로 매일 수백만 개에 달하는 샘플을 분석하여 수십억 개의 아티팩트 도출
- 보안 팀에서 위협 우선 순위를 쉽게 지정할 수 있도록 이해하기 쉬운 위협 점수 제공

AMP에서는 이와 같은 모든 인텔리전스 및 분석을 사용하여 보안 관련 의사 결정을 알리거나 사용자를 대신하여 자동으로 적절한 조치를 취합니다. 예를 들어, 지속적으로 업데이트되는 인텔리전스를 기반으로 시스템에서는 알려진 악성코드와 정책 위반 파일 유형을 차단하고, 악의적인 것으로 알려진 연결을 동적으로 블랙리스트에 올리고, 악성으로 분류된 웹사이트 및 도메인에 대한 파일 다운로드 시도를 차단할 수 있습니다.

지속적 분석 및 회귀적 보안

대부분의 네트워크 및 엔드포인트 기반 안티멀웨어 시스템에서는 파일이 제어 지점을 통과해 광범위한 네트워크로 들어오는 특정 시점에서만 해당 파일을 검사합니다. 분석이 멈추는 곳이 바로 이 지점입니다. 악성코드는 나날이 정교해져 초기 탐지를 매우 교묘하게 우회하고 있습니다. 슬립(sleep) 기술, 다형성(polymorphism), 암호화, 알 수 없는 프로토콜의 사용 등은 악성코드가 정체를 숨길 수 있는 수많은 방법 중의 일부일 뿐입니다. 눈에 안 보이므로 당연히 방어할 수 없으며 대부분의 주요 보안 침해는 바로 이런 식으로 발생합니다. 보안 팀은 위협이 들어오는 시점에 이를 잘 알아채지 못하고 그 이후에는 아예 찾아내지를 못합니다. 위협을 신속히 탐지하거나 격리할 수 있는 가시성도 없으므로 머지않아 악성코드는 목적을 달성하고 시스템은 손상됩니다.

Cisco AMP는 다릅니다. 그 특정 시점을 인식하고 선제적 탐지 및 차단 방식을 이용하더라도 100% 보호는 불가능하므로, AMP 시스템에서는 초기 인스펙션 후에도 파일과 트래픽을 지속적으로 분석합니다. AMP에서는 의심스럽거나 악의적인 행동을 보이는 숨은 위협을 신속하게 밝혀내기 위해 엔드포인트, 모바일 디바이스, 네트워크에서 이루어지는 모든 파일 활동과 통신을 모니터링하고, 분석하며, 기록합니다. 문제의 첫 징후가 나타나면 AMP에서는 보안 팀에게 알리고 위협의 행동에 대한 상세 정보를 제공합니다. 따라서 다음과 같은 주요 보안 문제에 답할 수 있습니다.

- 악성코드는 어디에서 시작되었습니까?
- 침입 시점과 방법은 무엇입니까?
- 악성코드는 그동안 어디에 있었고 어떤 시스템에 영향을 주었습니까?
- 위협은 무엇을 했으며 지금은 무엇을 하고 있습니까?
- 위협을 멈추고 근본 원인을 제거하려면 어떻게 해야 합니까?

보안 팀에서는 이러한 정보를 바탕으로 상황을 빠르게 파악할 수 있고 AMP의 억제 및 치료 기능을 통해 필요한 조치를 취할 수 있습니다. 관리자는 AMP의 간편한 브라우저 기반 관리 콘솔에서 단 몇 번만 클릭하면 파일이 다시 다른 엔드포인트에서 실행되는 것을 영구 차단할 수 있어 악성코드를 억제할 수 있습니다. AMP에서는 파일이 상주했던 모든 곳을 파악하고 있으므로 해당 파일을 메모리에서 꺼내 다른 모든 사용자를 위해 격리할 수 있습니다. 악성코드가 침입해도 보안 팀에서는 악성코드를 제거할 목적으로 더 이상 전체 시스템을 다시 이미지화할 필요가 없습니다. 그렇게 할 경우 많은 시간, 비용, 리소스가 소모되고 중요한 비즈니스 기능이 중단됩니다. AMP를 사용한 악성코드 복원은 IT 시스템이나 비즈니스에 부수적 피해를 입히지 않습니다.

이는 지속적인 분석, 지속적인 탐지, 회귀적 보안의 위력입니다. 이러한 기능을 통해 시스템에 있는 모든 파일의 활동을 기록하고, "좋은" 파일이 "나쁜" 파일이 된 것으로 추정되면 이를 탐지한 후, 저장된 기록 내역을 거슬러 올라가 위협이 시작된 지점과 관련 행동을 파악할 수 있습니다. 그리고 나서 AMP에서 제공하는 내장형 대응 조치와 복원 기능으로 위협을 제거할 수 있습니다. 또한 AMP에서는 위협의 시그니처부터 파일 행동에 이르기까지 파악된 모든 사항을 기억한 후, AMP의 자체 위협 인텔리전스 데이터베이스에 해당 데이터를 기록하여 최전선 방어를 한층 더 강화합니다. 따라서 해당 파일은 초기 탐지를 다시는 우회할 수 없습니다.

AMP를 사용하면 보안 팀에서는 심층적인 가시성 및 제어 기능을 확보하게 됩니다. 따라서, 빠르게 효율적으로 공격을 탐지하여 숨은 악성코드를 발견하고, 침해의 특성과 범위를 파악하며, 시스템 손상이 발생하기 전에 악성코드(제로데이 공격 포함)를 신속히 억제 및 치료하고, 추후 유사 공격의 재발을 방지할 수 있습니다.

주요 기능

AMP의 지속적 분석 및 회귀적 보안 기능은 다음과 같은 강력한 기능을 통해 구현됩니다.

- **IoC(Indications of Compromise: 보안침해지표):** 파일 및 텔레메트리 이벤트의 상관관계를 분석하고 잠재적인 활성 침해로 우선 순위를 지정합니다. AMP에서는 여러 소스의 보안 이벤트 데이터(예: 침입, 악성코드 이벤트)를 대상으로 그 상관관계를 자동으로 파악하여 보안 팀이 해당 이벤트를 더 큰 규모의 연계 공격에 연결하고 고위험 이벤트의 우선 순위를 지정하는 데 도움이 됩니다.
- **파일 평판:** 고급 분석 및 종합 인텔리전스를 수집하여 파일이 정상 파일인지 또는 악성 파일인지 여부를 판단함으로써 보다 정확한 탐지를 지원합니다.
- **정적 및 동적 악성코드 분석:** 고도의 보안성을 갖춘 환경에서 악성코드를 실행, 분석 및 테스트하는 방법으로 이전에 알려지지 않았던 제로데이 위협을 검색할 수 있습니다. AMP Threat Grid 샌드박스 기능과 정적 및 동적 악성코드 분석 기술을 AMP 솔루션 내에 통합하여 대규모 행동 분석 지표를 기준으로 검사하는 더욱 포괄적인 분석을 제공할 수 있습니다.
- **회귀적 탐지:** 장기간의 분석 후에 파일 성향이 변경되면 알림이 전송되므로 관리자는 초기 방어를 우회하는 악성코드를 인지하고 가시화할 수 있습니다.
- **파일 전파 흔적 분석:** 가시성을 확보하는 한편 악성코드 침입 범위를 파악하는 시간을 줄이기 위해 전체 환경에서 오랜 시간 동안 파일 전파 경로를 지속적으로 추적합니다.
- **디바이스 전파 흔적 분석:** 보안 침해 전후의 이벤트에 대한 근본 원인과 내역을 신속하게 파악하기 위해 디바이스 및 시스템 레벨에서 여러 활동과 통신을 지속적으로 추적합니다.
- **엘라스틱 검색(Elastic Search):** 파일, 텔레메트리, 종합적 보안 인텔리전스 데이터의 전 범위를 대상으로 간단하면서도 무제한적인 검색을 수행하여 위험 노출의 범위와 상황을 IoC 또는 악성 애플리케이션과 연계해 빠르게 파악할 수 있습니다.
- **파일 보급도:** 조직에서 실행된 모든 파일을 보급도(prevalence)별로 오름차순으로 정렬하여 표시하면, 이전에 소수의 사용자 외에는 탐지하지 못했던 위협을 효과적으로 드러낼 수 있습니다. 소수의 사용자만 실행했던 파일은 확장 네트워크에 있어서는 안 될 악성 파일(예: 표적화된 지능형 지속 위협)이거나 의심스러운 애플리케이션일 수 있습니다.
- **엔드포인트 IoC:** 사용자는 자신만의 IoC를 제출하여 표적 공격을 포착할 수 있습니다. 보안 팀은 환경에서 특정 애플리케이션을 공격하는 잘 알려지지 않은 지능형 위협을 더욱 심층적으로 조사할 수 있습니다.
- **취약점:** 시스템에서 실행되는 취약한 소프트웨어, 이러한 소프트웨어가 포함된 호스트, 그리고 손상 가능성이 가장 높은 호스트의 목록을 표시합니다. Cisco의 위협 인텔리전스 및 보안 분석에 기반한 AMP에서는 악성코드의 표적이 되고 있는 취약한 소프트웨어와 잠재적 공격 유형을 식별하여 패치가 필요한 호스트의 우선 순위 목록을 제공합니다.
- **아웃브레이크 제어(Outbreak control):** 의심스러운 파일 또는 공격 발생을 효과적으로 통제하여 콘텐츠 업데이트로 시간을 지체하지 않고도 감염을 치료할 수 있습니다. 아웃브레이크 제어 기능의 구성은 다음과 같습니다.
 - 단순한 맞춤형 탐지 기능 - 모든 시스템 또는 선택한 시스템에서 특정 파일을 빠르게 차단
 - 고급 맞춤형 시그니처 - 다형성 악성코드군을 차단
 - 애플리케이션 차단 목록 - 애플리케이션 정책을 시행하거나 악성코드 게이트웨이로 이용되는 손상된 애플리케이션을 격리하여 재감염의 악순환을 중지
 - 맞춤형 화이트리스트 - 보안이 유지되거나 맞춤형으로 설계된 애플리케이션 또는 미션 크리티컬 애플리케이션이 어떤 상황에서도 지속적으로 실행될 수 있도록 보장
 - 디바이스 흐름 상관관계 - 소스에서의 악성코드 콜백 통신 중지(특히 기업 네트워크 외부의 원격 엔드포인트 대상)

위치에 관계없는 보호를 지원하는 구축 옵션

사이버 범죄자는 조직 내부로 이어지는 다양한 진입 지점을 노려 공격을 개시합니다. 이렇게 은밀히 잠입하는 공격을 제대로 포착하려면 가능한 한 많은 공격 벡터를 심층적으로 파악할 수 있는 가시성이 필요합니다. AMP 솔루션은 광범위한 네트워크 전체에서 다양한 제어 지점에 구축할 수 있습니다. 즉 원하는 방법으로 원하는 위치에 솔루션을 구축하여 구체적인 보안 요구사항을 해결할 수 있습니다. 옵션에는 아래 목록의 내용이 포함됩니다.

제품 이름	세부 사항
Cisco AMP for Endpoints	사용자의 성능에 영향을 주지 않는 AMP의 저용량 커넥터를 사용하여 Windows PC, Mac, Linux 시스템, Android 모바일 디바이스, 가상 환경을 보호합니다. AMP for Endpoints를 AnyConnect v4.1에서 실행할 수 있습니다.
Cisco AMP for Networks	AMP를 Cisco FirePOWER™ NGIPS 보안 어플라이언스에 통합된 네트워크 기반 솔루션으로 구축합니다.
Cisco AMP on ASA with FirePOWER Services	AMP 기능을 Cisco ASA Adaptive Security Appliance 방화벽에 통합 구축합니다.
Cisco AMP Private Cloud Virtual Appliance	AMP를 온프레미스 에어 갭(air-gapped) 솔루션으로 구축합니다. 이는 특히 퍼블릭 클라우드 사용을 제한하며 높은 개인 정보 보호 수준이 필요한 조직을 위한 설계입니다.
Cisco AMP on CWS, ESA, or WSA	AMP 기능은 Cisco CWS(Cloud Web Security), ESA(Email Security Appliance), WSA(Web Security Appliance) 등을 위해 회귀적 기능 및 악성코드 분석을 제공하는 솔루션으로 이용할 수 있습니다.
Cisco AMP for Meraki MX	AMP를 지능형 위협 차단 기능을 갖춘 간소화된 클라우드 기반 보안 관리용 Meraki MX Security Appliance의 일부로 구축하십시오.
Cisco AMP Threat Grid	AMP Threat Grid는 Cisco AMP와 통합되어 향상된 악성코드 분석을 제공합니다. 또한 독립형 지능형 악성코드 분석 및 위협 인텔리전스 솔루션으로 클라우드에서 또는 어플라이언스에 구축될 수 있습니다.

이제 "어디서나" Cisco Advanced Malware Protection의 보호를 받을 수 있습니다. 은밀한 악성코드를 신속하게 탐지해 제거하려면 네트워크 에지에서 엔드포인트까지 여러 공격 벡터 전반에 걸쳐 이와 같은 가시성 및 제어 기능이 빠짐없이 보장되어야 합니다. 철저하고 신속한 조치를 위해 보안 인프라 전반에서 정보를 공유하는 것도 필요합니다. 이 모든 솔루션 간의 상호 연결, 커뮤니케이션 및 통합이 중요한 역할을 합니다. 단독 상태에서 실행되는 포인트 제품이 아닙니다. 이 솔루션을 함께 구축함으로써 상호 연동을 통해 체계적이고 신속하게 위협에 대응하는 통합 방어 체계가 탄생합니다. AMP 솔루션에서 모든 구축 환경의 위협 인텔리전스, 공격 지표, 이벤트 정보, 쿼린트 정보를 자동으로 공유하는 에코시스템이 형성됩니다. AMP의 "모든 곳을 예의 주시하는 기능"을 통해 조직에서는 악성코드의 탐지 소요 시간 및 치료 시간을 대폭 줄일 수 있습니다.

왜 Cisco를 선택해야 할까요?

이제 문제는 보안 공격의 가능성이 아니라 언제 공격을 받느냐입니다. 특정 시점 탐지만으로는 모든 공격에 대한 선제적 탐지 및 차단을 완벽히 보장할 수 없습니다. 위협이 침투할 수도 있습니다. 따라서 보안 침해에 대비하려면 조직에서는 침입을 신속히 탐지하여 이에 대응하고 치료할 수 있는 적절한 툴을 갖추고 있어야 합니다.

Cisco AMP는 인텔리전스 기반의 통합 엔터프라이즈급 지능형 악성코드 분석 및 차단 솔루션입니다. 이 솔루션은 네트워크 방어를 강화하기 위한 글로벌 위협 인텔리전스, 실시간으로 악성 파일을 차단하기 위한 분석 엔진, 모든 파일 행동과 트래픽을 초기 검사가 완료된 후에도 지속적으로 모니터링하고 분석하기 위한 기능 등을 제공합니다. 이러한 기능은 모두 잠재적 위협 활동을 심층적으로 파악할 수 있는 탁월한 가시성과 악성코드를 신속히 탐지, 억제, 제거할 수 있는 제어 능력을 제공합니다.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital® 금융 지원 솔루션을 통해 여러분이 비즈니스 목표를 달성하는 데 필요한 기술을 도입하고 경쟁력을 강화할 수 있습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용할 수 있습니다. [자세히 알아보십시오.](#)

다음 단계

Cisco AMP에 대한 자세한 내용은 <http://www.cisco.com/go/amp>를 참조하십시오. 또한 이 간략한 [개요 비디오](#), [요약](#) 또는 [상세 기술 데모](#)를 보거나 [고객의 평가](#)를 들어보실 수 있습니다. 또는 AMP와 [경쟁 제품 비교](#) 자료를 참조하거나 Cisco 세일즈 담당자에게 문의하여 Cisco AMP 전문가와 함께 [POV를 설정](#)하실 수도 있습니다.



미주 지역 본부
Cisco Systems, Inc.
캘리포니아 주 산호세

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. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 www.cisco.com/go/offices에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)