Cisco Advanced Malware Protection for Networks

제품 개요

오늘날의 악성코드에 효과적으로 맞서려면 새로운 접근, 전략, 기술이 필요합니다. Cisco® AMP(Advanced Malware Protection) for Networks는 네트워크 기반의 지능형 악성코드 차단 솔루션으로서 특정 시점 탐지에 머무르지 않고 공격 전/중/후의 전 범위에서 조직을 보호합니다. Cisco FirePOWER™ 네트워크 보안 어플라이언스를 위해 설계된 이 솔루션은 단일 시스템에서 여러 위협 벡터의 악성코드 위협을 탐지, 차단, 추적 및 억제합니다. 또한 고도로 정교하고 표적화된 제로데이 및 지속적인 지능형 악성코드 위협을 차단하는 데 필요한 가시성과 제어를 제공합니다.

Cisco AMP for Networks는 다음 이점을 제공합니다.

- **특정 시점 방어의 한계를 넘는 보호:** Cisco AMP for Networks는 특정 시점 방어의 한계를 넘어 파일 및 트래픽을 지속적으로 분석합니다. 이 기능으로 과거의 시점으로 돌아가 프로세스, 파일 활동, 통신을 추적하는 회귀적 보안을 실현할 수 있습니다. 감염의 전 범위를 파악하고 근본 원인을 규명하며 문제를 해결할 수 있습니다. 이에 따라 기업 조직을 더 효과적이고 효율적이며 광범위하게 보호할 수 있습니다.
- **정책 위반 파일 및 기타 제한:** Cisco AMP for Networks는 웹, 이메일, 기타 공격 벡터를 통해 들어오는 데이터를 추적하여 자동으로 파일과 애플리케이션을 인식합니다. 그런 다음 사용자가 설정한 애플리케이션 및 파일 제어 정책에 따라 광범위한 파일 필터링을 수행합니다.
- **익스플로잇 시도 탐지 및 차단:** 이 Cisco 솔루션은 인라인 구축으로 클라이언트 측 익스플로잇 시도를 탐지하여 차단할 수 있습니다. 또한 Adobe Acrobat, Java, Flash를 비롯하여 자주 표적이 되는 클라이언트 애플리케이션의 취약점을 노리는 익스플로잇 시도도 막아냅니다.
- **악성 파일 식별, 차단 및 분석:** 악성 파일을 표적 시스템에서 차단하고 미확인 속성을 가진 파일을 분석합니다. 파일 속성이 반환되지 않으면 의심스러운 파일이 추가 분석을 위해 Threat Grid에 자동으로 전송됩니다.
- **단순한 샌드박싱의 한계 넘기:** AMP for Networks에는 내장형 샌드박싱 기능이 포함되지만, Threat Grid와의 통합으로 완전히 새로운 차원의 악성코드 분석 및 위협 인텔리전스를 제공합니다. Threat Grid는 광범위한 규모의 글로벌 위협에 대응하기 위해 파일의 동작, 이해하기 쉬운 위협 점수 및 수십억 개의 악성코드 아티팩트를 원하는 대로 분석할 수 있도록 350개 이상의 고유한 행동 지표를 제공합니다.
- **지속적인 파일 및 트래픽 분석:** 어떤 파일이 악성으로 분류되면, 그 파일이 네트워크를 지난 지 몇 시간 또는 며칠이 경과했더라도, AMP for Networks 시스템에서 회귀적 경고를 발효하므로 피해를 줄이기 위한 조치를 취할 수 있습니다.
- **각기 다른 이벤트의 상관성을 분석하여 복잡한 공격 파악:** Cisco AMP for Networks는 지속적인 공격과 관련된 위험을 규명합니다. 여러 이벤트 소스에서 제공한 보안 이벤트 데이터를 통합하여 공격받았을 가능성이 있는 디바이스의 목록을 우선순위에 따라 자동으로 생성합니다.

- **악성코드의 확산 및 통신 추적:** Cisco AMP for Networks File Trajectory로 네트워크 전 범위에서 파일의 전송 경로를 추적할 수 있습니다. 파일 전파 흔적 분석 화면에서는 파일별 지도를 통해 시간의 경과에 따른 파일의 전송 과정과 파일에 대한 추가 정보를 시각적으로 표시합니다.
- **악성코드 억제로 손실 및 보안 침해 예방:** AMP for Networks에서는 간단한 정책 업데이트를 통해 최신 위협 요소와 악성코드 유포를 막을 수 있습니다. 맞춤형 탐지 목록을 사용하면 벤더가 제공한 업데이트를 기다리지 않고 언제라도 조치를 취할 수 있습니다.

효과적인 보안은 탐지 이상의 기능 필요

특정 시점 방어 기술만으로는 결코 100%의 실효성을 거둘 수 없습니다. 탐지를 피한 하나의 위협이 전체 환경을 침해할 수 있습니다. 교묘한 공격자들은 상황 인식형 표적 악성코드를 구사하며 뛰어난 리소스, 전문성, 인내심을 바탕으로 언제든 특정 시점 방어를 무력화하면서 어떤 기업도 무너뜨릴 수 있습니다. 게다가 특정 시점 방어 기술로는 침해 발생 후의 범위 및 정도를 전혀 알 수 없으므로 보안 침해의 확산을 저지하거나 유사한 공격의 재발을 막을 수 없게 됩니다.

Cisco AMP for Networks는 특정 시점의 탐지에 머무르지 않고 통합 제어 및 지속적인 분석 기능을 사용하여 위협을 탐지, 확인, 추적, 분석, 해결함으로써 지능형 악성코드 공격의 전/중/후 전 범위에서 보호하는 유일한 네트워크 기반 시스템입니다. 공격 전 단계에서 Cisco AMP for Networks는 알려진 악성코드 및 정책 위반 파일 형식 및 통신이 네트워크에 진입할 수 없게 하여 공격 표면을 축소합니다. 공격 중에는 익스플로잇 시도와 악성 파일 및 트래픽을 탐지하여 차단합니다.

공격 후 AMP 시스템은 선점형 탐지 및 차단 방식이 100% 효과적이지 않음을 인식하고 파일 및 네트워크 트래픽을 지속적으로 분석하여 초기 탐지망을 통과했을 숨은 위협을 찾아냅니다. 새로운 IoC(indications of compromise: 보안 침해 지표)가 발생하면 자동으로 여러 소스의 보안 이벤트 데이터, 즉 회귀적 악성코드 알림, 침입 이벤트, 악성코드 콜백 시도 등의 연관성을 분석하여 우선순위 기반의 단일 화면에 표시합니다. 따라서 이제는 공격이 발생하더라도 이 인텔리전스 자동화 기능을 활용하여 사후에도 신속하고 효율적으로 활성 공격과 그 범위를 파악하고 억제할 수 있습니다. 따라서 중요한 억제까지의 소요 시간이 단축되고 악성코드가 피해를 일으키기 전에 그 확산을 막을 수 있습니다.

Cisco AMP for Networks는 일상적으로 다루는 실행 가능 이벤트의 수도 줄이고 실행 가능한 통찰력을 제공하여 가장 중요한 고위험 지능형 악성코드 위협의 해결에 주력할 수 있게 합니다.

뿐만 아니라 Cisco AMP for Networks는 Cisco AMP for Endpoints와 호환도 가능합니다. Cisco AMP for Endpoints는 PC, Mac, Linux, 모바일 디바이스, 가상 시스템을 위한 Cisco의 종합 지능형 악성코드 차단 제품으로서 디바이스에 소프트웨어 기반 커넥터로 구축할 수 있습니다. 보호 네트워크에 연결되었거나 인터넷에서 로밍하는 엔드포인트를 보호합니다. Cisco AMP for Networks와 Cisco AMP for Endpoints를 모두 구축함으로써 확장된 IT 에코시스템의 전반에서 완벽한 가시성과 제어를 실현할 수 있습니다.

최고의 보안 인텔리전스 및 악성코드 분석

Cisco AMP for Networks는 빅 데이터 및 탁월한 보안 인텔리전스에 기반합니다. Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, Threat Grid 위협 인텔리전스 및 악성코드 분석 엔진은 가장 폭넓은 가시성, 최대 규모의 설치 기반, 그리고 여러 보안 플랫폼에 실행할 수 있는 기능과 더불어 업계 최대 규모의 실시간 위협 인텔리전스를 보유하고 있습니다. 이 데이터는 클라우드에서 AMP for Networks로 전달되므로 항상 최신 위협 인텔리전스를 사용할 수 있습니다.

다음을 비롯하여 방대한 규모로 수집되는 실시간 위협 인텔리전스를 활용할 수 있습니다.

- 매일 수신하는 110만 개의 악성코드 샘플
- 130억개의 웹 요청

- 전 세계 160만 개의 센서
- 엔지니어, 기술자, 연구원으로 구성된 팀
- 일일 100테라바이트의 데이터
- 24시간 운영

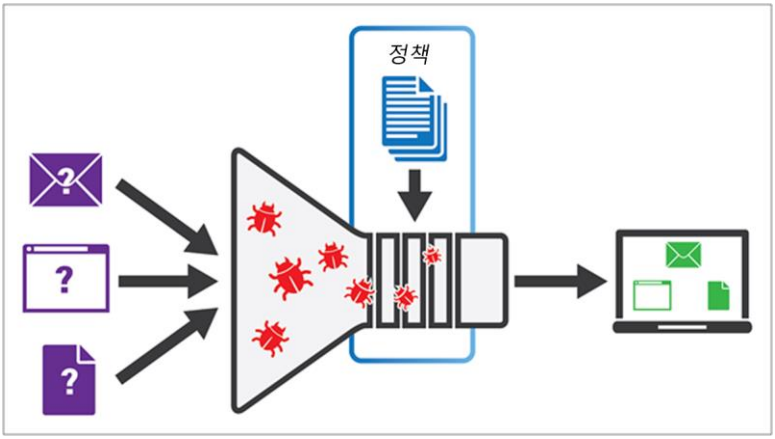
AMP for Networks는 이 강력하고 풍부한 상황별 정보에 대한 파일, 행동, 텔레메트리 데이터, 활동의 상관관계를 자동으로 분석하여 네트워크에 침투하려는 위협을 차단합니다. 네트워크 안의 위협에 대한 보안 팀의 인식이 개선되므로 사고 대응이 더 쉽고 빨라집니다.

Threat Grid 기술을 AMP for Networks에 통합시켜 파일 구조뿐 아니라 파일 전송 작업도 평가하는 350여 가지의 고유한 행동 지표를 제공하여 관련 HTTP 및 DNS 트래픽, TCP/IP 스트림, 영향을 미치는 프로세스, 레지스트리 활동 등 미확인 악성코드에 대한 고급 정보를 제공합니다. 또한 Threat Grid는 다양한 상황에서 실행 가능한 콘텐츠를 매일 제공합니다. 8백만 개 이상의 샘플이 매월 분석되므로 수십억 개의 아티팩트가 생성됩니다. 마지막으로 고도로 정확한 콘텐츠 피드를 기존 보안 기술과 원활하게 통합되는 표준 형식으로 제공하여 각 조직의 다양한 상황에 적용되는 인텔리전스를 생성할 수 있도록 합니다.

정책 위반 파일 및 기타 제한

Cisco AMP for Networks에서는 시스템에서 허용되는 파일 형식을 정의할 수 있습니다. 웹, 이메일로 수신한 파일이든 기타 공격 벡터에서 온 파일이든 상관없이 시스템은 파일과 애플리케이션을 자동으로 인식합니다. 그런 다음 설정한 애플리케이션 및 파일 제어 정책에 따라 광범위 파일 필터링을 수행합니다(그림 1 참조). 이 정책은 인바운드 및 아웃바운드 파일에 적용 가능하므로 다운로드 및 업로드한 파일을 제어할 수 있으며 외부 및 내부 위협 요인을 모두 다룹니다.

그림 1. 정책 위반 파일 제한



글로벌 보안 인텔리전스 피드도 갖추고 있어 악성으로 확인된 연결을 동적으로 블랙리스트에 추가합니다. URL 필터링 라이센스 옵션을 사용하면 악성으로 분류된 웹사이트 및 도메인의 파일 다운로드 시도를 차단할 수 있습니다.

익스플로잇 시도 탐지 및 차단

Cisco AMP for Networks는 Cisco FirePOWER NGIPS(Next-Generation Intrusion Prevention System)를 기반으로 합니다. 이 시스템을 인라인 형태로 구축하면 일명 드라이브바이 공격이라고도 하는 악성 파일 다운로드로 이어질 수 있는 클라이언트 측 익스플로잇 시도를 탐지하여 차단합니다. NGIPS 시스템은 웹 브라우저, Adobe Acrobat, Java, Flash 등 자주 표적이 되는 기타 클라이언트 애플리케이션에 대한 그 밖의 취약점 익스플로잇 시도도 막을 수 있습니다. 공격 체인에서 최대한 신속하게 조치하여 부수적 피해를 줄임으로써 막대한 정리 비용의 부담을 방지합니다.

악성 파일 탐지, 차단, 분석

Cisco AMP for Networks는 Cisco Collective Security Intelligence 클라우드를 활용하여 웹, 이메일 등 여러 공격 벡터의 전 범위에서 실시간으로 파일 속성을 수집합니다. 알려진 악성 파일은 대상 시스템에 도착하기 전에 차단됩니다. 알려지지 않은 속성을 가진 파일은 분석을 위해 Threat Grid 위협 인텔리전스 및 악성코드 분석 엔진에 자동으로 제출됩니다. 분석한 파일에 대해 위협 점수가 산정되며 관리 콘솔에서 제공하는 Threat Grid의 상세한 위협 보고서를 의사 결정에 참조할 수 있습니다. 어떤 형식의 파일도 시스템에 저장하고 안전하게 검색하여 직접 추가 분석을 수행할 수도 있습니다.

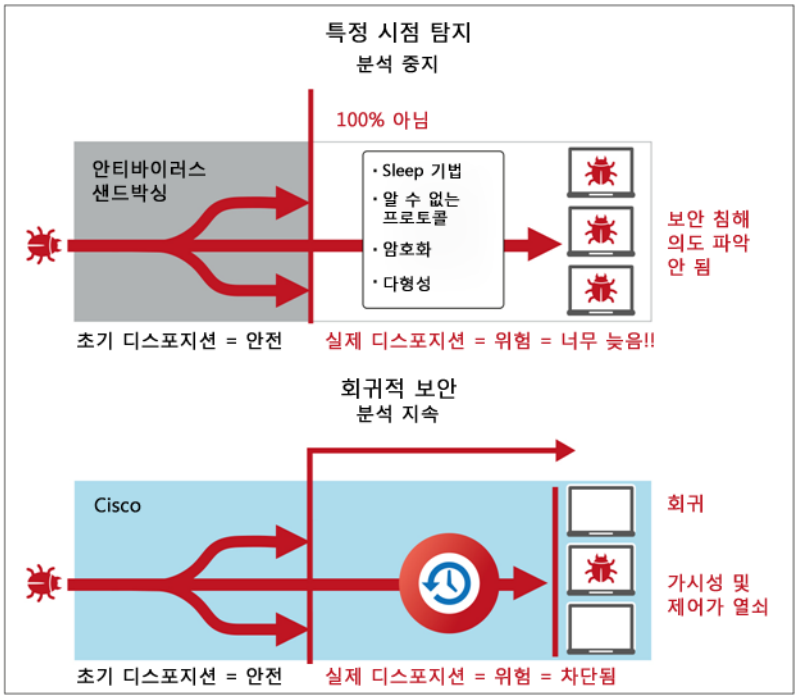
지속적인 파일 및 트래픽 분석

일반적인 네트워크 기반 악성코드 차단 시스템은 악성코드가 네트워크 디바이스를 지나는 특정 시점에만 이를 검사합니다. 어떤 탐지 기술도 100% 효과적이지는 않고 지능형 악성코드는 스스로를 위장하여 1차 방어선을 통과할 수도 있으므로 초기 검사가 끝난 후에는 더 이상 가시성을 확보하지 못할 때가 많습니다.

Cisco는 특정 시점 탐지 외에 빅데이터 기반의 지속적인 분석도 실시하여 이러한 문제를 해결합니다. 이러한 지속적인 분석으로 악성코드가 최초 검사 후 디바이스를 통과했더라도 악성코드 판정을 내릴 수 있습니다. 지속적인 분석은 회귀적 보안을 가능하게 하는 핵심 요소입니다(그림 2).

Cisco AMP for Networks 시스템의 회귀적 알림을 통해 관찰된 파일이 몇 시간 또는 며칠 전에 네트워크를 지났더라도 악성으로 판정된 시점을 확인하여 조치를 취하고 피해를 줄일 수 있습니다.

그림 2. 특정 시점 방어와 지속적 분석 및 회귀적 보안 비교



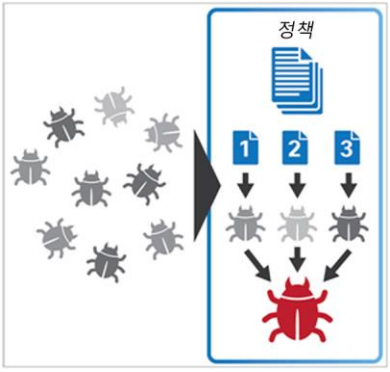
각기 다른 이벤트의 상관성 분석으로 복잡한 공격 파악

Cisco AMP for Networks에 포함된 Cisco FireSIGHT™ Management Center(그림 3)는 Cisco의 검색 및 인식 기술이 구현된 대시보드입니다. 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크, 지오로케이션 정보, 취약점에 대한 정보를 수집합니다. Cisco AMP for Networks는 이와 같이 서로 다르지만 연관된 이벤트를 취합하여 FireSIGHT Management Center에서 종합적인 IoC로 표시합니다.

그림 3. Cisco FireSIGHT Management Center

이 보기에서는 공격당했을 가능성이 있는 디바이스를 우선순위에 따라 자동으로 나열합니다. 여러 이벤트 소스의 보안 이벤트 데이터를 조합하여 진행 중인 공격과 관련된 위험을 나타냅니다(그림 4). 이와 같이 추가적인 상황 데이터를 통해 현명한 결정을 내리고 최상의 조치를 취할 수 있습니다.

그림 4. 이벤트 상관관계

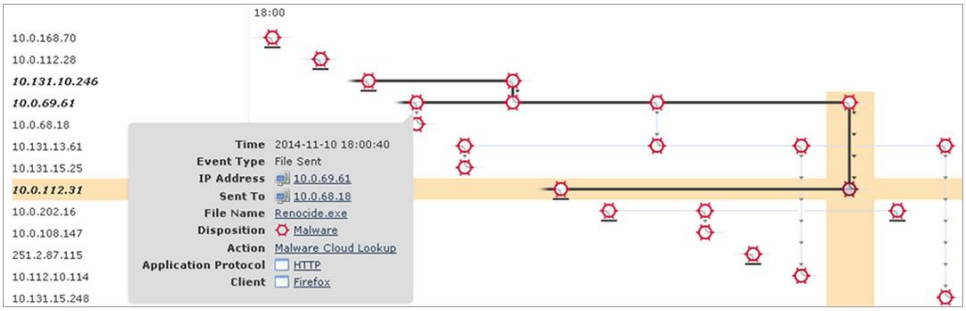


악성코드의 확산 및 통신 추적

Cisco AMP for Networks는 파일 전파 흔적 분석 기능을 사용하여 네트워크 전 범위에서 파일의 전송 경로를 추적할 수 있습니다. 파일 전파 흔적 분석 화면에서는 파일별 지도를 통해 시간의 경과에 따른 파일의 전송 과정과 파일에 대한 추가 정보를 시각적으로 표시합니다.

파일 전파 흔적 분석은 잠재적 감염의 영향과 범위를 파악하는 데 필수적입니다. 핵심적인 FireSIGHT 데이터가 함께 제공되어 의사 결정을 지원합니다. 표적 시스템 및 그 시스템의 사용자, 프로토콜 및 통신 시도와 같은 상황 정보는 모두 이 파일과 관련된 위험을 더 확실하게 파악하는 데 사용할 수 있습니다.

그림 5. 파일 전파 흔적 분석



악성코드 억제로 손실 및 공격 예방

활성 공격에 대한 조치를 결정할 때 Cisco AMP for Networks로 신속하게 공격을 억제할 수 있습니다. 간단한 정책 업데이트로 파일 블랙리스트를 작성하고 악성코드 통신을 차단할 수 있습니다. 맞춤형 탐지 목록을 사용하여 언제라도 조치를 취할 수 있습니다. 벤더가 제공하는 업데이트가 적용될 때까지 기다릴 필요 없습니다.

서드파티 테스트에서 우수한 결과를 보인 Cisco AMP

Cisco가 NSS Labs 보안 침해 탐지 시스템 보고서 부문에서 2년 연속 선두에 올랐습니다. 2015 년 NSS Labs 보안 침해 탐지 시스템 비교 분석 보고서에서 Cisco AMP는 다음과 같은 성과를 거두었습니다.

- 99.2% 보안 실효성 - 전체 테스트 대상 벤더 중 선두
- 벤더 중 유일하게 테스트 중에 모든 우회적 기술을 100% 차단
- 엔드포인트 또는 애플리케이션 레이턴시에 미치는 영향을 최소화하면서 뛰어난 성능 실현

침입 탐지 및 예방 표준인 Snort의 제정에 참여한 Cisco의 근본은 보안에 있습니다. FirePOWER 어플라이언스 제품군은 전례 없는 수준의 처리량 성능, 비용 효율성, 확장성을 자랑합니다. 그리고 FireSIGHT Management Center는 상황 인식 기능으로 네트워크의 구성을 파악하여 더 우수한 정확성과 자동화를 실현합니다.

표 1에서 동급 최고인 Cisco AMP for Networks의 기능을 살펴볼 수 있습니다.

표 1. Cisco AMP for Networks의 기능 및 이점

기능	이점
지속적인 분석	AMP for Networks에서는 특정 시점 방어에 머무르지 않고 클라우드 기반 빅 데이터 분석 기술을 바탕으로 일정 기간 수집된 데이터를 지속적으로 재평가하여 드러나지 않은 공격을 탐지합니다.
회귀적 보안	회귀적 보안이란 과거의 시점으로 돌아가 각종 프로세스, 파일의 활동, 통신을 추적하여 감염 사실을 종합적으로 파악하고 근본 원인을 규명한 다음 위협 요소를 제거하는 것을 의미합니다. IoC(indication of compromise: 보안 침해 지표)가 나타날 때, 이를테면 이벤트 트리거, 파일 속성의 변화, IoC 트리거가 발생할 때 회귀적 보안이 필요하게 됩니다.

기능	이점
FireSIGHT Management Center	단일 창에서 환경 전반에 대한 가시성을 확보합니다. 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크, 지오로케이션 정보, 취약점까지 종합적인 상황을 기반으로 파악하면서 보안에 대한 현명한 결정을 내릴 수 있습니다.
종합적 보안 인텔리전스	Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, Threat Grid는 가장 폭넓은 가시성, 최대규모의 설치 기반, 그리고 여러 보안 플랫폼에 실행할 수 있는 기능과 더불어 업계 최대 규모의 실시간 위협 인텔리전스를 보유하고 있습니다.
보안 침해 지표	IoC는 상관관계 분석을 통해 잠재적으로 유효한 침해로 우선 순위가 지정된 파일 및 텔레메트리 이벤트입니다. Cisco AMP for Networks는 여러 소스의 보안 이벤트 데이터(예: 침입, 악성코드 이벤트)를 대상으로 그 상관관계를 자동으로 파악합니다. 따라서 보안 팀이 해당 이벤트를 더 큰 규모의 연계 공격에 연결하고 고위험 이벤트의 우선순위를 지정할 수 있습니다.
파일 평판	고급 분석 및 종합 인텔리전스를 수집하여 파일이 정상 파일인지 또는 악성 파일인지 여부를 판단함으로써 보다 정확한 탐지를 지원합니다.
파일 분석 및 샌드박싱	Threat Grid의 고도의 보안성을 갖춘 환경에서 악성코드 행동을 실행, 분석 및 테스트하여 이전에 알려지지 않았던 제로데이 위협을 검색할 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.
통합된 SSL 해독	SSL 암호화 네트워크 트래픽을 식별하고 해독하며 이 트래픽에 대한 검사 및 탐지를 수행합니다. 또한 SSL 인증서 정책을 적용하고 네트워크에 대한 중앙 SSL 정책 제어를 지원할 수 있습니다.
AMP for Endpoints와의 통합	Cisco AMP for Networks는 PC, Mac, Linux, 모바일 디바이스, 가상 시스템을 지능형 악성코드로부터 보호하는 제품인 Cisco AMP for Endpoints와 호환됩니다. 두 시스템을 모두 구축함으로써 확장된 IT 에코시스템의 전 범위에서 탁월한 가시성과 제어를 실현할 수 있습니다.
AMP Threat Grid와의 통합	AMP Threat Grid의 샌드박싱 기술 및 지능형 악성코드 분석 기능을 AMP for Networks와 통합하면 파일의 동작, 이해하기 쉬운 위협 점수 및 수십억 개의 악성코드 아티팩트를 분석하는 350개 이상의 고유한 행동 지표를 원하는 대로 사용하여 광범위한 규모의 글로벌 위협에 대응할 수 있습니다.

제품 성능 및 사양

Cisco AMP for Networks는 어떤 Cisco FirePOWER 보안 어플라이언스에도 구축할 수 있습니다. 그러나 Cisco AMP 전용 어플라이언스인 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390(표 2 참조)에서 Cisco AMP for Networks 솔루션의 모든 이점을 누릴 수 있습니다. 까다로운 환경에서 구체적인 목표를 달성하기 위해 전용 처리 성능과 스토리지를 갖춘 어플라이언스 모델에 구축됩니다.

표 2. 하드웨어 사양: 전용 Cisco AMP for Networks Appliance

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
Advanced Malware Protection 처리량[1]	500Mbps	1Gbps	2Gbps	5Gbps	10Gbps	15Gbps	20Gbps
최대 모니터링 인터페이스[2]	12	12(3 x 4포트 RJ45 Netmod)	12(3 x 4포트 RJ45 Netmod)	28(7 x 4포트 RJ45 Netmod)	24(6 x 4포트 RJ45 Netmod)	20(5 x 4포트 RJ45 Netmod)	16(4 x 4포트 RJ45 Netmod)
고정 모니터링 인터페이스	4 x 10/100/1000(RJ45)	0	0	0	0	0	0
모듈형 인터페이스	8 SFP(1GB) 페일오버 없음	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)
Netmod 확장 슬롯	0	3	3	7	6	5	4
프로그래밍 가능 페일오픈(FailOpen) 인터페이스	4 x 10/100/1000(RJ45)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)	예(Netmod 필요)
관리 인터페이스	1 x 10/100/1000(RJ45)	1 x 10/100/1000(RJ45)	1 x 10/100/1000(RJ45)	2 x 10/100/1000(RJ45)	2 x 10/100/1000(RJ45)	2 x 10/100/1000(RJ45)	2 x 10/100/1000(RJ45)

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
평균 대기 시간	150마이크로초 미만	150마이크로초 미만	150마이크로초 미만	150마이크로초 미만	150마이크로초 미만	150마이크로초 미만	150마이크로초 미만
스토리지 용량(SSD)	120GB	400GB+	400GB	400GB+	800GB+	1200GB+	1600GB+
스택 지원	아니요	아니요	아니요	예	예	예	예
냉각 팬	5	10	10	6	12	18	24
전원 공급 장치	2(핫 스왑)	2(핫 스왑)	2(핫 스왑)	2(핫 스왑)	4(핫 스왑)	6(핫 스왑)	8(핫 스왑)
폼 팩터	1U	1U	1U	2U	4U	6U	8U
치수(인치, 깊이 x 너비 x 높이)	21.6 x 19.0 x 1.73	27.25 x 16.93 x 1.7	27.25 x 16.93 x 1.7	29 x 17.2 x 3.48	29 x 17.2 x 6.96	29 x 17.2 x 10.44	29 x 17.2 x 13.92
최대 배송 중량	29파운드 (13.2Kg)	54파운드 (25.5Kg)	54파운드 (25.5Kg)	67파운드 (30.5kg)	2 x 67파운드	3 x 67파운드	4 x 67파운드
AC 전압[3]	100 - 240VAC(공칭) 90 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)	100 - 240VAC(공칭) 85 - 264VAC(최대)
전류[4]	8A(전 범위에서 최대)	8A(전 범위에서 최대)	8A(전 범위에서 최대)	11A(전 범위에서 최대)	2 x 11A	3 x 11A	4 x 11A
DC 전압 옵션	아니요	아니요	아니요	예	예	예	예
최대 전원 출력[5]	450W	650W	650W	1000W	2 x 1000W	3 x 1000W	4 x 1000W
평균 전력 소비량[7]	200W	400W	400W	635W	2 x 635W	3 x 635W	4 x 635W
작동 온도	5° C - 40° C	10° C - 35° C	10° C - 35° C	5° C - 40° C	5° C - 40° C	5° C - 40° C	5° C - 40° C
주파수 범위	47Hz ~ 63Hz	47Hz ~ 63Hz	47Hz ~ 63Hz	47Hz ~ 63Hz	47Hz ~ 63Hz	47Hz ~ 63Hz	47Hz ~ 63Hz
공기 흐름	Front to Back	Front to Back	Front to Back	Front to Back[6]	Front to Back[6]	Front to Back[6]	Front to Back[6]
BTU/Hour 등급(과부하)	900BTU	1725BTU	1725BTU	2900BTU	2 x 2900	3 x 2900	4 x 2900
작동 습도	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%
RoHS 규정 준수	예	예	예	예	예	예	예
안전법 인증 ®	예	예	예	예	예	예	예

[1] AMP AMP 처리량 수치는 활성화된 방화벽, IPS, AMP 기능을 포함한 것입니다. 실제 정확한 네트워크 성능은 프로토콜 구성, 검사 대상 평균 패킷 크기 등 Cisco에서 제어할 수 없는 조건에 따라 달라집니다.

[2] Netmod는 페일오버 또는 비페일오버(non-failover)일 수 있습니다.

[3] 모든 섀시는 입력 전압이 동일합니다.

[4] 각 섀시에서 전류를 끌어옵니다.

[5] 각 섀시의 전원 공급 장치는 섀시에 대한 출력 전원이 정격 1000W입니다.

[6] 어플라이언스당 2- 1"sq. 측면 흡입구가 있습니다.

[7] 전원 공급 장치는 1+1 이중화입니다.

[8]AMP 8360, 8370, 8390은 스택형 어플라이언스이므로 특정 사양에 각 스택의 수(각각 2, 3, 4)를 곱하면 됩니다.

* NGIPS/NGFW 성능 수치에 대한 세부사항은 Cisco Firepower 어플라이언스 데이터 시트(http://www.cisco.com/go/ngips)에서 참조할 수 있습니다.

** FirePOWER 어플라이언스와 전용 AMP 어플라이언스는 동일 플랫폼 번호(예: FP8350과 AMP8350)를 유지하며 어플라이언스 + 통합 악성코드 스토리지 팩도 동일합니다.

소프트웨어 요구 사항

소프트웨어 요구 사항은 표 3에 나와 있습니다.

표 3. 소프트웨어 요구 사항

네트워크 기반 AMP: • 모든 Cisco FirePOWER 7000 및 8000 Series 어플라이언스, 가상 64비트 어플라이언스에서 지원 • v5.3 이상 필요 • Cisco FireSIGHT Management Center 필요(Management Center는 Collective Security Intelligence 클라우드 또는 온프레미스 Cisco AMP Private Cloud Virtual Appliance와의 인터넷 연결 필요)	평판 조회가 지원되는 파일 형식(확장자의 예): • Microsoft Office 문서(doc, xls) • 휴대용 문서(pdf) • 아카이브 파일(jar) • 멀티미디어 파일(swf) • 실행 가능 이진 파일(msexe, jar.pack)
지원 애플리케이션 프로토콜: • HTTP • SMTP • IMAP • POP3 • FTP • NetBIOS-ssn(SMB)	평판 조회 속성: • Clean(정상으로 확인) • Unknown(중성 또는 충분한 데이터 없음) • Malicious(악성으로 확인)
양방향 검사 및 제어	파일 식별 작업 • 탐지 또는 차단(파일 형식, 전송 방향, 프로토콜 기준) • 악성코드 클라우드 조회(평판 쿼리)
지리적 소스 또는 목적지 기준 파일 차단 지원	IoC 상관성 분석에 지원되는 이벤트 유형 또는 데이터 소스 • IPS 이벤트(네트워크) • Cisco AMP for Endpoints • 악성코드 이벤트(네트워크) • 보안 인텔리전스(네트워크 및 엔드포인트) • Cisco FireSIGHT 상황 데이터
CollectiveSecurity Intelligence 클라우드에서 제공하는 동적 블랙리스트 지원	맞춤형 탐지(사용자 정의 블랙리스트와 화이트리스트)
Collective Security Intelligence 클라우드에 동적 분석을 위해 자동 제출: • Microsoft 실행 파일(msexe, dll) • 분석 후 위협 점수 및 동적 분석 보고서 제공	

플랫폼 지원 및 호환성

Cisco AMP for Networks는 선택된 Cisco FirePOWER Appliance, Cisco FirePOWER Appliance Subscription for AMP, 그리고 선택 사항인 IPS, 애플리케이션, URL 필터링 서브스크립션으로 구성됩니다. Cisco AMP for Networks는 Cisco Firesight Management Center를 통해 관리됩니다.

워런티 정보

워런티 정보는 Cisco.com의 제품 워런티 페이지를 참조하십시오.

주문 정보

주문하려면 Cisco 주문 홈 페이지를 방문하거나 Cisco 세일즈 담당자에게 문의하거나 800 553-6387로 전화하십시오.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 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.

추가 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco AMP for Networks

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/offices**에서 확인하십시오.

Printed in USA C78-733182-06 05/16