Cisco Advanced Malware Protection for Endpoints

제품 개요

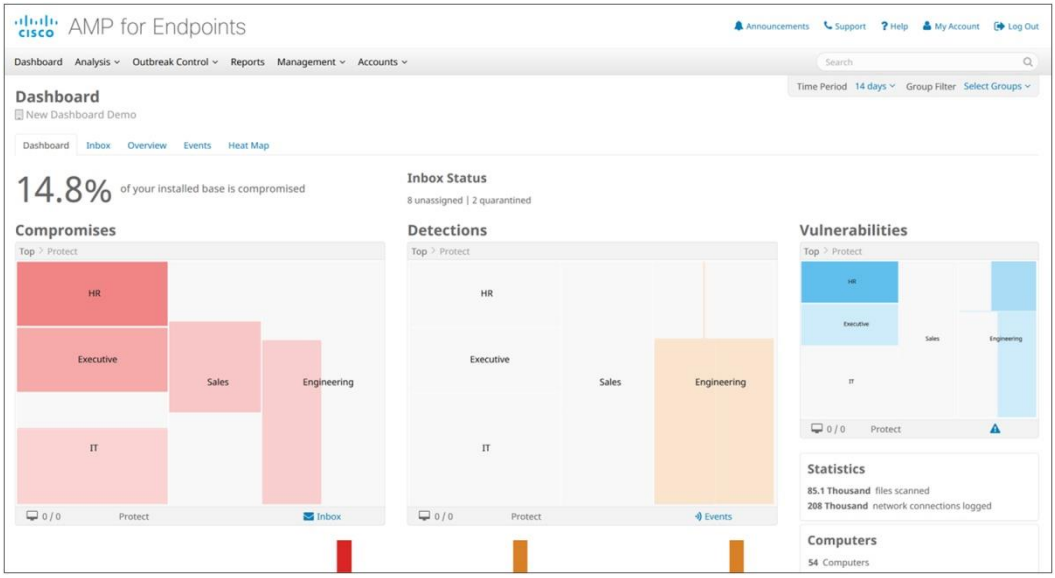
오늘날 기업들은 끊임없이 사이버 공격의 위협을 받고 있으며 보안 침해는 매일 일어나고 있습니다. Cisco AMP(Advanced Malware Protection) for Endpoints는 클라우드 관리형 엔드포인트 보안 솔루션으로서 사이버 공격을 방지할 뿐 아니라 1차 방어선을 통과하여 침투한 위협도 신속하게 탐지, 억제, 치료하기 위한 가시성, 상황 정보, 제어 기능을 제공합니다. 이 모든 기능을 비용 효율적으로, 운영 효율성 저하 없이, 실제 피해가 발생하기 전에 가동할 수 있습니다.

AMP for Endpoints는 최신 글로벌 위협 인텔리전스로 방어를 강화하고 내장된 안티바이러스 엔진으로 진입 지점에서 공격을 탐지 및 차단하며 내장된 샌드박싱 기술로 알려지지 않은 파일을 분석하고 사전 방어적 보호 기능으로 공격 경로를 차단하고 취약점을 최소화하면서 공격을 예방합니다. 그러나 악성코드가 이 방어 체계를 우회하여 유입되더라도 AMP for Endpoints가 지속적으로 모든 파일 활동을 모니터링하고 기록하면서 신속하게 악성 행동을 탐지하고 회귀적 방식으로 보안 팀에 알리며 시간의 추이에 따른 악성코드의 행동, 즉 그 출처, 경로, 기능 등에 대한 심층적인 가시성 및 세부적인 기록을 제공합니다. 그런 다음 AMP에서 자동으로 위협을 억제하고 치료할 수 있습니다. AMP는 Windows, Mac OS, Linux, Android 및 iOS를 실행하는 노트북, 워크스테이션, 서버 및 모바일 디바이스 같은 엔드포인트를 보호합니다. AMP for Endpoints 5분 요약.

장점은 다음과 같습니다.

- **예방에 국한되지 않는 보호:** Cisco AMP for Endpoints는 공격 예방에 머무르지 않습니다. 지속적으로 파일 및 트래픽을 분석합니다. 이 기능은 회귀적 보안(retrospective security)을 사용하는 데 도움이 됩니다. 과거의 시점으로 돌아가 각종 프로세스, 파일의 활동, 통신을 추적하여 감염 사실을 종합적으로 파악하는 한편 침입 경로를 규명한 다음 위협 요소를 치료할 수 있습니다. 이에 따라 기업 조직을 더 효과적이고 효율적이며 광범위하게 보호할 수 있습니다.
- **탁월한 가시성을 실현하는 모니터링:** Cisco AMP for Endpoints는 회귀 분석 이상의 기능을 제공합니다. 각종 회귀 분석 형태를 연결하고 결부시켜 일련의 활동으로 정리, 이를 실시간 분석에 제공함으로써 새로운 차원의 지능화를 실현합니다. 또한 개별 엔드포인트에서 또는 엔드포인트 환경의 전반에서 악의적 행동의 패턴을 찾아낼 수 있습니다.
- **시간의 경과에 따른 행동을 조명하는 고급 분석:** Cisco AMP for Endpoints는 대표적인 공격 및 위험 영역을 우선 순위에 따라 종합적으로 모니터링하는 고급 행동 탐지 기능을 통해 자동화를 실현합니다.
- **쫓기는 자에서 쫓는 자로 바뀐 조사 방식:** Cisco AMP for Endpoints는 조직이 침해 발생 후에 수사의 일부로 사실과 증거를 찾는 대신 악성코드 탐지 및 행동 IoC(Indication of Compromise: 보안 침해 지표)와 같은 실제 이벤트에 따라 보안 침해를 집중적으로 쫓는 활동을 수행할 수 있도록 합니다.
- **간소화된 차단:** Cisco AMP for Endpoints는 대시보드 및 경로 분석 보기를 보완하는 연쇄적인 이벤트 및 상황에 대한 가시성을 제공합니다. AMP를 사용하여 특정 애플리케이션 및 파일, 악성코드, 그리고 기타 침입 경로를 표적으로 삼을 수 있습니다. 신속하면서도 용이하게 공격 체인을 차단합니다.
- **실행 가능한 상황 기반의 대시보드:** 보고서가 이벤트 열거 및 취합에 그치지 않습니다. Cisco AMP for Endpoints의 실행 가능 대시보드에서 간단하게 관리하고 신속하게 대응할 수 있습니다. (그림 1 참조)
- **상호 운용성이 뛰어난 통합 플랫폼:** Cisco AMP for Endpoints는 Cisco AMP for Networks 솔루션 및 기타 AMP 구축과 완벽하게 통합되므로 조직 전반에 대한 가시성 및 제어가 개선됩니다.

그림 1. 실행 가능한 상황별 대시보드



효과적인 보안을 위한 가시성, 상황 정보, 제어 개선

최신 위협에 대한 차단, 사고 대응 및 치료를 과중한 예산 부담이나 운영 효율성 저하 없이 제공하여 지능형 악성코드 문제의 전체 라이프사이클을 효과적으로 처리하는 솔루션을 찾기란 쉬운 일이 아닙니다. 그 이유 중 하나는 대부분의 솔루션에 탐지 및 차단 기술과 사고 대응 및 치료 기술을 이어주는 연속성과 인텔리전스가 결여되어 있기 때문입니다

이러한 인텔리전스가 결여되면 보안 침해의 전체 범위 및 정도를 알 수 없어 사고 대응 및 치료 프로세스가 보안 침해가 발생한 후 한참 뒤에 시작됩니다. 또한 연속성이 결여되면 이러한 프로세스 중에 감염된 시스템 및 침입 경로를 놓치게 되고 재감염의 악순환이 끝없이 계속됩니다.

결과적으로 보안 전문가는 네트워크에 침입한 지능형 악성코드의 범위에 대한 가시성 없이 침해 발생 후에 억제 및 치료 작업을 힘들게 진행해야 하므로 다음과 같은 근본적인 질문을 해결하지 못합니다.

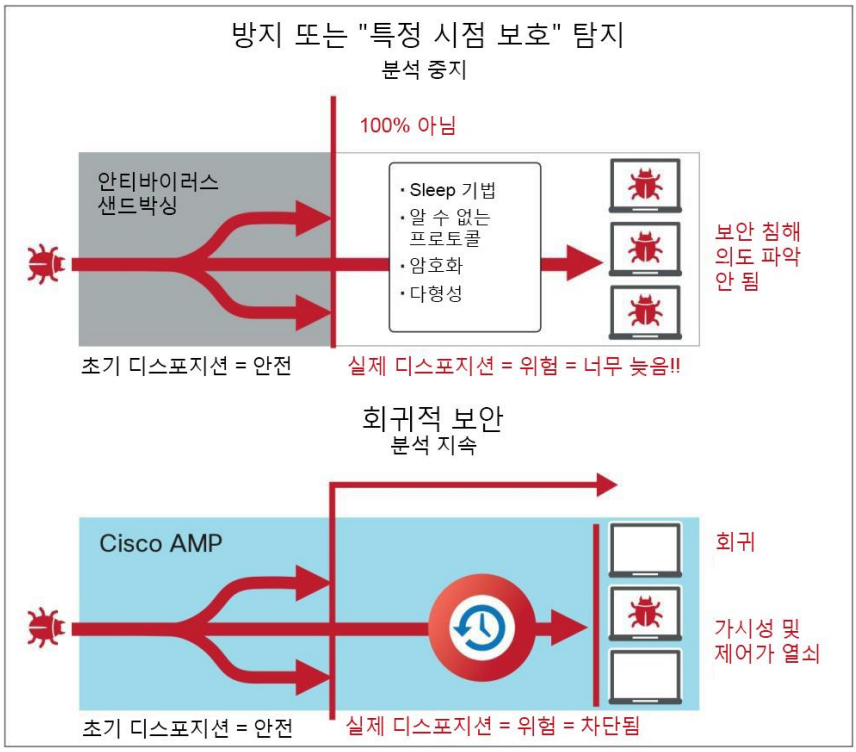
- 어떤 방법으로 어디에서 진입했습니까?
- 어떤 시스템이 감염되었습니까?
- 위협 요소가 어떤 활동을 했습니까?
- 위협을 차단하고 침입 경로를 제거할 수 있습니까?
- 공격으로부터 환경을 복구하려면 어떻게 해야 합니까?
- 어떻게 재발을 방지합니까?

Cisco AMP for Endpoints - 지능형 악성코드를 발견, 분석, 차단 및 치료

예방적 보안 툴만으로 모든 공격을 100% 방지하는 것은 불가능합니다. 탐지를 피한 하나의 위협이 전체 환경을 침해할 수 있습니다. 교묘한 해커들은 상황 인식형 표적 악성코드를 구사하며 뛰어난 리소스, 전문성, 인내심을 바탕으로 언제든 예방 차원의 방어 기능을 무력화하면서 어떤 기업도 무너뜨릴 수 있습니다. 게다가 "특정 시점" 탐지 툴과 같은 예방 툴로는 침해 발생 후의 범위 및 정도를 전혀 알 수 없으므로 보안 침해의 확산을 저지하거나 유사한 공격의 재발을 막을 수 없게 됩니다.

Cisco AMP for Endpoints는 공격을 예방할 뿐 아니라 더 나아가 악성코드 유입 시 지속적인 모니터링, 탐지, 대응 기능도 수행합니다. 빅 데이터 분석과 연계된 치밀한 탐지 기능으로 엔드포인트의 파일 및 트래픽을 지속적으로 분석하여 지능형 악성코드의 출현 여부를 파악합니다(그림 2). 또한 정교한 기계 학습 기술이 각 파일과 관련된 400개 이상의 특성을 평가하여 지능형 악성코드를 분석하고 차단합니다. 이 조합은 기존 방어 체계의 한계를 극복하는 보호를 실현합니다. 공격 당시로 시간을 돌릴 수 있는 회귀적 보안은 최초 진입 후 악성이 되는 파일을 탐지하고 알림을 제공할 수 있습니다.

그림 2. 예방(즉 "특정 시점 탐지") 툴과 지속적 분석 및 회귀적 보안 비교



전례 없는 수준의 가시성 및 지능적 악성코드 제어

오늘날의 악성코드는 전보다 훨씬 교묘합니다. 시스템을 침해한 후에 탐색을 피할 수 있을 뿐 아니라 해커가 지속적으로 조직 안에서 이동하기 위한 거점을 남겨둘 수 있는 수준으로 빠르게 발전했습니다. 슬립(sleep) 기술, 다형성(polymorphism), 암호화, 알 수 없는 프로토콜의 사용 등은 악성코드가 정체를 숨길 수 있는 수많은 방법 중의 일부일 뿐입니다. Cisco AMP for Endpoints의 지속적 분석 및 회귀적 보안 기능은 교묘하게 탐색을 피하는 악성코드를 찾아내고 지능형 위협과의 전투에서 다음과 같은 핵심 질문에 대한 해답을 제공합니다.

- **어떤 방법으로 어디에서 진입했습니까? 어떤 시스템이 감염되었습니까?**

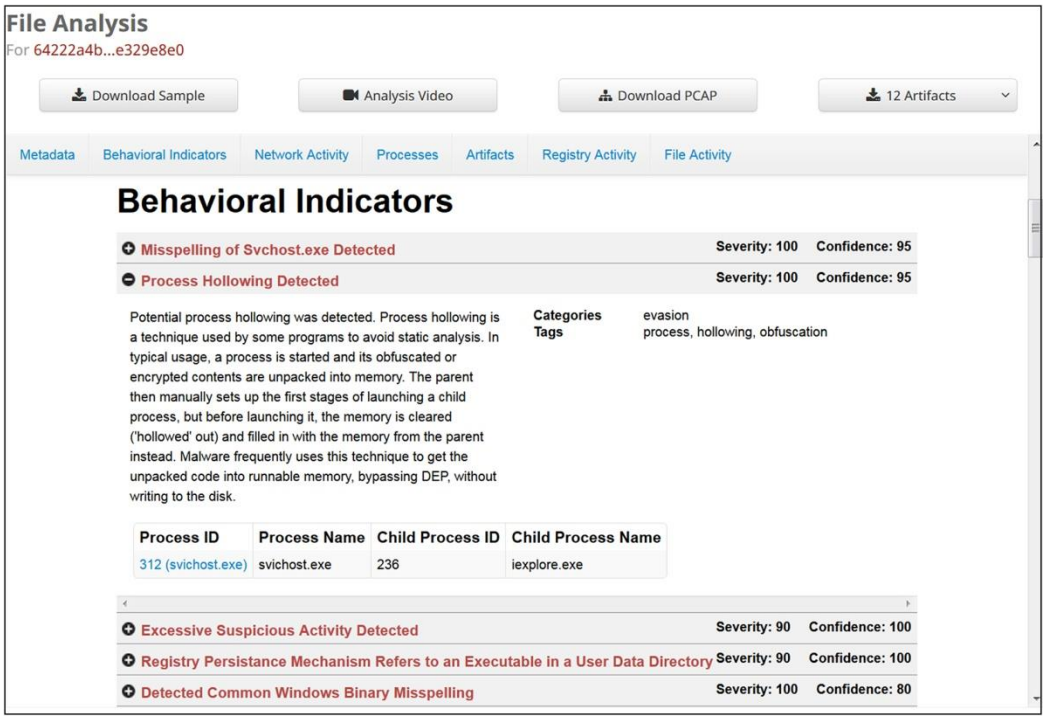
  파일 경로 분석 및 디바이스 경로 분석과 같은 강력한 혁신 기술(그림 3)은 AMP의 빅 데이터 분석 및 지속적 분석 기능을 통해 잠재적 침해와 관련된 최초 감염자 및 침입 경로를 포함하여 악성코드의 영향을 받은 시스템을 보여줍니다. 이러한 기능을 사용하면 악성코드 게이트웨이는 물론 해커가 다른 시스템으로 가는 거점을 마련하는 데 사용하는 경로를 식별할 수 있으므로 문제의 범위가 신속하게 파악됩니다.

그림 3. 디바이스 경로를 통한 심층 분석

- **위협 요소가 어떤 활동을 했습니까?**

  Talos Security Intelligence and Research Group에서 지원하고 AMP에 내장된 샌드박싱 기술(Threat Grid)이 뒷받침하는 Cisco AMP for Endpoints의 파일 분석(그림 4)은 악성코드 및 의심 파일의 행동 분석을 위한 고도로 안전한 샌드박스 환경을 제공합니다. 파일 분석 기능은 파일 행동에 대한 세부 정보를 생성하며 여기에는 행동의 심각도, 원래 파일 이름, 악성코드 실행에 대한 스크린샷 및 샘플 패킷 캡처가 포함됩니다. 이 정보를 통해 보안 침해를 억제하고 이후 공격을 차단하기 위해 필요한 사항을 더욱 명확하게 파악할 수 있습니다.

그림 4. 파일 분석



디바이스 경로 분석 기능은 엔드포인트의 파일 및 네트워크 활동을 시간순으로 추적하여 위협 활동을 더 빠르게 분석할 수 있도록 합니다. 상위 프로세스, 원격 호스트 연결 및 악성코드를 통해 다운로드되었을 수 있는 알 수 없는 파일 등 보안 침해 전후의 이벤트를 완벽하게 파악할 수 있습니다.

IoC(Indications of Compromise: 보안 침해 지표)는 감지가 어렵고 삭제되거나 해커가 이동하기 전에 즉시 수사를 시작하지 않으면 소용이 없는 경우가 많습니다. 보안 팀은 Cisco AMP for Endpoints의 검색 기능을 사용하여 단순하면서도 유연한 검색을 통해 공격 노출 범위를 신속하게 추적한 다음 엔드포인트의 데이터를 스캔하여 가져오는 과정 없이 즉시 결과를 제시할 수 있습니다.

- **위협 및 침입 경로를 차단할 수 있습니까? 재발을 방지할 수 있습니까?**

  Cisco AMP for Endpoints의 Outbreak Control(보안 침해 통제)은 보안 벤더의 업데이트를 기다릴 필요 없이 악성코드 및 악성코드 관련 활동의 확산을 효과적으로 저지할 수 있는 기능 집합(예: 콜백 통신 또는 삭제된 파일 실행)을 제공합니다. 이 기능은 마우스 클릭 몇 번으로 수사에서 제어로 바로 이동할 수 있도록 하여 위협으로 인한 피해가 확산되거나 확대될 수 있는 시간을 크게 줄이고 제어를 시행하는 데 소요되는 시간을 단축합니다.

뿐만 아니라 AMP는 전체 스캔 없이 시스템을 자동으로 치료할 수 있습니다. 이 기술은 과거에 분석된 파일과 최신 위협 인텔리전스를 지속적으로 교차 참조하고 이전에 깨끗하거나 알려지지 않은 파일로 여겨졌던 파일 중 현재 위협인 것으로 알려진 파일을 격리합니다.

PC, Mac, Linux 시스템, 서버, 모바일 디바이스 및 네트워크 보호

Cisco AMP for Endpoints는 PC, Mac, Linux 시스템, 서버, 모바일 디바이스(Android 및 iOS) 같은 모든 엔드포인트 전반에서 지능형 악성코드를 차단하며 보안 인텔리전스를 향상시킵니다. 경량의 커넥터 아키텍처는 빅 데이터 분석을 사용하여 지능형 악성코드에 대한 심층 방어 요건을 간소화합니다.

또한 Cisco AMP for Endpoints는 Cisco AMP for Networks 및 기타 AMP 구축과의 통합을 지원하므로 단일 관리 창에서 확대된 네트워크 및 엔드포인트 전체를 포괄적으로 보호할 수 있습니다. 이제, 지속적 분석, 회귀적 보안 및 다중 소스 보안 침해 지표를 사용하여 엔드포인트에서 인라인으로 이동하는 잠행 공격을 네트워크 레벨에서 식별하고 이러한 이벤트의 상관관계를 분석하여 신속하게 대응하며 가시성 및 제어를 대폭 개선할 수 있습니다.

기업 보호 확대

AMP는 기업 환경에 최적화되었습니다. Cisco AMP for Endpoints 커넥터는 개인 정보 보호를 고려하여 메타데이터를 분석에 사용합니다. 분석에서 실제 파일은 필요하지 않으며 클라우드에 전송되지도 않습니다. 개인 정보 보호 요건이 까다로운 조직을 위해 프라이빗 클라우드 옵션도 제공됩니다. 이 단일의 온프레미스 솔루션은 빅 데이터 분석, 지속적 분석 및 구내에 로컬로 저장되는 보안 인텔리전스를 사용하여 지능형 악성코드를 포괄적으로 차단합니다.

Cisco AMP for Endpoints 콘솔 인터페이스에서 Windows 시스템, Mac 시스템, Linux 시스템, Android 및 iOS 모바일 디바이스에 대한 관리, 구축, 정책 컨피그레이션 및 보고를 모두 수행할 수 있으므로 관리도 편리합니다.

성능의 경우 PC, Mac, Linux, Android 및 iOS에 구축된 Cisco AMP for Endpoints는 경량의 커넥터 아키텍처를 사용하므로 필요한 스토리지, 컴퓨팅 및 메모리가 다른 보안 솔루션보다 작아 공격 차단 속도가 빠릅니다.

포괄적인 진정한 보안 인텔리전스 확보

Cisco AMP for Endpoints는 빅 데이터 및 탁월한 보안 인텔리전스에 기반합니다. Cisco Talos Security Intelligence and Research Group 및 AMP Threat Grid 위협 인텔리전스 피드는 폭넓은 가시성, 최대규모의 설치 기반 및 여러 보안 플랫폼 전반에 걸친 실행 가능성을 제공하는 업계 최대 규모의 실시간 위협 인텔리전스 모음입니다. 이 데이터는 클라우드에서 AMP for Endpoints 클라이언트로 전달되므로 항상 최신 위협 인텔리전스를 사용할 수 있습니다.

Threat Grid 샌드박싱 기술을 AMP for Endpoints에 통합하면 파일의 구조는 물론 파일 제출 동작까지 평가하는 800개 이상의 고유한 행동 지표를 사용하여 연결된 HTTP 및 DNS 트래픽, TCP/IP 스트림, 영향을 받은 프로세스 및 레지스트리 활동 등 알 수 없는 악성코드에 대한 정보를 얻을 수 있습니다.

또한 Threat Grid는 다양한 상황에서 실행 가능한 콘텐츠를 매일 제공합니다. 8백만 개 이상의 샘플이 매월 분석되므로 수십억 개의 아티팩트가 생성됩니다. 마지막으로, Threat Grid는 고도로 정확한 콘텐츠 피드를 기존 보안

기술과 원활하게 통합되는 표준 형식으로 제공하여 각 조직의 다양한 상황에 적용되는 인텔리전스를 생성할 수 있도록 합니다.

서드파티 테스트에서 우수한 결과를 보인 Cisco AMP for Endpoints

2016년 NSS Labs Breach Detection Systems Comparative Analysis Report에 따르면 Cisco AMP for Endpoints는 NSS Labs Breach Detection Systems Report에서 3년 연속 리더 그룹에 선정되었습니다. 2016년 NSS Labs 제품 비교 테스트에서 Cisco AMP는 다음과 같이 우수성을 입증했습니다.

- 100% 보안 실효성 - 전체 테스트 대상 벤더 중 선두
- 테스트 과정에서 악성코드, 익스플로잇, 우회적 기술을 100% 탐지하여 차단한 유일한 벤더
- 테스트 대상 벤더 중 가장 짧은 탐지 시간
- 엔드포인트 또는 애플리케이션 레이턴시에 미치는 영향을 최소화하면서 뛰어난 성능 실현

또한 Cisco AMP for Endpoints는 IDC가 작성한 IDC Marketscape: Worldwide Endpoint Specialized Threat Analysis and Protection 2017 Vendor Assessment 보고서에서 선두주자로 선정되었습니다. 이 보고서에서 IDC는 AMP for Endpoints를 다음 영역에서 특히 뛰어나다고 평가했습니다.

- 가장 강력하고 포괄적인 관리 콘솔 중 하나
- 조사에 필요한 풍부한 상황별 정보 제공
- 파일 활동에 대한 지속적인 분석 및 회귀 분석, 새로 탐지한 위협과 관련이 있을 수 있는 이전 활동의 상관성을 분석하기 위한 기록 데이터를 검색할 수 있는 기능
- 엔드포인트 솔루션에 포함된 기능으로 샌드박싱 분석을 제공하는 기능
- 엔드포인트, 네트워크, 이메일 및 웹 보안 솔루션 간에 정보를 공유하고 상관관계를 분석하기 위한 우수한 AMP 통합 아키텍처의 강력한 기능

Cisco AMP for Endpoints는 Gartner의 2017년 The Evolving Effectiveness of Endpoint Protection Solutions 보고서에서도 우수한 평가를 받았습니다. 이 보고서는 AMP for Endpoints 및 기타 11가지 엔드포인트 보안 솔루션이 다음 3가지 주요 범주에서 보여준 성능을 강조해서 설명했습니다.

- 공격 표면 감소
- 사전 실행 엔드포인트 보호 기술
- 사후 실행 엔드포인트 보호 기술

표 1에서 동급 최고인 Cisco AMP for Endpoints의 기능을 살펴볼 수 있습니다. 표 2에는 소프트웨어 요건이 나열되어 있습니다.

표 1. Cisco AMP for Endpoints의 기능 및 혜택

기능	이점
지속적인 분석	파일이 엔드포인트로 들어온 후에는 파일의 성향에 관계없이 AMP for Endpoints가 지속적으로 모든 파일의 활동을 감시하고 분석하고 기록합니다. 이후 악의적인 행동이 탐지되면 AMP가 악성코드의 출처, 경로, 기능 등 시간의 경과에 따른 악성코드 행동의 내역을 알려 줍니다. 이를 통해 보안 침해의 범위를 파악하고 신속하게 대응할 수 있습니다. 지속적 분석 4분 요약

기능	이점
회귀적 보안	회귀적 보안이란 과거의 시점으로 돌아가 각종 프로세스, 파일의 활동, 통신을 추적하여 감염 사실을 종합적으로 파악하고 침입 경로를 규명한 다음 위협 요소를 제거하는 것을 의미합니다. 보안 침해 지표가 나타날 때, 이를테면 이벤트 트리거, 파일 속성의 변화, 보안 침해 지표 트리거가 발생할 때 회귀적 보안이 필요하게 됩니다. 데모 보기
대시보드	호스트, 디바이스, 애플리케이션, 사용자, 파일 및 위치 정보와 APT(Advanced Persistent Threat: 지능형 지속 위협), 위협 감염 경로 및 기타 취약점을 보여주는 단일 창에서 환경에 대한 가시성을 확보하고 포괄적인 상황별 보기를 제공하여 정보에 입각한 보안 의사 결정을 내릴 수 있도록 합니다.
종합적인 글로벌 위협 인텔리전스	Cisco Talos Security Intelligence and Research Group 및 Threat Grid 위협 인텔리전스 피드는 폭넓은 가시성, 최대규모의 설치 기반 및 여러 보안 플랫폼 전반에 걸친 실행 가능성을 제공하는 업계 최대 규모의 실시간 위협 인텔리전스 모음입니다.
보안 침해 지표	파일, 텔레메트리, 침입 이벤트의 상관 관계를 분석하고 잠재적인 활성 보안 침해로 우선 순위를 지정하여 보안 팀이 신속하게 악성코드 사건을 파악하고 합동 공격과의 연관관계를 밝힐 수 있도록 지원합니다.
파일 평판	고급 분석 및 종합 인텔리전스를 수집하여 파일이 정상 파일인지 또는 악성 파일인지 여부를 판단함으로써 보다 정확한 탐지를 지원합니다.
안티바이러스 엔진	오프라인 및 시스템 기반 탐지(예: 루트킷 스캐닝)를 수행하여 로컬 IOC 스캐닝, 디바이스 및 네트워크 플로우 모니터링 같은 Cisco의 고급 엔드포인트 보호 기능을 보완합니다. 자체 안티바이러스 및 고급 엔드포인트 보호 기능을 하나의 에이전트로 통합하려는 고객은 이 엔진을 활성화하여 사용할 수 있습니다.
파일 분석 및 샌드박싱	고도의 보안성을 갖춘 환경에서 악성코드 행동을 실행, 분석 및 테스트하는 방법으로 이전에 알려지지 않았던 제로데이 위협을 검색할 수 있습니다. Threat Grid의 샌드박싱 기술을 AMP for Endpoints 솔루션 내에 통합하여 대규모 행동 지표를 기준으로 검사하는 더욱 동적인 분석을 제공할 수 있습니다. 데모 보기
회귀적 탐지	장기간의 분석 후에 파일 성향이 변경되면 알림이 전송되므로 관리자는 초기 방어를 우회하는 악성코드를 인지하고 가시화할 수 있습니다.
파일 경로 분석	가시성을 확보하는 한편 악성코드 침입 범위를 파악하는 시간을 줄이기 위해 전체 환경에서 오랜 시간 동안 파일 전파 경로를 지속적으로 추적합니다.
디바이스 경로 분석	보안 침해 전후 이벤트의 감염 경로와 내역을 신속하게 파악하기 위해 디바이스 및 시스템 레벨에서 여러 활동과 통신을 지속적으로 추적합니다. 데모 보기
엘라스틱 검색	파일, 텔레메트리, 종합 보안 인텔리전스 데이터의 전 범위를 대상으로 간단하면서도 무제한적인 검색을 수행하여 위험 노출의 범위와 상황을 보안 침해 지표 또는 악성 애플리케이션과 연계해 빠르게 파악할 수 있습니다.
엔드포인트 검색	간단한 인터페이스에서 빠르고 편리하게 모든 엔드포인트를 대상으로 검색을 수행하여 악성코드 에코시스템의 일부로 남겨진 아티팩트가 있는지 확인함으로써 클라우드에 저장된 데이터뿐 아니라 엔드포인트 자체로 검색 기능을 확장합니다.
발생률이 낮은 실행 파일	조직 전반에서 실행된 모든 파일을 발생률(prevalence) 순서에 따라 표시하는 방법으로 소수의 사용자가 경험했고 아직 탐지되지 않은 위협을 효과적으로 드러냅니다. 소수의 사용자만 실행했던 파일은 현재의 광범위한 네트워크에서 원하지 않는 악성 파일(예: 특정 목표 대상 지능형 지속 위협)이거나 미심쩍은 애플리케이션일 수 있습니다.
엔드포인트 보안 침해 지표	사용자는 고유한 보안 침해 지표를 제출하여 표적 공격을 포착할 수 있습니다. 보안 팀은 엔드포인트 보안 침해 지표를 통해 환경에서 특정 애플리케이션을 공격하는 잘 알려지지 않은 지능형 위협을 더욱 심층적으로 조사할 수 있습니다.
취약점	취약한 소프트웨어를 식별하고 공격 경로를 차단합니다. 이 기능은 취약한 소프트웨어가 포함된 호스트 목록, 각 호스트에 있는 취약한 소프트웨어 목록 및 침해 가능성이 가장 높은 호스트를 보여줍니다. AMP는 Cisco의 위협 인텔리전스 및 보안 분석을 바탕으로 악성코드의 표적이 되고 있는 취약한 소프트웨어를 식별하고 가능한 익스플로잇을 보여주며 패치가 필요한 호스트의 우선 순위 목록을 제공합니다.
명령줄 가시성	이 기능은 실행 파일을 시작하는 데 어떤 명령줄 인수가 사용되는지 모니터링합니다. 명령줄 인수를 파악하여 Windows 유틸리티와 같은 합법적인 애플리케이션이 악의적 목적에 사용되고 있는지 여부를 판단합니다. 예를 들어 vssadmin이 섀도 복사본 삭제 또는 안전 부팅 비활성화에 사용되고 있는지 알아보고 PowerShell 기반 익스플로잇을 확인하고 권한 승격, ACL(Access Control List) 수정, 시스템 열거 시도를 조사합니다.

기능	이점
API(Application Programming Interface)	양방향(읽기 및 쓰기) API가 AMP for Endpoints에서 지원되므로 사용자는 더 수월하게 서드파티 보안 툴 및 SIEM과 통합함으로써 관리 콘솔에 로그인하지 않고도 AMP for Endpoints 어카운트의 데이터 및 이벤트에 액세스할 수 있습니다.
아웃브레이크 제어	의심스러운 파일 또는 아웃브레이크를 제어하고 콘텐츠 업데이트를 기다릴 필요 없이 빠르고 완벽하게 감염을 제어하고 치료합니다. 아웃브레이크 제어 기능에는 모든 시스템 또는 선택한 시스템에서 특정 파일을 빠르게 차단하는 간편한 맞춤형 탐지 기능, 다형성 악성코드군을 차단하는 고급 맞춤형 시그니처, 애플리케이션 정책을 적용하거나 악성코드 게이트웨이로 이용되는 손상된 애플리케이션을 봉쇄하여 재감염의 악순환을 멈추는 애플리케이션 차단 목록, 보안 애플리케이션, 맞춤형으로 설계된 애플리케이션 또는 미션 크리티컬 애플리케이션이 어떤 상황에서도 지속적으로 실행될 수 있도록 보장하는 맞춤형 화이트리스트 및 특히 기업 네트워크 외부의 원격 엔드포인트에서 소스 측의 악성코드 콜백 통신을 중지하는 디바이스 흐름 상관관계가 포함됩니다. 데모 보기
Threat Grid와의 통합	Threat Grid의 샌드박싱 기술 및 지능형 악성코드 분석 기능을 AMP for Endpoints와 통합하면 파일 동작, 이해하기 쉬운 위협 점수 및 수십억 개의 악성코드 아티팩트를 분석하는 800개 이상의 고유한 행동 지표를 원하는 대로 사용하여 광범위한 규모의 글로벌 위협에 대응할 수 있습니다. 서드파티의 샌드박스를 구축하거나 어떤 유형의 외부 통합에 대해서도 고민할 필요 없습니다.
CTA(Cognitive Threat Analytics)와의 통합	AMP for Endpoints가 호환되는 웹 프록시(예: Cisco WSA 또는 Blue Coat ProxySG와 같은 서드파티 웹 프록시)와 함께 구축되면 에이전트 없이 탐지할 수 있습니다. 환경 전반에서 평균적으로 30% 더 많은 감염을 탐지하고 파일 없이 메모리에서만 활동하는 악성코드 및 웹 브라우저에서만 실행되는 감염을 발견하며 악성코드가 OS 레벨에 침투하기 전에 차단하고 AMP for Endpoints 커넥터가 설치되지 않은 디바이스에 대한 가시성을 확보합니다. AMP for Endpoints 관리 콘솔에서 CTA 탐지 이벤트를 확인합니다. 개요 참조
AMP Private Cloud Virtual Appliance	AMP for Endpoints를 온프레미스 에어 갭(air-gapped) 솔루션으로 구축할 수 있습니다. 이는 특히 퍼블릭 클라우드 사용을 제한하며 높은 개인 정보 보호 수준이 필요한 조직을 위한 설계입니다.
AnyConnect v4.1에서 실행	Cisco AnyConnect v4.1 원격 액세스 VPN 클라이언트를 설치한 경우 AMP for Endpoints 커넥터를 해당 원격 엔드포인트에서 실행하도록 선택할 수 있습니다. 이 기능을 사용하면 VPN 지원 엔드포인트로 엔드포인트 위협 차단을 확대하고 원격 호스트에서 발생 가능한 잠재적 공격을 최소화할 수 있습니다. 또한 원격 엔드포인트에 대한 더 많은 정보를 확보하여 공격 중 또는 공격 후의 치료 프로세스를 가속화할 수 있습니다.

표 2. 소프트웨어 요구 사항

Cisco AMP for Endpoints	• Microsoft Windows XP 서비스 팩 3 이상 • Microsoft Windows Vista 서비스 팩 2 이상 • Microsoft Windows 7 • Microsoft Windows 8 및 8.1 • Microsoft Windows 10 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Mac OS X 10.7 이상 • Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2 및 7.3 • Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 및 7.3
Android 모바일 디바이스에서의 Cisco AMP for Endpoints	• Android 버전 2.1 이상
Apple iOS에서의 Cisco AMP for Endpoints	MDM이 감독하는 iOS 버전 11

플랫폼 지원 및 호환성

Cisco AMP for Endpoints에는 Cisco AMP for Endpoints 라이선스 및 서브스크립션(1년, 3년 및 5년 옵션)과 경량의 커넥터가 포함됩니다. Cisco AMP for Endpoints는 Cisco AMP for Networks 및 기타 AMP 구축과 호환됩니다. Cisco AMP for Endpoints는 원격 엔드포인트의 Cisco AnyConnect v4.1에서도 실행할 수 있습니다.

워런티 정보

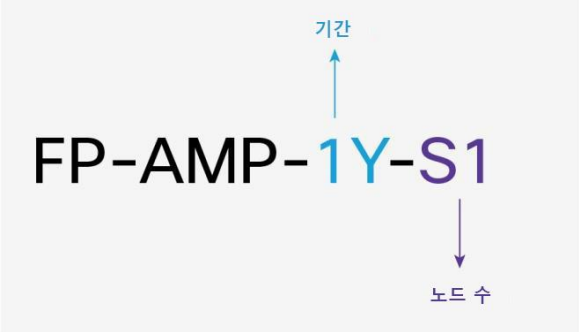
워런티 정보는 Cisco.com의 제품 워런티 페이지에서 확인하십시오.

주문 정보

Cisco AMP for Endpoints는 해당 라이선스 및 서브스크립션 부품 번호를 사용하여 주문할 수 있습니다.

1. 먼저 AMP for Endpoints 라이선스 부품 번호(FP-AMP-LIC=)를 검색합니다.
2. 구매하려는 AMP for Endpoints 커넥터의 수와 일치하는 수량을 입력합니다.
3. 수를 입력하면 올바른 서브스크립션 부품 번호가 자동 선택됩니다. 1년 서브스크립션이 기본값입니다.
4. AMP for Endpoints 어카운트는 1년, 3년, 5년 기간 기반의 서브스크립션입니다. 3년 또는 5년 기간의 경우 FP-AMP-LIC= 부품 번호의 서비스/서브스크립션 기간을 수정해야 합니다.
5. 그림 5에는 AMP for Endpoints 부품 번호의 체계가 나와 있습니다.

그림 5. AMP for Endpoints 서브스크립션 부품 번호 예



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

Cisco Advanced Malware Protection for Endpoints 서브스크립션 SKU

Cisco Advanced Malware Protection for Endpoints 서브스크립션 SKU		
Part Number(부품 번호)	**구독 SKU**	**설명**
FP-AMP-LIC=	FP-AMP-1Y-S1	Cisco Advanced Malware Protection 1년, 노드 50~99개
FP-AMP-LIC=	FP-AMP-1Y-S2	Cisco Advanced Malware Protection 1년, 노드 100~499개
FP-AMP-LIC=	FP-AMP-1Y-S3	Cisco Advanced Malware Protection 1년, 노드 500~999개
FP-AMP-LIC=	FP-AMP-1Y-S4	Cisco Advanced Malware Protection 1년, 노드 1,000~4,999개
FP-AMP-LIC=	FP-AMP-1Y-S5	Cisco Advanced Malware Protection 1년, 노드 5,000~9,999개
FP-AMP-LIC=	FP-AMP-1Y-S6	Cisco Advanced Malware Protection 1년, 10,000-12,499개 노드
FP-AMP-LIC=	FP-AMP-1Y-S7	Cisco Advanced Malware Protection 1년, 12500-14999개 노드
FP-AMP-LIC=	FP-AMP-1Y-S8	Cisco Advanced Malware Protection 1년, 15,000-17,499개 노드

Cisco Advanced Malware Protection for Endpoints 서브스크립션 SKU		
Part Number(부품 번호)	**구독 SKU**	**설명**
FP-AMP-LIC=	FP-AMP-1Y-S9	Cisco Advanced Malware Protection 1년, 17,500-19,999개 노드
FP-AMP-LIC=	FP-AMP-1Y-S10	Cisco Advanced Malware Protection 1년, 20,000-22,499개 노드
FP-AMP-LIC=	FP-AMP-1Y-S11	Cisco Advanced Malware Protection 1년, 22,500-24,999개 노드
FP-AMP-LIC=	FP-AMP-1Y-S12	Cisco Advanced Malware Protection 1년, 25,000개 이상 노드
FP-AMP-LIC=	FP-AMP-3Y-S1	Cisco Advanced Malware Protection 3년, 노드 50~99개
FP-AMP-LIC=	FP-AMP-3Y-S2	Cisco Advanced Malware Protection 3년, 노드 100~499개
FP-AMP-LIC=	FP-AMP-3Y-S3	Cisco Advanced Malware Protection 3년, 노드 500~999개
FP-AMP-LIC=	FP-AMP-3Y-S4	Cisco Advanced Malware Protection 3년, 노드 1,000~4,999개
FP-AMP-LIC=	FP-AMP-3Y-S5	Cisco Advanced Malware Protection 3년, 노드 5,000~9,999개
FP-AMP-LIC=	FP-AMP-3Y-S6	Cisco Advanced Malware Protection 3년, 10,000-12,499개 노드
FP-AMP-LIC=	FP-AMP-3Y-S7	Cisco Advanced Malware Protection 3년, 12,500-14,999개 노드
FP-AMP-LIC=	FP-AMP-3Y-S8	Cisco Advanced Malware Protection 3년, 15,000-17,499개 노드
FP-AMP-LIC=	FP-AMP-3Y-S9	Cisco Advanced Malware Protection 3년, 노드 17500~19,999개
FP-AMP-LIC=	FP-AMP-3Y-S10	Cisco Advanced Malware Protection 3년, 20,000-22,499개 노드
FP-AMP-LIC=	FP-AMP-3Y-S11	Cisco Advanced Malware Protection 3년, 노드 22500~24,999개
FP-AMP-LIC=	FP-AMP-3Y-S12	Cisco Advanced Malware Protection 3년, 노드 25,000개 이상

Cisco Capital

시스코 금융 지원 솔루션

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. Cisco Capital은 여러분이 CapEx를 절감하고, 성장을 가속화하며, 투자비용과 ROI를 최적화하도록 지원합니다. 하드웨어, 소프트웨어, 서비스, 보완적인 써드파티 장비 구입 시 Cisco Capital의 금융 지원 솔루션을 유연하게 활용할 수 있습니다. 또한, 정해진 일자에 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세히 보기.

추가 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco AMP for Endpoints