Cisco Advanced Malware Protection for Endpoints

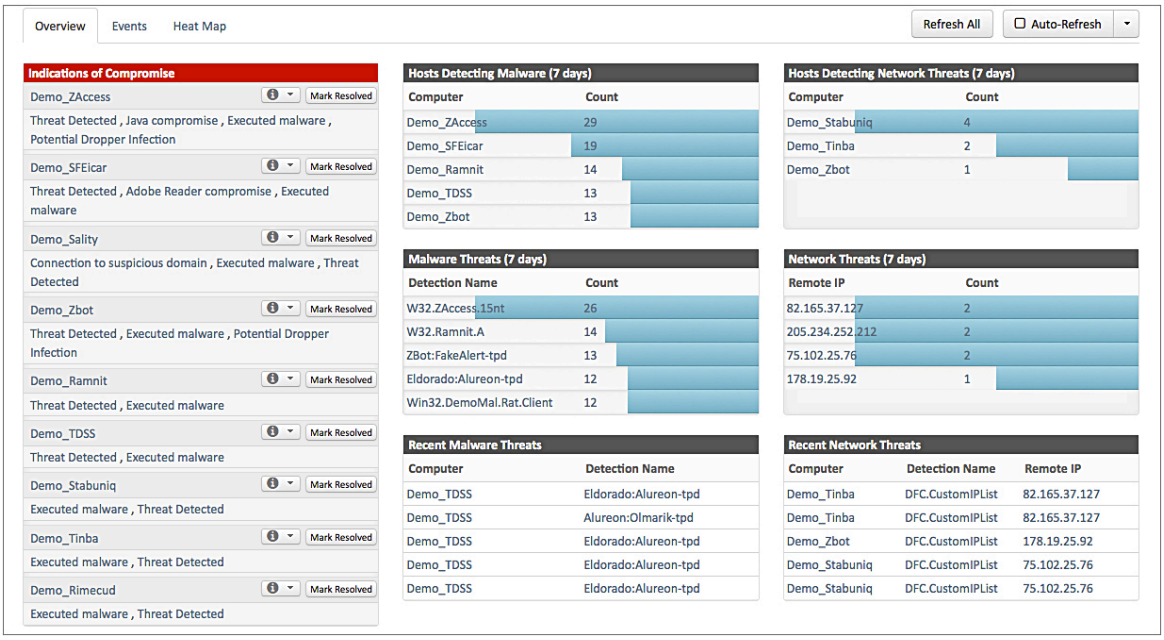
제품 개요

오늘날의 정교한 악성코드에 맞서려면 공격 전/중/후 전 범위에서 엔드포인트를 보호해야 합니다. Cisco® AMP(Advanced Malware Protection) for Endpoints는 특정 시점의 탐지에 머무르지 않고 다른 보안 레이어에서 놓친 지능형 위협을 차단하는 데 필요한 수준의 가시성과 제어를 제공합니다. 공격 전/중/후의 전 범위에서 조직을 포괄적으로 보호할 수 있습니다. Cisco AMP for Endpoints는 지능형 악성코드를 분석하고 차단하는 엔터프라이즈급 인텔리전스 솔루션으로서 빅데이터, 지속적인 분석, 고급 분석 기반의 원격 분석 모델을 통해 Windows PC, Windows POS 운영 체제, Mac, 모바일 디바이스, 가상 시스템 등 모든 엔드포인트에서 지능형 악성코드 공격을 탐지, 추적, 분석, 제어, 차단합니다.

혜택은 다음과 같습니다.

- **특정 시점에 국한되지 않는 보호:** Cisco AMP for Endpoints는 특정 시점 탐지에 머무르지 않고 지속적으로 파일과 트래픽을 분석합니다. 이 기능으로 회귀적 보안을 실현할 수 있습니다. 과거의 시점으로 돌아가 프로세스, 파일 활동, 통신을 추적하여 감염의 전 범위를 파악하고 근본 원인을 규명하여 문제를 해결할 수 있습니다. 그 결과, 더 효과적이고 효율적이며 퍼베이시브하게 조직을 보호할 수 있습니다.
- **탁월한 가시성을 실현하는 모니터링:** Cisco AMP for Endpoints는 회귀 분석 이상의 기능을 제공합니다. 각종 회귀 분석 형태를 실시간 분석에 사용 가능한 활동 기록에 연결하고 연관성을 찾아봄으로써 새로운 차원의 인텔리전스를 실현합니다. 또한 개별 엔드포인트에서 또는 엔드포인트 환경 전반에서 악성 행동의 패턴을 찾아냅니다.
- **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 입장에서 쫓는 입장으로 전환하는 조사 기능:** Cisco AMP for Endpoints는 조사 과정의 일부로 사실과 단서를 찾는 것에서 악성코드 탐지, 행동 IoC(indications of compromise) 등 실제 사건에 근거하여 보안 침해를 집중적으로 찾아내는 쪽으로 접근 방향을 전환합니다.
- **간소화된 차단:** Cisco AMP for Endpoints는 대시보드 및 궤적 뷰를 보완하는 연쇄적인 이벤트 및 컨텍스트에 대한 가시성을 제공합니다. AMP는 특정 애플리케이션, 파일, 악성코드, 기타 근본 원인을 대상으로 지정할 수 있습니다. 신속하면서도 용이하게 공격 체인을 차단합니다.
- **실행 가능한 컨텍스트 기반의 대시보드:** 보고서가 이벤트 열거 및 취합에 그치지 않습니다. Cisco AMP for Endpoints 보고 기능은 리스크의 관점에서 비즈니스 연관성 및 영향을 조명하는 실행 가능한 대시보드 및 트렌드를 포함합니다(그림 1 참조).
- **시너지 효과를 발휘하는 통합 플랫폼:** Cisco AMP for Endpoints는 Cisco AMP for Networks 솔루션에 완벽하게 통합하여 조직 전반에 가시성과 제어를 한층 더 확대할 수 있습니다.

그림 1. 실행 가능한 컨텍스트 기반 대시보드



효과적 보안을 위한 가시성 및 제어의 확대

지능형 악성코드 문제를 라이프사이클 전 범위에서 효과적으로 해결하는, 즉 과중한 예산 부담 없이 운영 효율성을 저해하지 않으면서 최신 위협에 대한 차단, 사고 대응책, 치료법을 제공하는 솔루션을 찾기란 쉽지 않습니다. 탐지 및 차단 기술과 사고 대응 및 치료 기술 간의 연속성 및 인텔리전스의 부재가 그 원인 중 하나입니다.

이러한 인텔리전스의 부재로 인해 공격의 전 범위와 강도를 파악하지 못하기 때문에 공격이 발생하고 한참 후에서야 사고 대응 및 치료 조치를 시작하는 경우를 자주 볼 수 있습니다. 또한 연속성의 부재로 이러한 조치 과정에서 감염된 시스템 및 근본 원인을 놓치게 되어 재감염이 반복되는 결과로 이어집니다.

그로 인해 보안 전문가가 네트워크의 지능형 악성코드의 범위를 제대로 파악하지 못하고, 공격 후에도 억제 및 치료에 어려움을 겪으며, 다음과 같은 근본적인 문제에 대한 해답도 얻지 못하는 결과가 발생하는 것입니다.

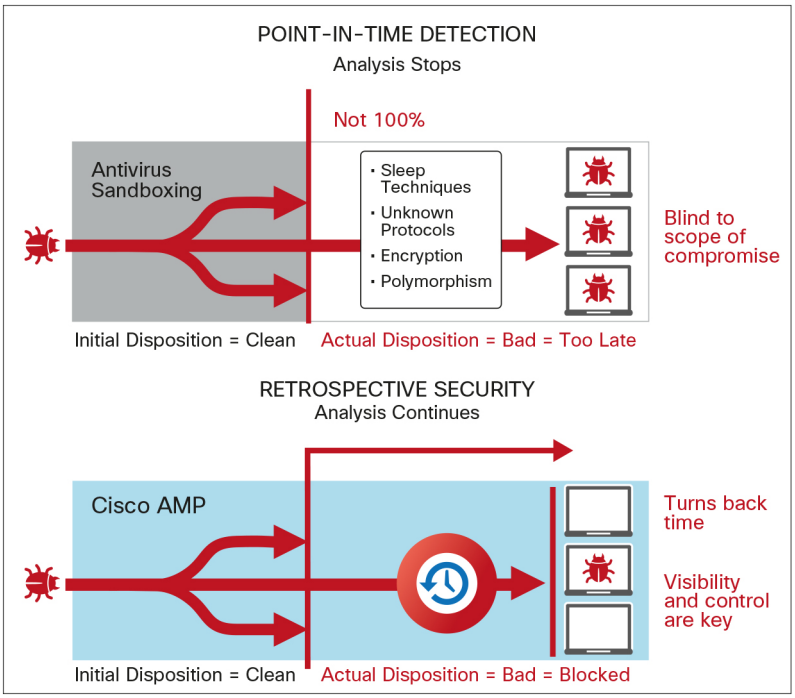
- 어떤 방법과 진입 지점이 사용되었습니까?
- 어떤 시스템이 감염되었습니까?
- 위협 요소가 무엇을 했습니까?
- 위협을 차단하고 근본 원인을 제거할 수 있습니까?
- 공격으로부터 어떻게 복구합니까?
- 공격의 재발을 어떻게 방지합니까?

지능형 악성코드를 검색, 분석, 차단, 치료하는 Cisco AMP for Endpoints

특정 시점 방어 기술만으로는 결코 100%의 실효성을 거둘 수 없습니다. 감시망을 빠져나가는 단 하나의 위협이 전체 환경을 침해하는 것입니다. 컨텍스트를 감지하는 타겟 악성코드의 사용으로 지능적인 공격자들은 리소스, 전문성, 인내심을 갖추고 있어 언제든지 특정 시점 방어 체계를 무력화하고 어떤 조직도 공격할 수 있습니다. 또한 특정 시점 탐지 기술은 공격 후에 그 범위와 정도를 파악하지 못하므로 공격의 확산을 막거나 유사 공격의 재발을 방지하는 데 도움이 되지 않습니다.

Cisco AMP for Endpoints는 특정 시점의 탐지에 그치지 않고 빅데이터 분석을 접목시킨 복합 탐지 기능을 통해 엔드포인트에서 지속적으로 파일과 트래픽을 분석함으로써 지능형 악성코드의 유무를 확인합니다(그림 2). 정교한 기계 학습 기술을 통해 각 파일과 관련된 400여 가지의 특성을 평가하여 지능형 악성코드를 분석하고 차단합니다. 이러한 기술의 조합으로 기존의 특정 시점 탐지 기술보다 차원 높은 보호를 수행합니다. 과거의 공격 시점으로 돌아가는 회귀적 보안 기술로 최초 진입 포인트 이후에 감염된 파일을 탐지하고 그에 대해 경고할 수 있습니다.

그림 2. 특정 시점 탐지와 지속적 분석 및 회귀적 보안 비교



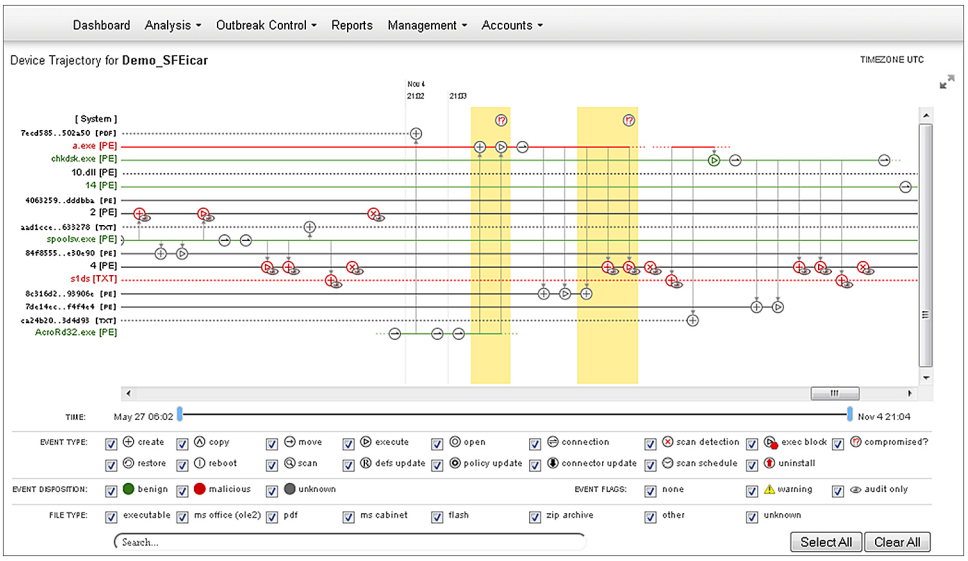
예전보다 많은 지능형 악성코드 제어

오늘날의 악성코드는 과거의 어느 때보다도 정교합니다. 빠른 속도로 진화하기 때문에 시스템 침입 후 감시망을 피해다니며 지속적인 공격의 확산을 돕는 교두보 역할을 할 수 있습니다. 슬립 기법, 다형성, 암호화, 미확인 프로토콜의 사용 등은 악성코드가 모습을 숨길수 있는 수많은 방법중 일부 몇 가지에 지나지 않습니다. Cisco AMP for Endpoints의 지속적 분석 및 회귀적 보안 기능으로 놓치기 쉬운 악성코드를 찾아내 지능형 위협과의 전쟁에서 다음과 같은 핵심적인 질문에 대한 답을 얻을 수 있게 합니다.

- **어떤 방법과 진입 지점이 사용되었습니까? 어떤 시스템이 감염되었습니까?**

  파일 궤적 및 디바이스 궤적과 같은 뛰어난 혁신적인 기술(그림 3)에서 AMP의 빅데이터 분석 및 지속적인 분석 기능을 활용하여 악성코드에 감염된 시스템을 표시합니다. 여기에는 잠재 공격의 최초 감염자 및 근본 원인에 대한 정보도 포함됩니다. 이러한 기능으로 공격자가 다른 시스템에 침투하는 데 사용 중인 악성코드 게이트웨이 및 경로를 밝혀 문제의 범위를 신속하게 파악할 수 있습니다.

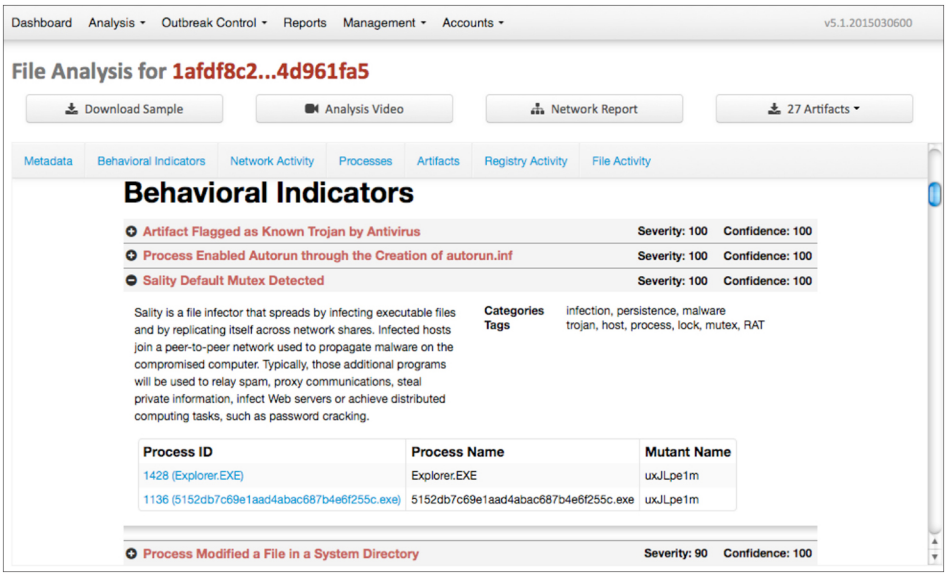
그림 3. 디바이스 궤적으로 심층 분석



- **위협 요소가 무엇을 했습니까?**

  Talos Security Intelligence and Research Group의 후원을 받고 AMP Threat Grid의 샌드박싱 기술을 이용한 Cisco AMP for Endpoints의 파일 분석(그림 4)에서는 안전하고 보안성이 높은 샌드박스 환경을 마련하여 악성코드 및 의심스러운 파일의 동작을 분석할 수 있도록 합니다. 파일 분석에서 동작의 심각성과 같은 파일 동작에 대한 세부사항, 원본 파일 이름, 실행 중인 악성코드의 스크린샷, 샘플 패킷 캡처 등을 생성합니다. 이러한 정보를 토대로 공격을 억제하고 향후 공격을 차단하는 데 필요한 조건을 정확하게 파악할 수 있습니다.

그림 4. 파일 분석



디바이스 궤적은 엔드포인트에서 일어난 파일 및 네트워크 활동을 시간순으로 추적하여 컴퓨터에 대한 위협 활동을 신속하게 분석하도록 지원합니다. 공격의 전후에 발생한 이벤트에 대한 완전한 가시성을 확보할 수 있습니다. 여기에는 상위 프로세스, 원격 호스트와의 연결, 악성코드에 의해 다운로드되었을 미확인 파일도 포함됩니다.

IoC(Indications of Compromise)는 대개 감지하기가 어려우며, 삭제되기 전에 즉각적인 조사를 하지 않으면 공격으로 진행됩니다. Cisco AMP for Endpoints의 Elastic Search를 사용하여 보안팀은 엔드포인트를 스캔하여 데이터를 가져올 필요 없이 간단하면서도 유연한 검색으로 즉시 결과를 얻어 신속하게 공격에 노출된 범위를 알아낼 수 있습니다.

- **위협을 차단하고 그 근본 원인을 제거할 수 있습니까? 재발을 방지할 수 있습니까?**

  Cisco AMP for Endpoints Outbreak Control은 보안 벤더의 업데이트를 기다릴 필요 없이 콜백 통신, 중단된 파일 실행 등의 기능으로 악성코드 및 악성코드 관련 활동의 확산을 효과적으로 막습니다. 마우스 클릭 몇 번으로 조사 단계에서 제어 단계로 전환할 수 있어 보안 위협이 확산되어 더 큰 피해를 일으키지 못하도록 신속하게 조치하고 정상화할 수 있습니다.

  또한 AMP는 전체 스캔 없이 자동으로 시스템을 치료할 수 있습니다. 이 기술은 과거에 분석된 파일을 최신 위협 인텔리전스와 지속적으로 상호 참조하고, 이전에 정상 또는 미확인으로 분류되었으나 이제 위협으로 확인된 파일을 격리합니다.

엔드포인트, 모바일 디바이스, 가상 시스템, 네트워크 보호

Cisco AMP for Endpoints는 PC, Mac, 모바일 디바이스, 가상 시스템의 모든 엔드포인트에서 지능형 악성코드로부터 보호하고 보안 인텔리전스를 강화합니다. 가벼운 커넥터 아키텍처에서는 빅데이터 분석을 활용하고, 이는 지능형 악성코드를 해결을 위해 심층 방어 요구 사항을 간소화합니다. 따라서 엔드포인트의 성능 및 리소스 면에서 큰 제약이 될 수 있는 기존의 안티바이러스 보안 레이어가 불필요합니다.

또한 Cisco AMP for Endpoints는 Cisco AMP for Networks와의 통합으로 확장된 네트워크 및 엔드포인트 전 범위에 걸친 포괄적인 보호를 단일 창 방식으로 제공합니다. 이제 지속적인 분석, 회귀적 보안, 멀티소스 IoC를 통해 엔드포인트부터 네트워크 레벨의 인라인까지 횡행하는 은밀한 공격을 식별하고, 이러한 이벤트의 상관성 분석으로 더 신속하게 대응하며, 더 우수한 가시성과 제어를 실현할 수 있습니다.

엔터프라이즈 환경을 위한 보호 확장

AMP는 엔터프라이즈 환경에 최적화되었습니다. 개인 정보 보호에 관해서는 모든 Cisco AMP for Endpoints 커넥터가 분석을 위해 메타 데이터를 사용합니다. 실제 파일은 필요하지 않으며 분석을 위해 클라우드에 보내지 않습니다. 개인 정보 보호 요구 사항이 까다로운 기업을 위해 프라이빗 클라우드 옵션도 제공합니다. 이 단일 온프레미스 솔루션은 빅데이터 분석과 지속적인 분석, 현지 온프레미스에 저장되어 있는 보안 인텔리전스를 활용하여 광범위한 지능형 악성코드 차단을 제공합니다.

관리의 편의성에 대해 말하자면, Cisco AMP for Endpoints 콘솔 인터페이스가 Windows 시스템, Mac 시스템, 모바일 디바이스, 가상 시스템에 대한 종합적인 관리, 구축, 정책 컨피그레이션, 보고를 수행합니다.

성능에 관해서는 PC, Mac, 모바일 디바이스, 가상 환경에 구축된 Cisco AMP for Endpoints는 가벼운 커넥터 아키텍처를 사용하므로 다른 보안 솔루션보다 필요한 스토리지, 컴퓨팅 리소스, 메모리가 다른 보안 솔루션보다 적어 공격으로부터 더욱 신속하게 보호할 수 있습니다.

진정한 통합 보안 인텔리전스

Cisco AMP for Endpoints는 빅데이터 및 최고의 보안 인텔리전스를 기반으로 합니다. Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, AMP Threat Grid 위협 인텔리전스 피드는 가장 폭넓은 가시성, 가장 대규모의 풋프린트, 그리고 여러 보안 플랫폼에 실행할 수 있는 기능과 더불어 업계 최대 규모의 실시간 위협 인텔리전스를 보유하고 있습니다. 그리고 이 데이터는 클라우드에서 AMP 클라이언트에 푸시되므로 항상 최신 버전의 위협 인텔리전스를 사용할 수 있습니다.

AMP Threat Grid 기술을 AMP for Endpoints에 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. AMP Threat Grid는 컨텍스트가 풍부하며 실행 가능한 콘텐츠를 매일 사용자에게 전달합니다. 매월 8백만 개 이상의 샘플을 분석하여 수십억 개의 아티팩트를 생성합니다. 마지막으로, 최고의 정확도를 자랑하는 AMP Threat Grid의 콘텐츠 피드는 표준 형식으로 제공되어 기존 보안 기술에 원활하게 통합되며 해당 조직에 부합하는 풍부한 컨텍스트의 인텔리전스를 생성할 수 있습니다.

서드파티 테스트에서 최고로 인정받은 Cisco AMP

2014 NSS Labs Breach Detection Systems Comparative Analysis Report에 따르면 Cisco는 Labs' Breach Detection Systems Security Value Maps에서 선두주자로 선정되었습니다. 이 제품 비교 테스트에서 AMP는 다음과 같은 성적을 거두었습니다.

- 전반적인 탐지율 선두
- 최단 탐지 소요 시간
- 보호하는 Mbps당 가장 낮은 TCO
- Security Value Map에서 탑으로 등극

NSS Labs의 결과는 Cisco AMP for Endpoints가 비용 대비 최고의 보안 실효성 및 가치를 제공함을 입증합니다.

표 1은 동급 최고로 인정받는 Cisco AMP for Endpoints의 기능을 간추린 것입니다. 표 2에서는 소프트웨어 요구 사항을 소개합니다.

표 1. Cisco AMP for Endpoints의 기능과 혜택

기능	혜택
지속적인 분석	Cisco AMP for Endpoints는 특정 시점 방어에 그치지 않고 클라우드 기반 빅데이터 분석 기술을 활용하여 일정 기간 수집된 데이터를 지속적으로 재평가하면서 드러나지 않은 공격을 찾아냅니다.
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. IoC가 나타날 때, 이를테면 이벤트 트리거나 파일 속성의 변화, IoC 트리거가 발생할 때 회귀적 보안이 필요하게 됩니다.
대시보드	단일 창 방식으로 환경 전반에 대한 가시성을 확보합니다. 호스트, 디바이스, 애플리케이션, 사용자, 파일, 지오로케이션 정보뿐 아니라 APT(Advanced Persistent Threat), 위협 근본 원인, 기타 취약점까지 종합적인 컨텍스트 뷰를 제공하여 보안에 대한 현명한 결정을 내릴 수 있도록 도와줍니다.
종합적인 보안 인텔리전스	Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, AMP Threat Grid 위협 인텔리전스 피드는 가장 폭넓은 가시성, 가장 대규모의 풋프린트, 그리고 여러 보안 플랫폼에 실행할 수 있는 기능과 더불어 업계 최대 규모의 실시간 위협 인텔리전스를 보유하고 있습니다.
IoC	IoC는 상관성을 가진 파일 및 원격 측정 이벤트이며, 우선 순위에 따라 잠재적 활성 공격의 지표가 됩니다. Cisco AMP for Endpoints는 멀티소스 보안 이벤트 데이터, 즉 침입 및 악성 코드 이벤트 등의 상관성을 자동으로 분석함으로써 보안팀이 각종 이벤트를 더 크고 복잡한 공격과 연결하고, 우선 순위에 따라 고위험 이벤트를 처리할 수 있게 합니다.
파일 평판	고급 분석 및 종합 인텔리전스를 수집하여 파일이 정상인지 악성인지 결정함으로써 더 정확한 탐지를 가능하게 합니다.
파일 분석 및 샌드박싱	고도로 안전한 환경에서 악성코드 동작을 통제하에 실행, 분석, 테스트하여 지금까지 확인되지 않은 제로데이 위협을 밝혀낼 수 있습니다. AMP Threat Grid의 샌드박싱 기술을 AMP for Endpoints에 통합함으로써 더 큰 규모의 행동 지표를 대상으로 탄력적인 분석이 가능해집니다.
회귀적 탐지	확장 분석 이후 파일 속성이 바뀌면 이를 알려 초기 방어 체계를 통과한 악성코드를 파악하고 모니터링합니다.
파일 궤적	환경의 전 범위에서 시간의 경과에 따른 파일 전파를 지속적으로 추적하여 가시성을 확보하고 신속하게 악성코드 공격의 범위를 파악합니다.
디바이스 궤적	디바이스 및 시스템 레벨에서 지속적으로 활동과 통신을 추적하여 공격의 근본 원인을 신속하게 규명하고 공격 전후의 이벤트 기록을 파악합니다.
탄력적 검색	파일, 원격 측정, 종합 보안 인텔리전스 데이터의 전 범위를 대상으로 간단하면서도 무제한적인 검색을 수행하여 IoC 또는 악성 애플리케이션의 위험 범위와 컨텍스트를 신속하게 파악할 수 있습니다.
배포 수준이 낮은 실행 파일	조직에 실행되었던 모든 파일을 배포 수준이 낮은 것부터 표시하여 소수의 사용자만 겪어 탐지되지 못했던 위협을 찾아낼 수 있습니다. 소수의 사용자만 실행했던 파일은 확장 네트워크에 있어서는 안 될 악성코드(예: 표적 APT)이거나 의심스러운 애플리케이션일 수 있습니다.
엔드포인트 IoC	사용자는 직접 IoC를 제출하여 표적 공격을 차단할 수 있습니다. 보안팀은 이 엔드포인트 IoC로 해당 환경의 애플리케이션에 특화된 덜 알려진 지능형 위협에 대한 심층 조사를 수행할 수 있습니다.
취약성	이 기능은 취약한 소프트웨어 있는 호스트의 목록, 각 호스트의 취약한 소프트웨어 목록, 공격 가능성이 가장 높은 호스트를 표시합니다. Cisco의 위협 인텔리전스 및 보안 분석을 기반으로 하는 AMP는 악성코드의 표적이 된 취약한 소프트웨어를 식별하고 잠재적 익스플로잇을 알리며 패치할 호스트를 우선 순위에 따라 나열합니다.

기능	혜택
보안 침해 통제	콘텐츠 업데이트를 기다리지 않고 의심스러운 파일이나 공격을 제어하고 감염이 발생하면 신속하고 확실하게 제어하고 해결합니다. 공격 제어 기능에서 간단한 맞춤형 탐지 기능으로 모든 시스템 또는 선택된 시스템에서 특정 파일을 차단할 수 있습니다. 고급 맞춤형 시그니처는 다형성 악성코드 그룹을 차단하며, 애플리케이션 차단 목록을 통해 애플리케이션 정책을 적용하거나 악성코드 게이트웨이로 쓰이는 감염된 애플리케이션을 억제하고 반복적 재감염을 방지할 수 있습니다. 맞춤형 화이트리스트로 안전한 맞춤형 또는 미션 크리티컬 애플리케이션에서 무엇이든 실행할 수 있습니다. 디바이스 플로우 상관성 분석으로 소스에서, 특히 기업 네트워크 바깥의 원격 엔드포인트를 위해 악성코드 콜백 통신을 차단할 수 있습니다.
AMP Threat Grid와의 통합	AMP Threat Grid의 샌드박싱 기술 및 지능형 악성코드 분석 기능을 AMP for Endpoints에 통합하여 350여 가지의 고유한 행동 지표를 통해 파일 작업을 분석할 수 있습니다. 이해하기 쉬운 위협 점수와 수십억 개의 악성코드 아티팩트를 자유자재로 사용하면서 최고의 확장성을 실현하고 글로벌 위협을 차단할 수 있습니다.
AMP 프라이빗 클라우드 가상 어플라이언스	AMP for Endpoints는 개인 정보 보호 요구 사항이 엄격하여 퍼블릭 클라우드 사용이 제한되는 기업을 위해 안전한 온프레미스 솔루션으로도 구축할 수 있습니다.
AnyConnect v4.1에서 시작	Cisco AnyConnect v4.1 원격 액세스 VPN 클라이언트가 설치된 경우 원격 엔드포인트에서 AMP for Endpoints 커넥터를 실행할 수 있습니다. 따라서 엔드포인트 위협 차단 기능을 VPN 지원 엔드포인트까지 신속하게 확장하고 원격 호스트에서 공격이 발생할 가능성을 최소화할 수 있습니다. 원격 엔드포인트를 더 통찰력 있게 모니터링하고 공격 중에 또는 공격 후에 신속하게 문제를 해결합니다.

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, 8.1 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Embedded POSReady 2009 • Microsoft Windows Embedded POSReady 7 • Mac OS X 10.7 이상
Android 모바일 디바이스의 Cisco AMP for Endpoints	• Android 버전 2.1 이상

* Windows Embedded POSReady 7 또는 2009 운영 체제에서 AMP for Endpoints 커넥터를 구축하는 경우, 다른 운영 체제 구축에서 검증하는 것처럼 시스템이 커넥터를 검증해야 합니다.

플랫폼 지원 및 호환성

Cisco AMP for Endpoints에는 Cisco AMP for Endpoints 라이센스와 서브스크립션(1년, 3년, 5년 옵션) 및 경량형 커넥터가 포함되어 있습니다. Cisco AMP for Endpoints는 Cisco AMP for Networks와 호환됩니다. Cisco AMP for Endpoints는 원격 엔드포인트의 Cisco AnyConnect v4.1에서 실행할 수 있습니다.

품질 보증 정보

품질 보증 정보는 Cisco.com의 Product Warranties(제품 보증) 페이지를 참조하십시오.

주문 정보

주문하려면 Cisco Ordering Home Page(Cisco 주문 홈 페이지)를 방문하거나 Cisco 세일즈 담당자에게 문의하거나 800 553-6387로 전화하십시오.

자세한 정보

자세한 내용은 다음 링크를 참조하십시오.

- Cisco AMP for Endpoints

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, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA

C78-733181-02 05/15