CISCO 직원 및 파트너사 기밀

Cisco AMP(Advanced Malware Protection) 엔드포인트, 네트워크, 이메일 및 웹 대상

플레이북

프로그램 소개

AMP(Advanced Malware Protection) Everywhere 플레이북에는 Cisco AMP 솔루션을 포지셔닝하고 판매하도록 지원하는 세부적인 정보, 영업 지원, 수요 창출 리소스가 포함되어 있습니다. 고객이 지능형 위협 및 보안 침해로부터 스스로를 지키도록 지원하면서 수익을 창출할 수 있는 절호의 기회를 놓치지 마십시오.

지능형 위협 시장 개요

시장 현황

조직은 공격에 노출되어 있으며 보안 침해 사고가 잇달아 뉴스 헤드라인을 장식하고 있습니다. 해킹은 전문성, 기업가 정신, 리소스를 두루 갖춘 사이버 범죄자 커뮤니티를 동력으로 삼으며 산업으로 자리잡았습니다. 풍부한 자금을 바탕으로 특정 조직을 겨냥하여 여러 공격 벡터를 통해 기계화된 다면적 공격을 능숙하게 구사하면서 끈질기고 가차 없는 면모를 보여줍니다.

빠르고 효과적이며 능률적인 방식으로 경제적 이익을 도모하는 이 범죄자들은 지능형 악성코드를 비롯한 각종 체계적인 기술을 구사합니다. 다형성(polymorphic) 악성코드, 환경 인식 악성코드 등을 포함하는 이러한 악성코드는 능수능란하게 그 정체를 숨기고 기존의 보안 툴을 피합니다. 그로 인해 조직들은 끊임없이 공격받고 있습니다.

과제

이제 문제는 보안 공격의 "가능성"이 아니라 "언제" 공격을 받느냐입니다. 이미 공격을 받았지만 그 사실조차 모를 수도 있습니다.

다음 수치에 주목하십시오.

- 조직의 95%는 악성코드의 표적이 된 적이 있습니다.
- 공격받은 조직의 데이터 중 60%는 수 시간 내에 유출됩니다.
- 보안 침해의 54%는 몇 개월이 지나도 드러나지 않습니다.
- 보안 침해의 원인조차 규명하지 못하는 조직이 55%에 달합니다.
- 업계 평균적으로 악성코드 탐지에 100일이 걸립니다.

이러한 수치는 오늘날 IT 보안 툴이 최신 지능형 공격에 대응하지 못하고 있음을 나타냅니다.

왜 그럴까요? 스스로를 방어하기 위해 안티바이러스, 스테이트풀 방화벽, 레거시 IPS(intrusion prevention system)에만 의존하는 곳이 많습니다. 이러한 "특정 시점" 보안 툴은 파일이 확장 네트워크에 진입하는 시점에서 이를 검사합니다. 주로 시그니처 및 파일 평판을 사용하여 확인된 "위험" 파일을 차단하고 "안전"하거나 "알려지지 않은" 파일은 네트워크 진입을 허용합니다. 하지만 안타깝게도 바로 이 지점에서 분석이 끝나고 문제가 발생합니다.

지능형 악성코드에 대해 알려진 바에 따르면, "안전" 또는 "알려지지 않음" 판정을 받은 것이 사실은 악성 파일일 가능성이 높습니다. 아직 확인되지 않았을 뿐입니다. 해당 파일의 위험성을 알리는 시그니처나 위협 인텔리전스가 없을 것입니다. 혹은 지능형 악성코드가 "안전한" 파일로 능숙하게 위장하여 탐지를 피하는 경우도 있습니다. 샌드박스가 구축되었더라도 지능형 악성코드는 슬립(sleep) 기술이나 다형성을 이용하여 회피할 수 있습니다. 일단 악성코드가 네트워크에 침투하면 이러한 툴에서는 초기 검사 이후에 위협 활동을 거의 또는 전혀 파악하지 못합니다. 따라서 IT 보안 팀은 아무것도 모르게 되고 계속 파일을 모니터링할 방법이 없으므로 만일의 악의적인 행동에 대해 조치를 취할 수도 없습니다.

뿐만 아니라 특정 시점 툴의 한계에도 불구하고 조직에서는 계속 더 많은 툴을 투입하여 문제를 해결하려는 듯 보입니다. 상호 연동되지 않는 서로 다른 보안 제품을 60개 이상 도입한 곳도 드물지 않습니다. 이종 제품들끼리 커뮤니케이션이 이루어지지 않거나 정보를 공유할 수 없을 때도 있습니다. 이는 드러나지 않는 위협을 파악할 수 있는 기능을 저하시킵니다. 이러한 이종 툴은 우선 순위가 없는, 또는 중복된 알림만 매일 수백 개씩 쏟아냅니다. 따라서 보안 팀의 입장에서는 불필요한 작업이 더욱 늘어날 뿐입니다. 제품이 많으면 IT 팀에서 관리해야 할 관리 시스템도 늘어나므로 자본 및 운영 비용이 상승하고 관리 복잡성이 심화됩니다.

대상 고객

Cisco AMP Everywhere 프로그램은 위협으로부터 조직을 보호하기 위해 종합적인 보안 솔루션을 필요로 하는 엔터프라이즈, 커머셜, SMB 또는 공공 부문 고객을 대상으로 합니다. 요즘에는 모든 업종의 모든 조직이 공격의 표적이 됩니다.

따라서 보안의 구매자도 다양합니다. Cisco AMP의 1차적 대상은 조직의 IT 보안 관리자, 최고 정보 보안 책임자(CISO), 사고 대응 담당자 그리고 더 광범위한 의미로 보안 팀입니다. 그러나 보안이 경영진의 관심 사항이 되었고 엔드포인트부터 네트워크까지 전 범위에서 보안이 구현되는 만큼 보안 이외의 다른 팀도 참여시켜야 합니다. 데스크톱 및 엔드포인트 팀, 네트워킹 팀, CIO, COO, CEO까지 구매자가 될 수 있습니다.

이 프로그램에서는 다음과 같은 기회를 공략해야 합니다.

신규 고객 발굴

- 보안이 필요하지 않은 조직은 없습니다. Cisco AMP 가치 제안, 즉 *공격 전/중/후에서 가시성, 상황 및 제어를 제공하는 위협 대응형 보안*을 공유하고 신규 기회를 발굴하십시오. *Cisco AMP로 보안 침해를 예방할 수 있으며 (언젠가는 일어날 상황이지만) 어떤 위협이 침투하더라도 실제로 피해가 발생하기 전에 신속하게 공격을 탐지, 억제 및 치료할 수 있습니다*.

고객 마이그레이션

- FireEye의 HX Endpoint Security, Palo Alto Networks의 TRAPS, Carbon Black, Crowdstrike와 같은 엔드포인트 기반 지능형 악성코드 제품 또는 보안 침해 탐지 제품을 사용하는 고객을 Cisco AMP for Endpoints로 마이그레이션합니다.
- Palo Alto Networks, FireEye, Lastline, Trend Micro, CheckPoint, Fortinet 등과 같은 경쟁업체의 네트워크 기반 지능형 악성코드 또는 보안 침해 탐지 제품을 사용 중인 고객을 Cisco ASA Firewall, FirePOWER NGIPS, Cisco ESA, WSA, CWS에 구축된 Cisco AMP for Networks로 마이그레이션합니다.
- 경쟁업체 제품 계약의 서브스크립션 기간을 곧 갱신해야 하거나 제품이 곧 단종될 고객을 마이그레이션합니다.
- 경쟁사 보안 제품을 사용하는데도 보안 침해를 당한 적이 있는 고객을 마이그레이션합니다.

기존 Cisco 고객 업셀

- CWS(Cloud Web Security), ESA(Email Security Appliance), WSA(Web Security Appliance), ASA Firewall, FirePOWER NGIPS, Meraki MX, Threat Grid와 같은 보안 제품을 구축한 현재 Cisco 고객에게 AMP 서브스크립션 애드온을 업셀합니다. AMP 기능은 이 다양한 Cisco 보안 제품에 통합 가능하며 라이선스 및 서브스크립션 애드온이 있으면 "활성화"할 수 있습니다.
- 고객에게 AnyConnect v4.1에서 AMP for Endpoints 커넥터를 다운로드하는 기능에 대해 교육합니다.
- AMP for Networks 또는 AMP for Email 같은 다른 종류의 AMP를 구축한 현재의 Cisco AMP 고객에게 AMP for Endpoints를 크로스셀합니다.
- 네트워크 아키텍처에서 보안 범주에 속하지 않는, 임의 레벨의 Cisco 제품이 있는 고객에게 Cisco AMP를 업셀합니다. 간소화된 Cisco 솔루션 방식의 가치를 세일즈에 활용하십시오. 즉 통합된 툴끼리 통신하고 정보를 공유하며 더 신속하게 탐지하고 OpEx를 줄이며 신뢰받는 단일 벤더를 통해 더 편리하게 관리한다는 점을 강조하십시오. Cisco의 Security Everywhere 방식에 대한 자세한 내용은 Cisco Executive Perspectives on Security, Security Everywhere 백서를 참조하십시오.

파트너십을 통해 고객 업셀

- Threat Grid는 다양한 서드파티 보안 툴과의 통합을 지원합니다. Guidance EnCase, Tripwire, Fidelis, RSA, Tenable과 같은 툴 또는 Splunk, QRadar, Blue Coat, Palantir, ArcSight 등을 위한 샘플 통합 레시피를 사용하는 고객이 있다면 Threat Grid 업셀 기회가 있습니다.

파트너를 위한 혜택

보안 침해는 매일 일어나고 있습니다. 보안은 보안 운영 팀과 IT 보안 관리자뿐 아니라 경영진에게도 최고 관심사입니다. 그리고 이사회의 쟁점이기도 합니다. 맹렬한 공격이 계속되고 기밀 보호 및 통제와 관련된 우려가 커지는 가운데 사업의 연속성을 제공하고 가치 있는 정보를 보호하며 브랜드 명성을 유지하려면 보안이 필수입니다.

따라서 크고 작은 조직 모두 Cisco와 같은 신뢰받는 보안 벤더가 가장 시급한 보안 문제를 해결할 솔루션을 제공해 주기를 바라고 있습니다. Cisco AMP(Advanced Malware Protection) 솔루션은 보안 침해를 예방할 뿐 아니라 기존의 보안 방어 시스템을 통과한 위협을 빠르게 탐지하고 숨어 있는 악성코드를 신속하게 치료하는 데 필요한 가시성, 상황, 제어 기능을 조직에 제공합니다. 또한 Cisco는 시장 주도력, 공격 전/중/후를 포괄하는 지능형 위협 차단, 혁신적인 제품, 지속적인 보안 투자, 긴 제품 수명을 바탕으로 고객의 자산을 보호할 최상의 벤더입니다.

1. 급성장 중인 사이버 보안 시장에서 첨단 기술 활용

- Cisco Advanced Malware Protection은 최고의 보안 기술로, 공격 전, 공격 중, 공격 후 상황에서 조직을 보호할 뿐만 아니라 지속적인 파일 분석을 통해 숨은 악성코드를 신속히 탐지해 보안 침해 범위를 파악하고 제거합니다.
- IT 보안 업계는 현재 매우 유망한 분야입니다. 수백만 달러가 매일 거래되고 있습니다. 엔드포인트 보안은 EDR(Endpoint Detection and Response) 시장이 연평균 성장률 48%로 모든 보안 분야 중에서도 가장 크게 성장 중인 부문입니다.
- 가장 심각한 지능형 악성코드로부터 조직을 보호하기 위해 은행, 소매업체, 대학, 사고 대응 업체를 비롯한 모든 부문에서 Cisco AMP를 사용합니다.
- NSS Labs에서는 보안 침해 탐지 시스템에 대한 비교 테스트를 통해 3년 연속(2014-2016) Cisco AMP를 보안 효율성 및 빠른 탐지 소요 시간 면에서 가장 뛰어난 솔루션으로 선정했습니다.

2. AMP로 Cisco의 "Security Everywhere" 전략 활용

- 조직들은 서로 다른 벤더의 상이한 제품을 다수 도입하는 것으로는 보안 문제를 제대로 해결할 수 없음을 깨닫기 시작했습니다. 보안 및 네트워크 구매자는 보안 제품들이 정보를 공유하고 공조하면서 지능형 공격에 맞서는 통합된 첨단 보안 에코시스템을 원합니다. Cisco 보안 제품은 고객에게 이러한 통합 솔루션을 제공합니다.
- Cisco AMP를 출발점으로 삼아 더 큰 보안 기회에 대한 논의로 발전시키십시오. Cisco는 방화벽 및 네트워크 어플라이언스부터 웹/이메일 보안 및 서비스까지 전사적 범위에서 종합적인 보호를 제공합니다.
- Cisco AMP 기술은 이러한 통합 보안 방식과 연계하여 몇 가지 다른 방식(예: 데이터 센터, 엔드포인트, 모바일 디바이스, 웹, 이메일, 네트워크)으로 구축하고 사용할 수 있습니다. 다양한 AMP 툴을 함께 구축하면 서로 정보를 공유하고 통신하며 연동되면서 더 신속하게 위협을 탐지, 분석, 치료합니다.

3. 인센티브 및 할인 프로그램을 통한 이윤 증대

- Cisco OIP(Opportunity Incentive Program) 및 VIP(Value Incentive Program)는 새롭게 비즈니스 기회를 발굴하는 파트너에게 보상을 제공하며, Cisco 아키텍처에 포함된 기술에 주력하여 영업하는 파트너에게는 리베이트를 제공합니다. 위 링크의 웹 페이지에서 "Security"로 필터링한 다음 해당 페이지에서 모든 AMP 프로모션을 표시하고 검색할 수 있습니다.
- Security Ignite 프로그램(Cisco AMP 등 Cisco의 신규 보안 비즈니스에 대해 할인 혜택 제공)도 이용하십시오.
- Cisco CFIP(Capital Customer Finance Incentive Program)에서는 고객에게 Cisco Capital 금융 상품을 통해 Cisco 솔루션을 판매하는 파트너에게 리베이트를 제공합니다. 자세한 내용은 www.cisco.com/go/capital/contacts를 참조하십시오.

Cisco AMP(Advanced Malware Protection) 소개

Cisco AMP(Advanced Malware Protection)는 지능형 악성코드 문제의 전체 라이프사이클을 다룰 수 있는 보안 솔루션입니다. 이 솔루션으로 보안 침해를 방지할 뿐 아니라 최전선 방어를 우회하는 보안 위협을 빠르게 탐지, 억제, 치료하기 위한 가시성, 상황, 제어 기능도 비용 효과적으로 운영 효율성 저하 없이 확보할 수 있습니다. Cisco AMP는 공격 전, 중, 후의 모든 단계에서 고객을 보호합니다.

- 공격 **전** 단계에서 Cisco AMP는 Cisco Talos Security Intelligence and Research Group 및 Threat Grid 위협 인텔리전스 피드의 글로벌 위협 인텔리전스를 활용하여 방어를 강화하고 이미 알려져 있거나 새롭게 대두되는 위협을 차단합니다.
- 공격 **중**에 Cisco AMP에서는 이러한 인텔리전스와 함께 잘 알려진 파일 시그니처 및 Threat Grid의 샌드박싱 및 악성코드 분석 기술을 결합하여 정책 위반 파일 유형, 익스플로잇 공격 시도, 네트워크에 침투하려는 악성 파일 등을 식별하고 차단합니다.
- 공격 **후** 또는 파일이 최초로 검사된 후에는 모든 파일 활동과 트래픽을 지속적으로 모니터링하고 분석합니다. 이 과정에서는 파일의 성향에 관계없이 모든 악성 행동 지표를 검색합니다. Cisco AMP에서는 알 수 없는 상태의 파일 또는 "안전"한 상태였던 파일의 행동에 이상이 나타나기 시작하면 즉시 탐지하여 보안 팀에 보안 침해 지표와 함께 알립니다. 그런 다음 악성코드의 출처, 감염된 시스템, 악성코드의 행동을 확인할 수 있는 종합적인 가시성을 제공합니다. 또한 몇 번의 클릭만으로 침입에 신속하게 대응하여 위협을 억제하고 치료할 수 있는 기능을 제공합니다.

이 기능을 통해 AMP는 새로운 악성코드를 13시간 이내에 탐지할 수 있으며 이는 업계의 평균 시간인 100일과 대조됩니다. 자세한 내용을 알아보려면 Cisco AMP 솔루션 개요 또는 Visibility and Control to Prevent, Detect, and Remediate Advanced Malware Everywhere 백서를 참조하십시오.

AMP 솔루션의 기능 및 장점

AMP는 지능형 공격을 차단하는 데 필요한 가시성, 상황, 제어를 고객에게 제공합니다. 이는 다음 기능을 통해 실현할 수 있습니다.

글로벌 위협 인텔리전스: Cisco Talos 전문가는 매일 수백만 개의 악성코드 샘플과 테라바이트 단위의 데이터를 분석하여 그 결과로 얻어진 정보를 AMP로 보냅니다. AMP는 이 풍부한 상황 정보를 기준으로 파일, 텔레메트리 데이터 및 파일 행동의 상관관계를 분석하여 알려진 위협과 새롭게 등장하는 위협을 사전에 차단합니다.

지능형 샌드박싱: 지능형 샌드박싱 기능은 700개 이상의 행동 지표를 기준으로 파일에 대해 정적 분석과 동적 분석을 수행합니다. 이를 통해 드러나지 않는 위협을 탐지할 수 있으며, 보안 팀이 정교한 공격을 파악하고 우선 순위를 정하고 차단하는 데에도 도움이 됩니다.

특정 시점 악성코드 탐지 및 차단: 네트워크 침투를 시도하는 악성코드를 실시간으로 차단합니다. AMP는 일대일 시그니처 매칭, 머신 러닝 및 퍼지 핑거프린팅 기술을 활용하여 네트워크 진입 지점에서 파일을 분석하고 알려진 악성코드와 알려지지 않은 악성코드를 포착합니다. 그 결과 탐지 및 자동 보호에 걸리는 시간이 단축됩니다.

지속적 분석 및 회귀적 보안: 파일이 네트워크로 들어온 후에는 파일의 성향에 관계없이 AMP가 지속적으로 활동을 감시하고 분석하고 기록합니다. 이후 악의적인 행동이 포착되면 AMP가 보안 팀에 악성코드의 출처, 경로, 기능에 대해 알리는 회귀적 알림을 보냅니다. 그러면 사용자가 클릭 몇 번으로 악성코드를 억제하고 치료할 수 있습니다. 또는 수작업 없이 자동으로 치료하도록 AMP를 설정합니다.

고객에게 가장 적합한 AMP 구축 방법 찾기

Advanced Malware Protection은 서브스크립션을 통해 제공되는 솔루션으로, 웹 기반 관리 콘솔에서 관리되며, 다양한 플랫폼에 구축됩니다.

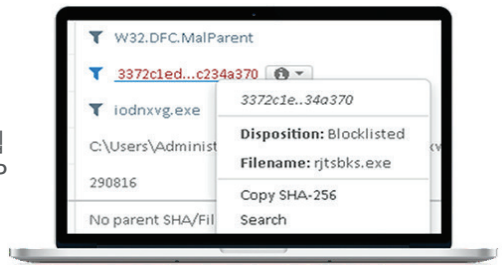
엔드포인트 보호: Cisco의 엔드포인트 보안 솔루션인 AMP for Endpoints를 사용하여 파일과 실행 파일 레벨의 활동에 대해 가시성을 확보하고, Microsoft Windows, Mac OS, Linux 및 Android를 실행하는 컴퓨터와 모바일 디바이스에서 악성코드를 제거합니다.

네트워크 보호: 네트워크 레벨의 위협 활동과 네트워크 에지의 위협 활동에 대한 심층적 가시성을 확보하고 지능형 악성코드를 차단합니다.

AMP 작동 위치... NGIPS(AMP for Networks) 차세대 방화벽
Meraki MX UTM 플랫폼 브랜치 라우터(ISR)

이메일 및 웹 트래픽 보호

이메일 및 웹 보안 어플라이언스나 클라우드 이메일 및 웹 보안 구축 환경에 AMP 기능을 추가하십시오.



포트폴리오

AMP for Endpoints	AMP의 저용량 커넥터 클라이언트 애플리케이션을 사용하여 Windows PC, Mac, Linux, Android 모바일 디바이스 및 가상 환경을 보호합니다. AMP for Endpoints를 AnyConnect v4.1에서 실행할 수 있습니다.
AMP for Networks	AMP를 Cisco FirePOWER NGIPS 보안 어플라이언스에 통합된 네트워크 기반 솔루션으로 구축합니다. AMP for Networks를 구축하는 최적의 방법은 AMP for Networks 전용 어플라이언스 번들을 사용하는 것입니다. 어플라이언스 모델: • **AMP 7150** — 최대 500Mbps의 네트워크 기반 AMP 성능, 120GB의 스토리지 • **AMP 8050** — 최대 1Gbps의 네트워크 기반 AMP 성능, 400GB의 스토리지 • **AMP 8150** — 최대 2Gbps의 네트워크 기반 AMP 성능, 400GB의 스토리지 • **AMP 8350—** — 최대 5Gbps의 네트워크 기반 AMP 성능, 400GB의 스토리지 • **AMP 8360—** — 최대 10Gbps의 네트워크 기반 AMP 성능, 800GB의 스토리지 • **AMP 8370—** — 최대 15Gbps의 네트워크 기반 AMP 성능, 1,200GB의 스토리지 • **AMP 8390** — 최대 20Gbps의 네트워크 기반 AMP 성능, 1,600GB의 스토리지 AMP for Networks는 Cisco ISR(Integrated Services Router)을 위한 위협 방어 기능을 제공하기 위해 구축할 수도 있습니다.
AMP Private Cloud Virtual Appliance	AMP를 네트워크 또는 엔드포인트에서 온프레미스 에어 갭(air-gapped) 솔루션으로 구축합니다. 이는 특히 퍼블릭 클라우드 사용을 제한하며 높은 개인 정보 보호 수준이 필요한 조직을 위한 설계입니다.
AMP on NGFW 및 ASA with FirePOWER Services	AMP 기능을 Cisco NGFW 또는 ASA 방화벽에 통합 구축합니다.
AMP on ESA(Email Security Appliance), WSA(Web Security Appliance), CWS(Cloud Web Security)	AMP 기능은 Cisco CWS(Cloud Web Security), ESA(Email Security Appliance), WSA(Web Security Appliance) 등에서 활성화하여 회귀적 기능 및 악성코드 분석을 제공할 수 있습니다.
AMP for Meraki	Cisco AMP 및 Threat Grid 기능은 지능형 위협 차단 기능을 갖춘 간소화된 클라우드 기반 네트워크 관리를 지원하는 Meraki MX에 추가할 수 있으며, 이렇게 할 경우 네트워크 내부, 여러 사이트 및 브랜치 위치 전체에 대한 광범위한 가시성이 제공됩니다.
Threat Grid	독립형 악성코드 분석 및 위협 인텔리전스 제품이며 클라우드에 또는 온프레미스 어플라이언스의 형태로 구축할 수 있습니다. Threat Grid 위협 인텔리전스 및 지능형 악성코드 분석 기능은 다른 AMP 구축에 각기 다른 용량으로 내장되어 있습니다.
Security Services for AMP	• **자문 서비스** — 종합적인 보안 전략의 일환으로 고객이 AMP를 위한 기회를 찾도록 지원합니다. • **통합 서비스** — 고객이 AMP 구현을 구축, 구성, 테스트, 튜닝하도록 지원합니다. • **매니지드 서비스** — Cisco의 첨단 보안 운영 센터로 구성된 글로벌 네트워크에서 전문 조사 팀이 휴일 없이 24시간 고객 네트워크를 모니터링하면서 지속적인 감시 및 심층 분석을 수행합니다.

이 목록에 있는 제품의 구축 옵션은 7페이지의 그림 1에 나와 있습니다.

그림 1. AMP 포트폴리오의 제품

구축 옵션	AMP - ESA, WSA, ASA, CWS, ISR	AMP for Networks (AMP on FirePOWER Network Appliance)	AMP for Meraki (AMP on Meraki MX 디바이스)	AMP for Endpoints	AMP Private Cloud Virtual Appliance
방법	ESA, WSA, CWS, ISR 또는 ASA 고객 라이선스	네트워크에 구축	Cisco Meraki® MX 라이선스	엔드포인트에 저용량 커넥터 설치	온프레미스 가상 어플라이언스 구축
적합한 사용자	신규 또는 기존 Cisco CWS, ISR, Email/Web Security, ASA 고객	Firepower NGIPS 고객	신규 또는 기존 Meraki 고객	Windows, Mac, Android, Linux도 Cisco AnyConnect® 클라이언트에서 구축 가능	개인 정보 보호 요건이 까다로운 환경
세부 사항	▪ WSA/WSA: 이메일/웹에 대한 뛰어난 가시성 ▪ CWS: 클라우드를 통해 제공되는 서비스에서 웹 및 지능형 악성코드 차단 ▪ ASA 또는 ISR: 방화벽에 대한 AMP 가시성	▪ 네트워크 내부의 광범위한 가시성 ▪ 공격 전, 중, 후의 다양한 기능 선택	▪ 네트워크 내부, 여러 브랜치 위치 전반에 걸친 광범위한 가시성 ▪ 지능형 위협 차단 기능을 갖춘 간소화된 클라우드 기반 보안 관리	▪ 포괄적인 위협 차단 및 대응 ▪ 세밀한 가시성 및 제어 ▪ 가장 광범위한 선택 가능 AMP 기능	▪ 고도의 개인정보 보호가 요구되는 환경을 위한 프라이빗 클라우드 옵션 ▪ 정식 에어 갭(air-gapped) 모드 또는 클라우드 프록시 모드로 구축 가능 ▪ 엔드포인트 및 네트워크용
Threat Grid	하이브리드 또는 온프레미스 통합	클라우드 통합 및 온프레미스 통합	하이브리드 또는 온프레미스 통합	파일 분석 기능으로 통합	온프레미스 통합

주문 방법

Cisco AMP 솔루션 주문 방법에 대한 자세한 내용은 주문 가이드를 참조하십시오.

AMP for Endpoints 소개

AMP 포트폴리오에는 다양한 유형의 구축이 포함되어 있습니다. AMP for Endpoints는 가장 많은 기능, 위협 활동에 대한 최고의 가시성, 제공되는 모든 AMP 구축에 대한 최고의 제어를 제공합니다.

Cisco AMP for Endpoints는 클라우드 관리형 엔드포인트 보안 솔루션으로서 사이버 공격을 방지할 뿐 아니라 1차 방어선을 통과하여 침투한 지능형 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, Linux를 실행하는 엔드포인트 및 Android 모바일 디바이스를 보호합니다.

AMP for Endpoints는 조직이 다음을 수행할 수 있도록 지원합니다.

차단: 사이버 공격을 방지하고 악성코드를 진입 지점에서 실시간으로 차단합니다. 어떻게 가능할까요?

- AV 대체: AV에 더 이상 비용을 지출하지 마십시오. 에이전트 증가를 줄이고 AMP의 내장형 AV 탐지 엔진을 사용하여 진입 지점에서 공격을 차단할 수 있습니다.
- 방어 강화: 위협 연구기관인 Talos 팀에서 제공하는 최신 위협 인텔리전스를 활용하여 위협 방어 체계를 강화하고 새로운 위협 및 제로데이 공격을 차단합니다.
- 사전 차단: Threat Grid에서 제공하는 AMP의 내장형 샌드박스 기능, 애플리케이션 취약점 기능, 발생률이 낮은 실행 파일 분석을 사용하여 공격 경로를 차단하고 의심스러운 위협을 역으로 분석한 후 이를 차단합니다.

탐지: 조직에서는 Cisco AMP for Endpoints를 사용하여 탐지 소요 시간을 업계 평균 시간인 100일에서 몇 시간 또는 몇 분까지로도 단축할 수 있습니다. 어떻게 가능할까요?

- 지속적인 모니터링 및 회귀적 보안: 파일이 차단을 우회하는 경우에도 AMP for Endpoints는 모든 파일 활동을 지속적으로 모니터링하고 기록하여 악성 행동을 신속하게 찾아내고 시간을 되돌려 잠재 공격자의 공격을 막아냅니다.
- 에이전트 없는 탐지: 엔드포인트 에이전트가 확인할 수 있는 것을 넘어섭니다. Cisco의 CTA 통합으로 에이전트 없는 탐지를 사용하면 감염 수를 30% 더 확인할 수 있습니다.
- 한 번 확인한 위협을 모든 위치에서 차단: 개방형 API 및 AMP Everywhere를 사용하여 보안 아키텍처 전반에 걸쳐 위협 정보를 공유하고 상관관계를 조사하여 더욱 통합된 위협 방어를 지원할 수 있습니다.

대응: 사이버 공격을 확인하고 이에 더욱 빠르고 효과적으로 대응합니다. 어떻게 가능할까요?

- 공격의 전체 범위 및 기록: 악성코드의 출처, 경로, 기능을 확인하여 이에 더욱 빠르고 효과적이고 효율적으로 대응할 수 있습니다.
- 손쉬운 위협 추적: AMP의 간단한 클라우드 기반 UI를 통해 모든 엔드포인트 전반에서 손쉽게 보안 침해 지표를 검색하여 조사 속도를 높이고 관리 복잡성을 줄일 수 있습니다.
- 물리적 억제 및 치료: 모든 PC, Mac, Linux, 모바일 디바이스에서 클릭 몇 번으로 체계적인 악성코드 대응 및 치료를 수행합니다.

또한, AMP for Endpoints는 사일로화된 포인트 제품이 아닙니다. 이 제품에는 고객이 AMP for Endpoints를 다른 보안 툴 또는 SIEM과 동기화할 수 있는 API가 포함되어 있습니다. 무엇보다도, AMP for Endpoints는 더 광범위한 AMP Everywhere의 통합 보안 에코시스템의 일부입니다. 다시 말해, AMP for Endpoints는 엔드포인트에서 네트워크 IPS, 방화벽, 웹 또는 이메일 게이트웨이 등에 이르는 정보를 공유하고 상관관계를 조사합니다. 따라서 한 곳에서 위협을 발견한 경우 전체 보안 에코시스템에서 체계적으로 대응할 수 있습니다. 즉, 이는 더욱 빠르고 종합적인 대응이 가능하다는 것을 의미합니다. 이러한 통합 아키텍처는 보안 팀의 역량을 배가시키는 요소입니다.

구축 방법

AMP는 클라우드 기반 "SaaS(Software as a Service)" 엔드포인트 보안 솔루션입니다. 엔드포인트에 AMP의 경량형 커넥터를 구축한 후 계정을 설정하면 됩니다. 지원할 엔드포인트 수를 선택하고 서브스크립션 기간을 1년, 3년 또는 5년으로 선택합니다. 구축 방법에 대한 자세한 내용은 AMP for Endpoints 데이터시트를 참조하십시오. AMP for Endpoints에 대한 자세한 내용은 www.cisco.com/go/ampendpoint에서 확인하십시오.

판매 방법에 대한 팁

1. 신규 기회를 추진하되, 이미 다른 종류의 AMP를 구축한 현재 15,000개의 고객사(2016년 10월 기준)와도 AMP for Endpoints 영업 상담을 진행하십시오. 엔드포인트에 대한 가시성, 상황, 제어 레벨을 적용할 경우에만 최종 방어선인 종합적인 엔드포인트 보호를 구현하고, 최신 지능형 공격을 차단할 수 있다는 사실을 고객에게 설명하면서 엔드포인트에 대한 상담을 진행하십시오.
2. 예방, 탐지, 대응 부분에서 AMP for Endpoints가 제공하는 가치를 명확하게 판매하십시오. Cisco 제품은 그 어떤 경쟁업체보다 이러한 기능이 뛰어납니다. 그러나 AMP Everywhere 아키텍처에 대해 강조하는 것도 잊지 마십시오. AMP for Endpoints는 아무것도 없는 새로운 기반에 구축되는 것이 아니라 네트워크, 웹, 이메일에서 나머지 Cisco 보안 아키텍처와 통합됩니다. 이는 다른 경쟁업체가 따라올 수 없는 차별화 요소이자 거래 체결을 성공으로 이끄는 요소입니다. 고객은 더욱 체계적이고 통합된 위협 방어를 제공하는 Cisco의 아키텍처 접근 방식을 높이 평가합니다. AMP 서브스크립션을 모든 솔루션과 어태치하십시오. AMP for Networks, AMP on Web, AMP on Email을 크로스셀하십시오.

자세히 보기

AMP for Endpoints에 대한 자세한 내용을 알아보고 판매 리소스를 활용하려면 다음 링크를 방문하십시오.

- www.cisco.com/go/ampendpoint
- 세일즈 리소스
- AMP for Endpoints 데이터시트
- AMP for Endpoints 한눈에 보기

AMP for Endpoints의 기능 및 장점

표 1.

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 분석에 소요되는 시간은 4분입니다.
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.
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.
AV 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.
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.
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.

표 1. 계속

기능	장점
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.
애플리케이션 프로그래밍 인터페이스(API)	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 계정의 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.
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.
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.

Cisco AMP로 고객의 과제 해결

고객의 과제 → 솔루션

고객이 IT 보안과 관련하여 직면하는 과제는 광범위합니다. 아래의 표를 참조하여 고객이 가장 시급한 과제 및 관심사에 적합한 Cisco AMP 솔루션을 찾도록 도우십시오.

고객 당면 과제	Cisco AMP 솔루션
악성코드가 정교하며 은밀하게 활동하면서 IT 환경에 침투하고 있습니다.	AMP는 공격 전, 중, 후의 모든 단계에서 고객을 보호합니다. 악성코드가 1차 방어선을 지나고 초기 검사를 통과하더라도 AMP가 계속 (파일의 성향과 상관없이) 파일을 모니터링합니다. 악성 활동의 1차 징후가 나타나거나 AMP 인텔리전스 클라우드에서 수집한 새로운 인텔리전스에서 파일이 악성일 가능성을 제시할 경우 AMP는 보안 팀에 회귀적 알림을 보내 보안 침해 지표를 전달합니다. 그런 다음 AMP는 위협에 대한 세부 정보를 제공하고 고객이 판단하기에 적합한 조치를 취할 수 있게 합니다. 또는 고객을 대신하여 자동으로 차단할 수도 있습니다. NSS Labs가 지능형 공격에 대한 평가에서 AMP를 보안 효율성의 선두주자로 꼽았습니다.
복수의 공격자가 여러 공격 벡터를 통해 연합 작전을 펼치곤 합니다.	AMP는 웹, 이메일, 엔드포인트, 모바일, 네트워크 등 여러 공격 벡터에 걸쳐 구축할 수 있습니다. 그러면 확장 네트워크의 모든 진입 지점에 대한 가시성을 확보하고 예전보다 신속하게 대응할 수 있습니다. 또한 AMP는 데이터 및 텔레메트리 이벤트의 상관성을 파악하여 연합 공격을 찾아냅니다. AMP 기술은 고객 아키텍처 전반의 다양한 AMP 구축 유형 및 기타 Cisco 보안 구축 모델(FirePOWER NGIPS, ASA, 웹 및 이메일 게이트웨이 등)과도 데이터를 공유하므로 정보 공유, 통신, 다각적인 공격을 위해 설계된 위협을 더 확실하게 포착할 수 있습니다.
위협이 침투하더라도 이를 알아볼 방법이 없습니다.	가시성은 Cisco AMP 기술의 핵심입니다. AMP는 위협을 심층 분석할 수 있는 가시성을 제공합니다. 첫째, Cisco는 알려진 위협 및 새로운 위협에 대해 최대한 많은 정보(예: 형태, 출처, 동작 등)를 제공하는 탁월한 위협 인텔리전스 및 악성코드 분석 기능을 제공합니다. 그러면 알려진 위협 및 새로운 위협에 대한 방어를 강화할 수 있습니다. 둘째, 파일 시그니처, 퍼지 핑거프린팅, 파일 평판 및 기타 엔진을 사용하여 침입 시도에 대한 가시성을 확보합니다. Cisco AMP는 시스템 침투를 시도한 어떤 위협을 탐지하여 자동으로 차단하는지 알려줍니다. 셋째, Cisco AMP는 공격 중 및 공격 후에도 위협에 대해 최고 수준의 가시성을 제공합니다. 어떤 파일이 "안전" 또는 "알려지지 않음"으로 분류되어 네트워크 진입이 허용되더라도 Cisco AMP는 계속 예의 주시하면서 (그 성향과 상관없이) 모든 동작을 기록합니다. 보안 팀은 Cisco AMP 콘솔에서 이러한 활동을 명확하게 볼 수 있습니다. 악성 활동이 포착되면 AMP는 보안 침해 지표의 형태로 회귀적 알림을 보내고 벌어진 상황, 악성코드 출처, 경로, 정확한 목적 등에 대한 즉시 액세스 가능한 정보를 제공합니다. Cisco AMP 콘솔에서 마우스를 몇 번만 누르면 위협에 대해 필요한 모든 정보를 얻고 침해 범위를 효과적으로 파악할 수 있습니다. Cisco AMP를 통해 얻을 수 있는 가시성 레벨에 대한 내용은 이 AMP for Endpoints 비디오를 참조하십시오.
위협이 침투하면 이를 제어할 방도가 없습니다.	제어할 수 없다면 가시성은 무용지물입니다. Cisco AMP는 위협을 차단, 억제, 치료할 수 있는 제어 기능을 제공합니다. Cisco AMP는 공격 이전 및 공격 상황에서 최상의 위협 인텔리전스로 공격을 예방하도록 지원하고 시그니처, 동작, 파일 평판, 퍼지 핑거프린팅, Cisco Threat Grid 인텔리전스 피드에서 수집한 새 정보, 회귀적 알림에 기반하여 위협을 자동으로 차단하고 억제합니다. 공격 이후에는 자동 제어 기능이 악성 동작을 차단합니다. 또는 악성 동작에 대한 알림을 보낸 다음 마우스를 수동으로 몇 번만 클릭하여 파일을 억제하고 치료할 수 있도록 합니다.
보안 경고가 너무 많아 부담스럽습니다.	IT 보안 관리자는 하루에 100건의 알림을 처리할 때도 있는데, 그러한 알림에서 위협에 대해 별다른 정보나 통찰력을 얻지는 못합니다. 관리해야 할 것이 많은데다 빈번한 알림 때문에 진짜 위협과 노이즈를 구별하기가 쉽지 않습니다. 그러나 AMP에서는 알림의 우선 순위를 정하여 위협 심각도, 시스템 노출 상황, 시스템 시간에 따라 해당 환경에 가장 시급한 문제를 표시합니다. 뿐만 아니라 AMP는 위협에 대해 "알림"을 보낼 뿐 아니라 "보안 침해 지표"도 제공하며, 보안 침해 지표를 통해 파일 및 텔레메트리 이벤트의 상관관계를 조사하고 잠재적인 활성 보안 침해로 우선순위를 지정합니다. Cisco AMP에서는 여러 소스의 보안 이벤트 데이터(예: 침입, 악성코드 이벤트)를 대상으로 그 상관 관계를 자동으로 파악하여 보안 팀이 해당 이벤트와 더 큰 규모의 연계 공격의 관계를 파악하고 고위험 이벤트의 우선 순위를 지정하는 데 도움이 됩니다. AMP에서 환경 전반의 엔드포인트 및 모바일 디바이스, 네트워크 어플라이언스, 방화벽, 기타 보안 제어 지점으로부터 데이터를 수집하고 그 상관 관계를 파악하므로 IT 환경 각처에 분산된 여러 악성코드가 다중 공격이 아닌 단일 공격의 일부로 연계될 때를 알려줄 수 있습니다.

고객 당면 과제	Cisco AMP 솔루션
IT 환경에 서로 다른 벤더의 보안 제품이 다수 구축된 상태입니다. 대부분은 서로 통신하지 않습니다.	서로 다른 벤더의 여러 보안 제품을 구축하면 서로 통신하지 않거나 정보를 공유하지 않을 수 있습니다. 그러면 위협을 찾아내 억제하는 데 더 많은 시간이 걸립니다. 예를 들어 어떤 엔드포인트 제품이 엔드포인트에서 위협을 찾아내고도 네트워크 어플라이언스에 알리지 않으면 그 위협은 네트워크에 머무르면서 다른 엔드포인트를 감염시킬 수 있습니다. 혹은 네트워크에서 명령 및 제어 콜백을 발견했는데 엔드포인트에서는 이를 파악하지 못한 경우, 통신을 종료하더라도 엔드포인트에서 확인되지 않은 이 악성코드를 제거하지 못할 수 있습니다. 그러나 Cisco AMP는 모든 구축 유형 및 기타 보안 디바이스 전반에서 정보를 공유합니다. AMP for Endpoints 구축은 AMP for Networks 구축, AMP for Email Security Appliance 구축, 기타 Cisco 보안 툴, 이를테면 방화벽, 웹/이메일 어플라이언스 등과 정보를 공유합니다. 위협이 한 곳에서 확인된 경우, 전체 보안 아키텍처에서 해당 사실을 알게 됩니다. 그러면 TTD(time to detection) 및 TTR(time to remediation)이 단축됩니다.
여러 보안 제품을 관리하려면 상당한 수고와 시간이 필요합니다.	물론 서로 다른 벤더의 여러 보안 제품을 관리하려면 관리 부담, 다중 인터페이스, 유지 보수 비용, 학습 부담을 감수해야 합니다. 이는 이종 제품의 구현, 관리, 실행 비용의 상승으로 이어집니다. Cisco의 통합형 AMP 솔루션(및 기타 보안 솔루션)은 모두 통신하고 연동하면서 더 관리하기 쉬운 보안 아키텍처를 탄생시키고 TCO(total cost of ownership) 및 OpEx도 줄입니다.
최상의 보안 툴을 원하며 운영 효율성도 높이고자 합니다. 그와 더불어 기존의 보안 투자도 최적화할 필요가 있습니다.	일반적으로 AMP for Endpoints는 안티바이러스 툴을 포함하여 엔드포인트에서 실행되는 다른 애플리케이션과 효과적으로 연동합니다. 저용량 커넥터를 통해 각종 디바이스 및 운영 체제(Windows, Mac, Linux, Android, 가상 머신)에 설치할 수 있습니다. Cisco AMP for Networks는 FirePOWER NGIPS를 통해 네트워크에 인라인으로 배치됩니다. Threat Grid(단일 솔루션에서 동적 악성코드 분석 및 위협 인텔리전스 제공)를 기존 AMP 인프라뿐 아니라 다른 보안 기술, 즉 방화벽, SIEM(security information and event management) 시스템, 프록시, 게이트웨이 등과 손쉽게 통합할 수 있습니다. 또한 Security Optimization Service를 이용하여 보안 설계 계획에서 최신 위협을 처리할 수 있으며, 보안 인프라에서 새로 발견된 공격을 방어하도록 할 수 있습니다.
무언가가 침투하면 시스템 리이미징을 반복합니다. 이는 관리의 어려움이 있으며 비즈니스 크리티컬 업무의 속도를 떨어뜨립니다.	항상 시스템을 리이미징할 필요 없습니다. AMP에서는 마우스 버튼을 한 번만 클릭하여 여러 엔드포인트에서 한꺼번에 파일을 치료하고 메모리에서 지울 수 있습니다. AMP는 악성코드의 출처, 경로, 기능을 파악하므로 확장 네트워크의 전반에서 그 위치를 찾아내고 부수적 피해 없이 또는 최소화하면서 제거할 수 있습니다.
동일한 유형의 악성코드가 계속 공격합니다.	Cisco AMP는 끊임없이 학습합니다. 본 것을 기억하면서 반복된 공격을 차단합니다. AMP는 위협을 발견하면 위협 인텔리전스로 카탈로그화하고 클라우드에 저장합니다. 다음에 AMP에서 해당 위협 또는 위협 유형을 또 발견하면 수많은 인텔리전스 소스에서 수집한 AMP 클라우드의 인텔리전스와 상호 참조한 다음 악성으로 확인된 파일은 자동으로 차단할 수 있습니다.
사용하기 편리하고 팀에게 신속하게 교육할 수 있는 툴이 필요합니다.	Cisco AMP는 사용하기 편리하고 직관적이며 클라우드 기반이고 인터넷과 웹 브라우저만 있으면 어디서나 액세스할 수 있습니다. 컨트롤, 기능, 위협 인텔리전스가 평이한 영어로 작성되어 있습니다. 또한 Cisco는 Cisco AMP 제품의 사용법을 학습할 수 있는 고객 대상 실습 교육도 제공합니다. Cisco AMP for Endpoints를 얼마나 쉽게 관리할 수 있는지 이 데모에서 확인하십시오.
보안 분석가가 악성코드를 조사하는 데 시간이 오래 걸립니다.	악성코드 분석은 매우 복잡하고 번거로운 작업입니다. Threat Grid는 자동화된 악성코드 분석 기능을 제공하므로 초보 분석가도 더 빨리 정보에 근거한 결정을 내릴 수 있으며, 티어 3 리버스 엔지니어에게 유용한 컨텍스트 기반의 고급 데이터를 제공할 수 있습니다. Threat Grid는 Cisco 보안 제품에 통합되어 이러한 프로세스를 자동화합니다. 타사 제품에 대해서는 REST API를 통해 분석을 위한 제출을 자동화할 수 있어 수작업으로 제출할 필요가 없으며 기존 보안 투자의 효과를 높입니다.

실천 방안

1. **연락:** 다음 시나리오에 해당하는 고객을 공략합니다(대상 고객 섹션 참조).
   - 신규 고객 발굴
   - 경쟁사 고객 마이그레이션
   - 기존 Cisco 고객 업셀
   - 서드파티를 통해 고객 업셀
2. **해결 과제를 파악하고 Cisco AMP와 연결:** 고객의 요구 사항 및 주요 보안 과제를 이해합니다. 그런 다음 AMP로 어떻게 이러한 문제를 해결할 수 있는지 보여줍니다. 판매에 도움이 되는 아래의 리소스 목록을 활용하십시오.
3. **구축 옵션 평가:** AMP 기술은 각기 다른 보안 요구 사항에 따라 다양하게 사용될 수 있습니다. 다양한 AMP 구축, 즉 AMP for Endpoints, AMP for Networks, Advanced Malware Protection Private Cloud Virtual Appliance, Threat Grid에 대한 통찰력을 제공합니다. 구축 속도를 높이고 고객의 전반적인 AMP 경험을 최적화하기 위해 통합 서비스 및 매니지드 서비스를 포지셔닝할 수 있습니다.
4. **레퍼런스 세일즈.** 다른 고객이 어떻게 AMP를 사용하여 조직을 보호하고 있는지 AMP 고객 사용 후기를 활용하여 보여줍니다.
5. **체험.** 고객이 AMP 기술을 직접 사용해보도록 권장합니다. dcloud.cisco.com에서 대화형 기능으로 기술을 체험하고 Cisco의 AMP 전문가와 교류하며 POV에 참여할 수 있습니다.
6. **경쟁사 배제.** 경쟁이 치열한 프로젝트라면 NSS Labs BDS 테스트 결과와 같은 경쟁 관련 리소스를 활용하여 AMP의 우수성을 입증합니다.
7. **금융 상품 제공.** 전략적 관점에서 기술 금융 상품을 활용하십시오. Cisco Capital® 금융 상품 옵션을 최대한 활용하십시오. 자세한 내용은 www.ciscocapital.com을 참조하십시오.
8. **시스코 서비스에 연결.** 보안 서비스를 포함하는 완전한 솔루션을 제공하여 고객에게 더 큰 비즈니스 가치를 제공합니다. AMP 통합 서비스, Cisco에서 제공하는 Cisco 브랜드 서비스, Cisco의 서비스에 파트너의 전문성을 추가할 수 있는 Cisco Collaborative Services 등 다양한 서비스 옵션이 있습니다. 자세한 내용은 www.cisco.com/go/attachservices를 참조하십시오.

추가 리소스

Cisco.com 페이지

- AMP(Advanced Malware Protection)
- 솔루션 페이지
- AMP for Endpoints
- AMP for Networks
- AMP Private Cloud Virtual Appliance
- Threat Grid
  - 클라우드 구축
  - 온프레미스 구축

솔루션 및 제품 개요 비디오

- AMP for Endpoints 개요 비디오
- AMP for Networks 개요 비디오
- Threat Grid 개요 비디오
- John Chambers가 말하는 Cisco 보안 및 AMP
- AMP 4분 개요: IT 보안 전문가 Tom의 요약
- Security Everywhere 비디오
- 보안에 대한 Cisco 경영진의 관점

데모

- AMP for Endpoints 데모
- 사고 대응을 위한 Threat Grid
- Threat Grid: 포털 개요 및 API 데모
- AMP on TechWiseTV(2015년 6월)
- AMP for Endpoints 데모(2014)
- AMP for Networks 데모(2014)

고객 사용 후기 비디오

- AMP의 모든 고객 사용 후기 재생 목록

경쟁 제품

- csoc.cisco.com

데이터 시트, 한눈에 보기(AAG), 인포그래픽, 백서

- AMP 솔루션 개요
- AMP 솔루션 AAG
- AMP for Networks: 데이터 시트 | AAG
- AMP for Endpoints: 데이터 시트 | AAG
- AMP Private Cloud Virtual Appliance: 데이터 시트
- Threat Grid 솔루션 개요
- Threat Grid—Appliance: 데이터 시트 | AAG
- Threat Grid—Cloud: 데이터 시트
- 악성코드 인포그래픽
- Visibility and Control to Prevent, Detect, and Remediate Advanced Malware Everywhere
- Security Everywhere 백서 (게이트 있음)
- Security Everywhere 백서(직접 연결)

세일즈 및 파트너 리소스

- AMP BDM and TDM 프레젠테이션
- Cisco 및 파트너 AMP 솔루션 통화 가이드
- AMP 및 Threat Grid 세일즈 개요
- AMP 및 Threat Grid 기술 개요
- AMP 주문 가이드

서드파티 검증

- Gartner Video-on-Demand: Cisco AMP로 지능형 위협에 맞서기 위한 전략
- Infonetics와 Cisco: 지능형 악성코드 및 위협에 맞서기 위한 실용적 전략
- NSS Labs Breach Detection Systems Report 2015

지능형 악성코드 차단 관련 자료의 리소스 사이트

- 파트너 리소스 링크
- 세일즈 리소스 링크
- 중견기업 비즈니스 솔루션

서비스

- 자세한 내용은 Security Services 참조.