Cisco AMP Threat Grid - 어플라이언스

악성코드와 지능형 위협에 맞서려면 최상의 보안 툴이 필요합니다. Cisco® AMP(Advanced Malware Protection) Threat Grid 어플라이언스는 최고의 악성코드 차단 솔루션인 통합 악성코드 분석과 컨텍스트 기반 인텔리전스를 결합했습니다. 보안 전문가가 능동적으로 사이버 공격을 방어하고 신속하게 복구할 수 있도록 지원합니다.

제품 개요

AMP Threat Grid 어플라이언스는 온프레미스 고급 악성코드 분석 기능을 심층 위협 분석 및 콘텐츠와 함께 제공합니다. 이 어플라이언스에 악성코드 샘플을 제출하여 규정을 준수하고 정책에 따라 제한할 수 있습니다. AMP Threat Grid에서 지속적인 단방향 스트림을 통해 통합 데이터를 제공하므로 악성코드를 차단하고 조직의 요구 사항을 준수할 수 있습니다.

AMP Threat Grid 어플라이언스에서는 최고의 보안 기술을 자랑하는 독자적인 고정 및 동적 분석 기술로 모든 샘플을 분석할 수 있습니다. 그 결과와 수억 개의 다른 분석된 악성코드 아티팩트의 상관성을 분석하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 보안팀은 관찰된 활동 및 특성의 샘플 하나를 수백만 개의 다른 샘플과 신속하게 상관 분석하여 이력 및 글로벌 컨텍스트에서 그 동작을 철저하게 파악할 수 있습니다. 이 기능으로 표적 공격뿐 아니라 지능적 악성코드의 위협까지 효과적으로 방어할 수 있습니다. AMP Threat Grid의 상세 보고서에서는 중요 행동 지표를 식별하고 위협 점수를 부여하여 지능적 공격의 우선 순위를 신속하게 결정하고 그로부터 복구할 수 있게 합니다.

기능 및 장점

AMP Threat Grid 어플라이언스의 기능과 이점이 표 1에 나와 있습니다.

표 1. Cisco AMP Threat Grid 어플라이언스의 기능 및 이점

기능	혜택
온프레미스 어플라이언스	최고의 보안 기술이 구현된 안전한 온프레미스 환경에서 고정 및 동적 악성코드 분석을 수행합니다. 기존 보안 인프라와 손쉽게 통합됩니다. 악성코드 분석 결과를 저장할 안전한 온프레미스 스토리지를 제공합니다.
고급 분석	악성코드 동작에 대해 종합적인 관점에서 보안 통찰력을 제공하며 AMP Threat Grid의 광범위한 데이터베이스에 있는 샘플 소스 및 관련 동작 정보에 직접 연결됩니다. 모든 정보 및 분석 결과에 편리하게 액세스하여 추가 조사를 수행할 수 있습니다.
고급 동작 지표	뛰어난 정확성으로 오탐 가능성이 낮고 실행 가능한 350여 개의 고급 행동 지표를 분석합니다. 각종 악성코드 그룹 및 악성 동작을 포괄하는 고급 고정 및 동적 분석을 통해 종합적인 지표를 생성합니다. 위협에 대한 가장 폭넓은 컨텍스트를 제공하여 신속하고 자신 있는 의사 결정을 지원합니다.
위협 점수	관찰된 동작의 신뢰도 및 심각도, 이력 데이터, 빈도, 클러스터링 지표 및 샘플을 고려하는 독자적인 분석 및 알고리즘으로 위협 점수를 자동 산정합니다. 각 샘플의 악성 동작 수준을 반영하여 위협에 대한 신뢰할 수 있는 우선 순위를 지정합니다. 더 효과적으로 위협의 우선 순위를 결정하여 Cisco AMP Threat Grid 피드를 사용하는 악성코드 분석가, 사고 대응자, 보안 엔지니어링팀, 제품의 효율성 및 정확도를 높입니다.
통합을 위한 API	기존 보안 및 네트워크 인프라에서 신속하고 간편하게 위협 인텔리전스를 운용합니다. AMP Threat Grid의 REST(representational state transfer) API와 신속하고 편리하게 통합할 수 있습니다. 게이트웨이, 프록시, SIEM(security information and event management) 플랫폼을 비롯한 각종 서드파티 제품에 대한 통합 지침을 제공합니다.

종합적인 온프레미스 악성코드 분석

규정 및 정책에 따라 클라우드에 악성코드 샘플을 제출하는 데 제약이 있는 기업의 경우 AMP Threat Grid의 전용 어플라이언스를 사용하여 로컬에서 AMP Threat Grid의 통합 위협 인텔리전스를 십분 활용하면서 악성코드를 분석할 수 있습니다. AMP Threat Grid는 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 매월 수백만 개의 샘플을 분석하고 테라바이트 단위의 악성코드 분석을 정제하여 실행 가능한 고급 인텔리전스를 생성합니다.

보안팀은 관찰된 악성코드 샘플의 활동과 특성을 수백만 개의 다른 샘플과 신속하게 상관 분석하여 이력 및 글로벌 컨텍스트에서 그 동작을 철저하게 파악함으로써 표적 공격과 지능적 악성코드의 더 광범위한 위협 모두에 효과적으로 대처할 수 있습니다. AMP Threat Grid의 상세 보고서는 주요 행동 지표를 위협 점수와 함께 표시하여 정확하고 신속하게 우선 순위에 따라 지능적 악성코드를 분류하고 그로부터 복구할 수 있도록 지원합니다. 다음과 같은 분석 기능이 제공됩니다.

- 악성코드의 동작을 완전히 파악하는 동적 및 고정 분석 엔진
- 네트워크 트래픽을 포함한 모든 악성코드 샘플 활동에 대한 자세한 분석 보고서
- SOC(보안 운영 센터) 분석가, 악성코드 분석가, 포렌식 분석가를 위한 사용자 인터페이스 워크플로

라이센스

표 2에서 보여주는 것처럼 Cisco AMP Threat Grid 어플라이언스 라이센스는 1일 기준으로 분석하는 파일의 최대 개수를 기준으로 합니다.

표 2. Cisco AMP Threat Grid 어플라이언스 모델 및 라이센스

	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
1일 기준 분석하는 파일의 최대 개수	1500	5000

제품 사양

제품 사양이 표 3에 나와 있습니다.

표 3. Cisco AMP Threat Grid 어플라이언스 제품 사양

기능	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
폼 팩터	1RU(1 rack unit)	1RU
네트워크 인터페이스	10GB 듀얼 구리	10GB 듀얼 구리
전원 옵션	AC 또는 DC	AC 또는 DC

주문 정보

Cisco AMP Threat Grid 어플라이언스를 주문하려면 Cisco 주문 홈 페이지를 방문하십시오. 표 4에 주문 정보가 나와 있습니다.

표 4. Cisco AMP Threat Grid 어플라이언스 주문 정보

부품 번호	제품 설명
Cisco AMP Threat Grid 5000 Appliance and Subscription	
TG5000-BUN	Cisco AMP Threat Grid 5000 Appliance and Subscription Bundle
TG5000-K9	Cisco AMP Threat Grid 5000 Appliance with Software
L-TG5000-1Y-K9	Threat Grid Content Subscription License for 5000 Model, 1 Year

부품 번호	제품 설명
L-TG5000-3Y-K9	Threat Grid Content Subscription License for 5000 Model, 3 Year
Cisco AMP Threat Grid 5500 Appliance and Subscription	
TG5500-BUN	Cisco AMP Threat Grid 5500 Appliance and Software Bundle
TG5500-K9	Cisco AMP Threat Grid 5500 Appliance with Software
L-TG5500-1Y-K9	Threat Grid Content Subscription License for 5500 Model, 1 Year
L-TG5500-3Y-K9	Threat Grid Content Subscription License for 5000 Model, 3 Year

Cisco 및 파트너 서비스

Cisco 및 Cisco 공인 파트너의 서비스를 이용하여 AMP Threat Grid의 고급 위협 피드 및 REST API와의 통합을 계획하고 구현할 수 있습니다. 계획 및 설계 서비스는 기존 인프라, AMP Threat Grid 고급 피드 형식, 운영 프로세스에 따라 조정되므로 고급 위협 피드를 가장 효과적으로 활용할 수 있습니다.

다음 단계

Cisco AMP Threat Grid 통합 악성코드 분석 및 위협 분석에 대한 자세한 내용은 http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html을 참조하십시오.

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 C78-733667-00 01/15