Cisco AMP Threat Grid - 어플라이언스

Cisco® AMP(Advanced Malware Protection) Threat Grid 어플라이언스는 최고의 악성코드 차단 솔루션 중 두 개인 통합 악성코드 분석과 상황 기반 인텔리전스를 결합한 솔루션입니다. 보안 전문가가 사이버 공격을 능동적으로 방어하고 신속하게 복구할 수 있도록 지원합니다.

제품 개요

AMP Threat Grid 어플라이언스는 온프레미스 지능형 악성코드 분석을 심층 위협 분석 및 콘텐츠와 함께 제공합니다. 규정준수 및 정책 제한사항이 있는 기업의 경우 샘플을 어플라이언스에 제출하여 악성코드를 로컬에서 분석할 수 있습니다.

AMP Threat Grid 어플라이언스에서는 독자적이며 고도로 안전한 정적 및 동적 분석 기술을 사용하여 모든 샘플을 분석할 수 있습니다. 수억 개의 다른 분석된 악성코드 아티팩트의 기록 내역과 전체적인 상황에서 도출된 행동 지표를 바탕으로 한 결과의 상관관계를 연구하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 이 기능을 통해 타기팅 공격뿐 아니라 지능형 악성코드의 위협까지 효과적으로 방어할 수 있습니다. 또한 중요 행동 지표 식별, 위협 점수 할당 등 AMP Threat Grid의 상세 보고서를 활용하면 지능형 공격의 우선순위를 신속하게 결정하고 복구할 수 있습니다.

기능 및 이점

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

표 1. 기능 및 이점

기능	이점
GloveBox	GloveBox는 네트워크가 감염될 위험 없이 악성코드를 분석하도록 안전한 환경을 제공하는 사용자 인터렉션 툴입니다. 툴이 어플라이언스에 내장되어 있으므로 분석가는 샘플이 분석되는 동안 애플리케이션 열기, 대화 상자 클릭, 심지어 필요한 경우에는 가상 머신 리부팅까지 샘플과 상호작용할 수 있습니다.
온프레미스 어플라이언스	데이터 기밀을 유지하기 위해 안전하고 고도의 보안이 된 온프레미스 정적 및 동적 악성코드 분석을 제공합니다. 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 행동 지표	뛰어난 정확성으로 오탐 가능성이 거의 없는 실행 가능한 700여 개의 고급 행동 지표를 분석합니다. 각종 악성코드 그룹 및 악성 동작을 포괄하는 고급 정적 및 동적 분석을 통해 종합적인 지표를 생성합니다. 위협에 대한 가장 폭넓은 상황을 제공하여 신속하고 자신 있는 의사 결정을 할 수 있도록 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 행동 수준을 반영하여 위협에 대한 신뢰할 수 있는 우선순위를 지정합니다. 더 효과적으로 위협의 우선순위를 결정하여 Cisco AMP Threat Grid 피드를 사용하는 악성코드 분석가, 사고 대응자, 보안 엔지니어링 팀, 제품의 효율성 및 정확도를 향상합니다.
원격 업데이트	수동 업데이트 기능이 포함되어 있어 최신 기술 자료를 보장하는 동시에, 기업 또는 규정 정책을 준수하여 모든 정보를 논리적 범위 내에서 유지할 수 있도록 합니다.
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

클라우드에 악성코드 샘플을 제출하는 데 있어 규정준수 및 정책 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.

보안 팀은 관찰된 악성코드 샘플의 활동과 특성을 수백만 개의 다른 샘플과 신속하게 상관 분석하여 이력 및 글로벌 상황에서 그 동작을 철저하게 파악함으로써 타기팅 공격과 지능형 악성코드의 더 광범위한 위협 둘 다에 효과적으로 대처할 수 있습니다. AMP Threat Grid의 상세 보고서는 주요 행동 지표를 위협 점수와 함께 표시하여 정확하고 신속하게 우선순위에 따라 지능형 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

라이선싱

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

표 2. 모델 및 라이선싱

	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
1일 기준 분석하는 파일의 최대 개수	1500	5,000

제품 사양

제품 사양이 표 3에 나와 있습니다.

표 3. 제품 사양

특성	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
폼 팩터	1RU(1 rack unit)	1RU
규격	1.7 x 16.9 x 29.8인치(H x W x D)	1.7 x 16.9 x 29.8인치(H x W x D)
네트워크 인터페이스	2 x 1GB Copper + SFP+	2 x 1GB Copper + SFP+
CIMC 인터페이스	1GB Copper	1GB Copper
전원 옵션	770W AC 또는 1050W DC	770W AC 또는 1050W DC

환경 사양

환경 사양이 표 4에 나와 있습니다.

표 4. 환경 사양

	Cisco AMP Threat Grid 5004	Cisco AMP Threat Grid 5504
온도: 작동	41 - 95°F(5 - 35°C)(작동, 해수면, 팬 고장(fan fail) 없음, CPU 속도 제한 터보 모드 없음)	41 - 95°F(5 - 35°C)(작동, 해수면, 팬 고장(fan fail) 없음, CPU 속도 제한 터보 모드 없음)
온도: 비작동	-40 ~ 149°F(-40 ~ 65°C)	-40 ~ 149°F(-40 ~ 65°C)
습도: 작동	10 - 90% 비응결	10 - 90% 비응결
습도: 비작동	5 - 93% 비응결	5 - 93% 비응결
고도: 작동	0 - 10,000 피트(0 - 3000m). 최대 주변 온도는 300m 당 1°C씩 하강	0 - 10,000 피트(0 - 3000m). 최대 주변 온도는 300m 당 1°C씩 하강
고도: 비작동	0 - 40,000 피트(12,000m)	0 - 40,000 피트(12,000m)

주문 정보

Cisco AMP Threat Grid 어플라이언스를 주문하려면 Cisco 주문 홈 페이지를 방문하십시오. 주문 정보는 표 5를 참조하십시오.

표 5. 주문 정보

부품 번호	제품 설명
Cisco AMP Threat Grid 5004 어플라이언스 및 서브스크립션	
TG5004-BUN	Cisco AMP Threat Grid 5004 어플라이언스 및 서브스크립션 번들
TG5004-K9	Cisco AMP Threat Grid 5004 어플라이언스(소프트웨어 포함)
L-TG5004-1Y-K9	5004 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 1년
L-TG5004-3Y-K9	5004 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 3년
L-TG5004-5Y-K9	5004 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 5년
Cisco AMP Threat Grid 5504 어플라이언스 및 서브스크립션	
TG5504-BUN	Cisco AMP Threat Grid 5504 어플라이언스 및 소프트웨어 번들
TG5504-K9	Cisco AMP Threat Grid 5504 어플라이언스(소프트웨어 포함)
L-TG5504-1Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 1년
L-TG5504-3Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 3년
L-TG5504-5Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 5년

Cisco 및 파트너 서비스

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

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.

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 C78-733667-04 11/16