Cisco AMP Threat Grid

주문 가이드

2016 년 12 월

이 주문 가이드는 Cisco 영업 팀, 파트너 및 총판사를 위해 제작되었으며 공개적인 사용 및 배포를 금지합니다. 문의 사항을 보내기 위한 이메일: tgsales@cisco.com

전화: 무료 전화(미국): +1-800-225-0905 해외: +1-408-902-4872 또는 8-902-4872(Cisco 내부용)

실시간 채팅(예: Click-to-Chat): http://tinyurl.com/ciscosac

목차

소개

이 주문 가이드는 Cisco® AMP Threat Grid 솔루션을 주문하는 Cisco 영업 팀, 파트너 및 총판사의 참조를 위해 작성되었습니다. 이 가이드는 다음과 같은 도움을 제공합니다.

- Cisco AMP Threat Grid 제품 및 서비스 솔루션 이해
- 구체적인 Cisco AMP Threat Grid 솔루션에 대한 이해 및 고객에게 적합한 솔루션 파악
- 주문이 거부될 위험을 줄이기 위해 부품의 수량과 종류를 올바르게 선택했는지 확인
- 이러한 솔루션과 관련하여 Cisco Commerce Workspace 및 Cisco Service Contract Center에서 진행되는 견적에서 이행까지 전체 프로세스에 대한 정보 제공

대상

이 가이드는 Cisco 글로벌 가격 리스트에 명시된 Cisco 보안 제품 및 서비스를 판매할 자격을 갖춘 Cisco 영업 팀, 파트너 및 총판사를 위해 작성되었습니다.

범위

이 주문 가이드에서는 Cisco 글로벌 가격 리스트를 토대로 Cisco 보안 제품 및 서비스의 견적을 작성하고 주문하며 가격을 책정하는 방법에 대해 알려드립니다.

솔루션 개요

2014년 6월 16일 Cisco는 악성코드 분석 및 위협 인텔리전스 테크놀로지를 제공하는 회사인 ThreatGRID의 인수를 완료했습니다. ThreatGRID의 프라이빗 및 퍼블릭 클라우드 기반 기술은 보안 팀이 지능형 사이버 공격 및 악성코드 보안 침해를 사전에 방어하고 빠르게 대응하기 위해 사용할 수 있는 실행 가능한 지표 및 분석을 동적 악성코드 분석과 결합합니다. ThreatGRID 솔루션은 Cisco® Advanced Malware Protection(AMP) 포트폴리오를 보완하고, 프라이빗 클라우드 제품은 엄격한 사내 데이터 보존 요건을 가진 고객을 보호하는 Cisco의 능력을 확장합니다.

Cisco는 ThreatGRID(지금은 Cisco SBG(Security Business Group)의 일부)를 인수함으로써 고객 회사의 주요 과제인 고도로 안전하고 지능적인 환경을 제공하려는 노력에 박차를 가할 수 있게 되었습니다. Cisco는 ThreatGRID와의 결합을 통해 확장된 네트워크 전체에서 데이터를 수집하고 상호 연결하는 기존의 강력한 기능을 더욱 강화하고, 교묘한 지능형 사이버 위협을 식별하고, 고객을 위한 종합적인 보안 솔루션을 제공할 것입니다.

새로운 Cisco 제품 이름

2014년 7월 Cisco는 ThreatGRID 제품 및 솔루션의 브랜드를 Cisco AMP Threat Grid로 변경하기 시작했습니다. 이제 모든 Cisco AMP Threat Grid 제품에 이 이름이 사용됩니다.

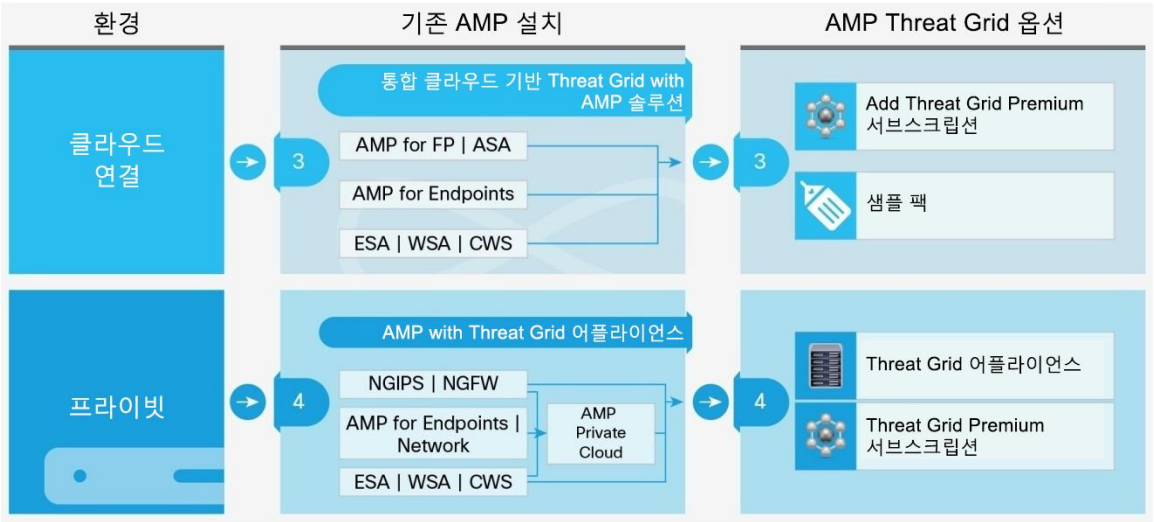
이름 및 브랜드와 관련하여 더 궁금한 사항이 있으면 Cisco 보안 영업 담당자 또는 파트너사에 직접 문의하시기 바랍니다.

제품에 대한 이해

Cisco AMP Threat Grid는 심층적인 지능형 악성코드 분석과 상황에 맞는 인텔리전스를 제공하여 고객이 환경에서 악성코드를 더 잘 이해하고 대처하도록 지원합니다. Cisco AMP Threat Grid는 독립형 솔루션으로 사용할 수도 있고 다른 Cisco AMP 솔루션의 구성 요소로 사용할 수도 있습니다. Cisco AMP Threat Grid는 클라우드의 SaaS(Software-as-a-service) 및 온프레미스 딜리버리 모델 둘 다를 통해 제공됩니다(그림 1과 그림 2).

그림 1. Cisco AMP Threat Grid 구축 모델: 독립형

그림 2. Cisco AMP Threat Grid 구축 모델: 기존의 AMP 설치 이용



Cisco AMP Threat Grid는 빅 데이터 접근 방식을 고급 회피 저항 기법과 결합하여 수신된 샘플을 분석합니다. 그 결과와 수억 개의 다른 분석된 악성코드 아티팩트의 상관성을 연구하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 고객은 관찰된 악성코드 샘플의 활동과 특성을 수백만 개의 다른 샘플과 신속하게 상관 분석하여 이력 및 글로벌 상황에서 샘플 동작을 철저하게 파악함으로써 타기팅 공격과 지능형 악성코드의 더 광범위한 위협 둘 다에 효과적으로 대처할 수 있습니다.

Cisco AMP Threat Grid는 고객이 주요 행동 지표를 위협 점수와 함께 식별하도록 도와주는 자세한 보고서를 제공하여, 정확하고 신속하게 우선순위에 따라 지능형 공격을 분류하고 그로부터 복구할 수 있도록 지원합니다.

- 지표는 분석에 상황을 적용하는 첫 번째 단계입니다. Cisco AMP Threat Grid 는 악성코드 제품군, 악의적인 행동 등을 다루는 정적 및 동적 분석을 통해 생성된 700 여 개의 지표를 제공합니다. 새로운 지표가 정기적으로 추가됩니다. Cisco 가 지표에서 제공하는 실행 가능한 정보 및 자세한 설명을 통해, 고객은 올바른 데이터를 활용하여 악성코드 및 기타 다양한 사용 기법에 대한 지식과 통찰력을 확보하는 한편 상황에 빠르게 대처할 수 있습니다.
- Cisco AMP Threat Grid에서 제공하는 위협 점수는 고객에게 특정 샘플이 얼마나 악의적인가를 알려줍니다. 이 점수는 관찰된 동작의 신뢰도 및 심각도, 이력 데이터, 빈도, 클러스터링 지표 및 샘플을 고려하는 독자적인 분석 및 알고리즘으로부터 산정됩니다. Cisco AMP Threat Grid의 위협 점수를 통해 고객은 위협의 우선순위를 효과적으로 설정하여 악성코드 분석가, 사고 대응 담당자, 보안 엔지니어 팀의 효율성과 정확성을 높일 수 있습니다.

잘 정의된 REST API를 통해서도 Cisco AMP Threat Grid의 집단 지성 및 결과를 사용할 수 있습니다. 고객은 또한 이 API를 사용하여 샘플을 제출하고 결과를 검색할 수 있습니다. API를 통해 일괄 처리, 맞춤형 위협 피드와 같은 기타 고급 인텔리전스 서비스도 이용할 수 있습니다.

Cisco AMP Threat Grid - 클라우드 서브스크립션 개요

Cisco AMP Threat Grid는 매월 600만 개가 넘는 샘플을 분석하는 클라우드 서비스입니다. 전 세계에서 수집되는 악성코드 샘플을 분석하여 매일 수 테라바이트 규모의 풍부하고 실행 가능한 콘텐츠가 생성됩니다. 이 기능을 통해 고객은 글로벌 위협에 대한 보안 운영과 적용 범위를 엄청나게 확장할 수 있습니다.

또한 Cisco AMP Threat Grid 고객은 샘플을 클라우드 포털에 직접 제출하거나, Cisco AMP Threat Grid API를 사용하여 자동화된 프로세스를 통해 제출할 수 있습니다.

전체 Cisco AMP Threat Grid 서비스는 Cisco AMP 솔루션(예: Cisco AMP for Endpoints, AMP for Networks, AMP for Content)을 통해 사용 가능한 기본적인 정적 및 동적 분석 기능을 뛰어넘는 완벽한 보완 기능을 제공합니다. 향상된 기능에는 프로세스 매핑 및 레지스트리 분석을 비롯한 심층 분석과 결과, 네트워크 연결, 해당 환경에서의 악성코드 실행 동영상, 실행 중인 샘플과 상호작용하는 기능, API 액세스 등이 포함됩니다(해당하는 경우). 분석한 인텔리전스 데이터에 대한 배치 피드도 이용 가능하며 더 광범위한 Threat Grid 데이터에서 맞춤형 피드를 생성할 수도 있습니다.

표 1에 나와 있듯이, 모든 클라우드 서비스 요소를 콘텐츠 서브스크립션이라고 합니다. **사용자 1명은 계정 1개와 같습니다. 계정 공유는 허용되지 않습니다.**

표 1. Cisco AMP Threat Grid Premium - Cloud 서브스크립션

부품 번호	설명
L-TG-S1-LIC-K9=	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건
L-TG-1Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 1년
L-TG-3Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 3년
L-TG-5Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 5년
L-TG-S2-LIC-K9=	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건
L-TG-1Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 1년
L-TG-3Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 3년
L-TG-5Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 5년
L-TG-S3-LIC-K9=	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건
L-TG-1Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 1년
L-TG-3Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 3년
L-TG-5Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 5년
L-TG-S4-LIC-K9=	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건
L-TG-1Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 1년
L-TG-3Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 3년
L-TG-5Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 5년

Cisco AMP Threat Grid Premium - Cloud 서브스크립션의 프라이빗 태깅

Cisco AMP Threat Grid는 프라이빗 태깅이라는 기능을 제공하는데, 이 기능을 통해 고객은 AMP Threat Grid 서비스에 제출되는 파일을 조직에 대해 "private"이라고 표시할 수 있습니다. 이 기능은 원하는 고객에게 높은 수준의 프라이버시를 제공합니다.

고객이 프라이빗 태깅을 사용하는 경우, 제출되는 고유한 파일 및 해당 결과는 Cisco AMP 또는 Cisco AMP Threat Grid 가입자로 구성된 글로벌 커뮤니티에서 공유되지 않고, 파일에 "private"이라는 플래그를 지정하여 제출하는 고객만 사용할 수 있습니다. 단, 둘 이상의 고객이 동일한 파일을 제출하는데 한 명은 private으로 표시하고 다른 고객은 표시하지 않는 경우는 예외입니다. 이 경우에는 파일이 더 이상 고유하지 않으므로 private 태그가 지정되지 않은 제출이 우선 적용됩니다. 일반적으로 고객은 어디서나 볼 수 있는 일반적인 파일보다는 고유한 파일에 대해 더 우려합니다. 절대적인 프라이버시를 원하는 고객의 경우 Cisco AMP Threat Grid 어플라이언스를 사용하는 것이 좋습니다.

프라이빗 태깅을 비롯한 모든 클라우드 서비스 요소를 콘텐츠 서브스크립션이라고 합니다(표 2).

표 2. Cisco AMP Threat Grid - Cloud, 프라이빗 태깅 서브스크립션

부품 번호	설명
L-TG-PT-S1-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개
L-TG-PT-1Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 1년
L-TG-PT-3Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 3년
L-TG-PT-5Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 5년
L-TG-PT-S2-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개
L-TG-PT-1Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개, 1년
L-TG-PT-3Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개, 3년
L-TG-PT-5Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개, 5년
L-TG-PT-S3-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개

부품 번호	설명
L-TG-PT-1Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 1년
L-TG-PT-3Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 3년
L-TG-PT-5Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 5년
L-TG-PT-S4-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개
L-TG-PT-1Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 1년
L-TG-PT-3Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 3년
L-TG-PT-5Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 5년

Cisco AMP Threat Grid 온프레미스 어플라이언스

클라우드에 악성코드 샘플을 제출하는 데 컴플라이언스 및 정책 제약이 있는 기업의 경우 Threat Grid의 전용 어플라이언스를 사용하여 로컬에서 클라우드 기능을 십분 활용하면서 분석할 수 있습니다. 로컬 분석 과정에서 제출되거나 생성된 어떤 정보도 조직 외부로 내보내지지 않습니다.

완전히 고립된 환경이 필요한 고객은 인터넷 액세스가 없는 구축 옵션을 이용할 수도 있습니다. 이러한 환경의 고객은 Threat Grid Premium Cloud 인텔리전스의 사용 및 심층 상황 분석을 통해 얻는 효율성과 통찰력의 이점을 활용할 수 없습니다(예: 인터넷 연결을 통해 침투하려고 시도하는 악성코드의 경우).

Cisco Threat Grid AMP 5000 Series 어플라이언스는 현재 사용 가능한 온프레미스 플랫폼입니다.

Cisco AMP Threat Grid 5000 Series 어플라이언스

Cisco AMP Threat Grid 5000 Series 어플라이언스 제품군은 확장 가능한 동일한 하드웨어 플랫폼을 기반으로 두 개의 용량 모델을 제공합니다.

두 어플라이언스 모델의 주요 차이점은 처리할 수 있는 1일 기준 파일 샘플 볼륨의 용량입니다. 5004 Series 모델은 하루 최대 1,500개 파일을 분석할 수 있는 반면, 5504 Series 모델은 하루 최대 5,000개 파일을 분석할 수 있습니다.

5004 Series의 특징은 다음과 같습니다.

- 1RU(1 랙 유닛) 폼 팩터
- 10Gb 듀얼 포트 구리 네트워크 인터페이스
- AC 또는 DC 전원 옵션
- 최신 Cisco AMP Threat Grid 소프트웨어 버전

고객은 1회 업그레이드 라이선스를 구매하여 5004 모델에서 5504 모델로 업그레이드할 수 있습니다. 업그레이드된 콘텐츠 서브스크립션 라이선스(즉, 5504 모델용)도 필요합니다.

편리하고 쉽게 주문할 수 있도록 Cisco AMP Threat Grid 어플라이언스 및 필수 콘텐츠 서브스크립션을 포함하는 번들이 생성되었습니다. 제품 부품 번호는 부록 A에 나와 있으며 "-BUN"으로 끝납니다.

모든 어플라이언스에는 어플라이언스 콘솔에 액세스하기 위한 콘텐츠 서브스크립션 라이선스가 필요합니다. 이 라이선스를 통해 사용자는 복잡한 검색, 데이터 피벗, API 액세스를 실행하여 어플라이언스에 대한 제출 및 제출을 기반으로 하는 결과 검색을 자동화할 수 있습니다(표 3). 현재 어플라이언스와 Threat Grid Premium Cloud 간에는 쿼리 페더레이션이 없습니다. 행동 지표 및 기타 어플라이언스 업데이트는 일정한 간격으로 어플라이언스에 직접 제공됩니다.

표 3. Cisco AMP Threat Grid 5004 & 5504 Series 어플라이언스용 라이선스

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

Cisco AMP Threat Grid – 샘플 팩

Cisco AMP Threat Grid 샘플 팩은 다음 통합 제품 중 하나 이상에 대한 AMP 콘텐츠 라이선스를 구매한 고객이 이용할 수 있는 추가 1일 기준 샘플 용량 라이선스입니다.

- Email Security Appliance
- Cloud Email Security
- Web Security Appliance
- AMP for Endpoints
- AMP for Networks
- Next Gen Intrusion Prevention System
- Next Gen Firewall

샘플 팩은 24시간 기간 동안 분석을 위해 AMP Threat Grid에 제출할 수 있는 샘플 수를 늘리고자 하는 고객을 위한 것입니다. 샘플 팩은 용량만 제공할 뿐이며 추가 보고, 데이터 분석, 반환된 데이터 피벗 기능 등은 제공하지 않습니다. AMP 콘텐츠 라이선스와 통합된 제품이 없는 AMP Threat Grid Premium Cloud 서브스크립션 또는 AMP Threat Grid 어플라이언스에는 샘플 팩을 사용할 수 없습니다.

추가 1일 기준 샘플 용량이 필요하여 Threat Grid 샘플 팩을 구매한 고객은 기존의 모든 통합 제품 1일 기준 샘플 한도 엔타이틀먼트가 단일 조직 계정으로 이동하게 됩니다. AMP Threat Grid Premium Cloud 서브스크립션을 보유한 고객은 1일 기준 샘플 한도가 통합 제품 1일 기준 샘플 한도와 결합되며 AMP Threat Grid 포털을 통해 모든 샘플을 볼 수 있게 됩니다. AMP Threat Grid Premium Cloud 서브스크립션을 통해 제공된 1일 기준 샘플 수를 포함하여 고객이 보유한 총 1일 기준 샘플 수는 조직 계정의 모든 디바이스에서 사용 가능합니다.

AMP Threat Grid 샘플 팩은 통합 제품 AMP 콘텐츠 라이선스 및 AMP Threat Grid Premium Cloud 서브스크립션의 모든 1일 기준 샘플 엔타이틀먼트를 포함하여 조직에서 총 1일 기준 샘플 10,000개까지 누적 가능합니다.

표 4에 나와 있듯이, 모든 샘플 팩 서비스 요소를 라이선스 서브스크립션이라고 합니다.

표 4. Cisco AMP Threat Grid 샘플 팩

부품 번호	설명
L-TGSP-S2-LIC-K9=	Cisco AMP Threat Grid 샘플 팩 라이선스 1일 기준 샘플 500개
L-TGSP-1Y-S2-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 500건, 1년
L-TGSP-3Y-S2-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 500건, 3년
L-TGSP-5Y-S2-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 500건, 5년
L-TGSP-S3-LIC-K9=	Cisco AMP Threat Grid 샘플 팩 라이선스 1일 기준 샘플 1500개
L-TGSP-1Y-S3-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 1500건, 1년
L-TGSP-3Y-S3-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 1500건, 3년
L-TGSP-5Y-S3-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 1500건, 5년
L-TGSP-S4-LIC-K9=	Cisco AMP Threat Grid 샘플 팩 라이선스 1일 기준 샘플 5000개
L-TGSP-1Y-S4-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 5000건, 1년
L-TGSP-3Y-S4-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 5000건, 3년
L-TGSP-5Y-S4-K9	Cisco AMP TG 파일 팩, 1일 기준 제출 5000건, 5년

Cisco AMP Threat Grid API

고객이 방대한 양의 위협을 지속적으로 파악하고 신속하게 대처하도록 지원하기 위해 Cisco AMP Threat Grid는 강력한 API에 대한 액세스를 제공합니다. API는 샘플 제출, 쿼리, 콘텐츠 생성, 데이터 강화를 자동화하며 모니터링, 차단, 네트워크 및 호스트 포렌식을 위한 서드파티 보안 제품과의 인텔리전스 통합도 자동화합니다. 이 기능은 Threat Grid Premium Cloud 서브스크립션 또는 Cisco AMP Threat Grid 5000 Series 어플라이언스에 포함되어 있습니다.

소프트웨어 라이선스, 어플라이언스 및 서브스크립션 옵션 이해

Cisco AMP Threat Grid는 독립형 제품으로 이용할 수도 있고 AMP 콘텐츠 라이선스의 일부로 이용할 수도 있습니다.

- Cisco AMP for Endpoints
- Cisco AMP for Networks
- Cisco Adaptive Security Appliance(ASA) 및 Cisco FirePOWER 어플라이언스
- Next Generation Intrusion Prevention System(NGIPS)
- Cisco Email Security Appliance(ESA)
- Cisco Web Security Appliance(WSA)

Threat Grid Premium Cloud 서브스크립션을 추가한 고객은 AMP Threat Grid Premium - Cloud 포털용으로 프로비전된 계정을 받게 됩니다. 어플라이언스를 주문하면 소프트웨어가 사전 설치된 상태로 배송됩니다.

소프트웨어 서브스크립션 지원

Cisco 보안 소프트웨어 서브스크립션 라이선스는 소프트웨어 서브스크립션 지원을 포함합니다. 이러한 지원은 비즈니스 크리티컬 애플리케이션의 가용성을 유지하고 보안을 강화하며 최적의 성능으로 운영하는 데 매우 중요한 역할을 합니다. 소프트웨어 서브스크립션 라이선스 기간 동안 최신 소프트웨어 업데이트와 주요 업그레이드 릴리스를 적시에 중단 없이 제공받게 됩니다. 이러한 업데이트와 업그레이드 릴리스에는 중대한 아키텍처 변경사항이나 새로운 기능이 포함될 수 있습니다. 소프트웨어 서브스크립션 지원을 통해 최신 버전의 Cisco 보안 솔루션으로 비즈니스 환경을 보호할 수 있습니다. 또한 문제를 신속하게 해결하고, 비즈니스 연속성을 유지하며, 경쟁력을 높이고, 생산성 향상을 통해 한정된 리소스를 최대한 효율적으로 활용하는 데 도움이 되는 다양한 온라인 툴과 커뮤니티에 액세스할 수 있습니다.

이 지원을 통해 고객은 구매한 소프트웨어 서브스크립션의 전체 기간 동안 다음과 같은 서비스를 이용할 수 있습니다.

- 최신 기능 집합으로 애플리케이션의 최적 성능을 유지하기 위한 소프트웨어 업데이트 및 주요 업그레이드
- 신속하고 전문적인 지원을 제공하는 Cisco TAC(Technical Assistance Center) 액세스
- 사내 전문성을 확대하고 비즈니스 민첩성을 높이는 온라인 툴 구축
- 추가 지식 및 교육 기회를 제공하는 협업적 학습

이러한 서비스는 추가 제품이나 이용료 없이 소프트웨어 서브스크립션과 함께 제공받을 수 있습니다.

Cisco AMP Threat Grid 5000에 유효한 Cisco Commerce Workspace 컨피그레이션 샘플

표 4에서는 Cisco AMP Threat Grid 5004 Series 어플라이언스용 Cisco Commerce Workspace 컨피그레이션과 필요한 콘텐츠 서브스크립션을 보여줍니다.

참고: 새로운 주문에서는 하드웨어 및 소프트웨어 서브스크립션이 결합된 번들 제품(BUN)을 주문해야 합니다. 콘텐츠 서브스크립션 및 Cisco SMARTnet™ 지원(CON-SNT-TG5004K9)도 필요합니다. 1 년, 3 년 소프트웨어 또는 5 년 서브스크립션을 선택할 수 있습니다. 기본값은 3 년입니다.

표 5. Cisco AMP Threat Grid 5004 Series 어플라이언스용 Cisco Commerce Workspace 컨피그레이션: 새로운 주문

라인	부품 번호	설명	참고
1.0	**TG5004-BUN**	**Cisco AMP Threat Grid 5004 어플라이언스 및 서브스크립션 번들**	**Cisco AMP 5004 Series용 기본 번들 제품**
1.1	**TG5004-K9**	**Cisco Threat Grid 5504 모델 하드웨어**	**TG5004 하드웨어 어플라이언스**
1.1.0.1	**CON-SNT-TG5004K9**	Cisco SMARTnet 오전 8시~오후 5시(8x5) NBD(익영업일) TG5004 기간: 12개월	포함 - Cisco SMARTnet 지원 계약(하드웨어 및 소프트웨어) – (기간 필요 – 수정 가능)
1.1.1	**CAB-9K12A-NA**	전원 코드, 125VAC 13A NEMA 5-15 플러그, 북미	포함 - 전력 코드 선택 필요
1.1.2	**TG-PWR-AC-770W**	Cisco Threat Grid 770W AC 전원 공급장치	포함 - 전원 공급장치 선택 필요
1.1.3	**TG5004-SW-K9**	5004 모델용 Threat Grid 소프트웨어	포함 - 하드웨어 OS/펌웨어 라이선스
1.1.4	**TG-CPU-E52697E**	2.30GHz, E5-2697 v4, 45MB 캐시, 18 코어, 28 스레드	포함
1.1.5	**TG-MEM-32GB-M4**	32GB DDR4-2400-MHz RDIMM/PC4-17000/듀얼 랭크/x4/1.2v	포함
1.1.6	**TG-RAID-1G-FBWC**	Cisco 12Gbps SAS 1GB FBWC 캐시 모듈(Raid 0/1/5/6)	포함
1.1.7	**TG-RAID-CISCO12G**	Cisco 12G SAS Modular Raid 컨트롤러	포함
1.1.8	**TG-HDD-1.2TB**	1.2TB SATA 10K RPM 12G SAS	포함

라인	부품 번호	설명	참고
1.1.9	**TG-SSD-120GB3510**	Threat Grid 3510 120GB 2.5인치 Enterprise 6G SATA SSD	포함
1.1.10	**TG-10G-NIC**	**Threat Grid X520 듀얼 포트 10GB SFP+ 어댑터**	**포함**
1.2	**L-TG5004-LIC-K9+**	5004 모델용 Threat Grid 콘텐츠 라이선스	어플라이언스 콘텐츠 라이선스 AMP Threat Grid
1.2.0.1	**L-TG5004-3Y-K9**	Cisco Thread Grid 서브스크립션 5004 모델, 콘텐츠 서브스크립션 3년	어플라이언스 콘텐츠 서브스크립션 AMP Threat Grid – (기간 필요 – 수정 가능)
1.3	**GLC-TE=**	카테고리 5 구리선용 1000BASE-T SFP 트렌시버 모듈	어플라이언스 네트워크 카드

Cisco AMP 솔루션 및 Threat Grid

Cisco AMP Threat Grid는 Cisco AMP for Endpoints, Cisco AMP for Networks, ASA with FirePOWER Services, Next Generation Intrusion Prevention System(NGIPS)은 물론 Cisco Email(ESA) 및 Web(WSA) 보안 솔루션에도 사용 가능한 고급 기능을 제공합니다. 이러한 기능을 통해 고객은 지능형 악성코드를 식별하고 처리할 수 있습니다.

Cisco AMP 솔루션은 확장된 네트워크, 엔드포인트, 모바일 디바이스, 가상 환경의 전 범위에서 데이터와 이벤트를 지속적으로 수집합니다. 이 솔루션은 사전 방어(Before), 실시간 조치(During), 사후 대응(After) 등 공격의 전 범위에서 악성코드 및 지속적인 위협을 모니터링하고 제어합니다.

또한 Cisco AMP 솔루션은 빅 데이터 분석, 지속적 분석, 실시간 보안 인텔리전스를 사용하여 악성코드와 지속적인 타기팅 공격을 탐지, 추적, 분석하고 위협 요소를 제거하며, 기업 환경을 보호합니다. 지속적인 분석에서는 특정 시점 탐지에 머무르지 않고 클라우드 기반 빅 데이터 분석 기술을 사용하여 일정 기간 수집된 신규 및 기존 데이터를 지속적으로 재평가하면서 드러나지 않은 공격을 탐지합니다. 그 덕분에 보안 팀은 강력한 회귀적 보안 툴을 통해 제로데이 타기팅 공격에서 흔히 나타나듯, 최초의 탐지 시스템을 통과했으나 나중에 모습을 드러낸 악성코드 공격을 파악할 수 있습니다. 아래의 다양한 AMP 솔루션은 다음과 같은 기능을 제공합니다.

- 악성코드 차단 및 지속적인 분석
- 전파 흔적 분석 툴을 통해 악성코드의 확산 및 활동 추적
- IoC(Indications of compromise, 보안 침해 지표)
- 근본 원인 분석
- 보안 침해 통제(Outbreak control)
- 영향 보고

이러한 AMP 솔루션 기능을 통해 보안 운영 팀은 가장 중대한 위협에 집중할 수 있으므로, 보안의 실효성 및 운영 효율성이 향상되고 사고 대응 시간이 단축됩니다. 이를 Cisco AMP Threat Grid 기능과 결합하여 고객은 지능형 악성코드 처리를 위해 필요한 수준의 가시성과 제어 기능을 확보할 수 있습니다.

Cisco AMP Threat Grid를 사용하면 기본 AMP 기능에서 제공하는 기본적인 분석 보고서 및 위협 점수를 뛰어넘어 더욱 심층적인 분석 및 인텔리전스를 얻을 수 있습니다. 이러한 기능에는 IoC 작성에 사용하기 위한 AMP Threat Grid에서 검색하지 못한 아티팩트, 다른 위협과의 관계를 강조 표시하기 위한 아티팩트 상관관계, Threat Grid Premium Cloud에 포함된 전체 인텔리전스 범위에 대한 액세스 등이 포함됩니다. AMP Threat Grid 어플라이언스 고객은 Cisco 클라우드로 파일을 보내지 않고 로컬에서 분석할 수도 있습니다.

자세한 내용은 Cisco Advanced Malware Protection Ordering Guide를 참조하십시오.

서비스 솔루션의 이해

Cisco Advanced Services

Cisco Global Security Solutions 팀은 종합적인 평가, 설계, 구축 및 최적화 서비스를 제공합니다.

Cisco Advanced Services Transaction

다음 AS-T(Advanced Services Transaction) 솔루션은 맞춤형 범위 및 가격이 적용되어 SOW(작업 명세서)에 기록됩니다. 파트너는 구매 시 시스코 서비스 어카운트 매니저와 협의해야 합니다.

Cisco Security Design Assessment Service

Cisco Security Design Assessment Service는 고객이 조직의 보안 인프라를 파악하고 강화하도록 지원합니다. 조직은 Cisco Security Design Assessment를 통해 다음과 같은 이점을 얻을 수 있습니다.

- 비즈니스 중심의 위험 회피형 접근법을 사용하여 강력하고 확장 가능한 보안 아키텍처를 만들 수 있습니다.
- 아키텍처 네트워크 디바이스 취약점 및 보안 모범 사례와의 차이를 파악하여 인프라를 좀 더 효과적으로 보호할 수 있습니다.
- 보안 위험을 완화하여 직원 생산성, 주요 지적 재산권 및 민감한 고객 데이터를 보호할 수 있습니다.

Cisco Network Device Security Assessment Service

Cisco Network Device Security Assessment Service는 이전 위협 및 새로운 위협으로부터 고객 네트워크를 보호하는 데 도움이 됩니다. Cisco 보안 전문가는 고객과 긴밀하게 협력하여 Cisco 네트워크 인프라 주변의 보호 시스템에서 허점을 파악합니다. 평가는 다양한 업종 및 정부기관에서 풍부한 보안 경험을 쌓은 컨설턴트에 의해 수행됩니다.

Cisco Security Assessment Service for Incident Response

Cisco Security Assessment Service for Incident Response는 고객에게 보안 문제가 발생할 경우 원격 및 현장 지원과 조사 서비스를 제공합니다. 계약 또는 SOW 세부사항이 협상 및 승인되는 동안 이 서비스를 시작할 수 있습니다.

Cisco Advanced Services Transaction을 주문하려면 AS 견적 툴과 표 6의 AS-T 부품 번호를 사용하십시오.

표 6. Cisco AS-T 솔루션 주문 정보

AS-T 부품 번호	설명	가격
AS-SEC-CNSLT(-A, -L)	Cisco Security Design Assessment Service	맞춤형 가격
AS-SEC-CNSLT(-A, -L)	Cisco Network Device Security Assessment Service	맞춤형 가격
AS-SEC-ADVIS	Cisco Security Assessment Service for Incident Response	맞춤형 가격

보안 어카운트 매니저는 정확한 AS-T 견적 및 SOW를 작성할 책임이 있습니다. 또한 Cisco Global Security Solutions 팀의 딜리버리 전문가(고위급 고객 서비스 관리자 또는 고객 서비스 관리자)와 함께 적절한 범위의 SOW를 성공적으로 만들어야 합니다.

고객 및 파트너를 위해 AS-T 견적과 주문을 생성하는 방법에 대해서는 AS-T 판매 및 딜리버리 가이드를 참조하십시오.

참고: Cisco 직원만 이 문서를 이용할 수 있습니다. 파트너는 배정된 Cisco 어카운트 담당자와 함께 SOW를 작성해야 합니다.

AS-T 견적 툴에서 프로젝트의 주요 요건을 입력하면 SOW와 함께 제출해야 할 필수 문서가 제공됩니다.

Cisco Technical Services

Cisco Technical Services는 Cisco Service Contract Center(SCC), Cisco Commerce Workspace 등과 같은 Cisco 툴에서 견적을 작성하고 주문할 수 있습니다. 툴 사용법은 서비스 솔루션, 파트너 유형, 서비스 첨부 시점, 서비스가 신규 서비스인지 기존 서비스 솔루션의 갱신인지에 따라 달라집니다.

Cisco SMARTnet Service

고객은 Cisco 하드웨어용 Cisco SMARTnet Service를 구매합니다(표 7 참조). Cisco SMARTnet Service를 구매한 고객은 다양한 Cisco 지원 툴과 전문 서비스를 이용하여 네트워크 가용성과 성능을 높이는 동시에 운영 비용을 절감할 수 있습니다. Cisco SMARTnet Service는 다음 기능을 제공합니다.

- 전 세계 어디서든 Cisco TAC 24시간 이용
- 온라인 기술 자료, 커뮤니티 및 툴 액세스
- 하드웨어 교체 옵션: 익영업일(가능한 지역의 경우)
- 운영 체제 소프트웨어 업데이트
- 유지 보수 및 간단한 소프트웨어 업데이트
- Smart Call Home을 활성화한 디바이스에서 스마트한 예방적 진단 및 실시간 알림

Cisco SMARTnet에 대한 자세한 내용은 다음 링크를 참조하십시오. http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_group_home.html.

기술 지원 서비스는 제품 판매 시 자동으로 첨부되므로 고객은 필요한 지원과 엔타이틀먼트를 받고 투자 수익을 극대화할 수 있습니다. Cisco Commerce Workspace에서 Cisco 제품을 주문하는 경우 적절한 SMARTnet Service 항목이 자동으로 견적에 추가됩니다(표 7). 고객은 적절한 서비스를 첨부하여 보안 제품을 구매하는 것이 좋습니다.

표 7. AMP Threat Grid용 Cisco SMARTnet Service 부품 번호

제품 설명	제품 부품 번호	Cisco SMARTnet 부품 번호
Threat Grid 5004 섀시, 메모리 카드, 하드 디스크 드라이브, PCIe 버스, PSU, 레일 킷 포함	TG5004-K9	CON-SNT-TG5504K9
Threat Grid 5504 섀시, 메모리 카드, 하드 디스크 드라이브, PCIe 버스, PSU, 레일 킷 포함	TG5550-K9	CON-SNT-TG5504K9

주문 프로세스의 이해

견적 작성, 주문, 제품 지원에 대한 자세한 내용은 표 8에 나와 있는 웹 페이지를 참조하십시오.

표 8. Cisco 리소스

주제	설명
일반적인 주문 지원	주문, 견적, 반품, 딜, 서비스 계약, 프로파일 및 로그인, 툴 액세스, 교육, 보고, 피드백 등에 대한 서비스 케이스를 열고 관리하려면 My Cisco Workspace를 사용하십시오.
기술 지원	파트너 및 고객은 기술 지원을 받거나 Cisco 프로세스, 툴, 시스템을 사용해 지원 케이스를 열 수 있습니다.

주제	설명
통합 관련 지원	SAC(Sales Acceleration Center)는 기술 및 아키텍처의 전 범위에서 프리세일즈 지원을 위한 단일 창구 역할을 합니다. SAC는 높은 레벨의 서비스를 통해 순조롭게 전환하고 트랜잭션 관련 문제를 해결할 수 있도록 지원합니다. SAC는 기존의 지원 프로세스를 보완하며 해당 문제나 주제에 따라 정확한 지원 리소스를 검색하는 데 도움이 됩니다. 이메일: sac-support@cisco.com 전화: 800 225-0905, 408 902-4872
IT 관련 지원 (Cisco 내부용)	IT 문제가 발생한 사내 직원은 Service Request Management 툴에서 케이스를 열고 진행 상황을 확인할 수 있습니다. 또한 Business Support and Operational Systems 페이지에서 자세한 정보와 점검 중인 기존 문제를 확인할 수 있습니다.
라이선싱 및 PAK 등록	셀프 서비스 옵션을 통해 여러 라이선싱 기능을 사용할 수 있습니다. 아울러 여기에서 양식을 작성하거나 Support Case Manager 툴에서 케이스를 열어 GLO(Global Licensing Operation) 팀의 지원을 받을 수도 있습니다.
파트너 프로그램 및 교육 지원	파트너 교육에 대해 자세히 알아보려면 Partner Education Connection을 방문하십시오. 전문화, 인증, 인센티브 프로그램 등에 대해 자세히 알아보려면 Partner Central을 방문하십시오.
Partner Helpline	Partner Helpline에서는 프리세일즈 제품 지원을 제공하고, Cisco Commerce Workspace에서는 전반적인 Commerce Workspace 지원을 제공합니다.
Technology Solutions Network(TSN)(Cisco 내부용)	TSN은 24x5로 운영되는 가상 시스템 엔지니어의 글로벌 네트워크로서 Cisco 영업 조직을 위해 프리세일즈 기술 서비스를 제공하고 인재 개발을 지원합니다. http://iwe.cisco.com/web/salessecentral/tsn
딜 등록 안내	기존 딜을 Cisco로 전환하는 데 도움이 필요할 경우 어카운트 매니저 및 보안 어카운트 매니저와 협업하여 필요한 조언을 받으십시오.
Cisco Commerce Workspace	하드웨어 및 신규 서비스 주문을 제출하고, 주문 상태를 확인하고, 구성을 생성하려면 https://cisco-apps.cisco.com/cisco/psn/commerce 를 이용하십시오. 교육 링크: http://www.cisco.com/web/partners/events/commerce_workspace.html
Cisco Service Contract Center(CSCC)	서비스 계약 검토 및 갱신, 그리고 변경은 http://www.cisco.com/web/services/ordering/cscc/index.html 을 이용하십시오. 교육 링크: http://www.cisco.com/web/services/resources/cscc/training/index.html
Cisco 웹 기반 툴 모음	모든 온라인 툴: http://www.cisco.com/web/ordering/root/index.html

부록 A: 모든 솔루션

사용자 1명은 계정 1개와 같습니다. 계정 공유는 허용되지 않습니다.

콘텐츠 서브스크립션 라이선스가 없으면 어플라이언스를 사용할 수 없습니다.

표 A-1에는 모든 Cisco AMP Threat Grid 어플라이언스에 대한 제품 설명 및 Cisco SMARTnet 부품 번호가 나와 있습니다.

표 **A-1**. Cisco AMP Threat Grid 주문 정보

Cisco AMP Threat Grid 어플라이언스, 5000 Series		
부품 번호	**제품 설명**	**SMARTnet 부품 번호**
TG5004-BUN	Cisco AMP Threat Grid 5004 어플라이언스, 지원 및 서브스크립션 번들	
TG5504-BUN	Cisco AMP Threat Grid 5504 어플라이언스, 지원 및 서브스크립션 번들	
TG5004-K9	Cisco AMP Threat Grid 5504 어플라이언스(소프트웨어 포함)	CON-SNT-TG5004K9
TG5504-K9	Cisco AMP Threat Grid 5504 어플라이언스(소프트웨어 포함)	CON-SNT-TG5504K9
L-TG5004-LIC-K9=	5004 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스	
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	
L-TG5504-LIC-K9=	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스	
L-TG5504-1Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 1년	

Cisco AMP Threat Grid 어플라이언스, 5000 Series		
L-TG5504-3Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 3년	
L-TG5504-5Y-K9	5504 모델용 Threat Grid 콘텐츠 서브스크립션 라이선스, 5년	

부품 번호	제품 설명
L-TG-S1-LIC-K9=	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건
L-TG-1Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 1년
L-TG-3Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 3년
L-TG-5Y-S1-K9	Cisco AMP Threat Grid, 계정 5개 및 1일 기준 제출 500건, 5년
L-TG-S2-LIC-K9=	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건
L-TG-1Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 1년
L-TG-3Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 3년
L-TG-5Y-S2-K9	Cisco AMP Threat Grid, 계정 10개 및 1일 기준 제출 1500건, 5년
L-TG-S3-LIC-K9=	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건
L-TG-1Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 1년
L-TG-3Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 3년
L-TG-5Y-S3-K9	Cisco AMP Threat Grid, 계정 25개 및 1일 기준 제출 2500건, 5년
L-TG-S4-LIC-K9=	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건
L-TG-1Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 1년
L-TG-3Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 3년
L-TG-5Y-S4-K9	Cisco AMP Threat Grid, 계정 100개 및 1일 기준 제출 10,000건, 5년
L-TG-PT-S1-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개
L-TG-PT-1Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 1년
L-TG-PT-3Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 3년
L-TG-PT-5Y-S1-K9	Threat Grid, 프라이빗 태깅 계정 5개 및 1일 기준 파일 500개, 5년
L-TG-PT-S2-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개
L-TG-PT-1Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 및 1일 기준 파일 1500개, 1년
L-TG-PT-3Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개, 3년
L-TG-PT-5Y-S2-K9	Threat Grid, 프라이빗 태깅 계정 10개 및 1일 기준 파일 1500개, 5년
L-TG-PT-S3-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개
L-TG-PT-1Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 1년
L-TG-PT-3Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 3년
L-TG-PT-5Y-S3-K9	Threat Grid, 프라이빗 태깅 계정 25개 및 1일 기준 파일 2500개, 5년
L-TG-PT-S4-LIC-K9=	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개
L-TG-PT-1Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 1년
L-TG-PT-3Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 3년
L-TG-PT-5Y-S4-K9	Threat Grid, 프라이빗 태깅 계정 100개 및 1일 기준 파일 10,000개, 5년

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

C07-733608-07 12/16