



Cisco AMP Threat Grid Appliance

데이터 보존에 관한 노트



버전 2.2

최종 업데이트: 2017년 3월 3일

All contents are Copyright © 2017 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

소개

이 문서는 다음과 같이 Threat Grid Appliance의 데이터 보존 정보를 포함합니다.

파일 또는 데이터 유형	일일 크기 사용 제한	보존 시간	필요한 공간
분석	1.2GB	최소 1,000일	1.3TB
디스크 아티팩트("Blob")	31.5GB	최소 4.3일	145GB
네트워크	3.6GB	최소 64일	250.5GB
프로세스	937.5MB	최소 64일	63.3GB
보고서	1.5GB	최소 1,000일	1.6TB
샘플	7.6GB	최소 64일	522.1GB
동영상	2.3GB	최소 64일	155.6GB

추가 정보

- 보존 시간은 샘플 속도를 하루에 10k로 가정합니다.
- 분석 보고서가 아직 릴리스되지 않은 10k 샘플 어플라이언스에서 최소 2년 동안 보존됩니다. TG5500/TG5504에서의 보존 시간의 두 배이며 TG5000/TG5500에서의 보존 시간의 3배 이상 긴 (예: TG5500의 보존 기간보다 3배 이상 긴 기간) 인수를 지닙니다. 즉 릴리스되지 않은 10k 샘플 어플라이언스의 보존 기간보다 최대 6배 이상 긴 보존 기간을 지닙니다.
- 동일한 보존 규칙이 분석 데이터에 적용됩니다.
- 기타 콘텐츠는 디스크 가용성에 따라 더 적은 시간 동안 유지됩니다.
- 용량 이하의 시스템을 실행하는 경우, 추가 콘텐츠는 더 오랜 기간 동안 보존됩니다.
- 시스템이 1.x에서 실행 중인 경우 가져온 디스크 아티팩트("blobs")는 2.2 마이그레이션에 포함됩니다.
- Blob는 2.2 마이그레이션 이후의 짧은 기간 동안에만 보존됩니다.
- 샘플이 여러 blob를 가질 수 있지만 150,000개의 blob/일 기준의 샘플 속도는 평균값을 나타냅니다. 속도가 다른 경우, 보존 기간에 영향을 줄 수 있습니다.