AMP for Endpoints 구축(2020년 1월 8일 기준 기존 고객 대상)에서 옵트인 및 Enable Orbitral Advanced Search

목차

Cisco는 최근 AMP for Endpoints용 2가지 패키지를 출시했습니다.Essentials 및 Advantage.Orbeth Advanced Search는 Advantage 패키지의 핵심 기능입니다.출시 일자(2020년 1월 8일)의 모든 기존 고객은 계약 기간의 나머지 기간 동안 무료로 사용할 수 있습니다.이 FAQ에는 패키지 및 출시 날짜 현재 기존 고객에게 미치는 영향에 대한 자세한 정보가 있습니다.

Orbeth Advanced Search는 100개가 넘는 카탈로그 쿼리를 제공하여 보안 조사 및 위협 추적을 단순하게 할 수 있도록 설계된 Cisco AMP for Endpoints의 새로운 고급 기능입니다.이렇게 하면 모든 엔드포인트에서 복잡한 쿼리를 신속하게 실행할 수 있습니다.또한 이 기능을 사용하면 현재 상태의 스냅샷을 생성하여 특정 시점에 어떤 엔드포인트에서 어떤 일이 발생했는지 더 심층적으로 파악할 수 있습니다.

Orbeth Advanced Search를 사용하면 다음과 같은 중요한 작업을 더 빠르고 효율적으로 수행할 수 있습니다.

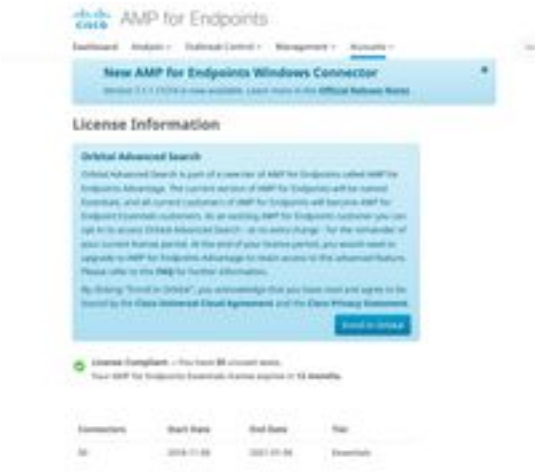
- **위협 추적**.거의 실시간으로 악의적인 아티팩트를 검색하여 위협 추적을 가속화합니다.
- **사고 조사**.신속하게 사고의 근본 원인을 파악하고 신속하게 문제를 해결합니다.
- **IT 운영**.디스크 공간, 메모리 및 기타 IT 작업 아티팩트를 추적하기만 하면 됩니다.
- **취약성 및 규정 준수**.운영 체제의 상태를 신속하게 확인하여 엔드포인트가 현재 정책을 준수하는지 확인합니다.

이 문서는 새로운 기능을 옵트인하고 엔드포인트에서 활성화하는 방법을 안내하는 단계별 가이드입니다.전체 궤도 사용 설명서도 제공됩니다.AMP for Endpoints 고객은 엔드포인트에 이미 커넥터(7.1.5 이상)가 설치되어 있는 경우 Orbetal Advanced Search를 쉽게 활성화할 수 있습니다. 최신 커넥터 버전 및 기타 정보는 Orbeability에 대한 AMP for Endpoints 콘솔 도움말 항목을 참조하십시오.현재 버전 1703(Creators Update) 이상을 실행하는 64비트 Windows 10 호스트에서는 Orbeth Advanced Search가 지원됩니다.

이러한 단계를 완료했으면 빠른 시작 가이드에서 Orbeability Advanced Search를 사용하는 방법에 대한 자세한 설명을 참조하십시오.

1단계:궤도 고급 검색에 옵트인

이전에 Orbeth Advanced Search 베타에 등록하지 않았거나 명시적으로 로그인한 적이 없는 경우 AMP for Endpoints 콘솔의 License Information 페이지에서 등록할 수 있습니다.Orbeability Advanced Search(오비탈 고급 검색)에 옵트인하려면 AMP for Endpoints(엔드포인트용 AMP) 콘솔에 로그인하고 Accounts(어카운트) **> License Information(라이센스 정보)** 드롭다운을 선택합니다.이 페이지에서 Enroll **in Orbeability를** 클릭하여 이 기능에 액세스할 수 있습니다.



참고:Orbeth Advanced Search에 옵트인하려면 권한(admin) 사용자여야 합니다.

2단계:기존 정책에서 궤도 고급 검색 사용

엔드포인트에 이미 Connector(버전 7.1.5 이상)가 설치되어 있는 경우 엔드포인트에 대한 기존 정책에서 Orbeability Advanced Search를 활성화하면 됩니다.

- AMP for Endpoints 콘솔로 이동합니다.Management(**관리) > Policies(정책)**에서 Orbeability Advanced Search(오비탈 고급 검색)를 활성화할 정책을 선택하고 **Edit(편집)** 버튼을 클릭하여 Edit Policy At Advanced Settings(고급 설정) *Edit Policy(정책 수정)* Orbeability(오비탈 **고급 검색)를 선택하고 Orbeability Advanced Search(오비정상 검색)가 활성화되어 있는지 확인합니다**.궤도 **고급 검색 활성화** 상자를 선택해야 합니다.그렇지 않은 경우 확인란을 선택하여 활성화합니다.

이 시점에서 이 정책과 함께 설치된 모든 커넥터는 해당 엔드포인트에서 Orbeability Advanced Search를 자동으로 활성화합니다.

3단계:새 정책 및 컴퓨터 그룹에서 궤도 고급 검색 사용(선택 사항)

위에서 설명한 것처럼, 기존 정책에서 Orbeability Advanced Search를 활성화한 후에는 해당 정책을 사용하는 모든 커넥터에서 Orbeth Advanced Search가 활성화되고 해당 정책을 사용하는 새 커넥터도 Orbeth Advanced Search가 활성화됩니다.예를 들어, "보호" 그룹에 1,000대의 컴퓨터가 있는 경우 해당 정책에서 Orbeability Advanced Search를 활성화하면 커넥터 버전 7.1.5 이상이 구축된 경우 해당 엔드포인트에서 Orbeability Advanced Search가 자동으로 활성화됩니다.

새 정책 및 그룹을 만드는 것은 선택 사항입니다.그러나 새 정책 및 그룹을 사용하여 특정 엔드포인트 그룹에서 Orbeability Advanced Search를 사용하려면 제품 설명서를 따라 새 정책 및/또는 그룹을 생성하고 위에 표시된 것처럼 정책에서 Orbeability Advanced Search가 활성화되었는지 확인합니다.

4단계: 궤도 콘솔 탐색

하나 이상의 엔드포인트에 설치된 커넥터 버전이 7.1.5 이상인 정책에서 Orbeth Advanced Search를 활성화한 후에는 엔드포인트에서 정보를 수집하기 위해 쿼리를 실행할 수 있습니다.

- Management(**관리) > Computers(컴퓨터**)로 이동하여 Orbeability Advanced Search(궤도 고급 검색)가 있는 컴퓨터 찾기 창을 확장하고 **Orbeability Query(궤도 쿼리)**를 클릭합니다 .Analysis(분석) > Orbeth **Advanced Search(**궤도 **고급 검색)**로 이동하여 Orbeth 콘솔**에** 액세스할 수도 있습니다.
- Orbeth 콘솔이 새 브라우저 탭에 로드됩니다.필요한 경우 **Log in with Cisco Security(Cisco Security로 로그인)를** 클릭하여 기존 AMP Console 자격 증명을 사용하여 인증합니다.

참고:Orbeth Advanced Search는 https://orbital.amp.cisco.com에서 직접 액세스할 수도 있습니다.

- Endpoints 필드에는 쿼리할 컴퓨터가 표시됩니다.특정 GUID를 입력하거나 이 필드에 **모두** 입력하여 Orbeability Advanced Search가 활성화된 조직의 모든 엔드포인트를 쿼리할 수 있습니다.임의의 엔드포인트 샘플링을 수행하려면 생략 부호(...)를 클릭하여 **Add Random Endpoints** 대화 상자를 엽니다.
- **SQL** 필드에 사용자 정의 SELECT 문을 입력하거나 **Browse Query Catalog**를 클릭하여 **Query Catalog를** 열 수 있습니다. 이 카탈로그에는 쿼리에 추가할 수 있는 수십 개의 쿼리가 포함되어 있습니다.**SQL SELECT 문을 작성하여 오비탈을 사용하는 방법을 알 필요가 없습니다.**

- 쿼리**를 클릭합니다**.쿼리는 지정된 엔드포인트에 대해 실행되며, 결과는 오른쪽 창에 표시됩니다.쿼리를 편집하고 다시 실행할 수 있습니다.결과를 다운로드할 수 있습니다.쿼리를 구성할 수 있는 예약 기반으로 실행할 작업으로 저장할 수 있습니다.
- Orbeth Advanced Search를 시작하는 방법에 대한 자세한 내용은 Quick Start(빠른 시작)를 참조하십시오.