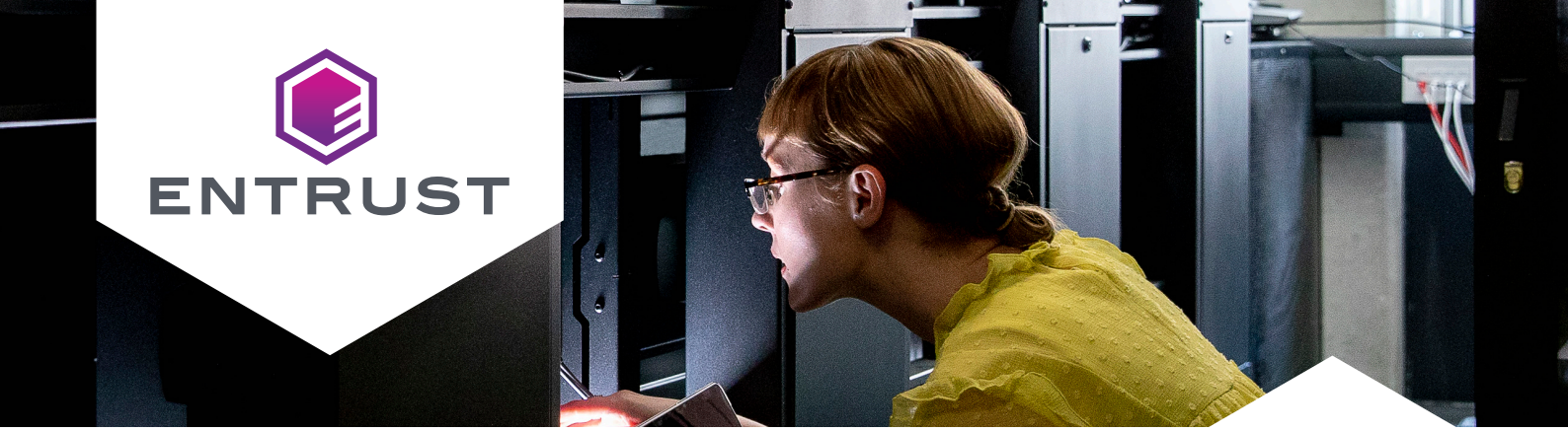


Entrust Certificate Hub

머신 ID 검색, 제어 및 관리 자동화

비즈니스 과제

급증하는 머신 ID 관리 전략

기업 및 기관에서 발급하고 관리하는 인증서 수가 계속해서 빠른 속도로 증가하고 있습니다. 부분적인 이유로는 기존 사용 사례의 지속적인 확장과 원격 및 분산된 업무에 필요한 보안 요건을 들 수 있습니다. 그러나 가장 큰 이유는 머신 ID의 지속적인 증가입니다.

모바일 및 IoT 기기에서 애플리케이션 및 컨테이너에 이르기까지, 머신 ID 수는 이제 휴먼 ID 수를 훌쩍 뛰어넘습니다. 머신의 종류도 다양해지고 있습니다.

- 사물 인터넷(IoT)은 데이터를 전송하는 센서 등 새로운 물리적 기기를 도입
- 클라우드는 데스크톱, 서버 등 기존의 물리적 머신을 모방한 '가상' 머신 또는 소프트웨어 개발을 촉진
- DevOps는 '마이크로서비스'라는 개별 모듈로 구성된 컨테이너, 즉 셀프 컨테인드(Self-contained) 런타임 환경으로 클라우드를 가속화

머신 수의 폭발적인 증가는 새로운 기회를 제공하는 반면, 관리되지 않는 인증서 또는 '불량' CA로 인한 위험도 증가합니다. 대규모의 분산된 인프라, 짧은 수명의 인증서와 같은 문제를 처리해야 하는 복잡성은 말할 것도 없습니다.

IT 환경 전반에서 다른 시스템과의 통신을 비롯해 모든 시스템을 식별, 인증, 보호하는 것은 필수적입니다.

솔루션

중앙에서 관리하는 머신 ID 라이프 싸이클

Entrust Certificate Hub는 조직 전반의 모든 머신 ID를 통합해, 단순하고 직관적인 '단일 통합 모니터링(Single Pane of Glass)'을 구현합니다.

온프레미스 또는 관리형으로 제공되는 Certificate Hub는 머신 ID가 초래하는 복잡한 문제를 해결하기 위해, 머신 ID 관리에 가장 필수적인 구성 요소인 자동화를 제공합니다.

Certificate Hub에 관한 자세한 정보: entrust.com/ko

Entrust Certificate Hub

주요 기능 및 혜택

직관적인 인터페이스를 통한 중앙 집중식 가시성 및 관리

- 중앙 집중식 정책 구성 및 인증서 라이프 싸이클 관리를 위한 단일 실행 지점 제공
- 단순하고 직관적인 포털을 통해 소스에 관계없이 조직 전반의 인증서 보기 및 관리
- 여러 CA에서 조직 전반에 배포된 머신 ID를 검색해 단일 통합 모니터링(Single Pane of Glass)으로 중앙 집중식 가시성을 제공하는 고급 보고 기능
- Certificate Hub 소스 연결을 사용해, Entrust로 관리하는 모든 인증서를 가져올 수 있습니다. 인증서 가져오기 방법은 다음과 같습니다.
    - Discovery 스캐너
    - 'API 가져오기'를 통한 대량 가져오기
    - UI를 통한 수동 업로드
    - CA 데이터베이스와 소스 동기화
- 관리자와 최종 인증서 소유자 모두에게 편리한 브라우저 기반 사용자 인터페이스

편리한 관리자 제어, 보고 및 알림

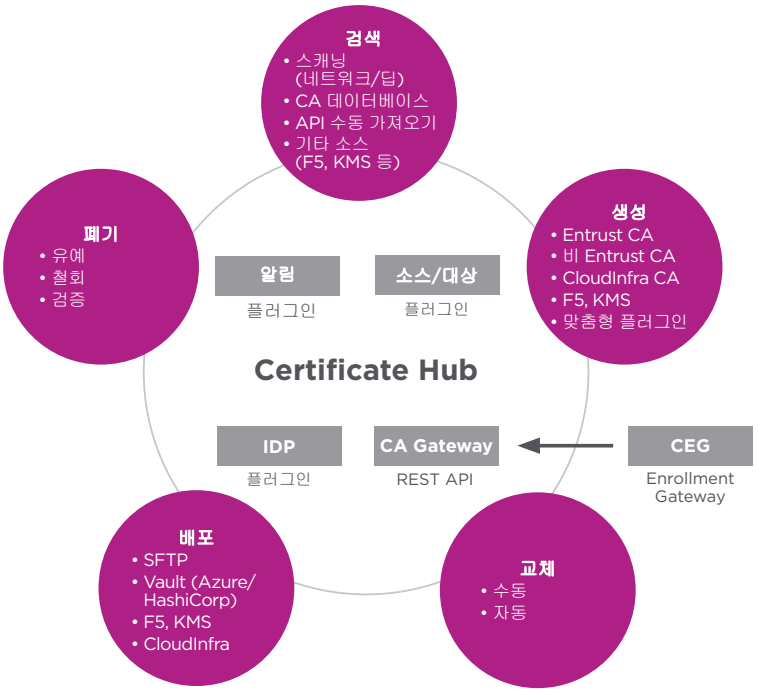
- 관리자는 액세스 권한, 시스템 메타데이터, 알림, 보고서 브랜딩 등을 맞춤 설정할 수 있음
- 맞춤 설정 역할을 통한 역할 기반 액세스 제어는 규제 준수, 직무 분리, 책임 위임을 지원하며, 인증 태그는 더욱 세분화된 액세스 제공
- 관리 및 모니터링되는 인증서의 자동 만료 알림
- 클라우드 KMS 서비스 및 CA에 연결해 알림 및 오케스트레이션 허용
- 관리자는 Discovery가 맞춤 설정 메타데이터를 자동으로 연결해 인증서를 보강하도록 구성할 수 있음
- Report Designer를 통한 사용자 정의 보고서 생성 및 예약
    - 인증서 및 관리 이벤트의 알림(이메일, SMS 등)을 지원하는 규칙 및 조치
    - 인증서 아카이브를 통해 규제 요건을 충족하는 보고, 알림, 인증서 관리 보기 제공
    - 간편한 인증서 알림 관리를 위한 일괄 작업 수행 기능
- 고급 보고 기능으로 모든 예정된 인증서 이벤트 또는 작업의 경고 및 알림 제공
- 딥 스캐닝 지원으로, 네트워크 스캐닝 및 검색에서 나아가 Java 키 저장소, 바이너리 파일, 압축 파일 등에 저장된 디지털 인증서 검색 및 감사

Certificate Hub에 관한 자세한 정보: entrust.com/ko

Entrust Certificate Hub

유연한 통합 및 확장성

- 그린필드 및 브라운필드 배포를 위한 머신 ID 관리
- Kubernetes 클러스터 또는 Entrust 소프트웨어 어플라이언스를 통해 구동
- 에이전트 또는 에이전트리스 인증서 배포 및 관리
- 외부 API를 통한 딥 스캐닝 도구와의 통합으로 모든 형태의 디지털 인증서(PEM, DER, P12 등) 검색 및 목록 생성
- AWS 또는 Azure에서 엔터프라이즈 프라이빗 또는 퍼블릭 클라우드 호스팅에 최적화된 온프레미스 배포
- 주요 작업 수행을 위한 역할 기반 액세스 제어에 사용되는 Enterprise IDP/Active Directory 통합
- OTS(Off-the-Shelf) 도구 및 자동화를 통한 배포 및 버전 업그레이드
- 확장을 위한 플러그형 아키텍처



지원되는 통합

Entrust Certificate Hub는 단일 통합 모니터링(Single Pane of Glass)을 통한 인증서 발급, 갱신 및 폐기로 광범위한 애플리케이션을 지원합니다.

CA	• ECA (Entrust CA) • ECS CA (Entrust 인증 솔루션 CA) • DigiCert CA • Microsoft CA • Standalone Microsoft CA • PrimeKey EJBCA
Cloud 및 DevOps	• Ansible • AWS • AZURE • Kubernetes • OpenShift • Rancher
KMS 및 Vaults	• Entrust Vault (Key 제어) • Azure Key Vault • HashiCorp Vault
인시던트 및 워크플로	• ServiceNow
HSM	• Entrust nShield (이전 nCipher) • Thales
등록 표준	• ACME • EST • INTUNE • MDMWS • SCEP • WSTEP
추출 레이어/확장성	• CA/Enrollment Gateway • IoT Agent • IT Agent (Windows/Mac) • REST API
서버/로드 밸런서 등	• Apache • F5 • Java • NGINX

Certificate Hub에 관한 자세한 정보: entrust.com/ko

Entrust Certificate Hub

작동 방식

중앙 집중식 가시성, 감독 및 보고

Certificate Hub는 조직 및 직원의 책임을 물을 수 있도록 인증서 소유자 추적 기능을 제공합니다. 맞춤형 메타데이터 필드 세트를 정의한 다음 소유자, 조직 또는 비용 센터와 같은 세부 정보로 인증서에 태그를 지정할 수 있습니다. 또한 소유자에게 앞으로 취해야 할 조치에 대해 알리고 활동을 모니터링하며 자동 보고서 생성 및 배포를 설정해 관리 가시성을 제공할 수 있습니다.

Certificate Hub:

- 배포된 인증서를 찾고 각 인증서의 위치, 유형, 알고리즘, 만료를 기록하고 이를 발급자와 연결해 정책 위반 여부를 파악할 수 있습니다. 외부 발급자의 인증서에 알림 및 경고를 추가할 수도 있습니다.
- 모든 Entrust 및 Microsoft CA를 제어할 수 있습니다. Discovery와 함께 구동되면, 발급된 모든 인증서의 목록이 작성되고 현재 배포된 위치로 연결되어 사용되지 않거나 분리된 인증서를 찾아냅니다.
- 기존 사용자 워크플로에 영향을 주지 않고 문제를 발견하며, 시기적절한 조치를 취하기 위해 신속한 보고 및 관리 도구를 제공합니다.
- 인증서를 알려진 발급자와 다시 연결하고 Entrust CA Gateway를 통해, 지원되는 CA에서 발급된 인증서의 직접 피드를 얻습니다. 발급과 검색의 상관관계를 파악해, 어떤 인증서가 배포되었는지에 대한 엔드투엔드 검증을 제공합니다.
- 인증서 발급, 갱신 및 폐기를 위한 최종 인증서 소유자 셀프 서비스 인터페이스를 제공합니다. 인증서 소유자는 조치를 취해야 할 때 자동 알림을 수신하고 활동 요약 보고서를 생성할 수 있습니다.

버전

투티어(Two Tiers)로 사용 가능

온프레미스형 배포든 서비스형 배포든 상관없이, Certificate Hub는 투티어(Two Tiers)로 사용할 수 있습니다.

검색

- 네트워크 검색 및 자동 인증서 가져오기를 통해 조직 전반에서 인증서 인벤토리 작성
- 사용하기 쉬운 보고서 디자이너 및 스케줄러로 조직 전반에 대한 가시성 제공
- 이메일로 알림 및 보고서를 발행해 인증서 소유자에게 취해야 할 조치를 상기시킴

제어 및 자동화

- 벤더에 관계없이 인증서 정책, 발급, 공인 및 사설 인증기관에 대한 액세스를 중앙에서 관리
- CA 데이터베이스 및 클라우드 서비스에서 자동 인증서 가져오기를 통해 CA 활동 모니터링
- 연결된 모든 CA에서 인증서 발급, 갱신 및 폐기 작업 수행
- API, SSH 및 클라우드 키 저장소 퍼블리싱을 통해 완전 관리형 교체 및 인증서 프로필 관리가 제공되는 엔드포인트로 키와 인증서를 직접 푸시
- AWS ACM CA, Azure Key Vault 및 F5 네트워크 등에 대한 소스 플러그인 지원

Certificate Hub에 관한 자세한 정보: entrust.com/ko

Entrust Certificate Hub

- CA가 아닌 키 관리 서버로 지원하는 KMIP에서 생성/저장된 키 관리
- SDK를 활용해 다음을 위한 맞춤형 플러그인 생성:
  - 모든 외부 **소스** 자동화로 외부 소스 포인트에서 인증서 자동 가져오기
  - 모든 외부 **대상** 자동화로 맞춤형 대상 포인트에 대한 수동 및 자동 인증서 발급

자세한 정보:
entrust.com/ko

ENTRUST

대한민국 서울특별시 강남구 삼성동 159-1
KWTC 트레이드타워 2503호 135-729
전화: 02-2088-4691
HSMinfo@entrust.com