digicert®

CERTCENTRAL® DISCOVERY

암호화 자산의 종합적 감시

개요

CertCentral® Discovery 조직에서 클라우드 및 네트워크 기반 인증서, 키 및 암호화 자산을 저장하고 관리하도록 하는 스캔 서비스입니다.

CertCentral® Discovery 풍부한 기능 집합은 유지 관리를 최소화하고 작업을 통합하는 자체 제어를 통해 비즈니스에 영향을 주기 전에 취약점을 감지하고 수정하는 데 필요한 통찰력과 도구를 TLS 및 보안 관리자에게 제공합니다.

주요 이점

- 인증서 및 암호화 자산의 환경에 대한 **가시성 확보**
- 문제가 발생하기 전에 이를 식별하고 수정하여 **위험 감소**
- 기업 보안 정책 시행으로 **위조 활동 감소**

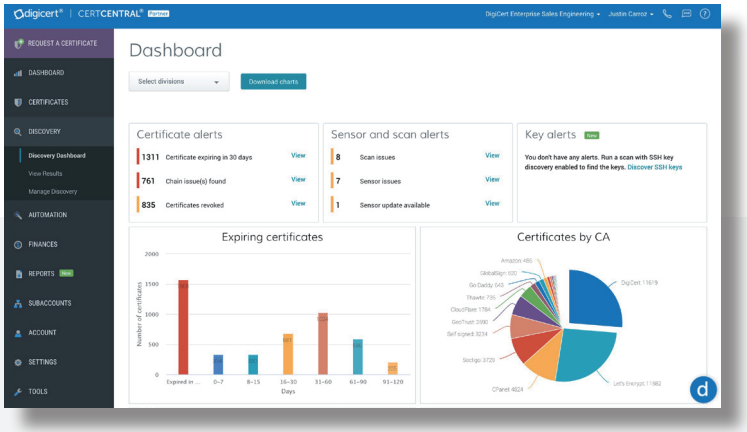
종합적인 발견을 위한 클라우드, 네트워크 및 파일 스캔

TLS & SSH 디스커버리는 속성과 함께 클라우드 및 네트워크 기반 TLS/SSL 인증서 및 SSH 키를 저장합니다. 또한 개인 루트는 이러한 루트에서 발급하여 발견된 인증서의 분석과 관리를 위해 가져올 수 있습니다.

인터넷에서 분리된 환경과 같이 보호된 영역에 있는 인증서는 중앙 집중식 경고 및 알림을 제공하도록 관리를 위해 가져올 수 있습니다.

TLS/SSH 디스커버리는 대규모 네트워크를 빠르게 스캔하고 여러 스캔을 동시에 수행할 수 있고 지정된 도메인을 차단하여 추가적으로 스캔 효율성을 개선할 수 있습니다.

개체 디스커버리는 공개 및 개인 TLS 인증서, SSH 키 및 사용자, S/MIME 및 코드 서명 인증서를 파일 시스템 및 시스템 레지스트리에 저장하고 알고리즘에 대해 아카이브(키 저장소, .zip 및 .jar) 및 바이너리 파일(.exe, .dll, .so)을 검사하여 IT 전문가에게 서버에 있는 암호화 자산의 전체적인 그림을 제공합니다.



TLS 인증서, SSH 키 및 서버 기반 암호화 자산의 종합적 감시

위험 감지 및 수정

자산 보안 위험: 보안을 개선하거나 구성을 수정하기 위한 프롬프트와 함께, 발견되어 가져온 모든 인증서에 대한 SSL 보안 등급을 검토합니다.

취약점 관리: 최근 알려진 TLS/SSL 보안 취약점에 대해 서버를 평가합니다. 취약한 프로토콜과 사이퍼 및 잘못 구성된 중간 또는 다른 신뢰 체인 문제를 검토하고 수정합니다.

경고 및 알림: 인증서 만기 임계값에 대해 인-콘솔 및 이메일 알림을 구성하고 추가 수신자로 알림을 확대하고 만기 알림 처리를 위해 보호된 구역에서 인증서를 가져옵니다.

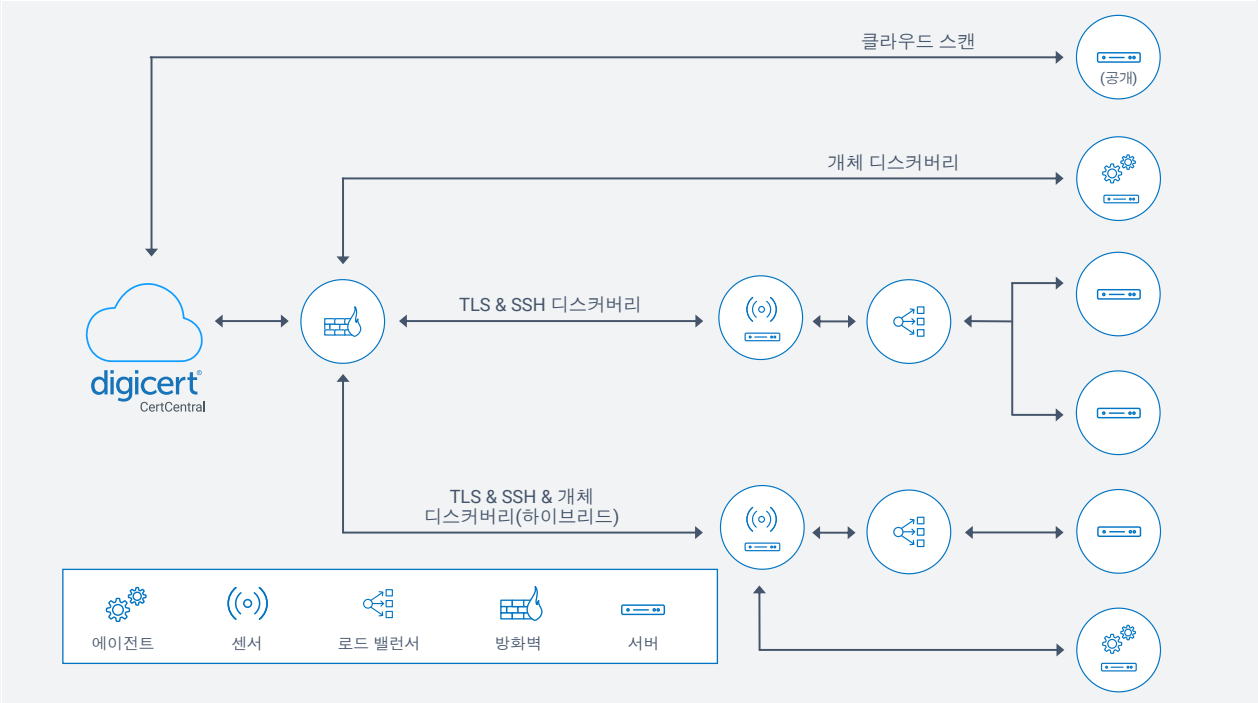
자체 제어 인프라

CertCentral® Discovery 자체 제어 인프라를 통해 전달되어 IT 유지 관리를 감소하고 지속적인 시스템 상태 및 감시를 제공합니다. 센서 및 에이전트는 지속적으로 디스커버리 서비스를 테스트하고, 자동으로 업데이트하고, 기능 중단에 대한 알림을 전달합니다.

지원되는 플랫폼

웹 서버: Apache HTTP, Apache Tomcat, NGINX, IBM HTTP, Microsoft ISS

로드 밸런서: CertCentral® Discovery 플랫폼 애그노스틱으로 네트워크에서 모든 기기에 대한 인증서를 찾을 수 있습니다.



오늘 시작하십시오.

자세한 내용은 https://www.digicert.com/kr/tls-ssl/certcentral-tls-ssl-manager 의 양식을 사용하여 당사에 문의하십시오.

DigiCert, Inc. 정보

DigiCert는 디지털 신뢰 분야의 세계적 선두 주자로 개인 및 기업의 디지털 세상 속 발자국에 대한 보안을 보장합니다. 디지털 신뢰 플랫폼 DigiCert® ONE은 공공 및 민간 신뢰 부문을 비롯해 웹사이트 보안, 기업 액세스 및 통신, 소프트웨어, 아이덴티티, 콘텐츠 및 기기 등의 넓은 분야에서 가시성과 제어의 중앙 집중화를 제공합니다. DigiCert는 수상 경력이 빛나는 자사의 소프트웨어를 산업 선두 주자라는 이름에 어울리는 기준, 지원 및 운영을 바탕으로 제공합니다. 그만큼 전 세계의 다양한 선두 기업들이 디지털 신뢰 제공사로 DigiCert를 선택하고 있습니다. 더 자세한 내용은 digicert.com을 방문하거나 @digicert.를 팔로우하여 확인할 수 있습니다.