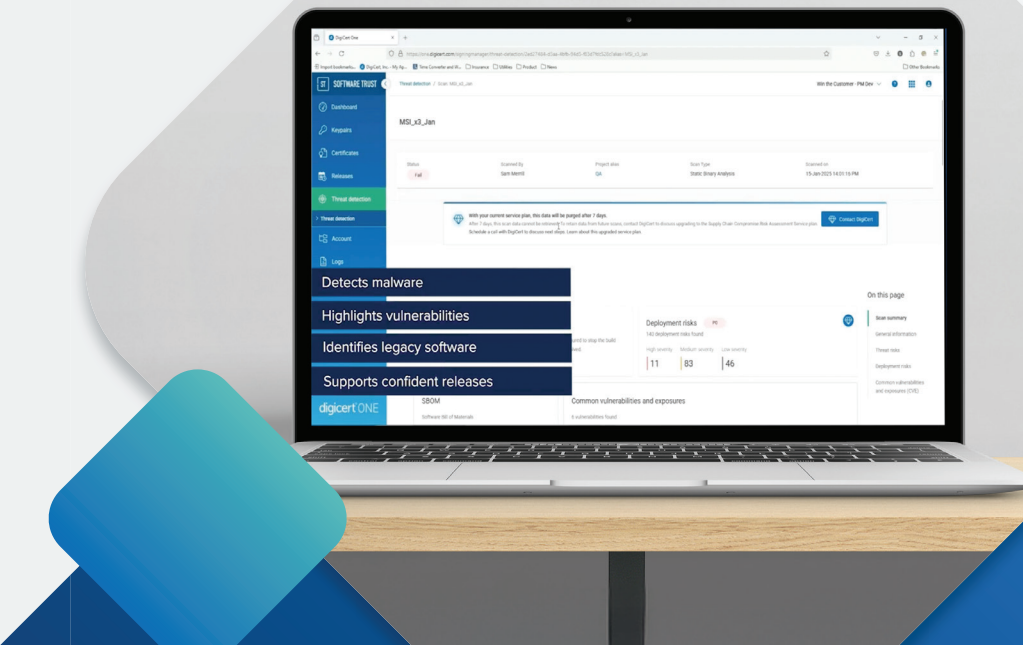
digicert®

캐논, 코드 서명에 대한 보안 강화와 엄격한 통제 도입



CASE STUDY

캐논, 코드 서명에 대한 보안 강화와 엄격한 통제 도입

개요

기업명: 캐논 주식회사
사업부문:디지털 프린팅 사업본부
https://global.canon/

업종:전기기기
본사: 도쿄도

주요 비즈니스 요구 사항:

- 애플리케이션, 프린터 드라이버 등에 대한 코드 서
- CA/B 포럼에서 요구하는 개인키 보호를 관리하는 코드 서명 시스템
- 컴플라이언스 관리

솔루션:

- DigiCert Software Trust Manager

주요 특징:

- 모든 코드 서명 업무의 완전한 시각화 및 제어를 통해 잠재적인 위협에 대한 신속한 탐지 및 대응이 가능
- 역할 기반 액세스 관리를 통해 서명 업무와 관리 업무를 분리하고 작업 부하를 줄이고 휴먼 에러 및 보안 침해 위험을 최소화
- 자동화된 워크플로우와 직관적인 도구로 코드 서명에 소요되는 시간이 절반으로 줄어들고 프로세스 간소화 및 기술 전문 지식에 관계없이 사용자에게 권한 위임 가능
- 중앙집중화된 엄격한 관리를 통해 기업의 보안 정책 및 법규를 철저히 준수하고, 기업의 보안 체계를 명확하게 파악

요구사항

자체 코드 서명 시스템에서 벤더의 시스템으로 대체하여 개인 키 보호에 대한 기본 요구 사항을 빠르게 충족

디지털 이미징 솔루션의 글로벌 리더인 캐논은 코드 서명 프로세스의 보안을 강화할 필요가 있었다. 매출의 약 50%를 차지하는 프린팅 부문은 다양한 산업군의 프린터와 복합기(MFP)를 생산하고 있다. 사내에서 개발되는 프린터 장비용 애플리케이션, 프린터 드라이버는 연결된 장치의 안전과 최신 운영체제와 호환성을 보장해야 한다. 최근까지 캐논은 자체 개발한 코드 서명 시스템을 사용해 왔으나, 진화하는 보안 요구 사항으로 인해 변경을 고려해야 했다. 보안 요구 사항 중 하나는 2023년 6월 이후 CA/B 포럼에 의해 안전한 개인키 보호가 요구된다는 점이다.

한편, 글로벌 소프트웨어 공급망에 대한 공격이 우려스러울 정도로 증가하고 있어, 코드 서명 프로세스를 중앙에서 관리하고 조직 전체에 걸쳐 작동하는 솔루션이 필요했다. 캐논은 자사 시스템의 대폭적인 개선 없이 계속 사용할 수 없어 타사 솔루션을 비교 검토한 결과, 디지서트가 제공하는 클라우드형 DigiCert Software Trust Manager를 이용하기로 결정했다. 이를 통해 엄격한 키 관리와 동시에 사업본부 내 서명 프로세스 가시화, 내부 컴플라이언스 통제를 실현했다.

"한 번의 서명으로 수행하는 작업 흐름의 절반 정도를 줄일 수 있었습니다."

여러 거점에서 진행되는 코드 개발

캐논의 주력 사업 중 하나인 프린팅 부문은 개인용부터 기업용, 그리고 인쇄 산업, 제조업, 식품용 등 인쇄와 관련된 모든 제품을 개발하고 있다. 이를 위해 애플리케이션과 펌웨어의 역할이 매우 크다. 해당 애플리케이션에 요구되는 보안 요구사항이 높기 때문에 전통적으로 코드 사이닝 인증서와 코드 서명 시스템을 사용해 왔다. 이를 통해 접속하는 컴퓨터 등의 안전을 보호하고, 최신의 다양한 OS에서도 작동할 수 있도록 보장한다.

CA/B 포럼의 BASELINE REQUIREMENT (기본 요건) 업데이트 대응 및 사내 플로우 변경

2022년 11월, 전 세계적으로 코드 사이닝 인증서와 그 개인키 유출 사건이 빈번하게 발생함에 따라 CA/B 포럼은 개인키 생성 및 보호 요건과 관련하여 코드 사이닝 인증서의 Baseline Requirement(기본 요건) 변경을 결정하였다. OV 코드사이닝 인증서의 개인키도 EV 코드사이닝 인증서와 마찬가지로 FIPS140-2 Level 2 또는 Common Criteria EAL 4+ 이상의 안전한 HSM에 저장해야 한다고 결정한 것이다. 캐논은 보다 엄격한 보안 요구사항이 있는 EV 코드 사이닝 인증서로 전환을 검토 중이며, 개인키 보호 요구사항은 사업부 내 업무에 큰 변화를 가져올 것으로 보인다.

따라서 기존에 사용하던 서명도 새로운 표준에 맞게 시스템을 개조하여 계속 사용할 것인가가 새로운 과제로 떠오르고 있다.

솔루션

코드 서명 업무 가시화 및 역할 기반 액세스 관리

이러한 상황 속에서 캐논은 자체 서명 시스템 개조 및 운영 비용과 외산 시스템의 비용, 키 관리, 서명 프로세스 가시화를 통한 내부 컴플라이언스 관리의 이점을 종합적으로 비교하여 DigiCert Software Trust Manager를 도입하기로 결정했다.

Software Trust Manager는 캐논이 조직 전체의 모든 코드 서명 작업을 추적하고 모니터링할 수 있도록 가시성과 제어 기능을 제공한다. 이러한 전사적인 모니터링을 통해 회사의 보안팀은 아래 세 가지를 파악할 수 있게 되었다:

- 코드 서명이 언제, 어떤 시스템에서 이루어졌는지?
- 누가 서명 업무를 수행했는가?
- 사용 된 인증서, 개인 키는 무엇인가?

이러한 세밀한 가시성을 통해 보안팀은 이상 징후와 잠재적 위협을 기존보다 더 빠르게 감지하고 대응할 수 있게 됐다. 또한, Software Trust Manager는 역할 기반 접근 제어를 제공함으로써 캐논은 개발자의 책임을 크게 줄일 수 있었다. 이제 개발자는 인증서나 키 관리까지 신경 쓸 필요가 없고, 코드 서명만 신경 쓰면 된다.

이러한 업무 분리는 개발자의 업무 부담을 줄였을 뿐만 아니라, 휴먼 에러와 잠재적 보안 침해의 위험도 최소화했다.

SoftwareTrust Manager 관리 담당자는 "SoftwareTrust Manager가 번거로운 키 관리 등을 서명 멤버로부터 해방시켜줌으로써 서명 멤버가 한 번에 서명하는 작업 흐름의 절반 정도를 줄일 수 있었다. 또한, 코드 서명 업무의 모든 것을 관리 및 통제할 수 있게 되어 사업본부 내 코드 서명 업무 관리에 소요되는 시간을 크게 줄일 수 있었다"고 말했다.

다양한 소프트웨어 개발 환경과 개발자의 취향에 대응하는 서명

캐논이 Software Trust Manager를 선택한 또 다른 큰 이유는 서명 업무 흐름의 효율화다. Software Trust Manager에서 서명을 하는 방법은 서명 도구와 플랫폼에 따라 여러 가지다.

특히 마이크로소프트의 SignTool을 통한 서명 방법에는 명령줄에서 호출하여 서명하는 방식과 'DigiCert Click-to-Sign'이라는 우클릭으로 서명할 수 있는 방식이 있으며, 특히 후자는 미리 설정을 해두면 쉽게 서명을 할 수 있기 때문에 업무 부하를 크게 줄일 수 있다.

일반 PC와 동일하게 조작할 수 있다는 점에서 폭넓은 사용자들의 지지를 얻을 수 있을 것으로 판단했다.

실제 사용자들은 "CLI 에서 서명하는 방식보다 우클릭으로 쉽게 서명을 할 수 있게 되어 IT 활용 능력에 상관없이 다양한 사람들이 서명을 할 수 있게 되었다"는 호평을 받고 있다.

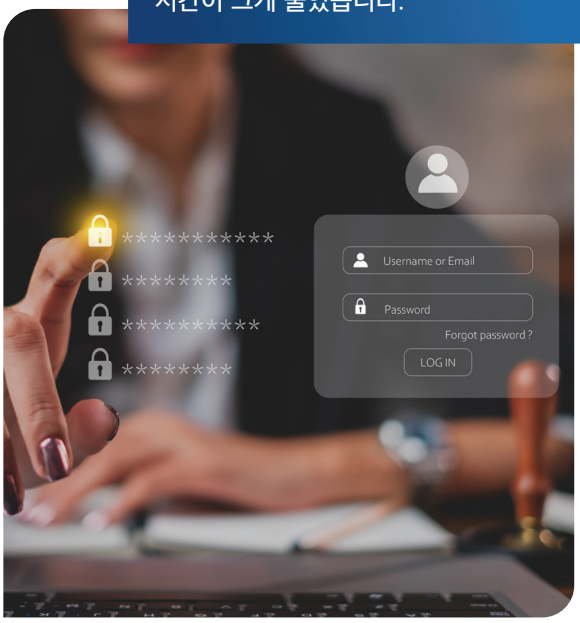
또한 Click-to-Sign은 서명 시스템에 애플리케이션을 업로드하고 서명 실행 후 서명 시스템에서 다운로드하는 기존 방식보다 서명에 소요되는 시간을 절반으로 줄일 수 있다고 한다. 또한 서명 멤버는 서명만 하면 자동으로 로그가 남기 때문에 관리 시스템에 이력 입력이 필요 없어 서명 관리 측면에서도 효율성과 데이터 무결성을 확보할 수 있게 되었다.

이처럼 획기적인 시간 단축을 실현하고 있는 Click-to-Sign이지만, 캐논의 개발을 지원하기 위해 여러 가지 요구사항이 제안되었다.

DigiCert는 신속한 개발을 통해 고객 혜택과 요구사항에 따라 단기간에 업데이트를 진행하기 때문에, 이를 실현하면 효율성이 더욱 향상될 것으로 보인다.

DigiCert Click-to-sign

"사업본부 내 코드 서명 업무 관리에 소요되는 시간이 크게 줄었습니다."



디지털 트러스트에 대한 캐논의 코드에 대한 접근 방식에 대한 전망

서명키 관리와 기존 관리 시스템 교체를 계기로 도입된 SoftwareTrust Manager의 도입이었지만, 보안 소프트웨어 개발 프레임워크가 다루는 범위는 매우 광범위하다. 소프트웨어에 서명을 하기 때문에 안전한 것이 아니라, 안전하게 만들어진 소프트웨어에 서명을 하는 것이다. 또한, 최근 소프트웨어는 많은 라이브러리와 컴포넌트를 조합하여 구성된다. 그 중 하나의 컴포넌트에서 취약점이 발견되면 해당 컴포넌트를 사용할 수 없게 하는 조치를 취해야 하고, 사용하는 컴포넌트의 취약점을 항상 관리해야 한다.

또한, 개발 방법도 항상 새로운 수단이 나오고 있으며, 이러한 변화에 대해서도 소프트웨어 개발 프레임워크의 방법을 활용하여 항상 사용자에게 안전을 제공해야 한다.

SoftwareTrust Manager는 이러한 소프트웨어 개발 프레임워크에 대응하기 위해 다양한 통합, 연계 기능을 구현하고 있다. 코드를 바이너리 스캔하여 취약점이나 비밀 정보를 찾아내는 위협 탐지 기능, 스캔 결과를 바탕으로 SBOM을 생성하는 기능, 생성된 SBOM에 대해 변조를 방지하는 문서 서명을 수행하는 기능 등을 갖추고 있다.

그래서 관리 담당자에게 여러가지 기능 중 가장 먼저 사용한 기능에 대해 물어보았다.

”이미 사용자는 코드 서명에 사용하는 개인키에 접근하지 않기 때문에 안전한 소프트웨어 서명과 키 관리를 실현할 수 있다. 하지만 만약 사용한 라이브러리나 컴포넌트에서 취약점이 발견된다면, 서명마다 개인키를 순환시켜 특정 서명을 한 소프트웨어만 무효화할 수 있다. 이 기능은 흥미롭다.” SoftwareTrust Manager 관리 담당자는 이렇게 말했다.

미래를 위한 준비

앞으로 일본뿐만 아니라 해외, 그리고 각 업계 단체에서 소프트웨어 코드의 보안 표준을 각각 정하고 있다. 이에 대응하기 위해서는 많은 노력이 필요하다. 또한 생성 AI의 발전으로 양자 컴퓨터의 실현이 앞당겨질 것이라는 보도가 많이 나오고 있다. 이는 양자컴퓨터로 인해 각종 발명이나 예측 등의 정확도가 높아질 것으로 기대되는 반면, 현재 활용되고 있는 암호는 쉽게 해독될 것으로 예상되기 때문이다.

이는 코드 서명도 마찬가지이며, 해독 및 변조될 수 있는 리스크가 문제가 된다.

이에 대응하기 위해서는 인증서, 서명, 그리고 그것들이 어떤 암호 강도 알고리즘인지에 대한 인벤토리를 정비하고, 각 표준-규격에 대한 대응 현황을 제대로 파악하여 우선순위를 정하고 대책 계획을 실행하는 것이 중요하다.

이때 SoftwareTrust Manager를 통해 인벤토리를 중앙에서 관리하고 엄격한 통제가 가능한 체제는 미래를 위한 강력한 대비책이 될 것이다.

“서명마다 비밀키를 로테이션함으로써 특정 서명을 한 애플리케이션만 해지시킬 수 있다.”