SYNOPSYS®
Silicon to Software™

CyRC

2019 오픈소스 리스크 분석 리포트

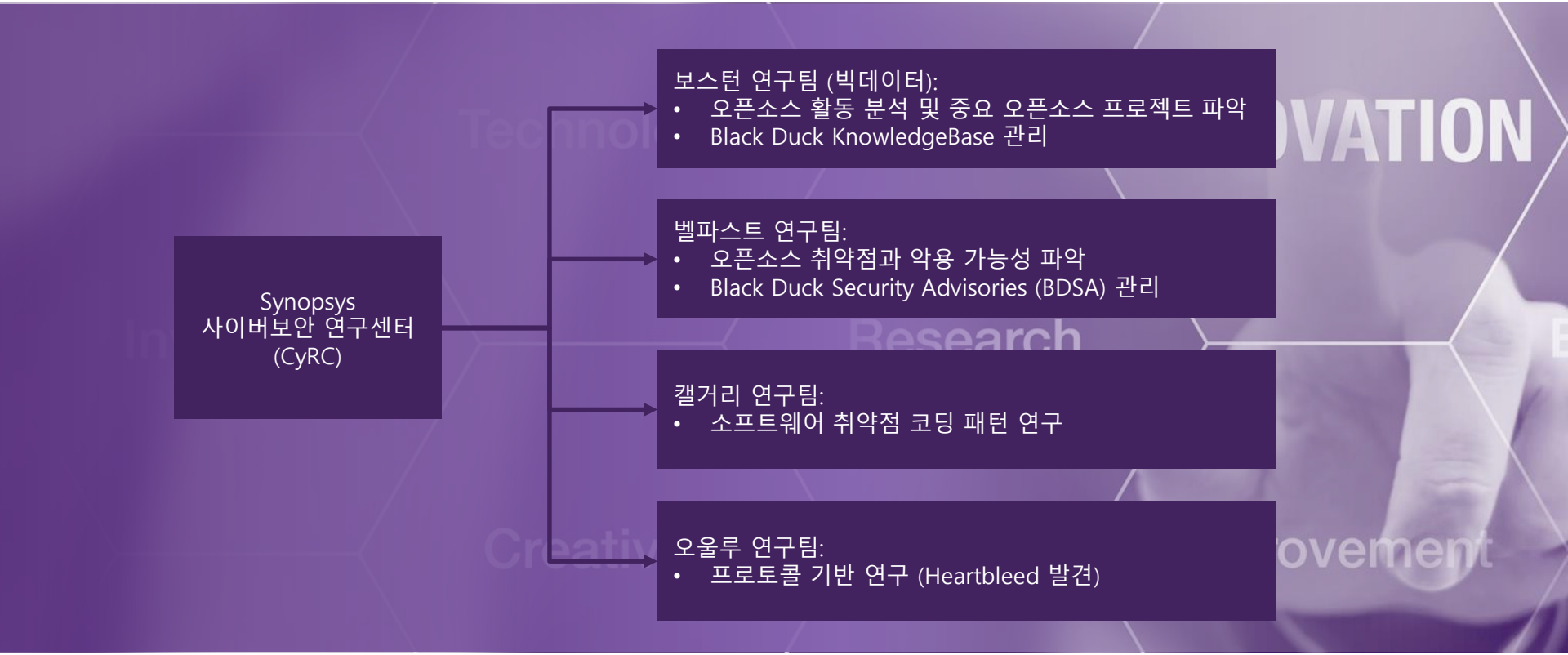
데이터로 보이는 오픈소스의 현재와 미래

Synopsys / 정성훈 차장

목차

1. 오픈소스 리포트 데이터의 이해
2. 리포트 분석
3. 결론

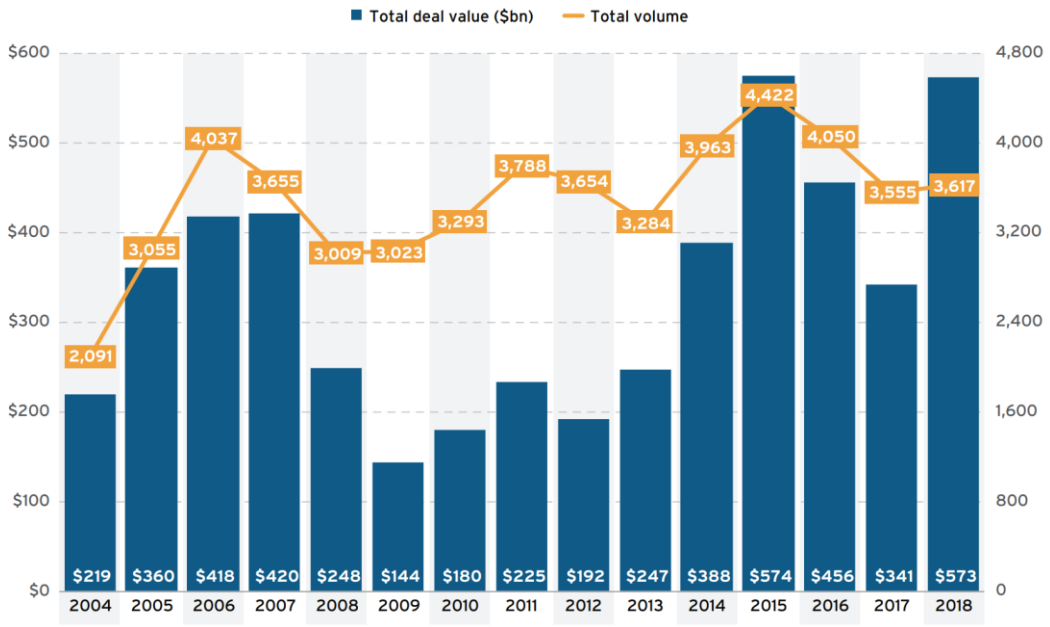
Synopsys 사이버보안 연구 센터(CyRC)



데이터 출처

기술 인수에 매년 수십억 달러가 사용

연간 전세계 기술 및 통신 분야 거래 흐름



출처: 451 리서치의 MSA KnowledgeBase.
공개 및 예상 값 포함

$573B
2018년 인수

68%
2017-2018년 성장

상위 5개 산업
소프트웨어

CyRC SYNOPSYS®

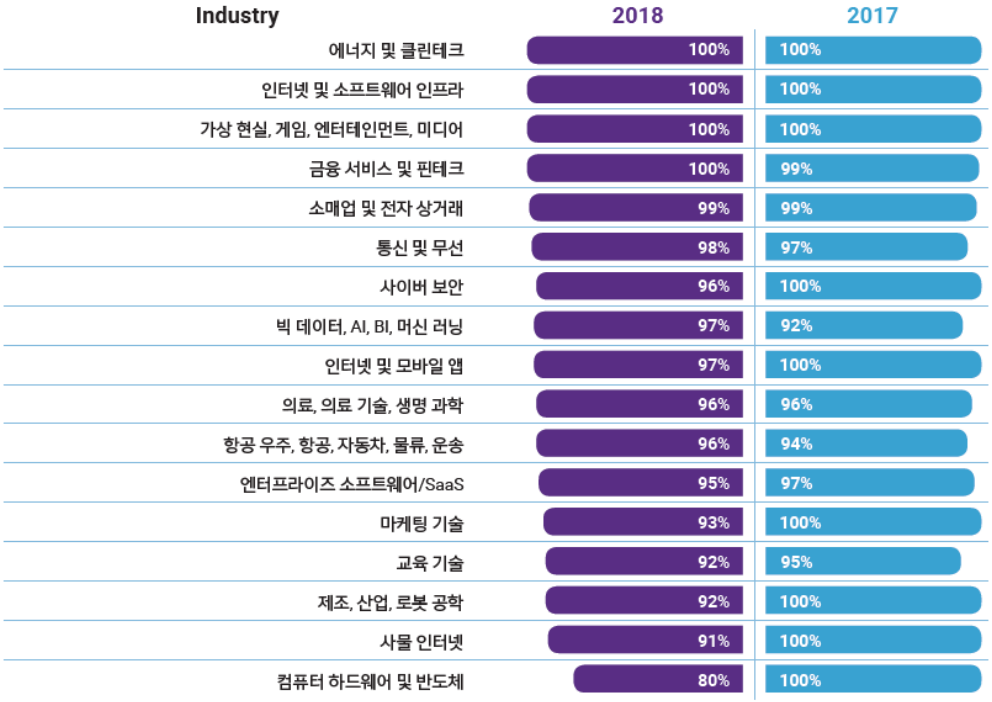
모든 산업에서 1200개 이상의 상용 코드베이스 연구 결과

Industry	Distribution
엔터프라이즈 소프트웨어/SaaS	23%
헬스 케어, 의료 기술, 생명 과학	11%
금융 서비스 및 핀테크	10%
빅 데이터, AI, BI, 머신 러닝	9%
소매업 & 전자 상거래	7%
항공 우주, 항공, 자동차, 물류, 운송	6%
인터넷 & 소프트웨어 인프라	5%
사물인터넷	5%
통신 & 무선	4%
사이버 보안	3%
가상 현실, 게임, 엔터테인먼트, 미디어	3%
제조, 산업, 로봇공학	3%
인터넷과 모바일 앱	3%
마케팅 기술	2%
교육 기술	2%
컴퓨터 하드웨어 & 반도체	2%
에너지 & 클린 테크	1%

리포트 주요 분석 내용

오픈소스로 구동되는 최신 응용프로그램

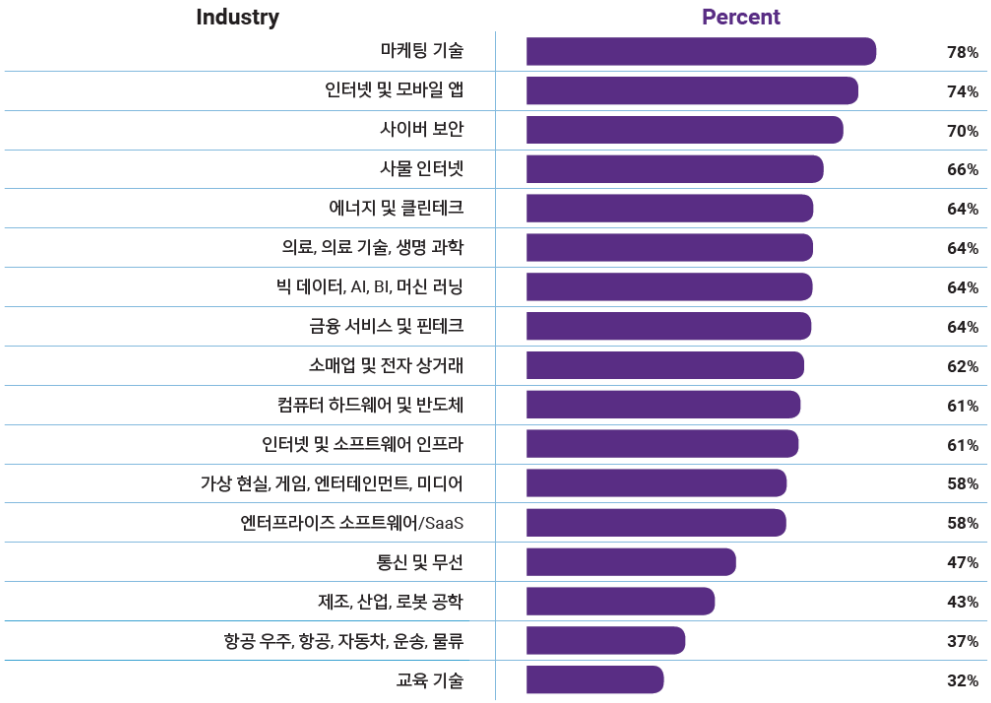
하나 이상의 오픈소스 구성 요소가 있는 코드베이스

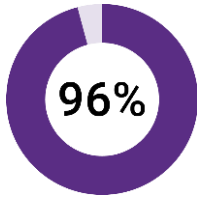


Industry	2018	2017
에너지 및 클린테크	100%	100%
인터넷 및 소프트웨어 인프라	100%	100%
가상 현실, 게임, 엔터테인먼트, 미디어	100%	100%
금융 서비스 및 핀테크	100%	99%
소매업 및 전자 상거래	99%	99%
통신 및 무선	98%	97%
사이버 보안	96%	100%
빅 데이터, AI, BI, 머신 러닝	97%	92%
인터넷 및 모바일 앱	97%	100%
의료, 의료 기술, 생명 과학	96%	96%
항공 우주, 항공, 자동차, 물류, 운송	96%	94%
엔터프라이즈 소프트웨어/SaaS	95%	97%
마케팅 기술	93%	100%
교육 기술	92%	95%
제조, 산업, 로봇 공학	92%	100%
사물 인터넷	91%	100%
컴퓨터 하드웨어 및 반도체	80%	100%

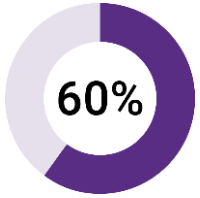
혁신의 기반이 되고 있는 오픈소스

코드베이스에서 오픈소스가 차지하는 비율





오픈소스를 포함한
코드베이스



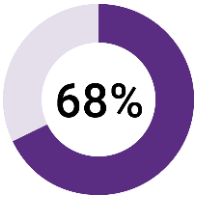
평균
오픈소스 비율

CyRC SYNOPSYS®

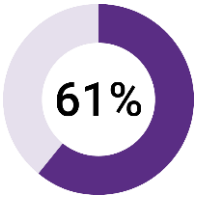
여전히 중요한 오픈소스 라이선스 컴플라이언스

라이선스 충돌이 있는 코드베이스의 백분율

Industry	2018	2017
마케팅 기술	79%	77%
소매업 및 전자 상거래	74%	61%
인터넷 및 소프트웨어 인프라	74%	78%
빅 데이터, AI, BI, 머신 러닝	72%	72%
사물 인터넷	72%	75%
교육 기술	70%	77%
의료, 의료 기술, 생명 과학	70%	71%
사이버 보안	68%	76%
통신 및 무선	68%	100%
항공 우주, 항공, 자동차, 운송, 물류	68%	78%
에너지 및 클린테크	67%	78%
금융 서비스 및 핀테크	65%	78%
엔터프라이즈 소프트웨어/SaaS	65%	83%
제조, 산업, 로봇 공학	64%	91%
가상 현실, 게임, 엔터테인먼트, 미디어	63%	92%
인터넷 및 모바일 앱	59%	64%
컴퓨터 하드웨어 및 반도체	52%	72%



라이선스 충돌이 있는
컴포넌트를 포함한
코드베이스

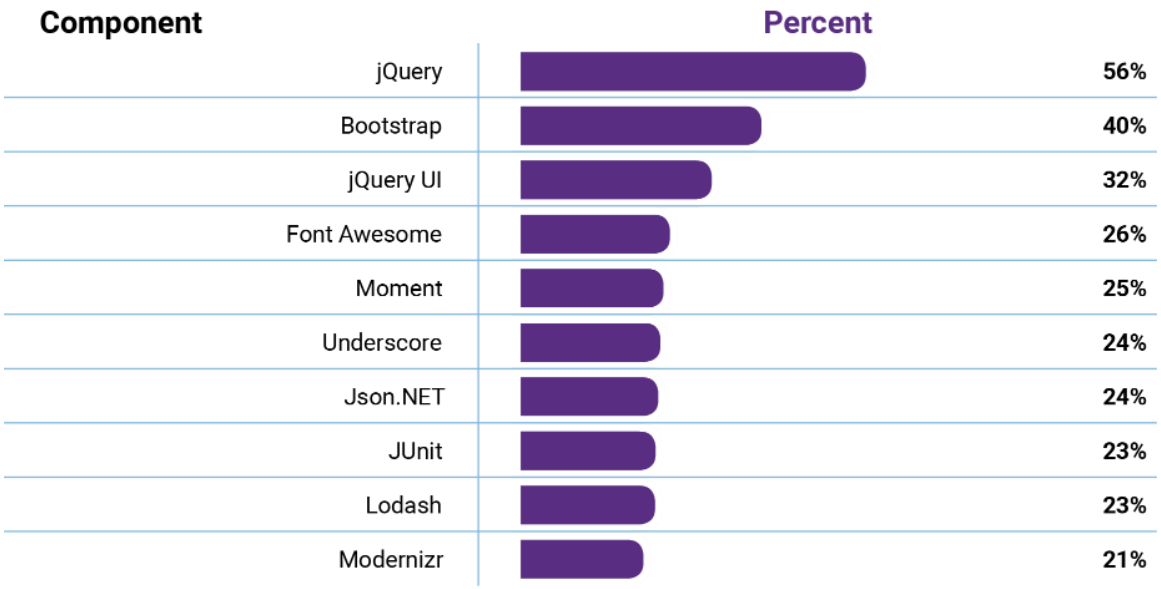


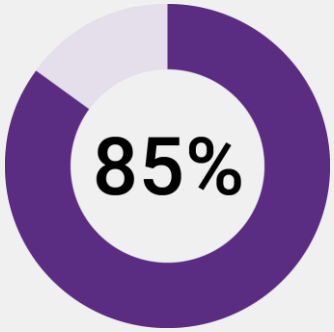
어떤 형태의
GPL 충돌을 포함한
코드베이스

CyRC SYNOPSYS®

오픈소스 사용에서의 운영 요소

상위 10개 오픈소스 컴포넌트가 포함된 코드베이스 비율





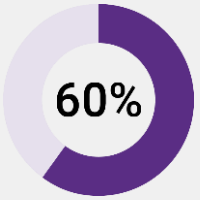
85%의 코드베이스가
4년이 지난 컴포넌트
또는 지난 2년 동안 개발
활동이 없었던
컴포넌트를 포함

CyRC SYNOPSYS®

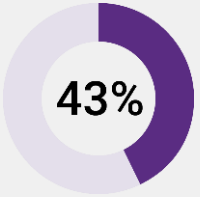
중요해 지고 있는 오픈소스 보안

상위 10개 고위험 취약점이 포함된 코드베이스 백분율

CVE	Percent
CVE-2018-7489	12%
CVE-2017-7525	11%
CVE-2017-15095	11%
CVE-2015-6420	10%
CVE-2014-0050	9%
CVE-2017-15708	9%
CVE-2014-0107	9%
CVE-2016-3092	6%
CVE-2016-8735	5%
CVE-2014-3567	5%



취약점을 포함한
코드베이스 비율



10년이 넘은
취약점을 포함한
코드베이스 비율

CyRC SYNOPSYS®

Jackson-databind (CVE-2018-7489, CVE-2017-7525 and CVE-2017-15095)

기능

Java 객체 데이터를 묶어 직렬화/역직렬화(Serialization/deserialization) 해 줌

핵심 문제점

Jackson-databind 2.7.0 혹은 이후 버전에서 특정 클래스 유형을 위한 동적 다형성 바인딩 모델(Dynamic polymorphic binding model) 적용하여 원격 코드 실행을 가능하게 하는 취약점 발생

CVE-2000-0388

많은 개발자들의 나이보다 더 오래된 취약점으로 2018 OSSRA 데이터세트에서 발견됨

보고 날짜

1990년 5월 9일

영향

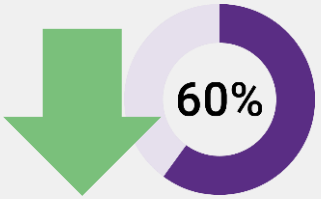
FreeBSD 3.4 이전 버전에서 TERMCAP 환경 변수를 처리 할 때 버퍼 오버플로가 발생하면 로컬 취약점 공격으로 권한 상승

발전하고 있는 오픈소스

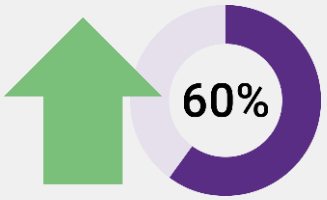
16% 코드베이스당 사용된 컴포넌트가 2017년 257개 대비 2018년에는 298개로 16% 증가했음

20 가장 널리 사용되는 오픈소스 라이선스가 전체 코드베이스의 98%를 차지함

대부분의 산업 영역에서 오픈소스 라이선스 충돌이 줄어듦

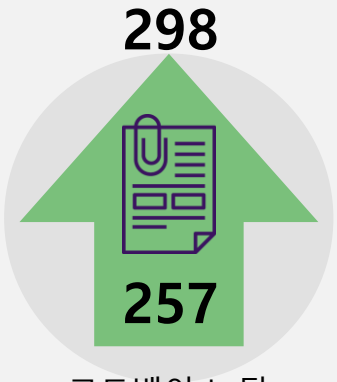


패치 되지않은 취약점 23% 감소

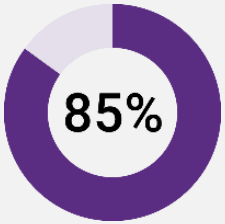


오픈소스 사용량 5% 증가

미래의 더 나은 오픈소스 사용을 위해 우리가 반드시 알고 있어야 할 부분



코드베이스 당
컴포넌트



사용되지 않거나 유지
관리되지 않는 구성 요소 포함

- **Rule #1** – 무엇이 있는지 모르면 패치도 할 수 없다.
  - 패치를 위해 코드 매치가 되어야 하며, 코드의 출처를 정확히 알아야 함
- 오픈소스는 소스 코드 자체에 관한 것 뿐만 아니라, 공유된 것의 재사용에 관한 것
  - 바이너리 레파지토리는 코딩을 단순화하지만 보안을 악화시킴
- "오픈소스"로 알려진 공급 업체는 없음

CyRC SYNOPSYS®

결론

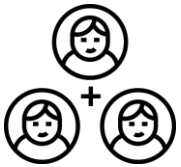
주요 내용

오픈소스 사용은 최신 애플리케이션에서의 핵심

- 이점을 얻을 수 있는 전략 수립
- 모든 개발 및 운영팀이 주요한 오픈소스 컴포넌트들을 잘 식별 할 수 있도록 교육

개발자와 오픈소스 거버넌스의 시작

- 오픈소스 컴포넌트 선택 시 라이선스의 영향을 이해하도록 모든 개발자들을 교육
- 오픈소스 컴포넌트 버전을 나중에 사용할 수 있도록 캐시한 경우 정기적으로 패치가 되는지 확인



오픈소스 커뮤니티와 소통

- 새로운 기능, 중요한 문제 및 패치에 대한 인지는 커뮤니티를 통해 이뤄짐
- 개발팀의 참여를 장려하고, 공유 소유 의식을 증진 시켜야 함

SYNOPSYS®

Build secure, high-quality software faster

CyRC SYNOPSYS®