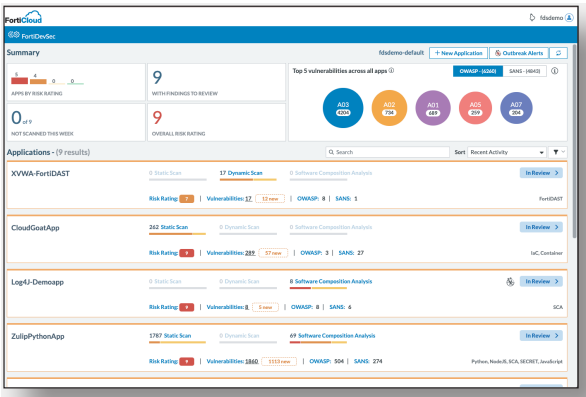
데이터 시트

FortiDevSec

형식

호스팅

CI/CD 파이프라인에서 지속적 애플리케이션 보안 테스트



소프트웨어 애플리케이션은 어디에나 있고, 비즈니스의 성패는 업무용 소프트웨어 애플리케이션을 점점 더 빨리 개발하고 배포하는 능력에 달렸습니다.

요즘은 출시 기간이 특히 중요하기 때문에, 기존의 워터폴 방식으로 애플리케이션을 개발하는 전례를 따라서는 뒷일을 도저히 감당할 수 없을 지경입니다.

워터폴 모델이란 순차적인 방식으로, 애플리케이션의 변경 사항을 기껏해야 몇 달에 한 번씩 배포하고, 개발팀은 이전 단계가 순조롭게 마친 상태에서야 다음 단계의 개발과 테스트로 넘어가게 됩니다.

지금의 애플리케이션 개발팀은 애자일 모델 및 DevOps 방법론을 도입해 신속한 앱 개발과 배포를 지향합니다. 애자일 모델에서는 개발과 테스트가 동시에 이루어지고, 끊임없이 반복됩니다. 애플리케이션 변경 사항을 클라우드에 매우 자주 배포하므로, 기획팀, 개발팀, 보안팀이 전보다 훨씬 긴밀하게 협업하고 소통하여 턴어라운드 타임이 대폭 단축됩니다. 이런 상황으로

인해 애플리케이션을 구축해 클라우드에 배포하기 위해 거치는 워크플로를 자동화해야 하게 되었고, 나아가 DevOps라는 역할이 대세로 떠오르게 되었습니다. 이런 자동화가 가능하려면 지속적 통합/지속적 배포(CI/CD) 도구를 사용해야 하기 때문입니다.

애플리케이션 보안(AppSec) 테스트 역시 CI/CD 과정 중 자동화 대상에 해당하며, CI/CD 패러다임에 보안 조치가 일부분이 되려면 개발 사이클의

초기 단계(원점 회기[shift-left])에 통합되야합니다이런 상황에서 현재 수많은 AppSec 테스트 제품이 제 몫을 다하지 못합니다. 개발자와 Devops 담당자는 보통 AppSec 테스트 제품의 전문 지식이 높지 않으며, 이런 도구가 기존 담당자들에게 높은 사용자 경험을 제공하지 않으므로 효과적으로 활용할 수가 없기 때문입니다. 간단히 말해, DevSecOps 기반이 아니라고 할 수 있겠습니다.

DevSecOps는 개발(development), 보안(security), 운영(operation)의 줄임말입니다. 소프트웨어 개발 수명 주기 전체, 즉 첫 설계 고안 시점부터 통합, 테스트, 배포, 소프트웨어 제공에 이르기까지 모든 단계에 보안을 자동화하여 통합하는 것을 가리킵니다.

주요 장점

- **DevSecOps 자동화**
  애플리케이션 보안 전문 지식이 없어도 DevOps 프로세스에 애플리케이션 보안 기능 추가
- **공격표면 전체 가시성 확보**
  소스 코드, 오픈 소스 또는 타사 구성요소, 컨테이너 이미지, IaC, 런타임 공격 벡터 등 웹 앱에 존재하는 모든 보안 리스크 이해
- **통합형 대시보드**
  사용하기 간편한 포털이 다양한 유형의 스캔을 통해 발견한 보안 리스크를 정규화, 집계, 통합
- **지능적 우선순위 지정**
  보안 문제를 순위가 매겨진 목록으로 표시하고 모든 스캔 유형에 걸친 지능형 스캔 분석도 함께 기재, OWASP 10대 취약성 및 CWE/SANS 상위 25개 취약성을 필터링하여 우선순위 지정
- **간편하고 손쉬운 관리**
  설정 및 관리 오버헤드 제거. 스캐너를 설정하거나 업데이트할 필요없이 최신 스캐너가 자동으로 업데이트 및 설정. 사일로화된 플러그인 없이 모든 스캔에 통합 구성 적용

주요 기능

혁신적인 제품

AppSec 테스트는 무척 단편화된 형태이기도 합니다. AppSec 스캔 중에는 앱의 취약성을 전부 알아내려면 애플리케이션에서 직접 실행해야 하는 종류가 많은데, 이들을 별개의 여러 제품이 제공하는 것이 보통입니다. 제품 여러 개를 사용해야 하는 솔루션은 단편화를 초래하고, DevSecOps로 AppSec을 지원하는 데 차질을 빚습니다.

지금 업계에는 아예 DNA부터 DevSecOps를 타고난, 혁신적인 AppSec 제품이 필요합니다. 이는 개발자와 DevOps가 특수한 보안 전문 지식 없이도 손쉽게 사용할 수 있는 제품이어야 합니다. 또한 SAST, DAST, SCA, , Secret, 컨테이너 이미지, IaC 파일 등 다양한 유형의 AppSec 스캔을 모두 다룰 수 있도록 종합적인 서비스 범위를 제공해야 하기도 합니다.

FortiDevSec은 Fortinet의 DevSecOps 제품입니다. FortiDevSec은 클라우드/SaaS 기반 지속적 앱 보안 테스트를 제공하며, 이는 처음부터 기본적으로 소프트웨어 개발자와 DevOps에 주안점을 두고 구축/개발된 제품 입니다. FortiDevSec을 이용하면 개발 수명 주기 초창기부터 곧바로 애플리케이션의 보안 취약성을 찾아 앱 보안에 원점 회귀 아키텍처를 적용할 수 있으므로, 앱이 배포(Production)되기 전에 문제를 신속하게 찾아 해결할 수 있습니다.

FortiDevSec은 대상 애플리케이션의 DevOps CI/CD 파이프라인에 .통합 됩니다. 소스 코드 스캔, 오픈소스/타사 라이브러리, 암호, 컨테이너 이미지, IaC(Infrastructure a Code) 파일 및 라이브 웹 앱 URL 스캔 등 종합적인 애플리케이션 스캔을 제공합니다. 그런 다음 보안 문제를 집계하여 사용이 간편한 웹 포털에 표시해 줍니다. 지능형 노이즈 감소를 통해 중대한 취약점에 대한 업무 우선순위를 지정할 수 있습니다.

최신 앱 개발을 위한 단순한 보안

최신 앱 개발은 애자일 모델을 사용한 신속한 애플리케이션 개발, 클라우드 네이티브 특성 이해, 마이크로 서비스 및 컨테이너 기반 아키텍처 사용합니다., 이는 CI/CD를 사용해 빌드와 배포 자동화, 애플리케이션 보안 테스트까지 자동화해야 할 필요성이 결합된 결과 입니다.

FortiDevSec은 개발자와 DevOps를 위해 지속적 앱 보안 테스트를 오케스트레이션하고 자동화하여 애플리케이션 CI/CD DevOps 수명 주기에 직접 통합합니다. DevOps는 CI/CD에 코드를 몇 줄 복사해 넣기만 하면 FortiDevSec을 통합할 수 있고, AppSec 전문 지식이 부족하더라도 AppSec의 동작효율이 증가하여 DevOps의 프로세싱의 일부분처럼 빠르게 동작 됩니다. . FortiDevSec는 각종 주요 CI/CD 도구, 개발 언어, 프레임워크를 모두 지원합니다.

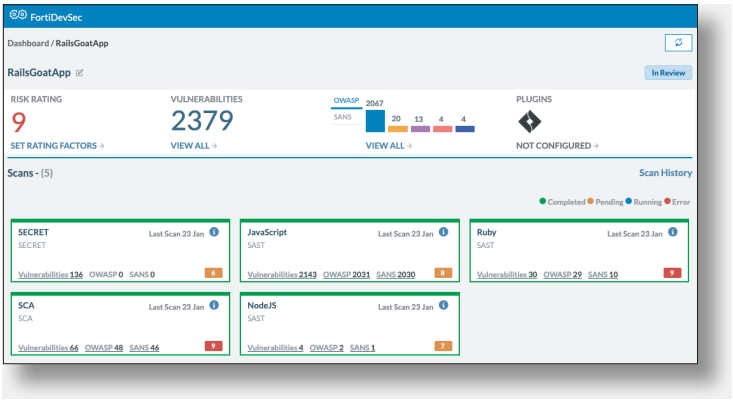
DevOps 입장에서는 이 제품을 이용하면 통합형 yaml 구성을 통해 모든 앱 보안 스캔 유형을 실시할 단 하나의 자동화 레이어를 얻게 되는 셈입니다. 스캐너를 여러 개 사용하기 위해 플러그인을 여러 개 포함할 필요도 없습니다. 스캐너는 도커화한 이미지로 제공되며 항상 최신 버전으로 업데이트되기 때문에 전반적으로 관리하기 매우 간편합니다.

주요 기능

종합적 취약성 관리

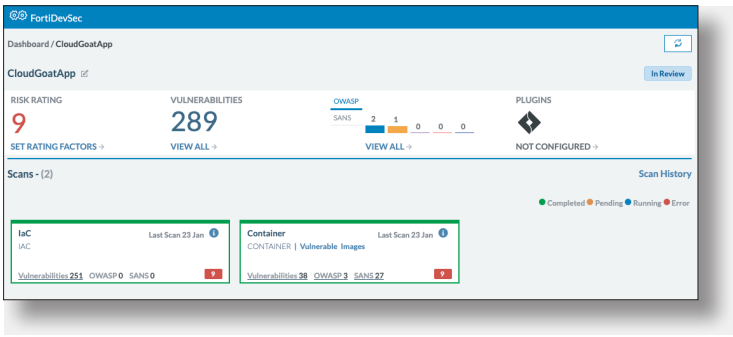
애플리케이션은 여러 가지 공격 벡터에 대비해 보안을 확보해야 하고, 그러려면 다양한 유형의 스캐너를 사용해 보안 테스트를 거쳐야 합니다.

정적 분석 또는 소스 코드 테스트(SAST)의 경우, 애플리케이션 자체의 소스 코드를 스캔합니다. SCA/OSS는 애플리케이션에 포함된 타사 라이브러리(대개 오픈소스 라이브러리)를 스캔합니다. 암호(Secret) 스캔은 코드 중 오픈되어 있는 비밀번호 텍스트를 스캔합니다. DAST, 즉 동적 테스트는 프런트 엔드를 이용해 웹 어플리케이션을 분석하여 시뮬레이션한 공격을 통해 취약성을 찾아냅니다. 컨테이너 스캔을 실시하면 구축 중에 생긴 컨테이너 이미지에 포함된 취약성을 찾을 수 있습니다. 코드형 인프라(IaC) 스캔의 경우 인프라가 생성되기도 전에 그 안에 포함된 구성 오류를 찾아냅니다.



FortiDevSec에는 위의 모든 스캔 유형이 포함되어 있어 종합적인 취약성 관리를 제공합니다. 동적 스캔(DAST)은 포티넷의 FortiDAST 단일 제품으로도 제공되며, FortiDevSec은 FortiDAST를 포함하고 있습니다.

FortiDevSec이 각각의 애플리케이션 내부를 잘 살펴 필요한 유형의 스캔이 무엇인지 자동으로 선택합니다. 이는 개발 언어나 프레임워크와 같이 대상 애플리케이션의 특성을 바탕으로 합니다. 스캐너는 FortiDevSec 에이전트에 도커화된 이미지 형식으로 자동 다운로드되고 업데이트됩니다.

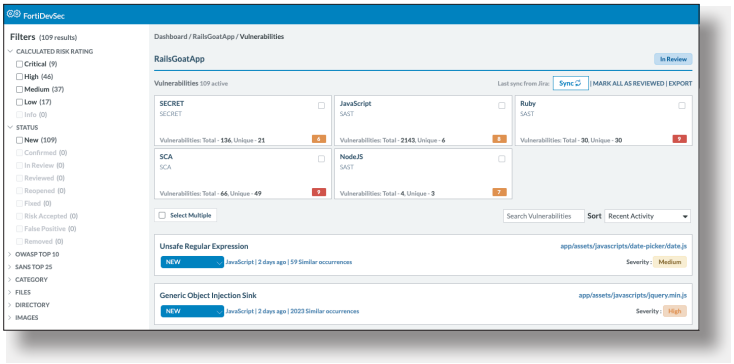


통합형 대시보드

FortiDevSec은 사용이 간편한 포털을 제공합니다. 사용자는 이 포털에 로그인하여 모든 애플리케이션의 모든 문제와 각종 다양한 스캔 유형을 모두 조회할 수 있습니다. 이제는 수도 많고 다양하며 단편화된 스캐너마다 여러 개의 포털을 사용하지 않아도 됩니다.

스캔 결과는 우선 여러 스캔 유형에 걸쳐 정규화됩니다. 리스크 등급 평가, 리스크 카테고리, 설명까지 모두 정규화합니다. 그런 다음 결과를 집계하고 다양한 필터와 함께 제시하여 사용자가 가장 중요한 것부터 우선순위를 정해 해결할 수 있습니다. OWASP 10대 취약성과 CWE/SANS 상위 25개 취약성은 따로 강조 표시되며, 사용자가 필터를 적용해 우선수위를 지정할 수 있습니다.

보고된 문제가 너무 많으면 개발자가 부담을 느끼게 마련입니다. FortiDevSec은 그런 상황의 스트레스를 덜기 위해 여러 스캔 결과에 걸쳐 지능적으로 결과의 상관관계를 정립하고, 그에 따라 리스크 등급 평가를 조절합니다. 이렇게 하면 보고된 문제에서 노이즈를 줄이는 데 도움이 되고, 따라서 개발자는 가장 중요한 문제를 해결하는 데만 집중하면 됩니다.



주문 정보

FortiDevSecOps는 사용자(즉, 개발자) 수에 따른 라이선스를 제공합니다.

여기에는 고객을 위해 FortiDevSec으로 보안 테스트를 실시하는 모든 애플리케이션을 다루는 개발자 전원을 포함합니다. 일반적으로 이런 개발자는 애플리케이션 코드 소스 리포지토리(예: GitHub)에서 계정과 체크인 코드를 하나 갖게 됩니다.

우선, FortiDevSec으로 스캔하는 애플리케이션의 리포지토리에 코드를 체크인/커밋하는 개발자의 수를 셉니다. 둘째, FortiDevSec으로 스캔하는 모든 애플리케이션에서 개발자 수를 세어 고객 라이선스 레벨에서 총 인원수를 계산합니다. 물론 개발자 한 사람이 애플리케이션을 둘 이상 다루는 경우도 있는데, 그럴 때는 두 번 세지 않아도 됩니다.

이렇게 계수한 개발자/사용자 수는 FortiDevSec 포털에 로그인하는 사용자 수와는 다릅니다. 대부분의 경우, 소스 코드 리포지토리를 이용해 계산한 개발자 총 인원수보다 후자의 수가 적습니다.

현재 FortiDevSec은 사용자 다섯 명까지 포함하는 SKU를 제공하고 있습니다. 이 SKU는 스택 가능하므로, 더 많은 사용자를 포함할 수도 있습니다. 이러한 사용자는 애플리케이션(해당 사용자가 직접 다루는 앱) 수에 제한 없이 온보딩에 액세스할 수 있고, SAST, 암호, 컨테이너, IaC 스캔 시 FortiDevSec에서 횟수 제한 없이 스캔을 이용할 수 있습니다.

스캔할 애플리케이션 수가 제한되는 것은 DAST 스캔 하나뿐입니다. DAST 스캔은 내부에서 다른 제품, 일명 FortiDAST로 제공합니다. 사용자 5인용 FortiDevSec 라이선스마다 앱 5개에 해당하는 DAST 스캔 기능이 포함됩니다. DAST 스캔이 필요한 애플리케이션이 다섯 개를 넘는 경우, 별도의 애드온 SKU/라이선스를 구매하시면 됩니다.

제품	SKU	설명
FortiDevSec	FC1-10-DEVSC-513-01-12	FortiDevSec(표준 기능 계층)은 모든 스캐너에서 개발자 사용자 최대 5명까지(스캔할 대상 앱을 다루는 개발자를 모두 세어 포함함) 무제한 스캔, 무제한 앱(SAST, SCA/OSS, 컨테이너, IaC 및 암호)을 제공합니다. 여기에는 DAST 또는 FortiDAST 제공 WebApp 취약성 스캔도 포함하지만, 앱 5개에 한합니다. DAST에 더 많은 앱을 추가하려면 애드온 SKU를 사용하세요. - 연간 구독 방식입니다. FortiCare 지원을 포함합니다.
FortiDAST add-on to FortiDevSec	FC1-10-DEVSC-216-02-12	애드온 FortiDAST 웹 취약성 검사 / FortiDevSec에 DAST 기능 제공. 두 가지 제품 모두 SAAS 버전에서 사용해야 합니다. 이 SKU를 이용하면 FortiDAST를 사용하는 앱 5개를 스캔할 액세스 권한이 제공됩니다. 이는 FortiDevSec 라이선스마다 기본적으로 포함된 DAST 앱 5개에 추가로 제공되는 서비스입니다.

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com

FDS-DAT-R03-20230127