IBM Security

IBM

클라우드에서 애플리케이션 보안 위험을 효과적으로 관리합니다

간단하며 자동화된 테스트를 통해서 보안 요건을 단순화하고 강화할 수 있습니다.

IBM 보안 백서

애플리케이션 보안이 중요한 이유는 무엇입니까?

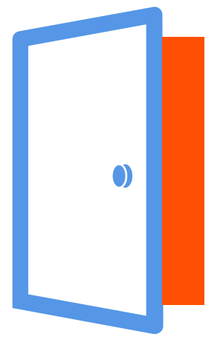
데이터 보안을 장려하기 위해 많은 노력을 했을 것입니다. 그러나, 실행하려는 애플리케이션이 활짝 열린 상태로 남아 있는 기업의 현관문과 같다면 어떻겠습니까? 귀사 조직이 보유한 데이터의 보안을 위해 개별 파일과 기록을 단순히 잠그는 것 이상의 노력을 기울여야 합니다. 애플리케이션 수준에서도 보안을 강화해야 합니다. 애플리케이션이 데이터에 대한 액세스를 제어 할 수 있으며 조직의 IoT(Internet of Things) 인프라까지도 액세스할 수 있기 때문입니다.

수많은 악명 높은 보안 침해는 데이터 보안 관행이 좋지 않아서가 아니라, 응용 프로그램이 취약했기 때문에 발생한 것입니다. 애플리케이션 보안을 배포하면 문제가 있거나 취약한 소프트웨어에 있는 안전하다고 생각하는 데이터를 사이버 범죄자가 아무런 거리낌 없이 절취하지 못하게 할 수 있습니다.

그렇더라도, 애플리케이션 보안은 종종 남아 있으며[1], 위반은 계속 발생합니다. 왜 그런가요? 그 이유 중 하나는, 애플리케이션을 잠그는 것은 파일을 암호화하거나 방화벽을 이용하여 네트워크를 보호하는 것보다 복잡하기 때문입니다. 응용 프로그램 저장소 및 클라우드 기반 인프라에 액세스하는 특수 애플리케이션이 나타났고, 응용 프로그램의 숫자와 유형도 증가했습니다. 한편, BYOD(Bring-Your-Own-Device) 정책이 널리 채택되면서 검사하지 않은 애플리케이션이 늘어나고, 애플리케이션에 연결된 IoT 데이터 소스가 급속도로 확산되었습니다.

애플리케이션 보안이 중요한 경우는 다음과 같습니다.

- 평판이 손상되지 않도록 합니다
- 고객의 신뢰를 유지합니다
- 수정 비용을 지출하지 않습니다
- 손상을 유발하기 전 보안 위험성을 감지하고 대응합니다



한 연구에 의하면, 응답한 개발자의 77 %가 애플리케이션을

77 %

시험을 하지 못하기 때문에 애플리케이션이 취약하다고 합니다.[2]

▸ IBM Application Security on Cloud로 할 수 있는 일에 대한 데모를 보십시오.

1 "애플리케이션 보안을 전략적으로 관리되는 분야로 만드는 방법," ***포네몬(Ponemon) 연구소,*** 2016년 3월.

2 "모바일 애플리케이션 불안정 상태," ***포네몬 연구소,*** 2015년 2월.

조직은 왜 어려운 애플리케이션 보안 성공을 이루려고 하는가?

애플리케이션 보안은 개발자, IT 인력 및 최종 사용자에 이르는 넓은 범위의 특성 상 복잡합니다. 이러한 요소의 조합에 따라 조직은 취약점에 의한 영향을 받을 수 있습니다.

급하게 진행하는 출시
널리 퍼진 "급하게 출시하는" 환경에서 개발자는 종종 시험 리소스가 부족하게 됩니다. 그러나, 애플리케이션 보안은 개발자에게만 의존하지 않습니다. 새로운 소프트웨어에서 제공하는 효율성을 사용자가 요구하기 때문에 애플리케이션을 빠르게 설치해야 한다는 점도 있습니다.

복잡한 애플리케이션
소프트웨어는 범위, 데이터 요구 사항, 언어 및 플랫폼이 매우 다양합니다. 문제가 있는 애플리케이션이 기업 데이터에 직접 연결된 것은 비슷한 데이터가 든 노트북을 잃어버린 것만큼 위험할 수 있으며, 문제점을 모른다면, 보다 더 위험할 수 있습니다. 안전하지 않거나 악의적인 애플리케이션은 보안 취약점을 악용 당하거나, 그 시작부터 안전하지 않았기 때문에 데이터가 노출 될 수 있습니다.

- 위험 기반 애플리케이션 보안 관리에 대한 자세한 정보.

애플리케이션 보안은 우선 순위 대상이 아닙니다
애플리케이션 레이어 취약점은 종종 우선 순위가 낮게 지정되며, 일반적으로 조직은 애플리케이션 중요도에 보호 목적의 우선순위를 지정하지 않습니다. 그리고 애플리케이션은 (보안 상의 상황과 같이) 조직 전반에 분산 된 경우가 많으며, 어떤 애플리케이션이 사용 되는지 어떤 취약성이 가장 심각한지에 대한 가시성이 거의 없습니다.

표준 부족
사용자는 보안 평가에 시간을 할애할 수 없으며, 효과적인 평가 방법을 모릅니다. 보편적인 애플리케이션 보안 표준이 거의 없으므로, 가이드 및 현업 전문 능력을 평가하거나 사용하기가 어려울 수 있습니다.

최근 포네몬 연구소 조사에 따르면

47 %

위험이 증가하거나 크게 증가했다고 응답했습니다[1]

1 "애플리케이션 보안을 전략적으로 관리되는 분야로 만드는 방법," ***포네몬 연구소***, 2016년 3월.

효과적인 애플리케이션 보안은 무엇입니까?

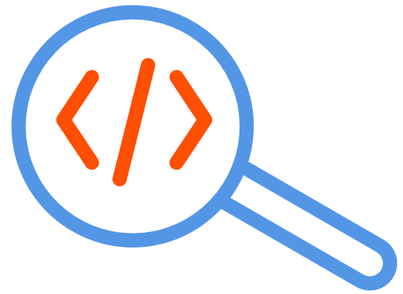
효과적인 애플리케이션 보안 관행은 보안을 프로세스로서 간주해야 하며, 목록 상에서 선택적으로 확인하는 항목으로 보지 않아야 합니다. 따라서, 애플리케이션 보안 평가는 반드시 종합적이며 지속적이어야 합니다.

개발자의 경우, 애플리케이션 보안 평가 프로세스는 지속적인 소스 코드 분석과 함께 소프트웨어 개발 수명 주기에 포함되어야만 합니다. 최종 사용자 조직의 경우, 배포된 모든 새로운 소프트웨어를 검사하고 조직이 이미 사용 중인 애플리케이션을 다시 테스트하여 이 프로세스를 지속합니다.

종합적인 애플리케이션 보안에는 다음이 포함되어야 합니다.

- **확인 및 분류 작업** 현재 사용 중인 애플리케이션
- **정적 평가**-애플리케이션 소스 코드에서 취약성을 검사하는 것은 특정한 보안 취약성 뒤에 숨어 있는 실제 코드를 찾아내는 가장 직접적인 방법입니다
- **동적 평가**-소프트웨어의 목적과 배포된 시점을 평가합니다(예를 들어, 예상되는 크로스 사이트 스크립팅 및 SQL 인젝션 공격에 대해 취약한가?)
- **모바일 애플리케이션 보안 평가** -시장에는 새로운 모바일 애플리케이션이 매우 많습니다
- **검사를 거친 이후에만** 새로운 소프트웨어 배포

애플리케이션은 정기적으로 재평가 되어야 하며, 이 평가는 오픈 웹 애플리케이션 보안 프로젝트(OWASP) 최상위 10개 목록으로 제공되어야 합니다.[1]-새로운 위협에 의해 과거에 안전했던 애플리케이션이 위험하게 될 수 있습니다.



2016년 9월 기준으로

2 백만

Apple iOS 애플리케이션을 다운로드하여 사용할 수 있습니다[2]

그리고,

2.4 백만

이상의 Google Android 애플리케이션도 있습니다.[3]

▸ 위험 기반 애플리케이션 보안 관리에 대한 자세한 정보.

1 Paul Ionescu, "현재 알려진 최상위 10개 애플리케이션 공격," *IBM Security Intelligence*, 2015년 4월 8일.

2 "2016년 6월 선도적인 앱 스토어에서 사용 가능한 앱의 개수," *Statista*, 2016년 6월.

3 "Android 애플리케이션의 개수," *AppBrain*, Accessed, 2016년 10월 13일.

오랜 시간 검증을 거친 IBM 애플리케이션 보안 모범 사례 사용하십시오

조직이 애플리케이션의 보안 위험성을 검사하는 경우, 제한된 예산 그리고 과중한 작업량이 할당 된 보안 및 IT 직원 등의 제약 조건 하에서 운영됩니다. 그러나, 이런 제한 사항이 있다고 해서 보안 보호 개선이 불가능한 것은 아닙니다. 이를 위해, 귀하의 조직은 다음의 모범 사례를 사용해야 합니다.

- **감시**- 계획적이며 자동화된 평가를 사용하여 임시 방편적인 시험이 아닌 철저하며 신뢰성 있는 결과를 제공합니다
- **지속성**- 애플리케이션은 제작 및 보안 시험을 거쳐야 하며, 재시험을 통해 취약성을 최신화해야 합니다
- **우선순위 지정**- 심각도 및 예상되는 비즈니스 영향에 따라 애플리케이션 보안 문제의 우선 순위를 지정하면 비즈니스에 가장 민감한 순서에 따라 문제를 해결할 수 있습니다
- **유연성**- 조직에서 배포한 모든 애플리케이션을 평가하려면 제한적인 구현 요구 사항을 피하는 것이 중요합니다
- **적응성**- 위협은 시간이 따라서 변합니다. 유연한 접근 방식을 사용하면 애플리케이션 보안 제어를 위한 변경이 줄어듭니다
- **적시성**- 개발 프로세스를 방해하거나 실행을 다시 하지 않으려면 개발 수명 주기의 모든 단계에서 애플리케이션을 테스트해야 합니다

IBM® Application Security on Cloud와 같은 통합 애플리케이션 보안 솔루션을 사용하면 보안 빈 틈을 최소화하고 예상되는 취약성 식별을 쉽게 할 수 있습니다. 다른 보안 제품 및 모범 사례와 통합하는 경우, 추가적인 사항이 아닌 포괄적인 보안 프로그램을 통하여 애플리케이션 부분에 대한 위험 완화를 제공합니다.

58 %

전략의 완벽한 배포가 안 된다고 답변했습니다.[1]

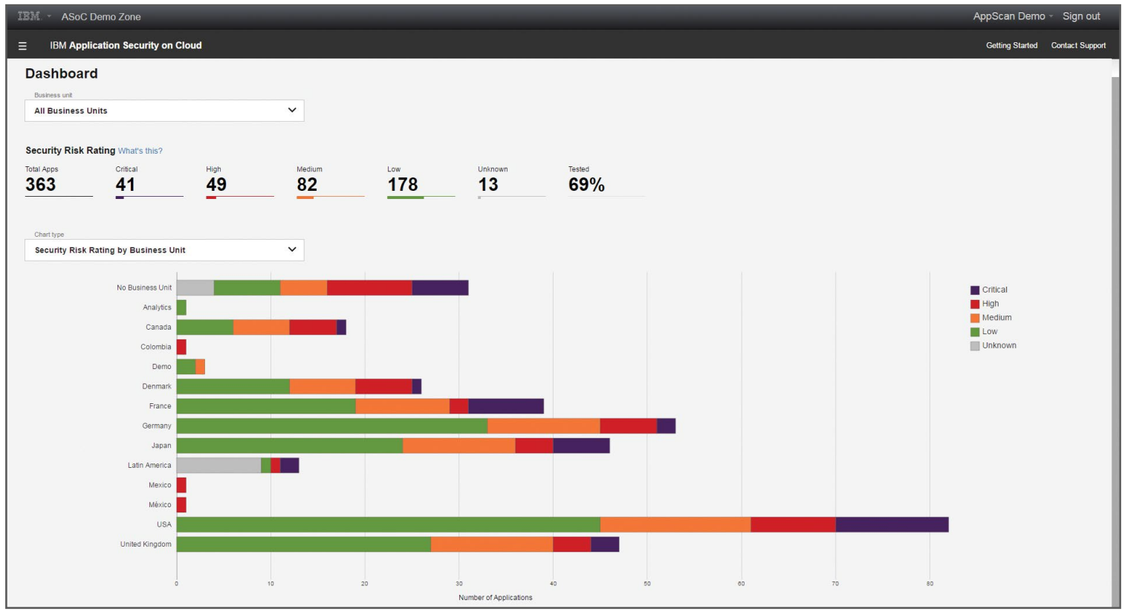
▸ IBM Application Security on Cloud가 취약성을 식별 및 수정하는 방법을 확인하십시오.

1 "2016년 모바일 보안 및 비즈니스 변화 연구," ***정보 보안 미디어 그룹,*** **IBM Corp.,** 지원, **2016**년.

종합적인 클라우드 기반 애플리케이션 보안 평가

잡다한 도구에 의존하지 말고 통합 솔루션을 구현하여 애플리케이션 보안 위험 관리를 강화하십시오. IBM Application Security on Cloud는 웹 및 모바일 애플리케이션을 위한 애플리케이션 보안 평가의 모든 단계를 통합하며, 포괄적이며 비용 효율적이고, 사용하기 쉬우며 배포하기 쉬운 클라우드 기반 솔루션입니다. IBM 클라우드 기반 제품은 오랜 기간 온-프레미스 보안 평가에 대한 IBM의 경험을 바탕으로 하며, 다른 보안 도구와 연동되어 종합적인 사이버 방어 보호를 쉽게 해 줍니다.

IBM Application Security on Cloud는 완벽한 구독 기반 솔루션으로, 실행 가능한 데이터를 제공하므로 애플리케이션을 평가하고 보안 보호를 개선할 수 있습니다. IBM Application Security on Cloud는 애플리케이션 위험 등급을 신속하게 평가할 수 있으므로 가장 심각한 취약성 수정 작업에만 집중할 수 있습니다.



IBM Application Security on Cloud 대시보드 보기.

다양한 프로그래밍 언어로 작성된 애플리케이션 코드에 대해 정적 보안 평가를 수행하고, 사전 제작된 그리고 생산 중인 소프트웨어 웹 애플리케이션에 대해 동적 분석을 수행할 수 있습니다. Android 및 iOS 애플리케이션을 배포하기 전에 테스트하십시오. IBM Application Security on Cloud는 보안 문제를 식별 및 보고하며, 노출 및 중요도에 따라 순위를 결정하고, 수정 단계를 권장합니다. 이 모든 결과를 다양한 DevOps 시스템과 통합 개발 환경(IDE)에 통합할 수 있습니다.

- IBM Application Security on Cloud 평가판 사용을 위해 등록하십시오. 또는 온-프레미스 IBM Security AppScan®시험판을 다운로드하십시오.

다양한 범위의 동반 제품 컨설팅 서비스도 제공되므로, 귀사의 보안 팀은 IBM Security가 제공하는 기능을 최대한 활용할 수 있습니다.

실제 상황에서 IBM Application Security on Cloud 사용 사례

IBM의 애플리케이션 보안 솔루션을 배포하는 조직은 (애플리케이션을 작성하거나 이를 배포하거나 무관하게) 전체 보안 전략의 일환으로 통합 및 자동화의 가치를 인식합니다.

소프트웨어 개발 수명 주기 전체 단계에서 코드 보호

• Washington, Bellevue 소재 Concur Technologies는 기업 비용 관리 전문 기업이므로 기밀 정보를 일상적으로 관리합니다. 이들 정보를 보호하는 것이 중요하지만, 이를 달성하는 것도 어렵습니다. 자사의 모바일 애플리케이션까지 포함한 대규모 모바일 환경을 지닌 조직인 Concur는 IBM Application Security in Cloud와 동일한 취약점 테스트 기술을 사용하여 AppScan을 배포했습니다. Concur는 개발 시점에서 AppScan을 사용하여 애플리케이션 보안 위험을 테스트했으며, 생산 코드를 편리하게 분석할 수 있었습니다.

빠르게 성장하는 기업의 위험 관리

• 국내 및 국외에서 놀라운 성장을 기록하고 있는 터키의 소매업 강자인 Migros는 1,500개에 가까운 매장과 100,000개 이상의 인터넷 연결형 엔드포인트 장치를 포함한 네트워크에서 인벤토리 및 지불 정보를 전송하는 애플리케이션을 사용하여 대규모 인프라를 보호합니다. 성장을 거듭하는 이 기업은 클라우드로 향한 변화 도중에 BYOD 정책을 구현하면서 어려움에 직면했습니다. Migros는 IBM 애플리케이션 보안 솔루션을 활용하여 위험을 최소화하면서 비즈니스를 확장할 수 있었습니다.

IBM은 응용 프로그램, 장치
및 데이터를 보호하기 위해
제조[1] 및 금융 서비스[2]와 같은[1] 회사에서 사용하는 완벽한[2] 도구의 포트폴리오를 제공합니다

▸ IBM Application Security on Cloud의 무료 체험 평가판을 신청하십시오.

1 "대규모 글로벌 자동차 제조업체: 커넥티드 차량 생태계를 보호합니다," ***IBM Corp.***, 2016년 7월.

2 "프로그레시브 보험사(Progressive Insurance): 알맞는 통제를 만들어서 데이터를 적극적으로 보호합니다," ***IBM Corp.***, 2016년 5월.

상세 정보

IBM Security 솔루션에 대한 자세한 사항은 해당 지역의 IBM 담당자나 IBM 비즈니스 파트너 사에 문의하거나 또는 다음 웹사이트를 참조하십시오.
ibm.com/applicationsecurity

IBM Security 솔루션 소개
IBM Security는 첨단 통합 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 세계적으로 IBM X-Force® 연구 및 개발의 지원을 받는 포트폴리오는 보안 정보를 제공해 조직이 총체적으로 사람, 인프라, 데이터 및 애플리케이션, ID 및 액세스 관리용 제안 솔루션, 데이터베이스 보안, 애플리케이션 개발, 리스크 관리, 엔드포인트 관리, 네트워크 보안 등을 보호하도록 지원합니다. 이러한 솔루션은 조직이 효과적으로 리스크를 관리하고 모바일, 클라우드, 소셜 미디어 및 기타 엔터프라이즈 비즈니스 아키텍처에 대한 통합 보안을 구현하도록 지원합니다. IBM은 세계에서 가장 광범위한 보안 연구, 개발 및 제공 조직을 운영하며, 130개가 넘는 국가에서 150억 개의 보안 이벤트를 모니터링하고, 3,000개가 넘는 보안 특허를 보유하고 있습니다.

또한, 애플리케이션 보안 프로그램을 구축하고 실행할 때 IBM Security Services를 사용하면 귀사 조직의 날로 발전하는 요구에 부응할 수 있습니다. 이를 통해 언제 어디서나 애플리케이션 보안 전문 지식에 액세스할 수 있습니다. 귀하의 팀의 신속하게 개입해야 하거나, 심층적인 컨설팅 서비스, 윤리적 해커가 수동으로 애플리케이션을 조사해야 하는 경우 등에서 IBM이 도움을 드립니다.

IBM Security
Route 100
Somers, NY 10589

미국에서 제작
2017년 10월

WGW03254-KRKO-01