하이브리드 클라우드 환경의 보안 유지

분산된 미션 크리티컬 데이터를 보호하고 전문가의 지원을 활용하세요.

자세히 알아보려면
위의 이미지를 클릭하세요

주요 특징

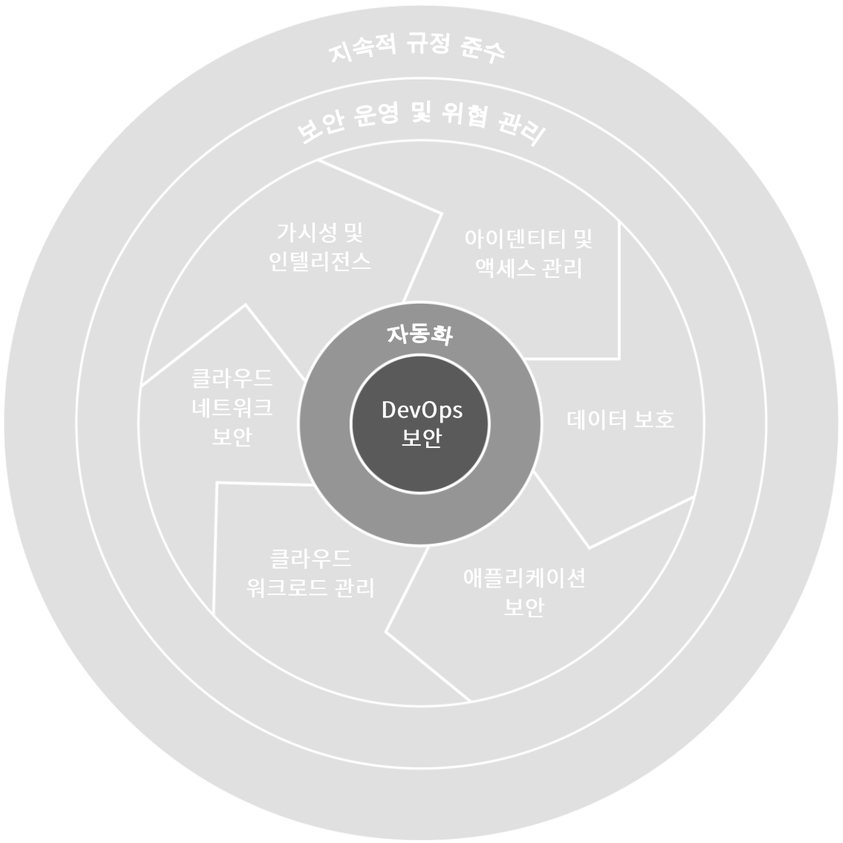
- **DevOps 보안:** 사후 고려 사항이 아니라 개발 단계부터 보안을 염두에 둔 애플리케이션 및 프로젝트를 가능하게 하기 위해 보안 정책 및 참조 아키텍처를 지원합니다.
- **자동화:** 하이브리드 클라우드를 위한 보안 정책 및 기술의 자동화된 프로비저닝을 통합합니다.
- **데이터 보호:** 다수의 클라우드를 포함하여 온프레미스 경계의 안팎에서 데이터를 보호합니다.
- **애플리케이션 보안:** 테스트부터 개발까지 애플리케이션 보안을 유지합니다.
- **아이덴티티 및 액세스 관리(IAM):** IAM 정책을 온프레미스에서 클라우드로 확장합니다.
- **가시성 및 인텔리전스:** 더욱 진보된 위협을 탐지하고 차단하기 위한 가시성과 인텔리전스를 확보합니다.
- **클라우드 워크로드 관리:** 워크로드 보안을 통해 엔드포인트, 정책 등의 위험으로부터 보호합니다.
- **클라우드 네트워크 보안:** 클라우드에 대한 네트워크 보안 강화를 통해 무력화 공격으로부터 기업을 보호합니다.
- **보안 운영 및 위협 관리:** 엔드포인트와 앱의 로그 이벤트 및 네트워크 데이터에 대한 가시성을 확보하여 위협을 탐지하고 방어합니다.
- **지속적 규정 준수:** 조직의 통제 프레임워크를 평가하고 새로운 규정을 파악하고 통제 조치를 지속적으로 향상하여 규정을 준수합니다.

비즈니스상의 요구에 따라 새로운 애플리케이션과 서비스의 배포 속도를 높여야 할 때 기업의 규모가 크든 작든 클라우드로 전환하는 사례가 점점 늘고 있습니다. 그 결과 IT 팀은 이제 Amazon Web Services(AWS), Microsoft Azure and IBM® Cloud™와 같은 멀티 클라우드 및 하이브리드 클라우드 환경에서 리소스를 감독하고 관리해야 합니다.

클라우드 환경도 기본적인 보안 기능을 제공할 수는 있지만, 이러한 환경에서 보안을 유지하고 규정을 준수하는 일은 여전히 기업의 IT 부서가 책임져야 합니다. 클라우드 서비스 제공업체(Cloud Service Providers, CSP)는 광범위하고 다양한 기본 보안 기능을 제공하지만 이처럼 기본적인 보안은 기업의 요구사항을 충족하기에 충분하지 않을 수 있으며 이로 인한 취약성이 악용될 수 있습니다. 또한, 하이브리드 IT 환경의 보안을 효과적으로 유지하는 일은 복잡하고 찾기 어렵거나 채택하려면 비용이 많이 들 수 있는 전문 기술을 요구합니다.

IBM Security는 기업의 자체 보안을 CSP가 제공하는 보안 기능으로 보완하여 데이터를 보호하고, 처음부터 DevOps 팀과 보안을 결합한 보안 프레임워크 및 툴을 마련하여 생산성을 향상하고, 가시성과 보고 기능을 통해 기업이 규정을 준수하도록 지원하는 제품 및 서비스로 구성된 포트폴리오를 제공합니다.

클라우드로 전환 시 보안을 최우선으로 고려



자세히 알아보려면
위의 이미지를 클릭하세요

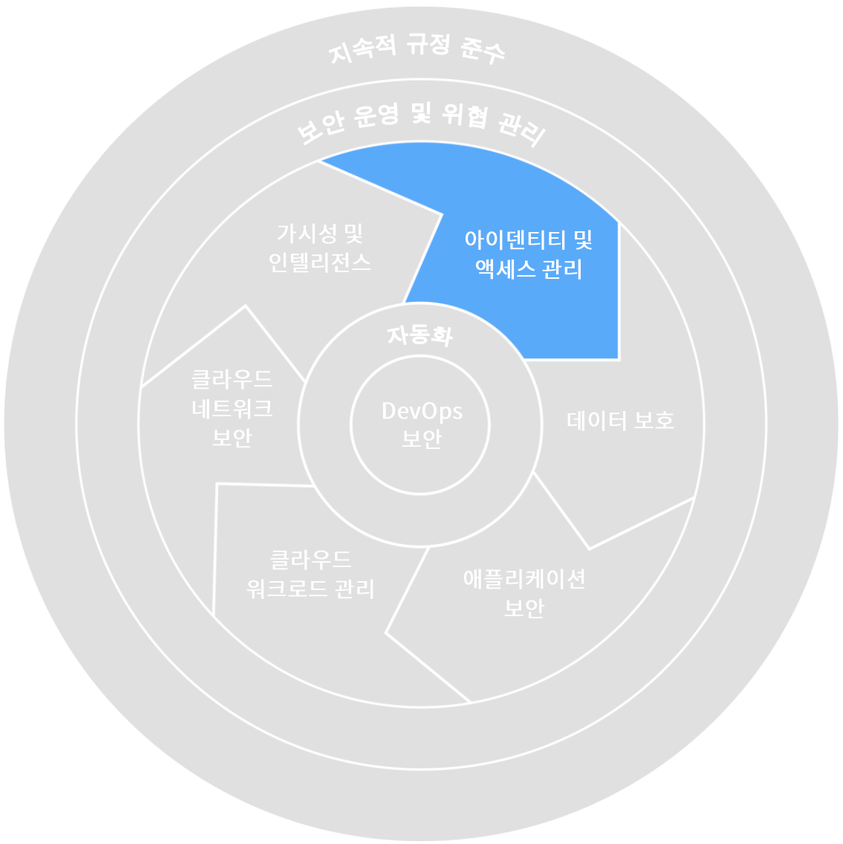
하이브리드 클라우드 아키텍처는 클라우드 채택이라는 측면에서 두 가지 클라우드의 장점을 결합할 수 있습니다. 온프레미스 리소스도 여전히 필요하겠지만, 하이브리드 클라우드 방식을 통해 기업은 퍼블릭 및 프라이빗 클라우드 아키텍처를 모두 활용함으로써 유연성을 제공하고[1] 비즈니스 요구사항을 충족시킬 수 있습니다.

클라우드 마이그레이션 또는 네이티브 클라우드 앱의 구축을 진행할 때 중요한 것은 설계 및 개발 단계에서 보안 조치를 통합하여 보안을 최우선으로 고려하는 것입니다. 클라우드 이니셔티브에 보안 영역을 포함하고 DevOps 팀과 긴밀히 협력한다면 기업은 잠재적 취약성과 데이터 침해가 발생할 경우 이에 대응하기 위해 사용하게 될 귀중한 시간과 리소스를 절약할 수 있습니다. 또한, 하이브리드 클라우드의 보안 유지는 CSP와 기업의 보안 팀이 공동으로 책임져야 한다는 것을 기억해야 합니다. 하이브리드 클라우드 환경에서는 기업의 보안 조치와 보안 인력이 클라우드 및 온프레미스 데이터와 워크로드의 보안을 유지하는 데 지속적으로 중요한 역할을 수행해야 합니다.

클라우드 환경에서는 조직과 CSP가 보안을 공동으로 책임져야 합니다.

1 NathanCrawford,“Comparingpublic,privateandhybridclouds,”(퍼블릭, 프라이빗, 하이브리드 클라우드 비교), *RCR Wireless*, 2018년 4월 20일.

강력한 IAM을 활용한 악의적 공격자 차단



자세히 알아보려면
위의 이미지를 클릭하세요

최근의 한 보고서에 따르면 기업 중 26%가 특권을 가진 계정에 대한 내부자의 오용과 관련된 공격을 경험한 것으로 나타났습니다.[1] 위협이 네트워크 내부 또는 외부에서 시작되었는지에 상관없이 강력한 IAM의 중요성은 아무리 강조해도 지나치지 않습니다. 위치에 상관없이 중요 자산을 보호하려면 IT 전문가는 온프레미스 환경에서부터 기존 네트워크 경계 너머로 확장될 수 있는 클라우드 기반 리소스와 엔드포인트까지 연계하여 IAM을 적용할 수 있어야 합니다.

IDaaS(identity-as-a-service) 솔루션인 IBM Cloud Identity를 사용하면 로컬 IAM 정책을 클라우드 기반 애플리케이션으로 확장하고 새로운 클라우드 애플리케이션을 신속하게 구축할 수 있습니다. 또한, 애플리케이션에서 직접 싱글사인온(single sign-on,SSO) 액세스가 가능하므로 사용자는 네트워크에 성공적으로 로그인하면 필요한 애플리케이션에 간편하게 액세스할 수 있습니다.

IBM Security는 IBM Cloud Identity 소프트웨어 솔루션과 더불어 IBM Identity and Access Management Services를 제공합니다. 이 서비스를 사용하면 아이덴티티 및 액세스 관리 보안 전문가가 고객과의 협력을 통해 엔터프라이즈 전반에 걸쳐 사용자 프로비저닝, 엔터프라이즈 싱글사인온, 다단계 인증, 사용자 활동 규정 준수와 같은 보안 및 비즈니스 목표에 맞게 솔루션을 설계해 줍니다.

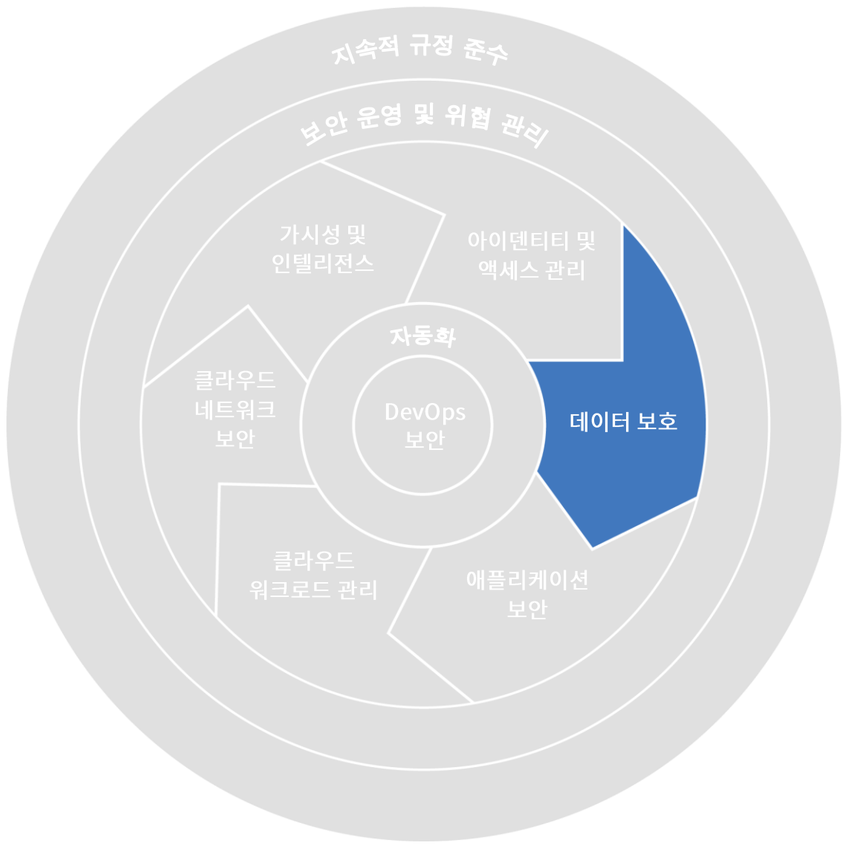
20억 개 이상의 레코드

가 2017년 한 해 동안 클라우드 서버 구성 오류와 네트워크화된 백업 인시던트로 인해 의도치 않게 노출되었습니다.[2]

1 "Zero-Day Exploits Are Most Prevalent Attack in Hybrid Cloud Environments, according to Capsule8-Sponsored Study" (Capsule8 후원 연구에 따르면, 하이브리드 클라우드 환경에서 가장 흔히 발생하는 공격은 제로데이 익스플로잇임), Capsule8, 2018년 2월 28일.

2 "IBM X-Force Threat Intelligence Index 2018," (IBM X-Force 위협 인텔리전스 지수 2018), *IBM Corp.*, 2018년 3월.

하이브리드 클라우드 환경 전반에서 데이터 보호



자세히 알아보려면
위의 이미지를 클릭하세요

어떤 IT 환경에서든 강력한 보안 조치가 없으면 조직은 데이터 노출, 생산성 감소, 규정 위반 위험(compliance risk)을 경험할 수 있습니다. 하이브리드 환경에서 내외부 위협으로부터 데이터를 보호하려면 여러 시스템과 데이터센터에 보안 조치가 일관적으로 적용되어야 합니다.

IBM Security Guardium®은 데이터가 온프레미스에 저장되건, 클라우드에 저장되건, 전체 데이터 보호 프로세스를 지능적으로 파악하도록 지원하고 기밀 데이터 요소에 대한 세분화된 액세스 제어 기능을 제공합니다. 이를 통해 기밀 데이터를 검색 및 분류하고 사용 패턴을 파악하며 규정 위반 위험을 평가할 수 있습니다.

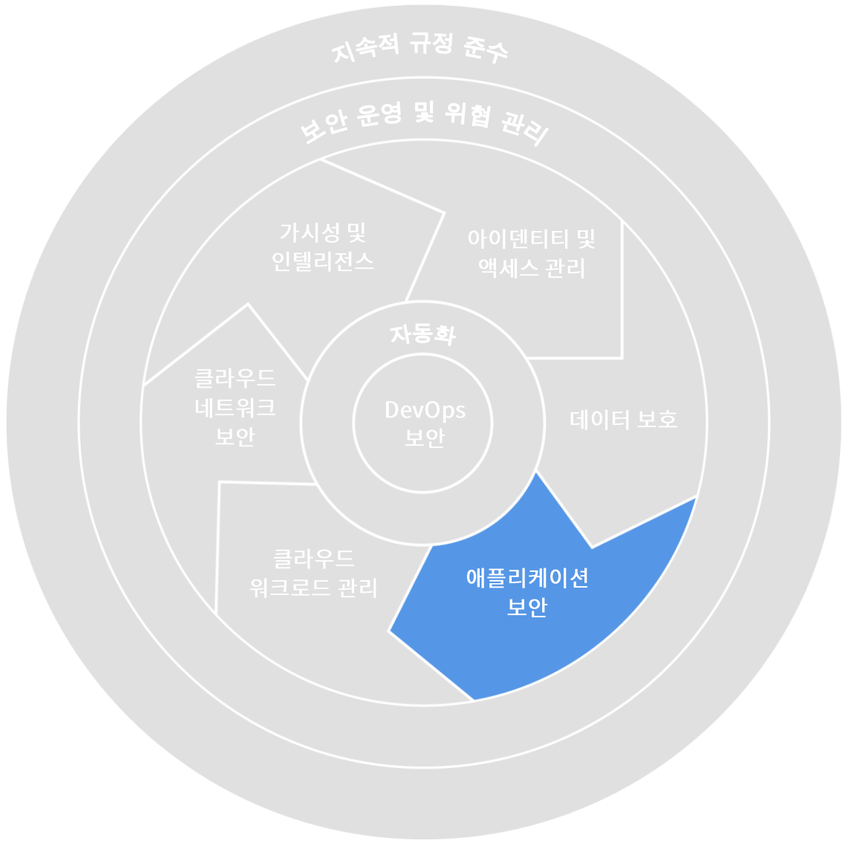
IBM Data Security Services는 위험의 균형을 유지하는 정책과 데이터 보호 기술을 통합하여 조직의 중요 데이터를 보호할 수 있도록 지원합니다. 또한, 데이터 보안 전문가가 컨설팅 서비스와 통합 서비스를 통해 시장 선도적인 데이터 손실 방지 및 암호화 기술을 사용하여 데이터에 대한 통제를 최적화할 수 있도록 지원합니다.

148 달러(USD)

데이터 침해 시 도난당한 레코드 1개당 발생하는 평균 비용.[1]

1 "2018 Cost of a Data Breach Study: Global Overview," (2018 데이터 침해 비용 연구: 전 세계에 대한 개괄적 검토), *Ponemon Institute*, 2018년 7월.

개발부터 배포까지 클라우드 기반 애플리케이션의 보안 유지



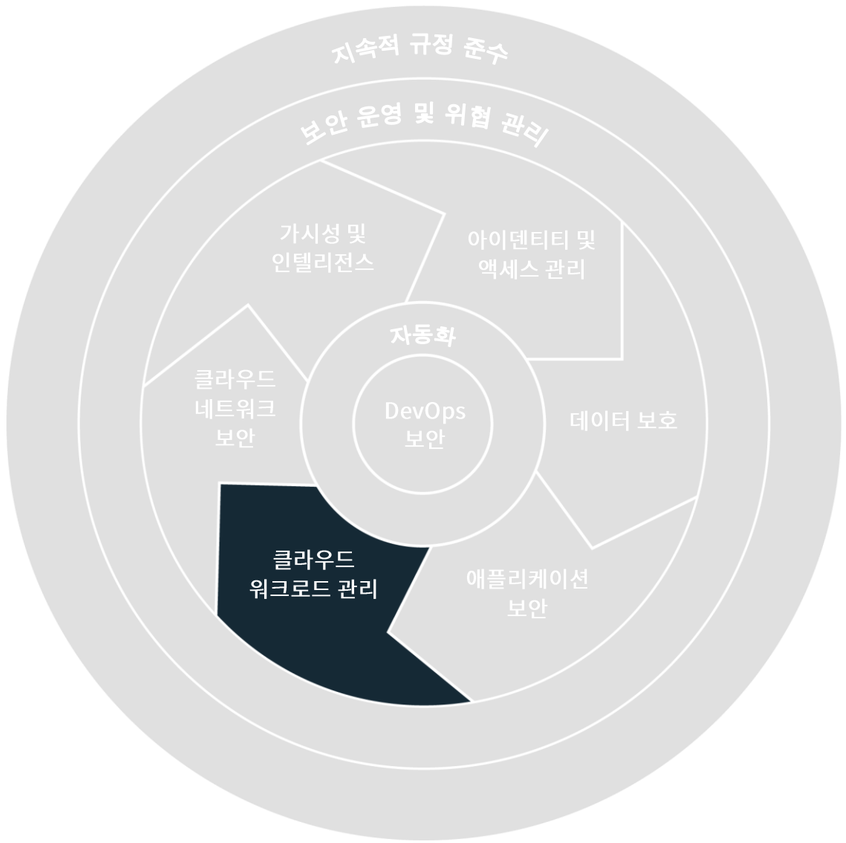
자세히 알아보려면
위의 이미지를 클릭하세요

클라우드에서 애플리케이션을 구축하면 DevOps 팀은 더 빨리 개발 테스트를 완료하고 애플리케이션을 배포할 수 있습니다. 그러나, 기존 네트워크 인프라의 범위 밖에서 보안을 유지하고 중요 자산에 대한 규정을 준수하는 일은 어려울 수 있습니다.

IBM Application Security on Cloud라는 강력한 솔루션을 사용하면 개발자와 IT 관리자는 클라우드에서 정적, 동적, 모바일 애플리케이션에 대한 보안 테스트를 실시할 수 있습니다. 이 솔루션을 통해 실시간으로 취약성을 탐지하고 해결하면서 애플리케이션을 클라우드에서 활용할 수 있도록 준비함으로써 마이그레이션, 배포, 확장을 가속화할 수 있습니다.

IBM X-Force Red Services는 침투 테스트와 취약성 관리 프로그램을 제공하여 보안 책임자가 애플리케이션뿐만 아니라 전체 디지털 및 물리적 에코시스템에 대해 보안 결함을 파악하고 이를 바로잡도록 지원합니다.

하이브리드 클라우드 워크로드 관리의 복잡성 해소



자세히 알아보려면
위의 이미지를 클릭하세요

클라우드로 전환하게 되면 개발부터 배포까지 워크로드 처리에 속도를 더할 수 있습니다. 그러나, 클라우드 기반 워크로드의 경우 관리 및 정비가 어려울 수 있습니다. IBM Security는 클라우드의 워크로드 관리를 지원하여 안정성과 보안이 계속 유지되도록 합니다.

IT 부서는 IBM BigFix®를 사용하여 운영 비용을 절감하고 엔드포인트 관리 주기를 단축하고 실시간으로 규정 준수를 시행할 수 있습니다.

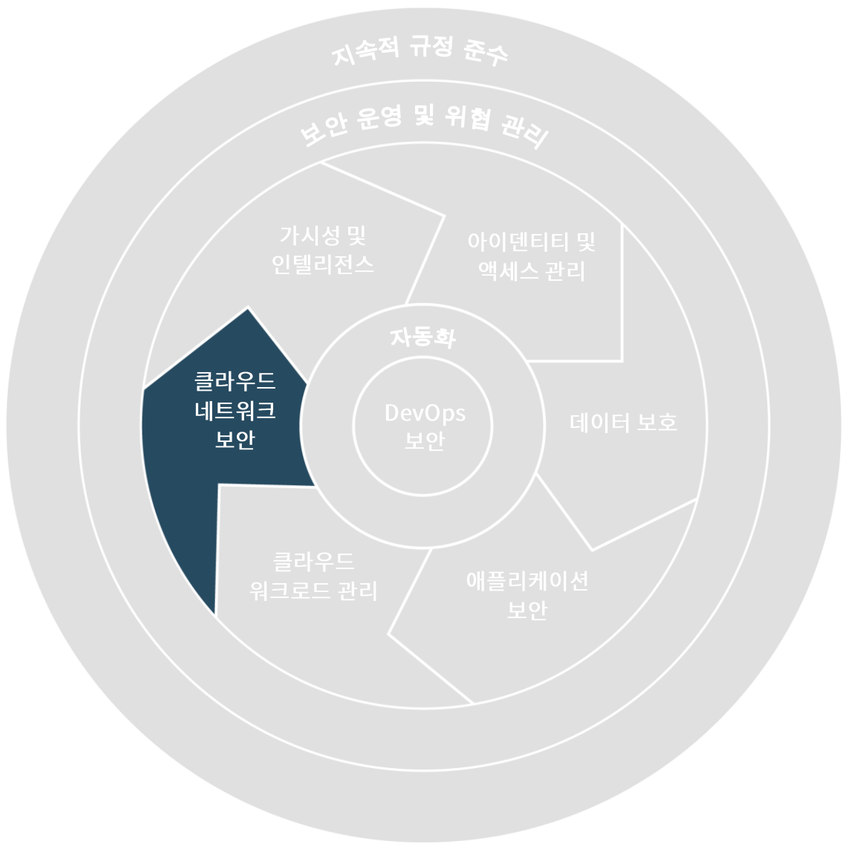
IBM X-Force Cloud Security Services는 온프레미스 클라우드뿐 아니라, AWS, Azure, IBM Cloud 등의 클라우드 환경에서 자문 및 관리형 보안 서비스를 제공하여 고객이 하이브리드 클라우드 보안의 모든 측면을 파악하고 통제할 수 있도록 지원함으로써 중대한 보안 허점이 해소됩니다.

42%

하이브리드 클라우드 환경을 채택한 조직 중 2017년에 보안 공격을 경험한 조직의 비율.[1]

1 "Zero-Day Exploits Are Most Prevalent Attack in Hybrid Cloud Environments, according to Capsule8-Sponsored Study," (Capsule8 후원 연구에 따르면, 하이브리드 클라우드 환경에서 가장 흔히 발생하는 공격은 제로데이 익스플로잇임), *Capsule8*, 2018년 2월 28일.

네트워크 보안 강화



자세히 알아보려면
위의 이미지를 클릭하세요

조직이 데이터 침해 발생 후 이를 알게 되기까지 평균 197일이 걸립니다.[1] IBM QRadar® Security Intelligence Platform은 보안 분석가가 이상을 탐지하고 진보된 위협을 발견하여 실시간으로 오탐(false positive)을 제거하도록 지원함으로써 이와 같은 심각한 시간차를 줄입니다. 이 솔루션은 고도로 분산된 환경에서도 위협에 대한 실행 가능한 인사이트를 제공하기 위해 중앙에서 로그와 네트워크 흐름 데이터를 수집하고 분석합니다.

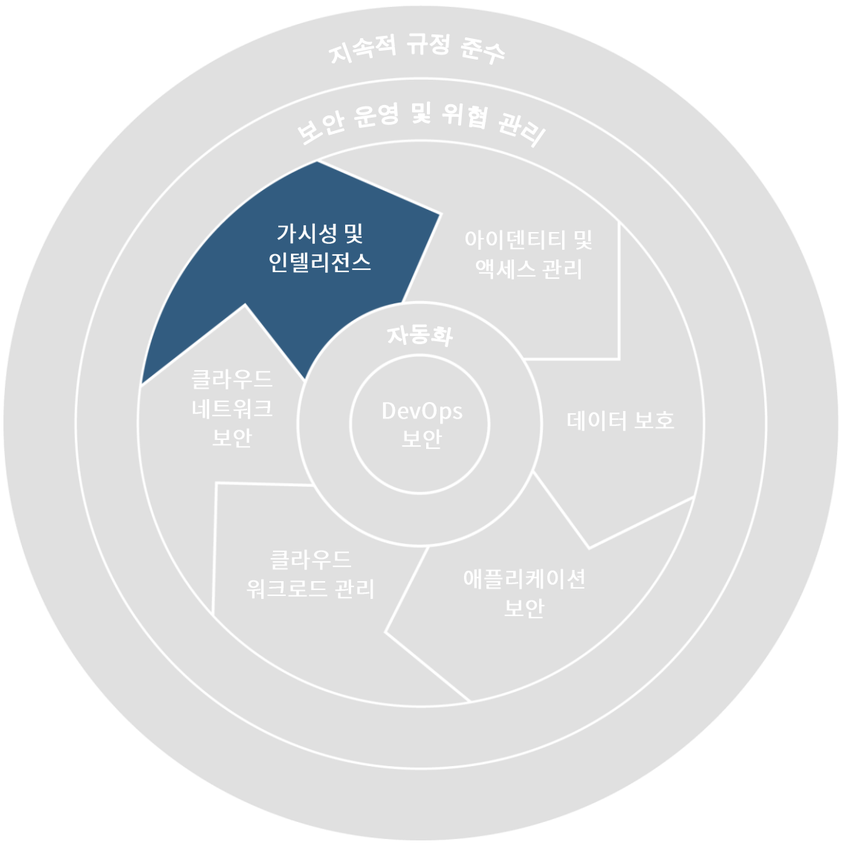
IBM Security Intelligence Operations and Consulting Services는 조직이 모든 네트워크 환경에 걸쳐 인텔리전스 기반 운영의 성숙도를 향상하도록 지원합니다. 보안 인텔리전스 운영 전문가가 보안 베스트 프랙티스를 기준으로 보안 역량과 성숙도를 평가할 수 있습니다. 고객이 보안관제센터를 조성하거나 개선하기를 원할 경우 IBM은 이를 계획, 설계 및 구축할 수 있습니다.

61%

퍼블릭 클라우드 서비스에 개인정보를 저장하는 조직의 비율.[2]

1 "2018 Cost of a Data Breach Study: Global Overview," (2018 데이터 침해 비용 연구: 전 세계에 대한 개괄적 검토), *Ponemon Institute*, 2018년 7월.
2 "Navigating a Cloudy Sky: Practical Guidance and the State of Cloud Security," (클라우드 스카이 탐색: 실무 지침 및 클라우드 보안 현황), *McAfee*, 2018년 4월.

보안 정보 및 이벤트 관리 시 노이즈 필터링



자세히 알아보려면
위의 이미지를 클릭하세요

보안 팀은 잠재적 보안 인시던트에 대한 알림과 이벤트 데이터의 집중 포화에 시달립니다. 오탐을 배제하기 위해 노이즈를 필터링하는 일은 진짜 인시던트를 신속하게 가려내어 태그를 지정하는 방법이 없다면 어려울 수 있습니다.
IBM Security 솔루션은 온프레미스 및 클라우드 환경에서 인공지능을 활용하여 의심스러운 행동을 표시하고, 위협 데이터에 대한 정확한 분석을 수행하며, 사용자 활동에 대한 포괄적인 가시성을 실시간으로 확보합니다.

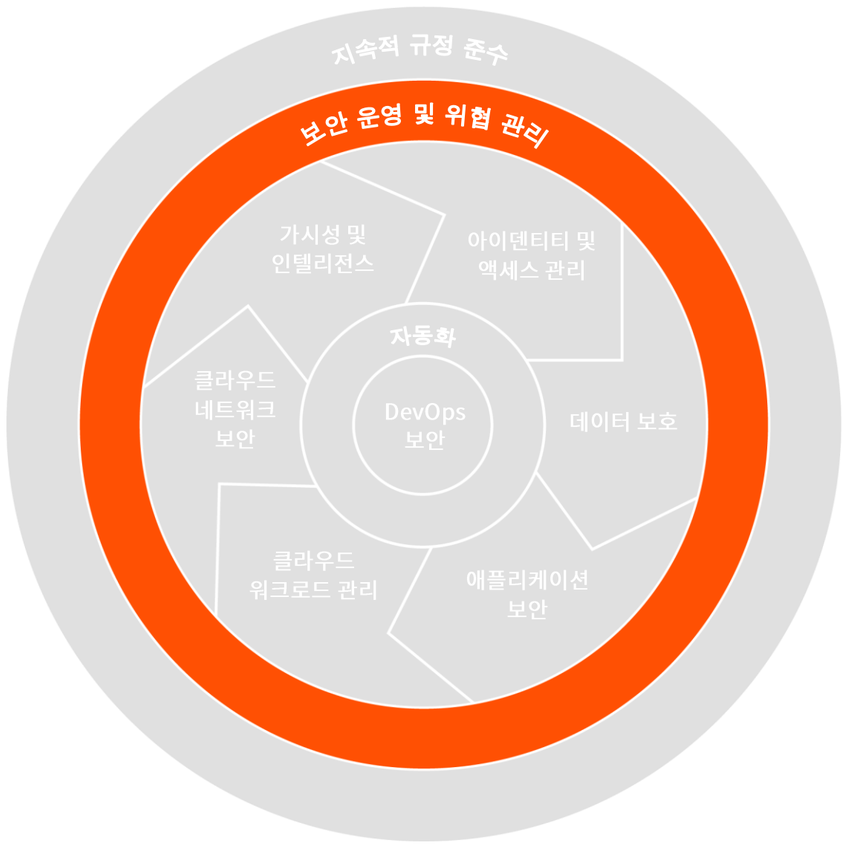
IBM QRadar Security Intelligence Platform은 강력한 보안 인텔리전스 솔루션으로서, 하이브리드 클라우드 IT 환경에서 찾기 어려운 최신 위협을 찾아내고 이상을 탐지하고 오탐을 제거하도록 지원합니다.

X-Force 팀은 IBM X-Force Cloud Security Services를 통해 보안관제센터(Security Operations Center, SOC)의 효과적 활동을 약화시킬 수 있는 오탐을 식별할 수 있습니다. 가장 취약한 부분부터 시작하여 정밀하게 허점과 약점을 테스트하고 전문적인 교정 조치를 제공합니다.

일부 조사에 따르면 랜섬웨어 피해액이 2017년에 두 배로 증가하여 최소 20억 달러(USD)에 이르렀으며 이메일 침해 스캠으로 인한 전 세계적 손실액은 2018년에 90억 달러(USD)를 웃돌 것으로 예측되었습니다.[1]

1 Selena Larson, "The hacks that left us exposed in 2017," (2017 해킹 및 데이터 유출 사고), *CNN Money*, 2017년 12월 20일.

보안 운영 및 위협 관리를 클라우드로 확장



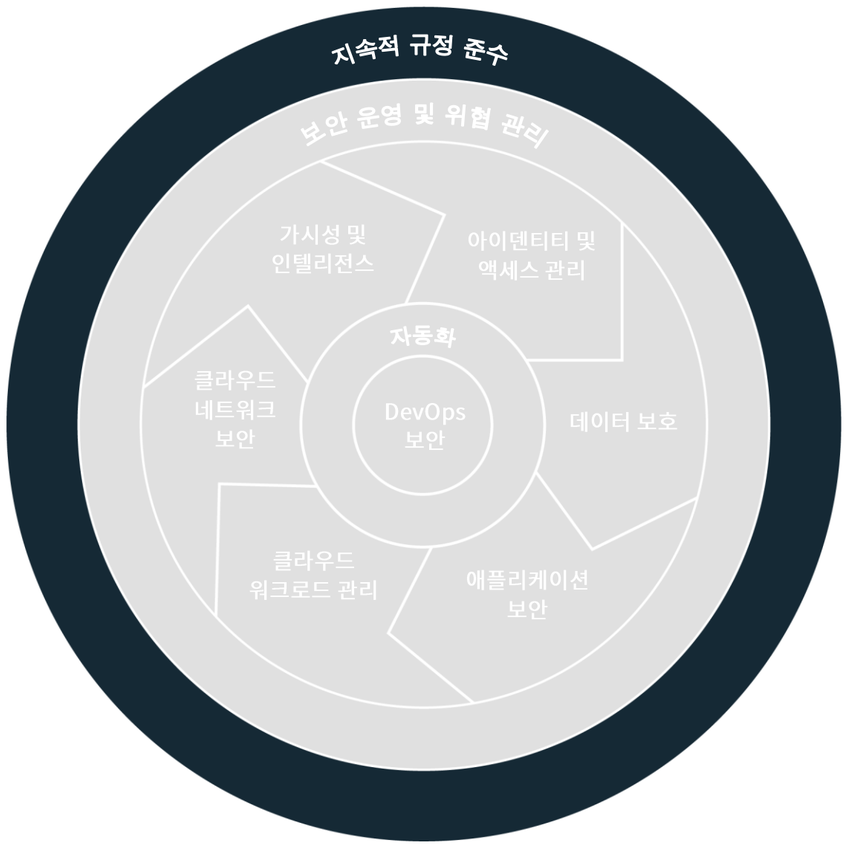
자세히 알아보려면
위의 이미지를 클릭하세요

하이브리드 클라우드 환경의 보안을 유지하는 데 필요한 핵심 기능을 마련한 후에는 보안 운영 및 위협 관리 프로세스로 지원해야 합니다. IBM Security는 보안 조치 및 모니터링 기능을 확장하여 클라우드 환경에서 위협을 방지하고 탐지하며 이에 대응하도록 지원합니다.

IBM QRadar Security Intelligence Platform은 고객이 실행 가능한 인사이트를 얻고 주요 위협을 신속하게 파악하고 전체 알림의 양을 줄일 수 있도록 지원합니다. 또한, QRadar는 폐쇄 루프 피드백을 제공하여 지속적으로 탐지 능력을 향상하고 자동화된 보안 인텔리전스를 통해 절약된 시간을 활용하여 예방적으로 위협을 추적하고 억제 프로세스를 자동화하도록 돕습니다.

IBM X-Force Cloud Security Services는 몇 분 안에 기본 보안 정책을 적용하여 프로비저닝을 자동화하도록 지원합니다. 클라우드와 온프레미스 환경에서 중앙집중식으로 보안을 유지하고 가시성을 확보하며, 단일 제공업체와 포털을 활용하여 보안 관리 및 모니터링을 간소화할 수 있습니다.

하이브리드 클라우드 환경에서 지속적으로 규정 준수 보장



자세히 알아보려면
위의 이미지를 클릭하세요

여러 규제 의무와 업계 요구사항을 준수하고 준수 상태를 유지하는 일은 대부분의 조직에게 어려운 과제이며 DevOps 팀에게 특히 그러합니다. 하이브리드 클라우드 환경에서는 비즈니스가 여러 클라우드로 확장되므로 규정 준수 활동이 더욱 복잡해지며 규정을 추적 및 준수하고 준수 상태를 유지하기가 더 어려워집니다.

IBM Security Guardium Analyzer는 규제 대상 데이터를 효율적으로 찾고, 데이터 및 데이터베이스 노출을 파악하며, 문제 해결 및 위험 최소화를 위한 조치를 취하도록 지원합니다. 또한, 개인정보보호 규정과 의무가 적용되는 개인정보 및 민감한 개인정보와 관련된 위험을 파악합니다. 이 솔루션은 규정 준수 활동을 간소화하여 규정 준수 관리자, 데이터 관리자, IT 관리자가 적절한 수준의 세부 사항을 포함한 필요 정보를 얻어 효율적으로 협력할 수 있도록 지원합니다.

IBM X-Force Cloud Security Services는 여러 클라우드 및 온프레미스 환경에 대한 가시성을 확보하고 정책을 실행할 수 있도록 하여 지속적인 규정 준수를 지원합니다. IBM 클라우드 보안 전문가가 지속적인 규정 준수를 위해 고객의 비즈니스에 필요한 전략을 제공합니다.

왜 IBM인가?

하이브리드 클라우드 보안을 관리하는 일은 복잡할 수 있지만 이 과제를 고객 혼자 해결하지 않아도 됩니다. 세계적 클라우드 제공업체인 IBM이 크로스 클라우드 환경의 보안을 위한 혁신적 제품, 전문화된 보안 서비스, 그리고 관리형 오퍼링을 제공합니다. 또한, IBM은 업계를 선도하는 하이브리드 클라우드 보안 기술을 제공합니다. 더불어, IBM Watson™의 인공 지능을 활용하면 확장성이 뛰어나고 상세한 위협 분석을 제공하여 보안 분석가의 능력을 보강할 수 있습니다.

자세한 정보

하이브리드 클라우드 보안을 위한 IBM의 제품과 서비스에 대해 자세히 알아보려면 IBM 영업대표 또는 IBM 비즈니스파트너에게 문의하거나 ibm.com/security 웹사이트에서 확인하세요.

IBM Security 솔루션 소개

IBM Security는 엔터프라이즈 보안 제품 및 서비스로 구성된 가장 발전된 통합 포트폴리오를 제공합니다. 세계적 명성의 X-Force 연구개발 팀이 지원하는 이 포트폴리오는 보안 인텔리전스를 통해 조직이 직원, 인프라, 데이터 및 애플리케이션을 전방위적으로 보호할 수 있도록 지원합니다. 이를 위해 아이덴티티 및 액세스 관리, 데이터베이스 보안, 애플리케이션 개발, 위험 관리, 엔드포인트 관리, 네트워크 보안 등을 위한 솔루션을 제공합니다. 이러한 솔루션을 통해 조직은 효과적으로 위험을 관리하고 모바일, 클라우드, 소셜 미디어 및 기타 엔터프라이즈 비즈니스 아키텍처를 위한 통합적 보안을 구현할 수 있습니다. IBM은 세계에서 가장 광범위한 수준의 보안 연구, 개발, 제공 조직을 운영하며 130개국 이상에서 월간 1조 건에 달하는 보안 이벤트를 모니터링하고 3,000개 이상의 보안 특허를 보유하고 있습니다.

IBM Security

New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2018년 12월

54022054-KRKO-02