온라인으로 함께 하는
제6회 IBM Security Summit

Bank of America 사례로 보는 클라우드 보안 베스트 프랙티스

한국IBM
조가원 실장
Consulting IT Specialist

클라우드의 가속화
Cloud with new normal

IBM Security

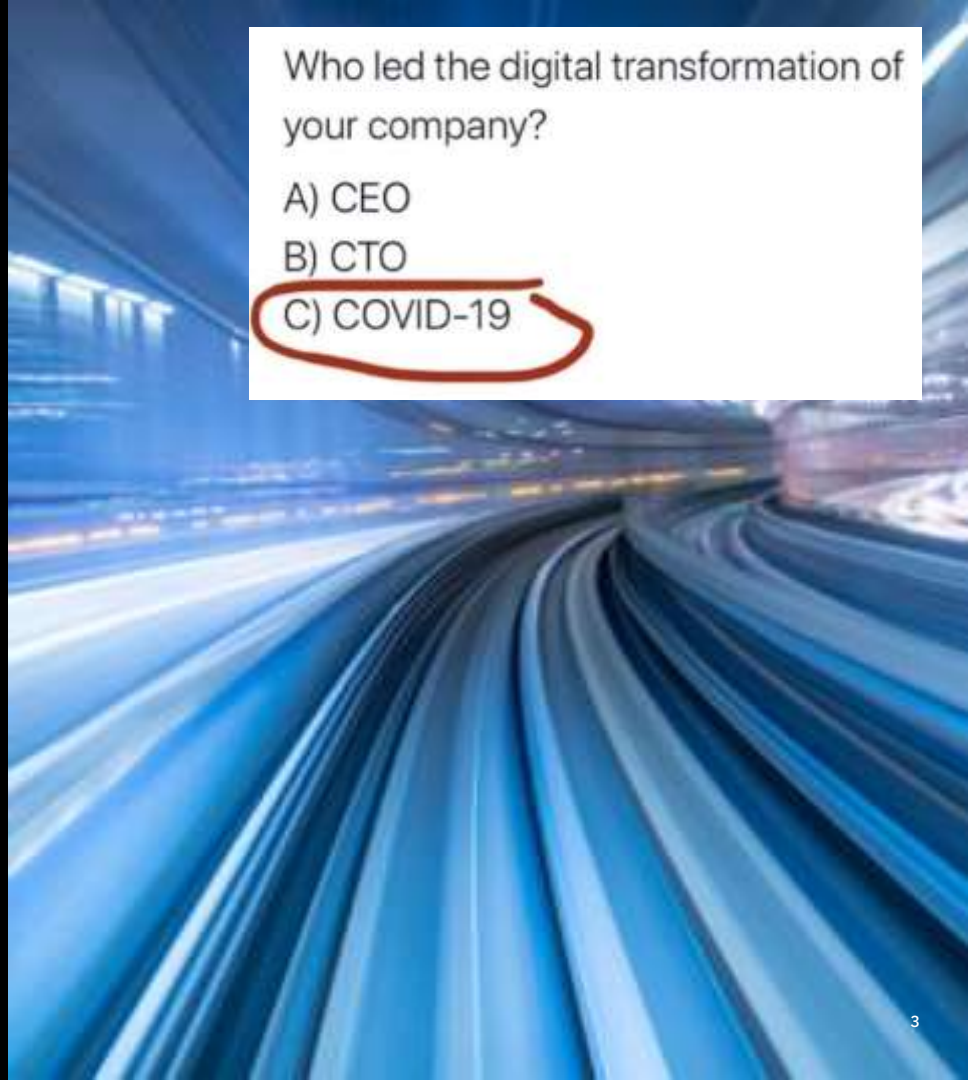
IBM

기업 클라우드 전략

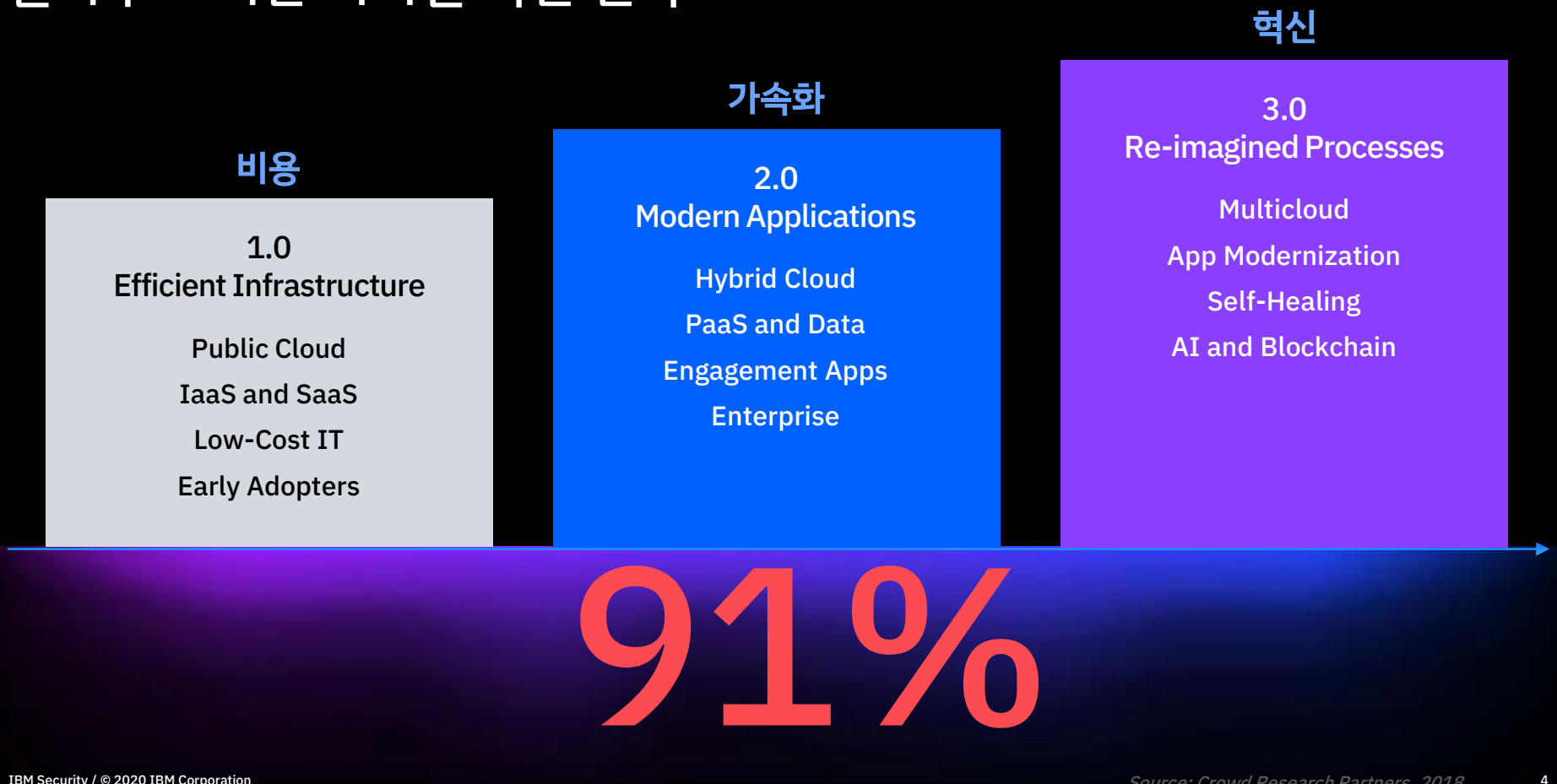
94%

20%

Source: Cloud adoption to accelerate IT modernization article, McKinsey & Company, April 2018



클라우드 기반 디지털 혁신 전략



Source: Crowd Research Partners, 2018

클라우드의 도래, 새로운 보안 전략

Risk based approach to protect Data & Workloads

Continuous Security with Actionable Insights

Continuous Compliance with Demonstrable Controls

클라우드 핵심 보안

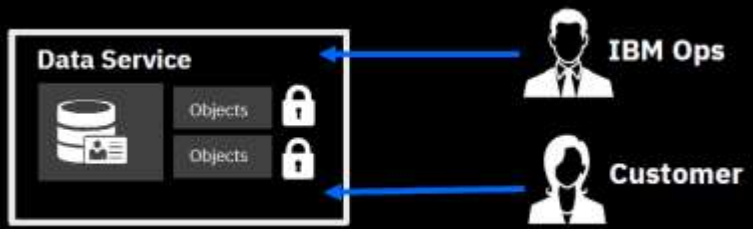
1. **End to end data protection, with exclusive control**
2. Workload centric security, integrated with DevSecOps
3. Continuous compliance, with demonstrable controls
4. Continuous security, with actionable insights

클라우드 서비스 제공자의 데이터 기밀성 보장

Operational Assurance

"We *will not* access your data"

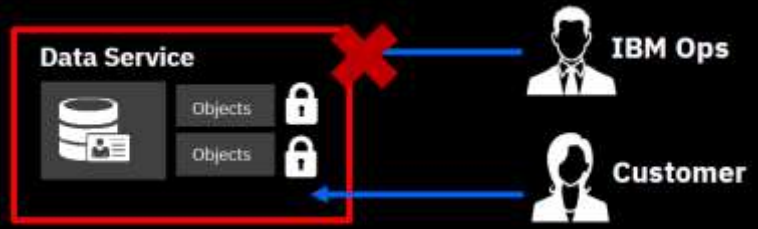
- 신뢰성
- 가시성
- 통제성



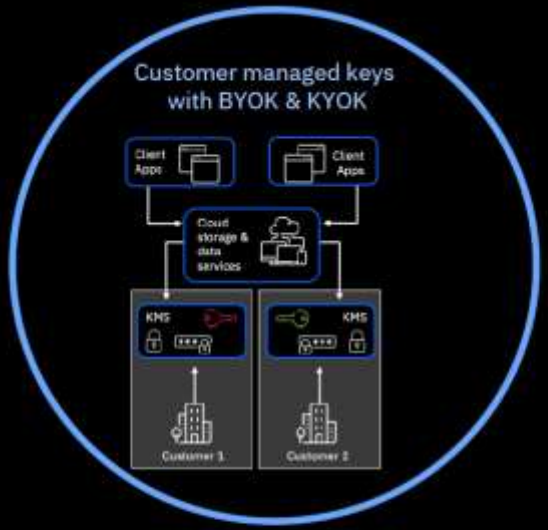
Technical Assurance

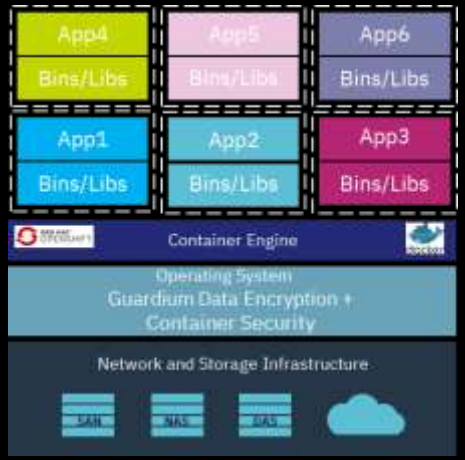
"We *can not* access your data"

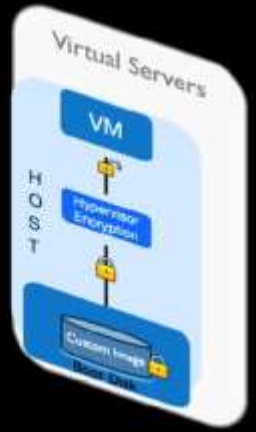
- 기술적 증빙
- 암호화 키의 외부 통제
- 런타임 격리



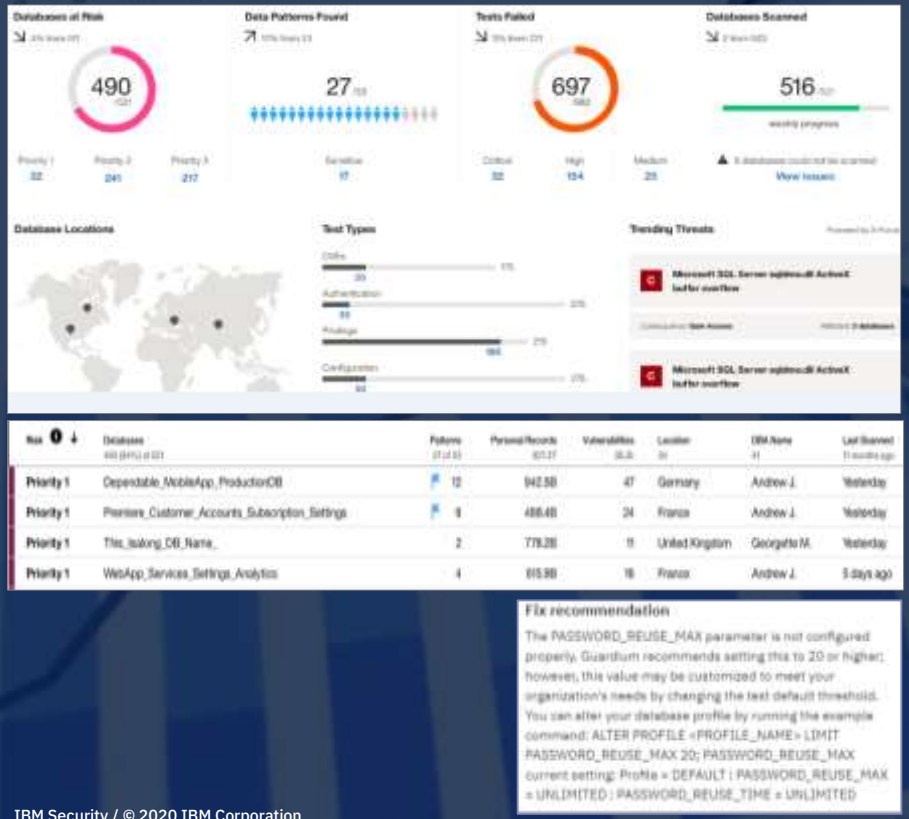
하이브리드 멀티 클라우드 환경에서의 암호화 및 통합 키 관리

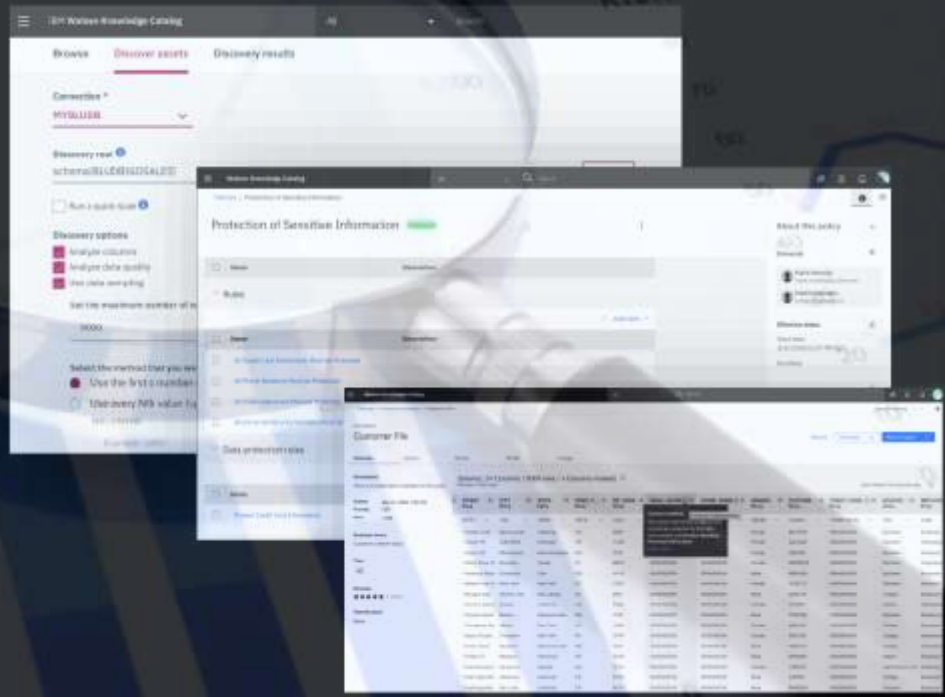






민감 정보를 비롯한 핵심 자산 식별 및 보호



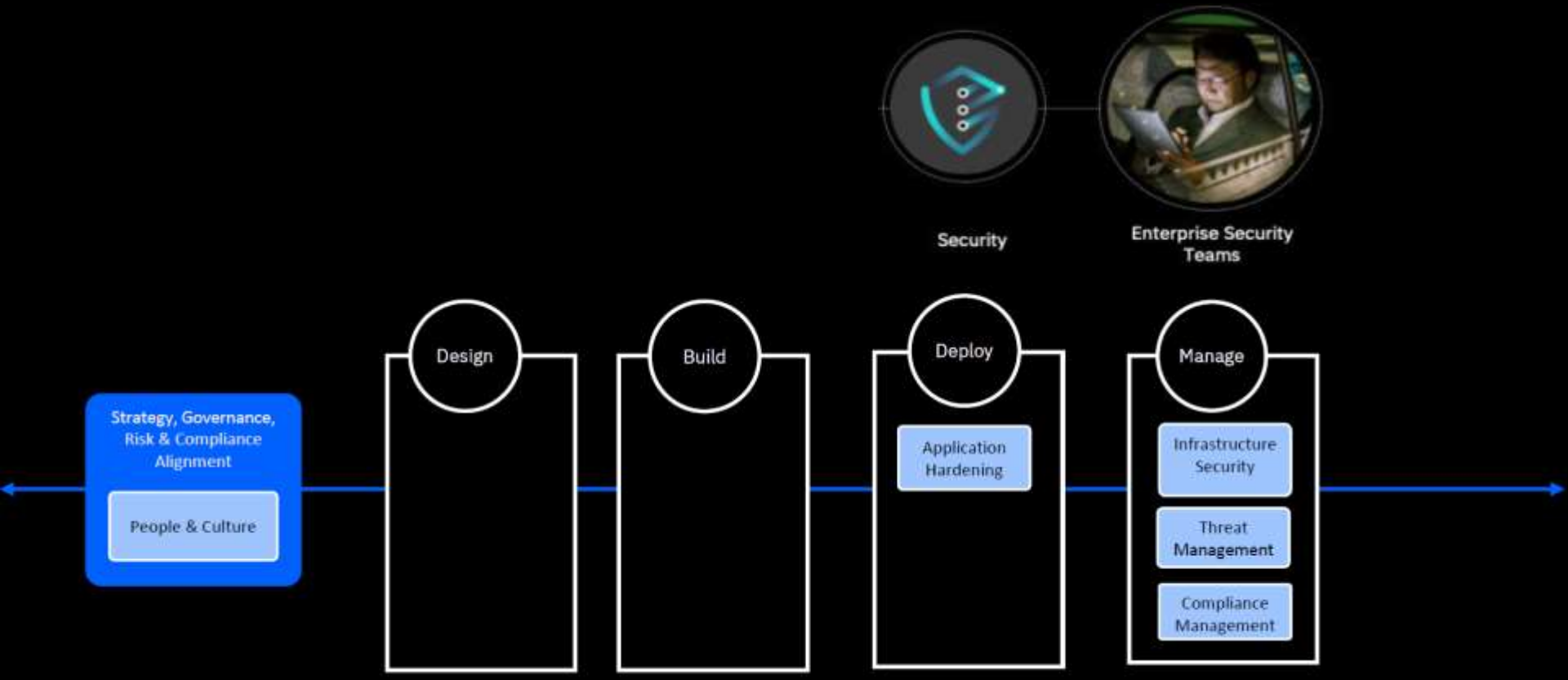


실시간 모니터링 기반 데이터 중심 가시성 확보

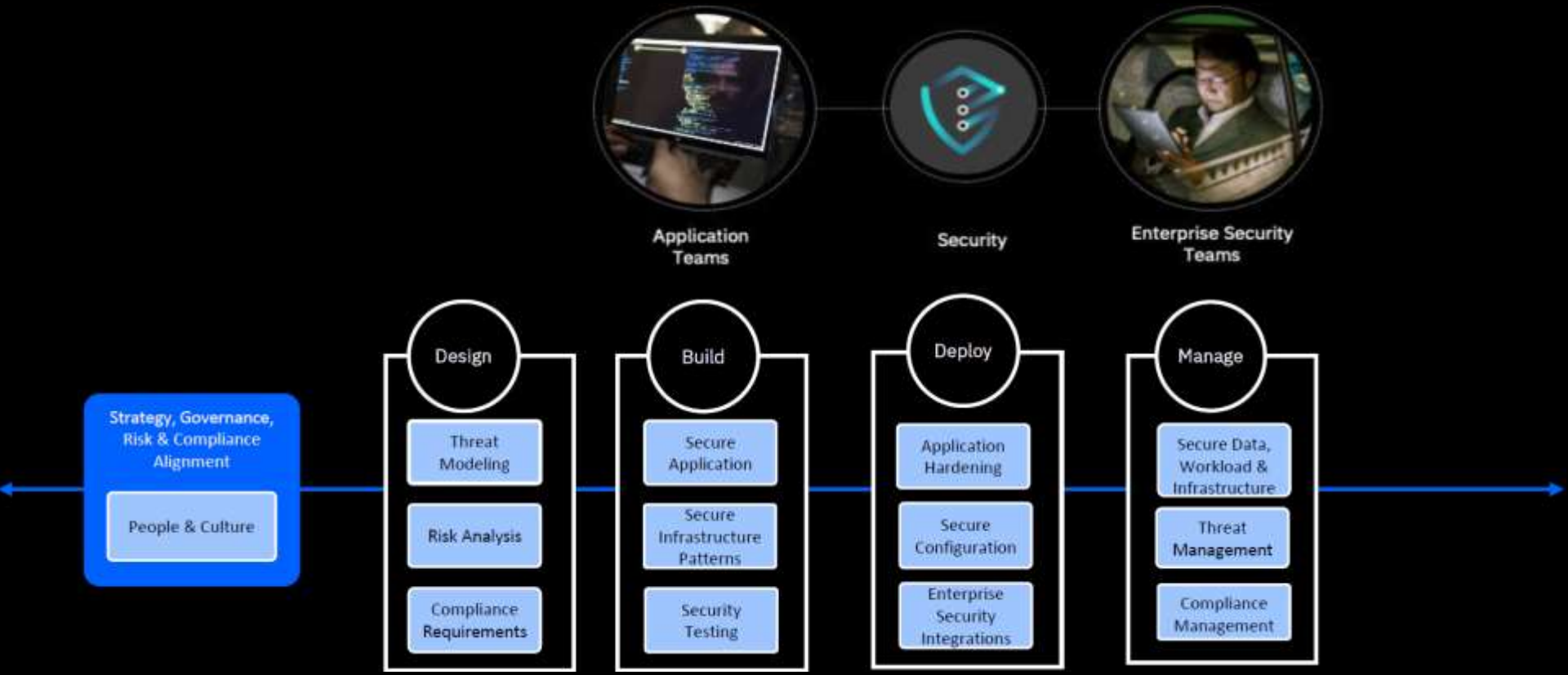
클라우드 핵심 보안

1. **End to end data protection, with exclusive control**
2. Workload centric security, integrated with DevSecOps
3. Continuous compliance, with demonstrable controls
4. Continuous security, with actionable insights

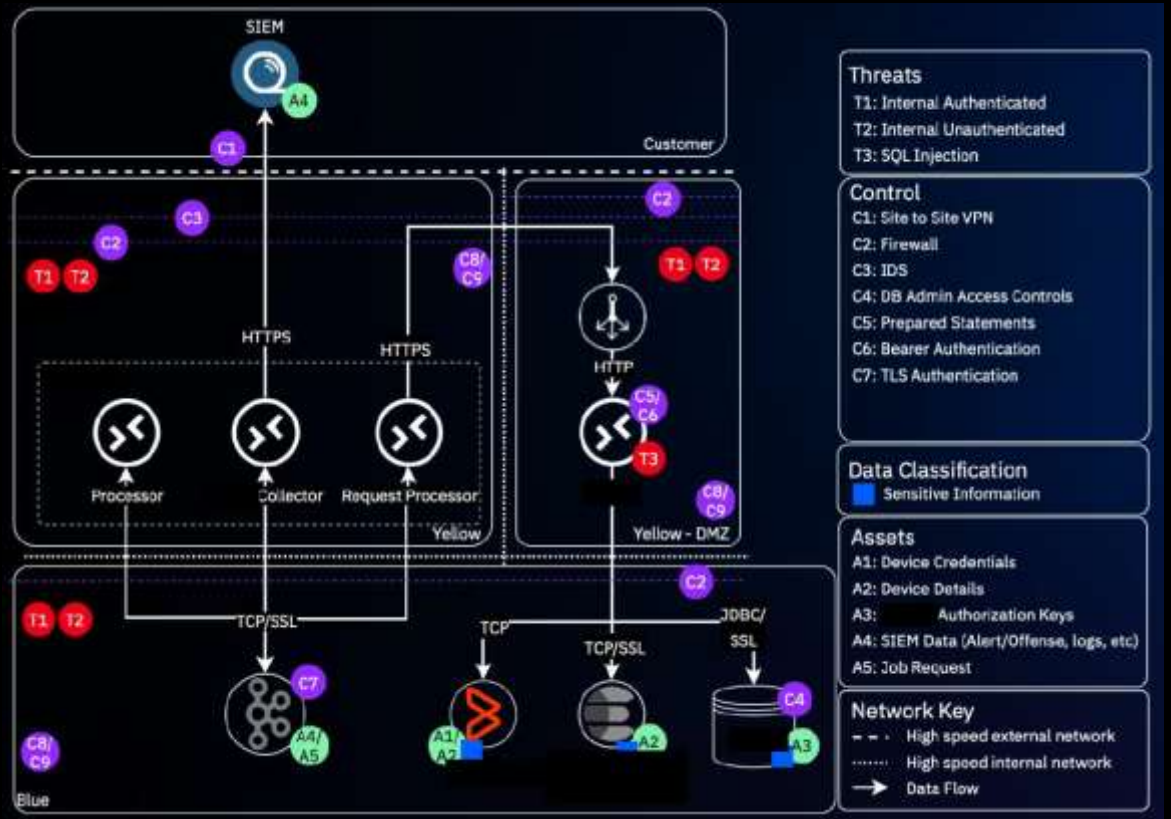
보안팀 책임이 강조되는 기존 보안 운영 모델



애플리케이션 개발자와 보안팀의 협업 모델 DevSecOps



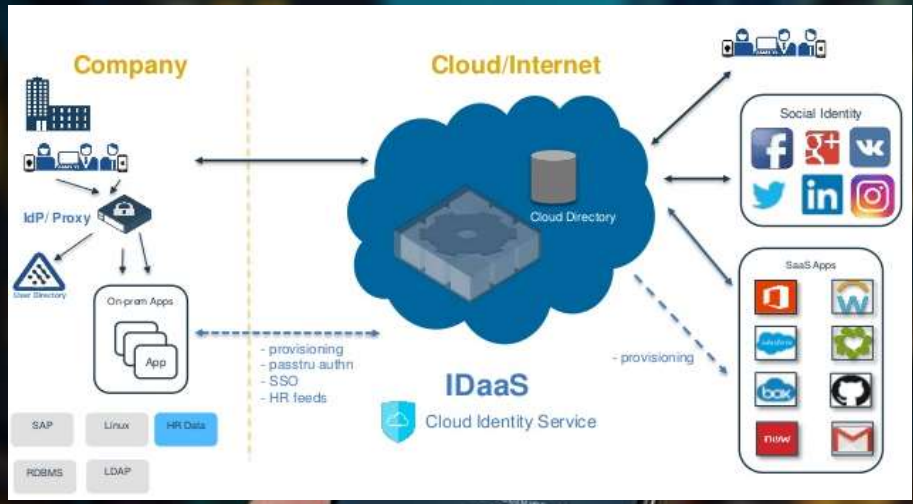
아키텍처에서의 잠재적 위협을 식별하는 위협 모델링



- 아키텍처 내 취약 요소
- 연관 위협
- 위협 방지 방안

워크로드/앱 접근 권한 관리

- 사용자/서비스 인증
- 서비스 ID/API 키
- 역할 기반 접근 통제(RBAC)
- 멀티 클라우드 연동
- 사용자 관리 및 프로파일
- 계정 도용 방지



클라우드 핵심 보안

1. **End to end data protection, with exclusive control**
2. Workload centric security, integrated with DevSecOps
3. Continuous compliance, with demonstrable controls
4. Continuous security, with actionable insights

엔드 투 엔드 컴플라이언스 지원을 위한 핵심 요소

대응 카탈로그 작성을 위한

중앙화된 규제 해석

표준화되고 재활용 가능한

보안 통제의 구현

감사 증적 수집/평가를 위한

자동화된 툴

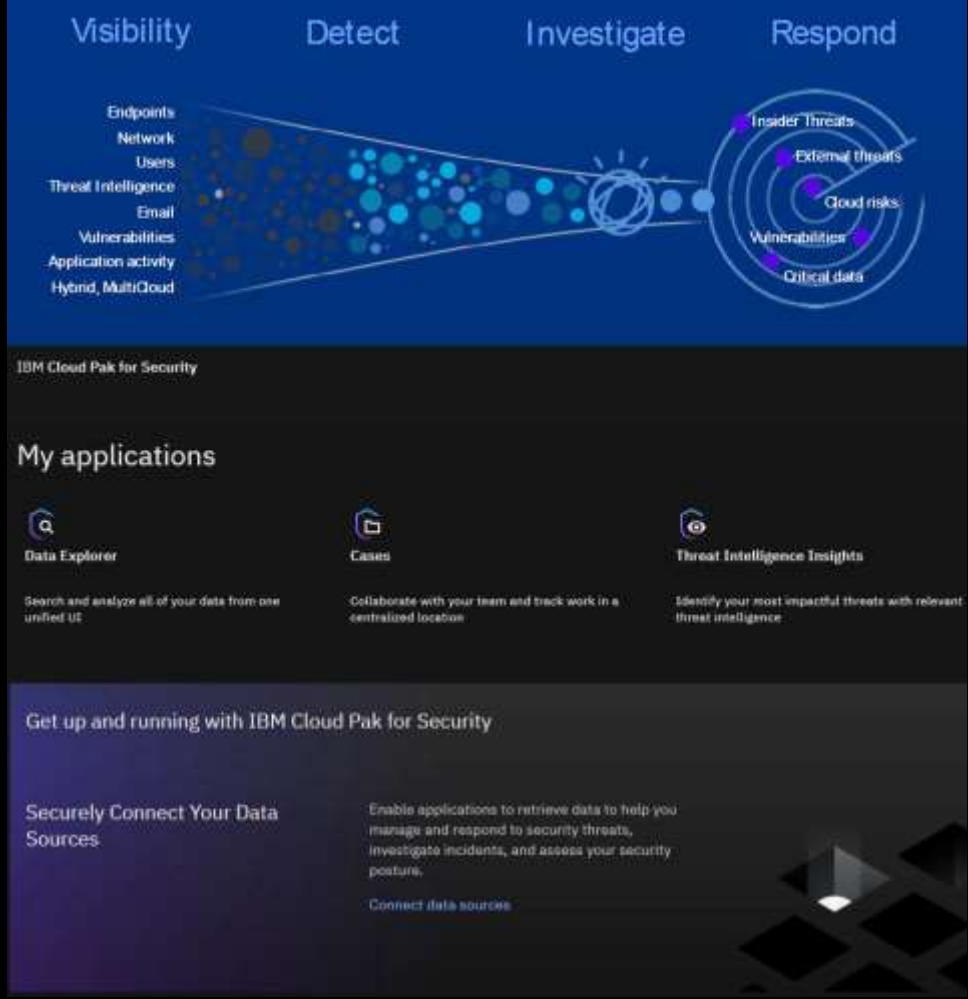
컴플라이언스 대응/반영 및 자동화된 감사증적 수집

클라우드 핵심 보안

1. **End to end data protection, with exclusive control**
2. Workload centric security, integrated with DevSecOps
3. Continuous compliance, with demonstrable controls
4. Continuous security, with actionable insights

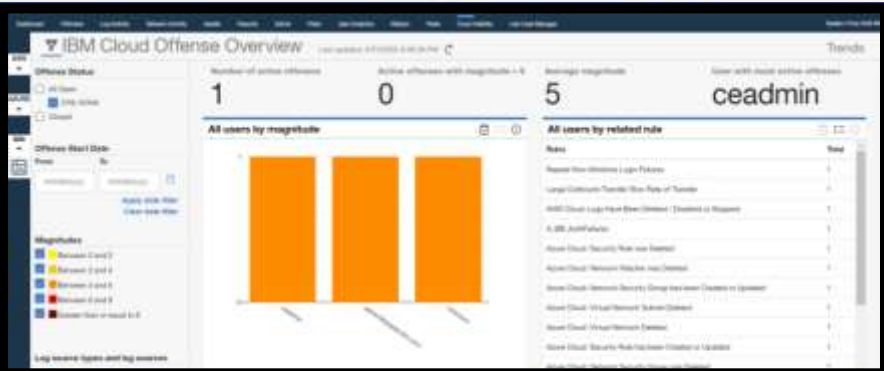
하이브리드 멀티 클라우드의 위협 관리

- 하이브리드 멀티 클라우드와 온프라미스 환경에 대한 통합 가시화
- 상관분석을 통한 위협 탐지
- 적극적 사고 대응 지원
- 자동화된 사고 대응

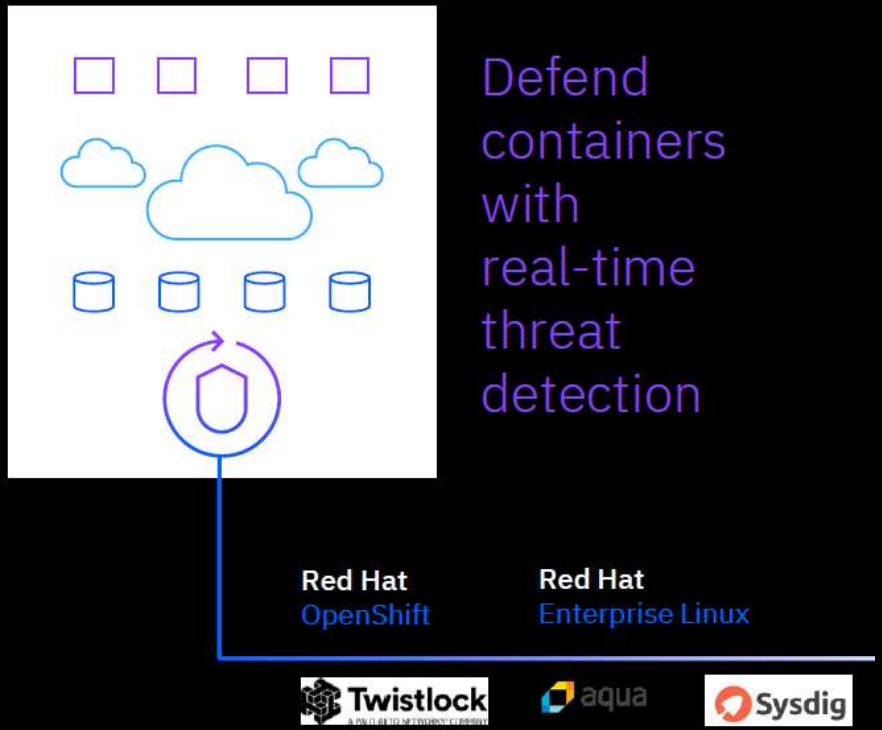


클라우드 워크로드 보안 및 위협 식별

- 온프라미스 및 IBM Cloud, AWS, Azure 등 다양한 IaaS 환경에 대한 보안 가시성 확보
- 실시간 클라우드 네트워크 분석 가시화
- 클라우드 구성 오류에 대한 빠른 탐지/방지
- 클라우드 위협에 대한 통합 가시화

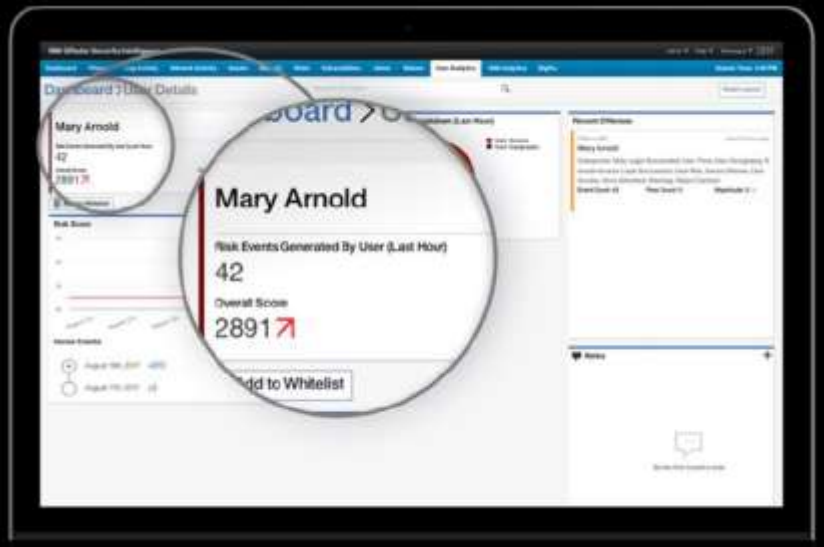


컨테이너 기반 앱 보호



- 컨테이너 기반 애플리케이션 가시화
- 컨테이너 IoC/계정 취약점 식별
- 위협 헌팅
- 이상 인증 및 권한 상승 식별
- 내부자 위협 및 데이터 유출 식별

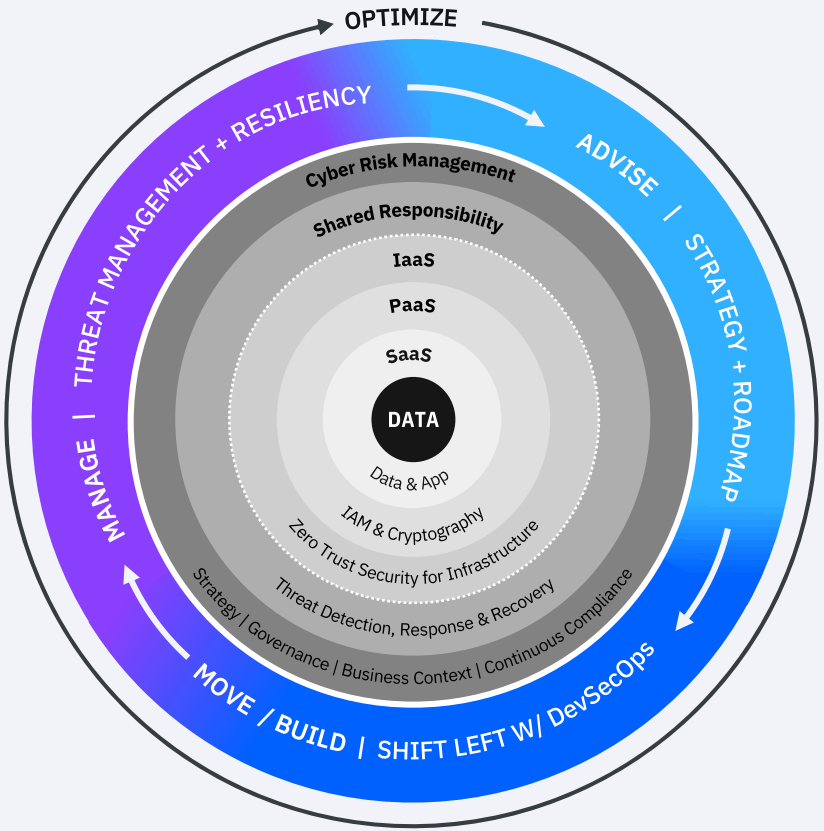
머신러닝 기반 클라우드 상의 내부자 위협 탐지



- 피싱 이메일, 멀웨어 탐지
- 악성 행위 예측을 위한 자속적인 사용자 학습
- 이상 행위, 남용, 미사용 계정 식별
- 기업 데이터 유출 보호
- SaaS, IaaS, PaaS 대상 멀티벡터 공격 탐지

User Behavior Analytics

성공적인 클라우드 전환을 위해서는 체계적인 보안 프로그램이 필요합니다



ADVISE

클라우드 혁신 전략의 핵심인 보안 및 컴플라이언스

MOVE / BUILD

성공적인 사례를 기반으로 안전한 환경으로 애플리케이션 이전 및 구축 지원

MANAGE

지속적인 보안 및 규정 준수 모니터링

감사합니다

Follow us on:

ibm.com/kr-ko/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

IBM Security

IBM