제조 및 유통산업을 위한
차세대 보안 전략 세미나

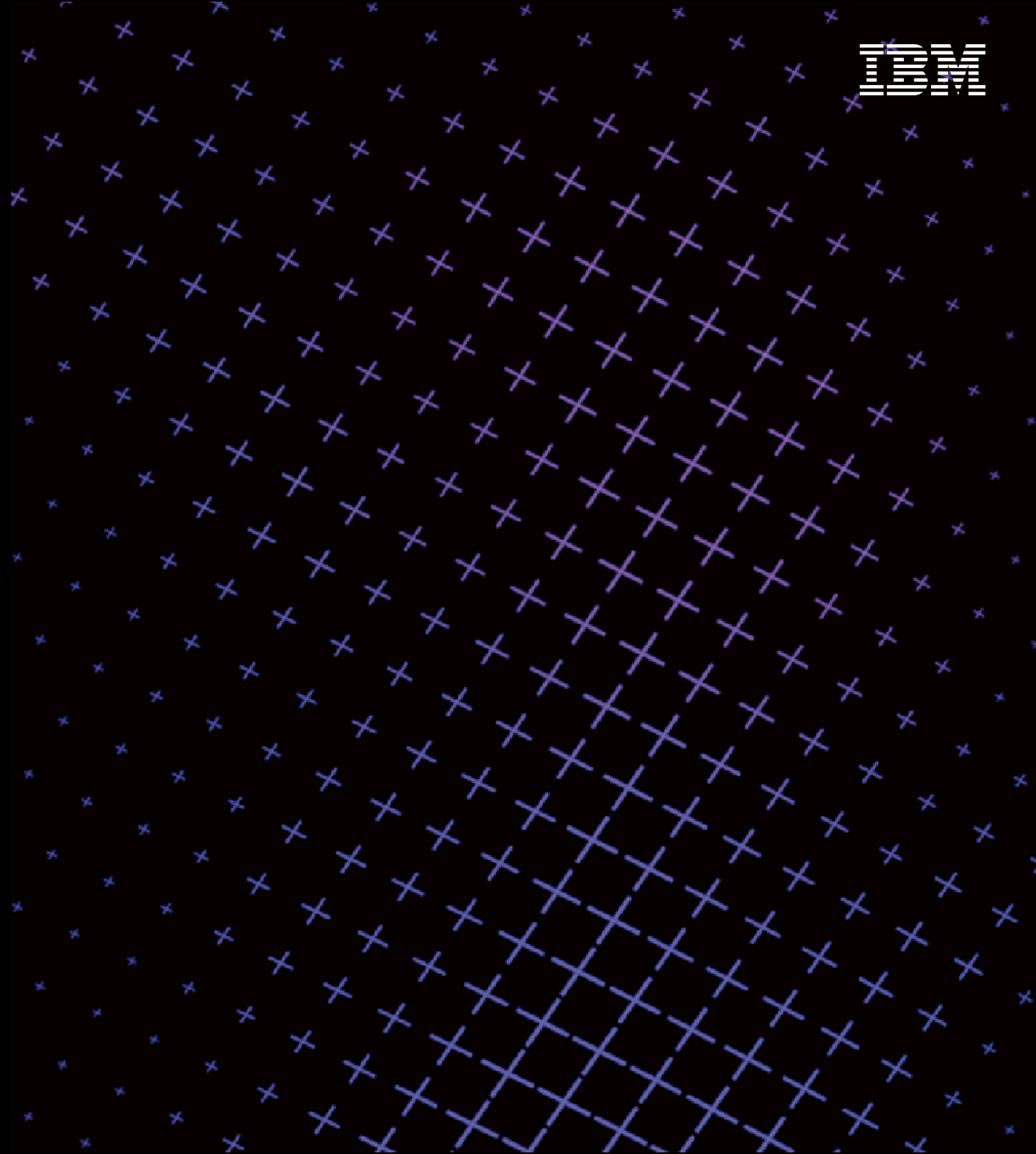
IBM Security

클라우드 전환에 따른 보안이슈와 대응방안

노용헌
클라우드 보안컨설턴트

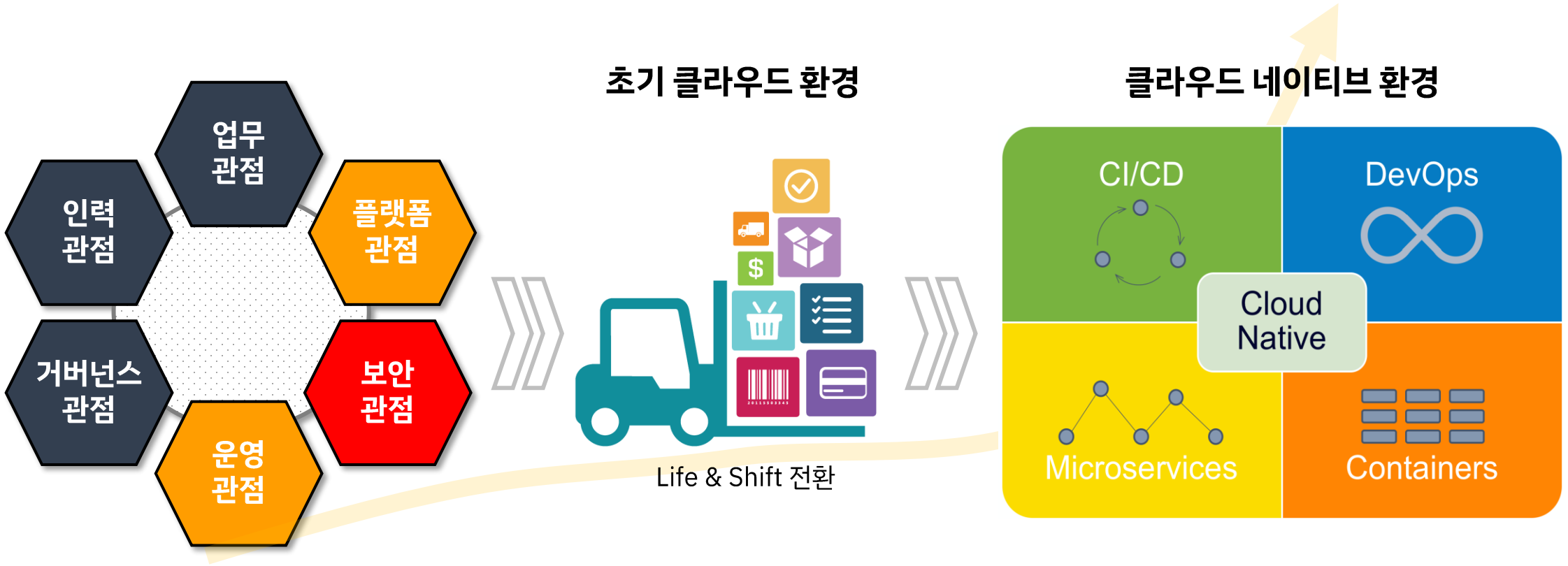
제조 및 유통산업을 위한

차세대 보안 전략 세미나

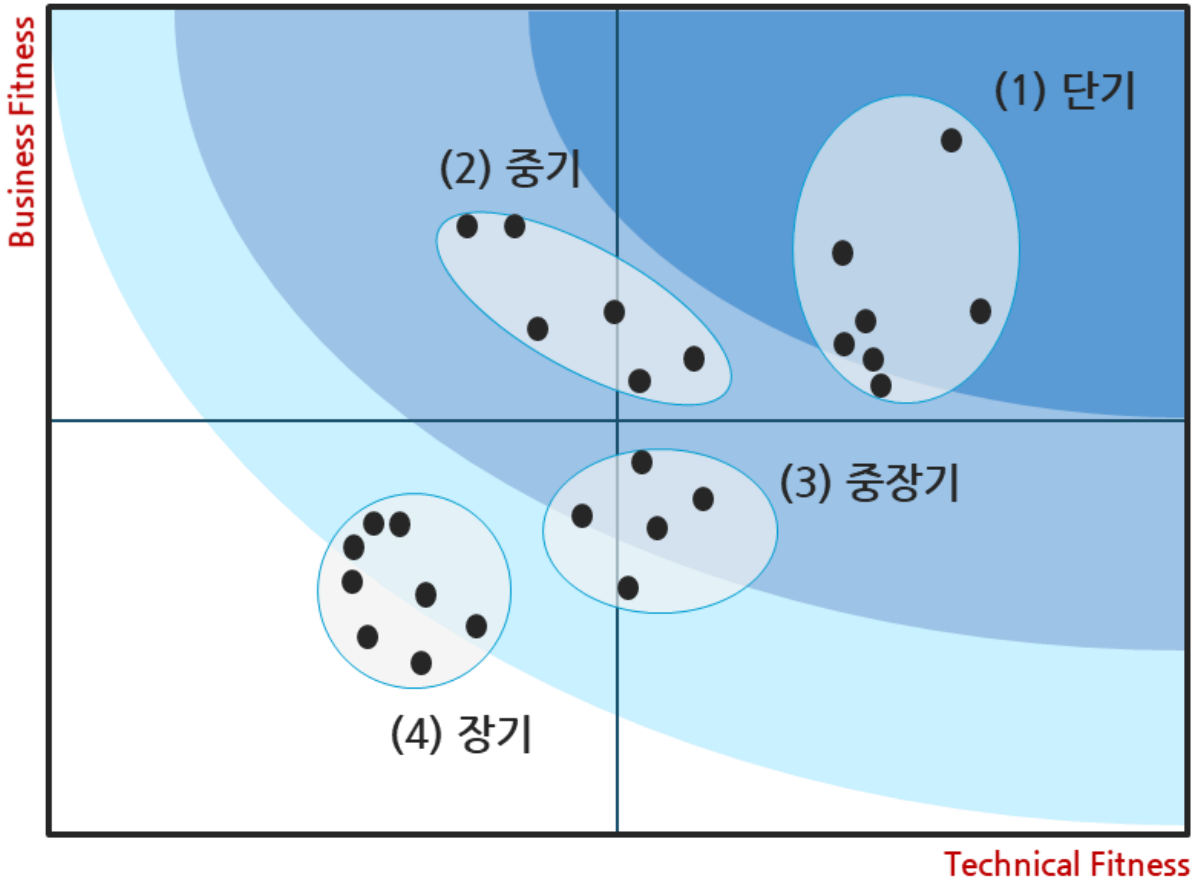


1. 클라우드로의 전환 프로세스
2. 클라우드에서의 보안이슈
3. Native 및 3rd Party 보안서비스
4. Well Secure Architecture 사례

클라우드로의 전환은 다양한 관점의 전략적 고민과 초기 Lift & Shift를 거쳐 Cloud Native 환경으로의 여정



클라우드 적합도 진단



1단계 단기 그룹: 클라우드 적합

- 현재 비용 절감, 확장성, 민첩성 등에 대한 요구사항이 분명하며, 규모가 작은 시스템
- 기술적 제약사항이 없거나 적은 비중요 업무 시스템

2단계 중기 그룹: 비즈니스 위험

- 내부 시스템으로 확장성, 민첩성 등의 요구사항이 있으며, 중간 규모의 시스템
- 기술적 제약 사항이 적은 일반 업무 시스템

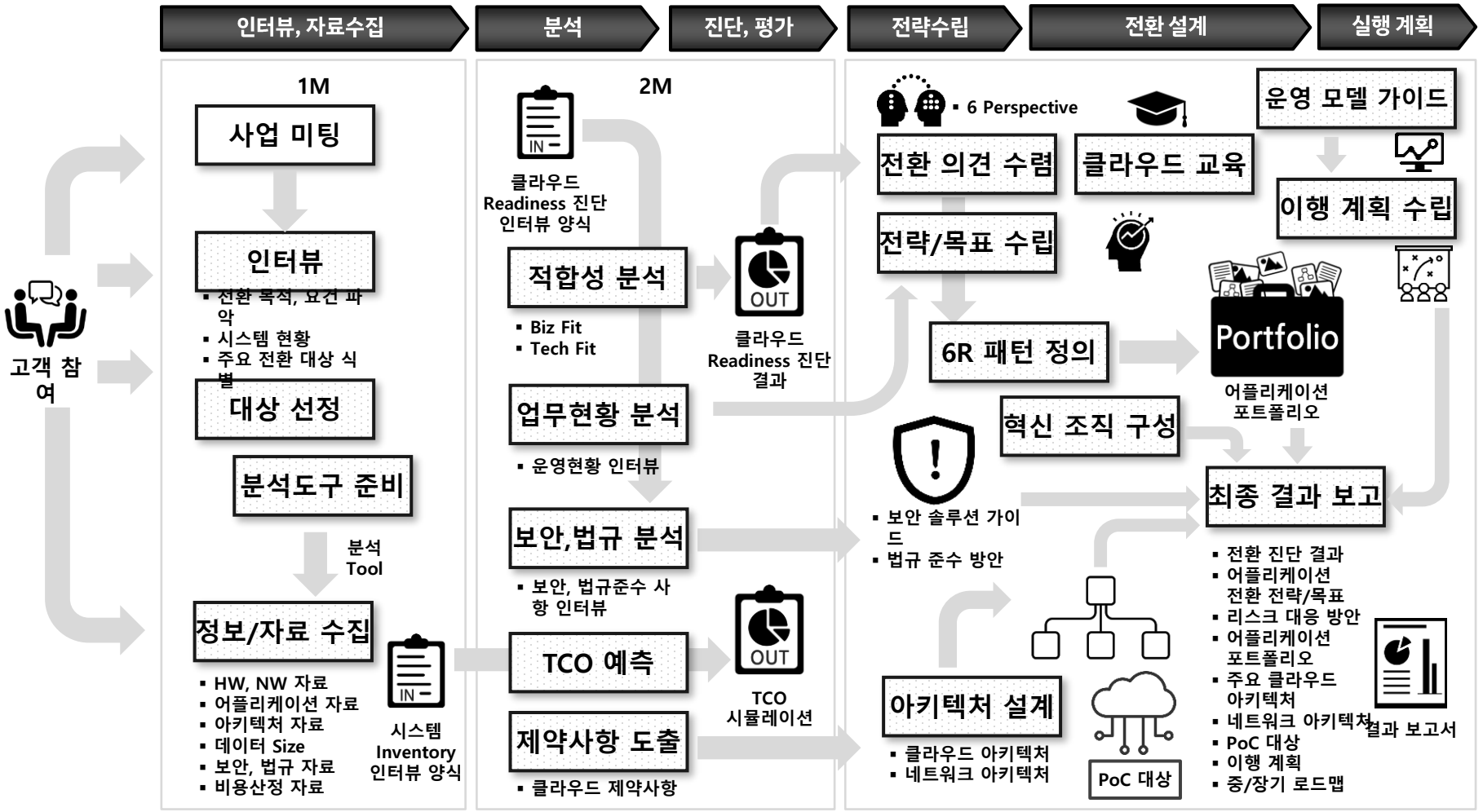
3단계 중장기 그룹: 비즈니스 위험

- 안정성과 성능 요구사항이 있는 일반/중요 시스템
- 하드웨어 및 솔루션 종속성 등의 기술적 제약 일부 존재

4단계 장기 그룹: 기술적 위험

- 주요 업무처리 시스템 및 개인신용정보를 포함한 중요 정보처리 시스템 등
- 시스템 규모가 크며, 하드웨어 및 솔루션 종속성 등의 기술적 제약이 많은 시스템

클라우드로의 전환은 자료 수집, 분석과 평가, 전략 수립 및 설계 후 실행 계획에 옮기는 철저한 전략이 필요



클라우드로의 전환 프로세스 (단계별)

블루프린팅 단계

- **Cloud 적합성 검증**
  시스템별 버전, 상용S/W 적용성 확인
- **마이그레이션 대상 자산 식별**
  시스템별 통합, 폐기 자산 확인
- **마이그레이션 패턴 정의**
  Re-Host/Re-Factor/Re-Platform
- **마이그레이션 복잡도 정의**
  Interface: 1-5 / 6-10 / >10
  Middleware/DB Upgrade
  App/DB Migration Reinstall
- **Overall Architecture 디자인**
- **PoC/Pilot Project 수행**

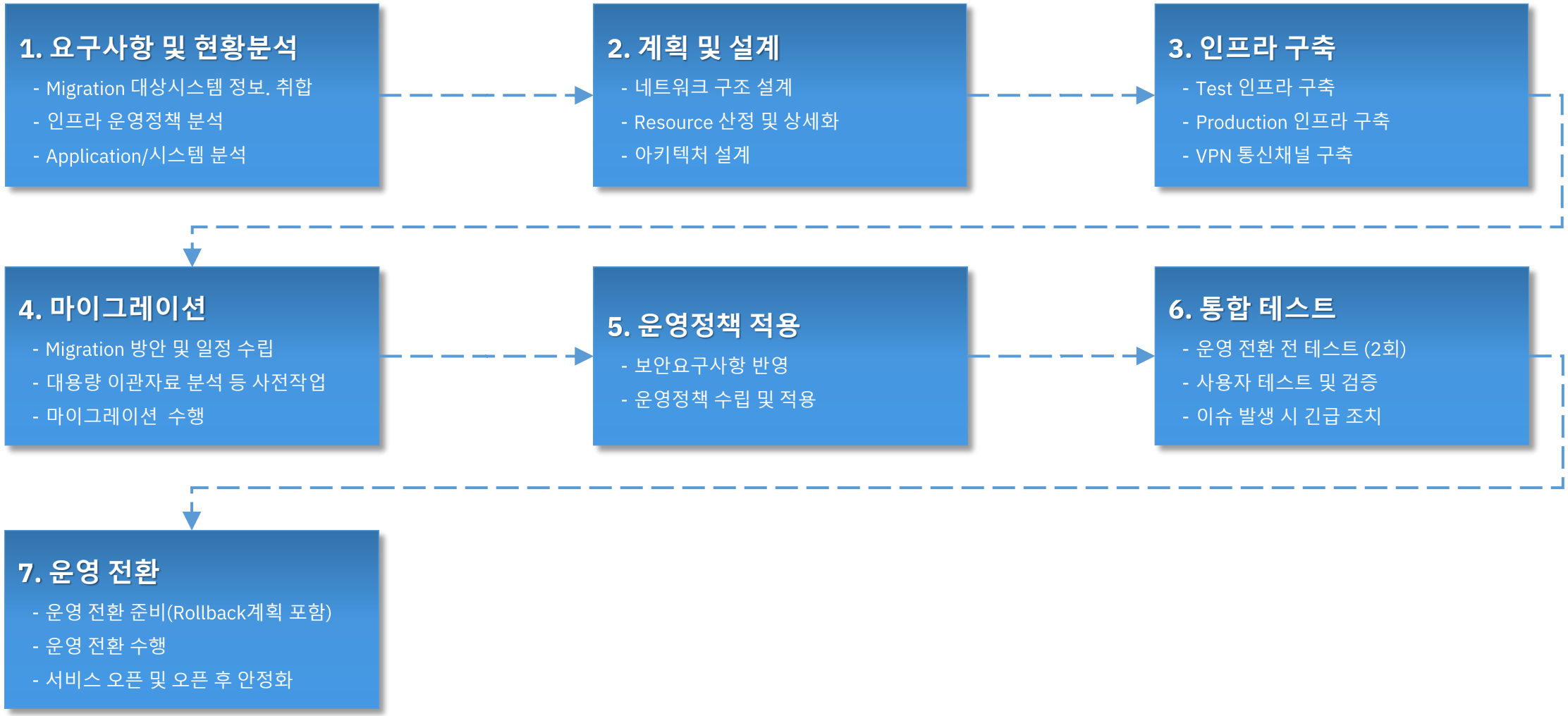
프로젝트 추진 단계

- **복잡도별 이관 우선순위 결정**
  우선순위별로 이관 진행
- **To-Be Instance별 Spec 산정**
  사용량에 따른 CPU, MEM 등 산정
  OS 및 DB 등 Upgrade 확정
  RDS 및 구축형 DB 확정
- **아키텍처 설계 및 구축**
  VPN: Office X CSP Region
  클라우드 네트워크 구조설계
  Test/Production 환경 구축
  계정관리 및 보안설정
  백업 등 운영정책 구성
- **우선순위별 마이그레이션**
  File 및 Database 마이그레이션
  Application 및 Binary 마이그레이션
  운영전환 시나리오, 롤백 플랜
  이관 후 테스트, 상태점검, 모니터링

안정화 단계

- **오픈 후 안정화**
  Network Usage Monitoring
  Performance Monitoring
- **내부 운영자 교육**
  네트워크 구성 내역
  시스템 연계를 위한 SG 구성 내역
  백업정책 구성 내역
  메일시스템 구성 내역
  사용내역 대쉬보드 설정
- **운영 및 모니터링**
  모니터링 항목 결정
  모니터링 체계 확정
  상시 모니터링 및 사용량 추이 분석

클라우드로의 전환 프로세스 (Task별)



Cloud에서의 보안 취약점(CSA기준)

ⓒ Getty Images Bank

- 데이터 유출
- 불충분한 ID, 자격 증명 및 액세스 관리
- 안전하지 않은 인터페이스와 API
- 시스템 취약점
- 계정 도용
- 악의적인 내부자
- APT
- 데이터 손실
- 불충분한 실사
- 클라우드 서비스 남용과 악의적인 사용
- DoS (DDoS)
- 공유 기술 취약점
- 스펙트라와 멜트다운

클라우드 컴퓨팅에 대한 12가지 주요 위협: 산업 인사이트 보고서, CSA

* CSA: Cloud Security Alliance

Cloud 보안사고에 대한 대응방안 (Cloud 보안사고는 기술적인 문제보다는 실수나 부주의가 원인)

No	보안 조치	내용
1	**클라우드 보안 옵션 적극 활용** (Using cloud security options)	클라우드서비스제공기업(CSP)가 제공하는 웹 어플리케이션 방화벽, DDoS 대응솔루션, VPN과 같은 네트워크 보안, 계정과 접근관리, 보안 모니터링 옵션 등을 적극 활용하여 보안을 설계한다
2	**접근 권한 관리** (Access authority management)	보안의 가장 기본이 되는 인증(Authentication) 및 인가(Authorization)는 우선 고려되어야 한다
3	**데이터 보호** (Data Protection)	클라우드 상의 가상서버(VM) 및 데이터베이스의 개인정보를 포함한 중요 데이터는 암호화 되어 보호되어야 하며, 해당 조치는 별도의 보안 솔루션을 통해서 수행하는 것을 고려해야 한다
4	**통합 보안 관제를 통한 가시성 확보** (Visibility thru Managed Security Service)	클라우드 보안에 대한 통합 보안 관제 환경을 구축하고 이를 통하여 가시성을 확보 및 보안위협을 탐지/대응해야 한다

보안 취약점에 대한 고려 사항 (Application/Database/Server/Network)

고려 사항

- 보안 요구수준을 충족하기 위해 보안 요소에 대한 누락없이 솔루션 및 방안 검토

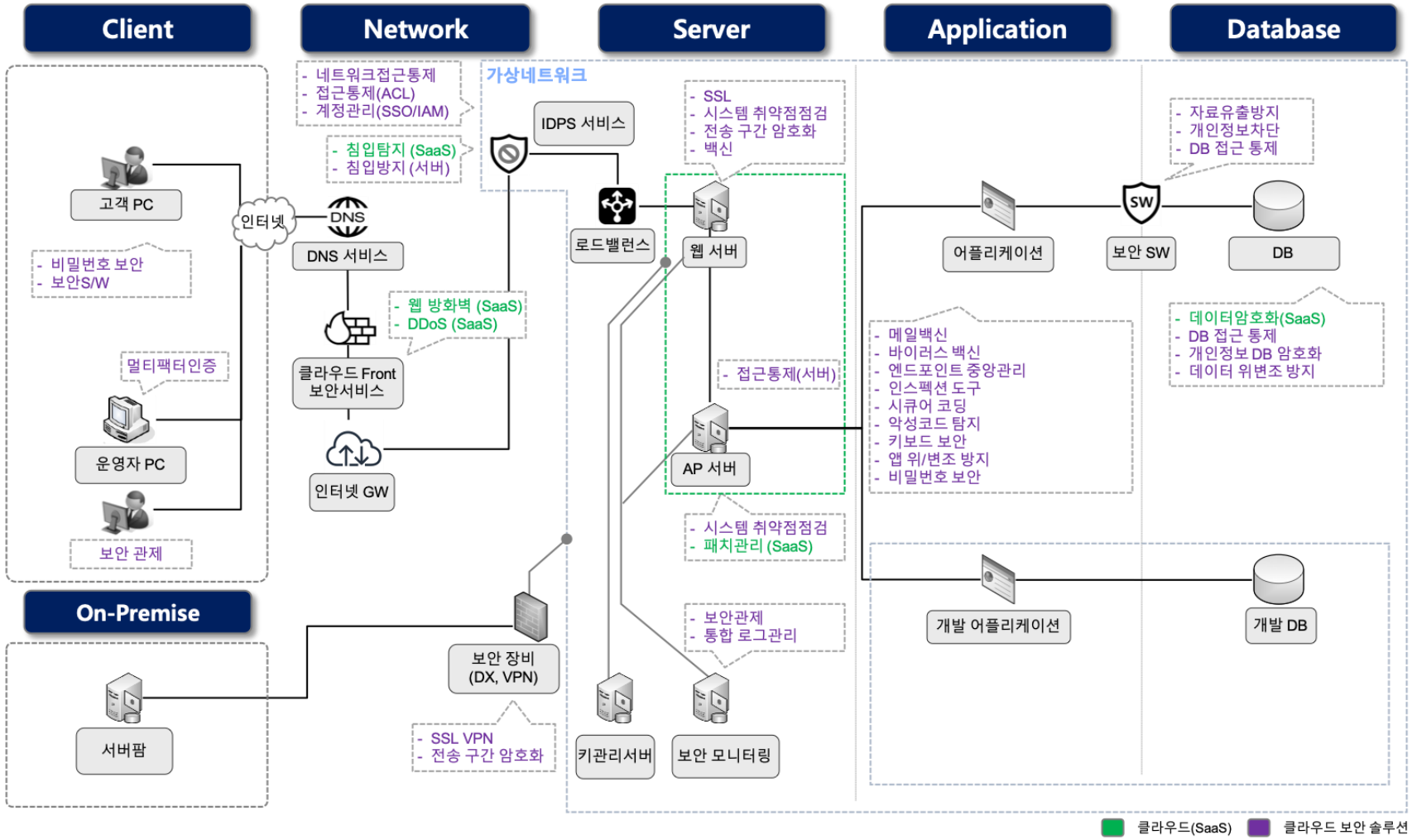
보안 항목별 + 시스템 / 인프라 별

- 클라우드에서 제공하는 기본 보안 기능 및 오픈 소스를 활용하여 비용을 절감할 수 있는 방안 검토
- 보안성 검토 및 취약점 제거를 위한 보안 컨설팅이 필요한 항목에 대한 고려

구분	인증/권한 관리	접근 통제	해킹/ 악성코드	취약점 분석	암호화	모니터링 및 장애추적	법규준수
Application	SSO/IAM		F/W	소스코드 진단	개인정보 암호화	Log Trail	개인정보보호
	MFA			모의해킹	KMS		
Database	IAM	DB Access Control	Vaccine		Encryption	보안관제 (MSSP)	
Server		Server Access Control		인프라 취약점 점검	SSL		보안성 검토
			Patch Management				
Network		ACL	IDS/IPS				
		Security Group	DDoS				
		Network Isolation			VPN		

클라우드 기본 기능 (무료) | 오픈소스 | 3rd Party 솔루션 도입 (CSP 유료 기능) | 보안 서비스

클라우드 환경에서의 보안 구성 개념도



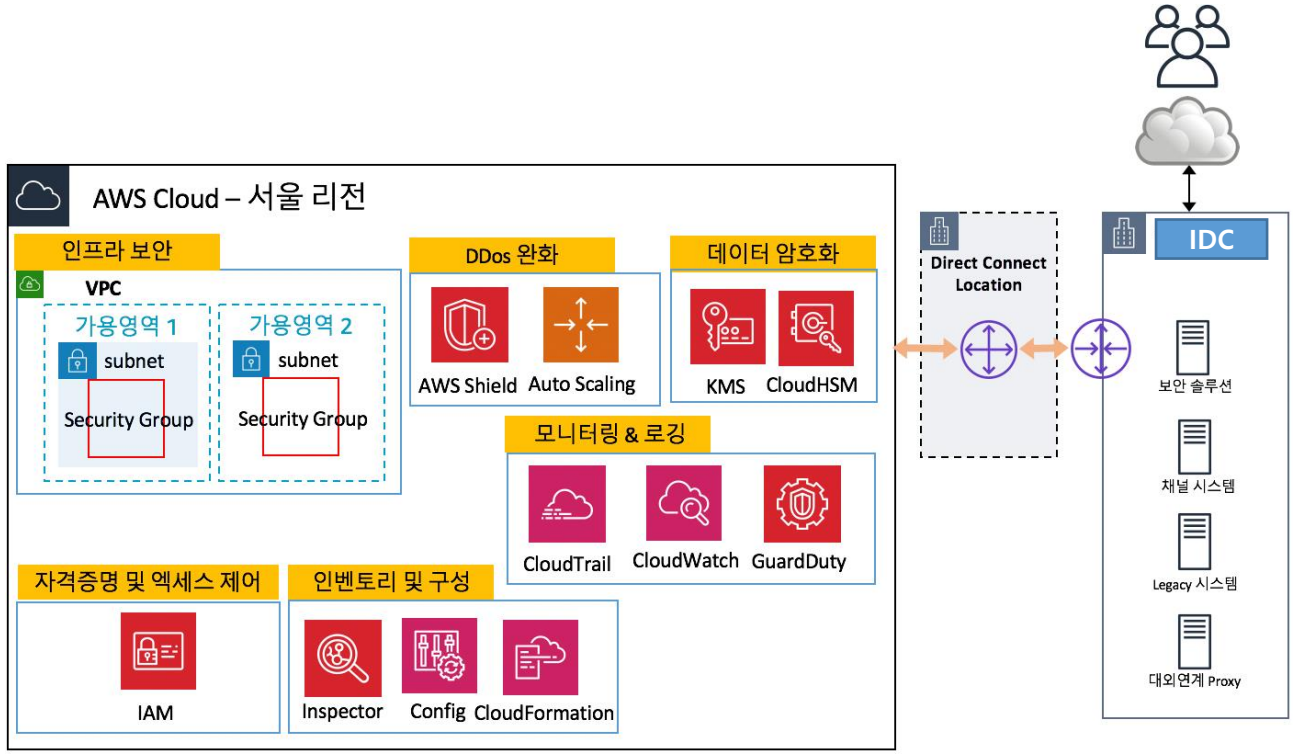
클라우드 환경에서의 보안 솔루션 활용 방안

→ CSP가 모든 보안서비스 제공하지 못함. 따라서 적절한 3rd Party 서비스 활용이 필요함

보안구분	적용 방안	CSP 제공
1. 패치관리	클라우드 서비스로 대체	O
2. 백신	보안 솔루션 사용	X
3. 보안관제	클라우드 서비스로 대체	O
4. DB 접근제어	보안 솔루션 사용	X
5. 데이터 암호화	클라우드 서비스로 대체	O
6. 소스코드 진단	보안 솔루션 사용	X
7. 망분리	보안 솔루션 사용	X
8. ACL	클라우드 서비스로 대체	O
9. IAM	클라우드 서비스로 대체	O
10. KMS	클라우드 서비스로 대체	O

보안구분	적용 방안	CSP 제공
11. SSL	클라우드 서비스로 대체	O
12. 개인정보암호화	보안 솔루션 사용	X
13. 방화벽	클라우드 서비스로 대체	O
14. WIPS	보안 솔루션 사용	X
15. 서버 접근 제어	클라우드 서비스로 대체	O
16. DDoS	클라우드 서비스로 대체	O
17. ID(P)S	클라우드 서비스로 대체	O
18. 데이터암호화	클라우드 서비스로 대체	O
19. 로그추적	클라우드 서비스로 대체	O
20. 인프라취약점	클라우드 서비스로 대체	O

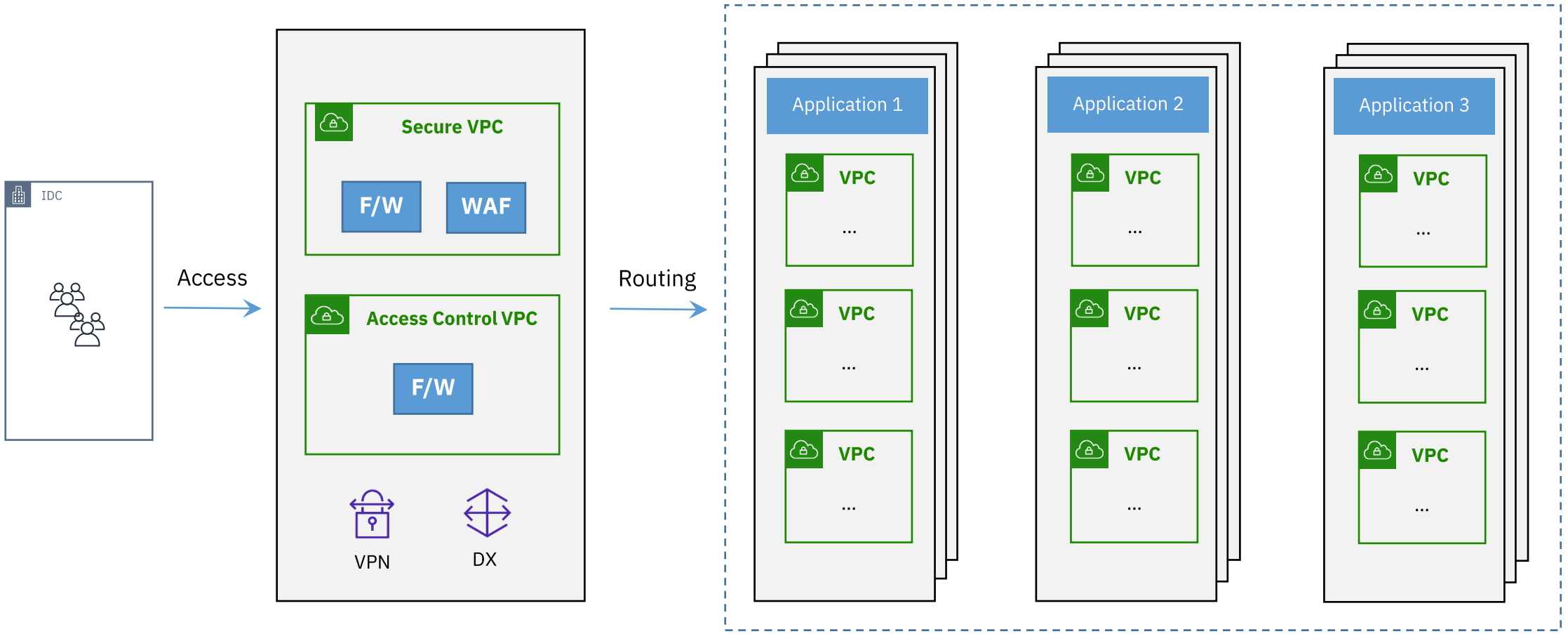
Well-Architecture for Security (단일 시스템인 경우)



보안 인프라 구성방안

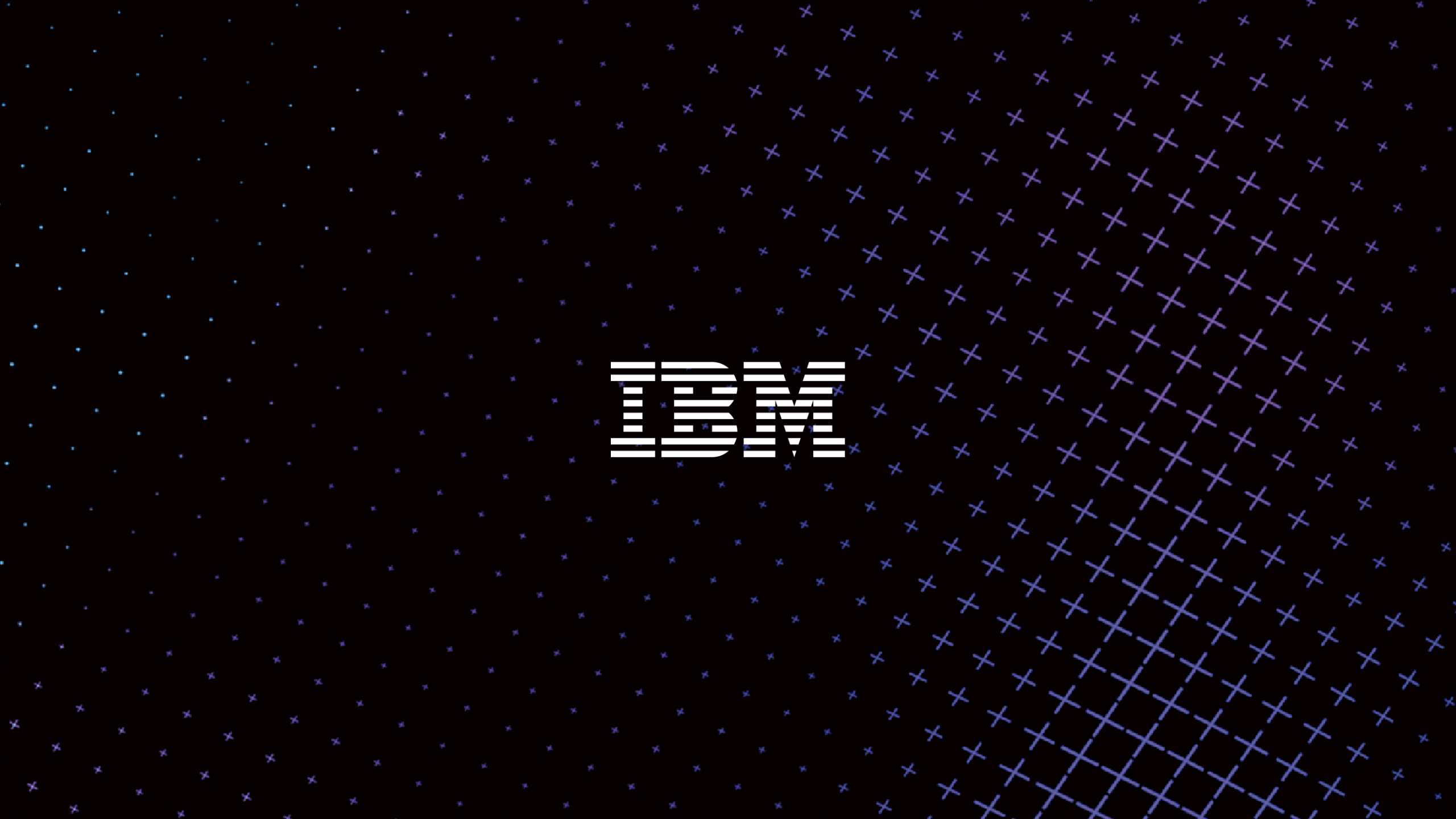
- 접근통제 구현: NACL, Security Group을 통한 서버 방화벽 구성
- 안전한 암호화 Key 관리: Key Management Service 활용
- 권한 및 자격증명: Identity and Access Management 활용
- 보안취약점에 대한 진단 및 평가: Inspector 서비스 활용
- Config를 통한 resource 변경 파악
- CloudFormation으로 Infra 환경 생성을 위한 템플릿 정의 및 관리
- CloudTrail을 활용한 클라우드 상의 모든 관리 작업에 대한 로깅 수행
- GurardDuty를 통한 위협 탐지
- Shield Service를 통한 DDoS 공격 대응
- Public Cloud와 On-Premise간은 Dedicated Line 이나 VPN 활용

Well-Architecture for Security (여러 시스템인 경우)



Lessons and Learned

- 클라우드 상에서 해당 어플리케이션의 보안성 검토를 진행한다
- On-Premise에서와 동일한 보안 구성이 적절한 지 검토한다
- 클라우드 자체의 Concept에 맞는 CSP Native 보안서비스를 충분히 검토한다
- Cloud-friendly한 3rd Party 보안솔루션 및 서비스의 활용을 검토한다
- 법규 및 규제사항을 검토하고 반영한다
- BCP / DRP 계획을 CSP와 함께 검토 및 수행한다
- 클라우드 상에서 지속적인 보안관제 서비스를 수행 또는 활용한다


IBM