
Microsoft
Solutions Partner
Cloud MSP
Specialization
Partner
Azure Landing Zone Deployment
LEADING INNOVATOR IN CLOUD
TDG

목차

1-1. Landing Zone 이란?

랜딩존이 무엇인지, 왜 필요한지 이해하기 위해 건축에 비유해보면, '집을 짓기 위한 기반 작업'으로 볼 수 있습니다. 랜딩존이 구성되었다는 것은 관리 요소 및 기반이 완성되었다는 것 을 의미합니다. 그렇기 때문에 시스템 구축의 속도가 향상되고 비용이 감소됩니다. 또한 일관된 규칙 적용이 적용되어 모니터링 및 관리가 용이합니다.

- 구축 속도 향상
- 비용 감소
- 일관된 규칙 적용
- 관리 용이

건축 프로세스(요약)

계획 및 설계

착공 및 시공

완공 및 사용승인

Landing Zone = 집을 짓기 위한 기반 작업!

이미지 출처 : freepik.com

1-2. Azure Landing Zone 장점

Azure 랜딩존은 Azure 클라우드를 도입하는 기업과 사용자들에게 유용하고 안정적인 운영 환경을 제공하기 위한 구성 요소를 포함하는 플랫폼입니다. 이를 구축하는 궁극적인 이유와 장점은 다음과 같습니다.

많은 배포, 테스트, 검증 작업 수행

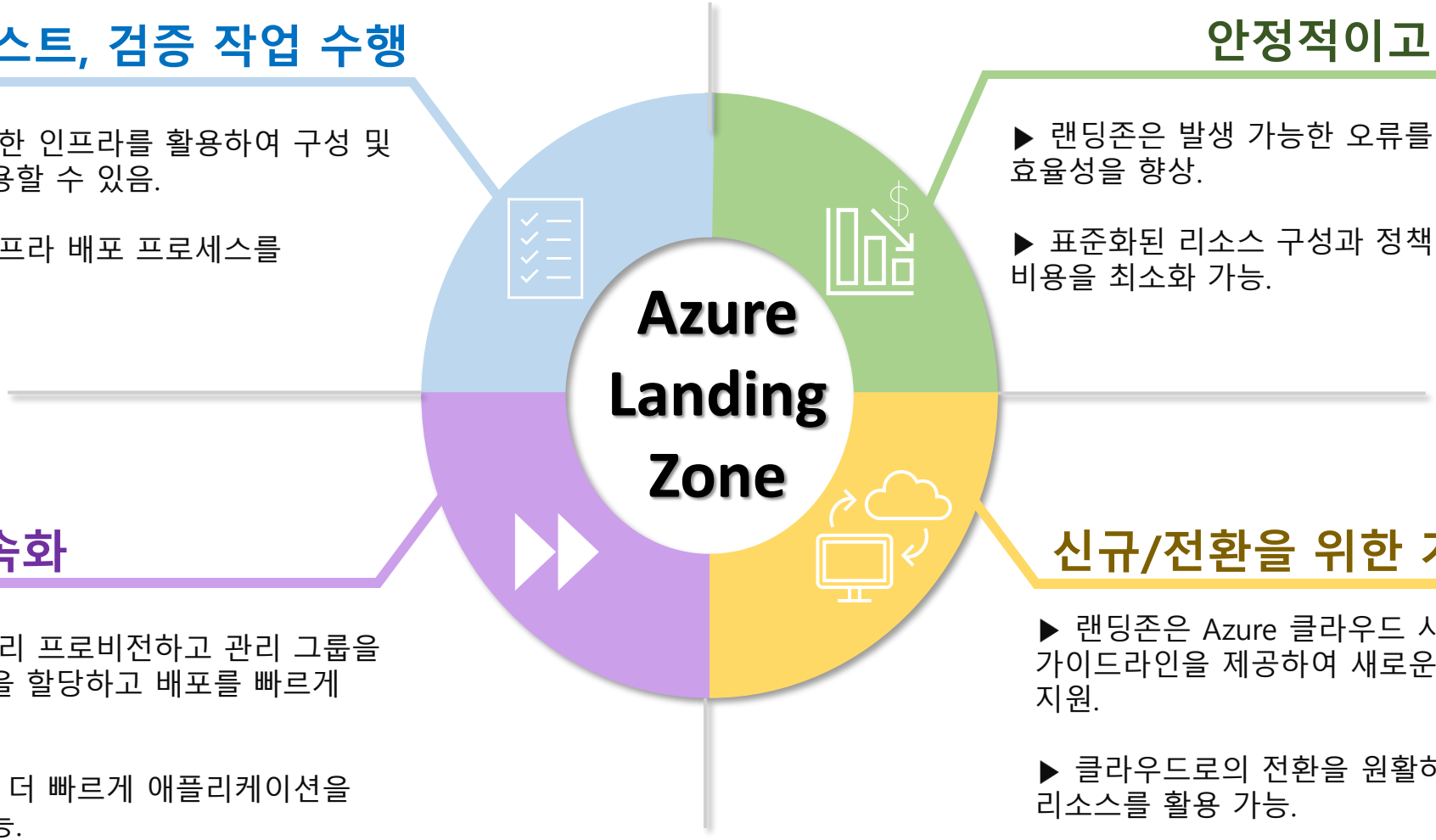
▶ 랜딩존은 반복 가능한 인프라를 활용하여 구성 및 컨트롤을 일관되게 적용할 수 있음.

▶ 애플리케이션 및 인프라 배포 프로세스를 효율적으로 관리 가능.

안정적이고 저렴한 운영

▶ 랜딩존은 발생 가능한 오류를 감소시키고 운영 효율성을 향상.

▶ 표준화된 리소스 구성과 정책 적용을 통해 운영 비용을 최소화 가능.



배포 빈도 가속화

▶ 랜딩존은 환경을 미리 프로비전하고 관리 그룹을 사용하여 정책 컨트롤을 할당하고 배포를 빠르게 수행할 수 있도록 함.

▶ 개발자 및 운영팀은 더 빠르게 애플리케이션을 배포하고 업데이트 가능.

신규/전환을 위한 가이드 라인 제시

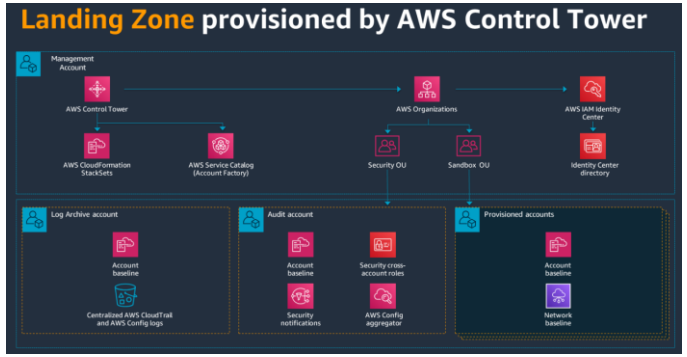
▶ 랜딩존은 Azure 클라우드 사용에 대한 가이드라인을 제공하여 새로운 기능 시나리오 전략을 지원.

▶ 클라우드로의 전환을 원활하게 수행하고 최적의 리소스를 활용 가능.

1-3. CSP 별 Landing Zone 차이점

Azure 랜딩존과 AWS 랜딩존 둘 다 클라우드 환경에서 안전하고 효율적인 리소스 관리를 위한 구조를 제공하지만 구체적인 구현 방식과 제공하는 도구 등 아래와 같이 몇가지 차이점이 있습니다.

Azure 랜딩존



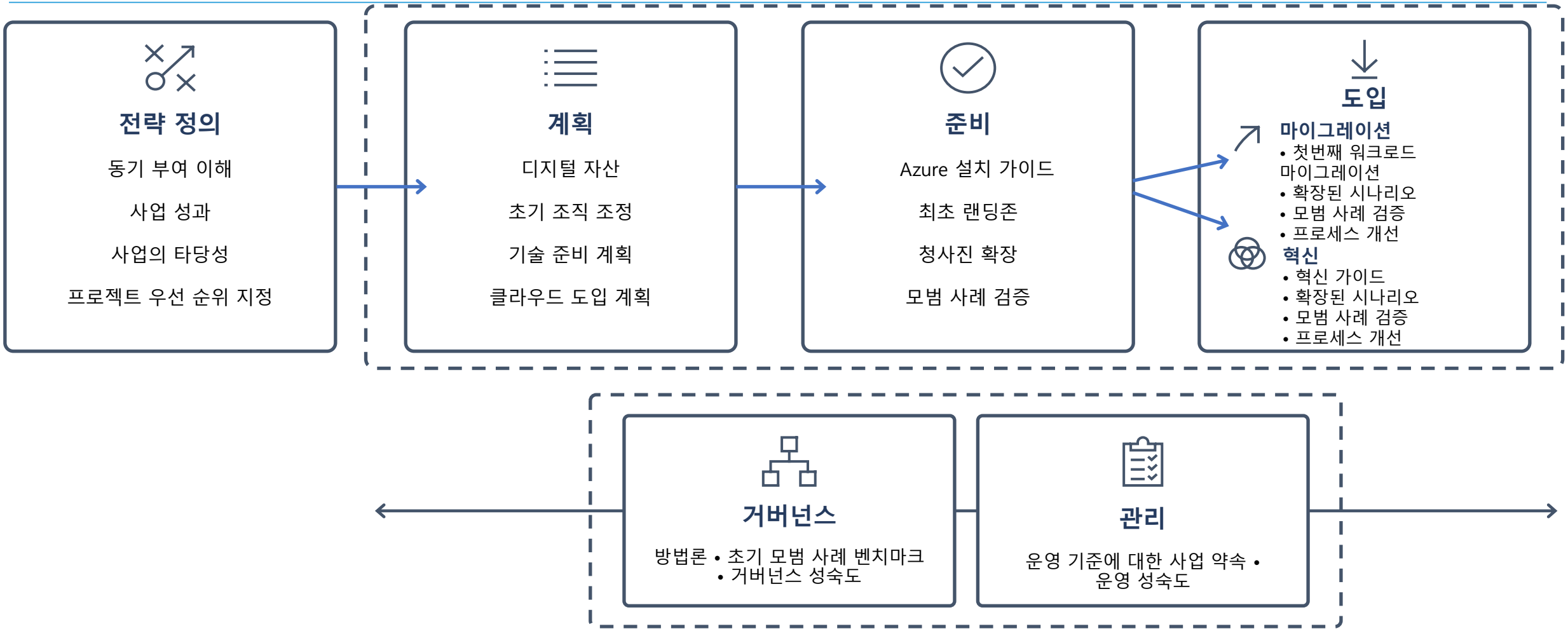
AWS 랜딩존

	Azure 랜딩존	AWS 랜딩존
구조	**구독 기반**, 관리 그룹과 정책을 통한 리소스 조직	계정 기반, AWS Organizations를 통한 리소스 조직
보안	Azure Policy와 Blueprints를 통한 보안 및 규정 준수 자동화	AWS Control Tower와 Service Catalog를 통한 보안 및 규정 준수 자동화
자동화	Azure Resource Manager 템플릿과 Bicep	AWS Cloud Formation 템플릿
관리	Azure Portal과 가속기를 통한 중앙 관리	AWS SSO와 AVM을 통한 사용자 계정 접근 관리
디자인영역	**8개의 디자인 영역에서 주요 디자인 원칙을 따름**	다계정 프레임워크를 사용하여 리소스와 워크로드를 여러 계정으로 분리
가속기	Azure 랜딩 존 포털 가속기를 통한 배포	AWS Account Vending Machine(AVM)을 통한 계정 프로비저닝
리소스 격리	**구독을 사용하여 애플리케이션 리소스 및 플랫폼 리소스 격리**	리소스와 워크로드를 여러 AWS 계정으로 분리하여 격리
구축 시간	가속기를 사용하여 빠른 배포와 구축 시간 단축 가능	랜딩 존의 계정 및 네트워크, 보안 요소가 이미 완성되어 있어 구축 속도 향상

2. Azure 랜딩존 설계

2-1. CAF (Cloud Adoption Framework) 정의

Azure 랜딩존 CAF (Cloud Adoption Framework) 는 클라우드 채택을 위한 전략, 계획, 준비, 채택, 관리 등의 과정을 제공하는 프레임워크 입니다. 조직이 클라우드에서 성공 하는 데 필요한 비즈니스 및 기술 전략을 만들고 구현 하는 데 도움이 되도록 설계된 증명된 가이드라인을 제공합니다.



2-2. Azure 랜딩존 설계 항목

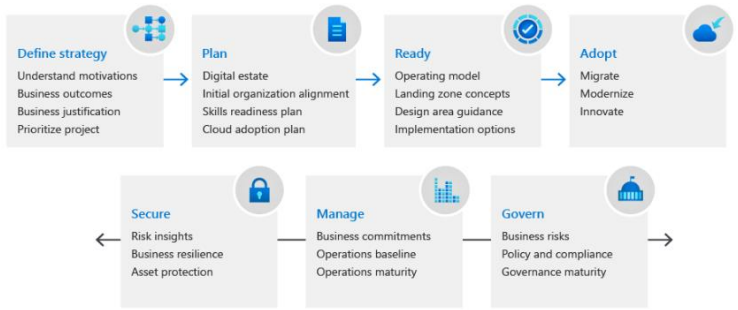
Azure Landing zone을 설계할 때는 총 8가지의 디자인 영역을 고려해야 합니다. 각 디자인 영역은 클라우드 환경을 보안, 규정, 효율, 혁신 등의 측면에서 최적화하는 데 필요한 설계 요구사항을 포함합니다.

Azure Landing Zones 설계 항목

3. Azure 랜딩존 운영

3-1. 운영 모델 및 책임

Azure 랜딩존의 운영 모델은 조직의 요구 사항과 비즈니스 목표에 맞게 조정되어야 하며, 효율적인 클라우드 운영을 위한 기반이 됩니다.

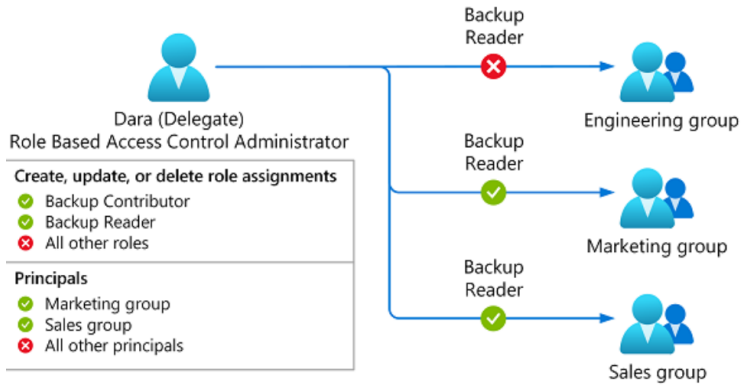


클라우드 운영 모델 정의

▶ Azure 랜딩존의 운영 모델은 클라우드 환경에서 효율적인 운영을 위해 필요한 프레임워크.

▶ 리소스 관리, 보안, 모니터링, 자동화 등을 포함.

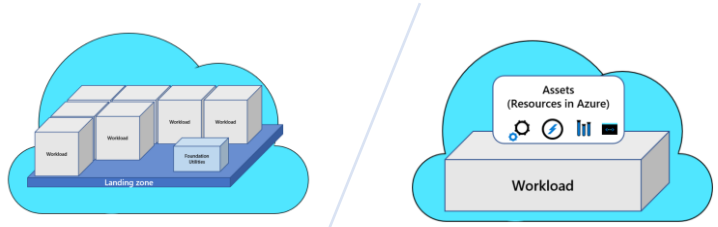
▶ 주요 원칙: 확장성, 유연성, 안정성, 비용 효율성.



역할 및 책임 할당

▶ Azure 랜딩존에서는 팀과 구성원 간에 적절한 역할과 책임을 할당하여 효율적인 운영을 지원.

※ 예시
- 운영 팀: 리소스 관리, 모니터링, 보안 설정 등을 담당.
- 개발 팀: 애플리케이션 배포, CI/CD, 자동화 작업을 수행.
- 보안 팀: 보안 정책, 역할 기반 접근 제어 등을 관리.



중앙 집중식 운영 **분산 운영**

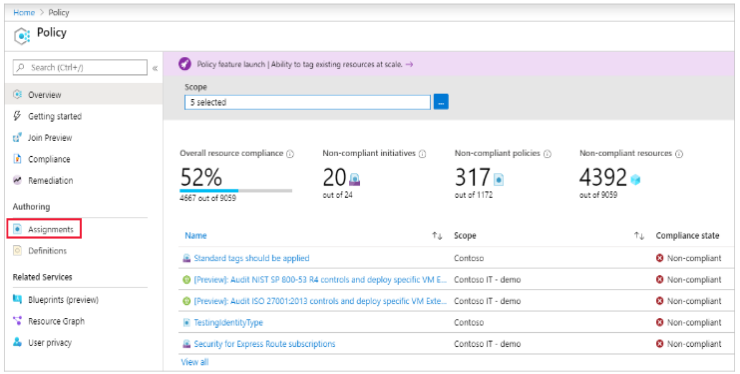
운영 방식 채택

▶ 중앙 집중식 운영
- 중앙에서 모든 결정을 내리고 관리하는 방식.
- 표준화, 일관성, 중앙 집중적인 보안 관리를 강조.
- 중앙 IT 팀이 리소스를 관리하고 모든 결정.

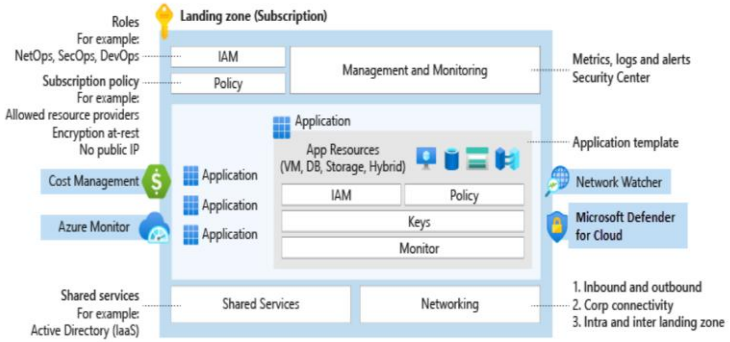
▶ 분산 운영
- 팀별로 자율적으로 운영하는 방식.
- 팀은 자체적으로 리소스를 관리하고 결정을 내림.
- 빠른 응답과 유연성을 강조.

3-2. 정책 및 거버넌스

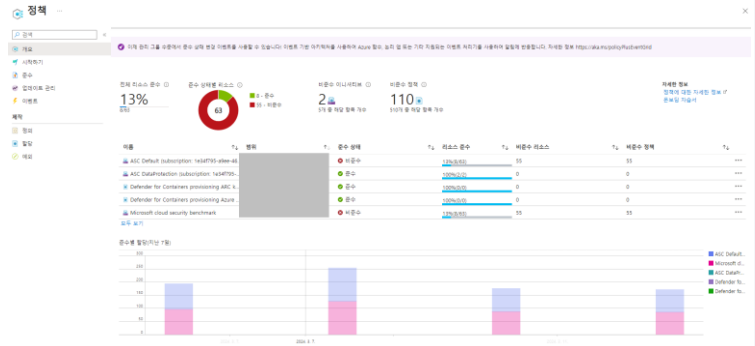
Azure 랜딩존의 정책 및 거버넌스는 리소스 관리와 보안을 강화하며, 조직의 비즈니스 요구 사항을 충족시키기 위한 중요한 요소입니다.



정책 설정 및 관리



거버넌스 구조



준수 및 감사 프로세스

▶ 정책 설정
- 리소스의 사용을 제어하기 위해 정책을 설정.

※ 예시
- 특정 리소스 유형의 생성을 제한하거나 암호화를 강제하는 정책을 설정 가능.

▶ 정책 관리
- 정책을 모니터링하고 관리하여 준수를 유지.
- 정책 준수 상태를 확인후, 정책 위반시 경고를 발생시키는 기능 활용.

▶ 거버넌스
- 조직 내에서 정책 준수를 강화하고 리소스를 효율적으로 관리하기 위한 구조를 의미.

▶ 구성 요소
- 정책 정의: 리소스에 적용되는 정책을 정의.
- 정책 할당: 정책을 리소스 그룹, 구독 또는 관리 그룹에 할당.
- 모니터링 및 보고: 정책 준수 상태를 모니터링하고 보고서를 생성.

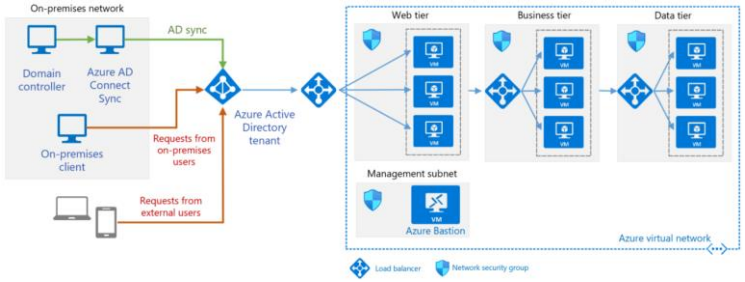
▶ 정책 준수 확인
- 정책 준수를 확인하고 리소스가 정책을 준수하는지 감사.

▶ 감사 로그
- 리소스의 변경 이력과 정책 준수 상태를 기록하는 감사 로그를 활용.

▶ 감사 프로세스
- 정기적으로 감사를 수행하여 정책 준수를 검증하고 보고.

3-3. 보안 및 ID 관리

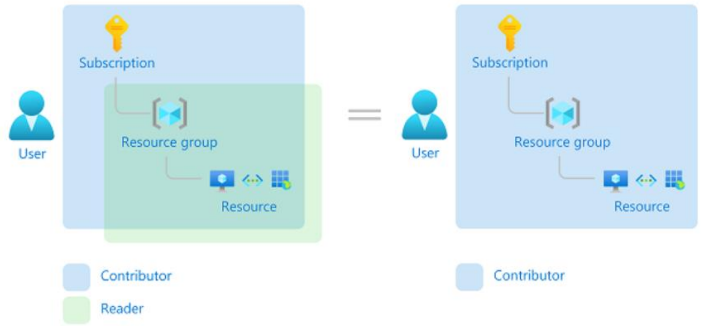
Azure 랜딩존의 보안 및 ID 관리는 리소스의 보안을 강화하고 사용자 액세스를 효율적으로 관리하기 위한 핵심 요소입니다.



Azure Entra ID와 통합

▶ Azure Entra ID (Azure AD) 는 클라우드 기반의 ID 관리 서비스.

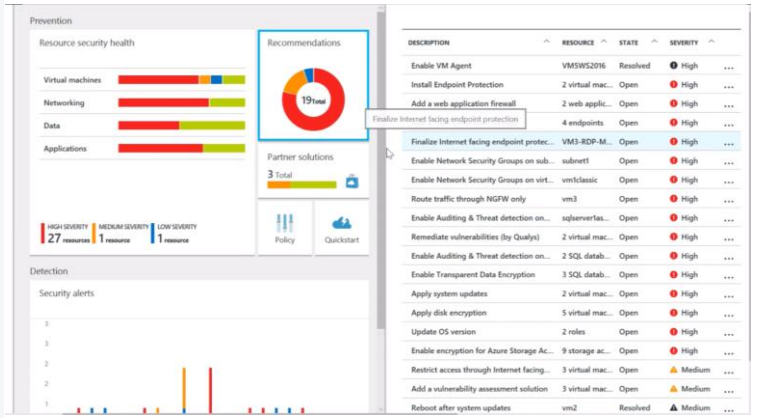
▶ 사용자 ID 관리를 위해 Azure Entra ID를 통합.
- 사용자 계정 생성 및 관리
- 다중 요소 인증 (MFA) 설정
- 역할 기반 접근 제어 (RBAC) 지원



Identity and Access Management (IAM)

▶ IAM 은 사용자/ 리소스 간 액세스를 관리하는 중요한 요소.

▶ IAM 의 기능.
- 역할 기반 접근 제어 (RBAC): 역할을 할당하여 사용자에게 필요한 권한을 부여.
- 서비스 주체 (Service Principal): 서비스 계정을 사용하여 애플리케이션과 리소스 간의 인증을 수행.
- 액세스 제어 정책: 리소스에 대한 액세스를 제어하는 정책을 설정.



네트워크 보안 그룹 및 Microsoft Defender for Cloud 활용

▶ 네트워크 보안 그룹 (NSG)
- 가상 네트워크 내에서 트래픽을 제어하는 방화벽 규칙을 정의.
- NSG를 사용하여 특정 포트 또는 IP 주소로의 트래픽 허용 or 차단.

▶ Microsoft Defender for Cloud
- 클라우드 보안 솔루션으로, 보안 상태 모니터링 및 보안 위협을 탐지.
- 보안 권장 사항 제공 및 보안 이벤트를 분석하여 대응 방안을 제시.

3-4. 모니터링 및 로그 관리

Azure 랜딩존의 모니터링 및 로그 관리는 리소스의 상태를 파악하고 문제를 조기에 발견하여 운영을 원활하게 유지하는 데 중요한 역할을 합니다.

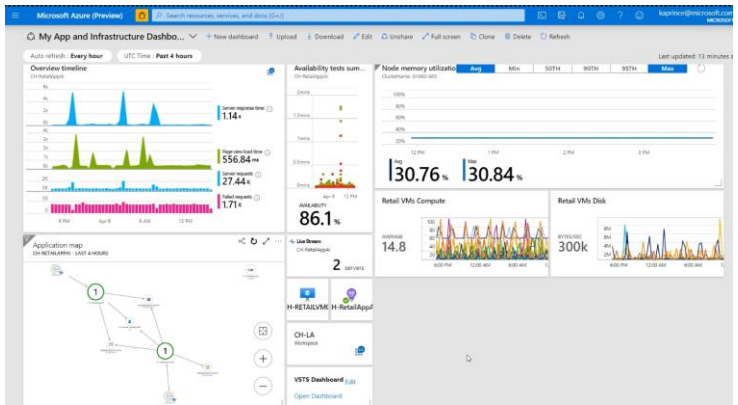
Azure monitor

Azure Log Analytics

모니터링 및 로그 관리 도구

▶ Azure Monitor
- 클라우드 리소스의 성능을 지속적으로 모니터링하는 서비스.
- 지표 (Metrics) 모니터링: 리소스의 CPU 사용률, 메모리 사용률, 네트워크 트래픽 등의 지표를 모니터링.
- 경보 (Alerts) 설정: 지정 조건이 충족되면 경보를 생성 후 관리자에게 알림.

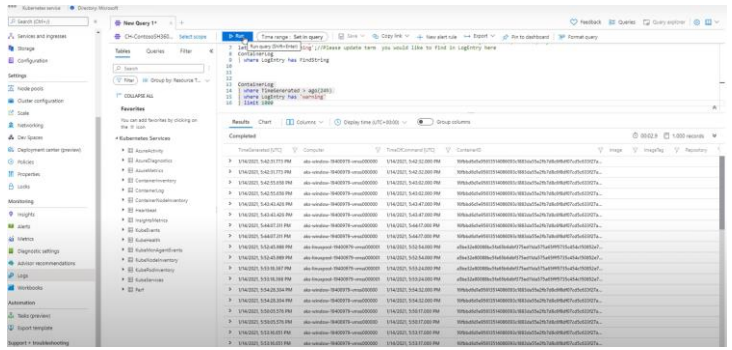
▶ Azure Log Analytics
- 로그 데이터를 수집, 분석 서비스.
- 로그 수집: 가상 머신, 애플리케이션, 보안 이벤트 등의 로그 데이터를 수집.
- 로그 분석: 로그 데이터를 쿼리하여 문제를 해결 및 보안을 강화.



성능 모니터링

▶ 리소스의 성능을 지속적으로 모니터링하여 최적화.

※ 예시
- 가상 머신의 CPU 사용률, 메모리 사용률, 디스크 I/O 등을 모니터링하여 성능 이슈를 식별.
- 애플리케이션의 응답 시간, 처리량 등을 모니터링하여 성능을 개선.



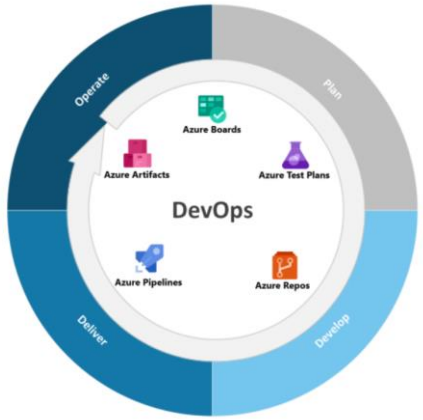
로그 수집 및 분석

▶ 로그 데이터를 수집 및 분석하여 문제를 해결하고 보안 강화.

※ 예시
- 보안 로그를 분석하여 악성 행위를 탐지하고 대응.
- 애플리케이션 로그를 분석하여 오류를 식별하고 수정.

3-5. 자동화 및 DevOps

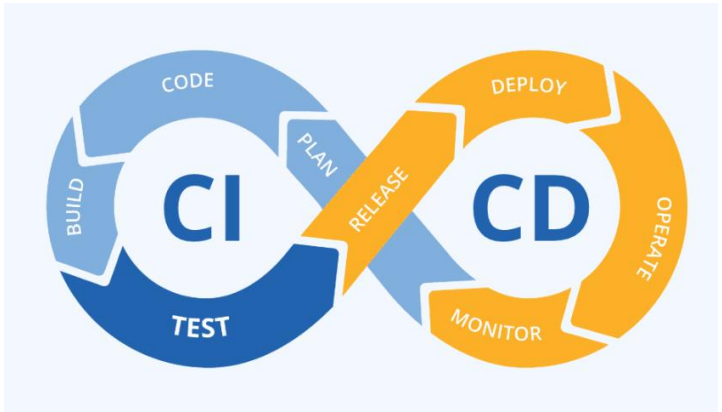
Azure 랜딩존의 자동화 및 DevOps는 개발과 운영을 효율적으로 통합하여 애플리케이션 배포를 자동화하고 일관성을 유지하는 데 도움이 됩니다.



인프라 자동화 도구
(예: Azure DevOps, GitHub Actions)

▶ Azure DevOps
- Azure DevOps 플랫폼으로, 애플리케이션 개발, 테스트, 배포를 자동화.
- CI/CD 파이프라인을 설정하여 코드 변경 사항을 자동으로 빌드하고 배포.
- 인프라 구성도 코드로 관리 가능.

▶ GitHub Actions
- GitHub에서 제공하는 CI/CD 서비스로, GitHub 리포지토리와 통합하여 자동화 작업을 수행.
- GitHub 리포지토리 내 코드 변경 사항을 감지하고 CI/CD 워크플로우를 실행.



지속적인 통합 및 배포 (CI/CD)

▶ 지속적인 통합 (Continuous Integration, CI):
- 코드 변경 사항을 지속적으로 통합하고 빌드하여 품질을 유지.
- 코드 커밋 시 자동으로 빌드 및 테스트를 실행.

▶ 지속적인 배포 (Continuous Deployment, CD):
- 빌드된 애플리케이션을 자동으로 스테이징 및 프로덕션 환경으로 배포.
- 변경 사항을 빠르게 배포하여 시스템을 최신 상태로 유지.

코드로서의 인프라 (IaC) 전략

▶ 인프라를 코드로 관리하여 일관성을 유지하고 변경을 추적.

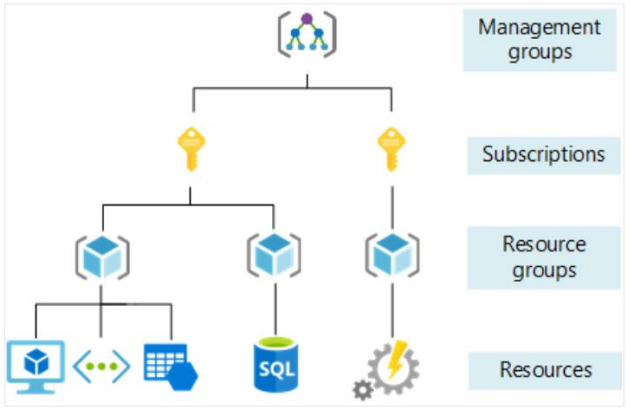
※ 예시
- ARM 템플릿: Azure 리소스를 정의하는 JSON 파일로, 인프라를 코드로 관리.
- Terraform: 다양한 클라우드 환경에서 인프라를 코드로 관리.

3-6. 운영 최적화

Azure 랜딩존의 운영 최적화는 비용 효율성과 리소스 최적화를 통해 클라우드 환경에서 효율적인 운영을 지원합니다.

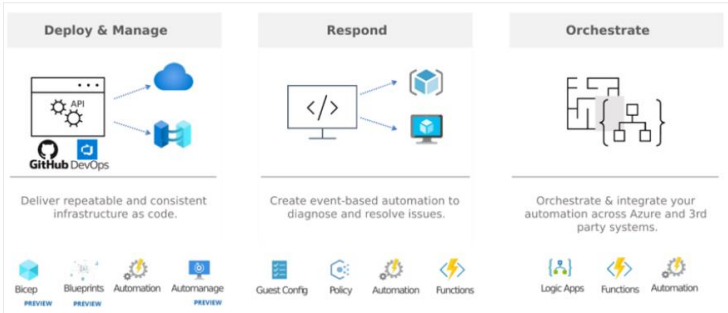
비용 관리 및 최적화

▶ 리소스 사용량을 지속적으로 모니터링하고 비용을 최적화.
- 비용 모니터링: 리소스 사용량, 비용, 예산을 추적하고 분석.
- 비용 예측: 미래 비용을 예측하여 예산을 계획.
- 비용 절감 전략: 예산 초과를 방지하고 비용 절감을 위한 전략 수립.



리소스 효율성 분석

▶ 리소스를 효율적으로 사용
- 리소스 최적화: 리소스 크기 조정, 예약 인스턴스, 스팟 인스턴스 등을 활용하여 리소스를 최적화.
- 자동 확장: 리소스의 수요에 따라 자동으로 확장하도록 설정.
- 비활성 리소스 관리: 사용되지 않는 리소스를 식별하고 정리.

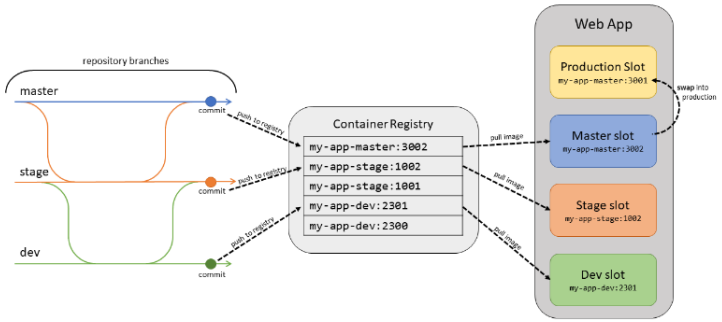


운영 프로세스 개선

▶ 지속적으로 운영 프로세스를 개선하고 효율성을 높임
- 프로세스 자동화: 반복적인 작업을 자동화하여 시간을 절약하고 오류를 감소.
- 지속적인 개선: 운영 프로세스를 지속적으로 검토하고 개선.
- 사용자 피드백 수렴: 사용자 피드백 수렴 후 운영 프로세스를 개선.

3-7. 지원 및 유지 관리

Azure 랜딩존의 지원 및 유지 관리는 리소스의 안정성과 성능을 유지하며, 사용자의 요구 사항을 충족시키기 위한 중요한 활동입니다.

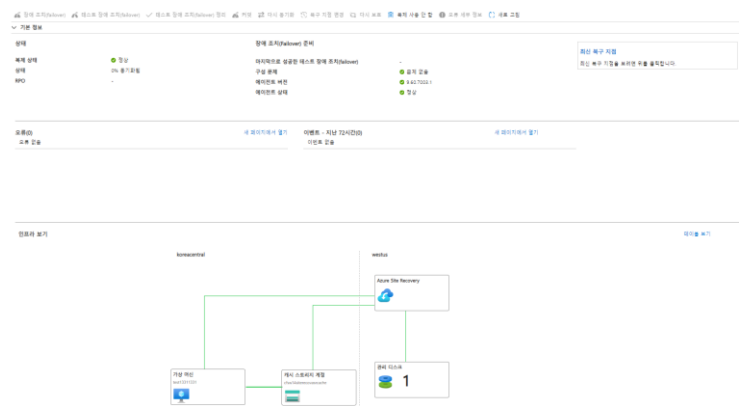


업데이트 및 패치 관리

▶ 시스템 업데이트와 보안 패치를 관리하여 리소스의 안정성과 보안을 유지.

▶ 주요 활동

- 시스템 업데이트: 운영 체제, 미들웨어, 애플리케이션 등을 최신 버전으로 업데이트.
- 보안 패치: 알려진 보안 취약점을 해결하기 위해 패치를 적용.



장애 복구 계획 및 실행

▶ 장애 발생 시 빠른 복구를 위한 계획을 수립하고 실행.

▶ 주요 활동

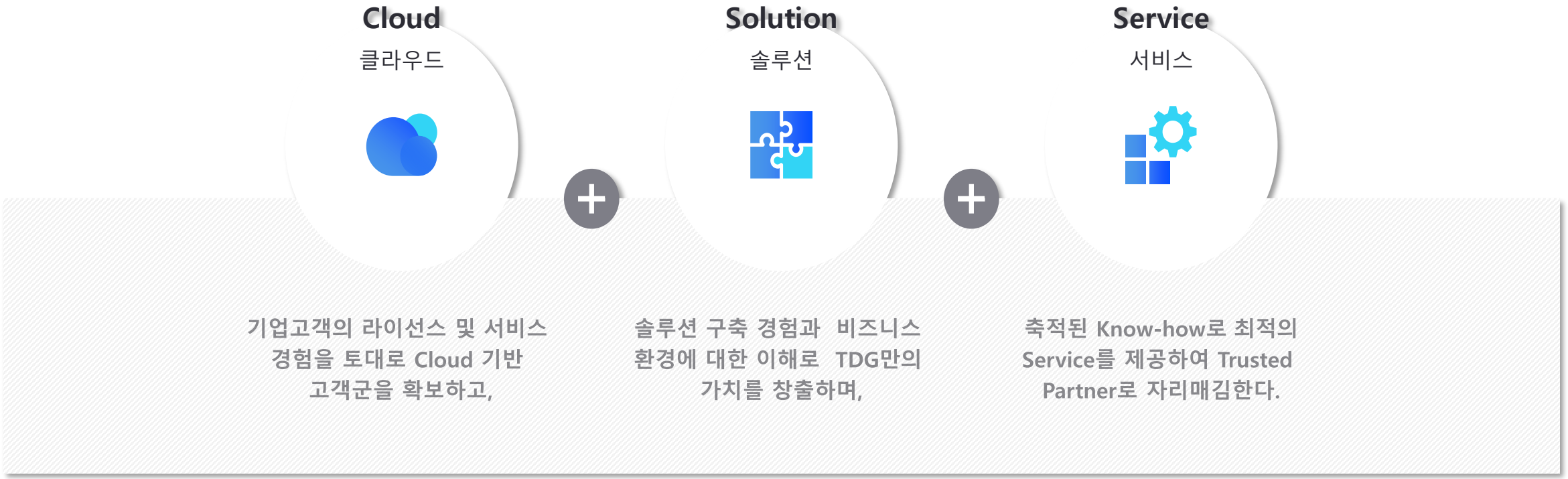
- 복구 계획 작성: 장애 시 어떤 조치를 취해야 하는지 계획을 수립.
- 복구 실행: 계획에 따라 장애를 해결하고 시스템을 정상 상태로 복구.

4-1. Specialty of TDG

- Azure에서 자체적인 관리 도구들을 제공하지만 Azure Landing zone 환경에 대한 구성부터, 설계와 구축 그리고 Azure Cloud에 대한 운영 관리는 많은 지식과 경험을 필요로 합니다.

- TDG는 Azure 인프라 구축의 경험을 바탕으로 최적의 솔루션으로 가이드를 드릴 수 있으며, 운영 서비스에 대해서도 다양한 옵션을 가지고 있어서 고객의 보다 폭 넓은 선택지를 제공해 드립니다.

- 특히 Microsoft 라이선스 및 서비스 전문기업으로 **LSP(Licensing Solution Partner) & MSP(Managed Service Provider) 관련 자격을 모두 보유하고 있으며** Azure에 대한 **프로젝트의 목적과 규모에 따라 프로모션 등을 좀 더 포괄적으로 적용**할 수 있는 제안이 가능합니다.



4-1. Specialty of TDG

TDG는 여러 금융회사의 클라우드 서비스를 관리하는 관리형 서비스 사업자로써 23년 대표평가부터 MSP 부문에 대한 평가에 참여하여 준수한 결과를 받았으며, 기술의 발전에 따라 변경되는 규제에 맞춰 고객을 지원하고 있습니다.

23년 전자금융감독규정 개정

▶ 23년 개정된 전자금융감독규정 신설 규정

<별표 2의4> <신 설>

클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치(제14조의2 관련)

9. 인적보안	필수 사항 (전자금융감독 규정상 규율사항)	- 제8조제1항제2호내지제3호
	추가 사항	- 클라우드서비스 제공자 및 클라우드서비스 운영을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리

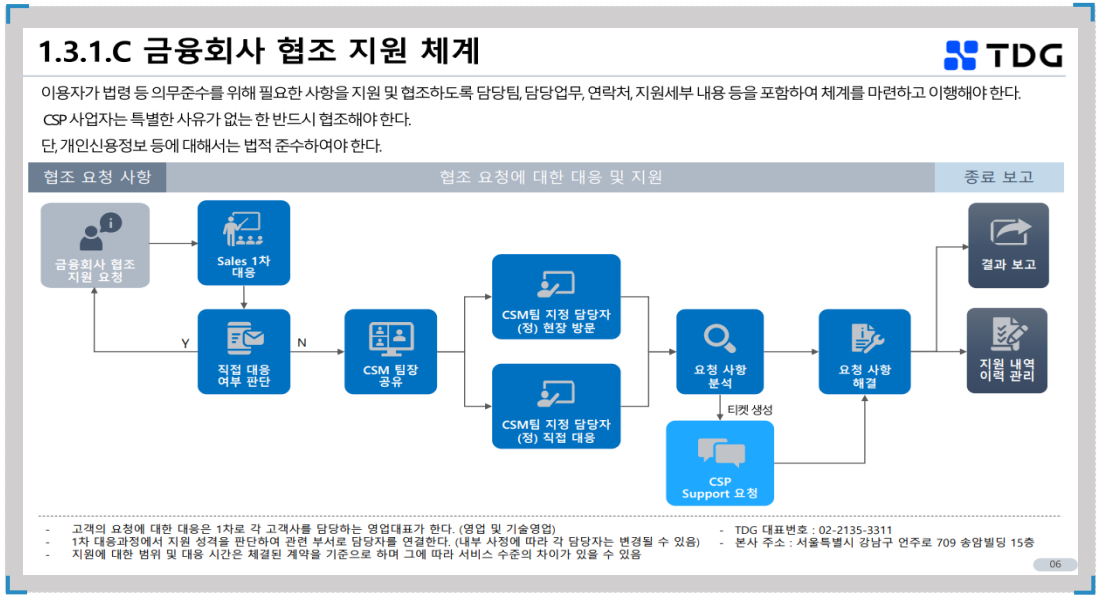
▶ 개정된 금융 클라우드 이용가이드의 인적 보안 항목

9) 인적 보안

나. 추가 사항

클라우드서비스 제공자 및 클라우드 서비스 운영을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리

금융 클라우드 사용을 위한 협조체계 보유



- 23년 개정된 전자금융감독규정에서 관리형 서비스 사업자(MSP)는 CSP 안전성 평가 수행에 대한 필수 대상은 아니지만 TDG는 여러 금융고객사를 지원하고 있기에 23년 대표평가에 참여하였습니다.
- 상기 평가를 통해서 금융보안원이 조직, 인적보안 및 접근 통제에 대한 31개 세부 항목에 대해 감사를 진행하여 검증하였고, 준수한 결과를 받음으로 클라우드 서비스를 관리 및 운용하는데 우수성을 확인할 수 있었습니다.

4-1. Specialty of TDG

TDG에서는 Azure Landing zone 구축 시 4가지 이점(4S) 제공을 목표로 합니다. 클라우드 전환을 원활하게 진행하고, 클라우드 환경을 안전하고 효율적으로 관리하고, 클라우드 혁신을 지속적으로 추구할 수 있는 환경으로 구성합니다.

안전성 — 최적의 Cloud 서비스 구축

Safe

- 사내 업무 환경에 최적화된 Cloud 서비스로 구축 (Azure)
- Cloud 인프라를 활용한 맞춤형 Cloud DR 구성

편리성 — Platform/Software 기반의 아키텍처 수립

Simplification

- Platform 최적 Architecture 컨설팅 지원(옵션)
- 개발도구, 보안, 미들웨어, 자동화 구축 제공 (옵션)

표준화 — 표준 개발/배포/운영 협업 환경 제공

Standardization

- PaaS 기반 일관성, 관리 효율성 제고
- 형상관리, 지속적 통합, 프로비저닝 표준화 환경 지원 방안 제시

신속성 — 신속한 통합 인프라 구축 제공

Speed

- 미들웨어, 서비스 설치/구성 자동화
- 템플릿 기반 개발/검수/운영 인프라 환경 신속 제공

IaaS/PaaS 구성	▪ 보안/기능 요건 NW/서버/스토리지 자원 구성 ▪ 기본 요건 기반 Platform Service 구성
Architecture 설계	▪ 고객사 Platform Architecture 분석 및 요구사항 도출 ▪ 클라우드에 적합한 Platform Service 요건 도출 ▪ 클라우드 Architecture 수립
기대효과 도출	▪ 클라우드 도입으로 인한 기대효과 도출 ▪ 효율성 분석
고객과의 긴밀한 협업	▪ 향후 실제 아키텍처 수립에 있어 적극적인 지원 ▪ 클라우드 구축 경험을 가진 파트너 지원

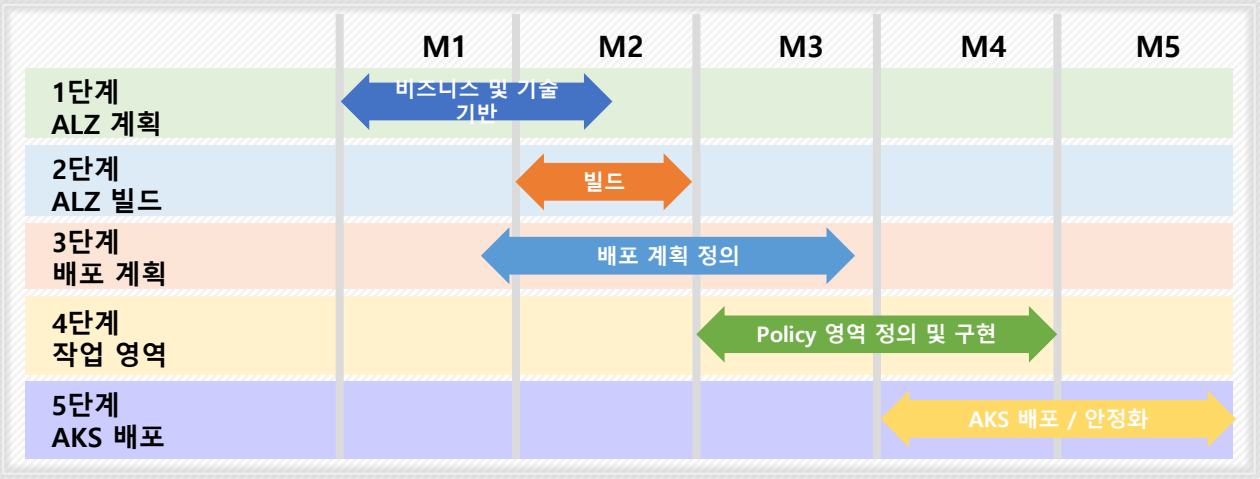
4-2. 일반기업 Azure 구축 사례

Azure 클라우드 내 Azure Landing zone 초기 환경을 구성하였습니다. Azure Policy 적용을 위해, Bulit-in, custom 기반의 정책을 Json 파일로 정의하고 Audit, Deny, DeployIfNotExist 등의 정책의 효과를 적용을 통하여 Azure 리소스의 거버넌스를 강화하고, 조직의 규정 준수 및 보안 기준을 유지하도록 하였습니다.

S기업 Azure Landing zone 구성

단계	기간	작업 내역
1단계 ALZ 계획	6 Week	✓ 운영 모델 선택 ✓ ALZ 구현 옵션 검토 ✓ 규정 준수 요구 사항 식별 ✓ 필요한 사용자 지정 식별
2단계 ALZ 빌드	4 Week	✓ ALZ 목표 및 결과 검토 ✓ ALZ 빌드 계획 정의 ✓ ALZ 파일럿 빌드 ✓ ALZ 파일럿 모니터링
3단계 배포 계획	7 Week	✓ 기존 워크로드 호환성 평가 ✓ 배포 계획 옵션 표시 ✓ 배포 계획을 실행하기 위한 리소스, 타임라인 및 차기 단계 정의
4단계 작업 영역	8 Week	✓ 정책정의서 정의 ✓ 정책정의서 분석 ✓ 정책정의서 구현 ✓ 배포 ✓ 정합성 검증
5단계 AKS 배포	8 Week	✓ 다중 테넌트 확인 ✓ 컨테이너 이미지 관리 및 보안요건 검토 ✓ 네트워크 모델(WAF 등) 및 스토리지 유형 설정 ✓ AKS 배포 → 컨테이너 레지스트리 생성 → Kubernetes 클러스터 생성 ✓ Private Security ML Model AKS 구축 → Azure Entra ID → Network - Landing Zone 구축 → Network - Hub 구축 → Network - Peering → Private link → Azure Private DNS → Azure Firewall → KeyVault → ACR(Azure Container Registry) → AKS Cluster 배포(고사양 GPU Node 사용)

Schedule



Output

No	서비스 구분	적용 대상 서비스	적용 완료 (~1/12)	모니터/통합문서 확인 (1/16)	SDP 테스트 (예정)	SDP 테스트 결과 확인 (예정)	효과
1	SQL 서버		O	O			Deny
2			O	O			Deny
3	SQL DB		O	O			Deny
4			O	O			Deny
5	저장소		O	O			Deny
6			O	O			Deny
7			O	O			DeployIfNotExist
8			O	O			
9			O	O			Deny
10	저장소 Tag 관리		O	O			Deny
11	파일 서비스		O	O			Deny
12	보안로그 그룹관리		O	O			DeployIfNotExist
13			O	O			Deny
14			O	O			DeployIfNotExist
15	Audit & Logging 관리		O	O			DeployIfNotExist
16			O	O			
17	Application Gateway		O	O			Deny
18			O	O			Deny
19	Key Vault		O	O			Deny

4-2. 일반기업 Azure 구축 사례

클라우드를 활용한 인터넷 VDI 구성으로 Azure에서 Citrix 기반으로 1,700 대를 구성하였습니다. One-Click Client 프로그램을 통해 VDI 접속 및 망 연계 클라이언트 프로그램을 설치 하도록 구성하였으며, 바탕화면에 VDI 접속 아이콘을 생성하여 사용자가 손쉽게 인터넷 VDI 사용이 가능하도록 구축하였습니다.

S기업 인터넷 VDI 도입(클라우드를 통한 망 분리 구축사례)

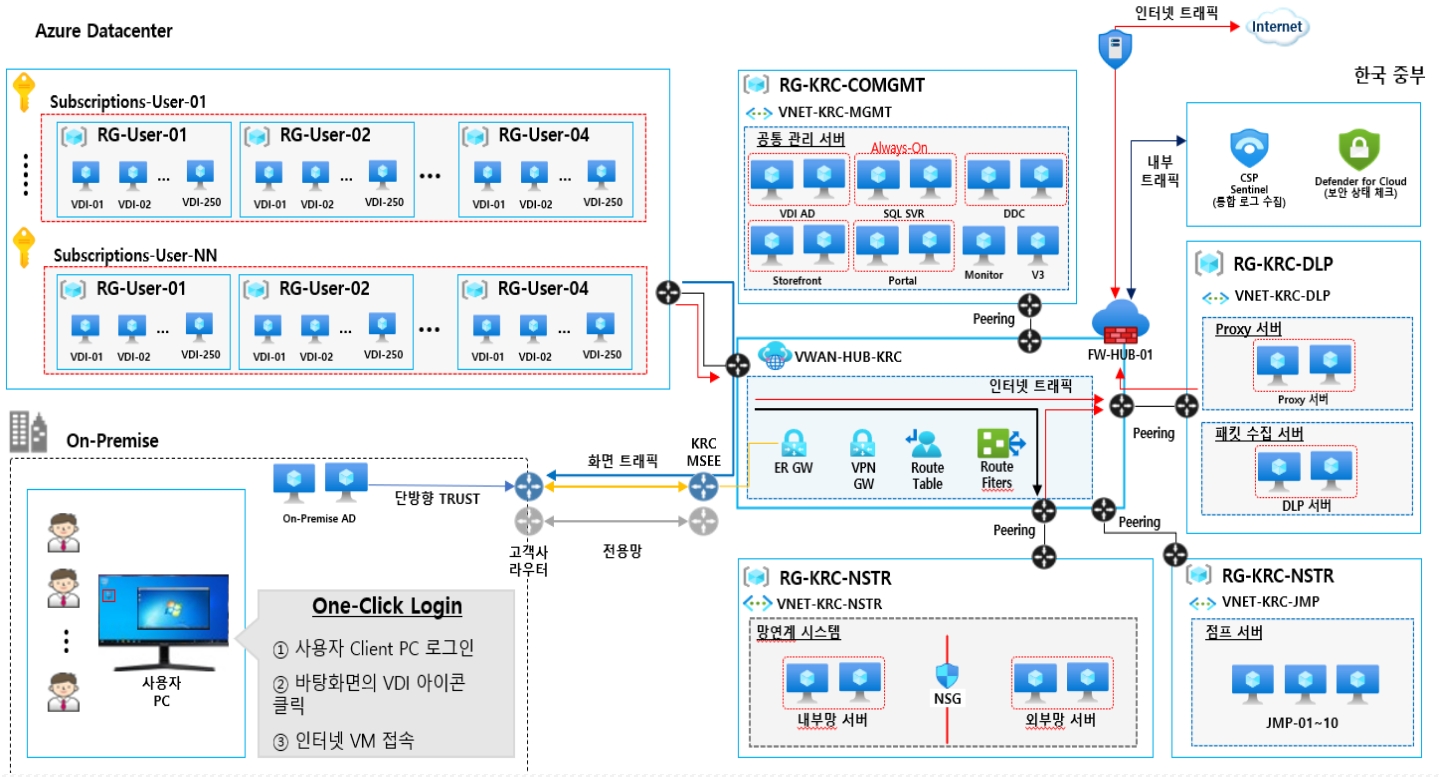
Challenges

- 인터넷을 통한 악성코드로 정보유출 및 시스템 파괴 등을 막기 위해 인터넷망과 업무망을 분리 구성하여 보안이 강화된 업무 환경 필요
- 내부 인터넷 사용의 제약사항으로 인한 외부 사이트 접속의 어려움
- 로그인 및 로그오프의 사용자 다수 클릭으로 인한 사용 불편함

Benefit

- 인터넷 VDI 접속이 가능한 One-Click Login 프로세스 구현
- VDI Auto 전원 컨트롤을 통한 비용 절감과 편의성 향상
- 보안 요건을 충족하여 외부 사이트 접속에 대한 제약사항 해소

시스템 구성 (예)



4-3. 금융권 구축 사례

제 1금융권에서 고객 대상 결제서비스를 제공하는 서비스로 개인정보, 전자상거래 정보가 보관되어 있어 금융 컴플라이언스에 대응하기 위한 망 분리, 재해복구센터 구성, 접근제어 및 DB 암호화 등이 적용되었습니다. 특히 금융의 중요정보 시스템의 경우 고도의 보안 환경이 요구되며, 이를 위해 제안사는 24시간 보안관제를 통해 실시간으로 장애 및 사고에 대한 즉각적인 대응이 가능하도록 운영 서비스를 제공하였습니다.

K사 금융 클라우드(**금융권 BCDR 구축사례**)

Challenges

- 금융권에서 고객대상 서비스를 위해서 대상 서비스를 위한 DR, 데이터 암호화, 접근제어 등의 보안이슈에 대한 대응 그리고 장애대응 및 Full-Time 보안관제가 요구되었습니다.

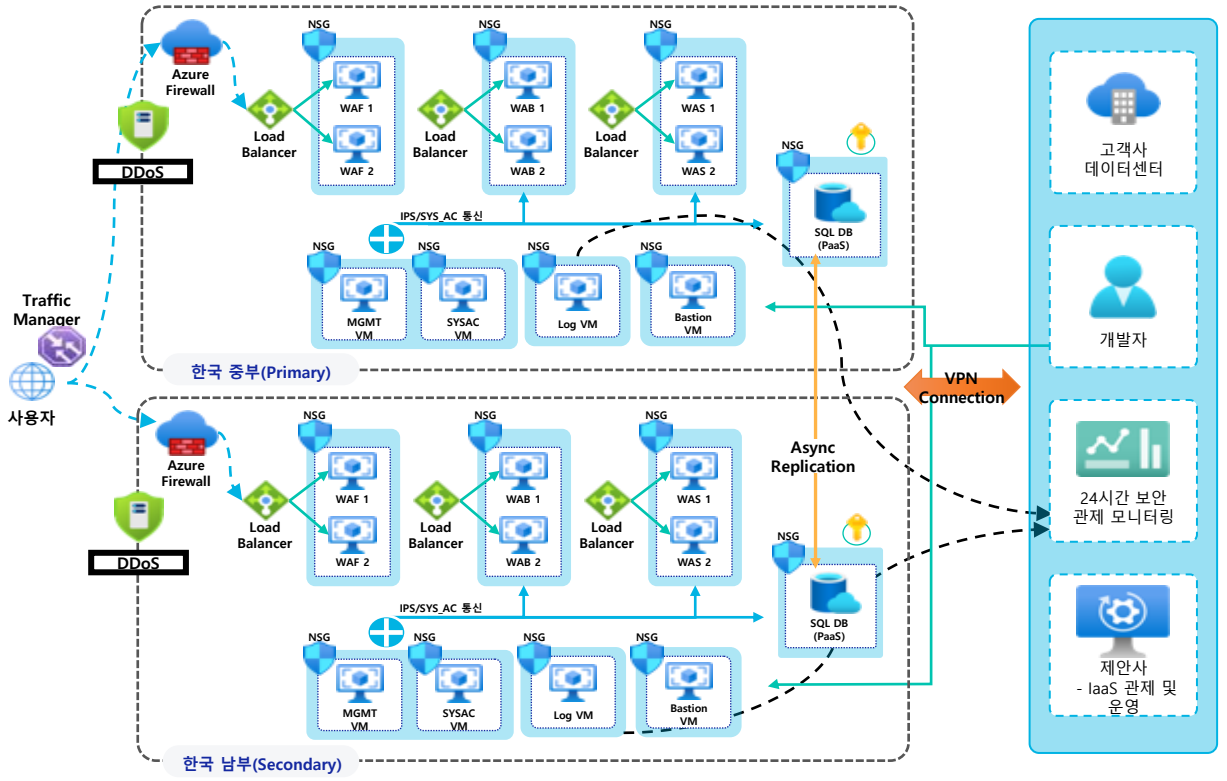
Challenges

- Azure Site Recovery로 **DR복구**, SQL MI 모델 적용, Azure Key Vault를 통한 데이터 암호화를 적용 그리고 제안사의 관제 및 운영 모델이 접목되었습니다.

Key Point

- Azure 기반의 보안, DR, 암호화 등이 포함된 라이브서비스를 실시간으로 구동하며 보안관제를 포함하여 고객에게 제공됩니다.

시스템 구성 (예)



4-3. 금융권 구축 사례

온-프레미스 HPC 연산 노드를 클라우드로 효율적이며 신속하게 확장하기 위해 IaaS 기반으로 연산 노드를 배포하도록 구성합니다.

N사 투자증권 HPC 도입 사례(비 중요 서비스 금융사 구축사례)

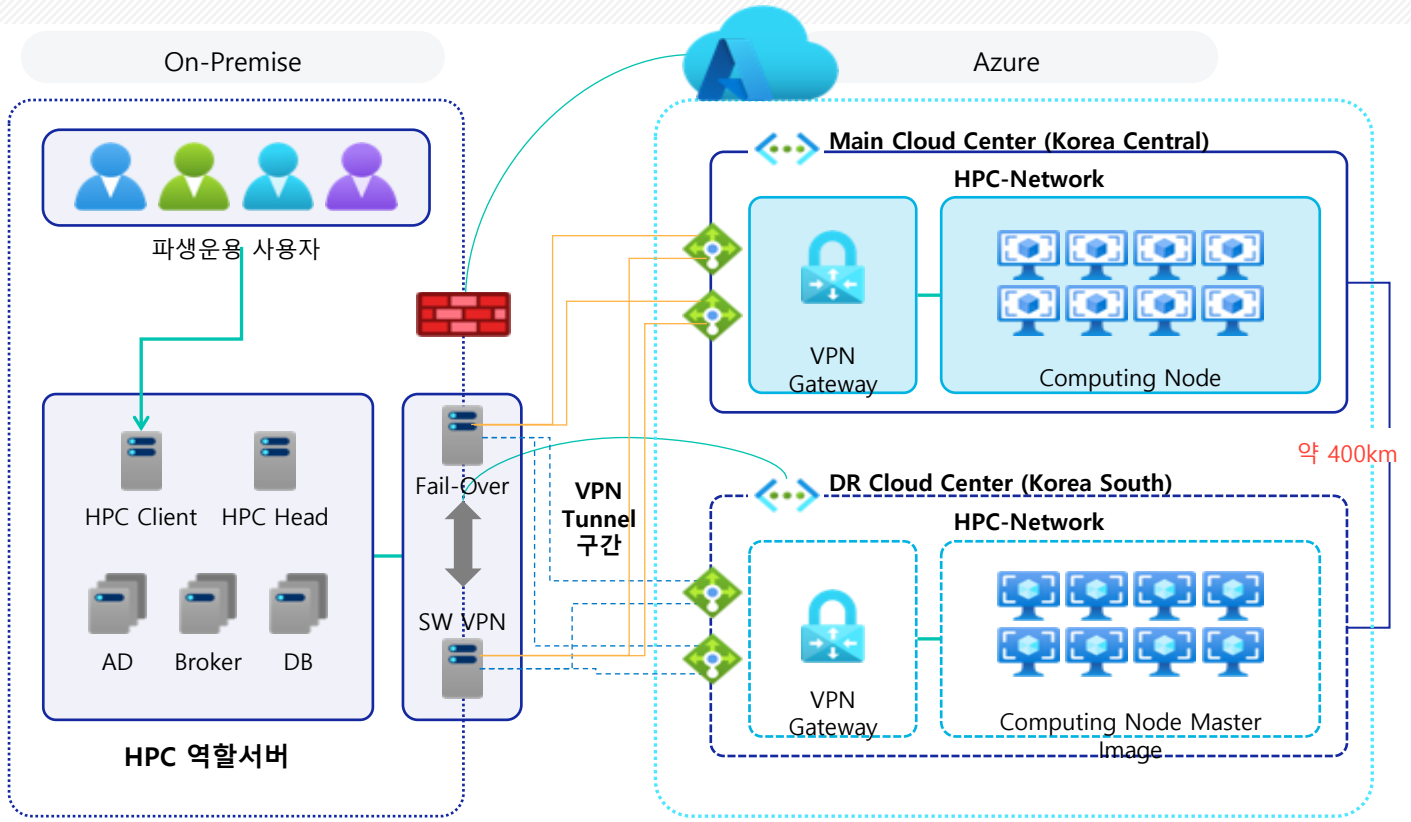
Challenges

- 클라우드 활용을 통해 현업이 불필요한 시스템 구매, 운영, 관리에 신경 쓰지 않고 최신 IT기술을 활용해 자신의 비즈니스에 집중할 수 있는 환경의 구현이 필요

Benefit

- 투자 비용 절감 : 투자 비용을 낮추고 , 운영관리 비용을 절감
- 안정성 확보 : 클라우드 플랫폼 및 HPC 인프라에 대한 단일 벤더의 통합적 기술 지원 체계를 통해 보다 안정적 운영 가능
- 확장성 및 민첩성 향상 : 필요 시 자원을 구매하지 않아도 빠르게 원하는 컴퓨팅 자원을 확장하여 사용 가능
- 운영관리 효율화 : 인프라 및 하드웨어 관리가 필요 없기 때문에 관리 편의성의 향상됨
- 고객사 정보보호팀의 보안검증까지 완료

시스템 구성 (예)



Contact

Tel 02-2135-3311
Fax 02-2135-3316
E-mail mkt@tdgl.co.kr

Address

서울특별시 강남구 언주로 709 송암빌딩 15층

Trust Digital Go-ahead

TDG