2022년 전망 금융IT 버추얼 컨퍼런스

“We make the best financial solutions.”

금융IT 시스템 Public Cloud 운영

2021. 12. 09
dongsik.lee@bankwareglobal.com

bankware global

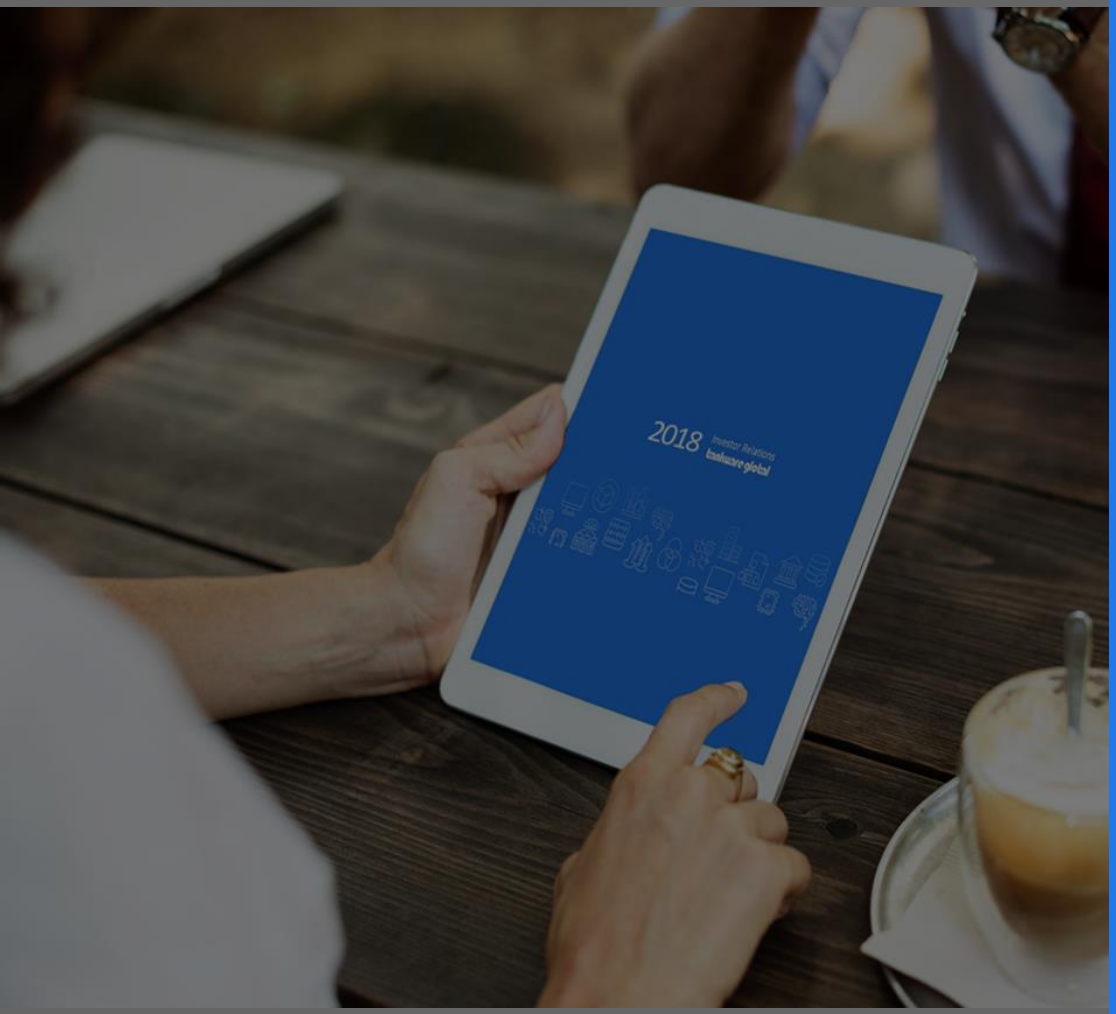


TABLE OF CONTENTS

금융IT 시스템 Public Cloud 운영

Public Cloud dedicated SaaS operation

- **Mobile-based ADPS & Microloan System**

ADPS 프로젝트 시작

- Microloan 프로젝트 시작(3월)
- 코어 뱅킹 Teller 업무 시작 (5월)
- 대출 Teller 업무 시작 (7월)

ADPS & MFS Teller 오픈

- Partner Web/App 오픈
- Customer Web/App 오픈

고객 서비스 오픈

- Network 방화벽 도입
- RDS 디스크 증설(1T-> 2T)
- DR 구성, 고객 Smoke 테스트
- Daily 보고서 자동화
- VPN Vocalink 연동
- 대출 Data 이관
- Web/App VAPT

2020년 서비스 운영

- RDS 디스크 증설 (2T-> 3T)
- SSL 인증서 갱신
- DR Scaling 구성 및 고객 Certification 인증
- 인프라 모니터링 자동화
- 보안/감사 로그 SIEM
- 엘도라도 (신규 추가 서비스) 프로젝트 시작
- Anti-DDoS 솔루션 PoC
- Web/App VAPT

2021년 서비스 운영

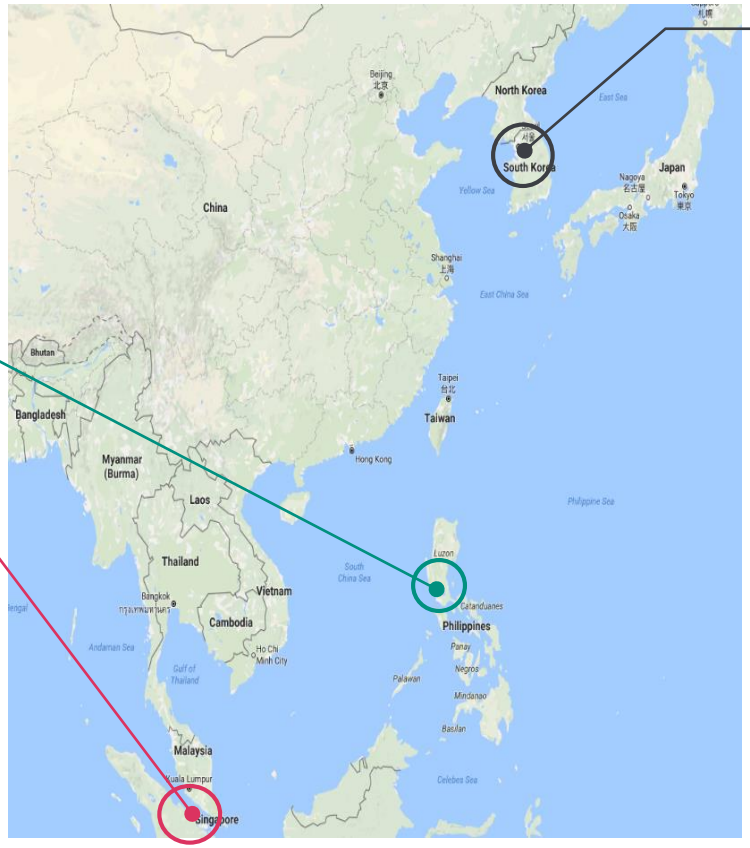
2018.03 | 2019.03-07 | 2019.12 | 2020 | 2021

Overview

금융IT 시스템 Public Cloud 운영

Business (Manila, Philippines)

Ali-Cloud Center (Singapore)



Operation & Maintenance (BwG Seoul)

- Public Cloud (Singapore Center)
  SaaS Operation Service (Seoul)
- Deposit, Microfinance, Payment, Agent, Top Up

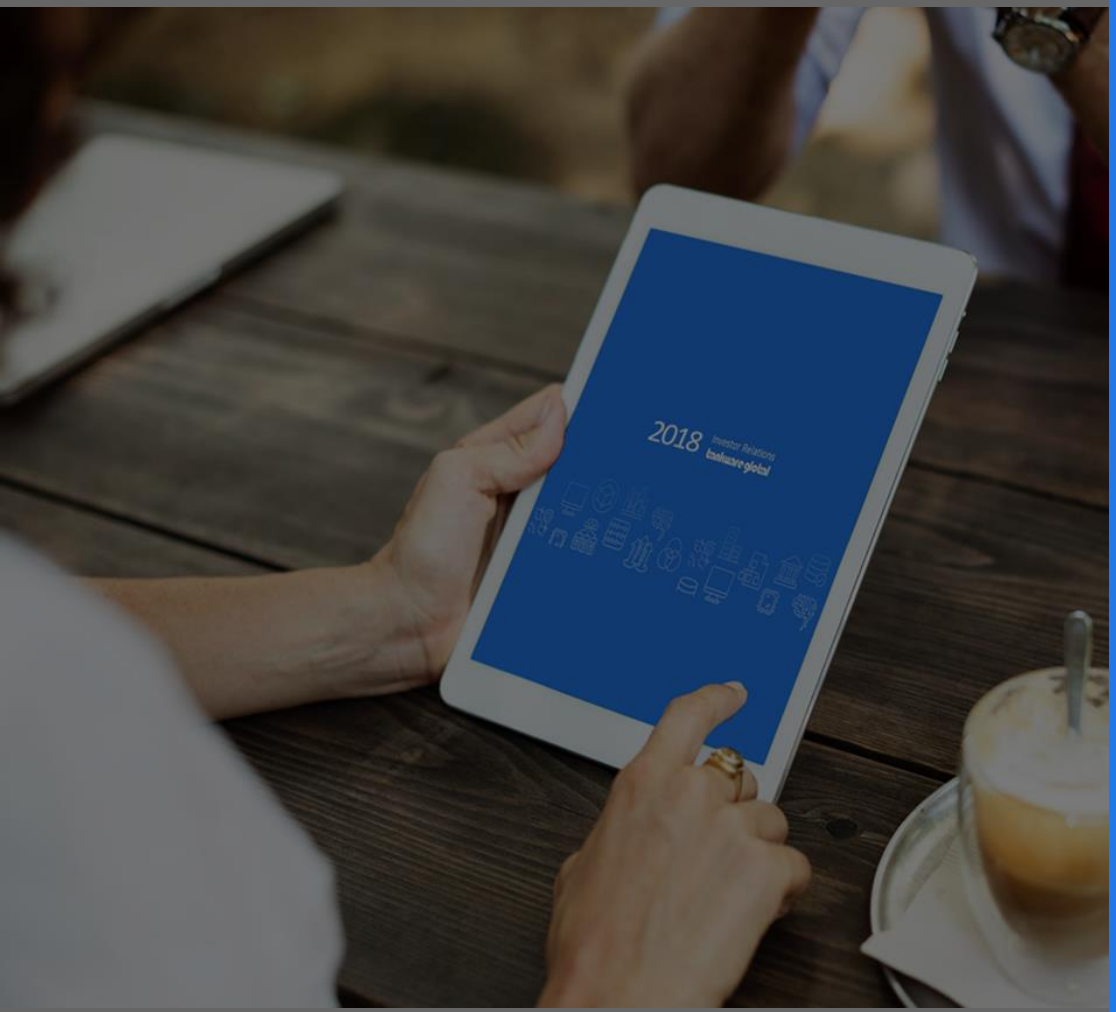


TABLE OF CONTENTS

Overview

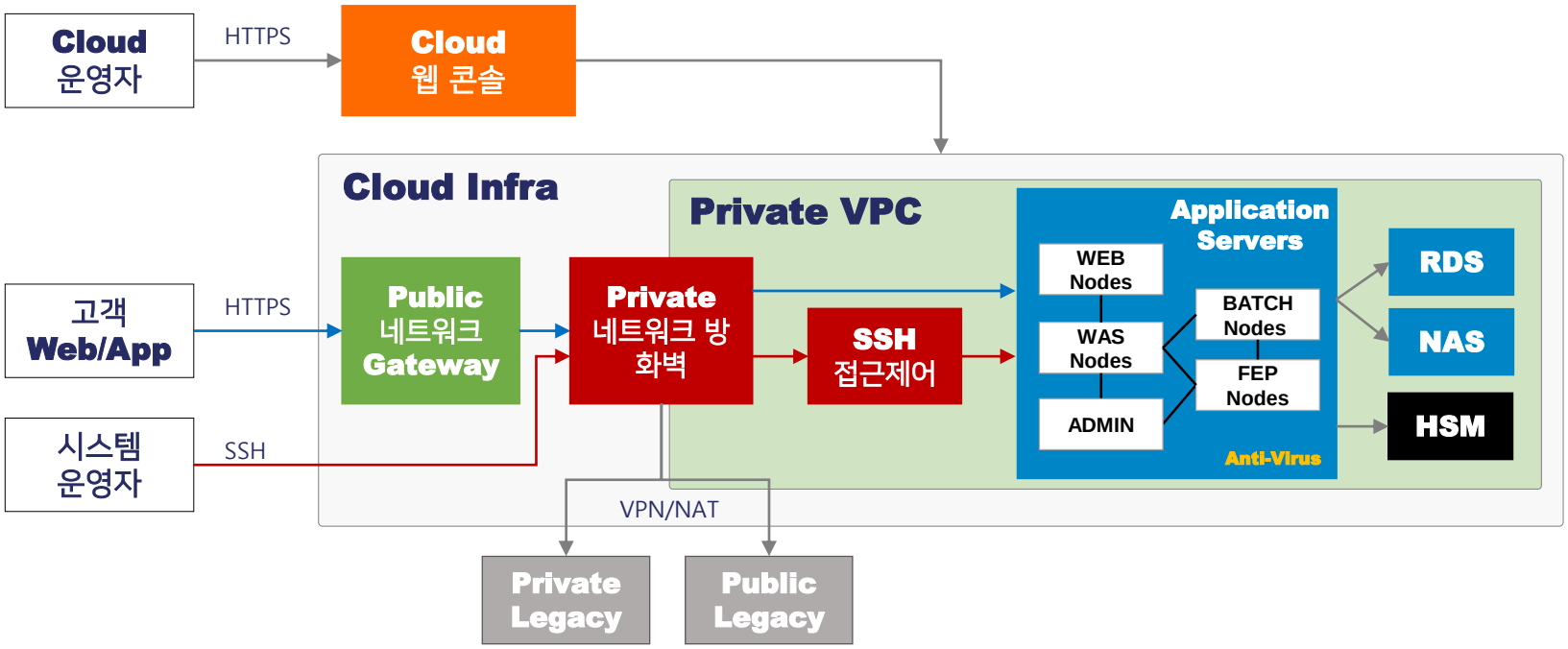
금융IT 시스템 Public Cloud 운영

Public Cloud 운영 시 7가지 고려사항

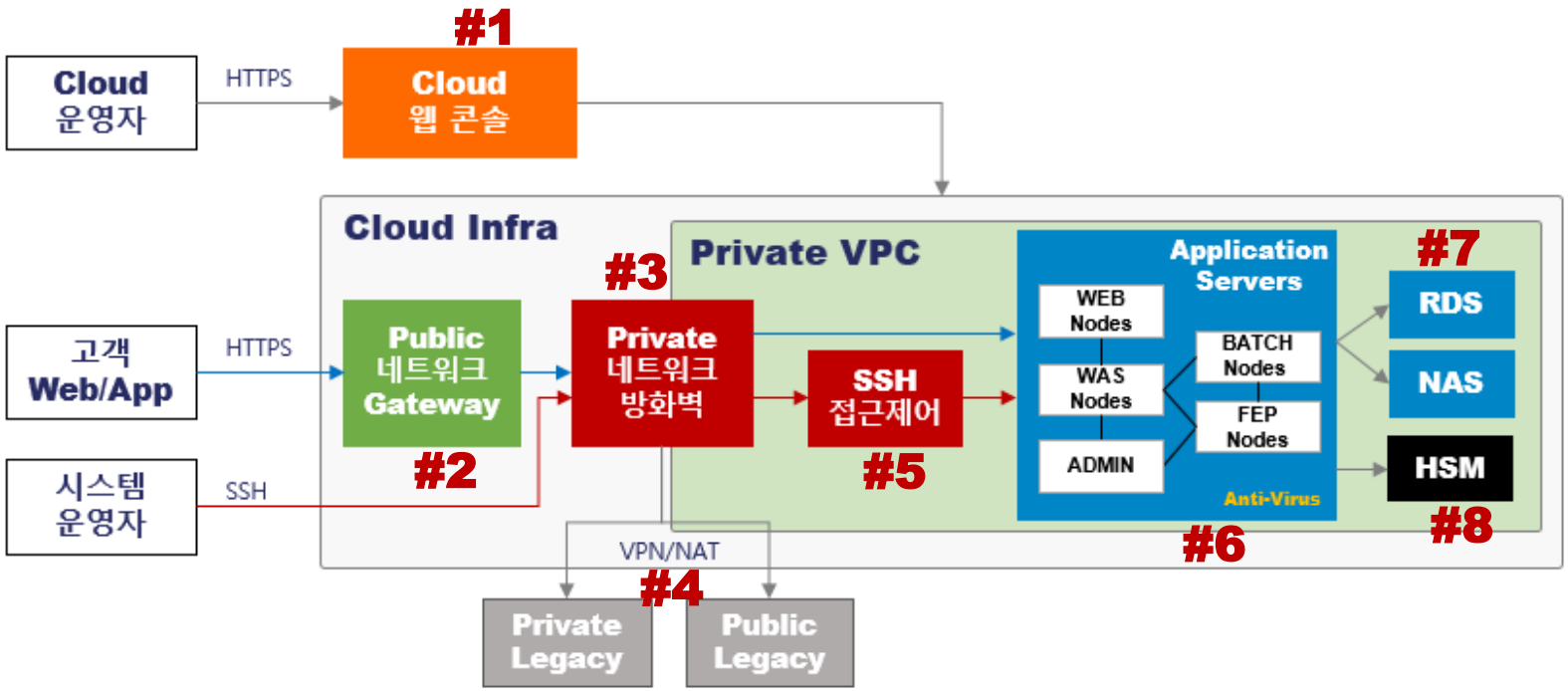
Key Considerations

1. 보안 및 신뢰

Microfinance Savings Banking on Public Cloud



1. 보안 및 신뢰



#1. MFA (Two Factor 인증)

#2. HTTPS & Anti-DDoS

#3. Private 네트워크 방화벽

#4. Legacy VPN/NAT 연결

#5. SSH 시스템 접근 통제

#6. Anti-Virus (서버 OS)

#7. TDE (데이터 무결성 검증)

#8. HSM (하드웨어 보안 모듈)

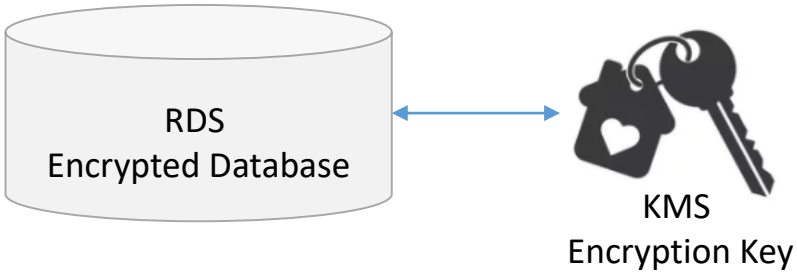
1. 보안 및 신뢰

Third Party 솔루션 도입 배경

No.	보안 제품	Public Cloud 제공 제품	Third Party 제품	비고
1	MFA (Two Factor 인증)	▪ 클라우드 제공 보안 기능	▪ N/A	Cloud
2	HTTPS & Anti-DDoS	▪ CDN, WAF, Anti-DDoS ▪ 각 제품별 개별 관리 화면에서 설정 및 관리	▪ 시장 점유율 34.55%의 가장 대중적인 서비스 ▪ 통합 Dashboard에서 CDN, WAF, Anti-DDoS 기능 설정 및 관리 가능 ▪ 고객의 선호도가 높음 ▪ 기능면에서 Public Cloud 제품 군과 차이가 거의 없음	PoC 진행중
3	Private 네트워크 방화벽	▪ WAF에서 HTTP(s) Inbound 트레픽 컨트롤 ▪ 서버 Instance간에는 Security Group을 이용 ▪ VPC간에는 VPN, Routing Table 사용 ▪ Subnet 간에는 별도 Network Access Control 사용 ▪ HTTPs(WAF), VPN, NAT 제품별 개별 기능으로 사용 (통합 Dashboard 제공 안함)	▪ External (public) /Internal (Private) 의 IPv4 및 Port 정책 기반의 네트워크 트래픽 중앙집중식 제어 가능 ▪ 고객의 대외 인터페이스 제품과 동일한 제품 군으로 고객의 선호도가 높음 ▪ 클라우드 Default 네트워크 설정에 의존적 (가상 이미지기반) ▪ 국내 최초의 Third Party Enterprise NGFW 클라우드 적용	Third Party
4	Legacy VPN/NAT 연결	▪ VPN, NAT 실시간 패킷 Trace 확인 어려움 ▪ 클라우드 VPC간의 내부 네트워크 연결 용으로 사용	▪ VPN, NAT 정책에 대해서 실시간 패킷 Logging 가능 ▪ #3의 네트워크 방화벽에 제공하는 VPN/NAT로 대외 연계	Third Party
5	SSH 시스템 접근 통제	▪ 클라우드에서 제공하는 SSH Key pair 생성 ▪ 클라우드 서버 엑세스를 위해 PEM 파일을 통해 연결	▪ 고객의 감사(Audit) 요건인 시스템에 대한 접근 제한 및 이력 레포트 가능 ▪ 사용자의 권한 별 개발/테스트/운영 시스템의 접근 통제 ▪ OTP 를 적용 불법적인 접속을 안정적으로 차단 ▪ 사용자 역할과 명령어 템플릿 그룹을 생성하고 사용자가 허용되지 않은 su, sudo 권한으로 rm, mv와 같은 명령어 실행에 대해 확인/기록/차단과 같은 권한 옵션 적용	Third Party
6	Anti-Virus (서버 OS)	▪ 클라우드의 Security monitoring 서비스 구매 시 기본적인 Vulnerabilities 레벨의 검사 기능 제공	▪ 각 서버 Instance에 Anti-virus 설치 및 중앙 통제 서버를 통해서 최신 바이러스 Definition 업데이트 및 정책기반 바이러스 Scanning	Third Party
7	TDE (데이터 무결성 검증)	▪ 클라우드 RDS제품의 제공 기능 ▪ KMS를 이용해서 마스터키 암호화 해서 저장	▪ N/A (별도로 고려하지 않음)	Cloud
8	HSM (하드웨어 보안 모듈)	▪ 클라우드 서비스에서 사용되는 암호화키를 생성 저장하는 기능 제공 ▪ **ATM 거래를 위해서 필요한 Card PIN 검증 기능이 없음**	▪ ATM Card 거래를 위한 3가지 Compliance 요건 충족 - PCI DSS, PCI PIN, PCI PTS HSM 규정 및 감사 요건	Third Party

#7. TDE (데이터 무결성 검증)

- **RDS** 데이터를 암호화 하여 디스크에 저장하기 위해 **TDE**를 설정
- 데이터 베이스 이미지의 도난 및 데이터의 유출 시 데이터를 보호
- **KMS** 를 이용해서 **Master key**를 저장하고 데이터 무결성 검증에 사용

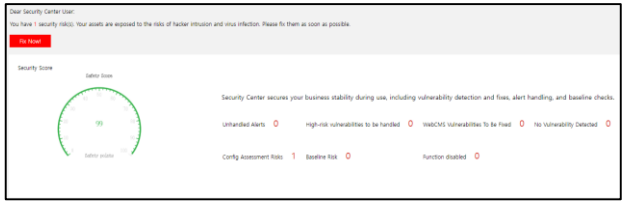


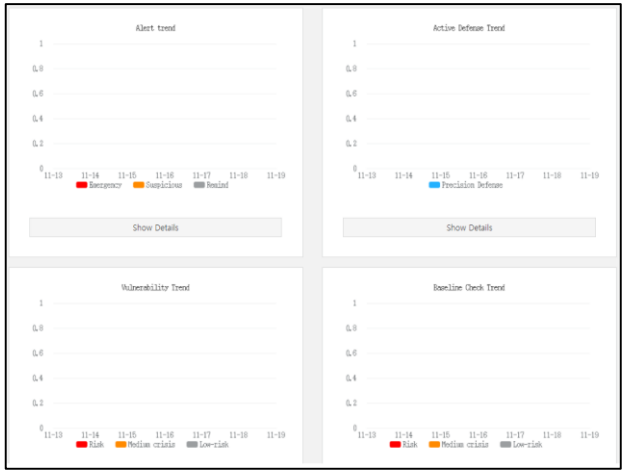
Key Considerations

1. 보안 및 신뢰

Daily 클라우드 보안 점검 보고서

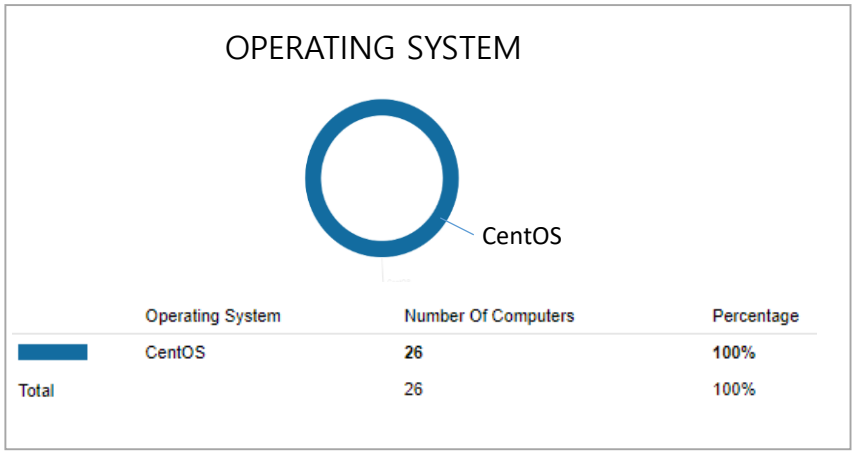
- 클라우드에서 현재 운영중인 서버 인프라에 대한 보안 상태를 고객에게 정기적으로 보고함으로서 인프라에 대한 신뢰 제공





Weekly Anti-Virus 상태 보고서

- 서버 **Instance**들에 설치되어있는 **Anti-Virus** 상태 모니터링 보고서



	Operating System	Number Of Computers	Percentage
	CentOS	26	100%
Total		26	100%

2. 위험관리 및 규정준수

01 고객이 요구하는 위험관리 규정을 준수

통합 로그 관리

- 고객 감사요건으로 서버 인스턴스의 Secure 로그 수집
- 클라우드 콘솔에서의 리소스 정보 변경 이력에 대한 Audit 로그 수집
- 수집된 로그를 고객의 On-premise 와 VPN 연결을 통해 실시간 전송

Operation Room 통제

- 인적 보안/물리 보안을 위해서 전자카드를 이용한 출입통제
- 운영실 접근 (출입문) 모니터링 CCTV 설치
- 비인가자에 대한 외부인 출입관리 대장 작성

24/7 운영 모니터링

- IDC 24시간 관제 서비스 업체 통해 운영 상황 모니터링
  - 클라우드 인프라 장애 여부
  - HTTPS 서비스 이상 여부
  - ATM 거래 정상 여부 확인

2. 위험관리 및 규정준수

02 BCP 따른 재해 복구 훈련

재해 복구 훈련 목적

- 자연재해, 해킹, 테러 등 위협 증가
- 시스템 중단으로 인한 비용 손실 및 고객 서비스 유지
- DR 구성에 대한 은행 및 금융 당국의 규제 대응

재해 복구 훈련 이력

- 매년 1회 재해 복구 훈련 수행
- 2020년 실제 온라인 Transaction 거래는 수행하지 않음 (조회성 테스트 업무만 수행)
- DR 인프라에 대한 고객의 Certification 요구
- **2021년 DR 시스템에서 1일(24시간) 전체 거래 성공** (온라인, 배치, 센터 컷, 외부 I/F 거래)

Cloud에서 DR 구성의 장점

- 서로 다른 두 Zone에서 Active / Standby 모드일지라도 물리적으로 PROD와 동일한 스펙의 인프라 구성이 필요 없음
- 클라우드의 장점인 Scaling을 적용하여 즉시 필요한 인프라 확장

*** BCP - Business Contingency Plan**

3. 파트너 관리

Cloud 공급자

- **"가장 중요한 파트너이지만, 가장 먼 파트너 이기도 합니다."**
- 클라우드에서는 모든 리소스에 대한 사용 책임은 사용자에게 있음을 명심 해야함
- 별도 유지보수 파트너의 MA를 받지 않는다면 전적으로 알아서 인프라를 구성하고 운영해야 함

  (인프라 구성 초기 클라우드 기술지원 파트너 또는 클라우드 공급자와 별도의 Support 모델에 대한 계약을 고려할 필요가 있음)

Third Party 솔루션 MA (기술지원)

- 인프라 구성 시 Third Party 솔루션들을 사용할 경우 변경요건이나 장애 시 즉각적인 기술지원이 가능함
  - **한국에서 최초로 클라우드 인프라에 네트워크 방화벽 설치 및 운영**

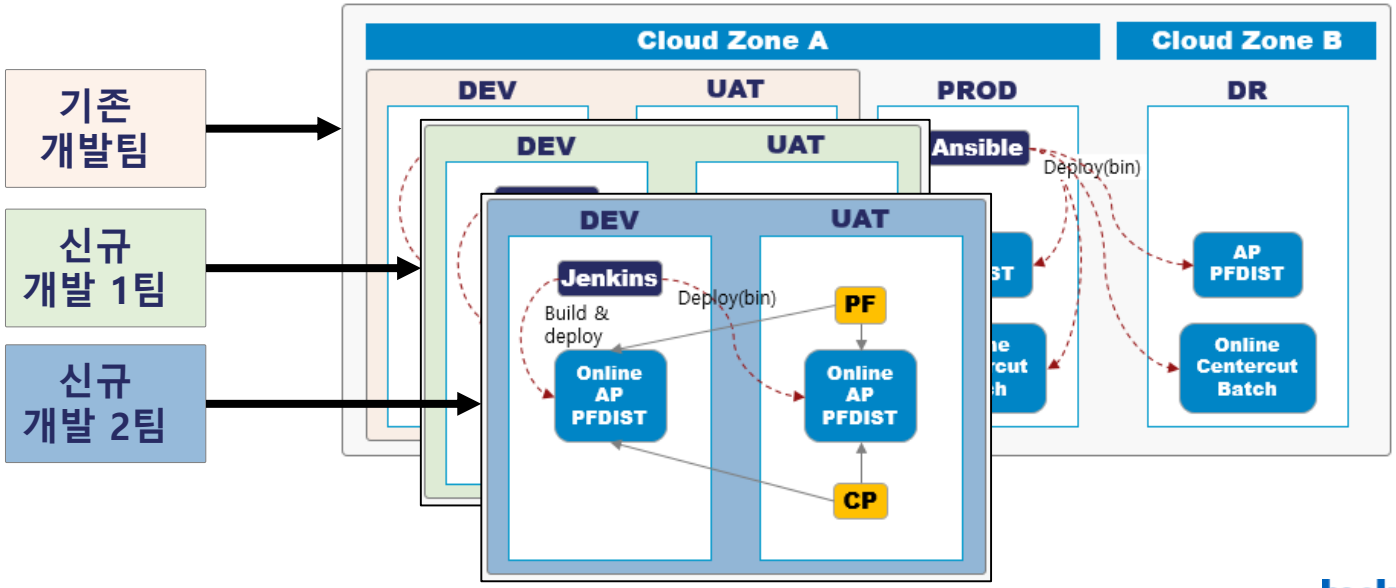
4. 고객 경험

DevOps 환경과 Agile 개발 방법 적용

- DevOps 기반 Agile 개발 환경으로 신규 서비스의 **신속한 배포**
- 빠른 신규 상품의 개발 및 출시로 **Speed to Market** 할 수 있는 환경을 제공

Cloud 인프라의 장점

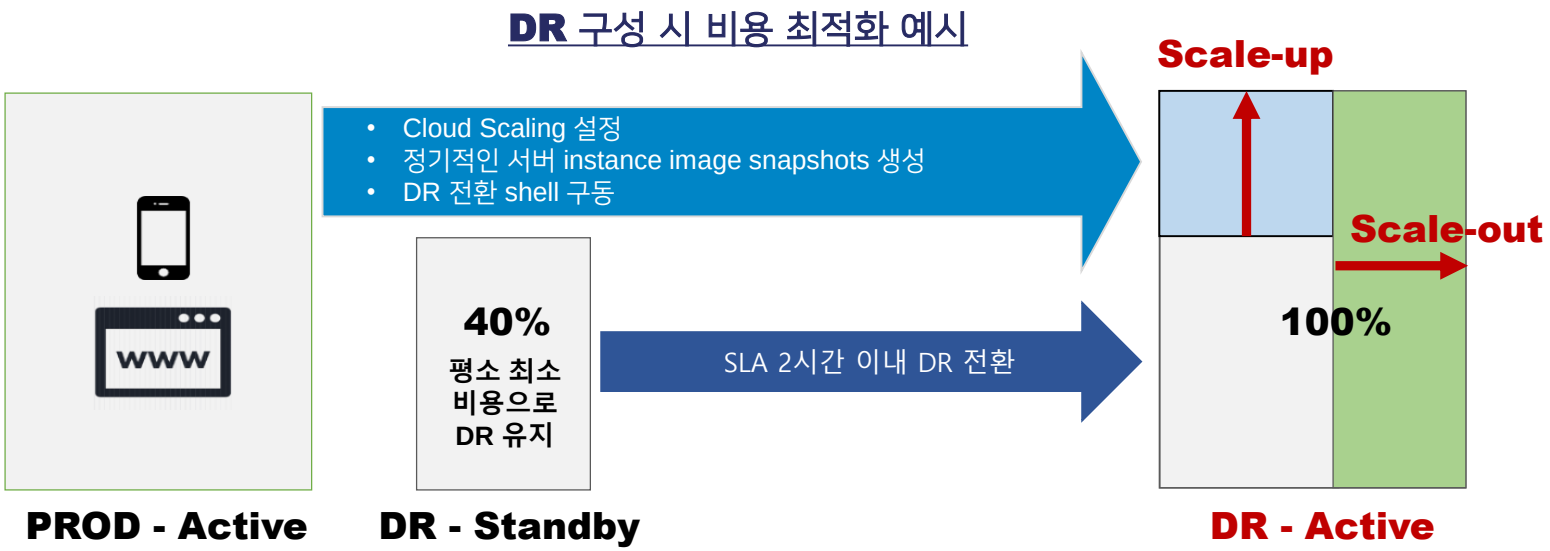
- 기존 운영되는 DevOps 환경에 영향을 주지않고 신규서비스를 추가 개발해야 하는 경우 새로운 Agile팀을 위해서 **새로운 리소스 (DEV, UAT, RDS 포함)를 복제해서 개발환경을 제공**
- 개발이 완료되면 언제든지 해당 리소스를 삭제 할 수 있기때문에 **비용측면에서도 효율적**



5. 비용관리 유연성

CapEx vs OpEx

- 초기 설비 투자 비용 불필요
- Pay As You Go (PAYG) 방식으로 **사용한 만큼 비용을 지불**
- 인프라 환경에 대한 최적화와 사용하는 **리소스에 변경 요건(Scale-up, Scale-out) 반영이 쉽고 빠름**
- 리소스에 대해서 Multi Zone/Region 간 HA 기능 제공
- 불필요한 장비의 관리, 기존 장비의 폐기 문제가 발생하지 않음



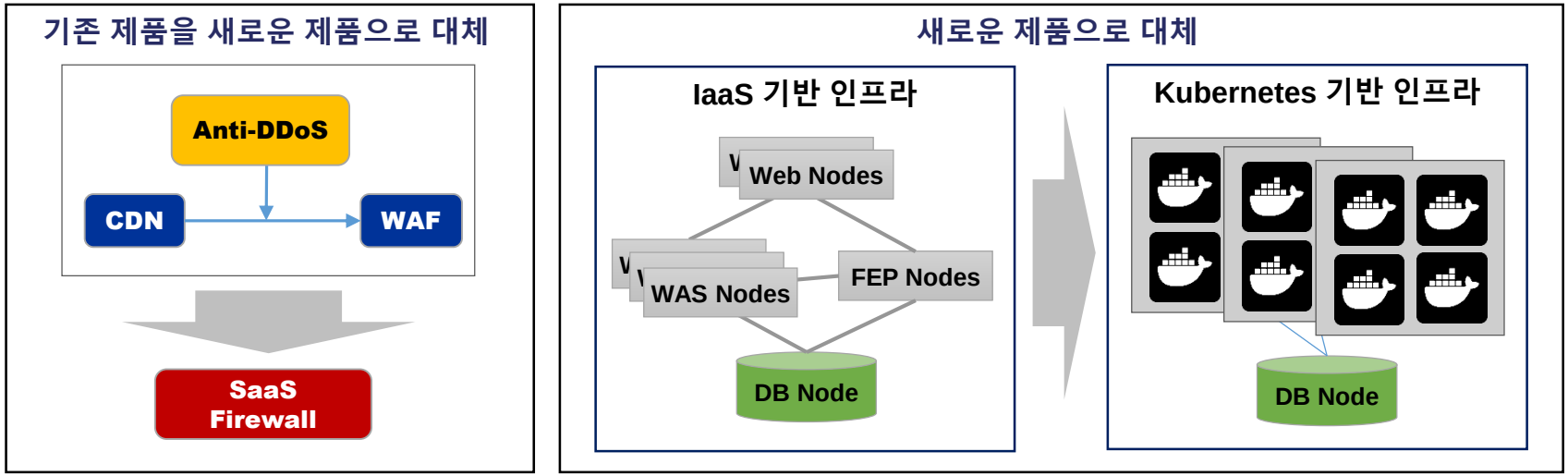
6. 혁신을 위한 민첩성

새로운 기술이나 서비스에 대한 빠른 적용

- DDoS 공격 방어(대규모 공격에 대한 대응)에 더 효율적인 솔루션을 검토하면서 기존 클라우드에서 제공하는 몇가지 서비스를 조합하는 패턴보다 **글로벌 시장점유율이 높은 All-in-One의 SaaS 서비스로 대체하는 방안** 검토

기존 인프라를 최신의 인프라로 전환

- IaaS 기반 Scale-up/Scale-out 형 인프라 구성을 **컨테이너 방식의 Kubernetes 구동형 인프라로 전환**이 용이함

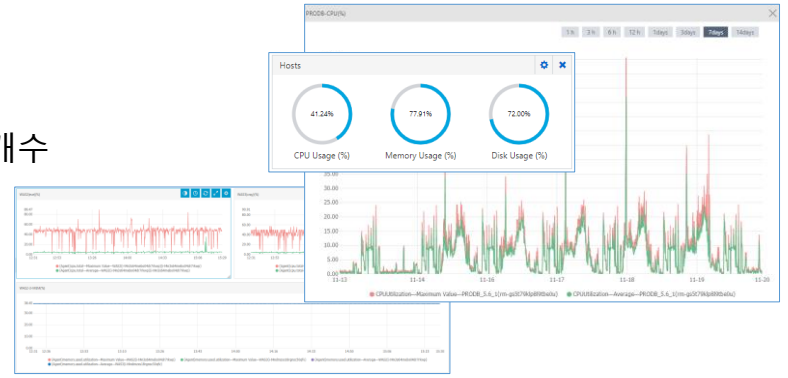


7. 운영 효율성

01 클라우드 리소스에 대한 효율적인 모니터링 도구 제공

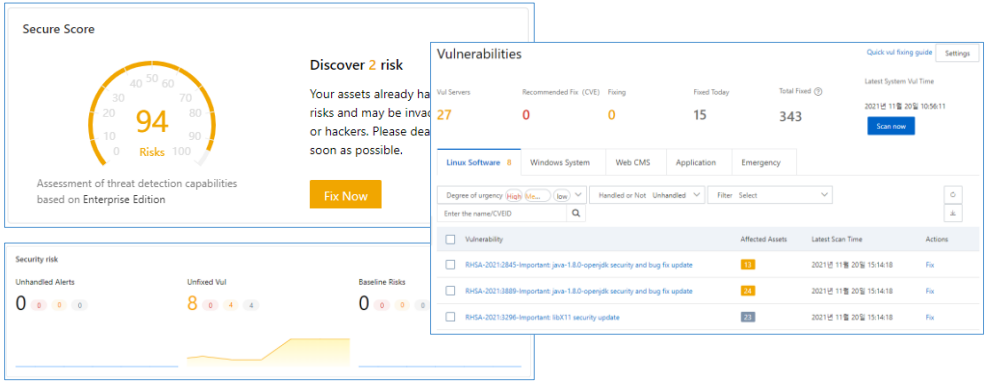
Cloud Monitor

- Custom Dashboard 기능으로 필요한 리소스 모니터링
- 실시간 RDS CPU/Memory/Disk 사용률 및 Active Session 개수
- 실시간 Online WAS 서버들에 대한 Utility



Security Monitor

- 클라우드 보안 스코어 관리
- 예방조치 자동 탐지 및 Alert (Precaution)
  - Vulnerabilities 취약점 점검
  - 리소스들의 Baseline 점검
- 위협 탐지 (Threat Detection)
  - 다양한 방어(Defense) 기능 제공



7. 운영 효율성

02 운영 모니터링 자동화로 시간 및 인력 효율성 최적화

Daily 모니터링 자동화

- Daily 인프라 Report
- ADPS & Microloans Daily Report

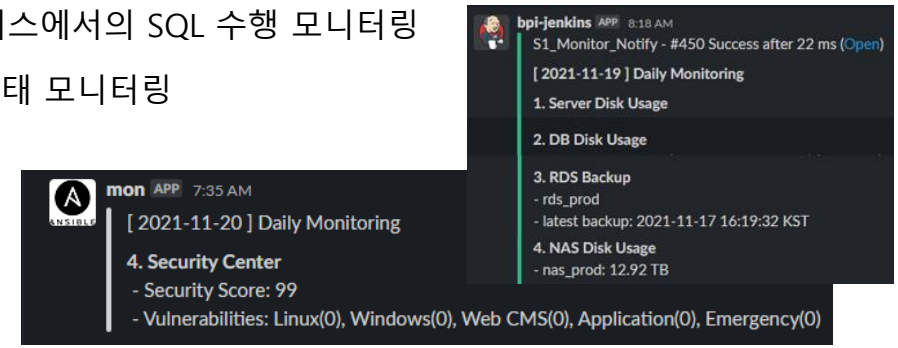
- **Batch**
- **Crontab Job**

+

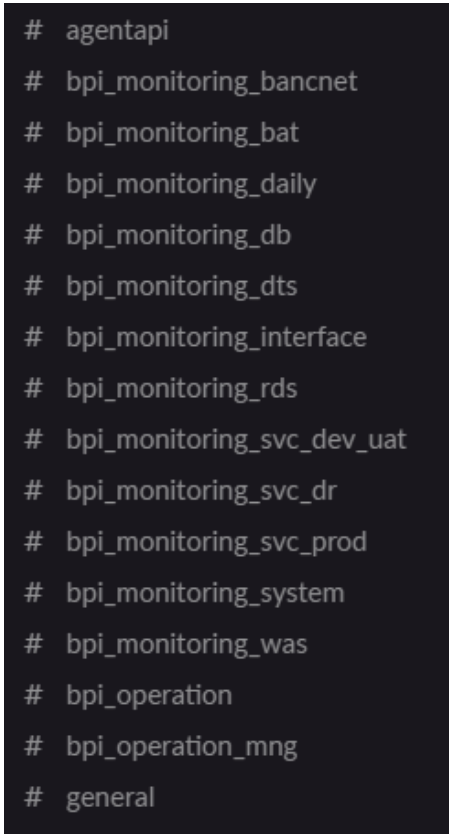
ALERT

서비스 장애에 대한 실시간 모니터링

- Threshold 기반 상시(초~분당) 모니터링
- 대외 서비스(ATM, NAT) 에러 또는 장애
- 스케줄러 작업 및 배치 장애
- 배치 실행 오류, 서비스에서의 SQL 수행 모니터링
- 네트워크 및 서버 상태 모니터링



Daily Report



Real-Time Report

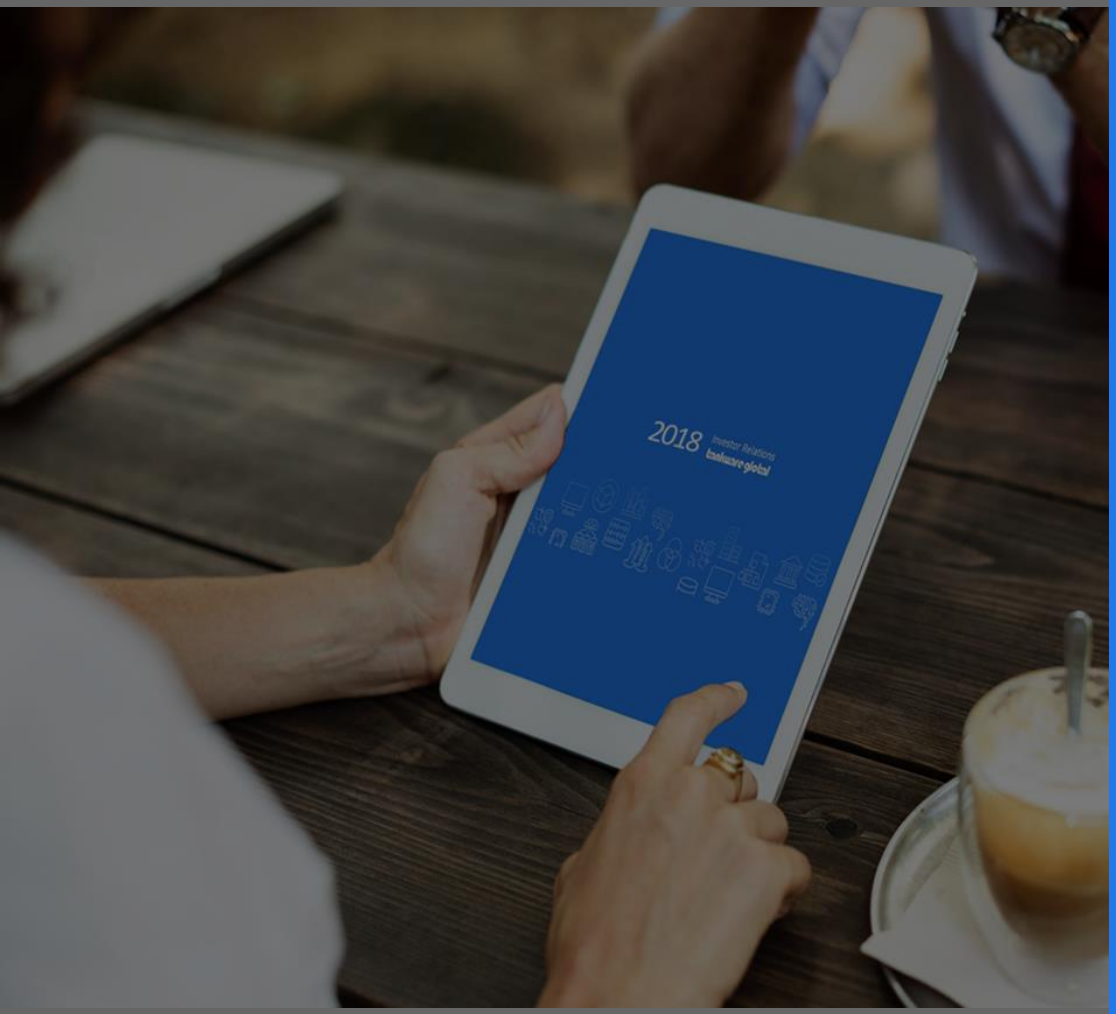


TABLE OF CONTENTS

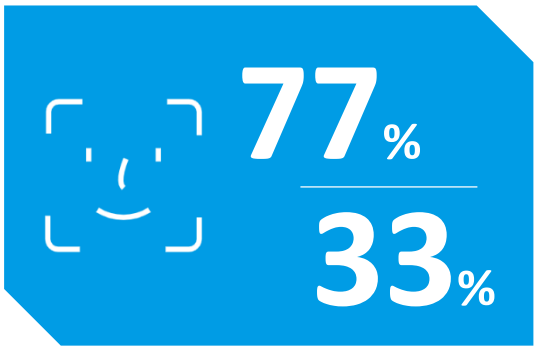
Summary

금융IT 시스템 Public Cloud 운영

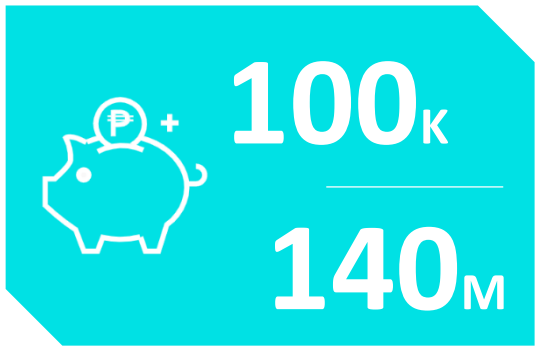
Bankware Global은 지난 3년 동안 고객의 비즈니스 성장을 지원함과 동시에 안정적인 인프라 운영을 제공하는 데 중점을 두었습니다.

현재는 안정적인 인프라 기반 위에서 서비스가 성장함에 따라 고객과 계좌 수가 꾸준히 증가하고 있으며, 곧 신규 채널 또한 추가 예정입니다.

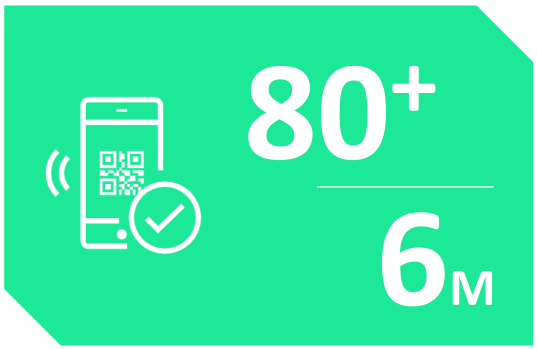
앞으로 Bankware Global은 어플리케이션 서비스 환경을 Kubernetes 기반으로 전환하여 좀더 유연한 구조의 인프라를 만들기 위해 노력 하고 있습니다.



No. of customers increased up to 40% for the first one year and 77% for two years. The average customer annual growth rate reached 33%.



Even under pandemic, more than 100,000 new loans were approved during 2020, and the total amount of loan released was over USD 140M.



More than 80 new loan products were launched in 6 months, and the business grows and expands with new kinds of products that suit the current market.

bankware global

글로벌 코어뱅킹 전문가, 뱅크웨어글로벌

주소 서울특별시 중구 통일로 86, 3층 312호(순화동 바비엥빌딩 3차)

전화 02 501 6415

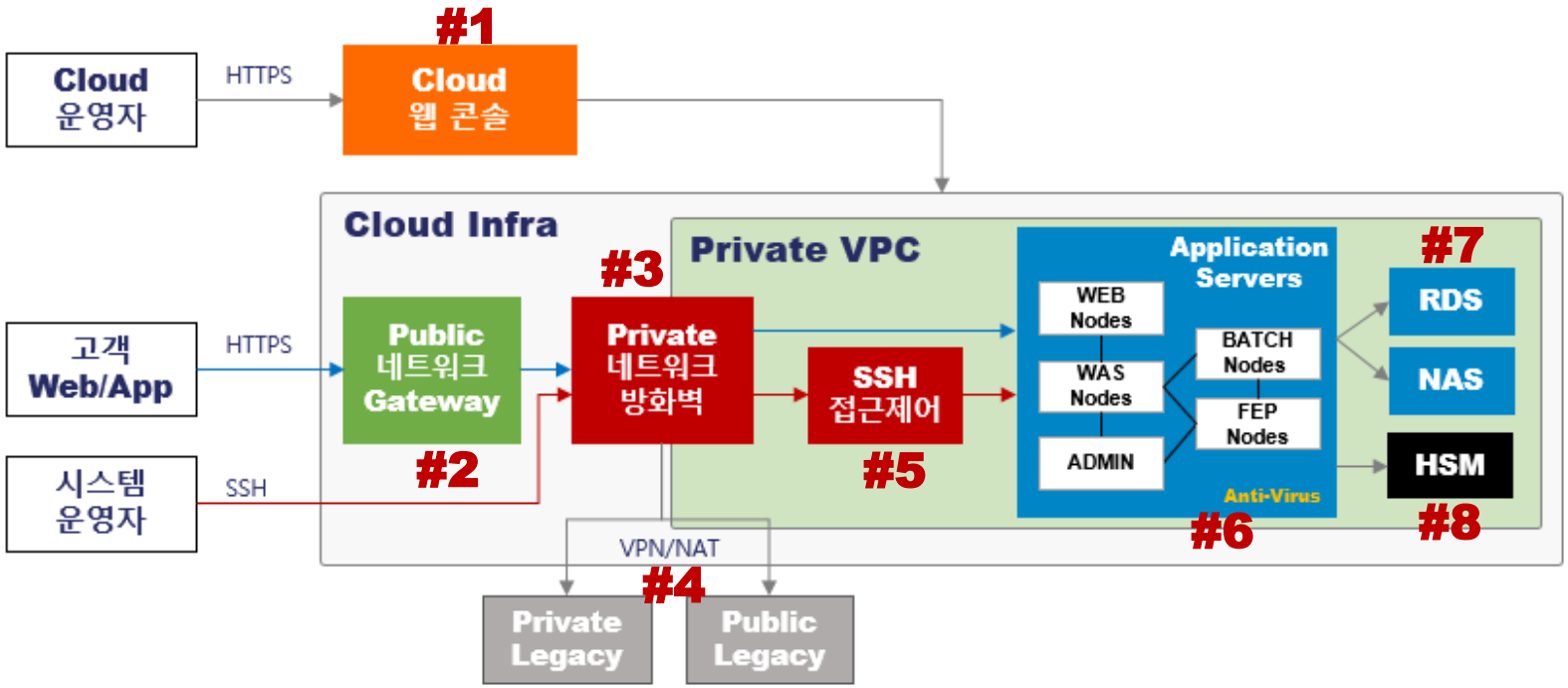
팩스 02 501 6416

이메일 admin@bankwareglobal.com

사이트 www.bankwareglobl.com

여기 부터는
참고자료

1. 보안 및 신뢰



#1. MFA (Two Factor 인증)

#2. HTTPS & Anti-DDoS

#3. Private 네트워크 방화벽

#4. Legacy VPN/NAT 연결

#5. SSH 시스템 접근 통제

#6. Anti-Virus (서버 OS)

#7. TDE (데이터 무결성 검증)

#8. HSM (하드웨어 보안 모듈)

Summary

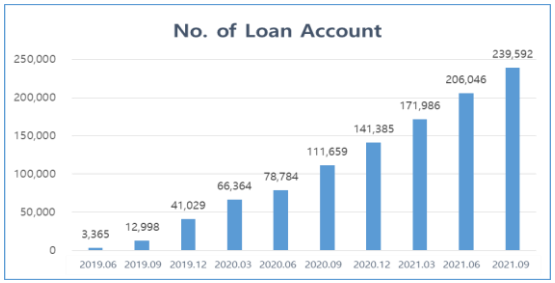
금융IT 시스템 Public Cloud 운영

Bankware Global은 지난 3년 동안 고객의 비즈니스 성장을 지원함과 동시에 안정적인 인프라 운영을 제공하는 데 중점을 두었습니다.

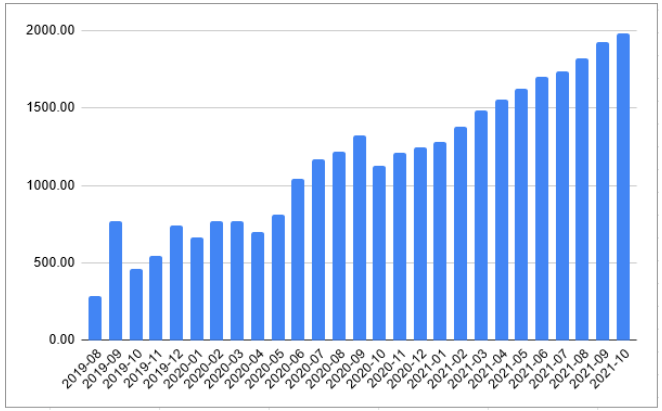
현재는 안정적인 인프라 기반 위에서 서비스가 성장함에 따라 고객과 계좌 수가 꾸준히 증가하고 있으며, 곧 신규 채널 또한 추가 예정입니다.

앞으로 Bankware Global은 어플리케이션 서비스 환경을 Kubernetes 기반으로 전환하여 좀더 유연한 구조의 인프라를 만들기 위해 노력 하고 있습니다.

비즈니스 성장 추이



데이터 증가량 추이



- 일 150 만 건의 거래 Transaction
- 월 50~60G 정도의 RDS 디스크가 증가됨
- 5~6개월 주기로 500G 씩 디스크 증설 (Scale-up)

bankware global