

nowⁿcloud

정보보안 클라우드 소개

eim.net

PROLOGUE



CONTENTS



1

개요 및 배경



2

나우앤클라우드



3

구성 아키텍처



4

회사 소개

I. 개요 및 배경

II. 나우앤클라우드

III. 구성 아키텍처

IV. 회사 소개

개요 및 배경

4차 산업혁명 환경에서 정보보호 중요성 대두

최근 보안 동향

- ☑ ICBM 등 새로운 기술 등장으로 이에 적합한 정보보안 이슈 발생
- ☑ 전통적인 보안 영역이외 혁신적인 사업 등장에 따른 신규 보안 기술 발달
- ☑ 중요 정보가 대량 집적됨에 따라 유출사고 발생시 피해량 증가
- ☑ 정보 소유자들의 적극적인 권리행사에 따른 보안 중요도 증가

정보보호 관련 법령 제정/선포

- ☑ 2011.09.30 개인정보보호법 시행
- ☑ 2016.09.01 개인정보 안정성 확보조치 기준 고시 시행
- ☑ 2016.08.16 의료법 시행 규칙 제 16조 개정
- ☑ 2020.01.09 개인정보보호법, 정보통신망법, 신용정보법 등 데이터 3법 개정안 국회 본 회의 통과
(<http://www.korea.kr/special/policyCurationView.do?newsId=148867915>)

클라우드 발전에 따른 보안요구 사항 증가

- ☑ 2015년 클라우드 컴퓨팅법 이후 2018년 전자금융감독규정 개정안에 따른 클라우드 허용으로 클라우드 보안성, 안전성 문제 대두
- ☑ Private, Public, Hybrid, Multi Cloud 등 다양한 클라우드 환경 등장에 따른 보안 정책 수립 필요

시사점

클라우드 기반의 보안필요

- Firewall, WAF, IPS/IDS, VPN, DB접근제어, DB암호화, 시스템 접근 제어 등 SW기반
- Multi Tenant(단일 기업 내 Project, Division 등)를 수용할 수 있는 Scale-Out 가능한 형태

지속 가능한 보안, 클라우드 파트너

- Private Cloud, Public Cloud 등 다양한 클라우드에 정보보안 솔루션 적용, 유지보수 및 운영 서비스가 가능한 파트너 선정 필요
- 보안과 더불어 클라우드에 같이 고민하고 해결안을 제시할 수 있는 파트너

▶ 관련 법령

“

개인정보보호법

”

개인정보보호법

공공행정 분야

- 공공기관의개인 정보보호에 관한 법률
- 전자정부법
- 주민등록법
- 가족관계의등록 등에 관한 법률
- 공공기관의정보 공개에 관한 법률 등

+

정보통신 분야

- 정보통신망이용 촉진 및 정보보호 등에 관한 법률
- 통신비밀보호법
- 정보통신기반보호법
- 전기통신사업법 등

+

금융/신용 분야

- 신용정보의이용 및 보호에 관한 법률
- 금융실명거래 및 비밀보장에 관한 법률
- 전자거래기본법
- 전자상거래등에 서의 소비자보호에 관한 법률

+

의료 분야

- 생명윤리 및 안전에 관한 법률
- 장기등이식에 관한 법률
- 응급의료에 관한 법률

+

교육 분야

- 초·중·등 교육법
- 교육정보시스템의 운영 등에 관한 규칙 등

적용 대상자

- 공공기관 및 정보통신기업
- 개인정보를 보유한 모든 기업
- 환자의 각종 질병정보를 갖고 있는 병원 및 의료기관
- 협회, 동창회, 전우회 등 회원정보 수집을 하는 비영리단체
- 고객정보를 보유한 자영업자

350만개

50만개

▶ 관련 법령

데이터 3법 주요 개정안

법안	세부 개정 안
개인정보보호법	<ul style="list-style-type: none"> 개인정보 관련 개념을 개인정보, 가명정보, 익명정보로 구분한 후 가명정보를 통계 작성 연구, 공익적 기록보존 목적으로 처리 허용 가명정보 이용 시 안전장치 및 통제 수단을 마련한다
	<ul style="list-style-type: none"> 행정안전부, 금융위원회, 방송통신위원회 등으로 분산된 개인정보보호 감독기관을 통합하기 위해 개인정보보호위원회로 일원화한다. 개인정보보호위원회는 국무총리 소속 중앙행정기관으로 격상한다.
	<ul style="list-style-type: none"> 정보통신망법에 규정된 개인정보보호 관련 사항을 개인정보보호법으로 이관한다 온라인상 개인정보보호 관련 규제 및 감독 주체를 방송통신위원회에서 개인정보보호위원회로 변경한다
신용정보법	<ul style="list-style-type: none"> 가명조치한 개인신용정보로서 가명정보 개념을 도입해 빅데이터 분석 및 이용의 법적 근거를 명확히 마련한다. 가명정보는 통계작성, 연구, 공익적 기록보존 등을 위해 신용정보 주체의 동의 없이도 이용, 제공할 수 있다.

개인정보보호법, 개인정보의 안정성 확보 고시

법 조항	세부 조치 내용	기술적 보호 조치
제 5조 (접근 권한의 관리)	<ul style="list-style-type: none"> 업무수행에 필요한 최소한의 범위로 차등 부여, 취급자별 계정 발급 접근권한 부여기록은 최소 3년간 보관 	<ul style="list-style-type: none"> ✓ DB접근제어 ✓ 시스템 접근제어
제 6조 (접근통제)	<ul style="list-style-type: none"> 개인정보처리시스템에 대한 IP 주소 분석 및 개인정보 유출시도 탐지 및 대응 외부에서 접속시 VPN 사용 P2P, 웹하드 등 비인가프로그래밍, 공유 설정 등 차단 	<ul style="list-style-type: none"> ✓ 방화벽 ✓ 웹방화벽 ✓ VPN ✓ IPS
제 7조 (개인정보의 암호화)	<ul style="list-style-type: none"> 고유식별정보, 비밀번호, 바이오정보 전송 및 저장시 암호화 	<ul style="list-style-type: none"> ✓ 정형 암호화 ✓ 비정형 암호화
제 8조 (접속기록 보관)	<ul style="list-style-type: none"> 최소 6개월 이상 로그 저장, 반기별 1회 점검 	<ul style="list-style-type: none"> ✓ DB접근제어 ✓ 시스템접근제어
제 9조 (악성프로그램 방지)	<ul style="list-style-type: none"> 백신등 보안프로그램 설치 	<ul style="list-style-type: none"> ✓ 백신

▶ 관련 법령

의료법 개정안	
법안	세부 개정 안
의료법	<ul style="list-style-type: none"> 제23조제 2항(전자의무기록의 표준화 등)
의료법 시행규칙	<ul style="list-style-type: none"> 제16조(전자의무기록의 관리·보존에 필요한 시설과 장비 등)
고시	<ul style="list-style-type: none"> 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준

의료법, 전자의무기록 관리 · 보존에 필요한 고시		
시설과 장비 기준	세부 조치 내용	기술적 보호 조치
전자의무기록 백업	<ul style="list-style-type: none"> 시스템 무중단 백업 백업데이터 긴급 복구 백업데이터 위·변조 방지 백업설비의 물리적 분리 	✓ 백업 솔루션
네트워크 보안	<ul style="list-style-type: none"> 네트워크 이중화 네트워크 보호시스템 	<ul style="list-style-type: none"> ✓ IDC(클라우드) ✓ 방화벽 ✓ IPS
시스템 보안	<ul style="list-style-type: none"> 데이터 암호화 DB접근 및 권한 제어 데이터 모니터링 보조시스템 운영 	<ul style="list-style-type: none"> ✓ 암호화, ✓ DB접근제어 ✓ 시스템 이중화
물리적 접근 방지 및 시설	<ul style="list-style-type: none"> 출입 통제 및 모니터링 CCTV 재해예방 시설 	✓ IDC
개인정보의 안정성확보조치	<ul style="list-style-type: none"> 개인정보보호법 시행령 	✓ 개인정보보호법 고시

법적 및 정보보안 요구사항의 분석된 내용을 기반으로
최적화된 정보보안 클라우드 제시 필요

시사점 종합

법/제도
분석

클라우드
설계

경제성

운영 전문가
확보

세부 사항

01

법/제도 분석

개인정보보호법, 정보통신망법, 신용정보보호법,
의료법 안정성 확보 조치 어려움

02

클라우드 설계

법안에 맞는 클라우드 및 정보보안 설계는 어떻게?

03

경제성

저가의 정보보안 솔루션이 없음.

04

운영 전문가 확보

클라우드 설계, 구축, 운영 전문가 필요
정보보안 솔루션 설계, 구축, 운영 전문가 필요

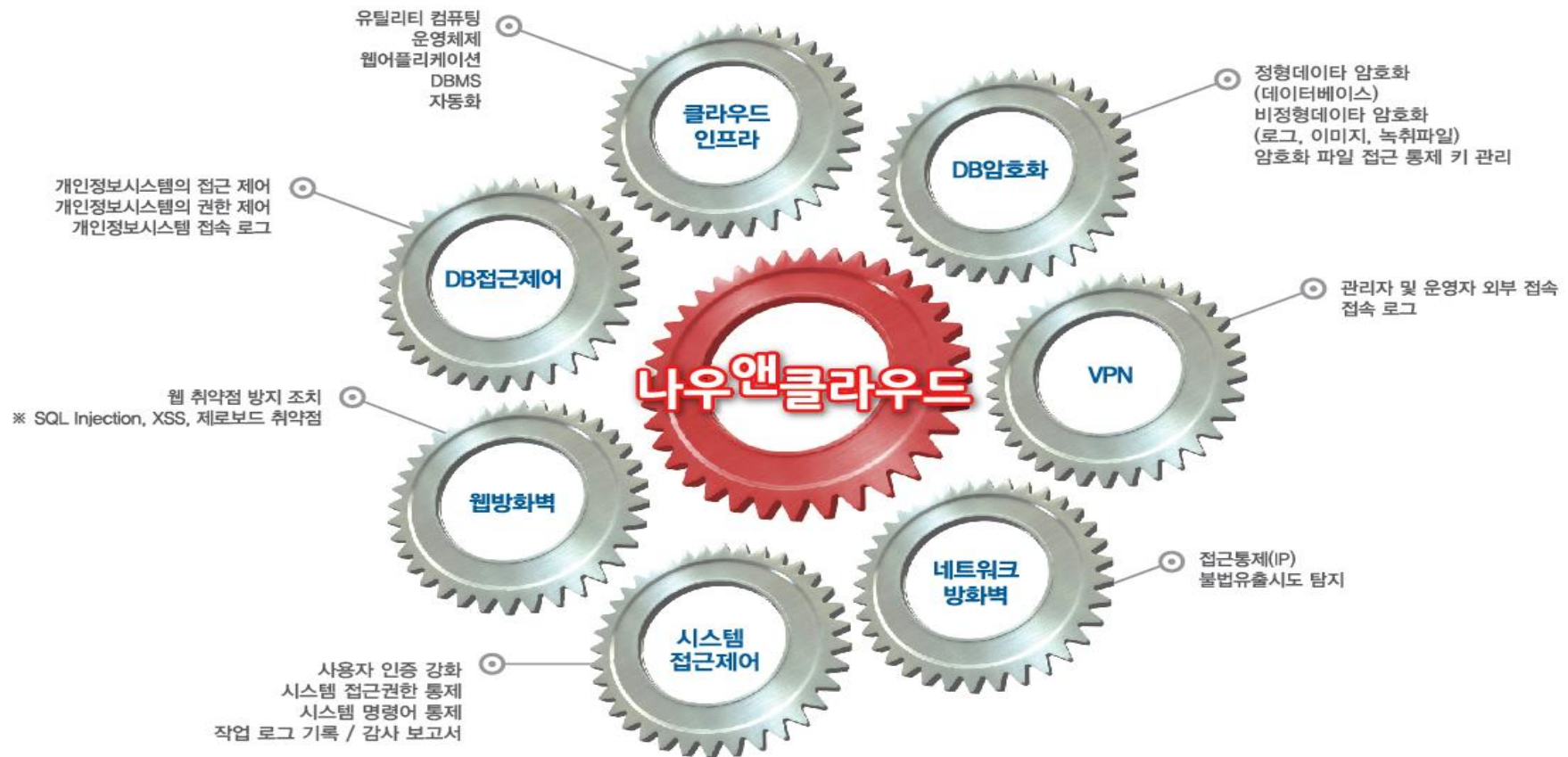
I. 개요 및 배경

II. 나우앤클라우드

III. 구성 아키텍처

IV. 회사 소개

“ 클라우드 + 정보보안 + 법적 기술적 보호조치 완벽 대응 원-스탑 서비스 ”
(클라우드 서비스 보안 시스템 및 그 방법 특허 획득)



▶ 나우앤클라우드 서비스



- 개인정보 보호법
- 정보통신망법
- 신용정보 보호법
- New Tech Trend 대응

클라우드 환경의 보안 컴플라이언스 Issue 해결

- 1 정보보안 운영 관제 서비스
- 2 UTM (방화벽, VPN, IPS/IDS)
- 3 시스템 접근제어
- 4 웹방화벽
- 5 DB접근제어
- 6 DB/데이터 암호화(비식별화 포함)
- 7 백신
- 8 Public Cloud 9 Private Cloud
- 10 보안 인증, 웹취약점 점검, 모의해킹

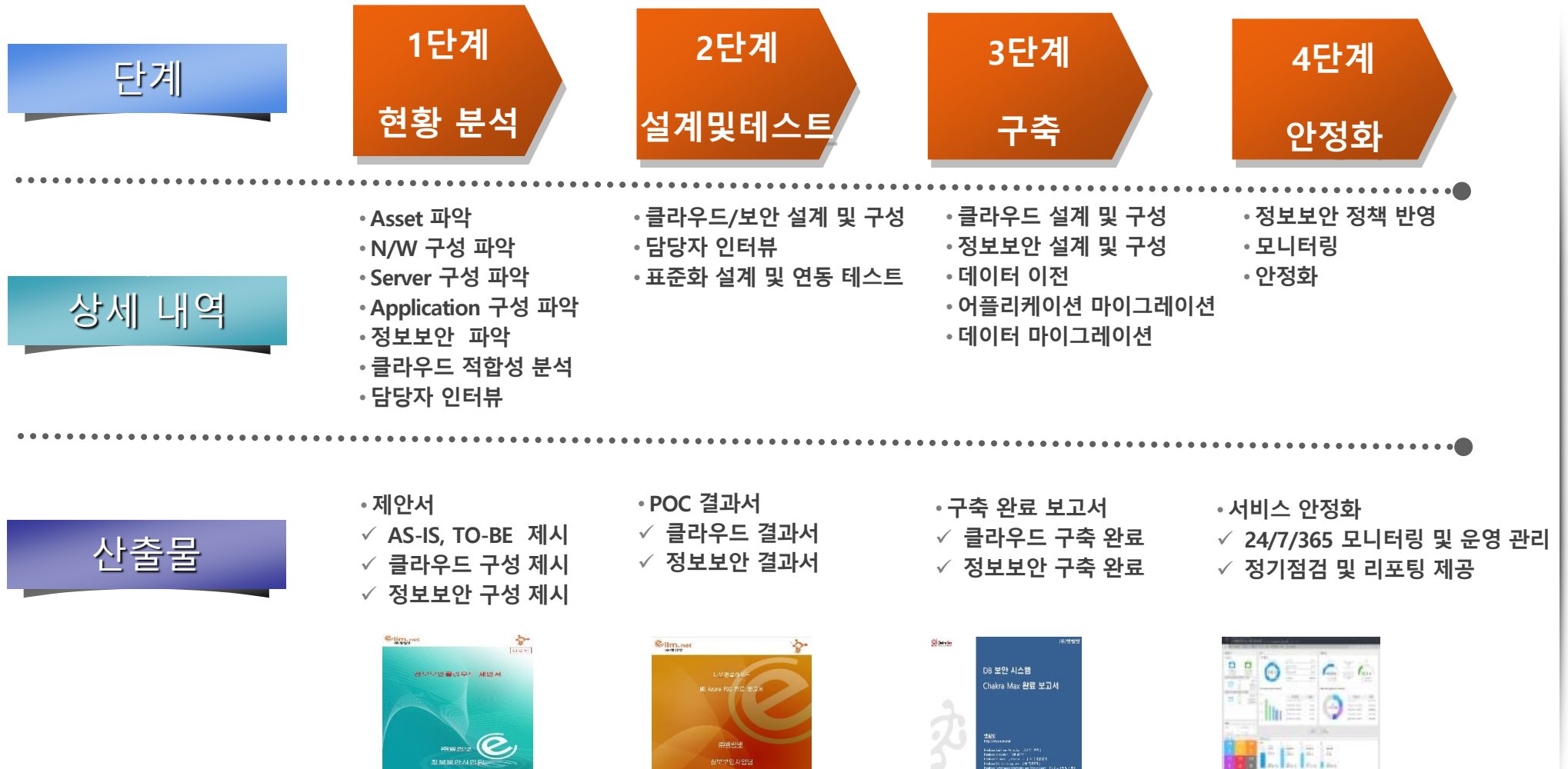
나우앤클라우드 서비스 & 보안 솔루션

- 1 24*365 정보보안 컨설팅, 운영 및 유지보수
- 2 Sophos, CheckPoint, PaloAlto
- 3 HI-Ware, RedCastle
- 4 WAPPLES, DeepFinder
- 5 Chakra MAX, DBSAFER
- 6 Vormetric, D'Amo
- 7 Alyac, Virus Chaser
- 8 MS Azure, Amazon Web Service
- 9 VMware, OpenStack
- 10 삼정회계KPMG

“

단계별 전문 담당자 배정 지원

”

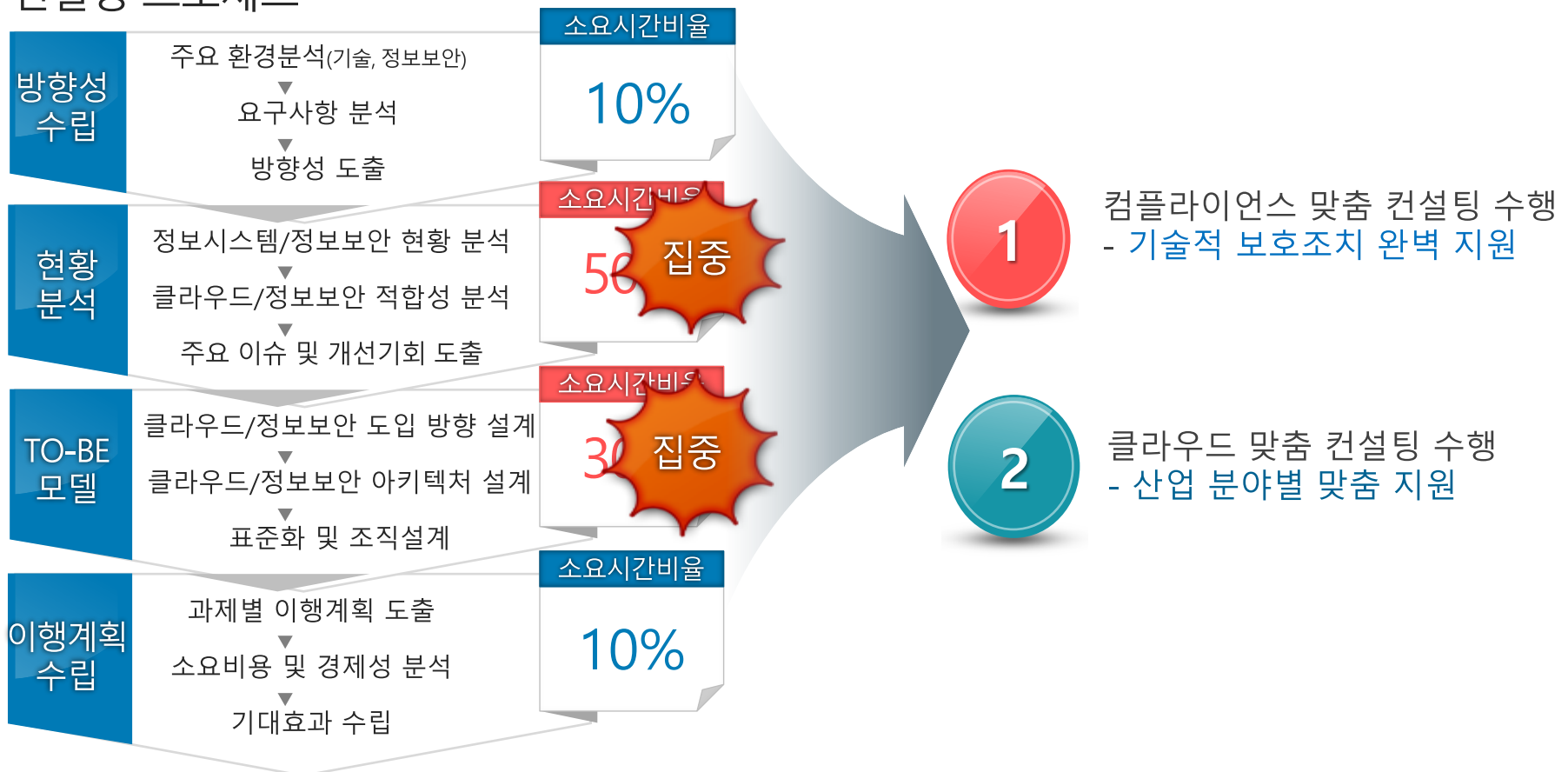


“

현황분석 및 TO-BE 모델에 집중 진행

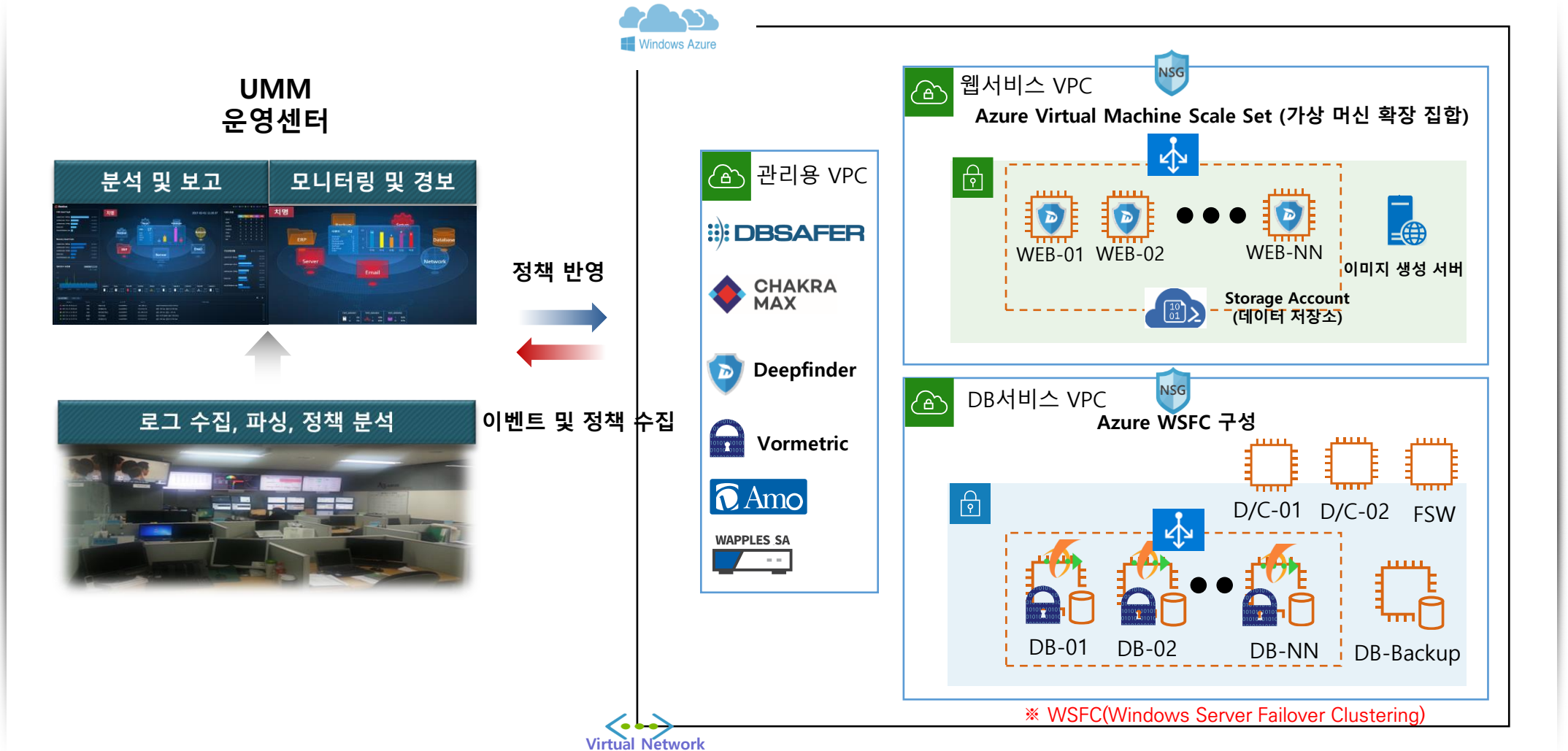
”

컨설팅 프로세스



▶ 나우엔클라우드 환경 구축

클라우드 환경내 컴플라이언스에 맞는 정보보안 솔루션을 설치하고 통합 정보보안 운영 관제 서비스에 필요한 환경들을 구축한다.



▶ 통합 정보보안 운영 관제 서비스(UMM)

UMM(Unified Monitoring for Information Security Management) 이기종 정보보안 솔루션의 정책 및 로그를 정규화, 축약, 필터링하여 이벤트 분석 및 보안 정책을 원활하게 반영하는 시스템

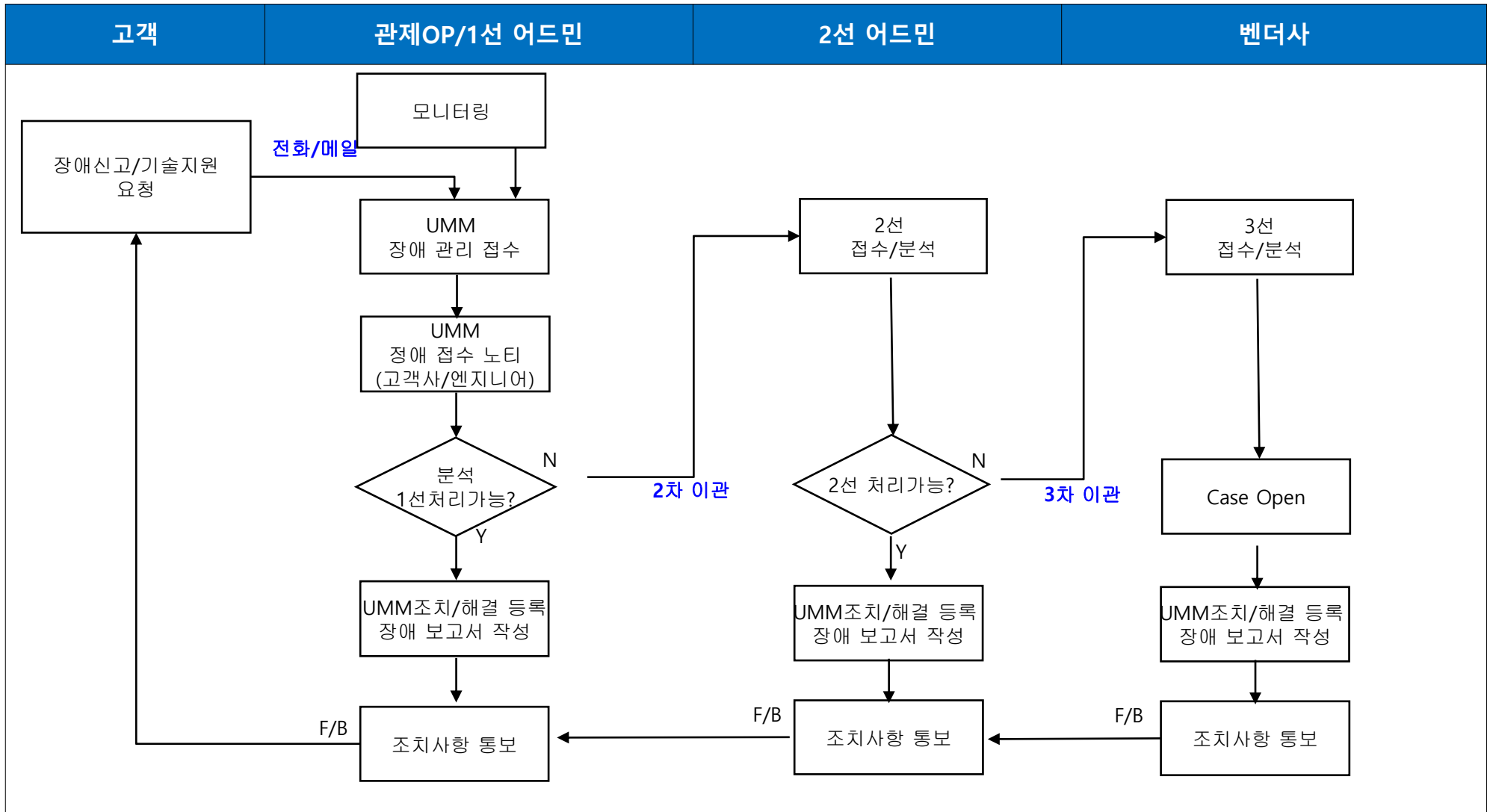


주요 기능 및 장점	
주요 기능	
통합 모니터링 및 장애 대응	이기종 정보보안 솔루션 프로세스 및 이벤트 로그 통합 모니터링 이기종 정보보안솔루션 자원 현황 모니터링 Alert Service 및 장애 복구
정보보안 솔루션 정책 관리	정보보안 솔루션 정책 관리 정보보안 솔루션 매니저 관리
고객 관리	고객 등록 및 조회 고객사 정보보안솔루션 정보 관리
CRS	정책 변경 관리 장애 대응 관리 월간 정기점검 및 리포팅 관리
장점	
<ul style="list-style-type: none"> • 이기종 정보보안솔루션의 통합 모니터링 및 장애 대응 편의성 제공 • 다양한 정보보안 솔루션 간의 보안정책 연관성 분석 및 관리로 정보보안 강화 • 보안 전문 인력의 노하우를 보안 정책 반영 • 신속한 고객 대응 	

정보보안 유지 보수 및 지원 범위

구분		기간	지원 내용
무상	컨설팅	도입 전	<input type="checkbox"/> 산업별 및 서비스에 맞는 클라우드 제안 <input type="checkbox"/> 법적 대응에 맞는 정보보안서비스 제안
	POC		<input type="checkbox"/> 클라우드 구축, 성능, 기능 결과 제공 <input type="checkbox"/> 정보보안솔루션 구축, 기능 결과 제공
	모니터링	검수완료 후 서비스 기간 내	<input type="checkbox"/> 프로세스 상태 체크 <input type="checkbox"/> 시스템 자원 현황 및 이벤트 로그 체크 <input type="checkbox"/> Alert Service
	운영관리		<input type="checkbox"/> S/W 패치 및 업그레이드 서비스 제공 <input type="checkbox"/> 정보보안 정책 반영 및 운영 관리 제공
	장애 복구		<input type="checkbox"/> 장애 복구 - 기본 업무 시간(09:00 ~ 18:00) : 2 시간 이내 대응 - 야간 및 공휴일 : 긴급 문제 발생 시 대응
	정기 점검		<input type="checkbox"/> 시스템 및 프로세스 상태 체크 <input type="checkbox"/> 정보보안 정책 체크 <input type="checkbox"/> 이벤트 로그 체크
	리포트		<input type="checkbox"/> 정기 및 수시 리포트 제공
	교육		<input type="checkbox"/> 정보보안 운영 교육
유상	무상 유지보수 제공 서비스	무상 유지보수 기간 만료	<input type="checkbox"/> 무상 유지보수 지원 내역

운영 프로세스



▶ SLA(Service Level Agreement)

구분		보상 조건	내용
SLA	서비스 불이행 시 보상조건	월 정보보안 서비스 이용요금의 장애 시간 만큼 감면	<input type="checkbox"/> 정보보안 솔루션의 장애로 인해 고객사 서비스에 장애 시간이 2시간 이상 초과 발생할 경우 <input type="checkbox"/> 운영팀의 기술적 실수로 서비스 이용 장애
		월서비스 이용 요금의 30% 감면	<input type="checkbox"/> 고객의 요청사항에 2회 이상 미 조치로 인해 정식으로 고객 불만이 접수된 경우
	예외 사항	보상을 받을 수 없는 경우	<input type="checkbox"/> 클라우드 장애로 인해 정보보안 서비스 이용 장애 ※(클라우드 SLA에 적용 됨) <input type="checkbox"/> 고객사 또는 제3자의 귀책 사유로 인한 서비스 이용 장애 및 지연 <input type="checkbox"/> 고객의 서비스에 발생한 사고의 확산을 방지하기 위한 서비스 중단 <input type="checkbox"/> 상기 외 합의 하에 책임이 면제되는 경우

정보보안 인증서 제공

교육 확인증

기업명 : 엘림넷
 사업등록번호 : 220-81-97656
 주소 : 서울시 서대문구 경계대로 15 엘림넷빌딩
 과정명 : 개인정보보호법 준수를 위한 의료기관에 대응
 교육 일시 : 2000년 00월 00일
 교육 시간 : 2시간

ELIMNET

위 기업은 개인정보보호법 교육을 성실히 진행하였음을 확인합니다.

2000년 00월 00일

(주)엘림넷
 대표이사 한환희

나우엔클라우드 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 나우엔클라우드 서비스 사용(임대형)
 제품명: 나우엔클라우드

License Certification Number: E180401NOWN001
 Validate date of License: 2018-04-01 ~ 2021-03-31
 Product Description:

Item	Product Number	Copy
나우엔클라우드	Nowncloud	1

나우엔클라우드 서비스에서 제공하는 클라우드, 서버, IP, VPN, DB압축, DB접근제어, 백업 등 보안 솔루션 도입 및 적용
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너WAF 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너WAF 도입(임대형)
 제품명: 이네트너WAF

License Certification Number: E180401ENTWAF001
 Validate date of License: 2018-04-01 ~ 2021-03-31
 Product Description:

Item	Product Number	Copy
이네트너 WAF	eNETnerWAF	2

Server내 웹서버 및 방화벽 (WAF) TOP 100명) 및 로그 저장 기능 제공
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너 UTM 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너UTM 도입(임대형)
 제품명: 이네트너UTM

License Certification Number: E180401ENTUTM001
 Validate date of License: 2018-04-01 ~ 2021-03-31
 Product Description:

Item	Product Number	Copy
이네트너 UTM	eNETnerUTM-SS105	1

OS 최신 업그레이드, 방화벽/서명암시/AVN 등 차단 및 실시간 업데이트
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너 DB암호화 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너DB암호화 도입(임대형)
 제품명: 이네트너DB암호화

License Certification Number: E180911ENTDB001
 Validate date of License: 2015-12-18 ~ 2018-12-17
 Product Description:

Item	Product Number	Copy
이네트너 DB암호화	eNETnerDB	1

DB 암호화 최신 업그레이드 및 세션 업데이트 (기밀 암호화 제공)
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너 DB접근제어 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너DB접근제어 도입(임대형)
 제품명: 이네트너DB접근제어

License Certification Number: E180911ENTDBAC001
 Validate date of License: 2015-12-18 ~ 2018-12-17
 Product Description:

Item	Product Number	Copy
이네트너 DB접근제어	eNETnerDBAC	1

DB 접근 및 권한 제어 및 로그 저장 기능 제공, 최신 정책 업데이트 적용
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너 PC필터 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너PC필터 도입(임대형)
 제품명: 이네트너PC필터

License Certification Number: E180401ENTPC001
 Validate date of License: 2015-12-18 ~ 2018-12-17
 Product Description:

Item	Product Number	Copy
이네트너 PC 필터	eNETnerPC-100	14

PC내의 개인정보, 비밀번호/문자열/문자열과 및 실시간 탐지 기능 제공
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희

이네트너백신 라이선스 인증서 ELIMNET License Certification

Issue Subject
 고객사: 엘림넷
 프로젝트명: 이네트너백신 도입(임대형)
 제품명: 이네트너백신

License Certification Number: E180401ENTVAC001
 Validate date of License: 2018-04-01 ~ 2021-03-31
 Product Description:

Item	Product Number	Copy
이네트너 백신	eNETnerServerVaccine	2

Server내 바이러스를 실시간 탐지하여 예방 및 치료해 PC를 보호하는 기능 제공
 상기 소프트웨어가 제공하는 인클로저 및 업데이트에 대해 위와 라이선스가 부여된 고객사에서 사용권을 드립니다.

2000년 00월 00일
 엘림넷
 대표이사 한환희



컴플라이언스 One Stop 서비스

- 개인정보보호법 기술적 보호조치
- 정보통신망법 기술적 보호조치
- 신용정보보호법 기술적 보호조치
- 의료법 기술적 보호조치
- 클라우드컴퓨팅발전법 기술적 보호조치



경제성 & 안전성

- 클라우드 & 정보보안을 위한 초기 투자 없음
- 클라우드 & 정보보안 전문 인력 지원
- 보안솔루션 국내 및 글로벌 인증 제품 제공
- 정보보안 마켓 1위 제품 제공



통합 정보보안 관리 서비스

- 이기종 정보보안 솔루션 통합 모니터링 제공
- 다양한 정보보안 솔루션 간의 정보보안 정책 연관성 분석 및 관리
- 24시간 365일 정보보안 모니터링 및 운영 관리
- 월간 정기점검 및 리포트 제공



업무 일원화 및 효율성

- 클라우드 & 정보보안 컨설팅, 설계, 구축, 운영 원-스탑 지원
- UMM을 통한 다양한 정보보안 솔루션의 통합 관리 및 업무 일원화
- 정보보안 솔루션 장애시 빠른 대응 지원

I. 개요 및 배경

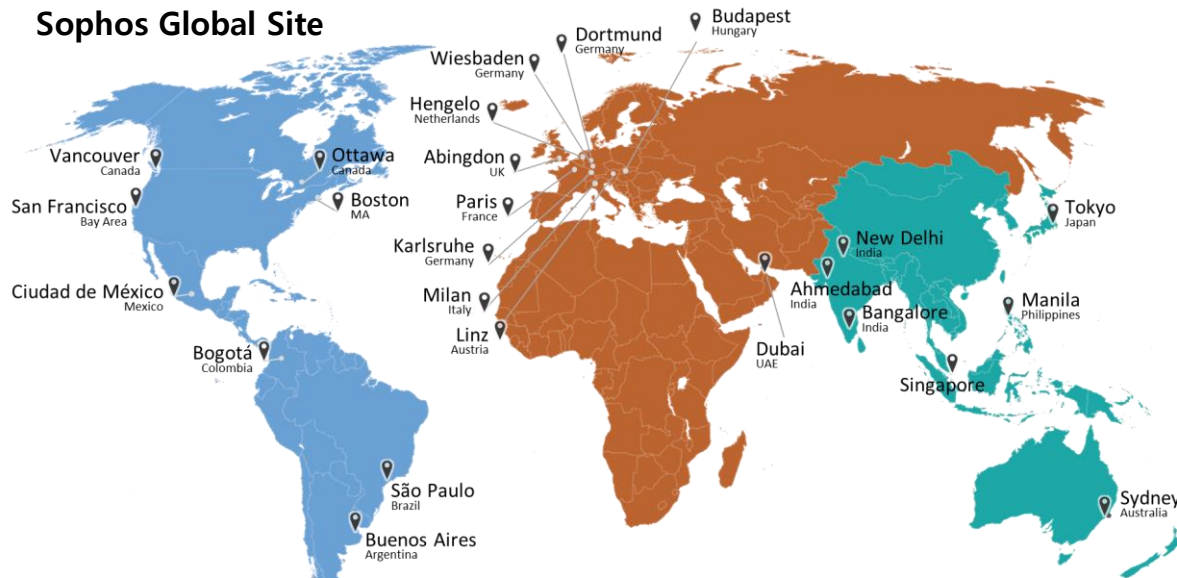
II. 나우앤클라우드

III. 구성 아키텍처

IV. 회사 소개

▶ UTM(Unified Threat Management) 소개

“ AI를 통한 Malware 분석으로 정확도와 예측력을 향상 ”



Sophos AI

Sophos Artificial Intelligence was formed in 2017 to produce breakthrough technologies in information security. We're currently focused on machine learning, large scale scientific computing architecture, human-AI interaction, and information visualization. Here we present our current projects, our team, our conference talks, our publications, and our open source code and research datasets.

FEATURED PUBLICATIONS

Featured projects



Petabyte-Scale AI Infrastructure

Aug 25, 2019

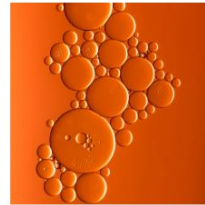
At Sophos, we train our ML models on millions, tens of millions, and



AI / Security Analyst Collaboration

Aug 25, 2019

Thus far, machine learning has been seen as separate from security



ML-NLP Based Targeted Phishing Detection

Aug 25, 2019

Detecting targeted phishing attacks is a hard problem, because there is

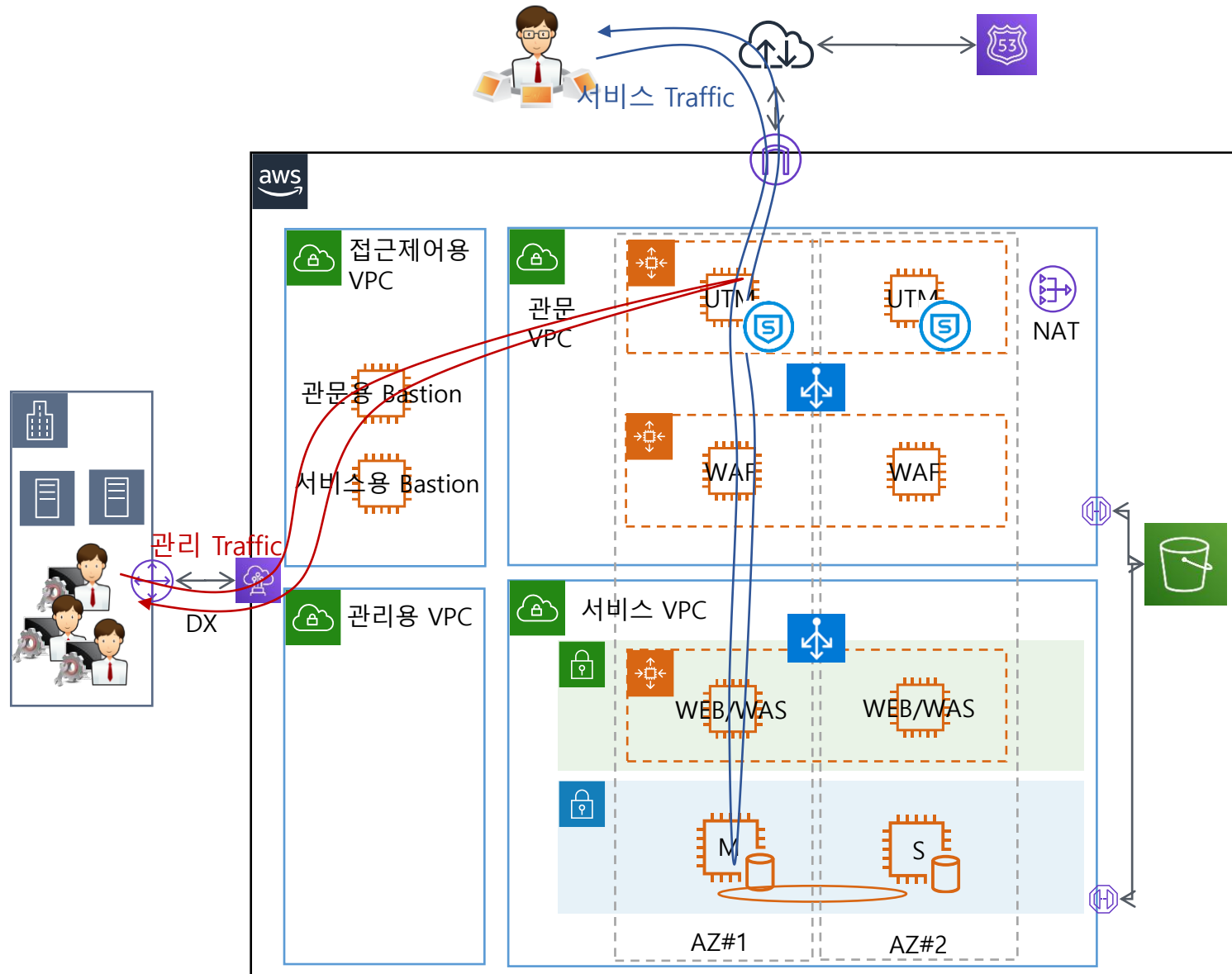
Sophos UTM

- 1985년 옥스포드 설립
- 3,500 임직원
- 327,000 고객
- 150개국 1억명 이상 사용자
- 45,000 파트너
- Sophos Labs 위협연구소

Sophos Labs

- **Labs**
: 최선의 예측을 위해 수억개에 이르는 Global Data Sample을 제공
- **Data Science**
: 사이버 보안의 이슈를 해결하기 위해 가장 효율적인 알고리즘을 생성
- **Data Science + Labs**
: 시스템 정확도와 예측력을 개선시키기 위해 Feed Back을 지속적으로 통합

UTM(Unified Threat Management) 구성



구성방식 및 특징점

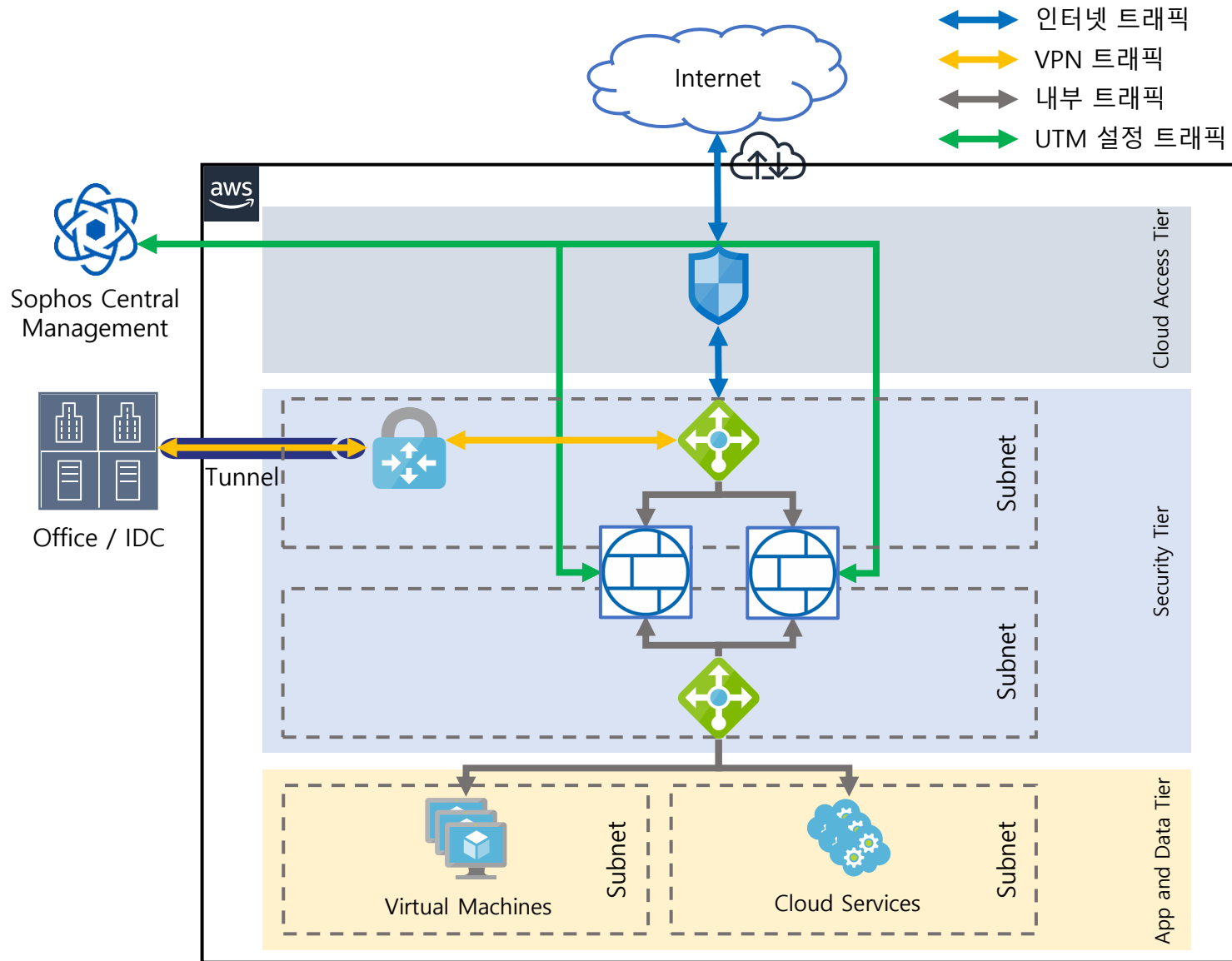
이중화 구성 방식

- Sophos Cold Standby**
 - 단일 인스턴스로 운영되며, Config, Log 등 정보가 S3에 저장
 - 장애시 S3의 정보를 활용하여 새로운 Sophos 인스턴스 생성
- Sophos Warm Standby**
 - 두개의 인스턴스로 운영되며, 운영간 변경된 정보는 S3에 저장
 - 장애시 두번째 인스턴스가 S3에 저장된 변경정보를 동기화하여 가동

주요 기능

- 방화벽
- IPS
- 웹방화벽
- 안티스팸
- SSL VPN / IPsecVPN

▶ UTM(Unified Threat Management) 이중화



구성방식 및 특징점

이중화 구성 방식

- **Active-Active (Cluster)**
 - 두개의 UTM을 Active-Active 구성으로 구동
 - 소포스 센트럴 매니지먼트(SaaS)에서 두개의 UTM 설정을 일원화하여 관리

주요 기능

- 방화벽
- IPS(침입방지시스템)
- 원격접속 VPN
- 사이트 to 사이트 VPN

주요 리소스

	UTM (XGFW)		L4 LB
	VPN Gateway		NSG

▶ 시스템접근제어 소개

“ 서버와 네트워크 접근 및 권한 통제를 통해 인프라 운영 관리 최소화하기 위한 솔루션 ”



주요 기능 및 특징점

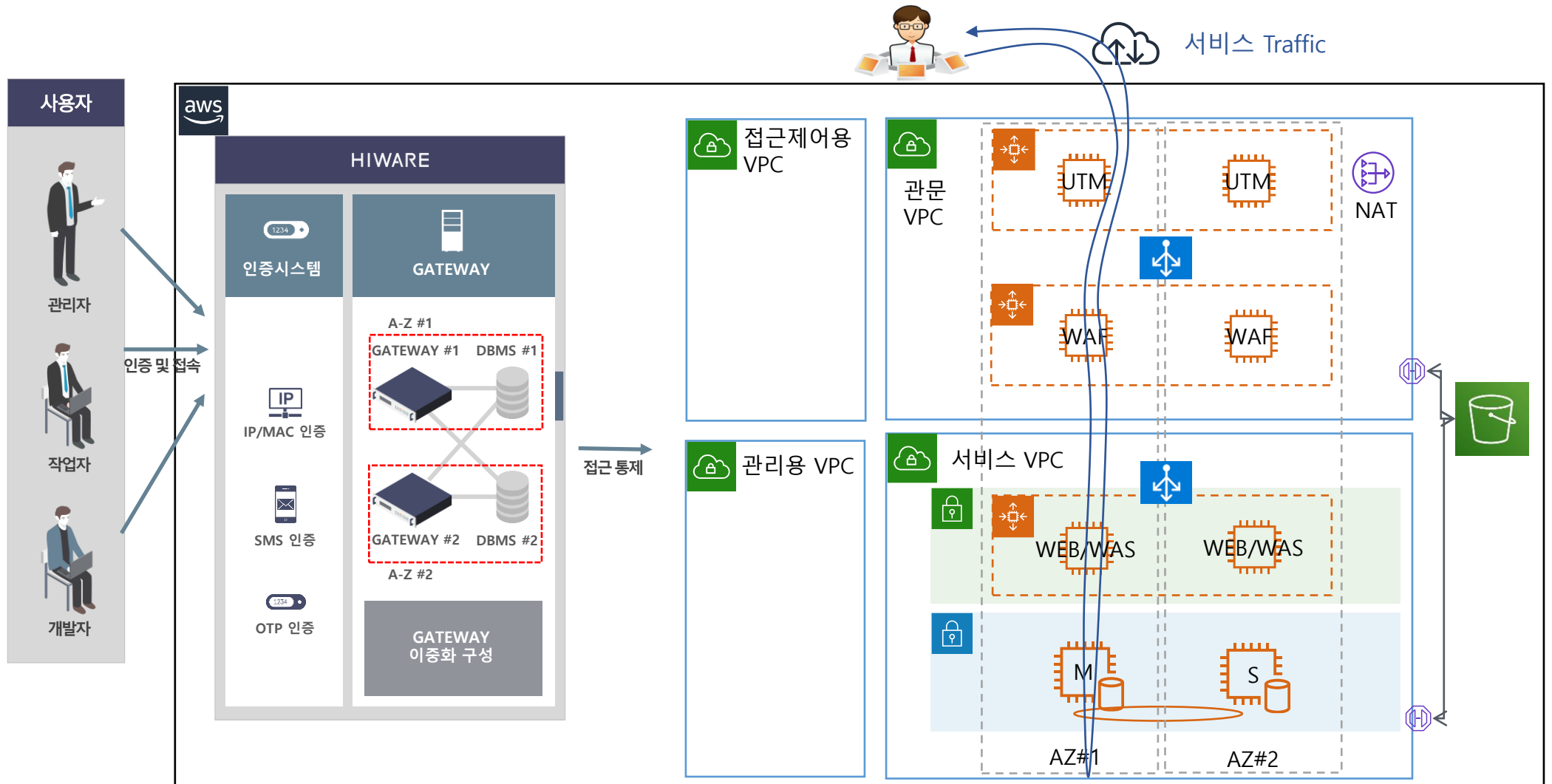
주요 기능

- **사용자 인증 강화**
 - IP/MAC 인증 및 이중인증 등 인증체계 강화
- **시스템 접근 권한 통제**
 - 사용자별 권한 차등 부여 및 접속 시간 통제
- **시스템 명령어 통제**
 - 다양한 조건별 명령어 권한 설정
 - 주요명령 입력시 통제, 로깅, 알림 제공
- **작업 로그 기록 / 감사 보고서**
 - 로그 기록으로 감시 및 추적성 강화

특장점

- **편의성**
 - 결제, 패스워드 변경 알림 제공
- **안전성**
 - 사용자/클라우드/망분리 등 다양한 환경 지원
- **기술력**
 - 국내 접근 통제 시정 점유율 1위
 - 산업통상자원부, 우수기술연구센터(ATC) 지정

구성 아키텍처 ▶ 시스템접근제어 구성

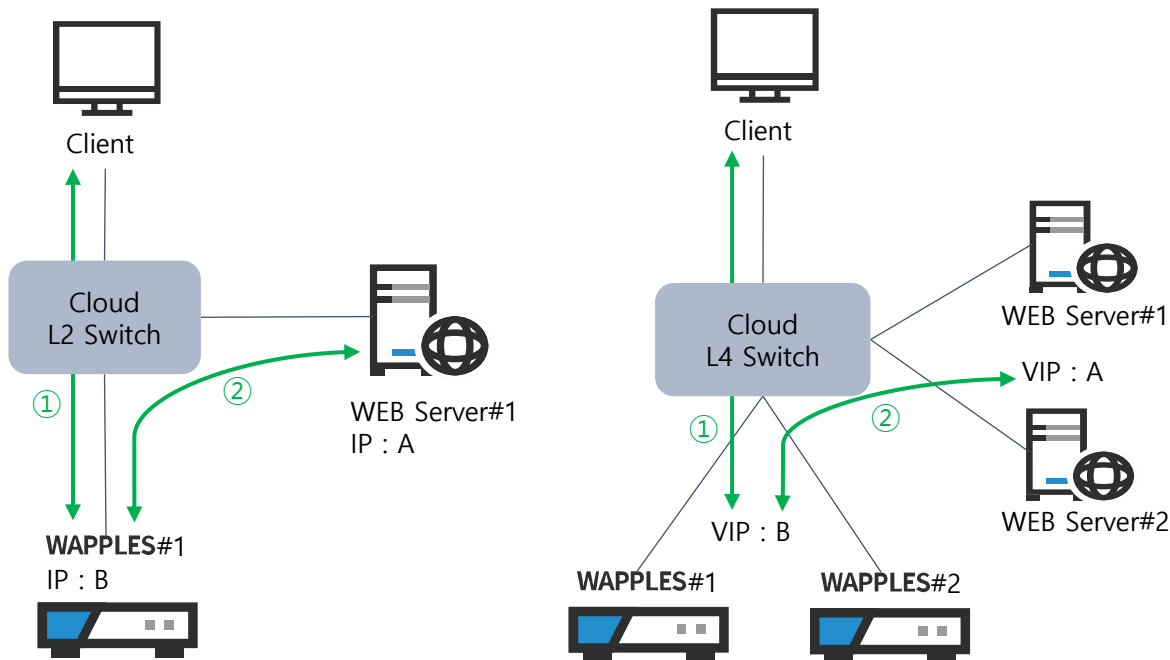


※ 이중화 구성 : 가용영역(A-Z)를 둘로 나누어 이중화를 구성함으로써 HIWARE에 구성 영역의 안정성을 확보

※ 자원 할당 : M4 2Xlarge
 • CPU : 4 Core
 • Memory : 32G

▶ WAF(Web Application Firewall) 소개

“ 웹취약점을 보호 및 방어하기 위한 솔루션 ”



주요 기능 및 특징점

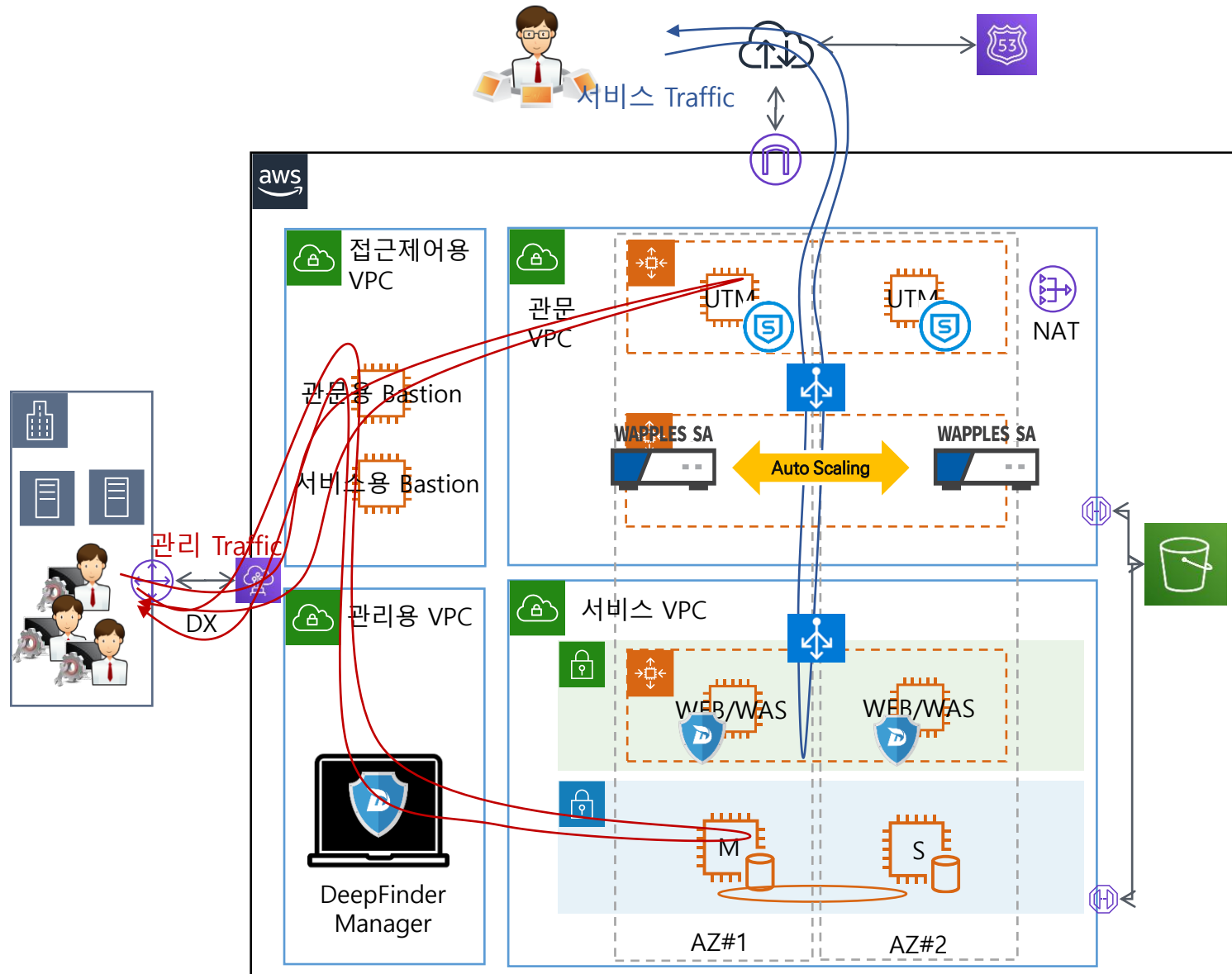
주요 기능

- 웹공격 탐지 및 차단
 - OWASP TOP 10, 국정원 8대 취약점 방어
- 정보 유출 방지
 - 개인정보 게시판 게시 및 파일 업/다운로드시 탐지 및 대응
- 부정 접근 방지
 - Brute Force Attack 등과 같은 비정상적인 접근 탐지 및 차단
- 위변조 방지

특장점

- 오탐 없는 높은 보안성 보장
 - 지능형 엔진 COCEP 탑재로 변경 공격 및 새로운 공격 즉시 탐지
- 보안 관리 편의성
 - 7가지 Preset 보안 정책 GUI로 정책 편집, 내보내기, 불러오기 제공
 - 통합관리시스템을 통한 다수의 WAF 통합 관리

WAF(Web Application Firewall) 구성



클라우드 구성

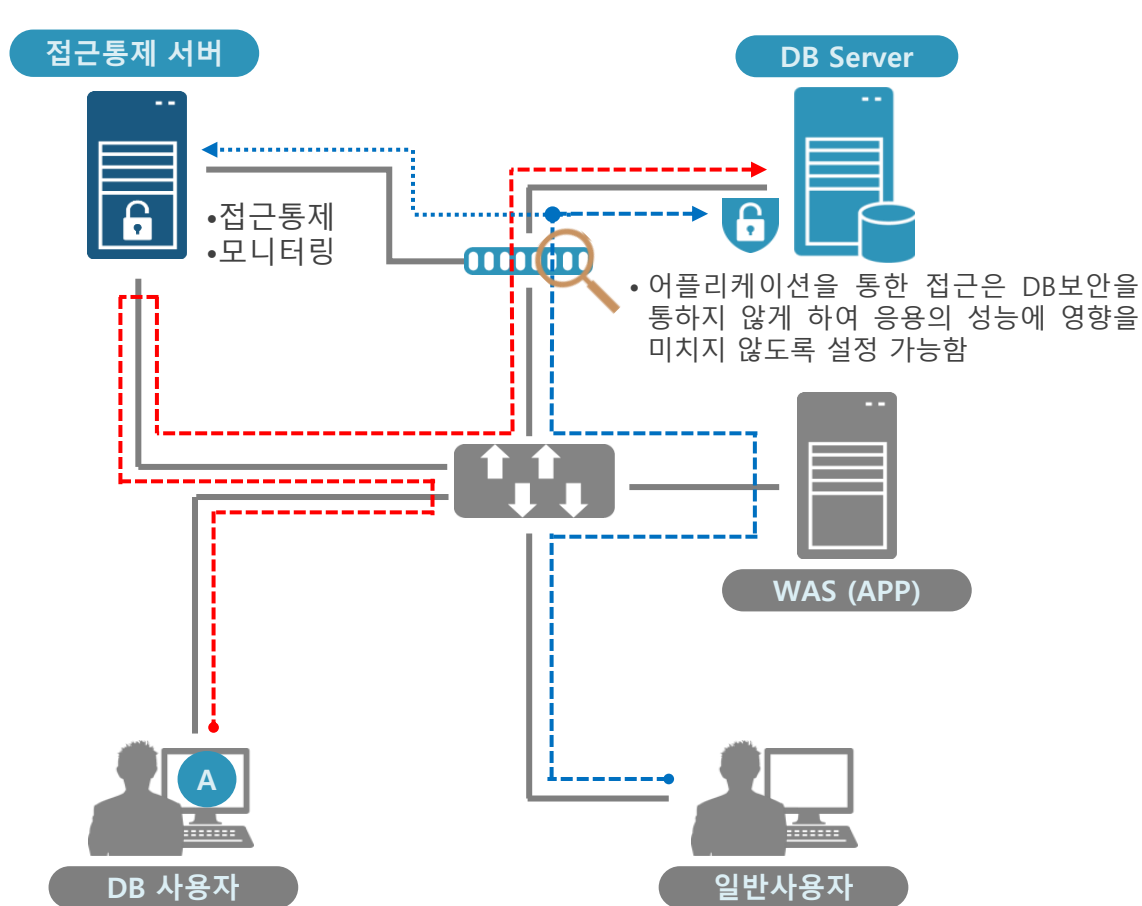
Proxy 구성 방식

- LB - 웹방화벽 - LB - 웹서버 구성
- 이중화 구성(A-S 혹은 A-A)을 통해 서비스 가용성을 확보하며, Auto-scaling 구성설정
- 웹방화벽에서 보호 도메인이 여러 개일 경우, 웹방화벽 상단의 LB에 여러 IP를 설정하고 port 로 구분하여 WAF로 전달 및 패킷검사
- DNS failover 구성을 통한 서비스 가용성 확보

Plug-in 구성 방식

- 웹서버에 Plug-in 설치 됨
- 정책 미치 로그 매니저 서버에서 통합 관리 됨

“ 대량의 내부정보유출의 위험을 최소화하기 위한 솔루션 ”



구성 방식 및 특징점

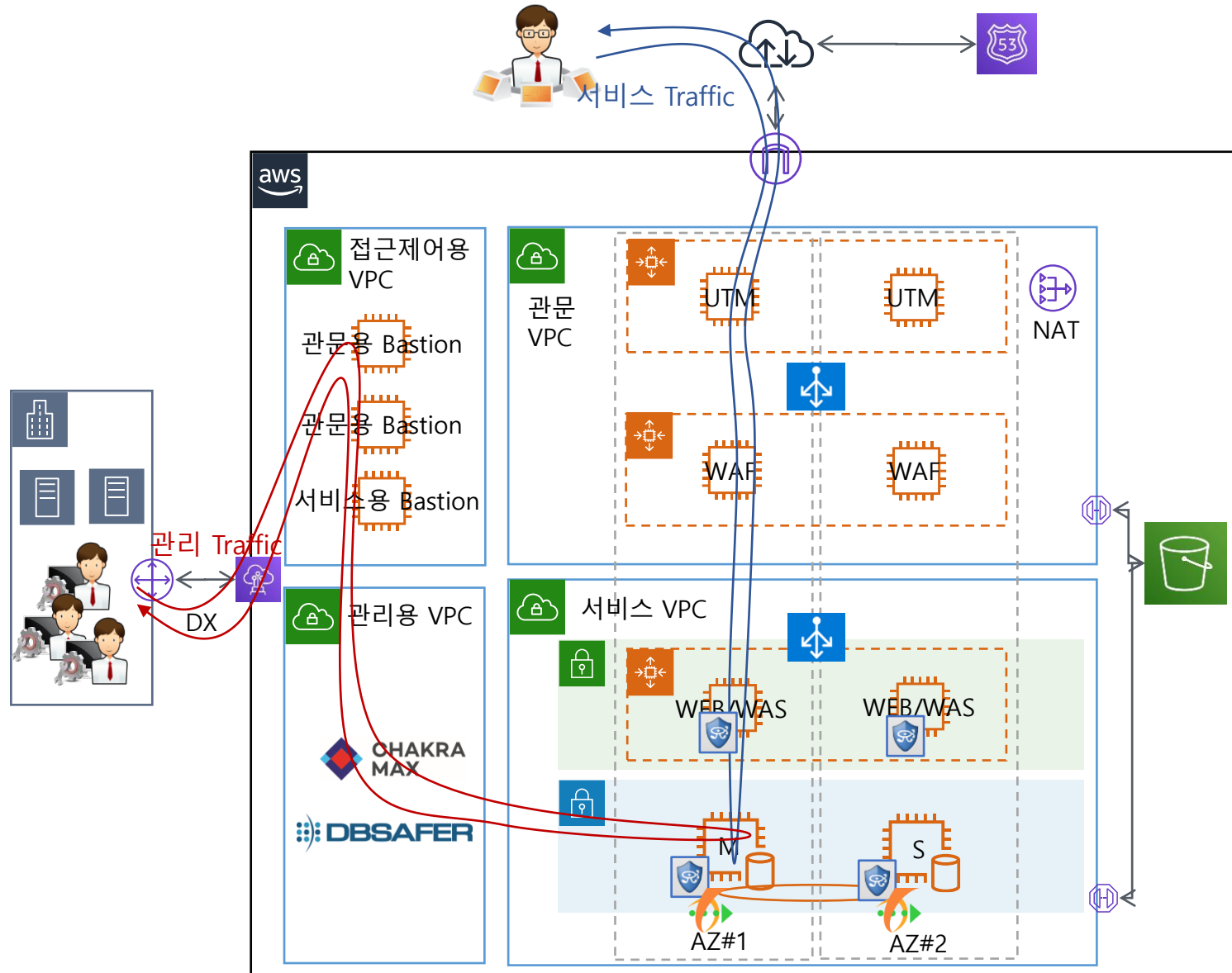
구성 방식

- **게이트웨이 방식**
 - Gateway를 통하여 DB 접근
 - 보안성 및 확장성이 뛰어남
- **Sniffing 방식**
 - 단순 모니터링 구성, 통제가 제한적임
- **Agent 방식**
 - 서버마다 Agent 설치
 - 우회접속 차단유리, 서버 리소스사용

주요 기능

- **접근 통제**
 - 가상계정, IP, APP등으로 접근통제
- **권한 통제**
 - 명령어, Table, Colum 단위로 가능
- **SQL감사/로깅**
 - 모든 SQL 내역 감사, 로깅, 검색
- **분석 및 보고서**
 - 다양한 통계 분석 및 보고서 제공

DB접근제어 구성



클라우드 구성 특징점

다양한 DBMS 지원

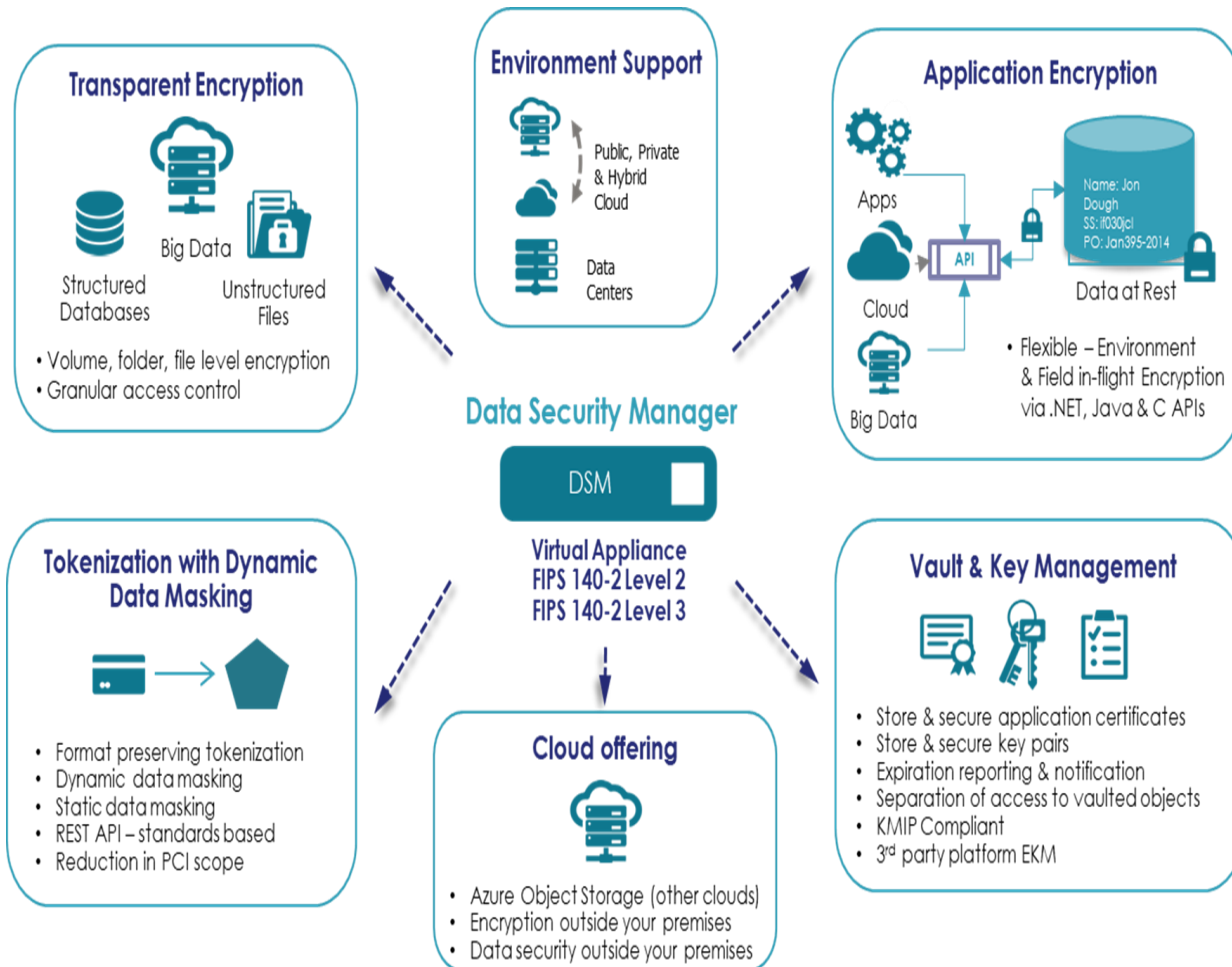
- Oracle/Time-Stan/Exadata, Microsoft SQL Server, IBM DB2 (Mainframe, UDB), SAP Sybase IQ/ASE, SAP HANA, Mysql / MariaDB, IBM Netezza, TeraData, PostgreSQL/Greenplum, Altibase /Tibero/Cubrid/Kairos/SunDB, Amazon RedShift/Aurora, Dameng DM7, Fujitsu Symfoware, PetaSQL, Firebird/Couch/Influx/ Kairos/MongoDB 등 다양한 DBMS지원

Legacy, Cloud 구성 DB 단일통제

- 단일 DB접근제어 관리 서버를 통하여 Legacy, Cloud에 구성된 DB를 통합 관리 가능
- 관리 서버의 위치는 협의 필요

Data(DB) 암호화 소개

“ 정형/비정형 데이터 암호화를 위한 최적의 솔루션 ”



주요 기능 및 특징점

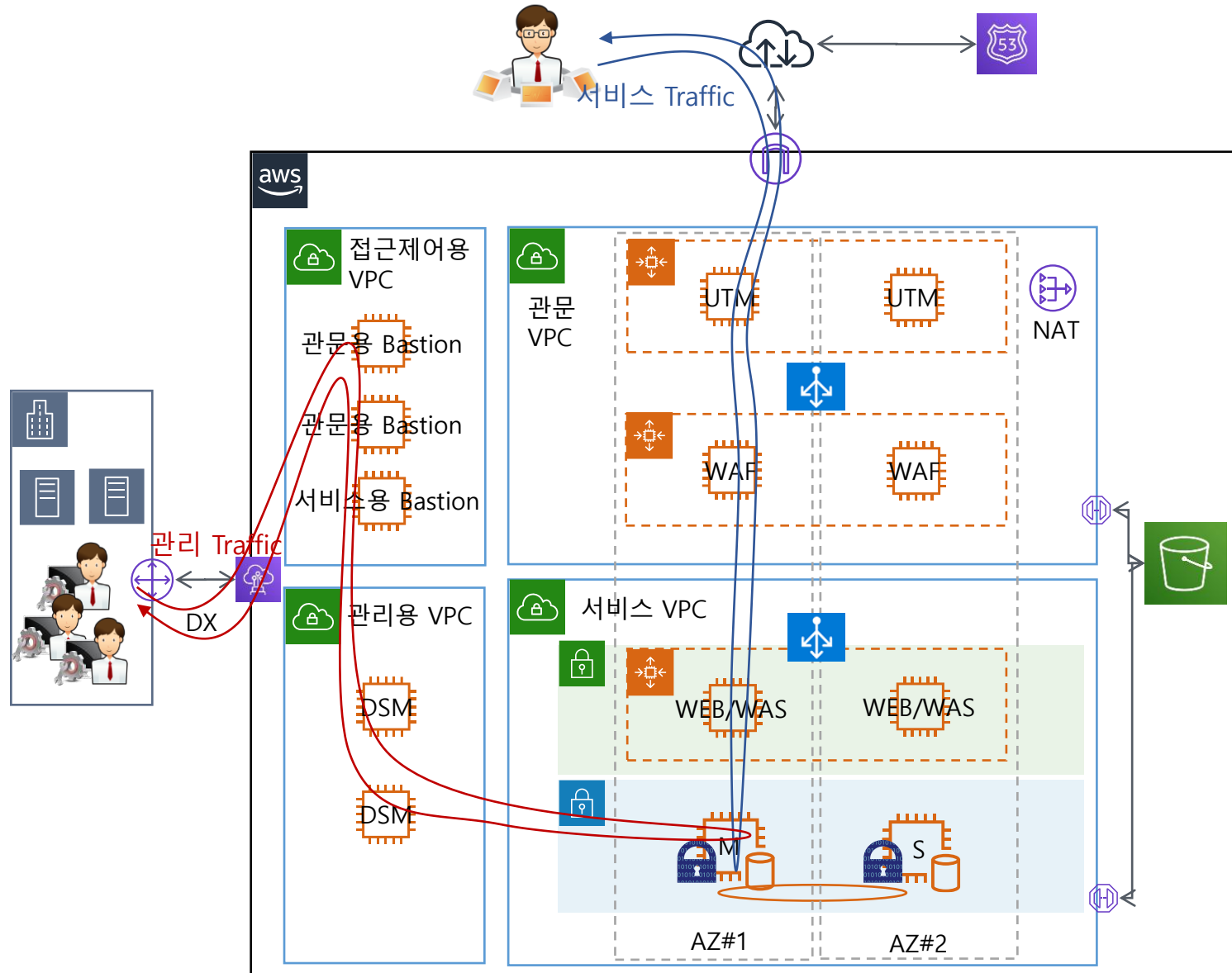
주요 기능

- **파일 암호화**
- 소스 수정없이 DB, Big Data, File 암호화
- **어플리케이션 암호화**
- API를 이용한 필드 단위 암호화
- **토큰화 및 데이터 마스킹**
- REST API를 제공하여 암호화 제공(개인정보 비식별 조치)
- **키 관리**
- 암호 키 및 보안 정책 관리

특장점

- **투명성**
- 어플리케이션 변경 불필요
- 다양한 DBMS 및 암호화 대상 지원
- **강력한 보안**
- 관리자 접근 통제 및 국내외 보안 인증
- **다양한 플랫폼 제공**

Data(DB) 암호화 구성



클라우드 구성 특징점

구성 방식

- DSM 이중화 구성**
 - 정책 및 키관리서버 이중화 구성
 - M/S 구성
 - DSM 장애시 서비스 장애 없음
- 암호화 방식**
 - EC2 DB 및 파일서버에 Plug-in 암호화 솔루션 설치
 - RDS 환경시 WAS/WEB API 제공
- 접근정책 제공**
 - 프로세스, 유저, 리소스 접근통제

I. 개요 및 배경

II. 나우앤클라우드

III. 구성 아키텍처

IV. 회사 소개




회사명	(주) 엘림넷
설립일	2000년 9월 21일
대표자	차현배 / 한환희
본 사	서울 금천구 가산디지털단지1로 205 KCC웰츠밸리14층
자본금	29억원
종업원수	60명
사업분야	인터넷(네트워크/정보) 보안, 비대면 플랫폼 서비스
매출액	416억 원(2020년 IFRS 연결기준)

▶ 주요 보유 기술 현황

프로그램 등록

- | | |
|-----------------------------------|--|
| • 다기능 화상회의 솔루션 NOWNNOW PRIME 100 | 등록번호 2010-01-199-004759 (등록일 2010년 8월 26일) |
| • 웹기반 화상회의 나우앤나우 프라임 웨비나 (Flex버전) | 등록번호 제 C-2013-014443호 (등록일 2013년 7월 16일) |
| • 온라인 설문조사/문제은행 플랫폼 나우앤서베이 | 등록번호 제 C-2013-014568호 (등록일 2013년 7월 18일) |
| • 능동형 웹방화벽 2.0 | 등록번호 제 C-2013-014569호 (등록일 2013년 7월 18일) |
| • 설문조사 솔루션 나우앤서베이 2.0 | 등록번호 제 C-2013-020542호 (등록일 2013년 10월 17일) |

특허 등록

- | | |
|--------------------------------------|------------------------------------|
| • 웹방화벽의 능동적 탐지, 차단을 위한 대응 시스템 및 그 방법 | 특허 제 10-1041997호 (등록일 2011년 6월 9일) |
| • 클라우드 서비스 보안 시스템 및 그 방법 | 특허 제 10-1219662호 (등록일 2013년 1월 2일) |

▶ 주소 사업





elim.net

감사합니다

본사(기존): 서울시 서대문구 경기대로 15 엘림넷빌딩(충정로)
본사(이전 주소): 서울시 금천구 가산디지털1로 205 KCC웰츠밸리 14층 1~7호
가산센터: 서울시 금천구 가산디지털1로 196 에이스테크노타워10차 201호
TEL : 02-3149-4823

elim.net