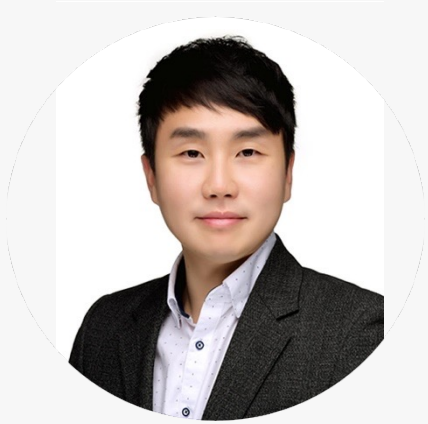
Digital Innovation Enabler

귀사의 보안은 안녕하십니까?

- 클라우드 네이티브 보안구성 전략 (클라우드 보안을 말하다)

LG CNS

발표자 소개



권오훈 책임

주요 약력

- LG CNS DT Innovation 사업부, 보안기술전략팀
- 동국대학교 경영학 박사수료(정보전략 전공)
- 금융 차세대 시스템 보안 구축
- 해외 클라우드 보안구축
- LG그룹(개인)정보보호 진단 및 컨설팅 수행
- KCI 및 정보보호학회지 등 주요 다수 논문 등재

Contents

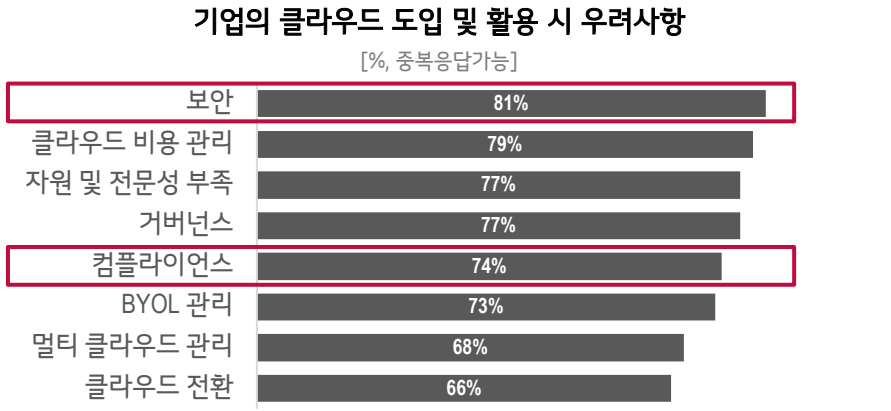
1. 클라우드 보안 소개

클라우드 환경에서 보안은 기존 IT보안과 무엇이 달라지나요?
클라우드 보안은 클라우드 서비스 제공자가 책임져주지 않나요?

클라우드 이용 확대에 따라 클라우드 환경에 맞는 보안 관리가 필요합니다.

클라우드 환경에서의 보안

- **클라우드 서비스 제공자(CSP)와 클라우드 사용 기업의 역할과 책임이 구분되며, 이는 컴플라이언스에도 적용됨**
  - CSP는 클라우드의 보안을 담당 (데이터센터의 물리적 보안 등)
  - 클라우드 사용 기업은 클라우드에서의 보안을 담당 (가상환경 관리 등)
- **클라우드 사용 기업에서 클라우드 환경에 대한 전문성이 부족한 경우가 많음**
  - 클라우드 관리 미흡 및 설정 오류 등

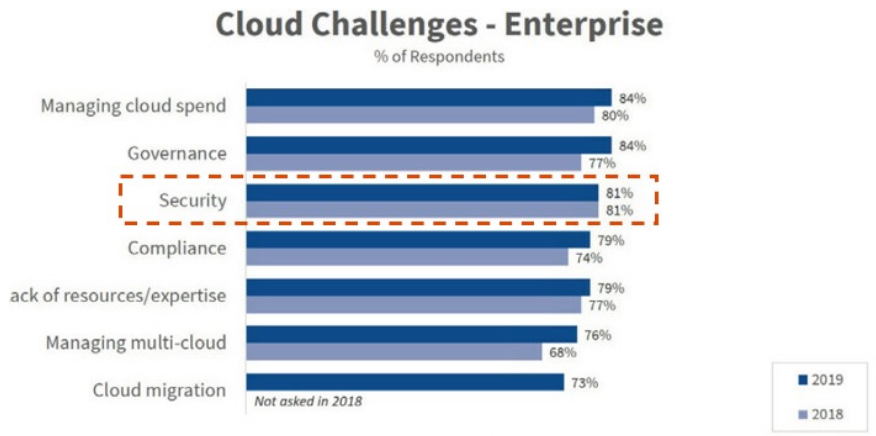


Source: Flexera State of the Cloud Report (2020)

클라우드 전환으로 인해 정보 기반 서비스를 안전하게 제공하는 역량의 중요성이 커지고 있습니다.

유연하고 안전한 비즈니스 환경 구축의 중요성

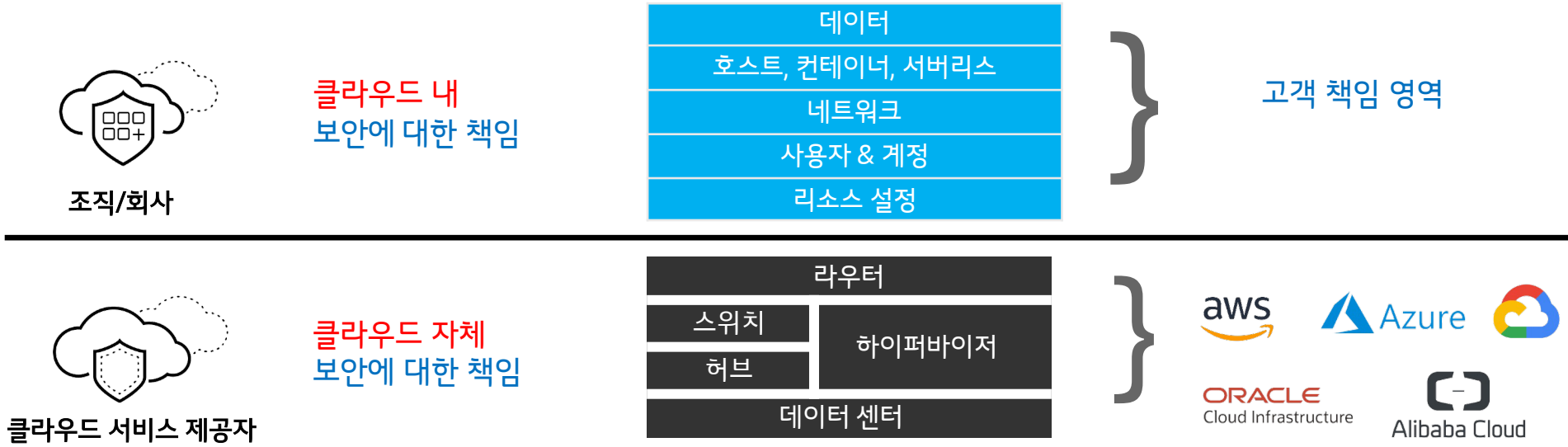
- **고객정보를 활용한 혁신서비스 제공**
  - 새로운 기술과의 효율적인 통합 가능, 시장 변화에 탄력적 대응
  - 마이데이터, AI 빅데이터 분석 기반 개인화 서비스, 오픈뱅킹 서비스
- **정보 보호를 위한 보안의 중요성 부각**
  - 개인정보보호법, 정보통신망법, 신용정보법, GDPR 등 강화되는 법적 규제와 금융위원회, 금융감독원 지침을 준수하는 Compliance 경영



Source: RightScale 2019 State of the Cloud Report from Flexera

‘책임 공유 모델’, 클라우드 보안을 이해하는 출발점

2023년까지 최소 99%의 클라우드 보안 실패는 고객사 잘못에 의한 것 - [Gartner]

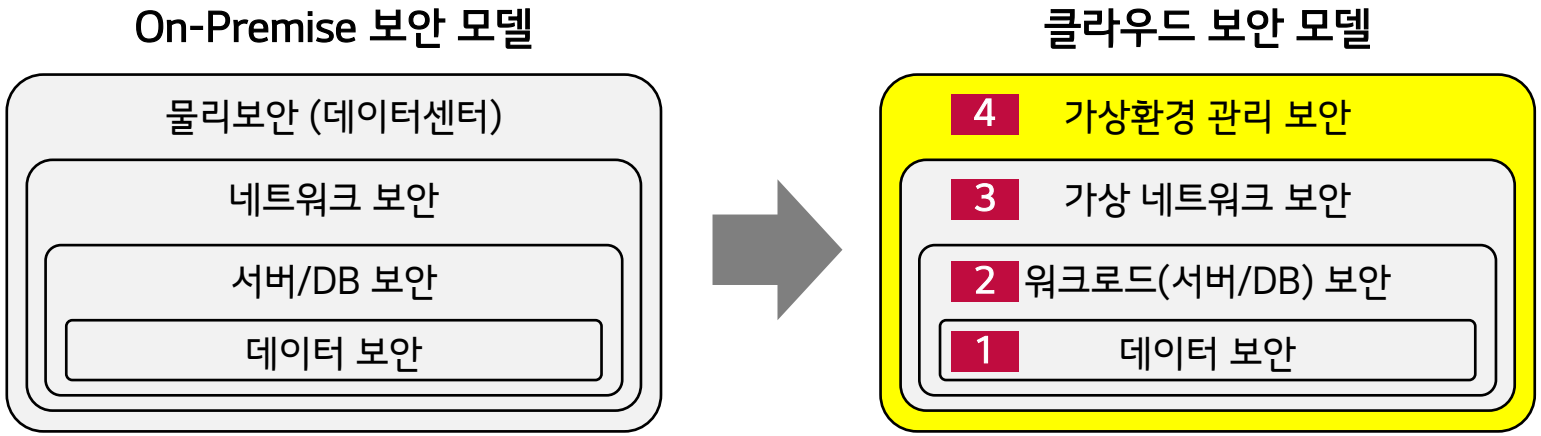


책임 공유 모델	
	인프라 서비스(IaaS)
	플랫폼 서비스(PaaS)
	소프트웨어 서비스(SaaS)

- 클라우드 서비스 제공자는 물리적 데이터 센터, 네트워킹, 서버/호스팅을 책임
- 클라우드 서비스 제공자는 운영체제의 패치 및 유지보수 등 더 많은 책임을 부담
- 사용자는 애플리케이션의 구성 설정 내에서만 변경할 수 있고 그 밖의 제어는 클라우드 서비스 제공자가 담당

※ NIST(National Institute of Standards and Technology) 책임 공유 모델에 대한 정의

- 클라우드 보안은 물리보안 계층이 없는 대신 가상환경 관리 보안 영역이 새롭게 존재합니다.



1	데이터 보안	기존 데이터 보안과 큰 차이는 없으나 암호화 대책 적용 방식에 차이가 있을 수 있음
2	워크로드 보안	서버 보안 뿐만 아니라 최근 많이 활용되는 컨테이너, 서버리스 보안 고려 필요
3	가상 네트워크 보안	SDN(Software Defined Network)으로 네트워크 설정 및 접근통제를 소프트웨어 방식으로 처리
4	가상환경 관리 보안	클라우드 자원 생성 시 각종 보안 설정에 대한 안전성을 점검하는 것이 중요

- **기존 보안 대응체계와 클라우드 보안 대응 체계는 아래와 같습니다.**

❒ 기존 보안 대응 체계

- **중요 정보를 중심으로 겹겹히 보호하는 "성곽 모델"**
- (NW)방화벽 → (NW)침입방지/탐지시스템 → (서버)서버보안 → (데이터) 암호화
- 알려진 공격에 대해 패턴을 비교하여 차단: 백신 등
- 통제된 공간에서 통제된 인원의 통제된 장비만 자원 접근 허용

❒ 클라우드 보안 대응 체계

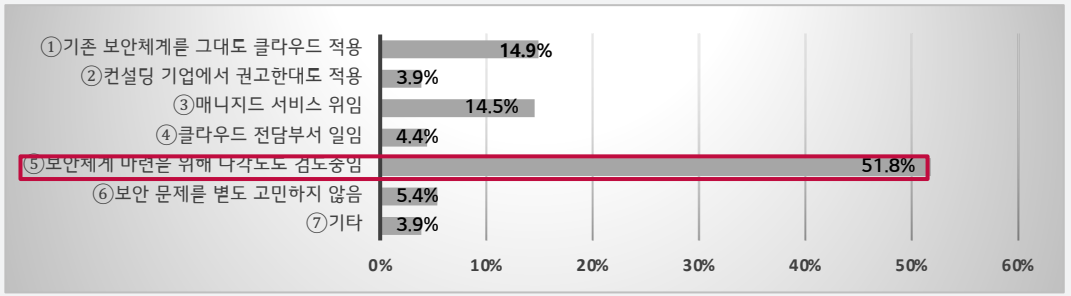
- **보안사고를 "예측하고 선제적으로 대응하여 사고를 예방하는 체계"**
- 보안대상, 위협, 취약점 정보를 실시간 분석하여 위험 가시화
- 사용자/End Point/NW 행위 분석 등 AI 통해 알려지지 않은 공격 식별
- 식별된 보안 위험에 자동 대응 및 사람/기계 공동 대응

2. 클라우드 보안 구성 전략

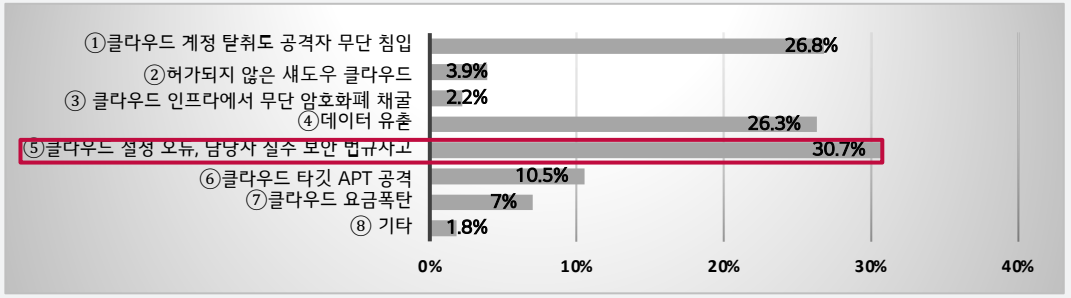
클라우드 보안은 무엇이 중요한가요?

클라우드 보안은 도입하기 위해서는 준비해야 핟 것이 무엇일까요?

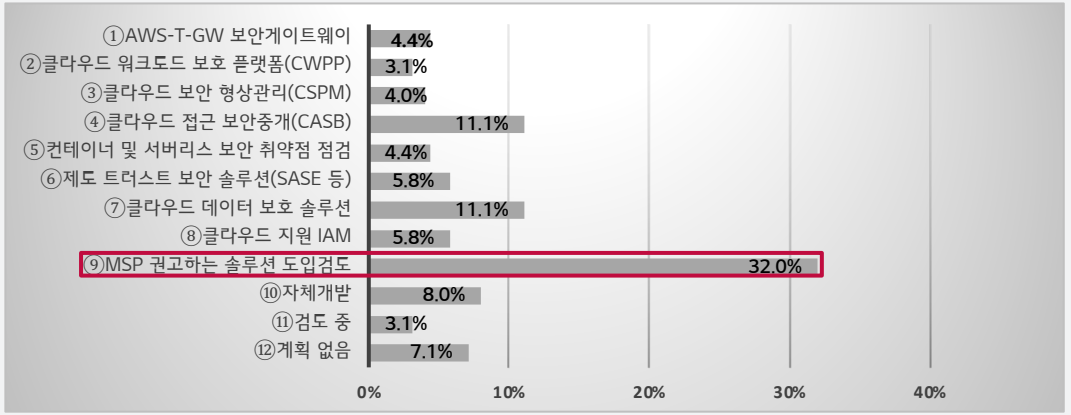
2. 클라우드 보안 구성 전략



【 클라우드 이용 시 보안체계는 어떻게 마련했나 】



【 클라우드 이용 중 가장 문제가 될 수 있는 것은? 】



【 향후 도입 계획이 있는 보안 솔루션은? 】

출처: 네트워크 타임즈 보안 담당자 설문조사(2020)

클라우드 보안 담당자의 고민

"Cloud IT Safety"

- 클라우드에 대한 '인프라 · 기술 · 보안서비스 · 관련 법규' 등 이해 필요
- Public 클라우드 사용 시, CSP 정보보호 역할, SLA, Native 보안서비스 이해 필요

"Compliance Activity"

- 클라우드 사용에 대한 Compliance 기준 부재
- 클라우드 사용에 대한 정책 · 지침 · 가이드 제정 및 개정 필요
- 클라우드 환경에서의 개발환경에 대한 관리방안 부재

"Cloud Security Solution"

- 보안위협, 필요 기능, 해결할 수 있는 최적의 보안솔루션 이해
- 가시성 확보를 통해 취약 설정 한눈에 파악

2. 클라우드 보안 구성 전략

- 클라우드의 장점인 민첩성과 확장성을 최대한 보장하면서도 안전한 서비스를 구현해야 합니다.

클라우드
보안담당자

- Cloud IT Safety — 클라우드 환경에 최적화된 보안 설계
- Compliance Activity — 정보보안 규제 준수 여부 모니터링
- Cloud Security Solution — 최적의 보안솔루션 이해

"손쉬운 보안 운영 및 관리"

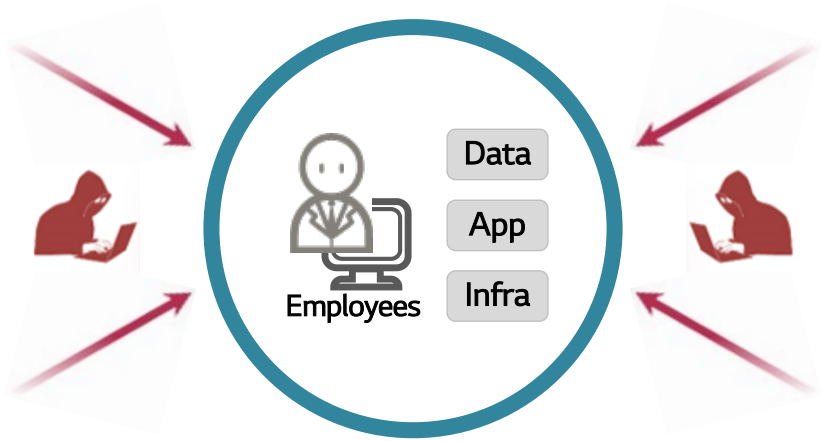
- 한번에 "투자" 보다는 사용한 만큼 비용을 내는 클라우드 장점 활용
- 컴플라이언스 준수 현황에 대한 가시성 확보
- 사각지대 미발생 대책 우선 고려
- 지속적인 개선을 통한 자동화 구현으로 업무 효율성 극대화

클라우드 Native 보안 서비스를 최대한 활용하여 클라우드의 장점을 극대화해야 합니다.

보안 환경 변화에 따른 제로 트러스트 재조명(1/3)

보안 환경 변화

기존(On-Premise)

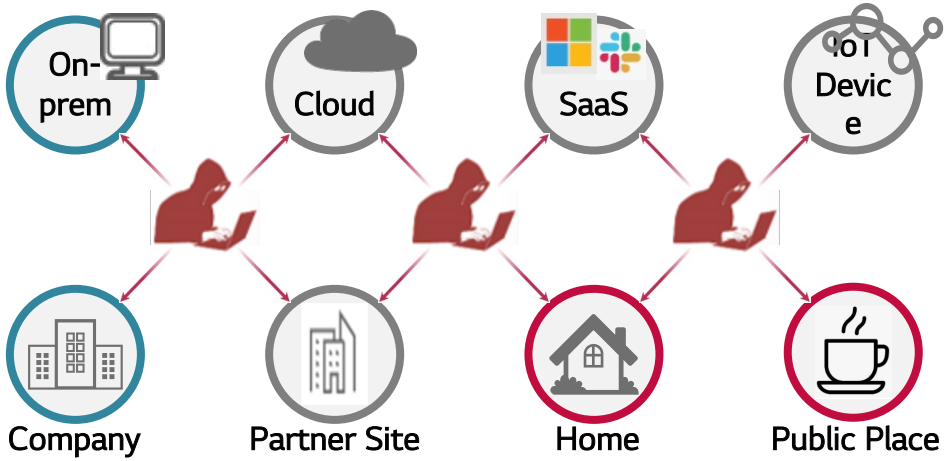


사용자 · 자원은 네트워크 경계 내부에 존재

✓ **중요정보를 중심으로 겹겹이 보호하는 "성곽 모델"**

- 방화벽, IPS, 웹방화벽 등 네트워크 경계 보안에 집중
- 경계를 중심으로 사고를 예방하는데 초점

현재(Cloud)



사용자 · 자원 · 보안 위협은 어디에나 존재

✓ **환경 변화에 대응하기 위한 새로운 보안모델 필요**

- 보호 대상 자원이 내부에만 존재하지 않아 보안관리 범위 확대
- 새로운 기술 및 서비스 이용 요구 증대로 보안통제 대상 확대
- 취약한 고리를 대상으로 표적형·지능형 공격 증가

보안 모델 변화에 따른 제로 트러스트 재조명(2/3)

환경, 기술 변화

보안 관리 범위 확대	**클라우드, SaaS 서비스 등 이용 증가** (자원의 물리적 위치 중요하지 않음)
	재택, 외부 협업에 따른 외부 네트워크에서 접속 증가 (사용자 접속 위치를 특정할 수 없음)
보안 통제 대상 확대	**새로운 기술, 서비스 폭발적 출시** (급변하는 기술, 서비스를 이해하는데 한계 존재)
	다양한 외부 기술, 서비스 사용에 대한 요구 증대 (모든 보안 위험 파악 후 대응 불가)
표적형 지능형 공격 증가	**사용자 디바이스에 대한 표적형 공격 증가** (디바이스를 거점으로 내부 시스템에 대한 공격 확산)
	지능형 공격 증가로 보안 사고 탐지 어려움 (피해 발생 후 보안 사고 인지)

보안 모델 변화 필요 (성곽 모델 → 제로 트러스트 모델)

내·외부 네트워크 경계가 아닌, 새로운 신뢰기반의 경계 구성

✓ 네트워크 장비 기반 물리적 세그멘테이션

➡ 소프트웨어 기반 **논리적 세그멘테이션** 필요

최소권한 부여, 신뢰가 검증된 주체만 접근을 허용하여 공격 발생 가능성 ↓

✓ 네트워크 중심의 세그멘테이션

➡ 서비스 중심의 **마이크로 세그멘테이션**

✓ 사용자 계정 중심의 신뢰 검증

➡ 다양한 정보를 바탕으로 **복합적, 동적 판단**에 기반한 신뢰 검증
사용자 속성, 위치, 기기 보안상태, 보안위협 등

공격 발생 시 신속한 탐지 및 복구를 통해 사업 연속성 유지

✓ 네트워크 경계에서 발생하는 로그 중심으로 보안 위협 대응

➡ **접근주체, 자원에서 발생하는 행위** 중심으로 보안 위협 대응

시장 동인

보안관리 범위 확대

- 클라우드로 기반 서비스 채택 증가로 보호대상이 내부 네트워크에 국한되어 존재하지 않음
- Covid19 이후 재택근무 증가로 외부 네트워크에서 내부 시스템에 대한 접근이 다수 발생

→ **기존의 내·외부 네트워크 경계가 아닌, 새로운 신뢰기반의 경계 필요**

표적형 공격 증가

- 취약한 고리 중 하나인 사용자 디바이스에 대한 표적형 공격 증가
- 사용자 디바이스를 거점으로 내부 시스템에 대한 공격 확산

→ **보안이 담보된 디바이스만 접근 허용**

Biz. 환경 변화

- 비즈니스 민첩성이 강조됨에 따라 사전에 모든 보안위험 파악 후 예방하는 것은 불가능

→ **보안사고 발생 시 피해 최소화를 위한 공격 표면 최소화 필요**

제로 트러스트 아키텍처 구현

- 클라우드 기반 서비스 채택 증가로 제로 트러스트개념을 구현하기 위한 확대
- 제로 트러스트 아키텍처의 주요 보안요건
  - 네트워크 위치에 관계없이 **신뢰하는 사용자와 디바이스만 접속** 허용
  - 모든 자원에 대한 요청은 **접근권한** 검증 후 허용
  - 발생하는 모든 사용이력은 저장, 모니터링, 분석되어 가시성을 제공하고 보안상태 유지

[제로 트러스트 아키텍처 개념]

- 발생하는 보안 위험 유형에 대해 식별, 예방, 탐지, 대응 및 복구 절차를 고려하여 구성 합니다.

❖ NIST Cybersecurity Framework에 따른 보안 대책

구분	Identify (식별)	Protect (예방)	Detect (탐지)	Respond (대응)	Recover (복구)
Controls	• 자산 관리	• 인식 통제	• 이상징후	• 대응 계획	• 복구 계획
	• 사업 환경	• 인식 제고/교육	• 보안 관제	• 의사소통	• 개선
	• 거버넌스	• 데이터 보안	• 탐지 절차	• 분석	• 의사소통
	• 위험 평가	• 보호 절차		• 위험 감소	
	• 위험 관리 전략	• 예방 기술		• 개선	
AWS Security	• Security Hub • Control Tower • Trusted Advisor • Service Catalog	• Shield • Network Firewall • WAF • Security Group • IAM • KMS • CloudHSM • Certificate Manager • Single Sign-On	• GuardDuty • Macie • Inspector • Config • Security Hub • CloudTrail • CloudWatch	• Systems Manager • Lambda	• Snapshot • Archive • S3 Glacier

3. 클라우드 보안 구축 사례

LG CNS 만의 독보적인 역량으로 구축된 클라우드 보안 구축 사례가 무엇이 있을까요?

3. 클라우드 보안 구축 사례

- LG CNS의 클라우드 보안 역량을 바탕으로 컨설팅, 기술자문 등 클라우드 전문 보안서비스를 오퍼링합니다.

클라우드 보안 전 영역에 컨설팅, 서비스, 구축 및 관리를 통해 비즈니스 가치 제공

보안 컨설팅	- 고객사에 최적화된 클라우드 정보보안 모델을 제시하여 선진 클라우드 정보보호 체계 마련 - 금융 클라우드 보안 컴플라이언스, 클라우드 마이그레이션 보안체계 수립, 클라우드 환경 ISMS-P 인증 등
보안 솔루션	- 클라우드 환경에 대한 보안 설정을 점검하고 조치할 수 있는 자체 개발 솔루션 제공 - AWS, Azure, GCP 클라우드 보안 설정 점검 - 국내 개인정보보호법 등 컴플라이언스 기준
설계 및 구축	- 내.외부 발생하는 보안 위협에 대응하기 위한 클라우드 보안 시스템 설계 및 구축 - 클라우드 Native를 이용한 보안체계 구축 - 클라우드 전용 보안솔루션 선정 및 구축(CSPM / CWPP / CASB / ZTNA / SASE 등)
관리형 보안 서비스	- 해킹 / 악성코드 등 외부 위협을 실시간 감지 및 대응할 수 있는 관제 운영 서비스 - 24 *365 보안 관제 서비스 - 클라우드 Native 서비스 보안 운영/관제 - 클라우드 전용 보안 솔루션 보안 운영/관제(CSPM / CWPP / CNAPP 등)

3. 클라우드 보안 구축 사례

Cloud Security Consulting | Cloud Security Solution | Cloud Security Implementation | Cloud Managed Security Service

주요 내용

고객사

- 국내/외 유통 서비스

요구사항

- 클라우드 환경 내, 고객사의 데이터 손실 최소화
- ISMS-P 요구사항에 따른 컴플라이언스 점검 필요
- 클라우드 보안 관련 정책 및 표준 확립
- 클라우드 환경에 적합한 보안 관리체계 구현
- 애플리케이션 현대화(AM) 체계 수립

주요 Task

- 클라우드 환경의 ISMS-P 기준의 보안 컨설팅
  - 보안 인증 통제항목 기준
  - 보안 가이드 수립, 정책 개정
  - 현황 점검, 개선방안 수립 등

특이 사항

- 클라우드 관련 정책서 지침 등 문서 부재
- 클라우드 자산에 대한 분류체계 미수립

Lesson Learned

- 컨설팅 세부 Task 중 정보 자산 식별이 기존 컨설팅에서는 현행화가 일부 잘 진행되지 않아 어려움을 많이 겪었으나 **클라우드 환경에서는 리소스 태그 에디터 등 서비스를 통해 사용하기가 용이** 하였음
  → 하지만, 자산의 중요도를 평가하는 측면에서는 스냅샷으로 찍어야 하는 부분이 어려움이 있었고 클라우드에 대한 레퍼런스가 **부족하여 ISMS-P 자산 관리의 본질을 잃지 않기 위해, 서비스 자체 Flexibility를 고려해 회사 특성에 맞도록 자원 관리 방안을 수립**해야 했음

- 클라우드 환경은 On-Premise 같이 특정 1대의 서버에 대한 중요도 평가가 이루어질 수 없고, Auto-scale 방식에 따라 서버의 생성/중지가 빈번히 발생하기 때문에 **'관리 절차' 에 대해 고려를 많이 함**
  → (예시)자원 그룹별 관리자/관리 부서가 존재하는지, 불필요한 인스턴스를 삭제하는 점검 체계가 갖추어져 있는지, 주기적으로 네이밍 규칙을 통해 관리하고 있는지 등

Cloud Security Consulting | Cloud Security Solution | Cloud Security Implementation | Cloud Managed Security Service

주요 내용

고객사

- 총 50여개 기업 및 300여개 프로젝트 도입
- L그룹사 (제조/화학/유통/서비스) 및 대기업 (금융, 항공 등) 및 중소규모 스타트업 등

요구 사항

- 컴플라이언스 보안 요건 기준으로 보안설정 점검
- 취약한 서비스 설정을 식별하고 개선
- 클라우드 보안 가시성 확보 및 중앙 집중화 필요
- 최신 사고사례를 반영한 지속적인 점검항목 업데이트

주요 Task

이름	LG CNS CAT (클라우드 보안 취약점 점검 솔루션)	
대상	AWS, Azure, GCP 자원 모니터링 및 취약점 점검	
범위	• 공통 : IAM • OS : EC2 • DBMS : RDS	• Storage : S3 • N/W : VPC 등
항목	• COMPUTING (디스크 Volume 암호화 적용 여부 등) • DATABASE (저장 시 암호화 적용 여부 등) • MANAGEMENT (감사로그 설정 등) • NETWORKING (내부 접근 시 ACL 체크 여부 등) • SECURITY (Root 계정 사용 여부 / MFA 미설정 등) • STORAGE (오브젝트 스토리지 접근 로그 생성 설정 등)	

Lesson Learned

- 최근 취약점 점검은 체크리스트 기반으로 2-3Day 걸쳐 점검 인력이 수동으로 직접 수행하였으나, **클라우드 자동화 점검 도구 도입 후, 점검 자체가 최소 5분 이내로 종료됨**
  → 자동화 점검 도구를 통해 빠른 리포팅 산출, 수동 점검 대비 2배 이상 신속한 점검이 가능하였고 주기적으로 발생하는 반복 업무 및 수행 리스크가 감소됨(예. 스크립트 수정, 환경변수 변경 등)

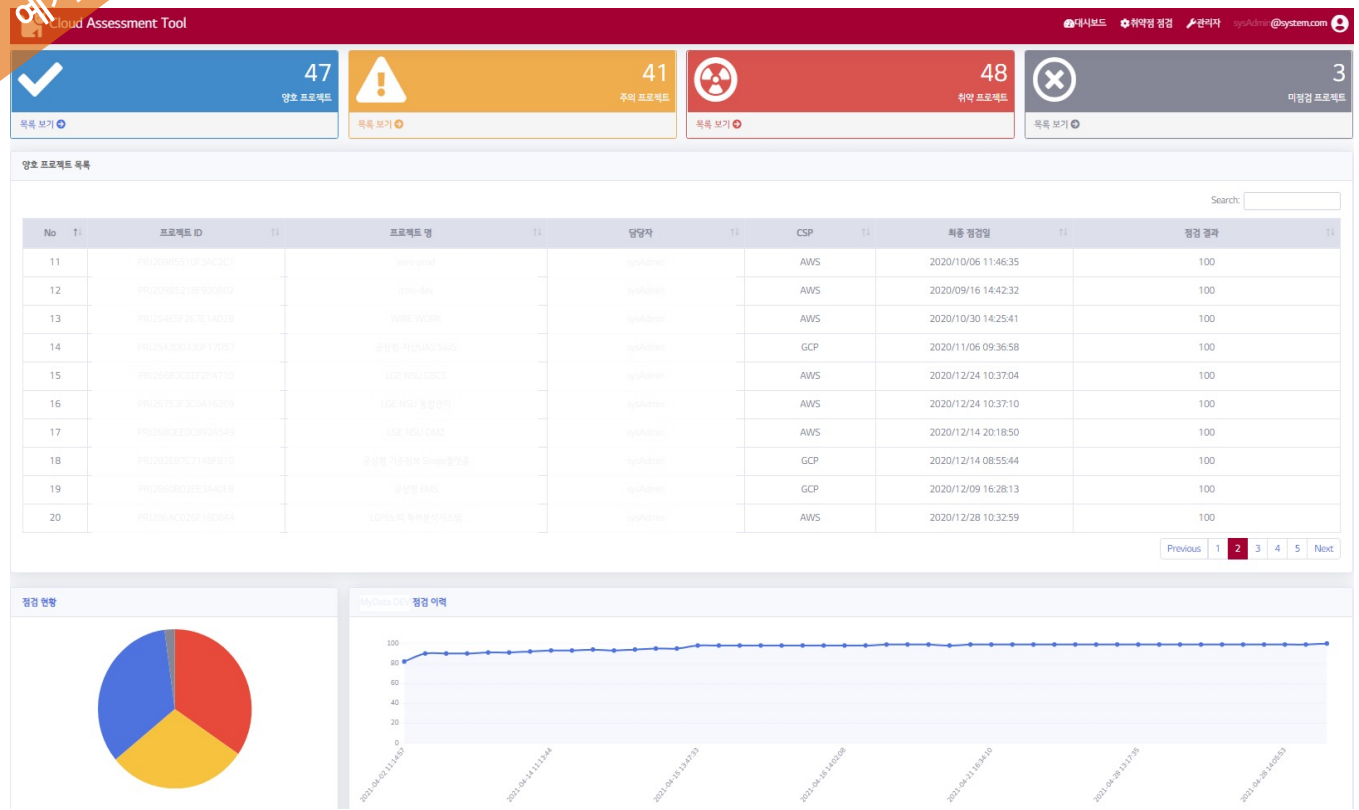
- 프로젝트 남은 잔여 시간을 더 중요한 개선 가이드 작성 할당 및 제공하는데 집중할 수 있어 **산출물(가이드 문서, 취약점 점검 결과 리포팅 등)에 대한 품질을 높일 수 있었음**

- 클라우드 자원 체계에 대한 효율적인 가시성 확보를 통해 **즉각적이고 지속적인 모니터링 수행 및 대응이 가능**하였고 **중앙 집중화 관리를 통해, 높은 보안 수준을 유지**하였음

Cloud Security Consulting | **Cloud Security Solution** | Cloud Security Implementation | Cloud Managed Security Service

- LG CNS의 'CAT(Cloud Assessment Tool)'을 활용하여 클라우드의 보안 설정을 점검하고 조치합니다.

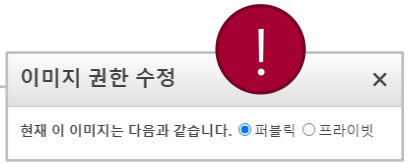
예시



AWS에서 자주 발생하는 취약한 설정들

S3 Bucket을
Public Access로 설정하는 경우

서버 이미지에
Public 접근 권한을 부여하는 경우



방화벽 In-bound Rule을
Anywhere로 선택하는 경우

Cloud Security Consulting | Cloud Security Solution | **Cloud Security Implementation** | Cloud Managed Security Service

주요 내용

고객사	• 해외 E-Commerce 차세대 클라우드 시스템 Open • 기존 On-Prem.에서 AWS Public 클라우드 전환 프로젝트
요구사항	• 클라우드 법적 요건 검토(CCPA, CIS/BP 사례 등) • 보안 솔루션 신규 도입 및 구축 • Public Cloud 전환 시 인프라/서비스별 보안 취약점 식별 및 조치
주요 Task	• Global 보안 표준 수립 - CIS, AWS BP 근거하여 보안 표준 수립 - Security Hub 구성 • 3rd Party / Native 보안 솔루션 구축 및 정책 구성 - SASE / UTM / WAF / SIEM • AWS Native 서비스 취약점 점검 - Inspector, Config 를 통해 취약점 최소화
특이 사항	• AWS Native 서비스 탐지정보 부정확: WAF, Inspector 등 소수 오탐 항목 발생 • 오픈 시점 전, 라우터 설정 오류로 인한 미 동부 Region 서비스 다운, DDoS 공격 증가

Lesson Learned

- '보안책임공유모델 ' 에근거한안전한클라우드설계및구축을수행하였으나오픈며칠전,AWS 라우터설정오류로인해미동부리전서비스가다운됨(영향도:콘솔/CLI 접속불가등)
  → AWS 장애전담팀에서위협도에따라 **Critical(15min)/High(1Hr)/Medium(4Hr)/Normal(12~24Hr) 빠르게구분**하고AWS Chime에서함께실시간원인식별및대응을빠르게지원해주었기에,신속한 조치를수행할수있었음(w/AWS 장애전담담당자,프로젝트담당자,고객사)

- 구축진행중,오픈시점에DDoS 공격(Flooding)이증가하여서비스이용이느려졌으나AWS WAF 선제적대응
  → WAF 정책내과다패킷흐름을조절해주는Rule과3rd Party에서 **제공하는룰서비스를적극 활용하여트래픽양을감소시킬수있었으나,구독비용이크다는단점**이있음

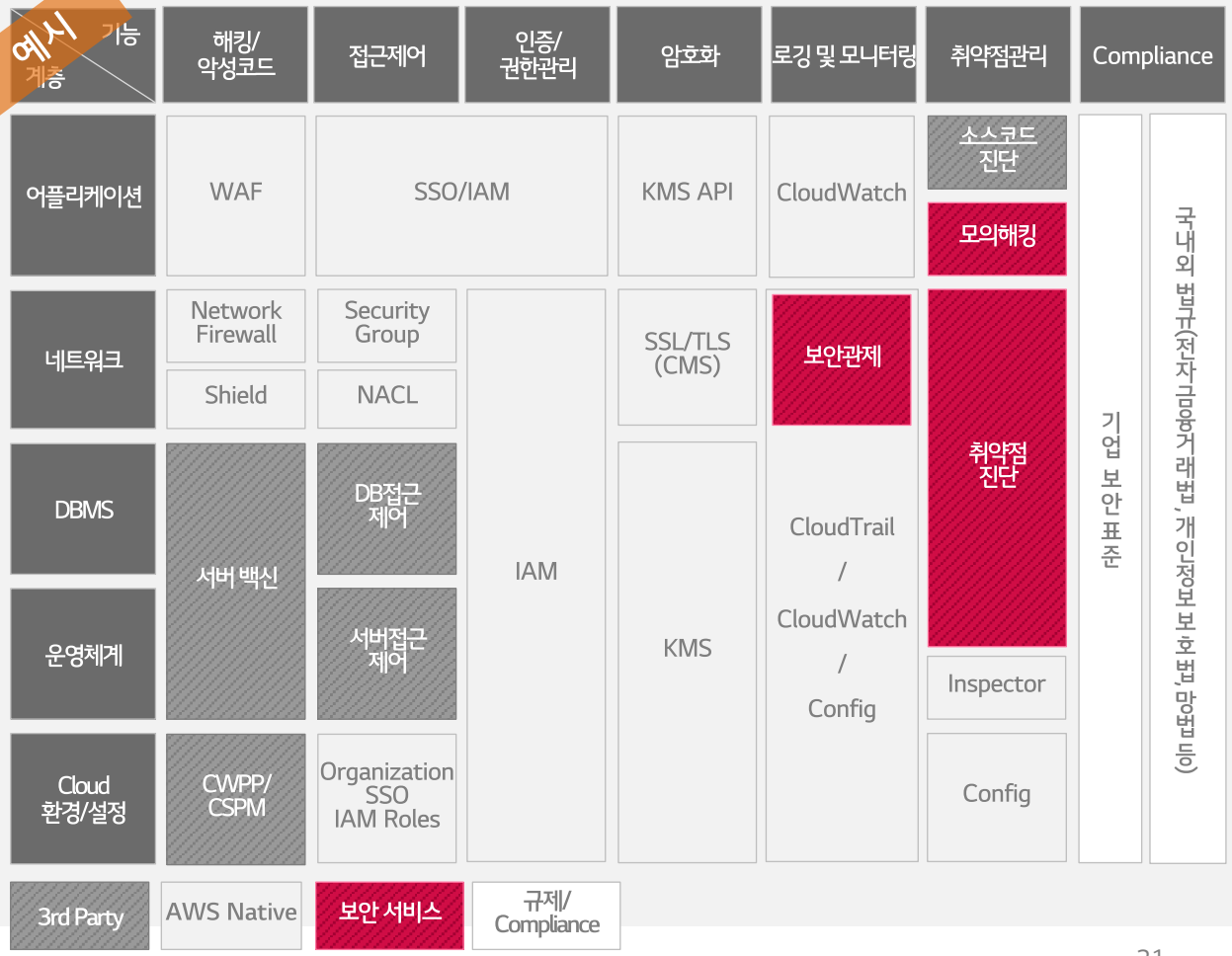
- AWS Config(자원변경점검)에서IP 노출이취약항목식별이기에DNS 변환작업을수행함(실제 Route53에서도메인네임등록작업을진행)
  → **AWS Shield 서비스(DDoS 탐지)와Route53을연계하기위해도메인네임작업은필수고려사항임**

- 구축에서는기존On-Prem. 보안솔루션이그대로클라우드에적용된경우가많지않음
  → 지원되는솔루션이있더라도 **기존IP 통제를도메인네임기반통제로변환하기위해솔루션에 적용되는보안정책을새롭게Re-Design 해야함**.이부분은반드시고려되어야함

3. 클라우드 보안 구축 사례

Cloud Security Consulting | Cloud Security Solution | **Cloud Security Implementation** | Cloud Managed Security Service

- 클라우드 환경도 기존 On-Premise 환경과 유사하게 전체 보안 아키텍처 관점에서 접근해야 합니다.



Native 보안 서비스 우선 적용

- 최소한의 클라우드 보안통제를 위한 기본 Baseline 설정
  - 필수 보안기능 활성화 (예: CloudTrail)
- 글로벌 클라우드 서비스 제공자의 Threat Intelligence를 최대한 활용할 수 있는 Native 보안 서비스 적용 (예: GuardDuty)

3rd Party 솔루션은 반드시 검증

- 국내 컴플라이언스 요건을 충족하기 위해서는 3rd Party 보안 솔루션이 필요하므로 도입 전 반드시 적용 가능성 검증
  - VM 위에 설치 가능한 소프트웨어 방식 솔루션인가?
  - 수시로 변경되는 IP가 아닌 도메인 기반 통제가 가능한가?
  - Auto Scaling 등 자원 변화에 유연하게 대응할 수 있는가?

Cloud Security Consulting | Cloud Security Solution | Cloud Security Implementation | Cloud Managed Security Service

주요 내용

고객사

- L그룹사 (제조/화학/유통/서비스) 및 대기업 (금융, 항공 등) 및 중소규모 스타트업 등

요구사항

- 클라우드 환경의 24*365 모니터링을 통해 위협에 대한 신속한 대응 필요
- 외부 보안 위협에 대해 사전 차단을 하여 안정적인 내부 인프라 운영

주요 Task

- 보안솔루션 모니터링 및 실시간 탐지를 통해 위부 위협 및 공격정보를 고객에게 제공

이벤트 수집	탐지	이벤트 확인/분석	후속 대응
• 방화벽, IPS, 웹방화벽 등 보안 장비 로그 설정 • SIEM을 통한 보안 장비 로그 수집	• 모니터링 조건 설정 • 외부 공격 확인 시 이벤트 발생	• 이벤트 내용 확인 및 정/오탐 분류 • 공격 유형 및 내용 분석	• 공격 시도에 대한 고객사 메일링 • 조치 대응 지원

구분	보안장비/솔루션
3rd Party 보안장비	• UTM, IPS, 웹 방화벽, HIPS 등
클라우드 Native 보안 솔루션	• AWS WAF, GuardDuty 등
클라우드 전용 보안 솔루션	• CSPM, CWPP, CNAPP 등

Lesson Learned

- 운영/관제는 이미 운영되고 있는 3rd Party 보안 솔루션에 대한 보안관제는 기존과 크게 다를 것이 없음
  → 하지만 중요한 건 클라우드 네이티브에 대한 보안관제임. 실제 공격이 클라우드 내 올라간 가상서버(EC2 등)에도 들어오긴 하지만 그보다 확장된 공격표면인 클라우드 자체에 대한 공격도 빈번함.
  → 이런 부분에 대한 모니터링/관제가 되지 않으면 실제 공격이 들어오는지 안 들어오는지 모를 수 있으니 주의 해야 함

4. LG’s Values

LG CNS의 클라우드 보안 서비스에는 어떤 것이 있나요?

Why LG CNS?

보안 컨설팅, 보안 시스템 구축, 솔루션 공급 및 보안 관제를 포함하는 토탈 보안 서비스를 제공합니다.

Core Competency

- 사이버보안 및 물리보안을 통합한 융합보안 구축 역량 및 솔루션 보유
- AI빅데이터, IoT, 클라우드 등 신기술을 활용하거나 스마트팩토리 등 신기술 서비스 보호를 위한 보안 프레임워크 구축
- 보안 컨설팅, 구축, 운영 등 전 영역을 경험한 다수의 보안 경력 10년 이상의 보안 전문가 확보

Certification

- AWS Security Consulting Competency 인증 ('20)
- KISA 보안관제 전문기업 지정
- KISA 공공 클라우드 보안 인증 – LG G-Cloud ('18)
- 정보보안 경영체계 국제규격 ISO 27001 인증 ('13)

aws partner network
Consulting Partner
Security Competency

글로벌 CSP와의 파트너십

aws
Microsoft Azure
Google Cloud
ORACLE CLOUD

Digital Innovation Enabler

Thank You