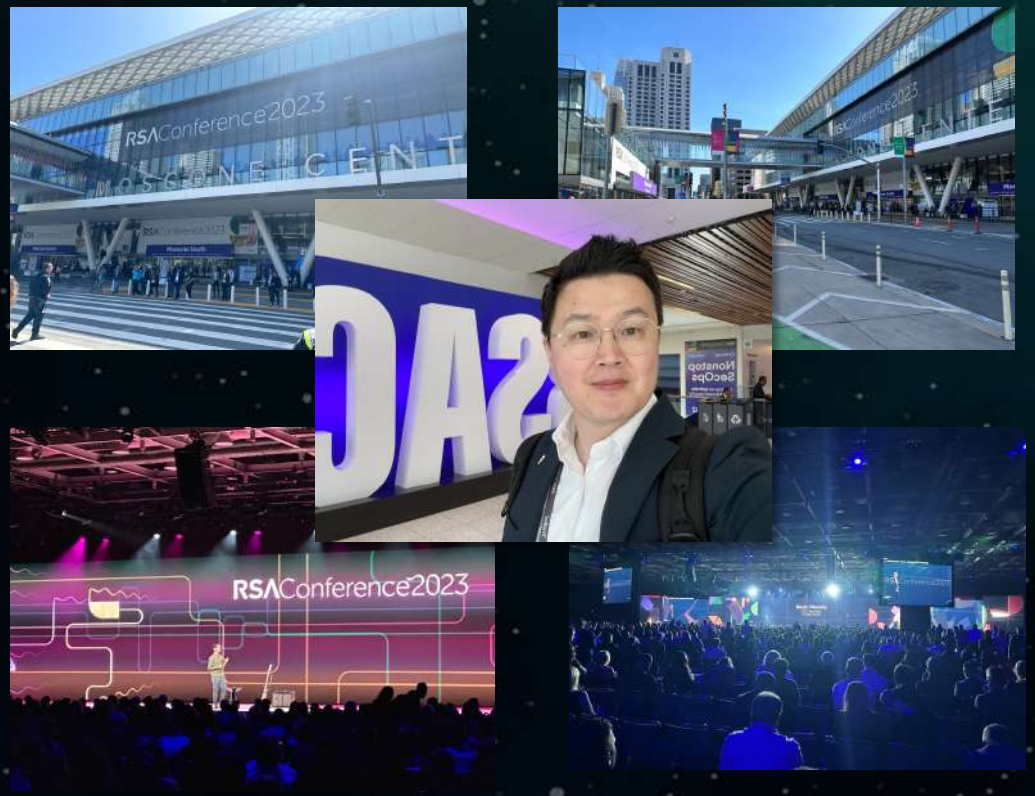
BESPIN GLOBAL

Zerotrust의 효과적인 구현 방안 및 베스트 프랙티스

정 현 석 상무, BESPIN GLOBAL

OpsNow Security

ZeroTrust, Cloud Native Security, XDR, DevSecOps, SaaS



RSAC 2023

Stronger Together

Security Product은 SW넘어 Cloud화

달라진 보안의 위상

Stronger Together(보안 집단지성)

복잡한 보안 서비스와 인력부족 문제

보안 글로벌 표준 중요

라스베가스 MGM 리조트, 해킹으로 인해 1억 달러의 피해 예상

Source : ADVFN

All ALPHV 라는 랜섬웨어 그룹에서 직원인척 사칭, MGM에 연락을 해 관리자 암호를 구두로 넘겨 받아 10분만에 해킹

이 해킹으로 인해 고객들의 연락처, 성별, 생년월일,
운전면허번호 등 개인정보가 유출
카드키, 슬롯머신, ATM 등 일주일 시스템 마비
기업의 근간이 흔들림
보안 SW 100개 이상 활용 중

ZDNet Korea

클라우드공격 630% 증가, 클라우드앱 노린 사이버 공격 6배↑

코로나19 확산으로 클라우드 기반 서비스 이용이 높아지면서 이를 노린 사이버 공격이 6배 이상 증가한 것으로 조사됐다.

미국 지디넷은 최근 사이버보안 업체 맥아피의 클라기반 서비스 사이버 보안 관련 리포트를 인용해 보도했다. 해당 보고서에 따르면 지난 1월부터 4월까지 클라우드 기반 서비스를 타깃으로 한 원격 공격은 630% 증가했다.. 이 보고서는 맥아피 이용자 3천만명에 대한 데이터를 기반으로 조사됐다.

물리적인 설비 설치 없이 컴퓨팅 인프라를 유동적으로 확장할 수 있는 클라우드 기반 앱 서비스가 각광을 받고 있다. 코로나19 확산 방지를 위해 회사들이 갑작스레 원격 근무를 시행하면서 화상회의, 협업툴 등 클라우드 기반 앱을 업무에 도입하는 추세다.

맥아피 클라우드 보안 담당 라지브 굽타 수석 부사장은 "코로나19 확산을 극복하기 위해 모두가 엄청난 노력을 들이고 있지만, 클라우드 앱 사용 증가세를 이용하려는 해커들도 늘었다"고 지적했다.

출처 : 지디넷

아주경제

IBM "한국기업 데이터유출 피해, 1곳당 41억"...4년간 늘어

전세계로 코로나19 확산이 진행되는 사이, 한국 기업들 1곳당 41억원 이상의데이터 유출 피해가 발생한 것으로 나타났다.

IBM시큐리티와 포네몬연구소는 작년 5월부터 올해 3월까지 세계 500개 기업이 1000~10만건 규모의 실제 데이터 유출을 경험한 사이버침해사고 조사내용을 분석한 결과를 2일 발표했다.

코로나 기간 동안 전세계 보안사고 관련 비용은 전년대비 10% 증가했다. 기업들은 사고당 평균 424만달러의 손실을 입었다. 17년동안 진행된 이 조사 이래 최대 규모였다. 또, 데이터유출 사고로 한국 기업이 입은 평균 손실 액수는 41억1000만원이었다.

한국IBM은 "조사 대상 한국 기업들의 손실 규모는 4년간 꾸준히 증가하는 추세"라면서 "인공지능(AI)과 하이브리드클라우드, 제로트러스트 접근방식을 통해 데이터유출 비용을 절감할 수 있다"라고 밝혔다.

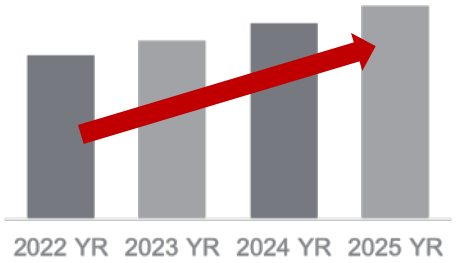
지난해 많은 기업이 재택근무를 도입했고, 60%의 조직이 코로나 기간 동안

출처 : 아주경제

보안 시장 환경

디지털 시대, 사이버보안은 비즈니스 임팩트와 연관

글로벌 보안 시장 '23년1,897억달러(239조)
연평균 12.4% 성장 전망



각국 기업 보안 경쟁력 확보 주력

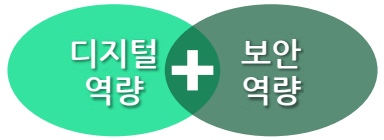
- 대한민국 정부와 미국, 유럽 등 각국은 정보보호산업육성을 자국의 안보와 직결된 문제로 인식, 경쟁력 확보에 주력
- 하루 대한민국 공공기관에 들어오는 공격횟수는 162만건(국정원)

복잡한 IT 환경으로 인한 높은 전문성 요구 현실은 보안 역량, 예산, 인력 부족

클라우드 & AI에 보안에 대한 전문성 부족
보안 솔루션 운영 역량↓

해킹사고로 기업의 근간 흔들림

- 사이버공격 글로벌 경제 피해 '13년 3조달러에서 '22년 6조달러 2배증가
- 보안은 디지털 비즈니스 핵심 역량



01 시장 환경 | 02 고객 환경 | 04 경쟁 환경 | 03 기술 환경

글로벌 보안 시장은 클라우드 보안 업체로 세대교체 진행 중

클라우드 보안 회사로 변신

- 주요 보안 기업은 클라우드 보안, 보안 통합 플랫폼 확보를 위해 적극적 M&A 수행

4가지 시장 리스크 존재

- 기술통합 한계
- 고객운영 어ㅁ려움
- 보안기술 변화속도
- 비싼 가격

클라우드보안은 기존 보안 과 완전히 다름 새로운 보안 기술과 환경을 요구

복잡한 보안 환경

- 보안은 통합적 시야 필요 & 종합기술 영역
- 새로운 기술 변화 : Zerotrust, SECaaS Cloud Native Security, AI Security
- 지속적인 보안환경 변화 및 속도 요구
- 클라우드, AI, 신기술에 대한 컴플라이언스, 정책, 거버넌스가 부족

클라우드 보안은 기존 보안과 다름, 완전히 새로운 보안 기술과 환경을 요구

Compliance	Security Policy	Governance	End Point	Cloud	Data	Development	SoC	Human
클라우드특성 미반영	기업, 클라우드 보안정책 부재	기술영역에서 그레이존 발생	Zertrust로 전환 필요	Cloud Native Security로 전환 필요	문서 중요도에 따른 문서분류 필요	DevSecOps 전환 필요	Cloud SoC SOA로 전환 필요	클라우드, 보안, 개발 통합적 역량 필요

보안의 방식의 변화

Focus on “Manage” ➔ Focus on “Change”	Network ➔ Zerotrust Model	Production ➔ Shift Left
Specific skill sets ➔ Cross functional skill set	Threat detection ➔ Threat anticipation and resolution	Traditional models of automation ➔ Behavior base models

집단 지성 필요 → AI보안 환경 → 통합보안환경 중요 → 자동화된 보안 → 지속적인 변화 와 속도 요구

보안 침해로 인한 비즈니스 임펙트 갈수록 높아짐,
하지만 보안 전문성 갈수록 열악

해킹사고로 기업의 근간 흔들림

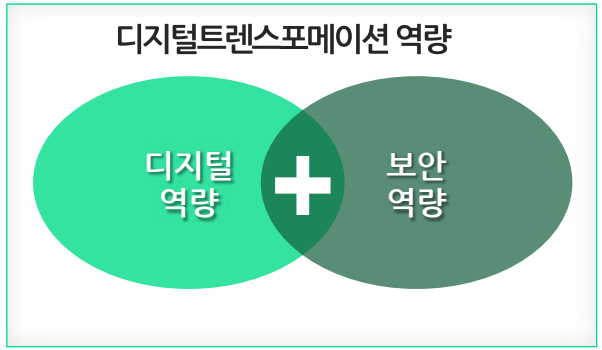
- 사이버공격 글로벌 경제 피해 '13년 3조달러에서 '22년 6조달러 2배 증가
- 클라우드 보안 공격 630배 증가

클라우드 & AI에 보안에 대한 전문성 부족
클라우드 보안 솔루션 운영 역량↓

- 클라우드 보안 기술 너무 어려워 운영하기 어려움

보안 담당자 비즈니스에 기여

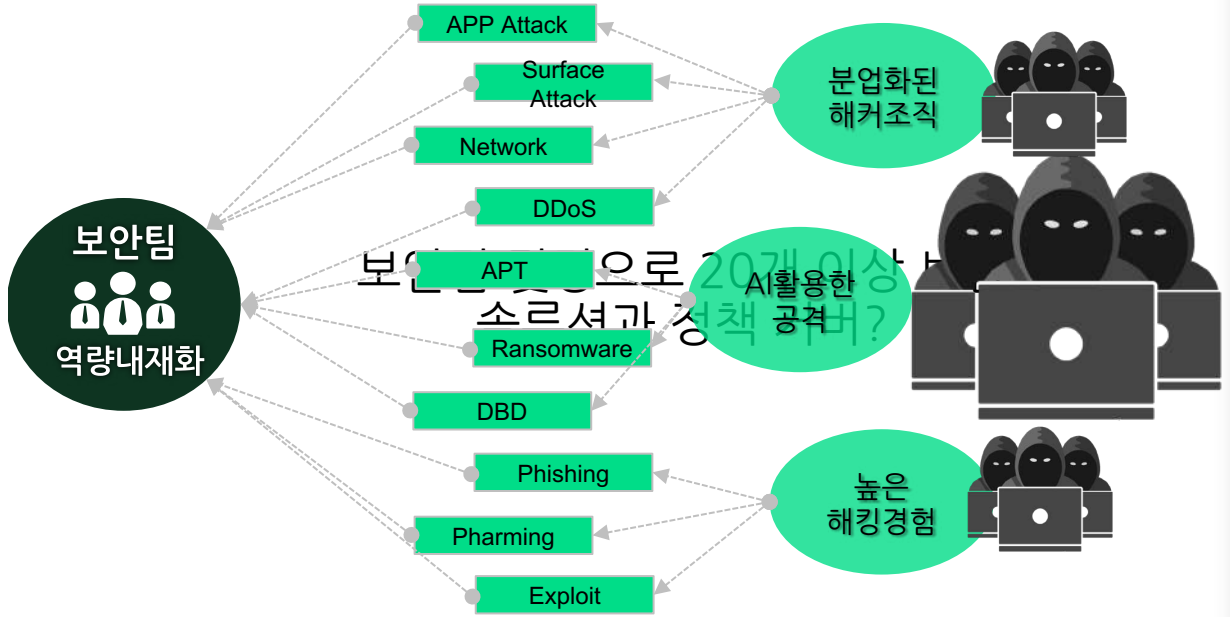
- 기업의 비즈니스가 디지털 중심으로 진화하면서 보안에 대한 중요성과 위협은 갈수록 높아지며, 보안역량을 갖추지 못한 기업은 혁신의 속도에서 계속 늦어질 수 밖에 없음



- *가트너는 2026년까지 이사회의 70%는 사이버 보안 전문 지식을 갖춘 한 명의 구성원을 포함할 것이라고 전망 이는 향후 보안 전문가는 비즈니스 기여한다는 것을 의미(Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024)*
- *가트너는 "2025년까지 사이버 보안 리더의 절반 가까이가 직장을 옮길 것이며, 이 중 25%는 전적으로 업무와 관련된 여러 스트레스 요인 때문이다."라고 예측 사이버 보안은 이제 기업 안에서 해결할 수 없는 주제가 되고 있음(Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024)*

비즈니스 임팩트 위해 보안 역량 중요하지만 내재화 불가능 영역

경험 많고 조직화된 해커조직을
보안팀 몇명으로 막을 수 있을까?



- 디지털 심화 보안의 중요성 높아짐
- 클라우드 보안 컴플라이언스 정책 미비
- 클라우드 & AI 발전 복잡한 보안 환경 야기
- 보안의 지속적 환경변화 속도를 요구
- 보안은 통합 기술이 중요 집단지성이 요구됨
- AI를 활용한 사이버 공격 증가

OpsNow Security

잘 만든 IT 자산이 보안 위협에 한방에 무너질 수 있다!

Ransomware

Crypto Mining

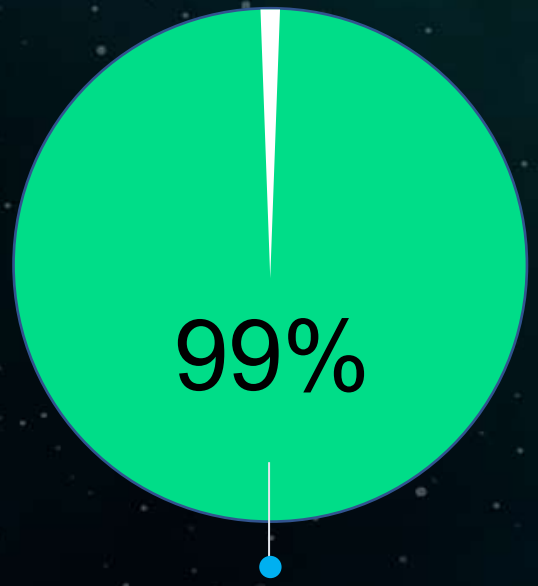
Data Extortion

Attack Servers

'25년 사이버공격 피해 규모

전세계 1경원
국내 1,000 조원

출처 : 미국정보보안사이트 : 사이버시큐리티벤처스



클라우드 보안 사고의 99%는 사용자 실수에 의한 발생

클라우드 보안에 대한 이해가 부족

클라우드 Identity와 Resource에 모두 정책이 있어 설정 관리가 어려움

클라우드는 접근이 쉬운 만큼 공격도 쉬움

자사가 사용하는 클라우드를 제대로 파악하지 못함

매년 새로운 기술이 생겨남

OpsNow Security

디지털시대 사이버보안 중요성 강조,
보안 방식의 변화 명령 “제로트러스트 방식으로 전환하라”

바이든 대통령 취임하자마자 '제로 트러스트' 명령!

THE WHITE HOUSE

Administration Priorities COVID Plan Briefing Room Español

BRIEFING ROOM

Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture

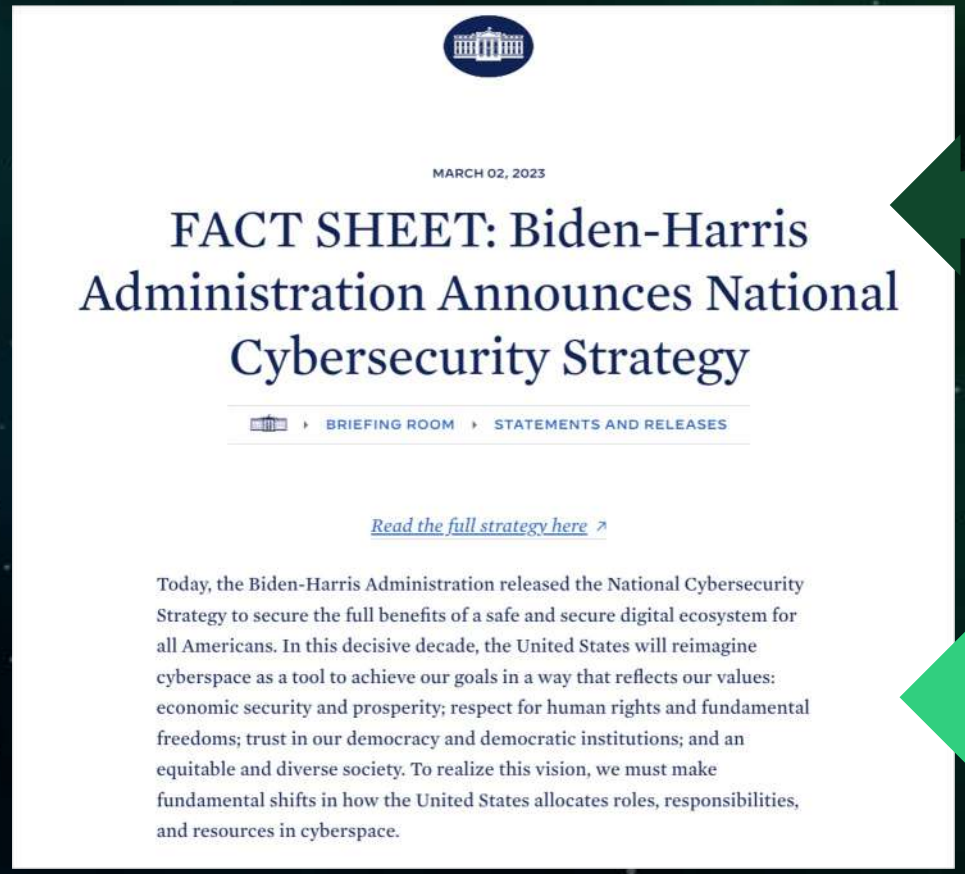
JANUARY 26, 2022 • PRESS RELEASES

Today, the Office of Management and Budget (OMB) released a Federal strategy to move the U.S. Government toward a “zero trust” approach to cybersecurity. The strategy represents a key step forward in delivering on President Biden’s Executive Order on Improving the Nation’s Cybersecurity, which focuses on advancing security measures that dramatically reduce the risk of successful cyber attacks against the Federal Government’s digital infrastructure.

The growing threat of sophisticated cyber attacks has underscored that the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. The Log4j vulnerability is the

사이버 보안은 국가 경제, 안보에 가장 중요

백악관의 ‘미국 전체 사이버 보안 전략’이 새롭게 발표



MARCH 02, 2023

FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy

BRIEFING ROOM • STATEMENTS AND RELEASES

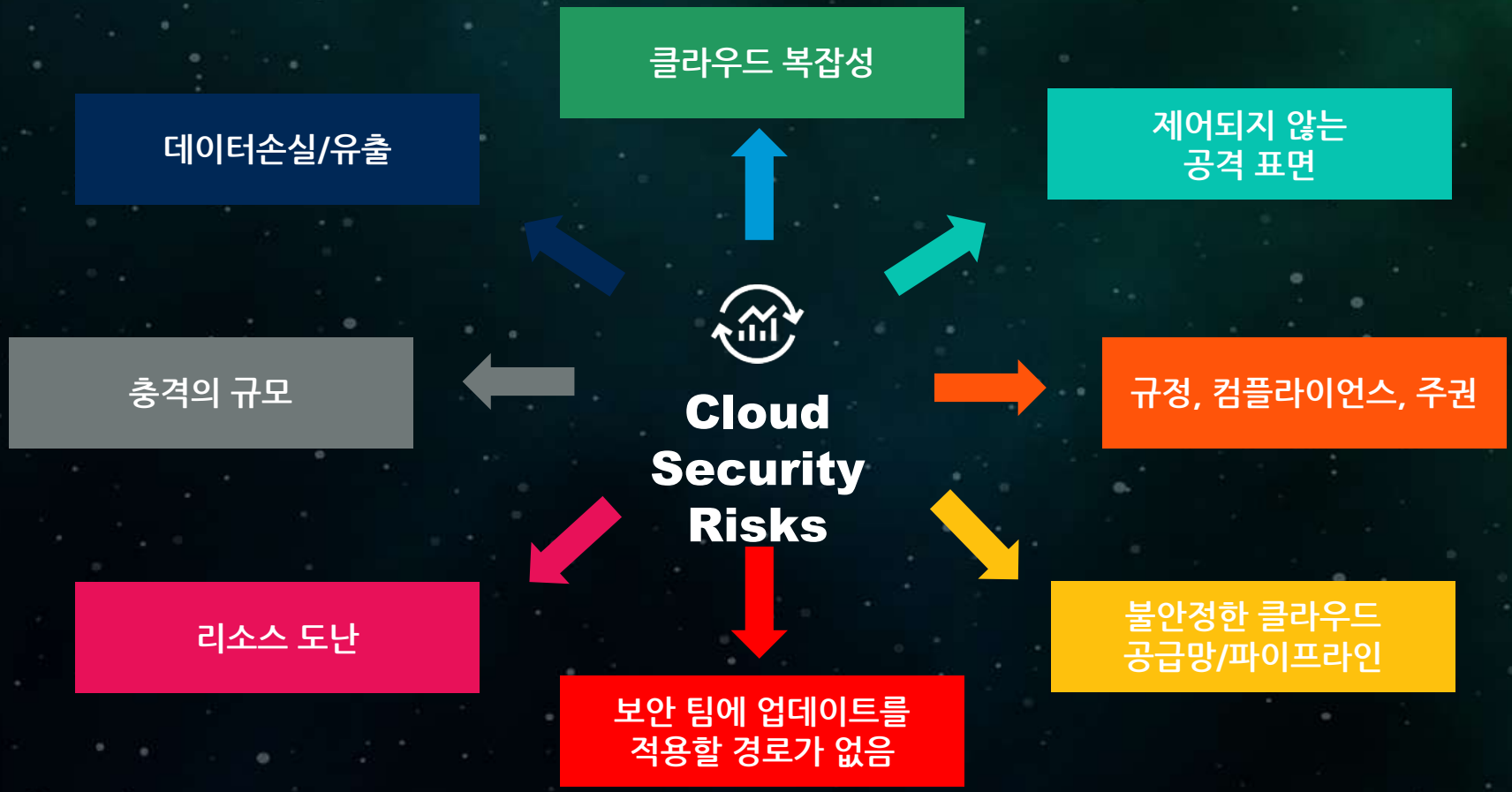
Read the full strategy here ↗

Today, the Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans. In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.

사회 기반 시설 강화하고 소프트웨어 개발사들의 책임을 더 무겁게 만들 계획

OpsNow Security

Cloud Security Risks



Source : Gartner

OpsNow Security

Cloud Security Challenges…….

- 가시성 부족
- 거버넌스 부족
- 정책오류
- 변화의 속도
- 기술격차
- 액세스 및 자격 복잡성
- 책임 공유의 오해
- 잘못된 오류
- Compliance Gaps
- 가드레일 부족

Cloud Security Challenges

Source : Gartner

OpsNow Security

Understand The Nuances of Shared Responsibility

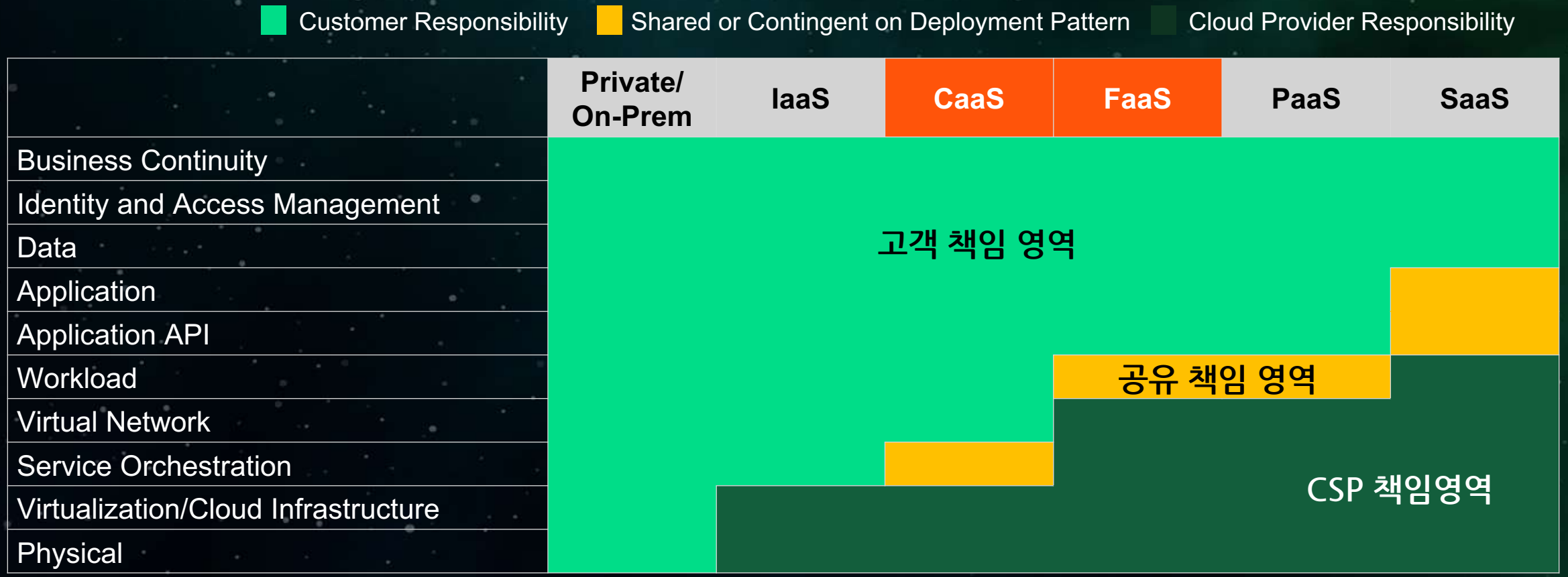
Customer Responsibility Shared or Contingent on Deployment Pattern Cloud Provider Responsibility

	Private/ On-Prem	IaaS	CaaS	FaaS	PaaS	SaaS
Business Continuity						
Identity and Access Management						
Data						
Application						
Application API						
Workload						
Virtual Network						
Service Orchestration						
Virtualization/Cloud Infrastructure						
Physical						

Source : Gartner

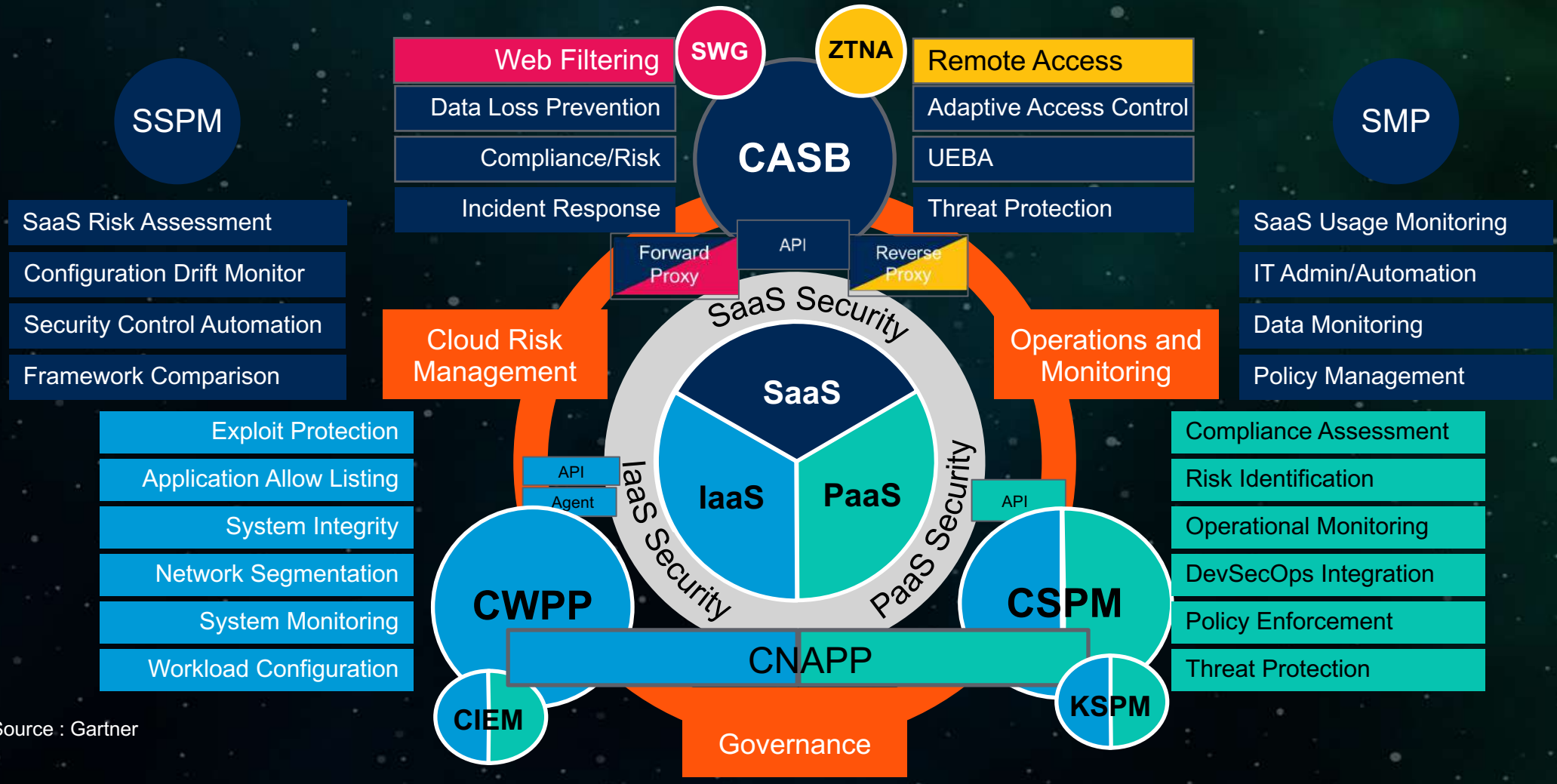
OpsNow Security

Understand The Nuances of Shared Responsibility



OpsNow Security

Cloud Security Strategy



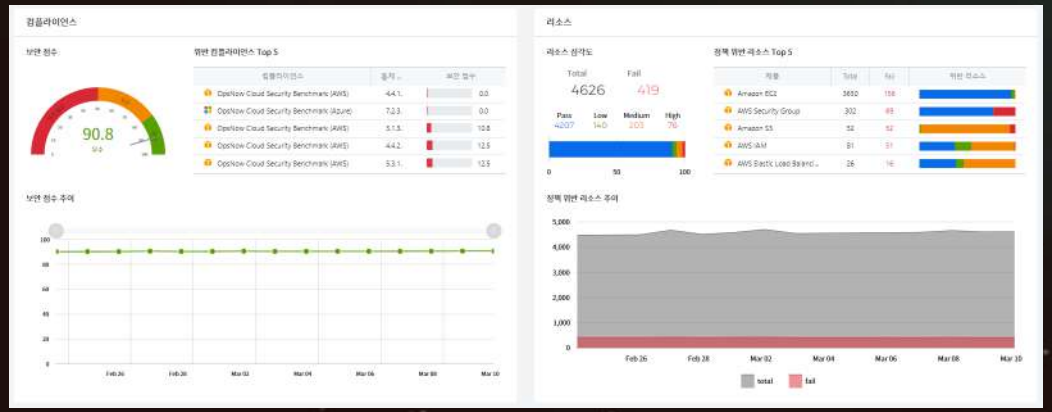
Source : Gartner

OpsNow Security

가장 안전한 클라우드 보안 환경을 위한 2가지 전략

클라우드 보안 가시화

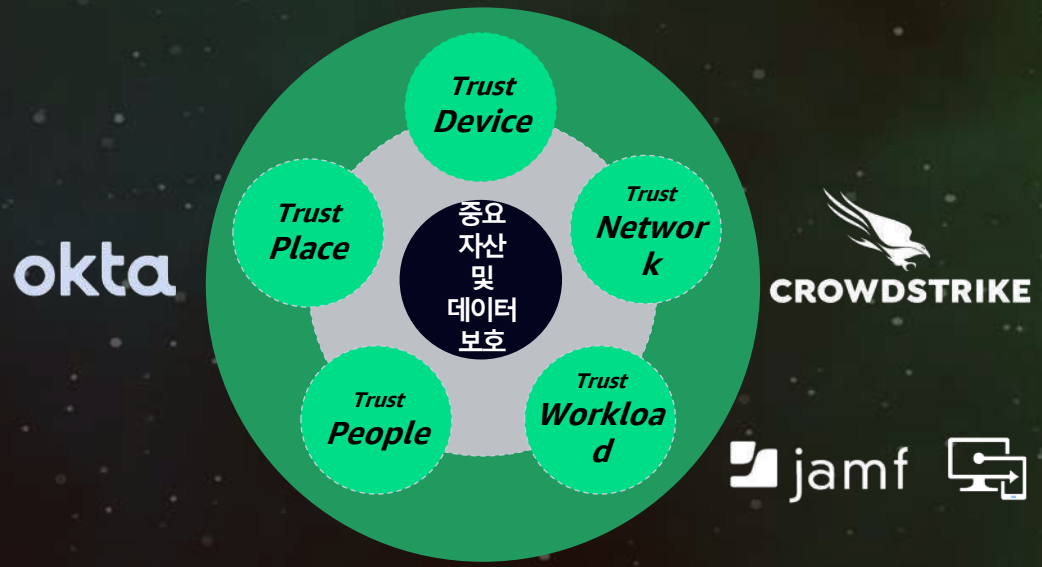
클라우드가 복잡하고 사용자 실수에 의한 보안사고가 많기 때문에 클라우드 보안 가시화 환경이 필요!



90점 이상으로 클라우드 보안을 관리

제로트러스트

클라우드 활용, 재택근무 환경을 위한 제로트러스트 환경 구축



정의된 사용자, 등록된 디바이스만 Secure Network 접속 가능,
모든 App, Data는 Secure Network 통해서만 접속 가능

OpsNow Security

Compliance

ISMS-P
ISO27001
금융보안
국가기본보안
산업기술보안
개인정보보호

Security Policy

보안정책
보안지침
보안가이드

Governance

조직
프로세스
보안위원회
감사

End Point

Vacine
EDR
VDI
E.Mail
IDP
SASE
MDM

Cloud

클라우드보안설정
CWPP
Network
Server
DB
Control Tower
IAM
Hybrid
SaaS

Data

개인정보
문서중앙화
암호화

Development

정적,동적분석
형상보안
개발환경 자동화
컨테이너보안
IaC
MSA 보안

SoC

Network SoC
Cloud SoC
SOA

OpsNow Security

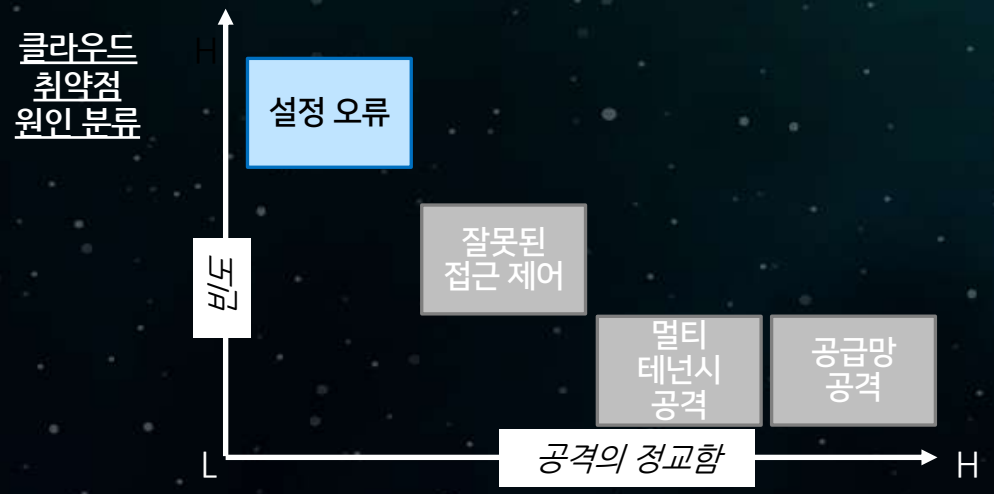
가장 문제는 클라우드 보안 중 클라우드 보안 설정

Compliance	Security Policy	Governance	End Point	Cloud	Data	Development	SoC
							
ISMS-P ISO27001 금융보안 국가기본보안 산업기술보안 개인정보보호	보안정책 보안지침 보안가이드	조직 프로세스 보안위원회 감사	Vacine EDR VDI E.Mail IDP SASE MDM	**클라우드보안설정** CWPP Network Server DB Control Tower IAM Hybrid SaaS	개인정보 문서중앙화 암호화	정적,동적분석 형상보안 개발환경 자동화 컨테이너보안 IaC MSA 보안	Network SoC Cloud SoC SOA

클라우드 보안 사고는 99%가 사용자 책임으로, 특히 설정 오류가 가장 큰 원인입니다

미국 국가 안보국

"클라우드 취약점의 가장 흔한 원인은 설정 오류[2]"



설정 오류 예시

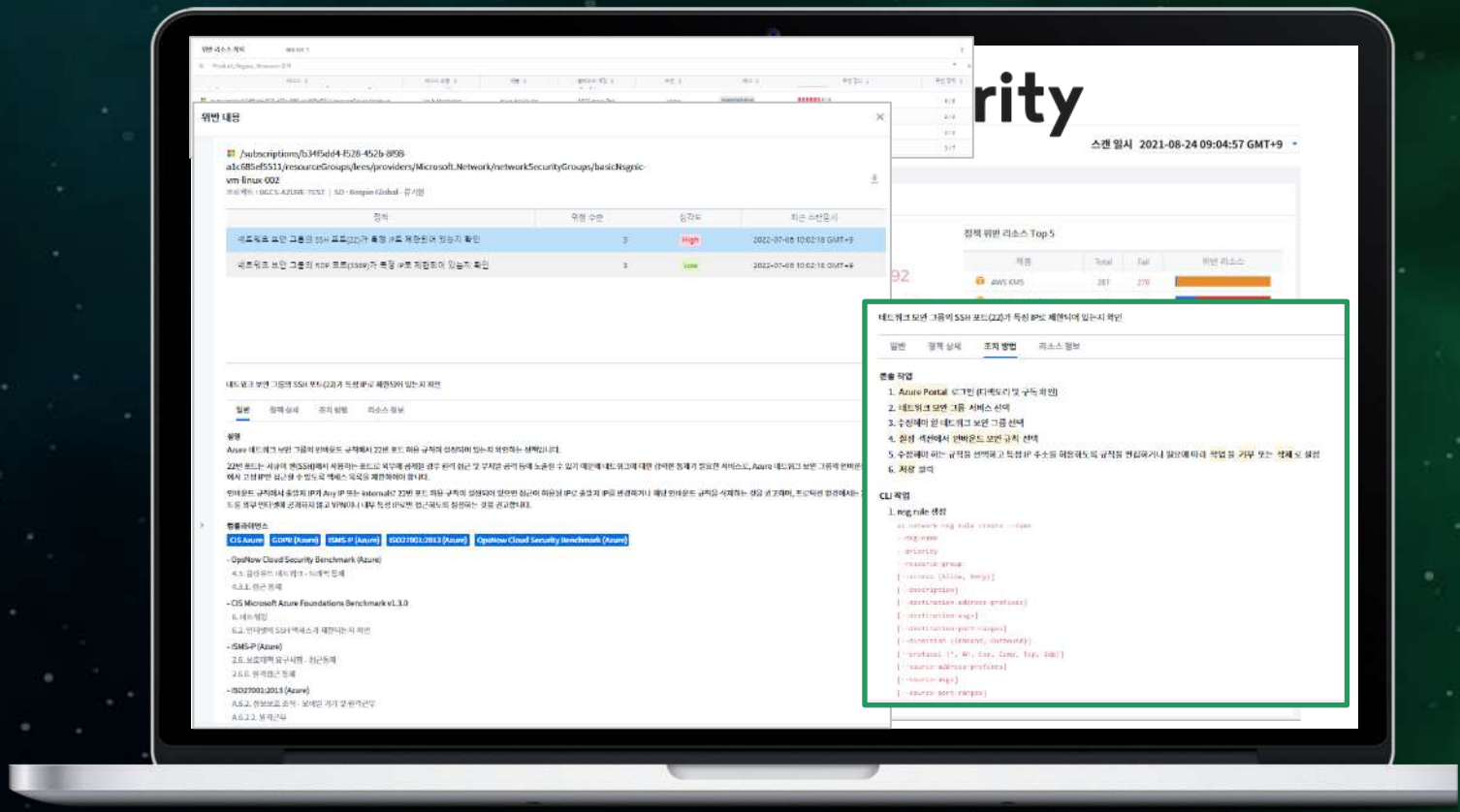
- 잘못된 IAM 정책 설정
  *IAM: Identity and Access Management
- 잘못된 보안 그룹 정책 설정
- 전송 중 암호화 미적용

사용하는 클라우드 리소스에 대한 사용자의 잘못된 보안 설정

OpsNow Security

클라우드 보안 정책 + 가시화 = 클라우드 보안 문제 80% 해결

- AWS, Azure, GCP 클라우드취약점
- 자동화된 클라우드 보안 구성 진단
- ISMS등 컴플라이언스 관리
- 보안점수, 보안 가시화
- 클라우드 보안 감사
- 이상행위 탐지
- 국내 컴플라이언스 제공 및 정책 커스터마이징



대규모 멀티 클라우드 운영 (3개 CSP, 300개 이상 Account)을 위해 해외 CSPM 제품을 사용하였으나
OpsNow Security로 교체 도입하여 합리적인 비용으로 보안운영 및관리 효율성이 증대

SK그룹 표준 CSPM

01 그룹 표준 클라우드 보안 정책

02 보안 운영 중심의 기능

03 합리적인 가격

04 클라우드 보안 협력

OpsNow Security
SK그룹 총판
SK 주식회사 C&C

기술 협력
BESPIN GLOBAL
OpsNow Security

그룹사 도입

주요 고객사

SK telecom, SK E&S, SK 쉴더스, SK 주식회사 C&C, SK 스토아, kakaogames, DAEKYO 대교, nc, SK 바이오팜, toss place, SILICON, SECUI, KT&G, K2, mono labs, LF, mobidoo, 이투스교육, 모두의주차장, FOBLGATE, coex, DearU, 폴컨스미디어, kodebox, theKconnect, VUNO View the Invisible, Know the Unknown

OpsNow Security

클라우드 사용, 재택 근무회사, 제로트러스트만이 유일한 해답

WFA , 재택근무에서의
안전한 보안환경

안전한 클라우드 접속
& 클라우드 통합계정

현업부서, 보안조직도 쉽고
단순하게 강력한 보안환경 구축

VPN한계 극복

공유오피스, 재택근무, 클라우드 20개 이상 사용, 8개 이상의 업무그룹
기존 보안 체계로는 해결할 수 없는 총체적 난국

복잡한 보안 환경

- **데이터센터, 클라우드 20개 이상 활용**(AWS, Azure, GCP, NCP, Private Cloud, SAP on AWS, Salesforce, Atlassian, GWS 등 다양한 SaaS)
- **자유로운 업무 환경 :** 공유오피스, 폐쇄 업무 공간, 재택 등 Work form Anywhere
- **다양한 업무 그룹 :** 일반직원, 내부 SaaS 개발, 내부 SaaS 운영, 외주 개발사, MSP, 외부 개발, 파견 담당자, 보안담당자, 사내 시스템 운영자 등 업무그룹이 7개가 넘음

내부에서 인증 처리 불가
다양한 AD 통합 이슈

- WFA(Work from anywhere 및 Cloud & AI 활용으로 **내부 인증 처리 불가**
- 많은 SaaS를 활용하면서 내부 서비스 외부 서비스의 **계정관리, SSO, MFA 가 3중 4중으로 많아짐**
- 내부에 여러가지 AD가 존재하고, Attribute 값이 상이하여 **통합 아이덴티티 구성이 어렵고, 관리가 가 복잡**해짐

계정 거버넌스 문제
라이프사이클 부재로 Shadow IT

- 다양한 SaaS 활용으로 인한 권한 관리 및 **계정 라이프사이클 관리가 안됨**
- 입사 > 부서이동 > 퇴사 > 감사에 대한 계정 거버넌스 문제 심각 **→사실 모든 보안 사고의 문제는 여기에서 벌어짐**
- 신규 기술을 활용하는데 제약이 없어서 **쉐도우 아이티를 막을 방법 부재**

내부 SaaS 인증 통합

- 회사에 다양한 SaaS서비스의 상이한 계정 관리 문제
- 계정 관리 및 보안 강화 필요성↑

공유오피스, 재택근무, 클라우드 20개 이상 사용, 8개 이상의 업무그룹
기존 보안 체계로는 해결할 수 없는 총체적 난국

복잡한 보안 환경	내부에서 인증 처리 불가 다양한 AD 통합 이슈	계정 거버넌스 문제 라이프사이클 부재로 Shadow IT	내부 SaaS 인증 통합
Zerotrust	SECaaS형 IDP (20개 이상 외부서비스 연동)	Okta 라이프관리를 통행 계정 거버넌스 수립(IDA)	내부 SaaS 서비스에 Okta 연동
통합 IDP	Okta로 통합 IDP 구성 (20개 이상 외부서비스와 여러개의 AD를 연동)	Okta에 등록하지 않는 모든 SW와 클라우드 접속 금지	Okta CIC 적용중

이 모든 문제를 Okta를 중심으로 제로트러스트로 해결!

복잡한 보안 환경	내부에서 인증 처리 불가 다양한 AD 통합 이슈	계정 거버넌스 문제 라이프사이클 부재로 Shadow IT	내부 SaaS 인증 통합
Zerotrust	SECaaS형 IDP (20개 이상 외부서비스 연동)	Okta 라이프관리를 통행 계정 거버넌스 수립(IDA)	내부 SaaS 서비스에 Okta 연동
통합 IDP	Okta로 통합 IDP 구성 (20개 이상 외부서비스와 여러개의 AD를 연동)	Okta에 등록하지 않는 모든 SW와 클라우드 접속 금지	Okta CIC 적용중
단순하고 편한 보안 환경	통합IDP 구축	자동화된 계정 거버넌스 구축	99.9999% 안전한 SaaS 계정환경

OpsNow Security

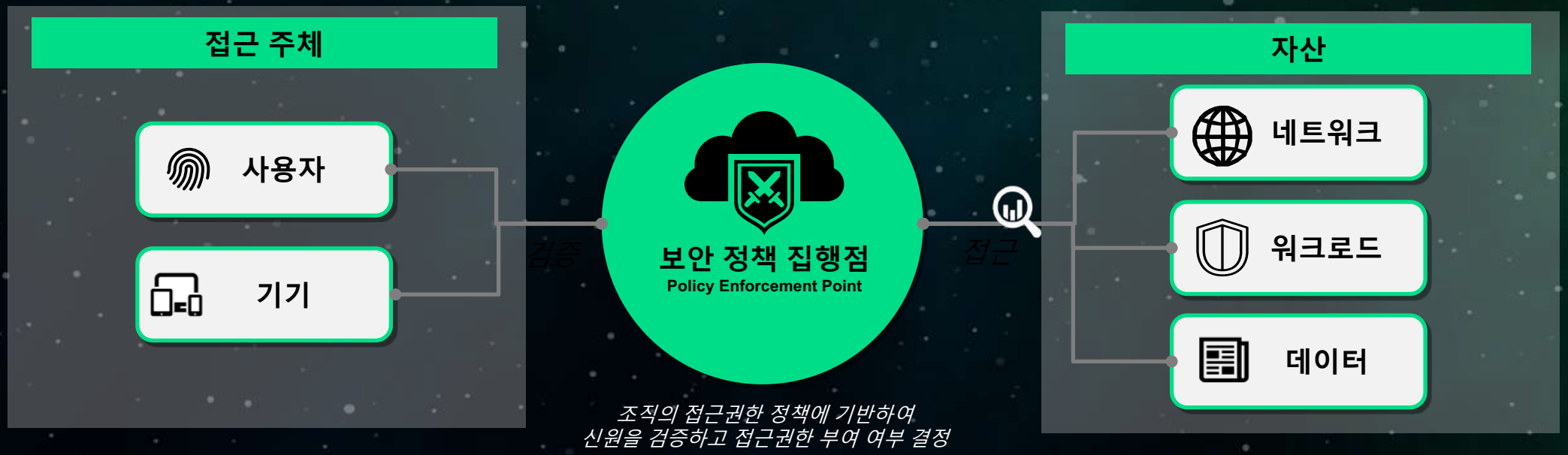
클라우드 사용, 재택 근무회사, 제로트러스트만이 유일한 해답

“ Never Trust, Always Verify ”

모든 신원을 검증하고
최소 권한만 부여함

모든 데이터를
물리적 위치 및 상태에
관계없이 보호함

모든 트래픽 로그를
수집 및 감사함



조직의 접근권한 정책에 기반하여
신원을 검증하고 접근권한 부여 여부 결정

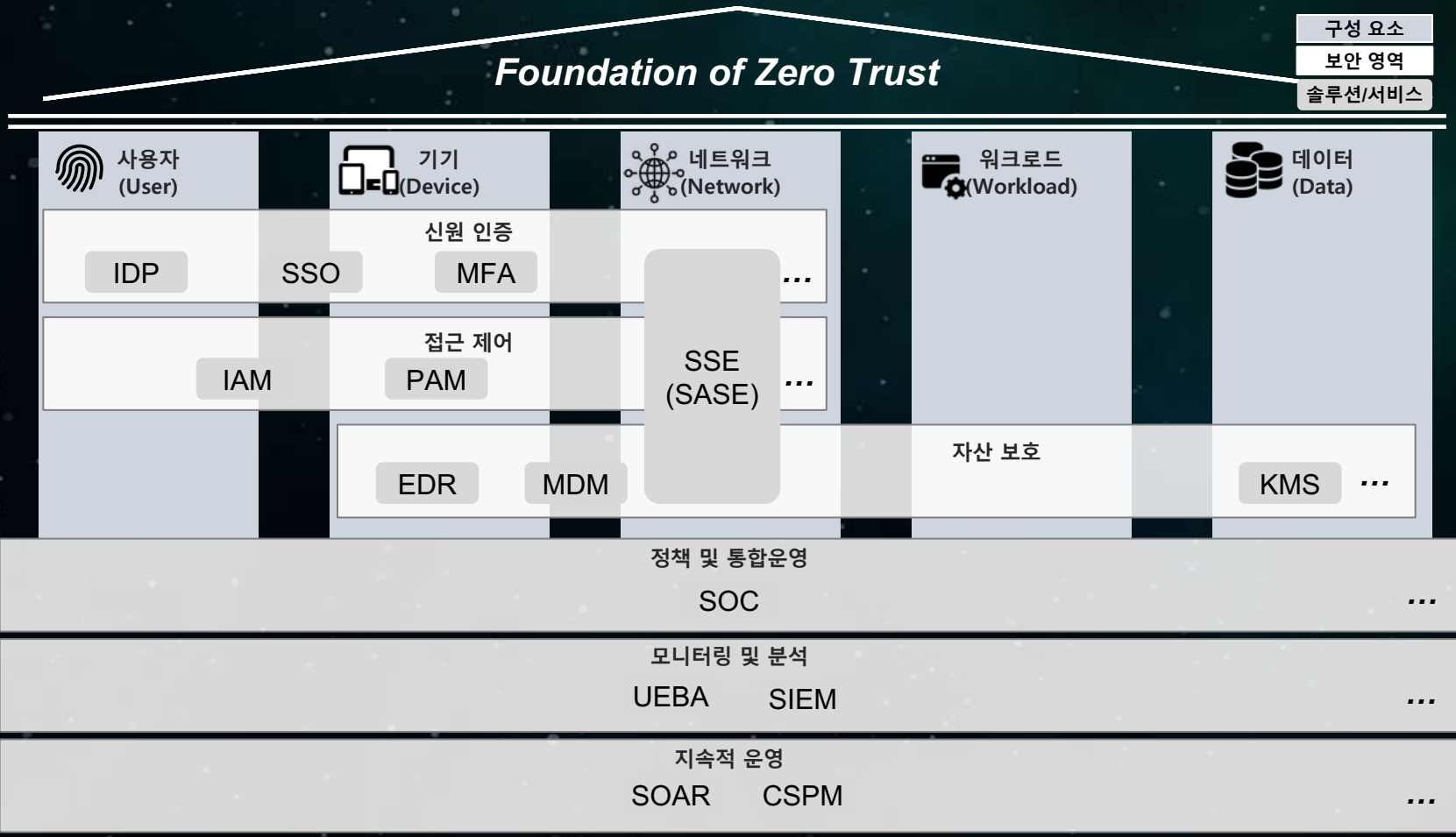
OpsNow Security

국내모든 직원, 생체인증, CYOD, 지속적 접근 검증

사용자	장소	단말기	네트워크	애플리케이션	스마트워크 데이터(문서)
베스핀글로벌 코리아 정직원을 그 대상으로 함 해외지사는 2023년부터 단계적 진행 사용자에 대한 인증은 **통합IDP(Okta)로 인증**하고, **MFA, 생체인증을 통해 사용자 확인**을 진행	스마트워크를 사용할 수 있는 장소는 모든 장소에서 접속 가능 스마트워크 접속 장소는 단말기의 접속 IP 를 통해 확인 베스핀글로벌 지사가 없는 해외IP는 모두 차단	스마트워크에 사용하는 PC 혹은노트북은 회사에서 제공한 표준 CYOD 장치만 인정 공동사용 불가 CYOD 모든 단말기에는 MDM이 설치되어 제어 보안 솔루션을 통해 점수가 낮으면 접속 불가 단말기 암호화? 저장금지?	높은 수준의 보안 사용목적에 따라 망이 분리 암호화 통신을 해야함 주고 받는 모든 것을 정책화 하고 모니터링 할 수 있고 제어 가능한 환경 특정 클라우드 서비스 사용시(AWS, GWC)는 허용된 사용자, 디바이스, IP로만 접근이 가능하도록 통제	Application 별(ERP, Groupware, Email, 국가핵심기술시스템 등) 접속할 때 승인된 담당자만 접속이 가능해야 함 사용자는 클라우드내 특정 어플리케이션만 이용 허가가 가능 해야함	문서를 협업/소통도구에 업로드시 문서 등급에 따라 업로드가 제한(추진중) 문서를 협업/소통도구에 업로드시 문서에 저장된 내용에 대해 개인정보, 특정문구를 검사하고 통제(추진중)
정의된 업무자 제외 모든 임직원 대상	**모든 장소에서 스마트워크 가능**	**회사에서 제공한 표준CYOD만 인정**	**국내, 모든 장소가능 해외, 특정 IP만 가능**	**승인된 사용자만 어플리케이션 접속**	**문서 등급에 따라 업로드/접근 제한**
					

OpsNow Security

“ Never Trust, Always Verify ”



1 신원 인증

사용자/기기 신원 주장의 유효성 검증

2 접근 제어

정책 기반 허가된 신원에 접근 권한 부여

3 자산 보호

비인가 접근에 대하여 자산 통제

4 정책 및 통합운영

중앙화된 보안 그룹 및 정책 설정

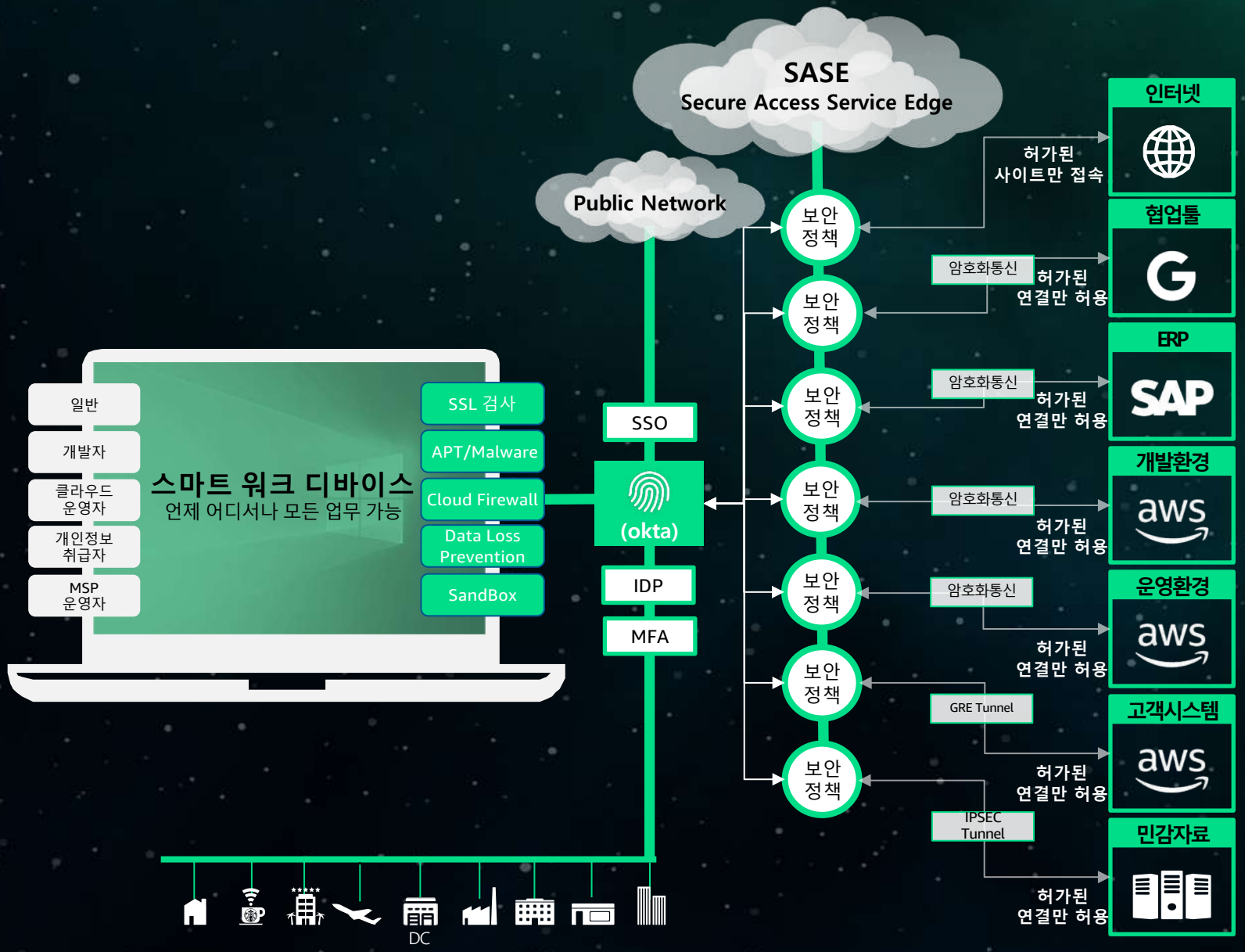
5 모니터링 및 분석

로그 기반 보안 위협 탐지

6 지속적 운영

운영 효율화 및 위험 관리

OpsNow Security

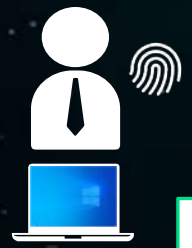


- 언제 어디서든 강력한 보안 환경
- 인터넷망, 업무망, 개발망, 운영망 고객접속망의 명확한 구분
- 안전한 클라우드 접속
- 강력한 인터넷 보안 환경
- Application 별 인증 체계
- Data 별 인증 체계
- MSP 고객사 별 3중 인증 접속 (사용자, 디바이스, IP)
- 모든 활동에 대한 감사 체계
- 편리한 인증 환경

사용자

OpsNow Security

사용자가 앱에 접속을 할 때마다 사용자와 기기의 정보를 실시간으로 검증



Device

Identity

Network

MDM

Intune jamf

- Device 관리/정보
- Software 관리
- 보안 정책 적용/관리

EPP/EDR

CROWDSTRIKE SentinelOne

- 악성코드 검사
- 보안 정책 적용/관리
- Endpoint 행위 기반 검사

Device Trust

Score

IDP (Identity Provider)

okta

- 사용자 / 인증 수단
  . Password / E-mail / 지문
- 인증 정보
  . Device (OS) / Browser
- **Device 정보**
  - 관리 기기 / 무결성
- 인증 정책
- 위협 정보
  . Black IP
  . Behavior

인증 정책

Score

SSE(SASE)

CLOUDFLARE

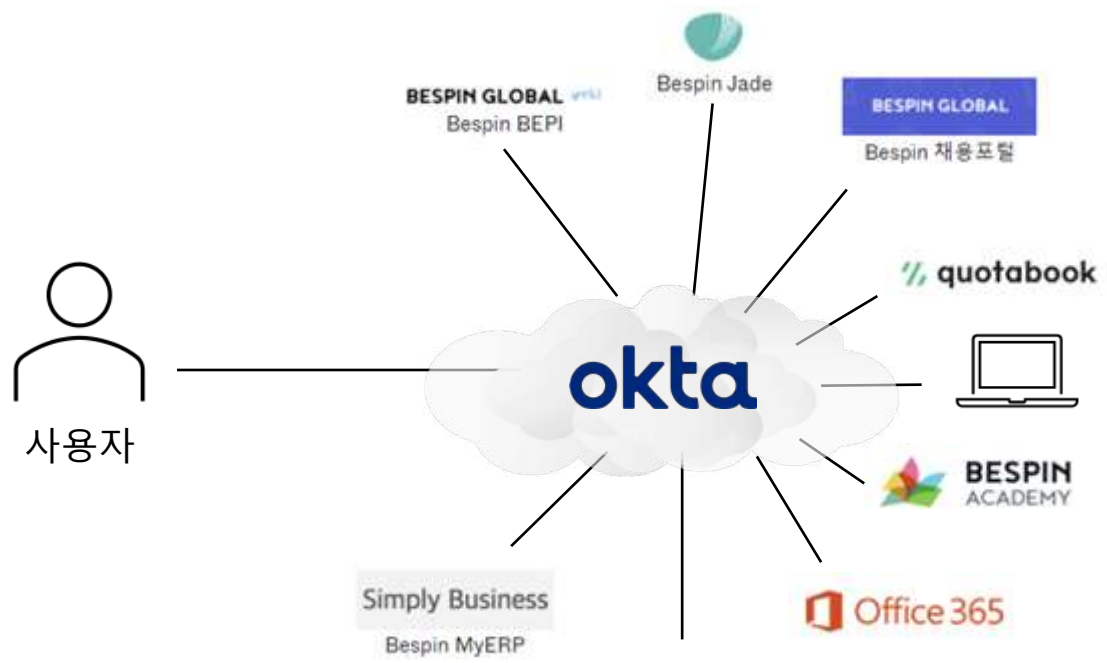
- **Device 검증**
  - Okta 인증 정보
  - Crowdstrike Score
  - Device Assurance
- Cloud Firewall
- URL Filtering
- DNS Filtering
- DLP / Sandbox
- SSL Inspection

통합인증을 통한 안전한 인증 및 편의성 강화

AS-IS

App마다 별도의 ID/Password를 관리해야 하여
번거롭고 분실/도용의 위험이 있음

TO-BE

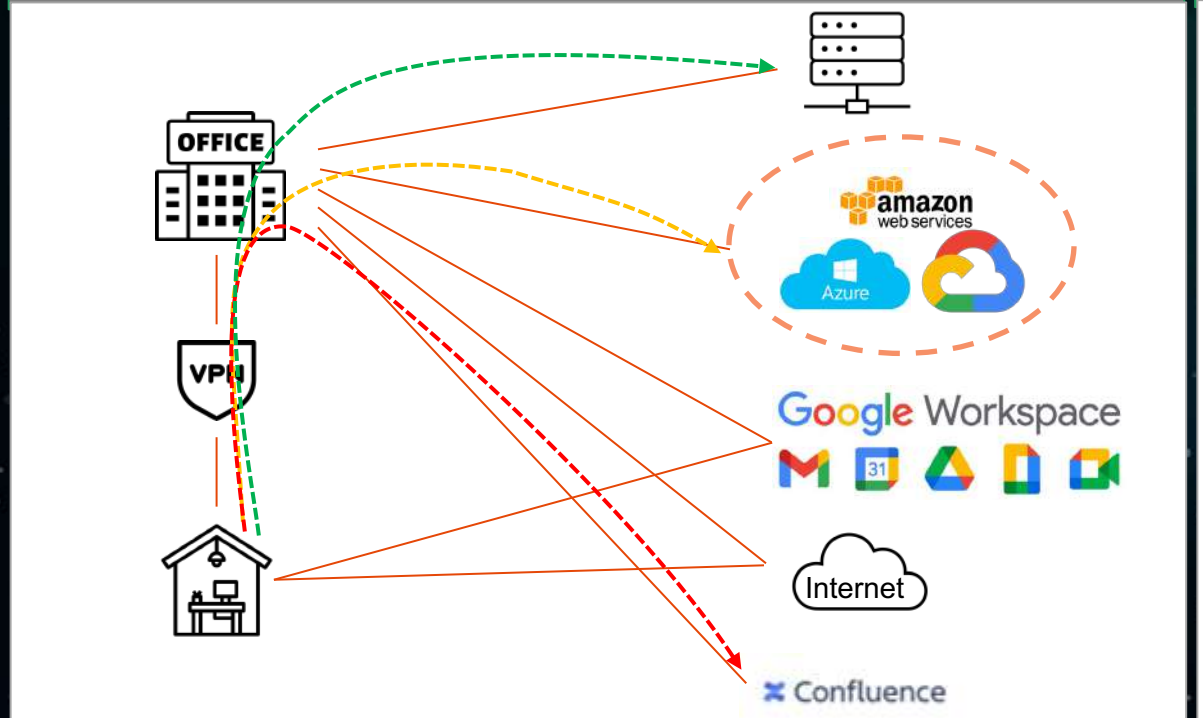


Okta를 통해 인증이 간편하고 안전해짐
통합IDP, SSO, MFA

OpsNow Security

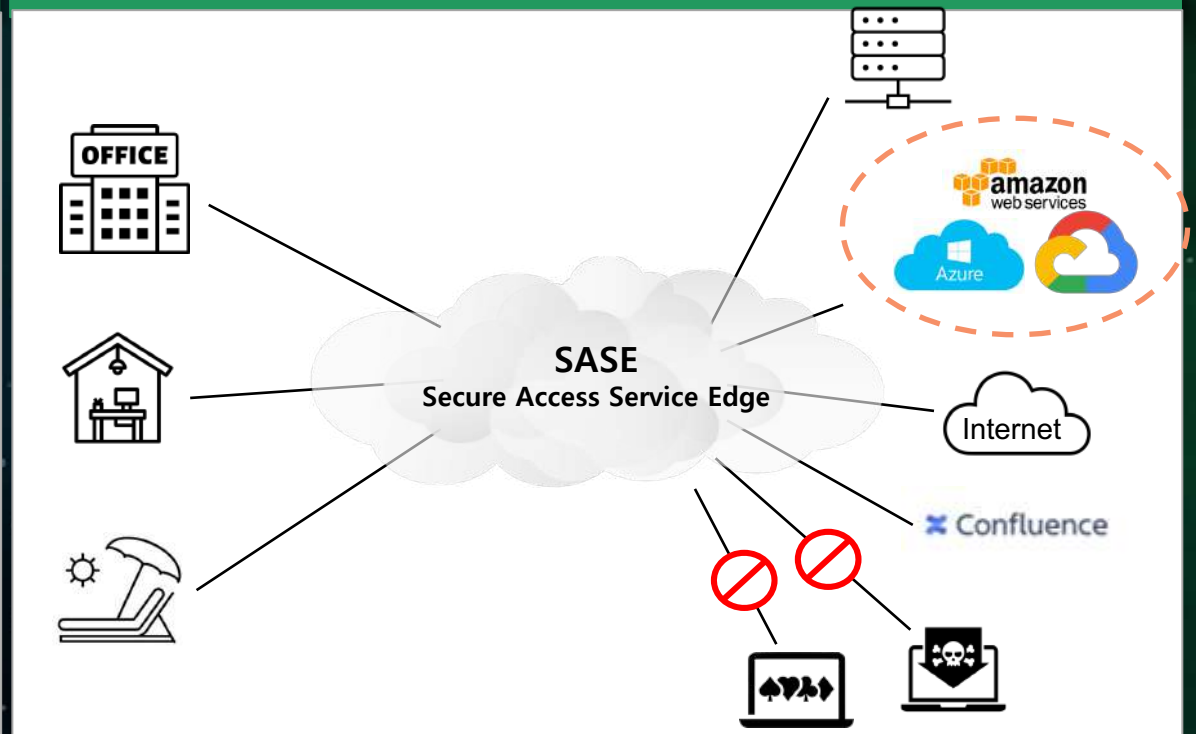
통합인증을 통한 안전한 인증 및 편의성 강화

AS-IS



사내 네트워크를 통해서만 접근할 수 있는 자원이 있어,
매번 VPN을 연결해야 하는 번거로움이 있음

TO-BE



장소에 구애받지 않고, 각 노트북에서 SASE를 통해
네트워크/자원에 접근할 수 있으며, 위험을 차단함

보안성 강화 및 편리성 강화

구분	AS-IS	TO-BE
주요 서비스 접속 (Google Workspace, Jade, Office365, ERP, Groupware)	어느 PC에서나 접속 가능	**회사 지급 PC에서만 접속 가능** (개인PC, PC방 등 공용PC 제한) ※ Jade 모바일 app은 제외
기기 대수	1인 다수	**1인 1PC 원칙**
VPN	Confluence 등 일부 서비스 접속 시 VPN 연결 필요	**VPN 연결 불필요**
Mail	모든 메일 서비스 사용 가능	**업무 Gmail (bespinglobal.com) 사용** Naver, Daum 메일 읽기만 가능 (쓰기 불가), 개인 Gmail 및 기타 웹메일 사용 금지
메신저	모든 메신저 사용 가능	**Google chat, slack, MS Teams 사용** 기타 메신저 사용 금지 (PC 카카오톡 차단 등)
파일 저장/공유	모든 온라인 드라이브/웹하드 사용 가능	**Google Drive (bespinglobal.com) 사용** 기타 개인 Drive 및 웹하드 사용 금지
원격 제어 프로그램	모든 원격 제어 프로그램 사용 가능	**Windows remote desktop (RDP), SSH 사용** 기타 원격 제어 프로그램 사용 금지
웹사이트	모든 웹사이트 접속 가능	비업무/유해(성인, 도박 등) 사이트 접속 금지
USB 사용	쓰기 차단	읽기/쓰기 차단
PC 로그인 시 인증	AD에서 인증	Windows - 생체 인증(Windows hello) MAC - Okta
로컬/게스트 계정 사용	가능	불가
새 Microsoft 계정 추가	가능	불가

OpsNow Security

클라우드 무료 취약점 컨설팅 제공합니다.

common-host-366004

- IAM & Encryption
- Compute
- Network
- Database
- Storage
- Log & Monitoring

OpsNow Security

OpsNow Cloud Security Benchmark

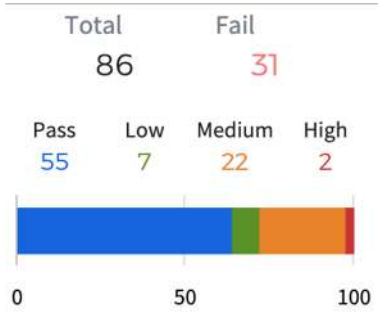
- 컴플라이언스
- \+
- 클라우드 모범사례
- \+
- 베스핀글로벌 노하우
- \+
- 클라우드 정책 수집

알티모빌리티 조직 보안 점수

GCP Account 1개의 보안 점수는 78.6점 으로 "표준" 단계에 해당

OpsNow Security를 통해 지속적으로 위반된 정책을 확인 하고, 조치하여 단계적으로 조직의 보안점수를 향상시키고 유지해야합니다.

리소스 심각도



점검 대상 리소스의 36%가 위반된 정책을 가짐

위반 리소스 중 심각도가 중간 이상인 항목 89%

Compute 서비스에 위반 리소스수가 가장 많음

VPC > Storage > IAM 순서대로 위반 리소스 수가 많음

분석 결과 총평

심각도가 높은 정책을 많이 위반하고 있어 빠른 조치 필요합니다.

CSPM 솔루션을 통해 최신 및 **표준화된 클라우드 보안 정책을 기반으로 자사의 클라우드 보안 기준을 마련하고 이를 기준으로 클라우드 구성 취약점 모니터링 필요합니다.**

OpsNow Security

컴플라이언스 기준 클라우드 구성 보안 취약점 진단 결과에 대해 자동으로 리포트를 제공합니다.

OpsNow360 Security

프로젝트 컴플라이언스 보안 진단 보고서

프로젝트 컴플라이언스 보안 진단 보고서

진단 일자 2023/04/24

2.1 보안 점수

OpsNow Cloud Security Benchmark (AWS) 기준으로 점검한 결과
BGCS-CSPM-TEAM 프로젝트의 보안 점수는
57.7점으로 **개선 필요** 수준으로 평가되었습니다.

개선 필요 0 ~ 69 표준 70 ~ 89 우수 90 ~ 100

2.2 연동 컴플라이언스 준수율

2023/02/25 기준 OpsNow Cloud Security Benchmark (AWS) 준수율은 **55.3%**입니다.

No	카테고리	Fail	Total	준수율
1	1.1. 클라우드 조직 및 계정관리 - 조직 및 권한 설계	2	3	33%
2	1.2. 클라우드 조직 및 계정관리 - 권한 및 역할관리	0	1	100%
3	1.3. 클라우드 조직 및 계정관리 - 사용 계정 보호	0	3	100%
4	2.3. 클라우드 환경관리 - 암호화 키 관리	163	324	50%
5	3.2. 클라우드 컴퓨팅 - 접근 관리	1	1	0%
6	4.2. 클라우드 네트워크 - 트래픽 통제	17	102	83%
7	4.3. 클라우드 네트워크 - 위협 관리	17	17	0%
8	6.2. 클라우드 데이터 - DB 및 스토리지 관리	9	15	40%
9	6.3. 클라우드 데이터 - 접근 관리	0	4	100%
10	6.4. 클라우드 데이터 - 데이터 보호	3	6	50%
11	7.2. 클라우드 모니터링 - 보안 모니터링	1	1	0%
총 합계		213	477	55.3%

2.3 심각도별 위반 정책 수

Total	Pass	Fail	Low	Medium	High
477	264	213	92	119	2

4.1 위반 정책 목록

OpsNow Cloud Security Benchmark (AWS) 내 111개의 정책 중 위반 정책은 **13**개입니다.

1.1. 클라우드 조직 및 계정관리 - 조직 및 권한 설계

통제항목	정책	평가 리소스 수	위반 리소스 수	준수율	심각도
1.1.2. 루트 계정 보호	루트 계정에 MFA가 설정되어 있는지 확인	1	1	0%	High
	루트 계정이 하드웨어 MFA 장치를 사용하는지 확인	1	1	0%	High

2.3. 클라우드 환경관리 - 암호화 키 관리

통제항목	정책	평가 리소스 수	위반 리소스 수	준수율	심각도
2.3.1. KMS 키 관리	삭제 예정인 CMK가 존재하는지 확인	81	81	0%	Medium
	CMK 키 자동 교체가 설정되어 있는지 확인	81	81	0%	Low
	CMK 키 정책의 정책 요소에 별표(*)가 제외되어 있는지 확인	81	1	99%	Low

3.2. 클라우드 컴퓨팅 - 접근 관리

통제항목	정책	평가 리소스 수	위반 리소스 수	준수율	심각도
3.2.1. 접근 제어	람다 함수 생성시 VPC 설정이 되어있는지 확인	1	1	0%	Medium

4.2. 클라우드 네트워크 - 트래픽 통제

통제항목	정책	평가 리소스 수	위반 리소스 수	준수율	심각도
4.2.1. 접근 통제	Default Security Group의 모든 트래픽이 차단 설정되어 있는지 확인	17	17	0%	Medium

4.3. 클라우드 네트워크 - 위협 관리

통제항목	정책	평가 리소스 수	위반 리소스 수	준수율	심각도
4.3.2. 위협 분석	VPC Flow Log가 활성화 되어있는지 확인	17	17	0%	Medium

OpsNow Security

찾아가는 제로트러스트 세미나를 해 드립니다.

- 클라우드 보안 트렌드
- 클라우드 보안 개념
- 제로트러스트 구축 사례
- DevSecOps
- 국가핵심기술 클라우드 보안
- Cloud SIEM
- Edge Security
- 문서보안 in Cloud
- 클라우드 보안 자동화
- 클라우드 표면 관리 방안
- 기타 클라우드 보안 교육

Thank you!