Cyber Security Conference 2021

SAMSUNG SDS

클라우드 기반 WAAP

클라우드를 클라우드로 보호하는 클라우드 보안 아키텍처링 사례

강세현 프로 삼성SDS 보안플랫폼팀

클라우드 기반 Web Application & API Protection - WAAP

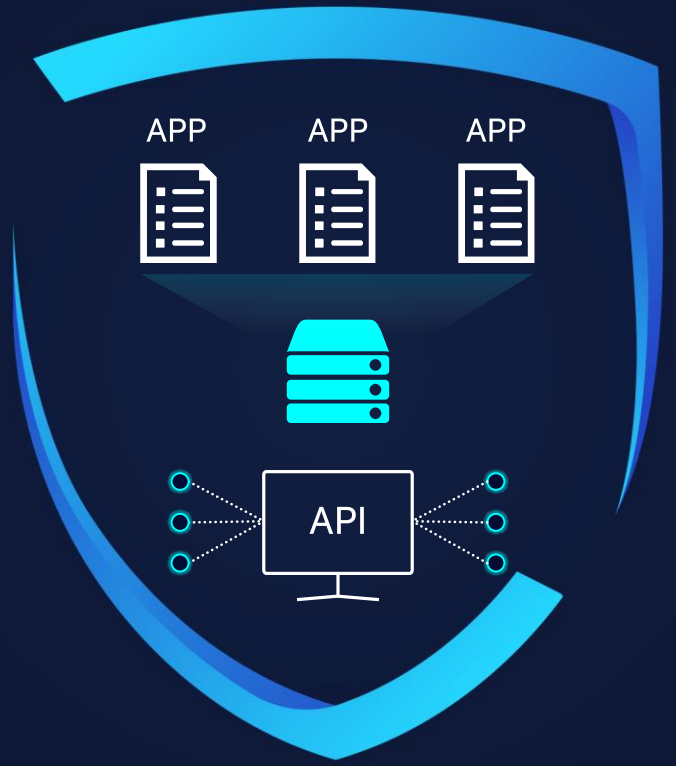
WAAP는 Web Application과 API를 대상으로 하는 공격을 보호하기 위한 수단입니다.

App 취약점 공격

- Injection
- XSS

DDoS

- 대용량 트래픽
- 리소스 고갈



악성 Bot 트래픽

- 사용자 위장
- 스팸 공격

API 취약점 공격

- Request 조작
- 취약한 인증

클라우드 기반 Web Application & API Protection - WAAP

WAAP은 웹 서비스에 대한 기본적인 보안이며, WAAP을 제공하지 못하는 기업은 살아남기 힘듭니다.

WAAP '만' 제공하는 기업
한번도 HW WAF를 만들어 본 적 없는 기업

Akamai, Limelight Networks, Cloudflare, amazon, Google, Oracle, Microsoft, CDNetworks

WAAP '을' 제공하는 기업
HW WAF를 만들지만 클라우드 비중이 더 큰 기업

imperva, Barracuda (Your journey, secured.), f5, radware (availability | performance | security), Fortinet

WAAP '은' 제공 못하는 기업
HW WAF만 만드는 기업

Dropped

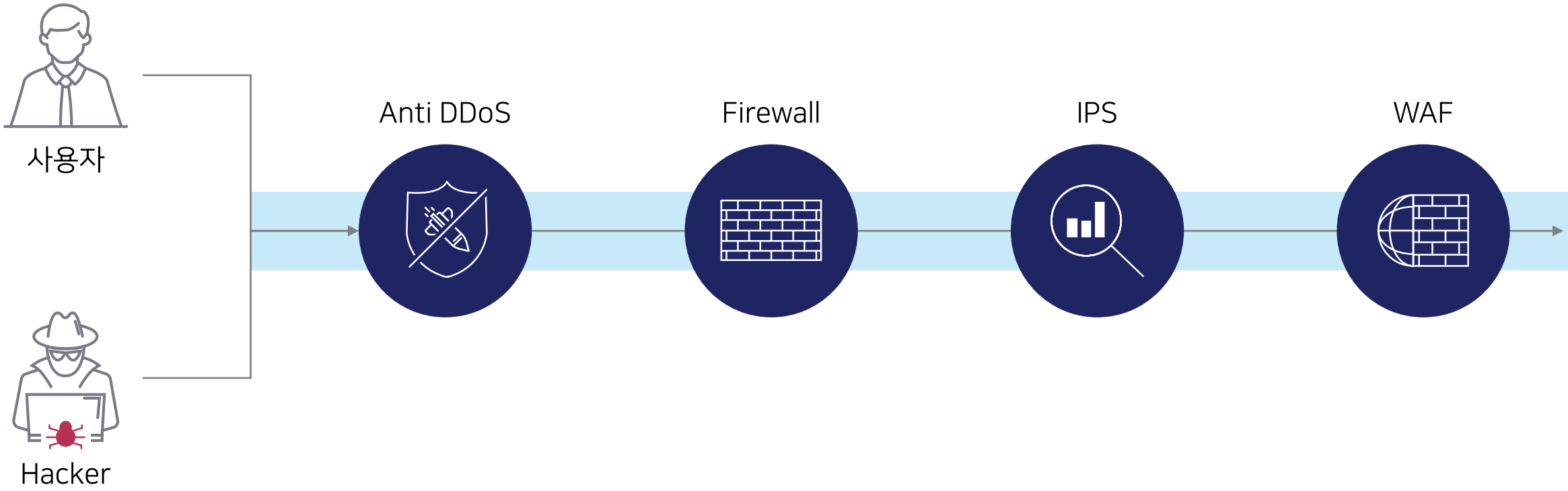
WAAP '도' 제공하는 기업
HW WAF 비중이 더 큰 기업

클라우드로 클라우드를 보호하는 클라우드 보안 아키텍쳐링 사례

삼성SDS가 고객의 문제 상황을 어떻게 해결해 나갔는지 그 과정을 함께 살펴보도록 하겠습니다.

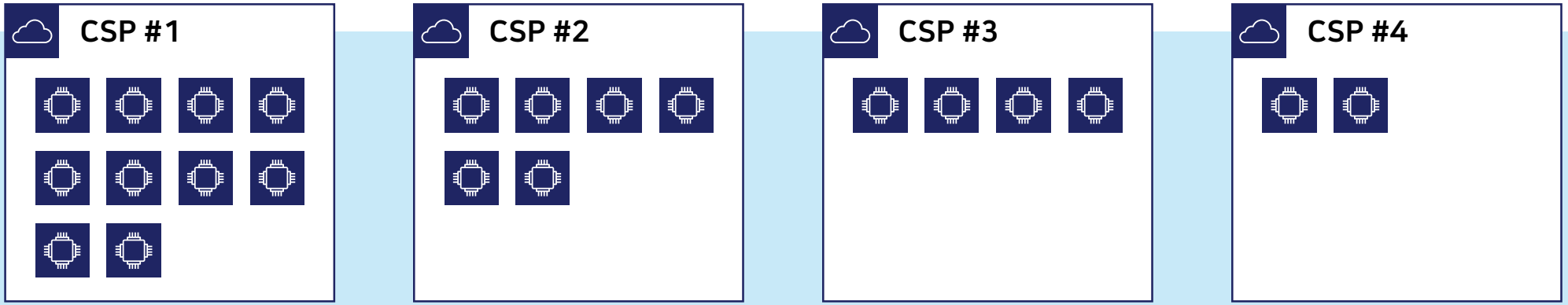
고객 요구사항

고객은 클라우드 상에도 On-premise에서 사용하던 보안 솔루션이 빠짐없이 구현되기를 원했습니다.



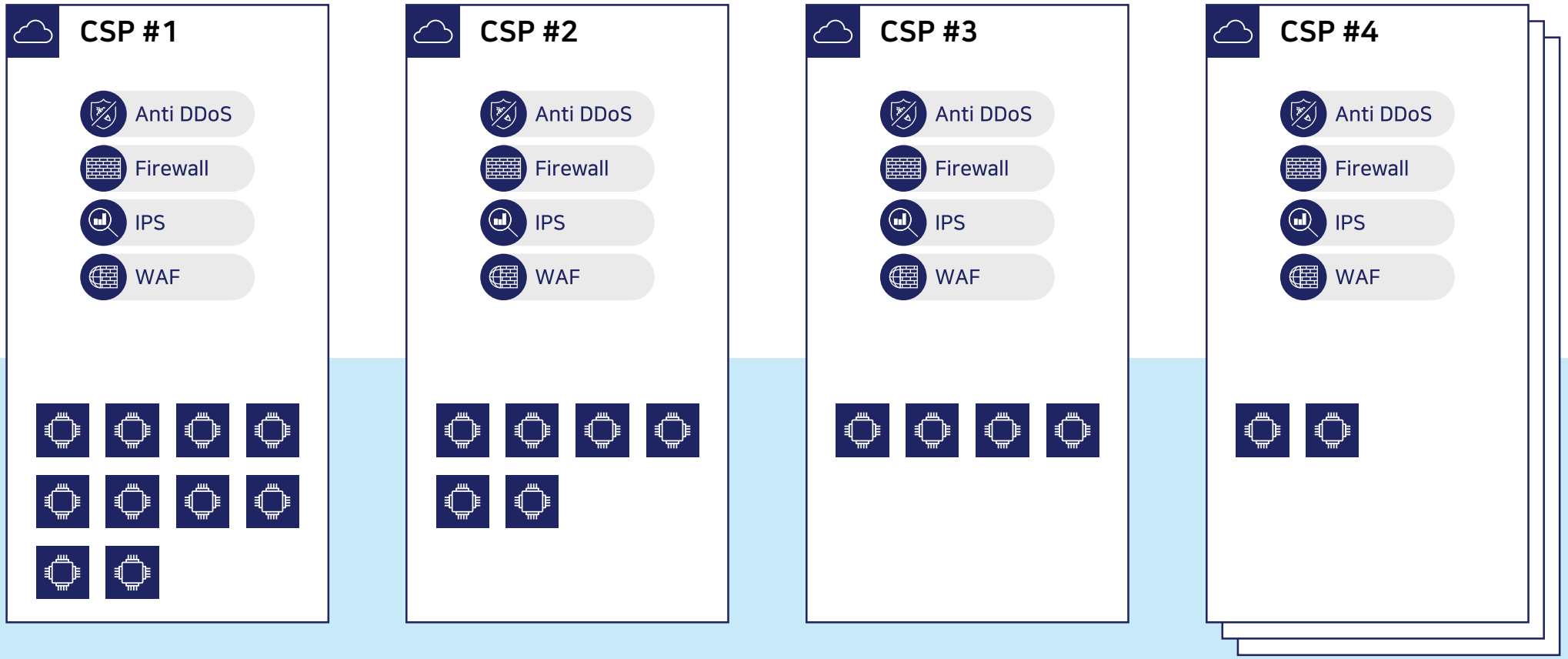
고객 상황

고객은 운영중인 다양한 서비스를 모두 Public 클라우드로 전환하고자 하였습니다.
서비스 별 특성에 따른 효율적인 구성을 위해 멀티 클라우드를 사용하였고, 클라우드마다 사용량은 상이했습니다.



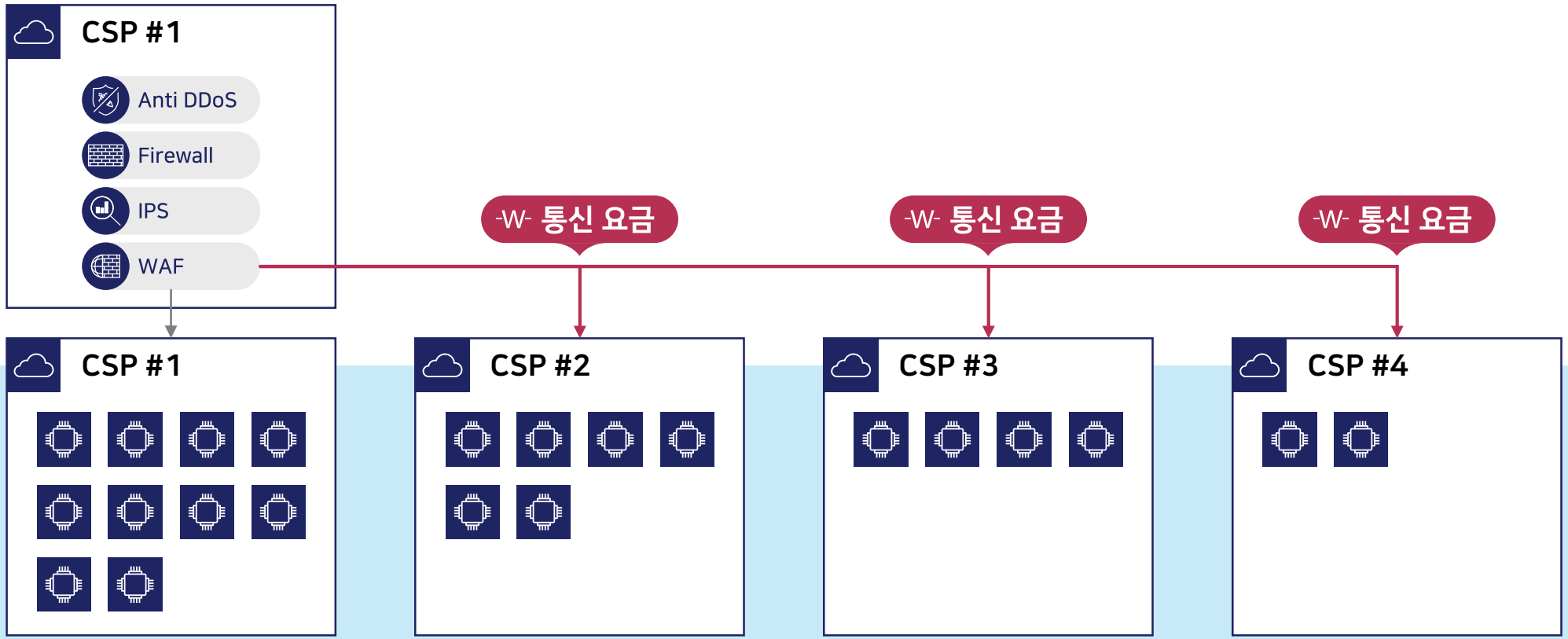
문제 상황

클라우드 인프라를 제공하는 다수의 CSP 별로 보안 솔루션을 구축하면,
서비스를 위한 인프라 비용보다 보안으로 인한 비용이 더 크게 발생하는 문제가 발생했습니다.



해결 방안의 모색

모든 CSP가 공용으로 이용할 수 있는 보안 관문을 직접 만들어 보려고도 했습니다.
하지만 CSP 사이의 통신 요금이 고객에게 전가되기 때문에 여전히 비용 효율적이지 못했습니다.

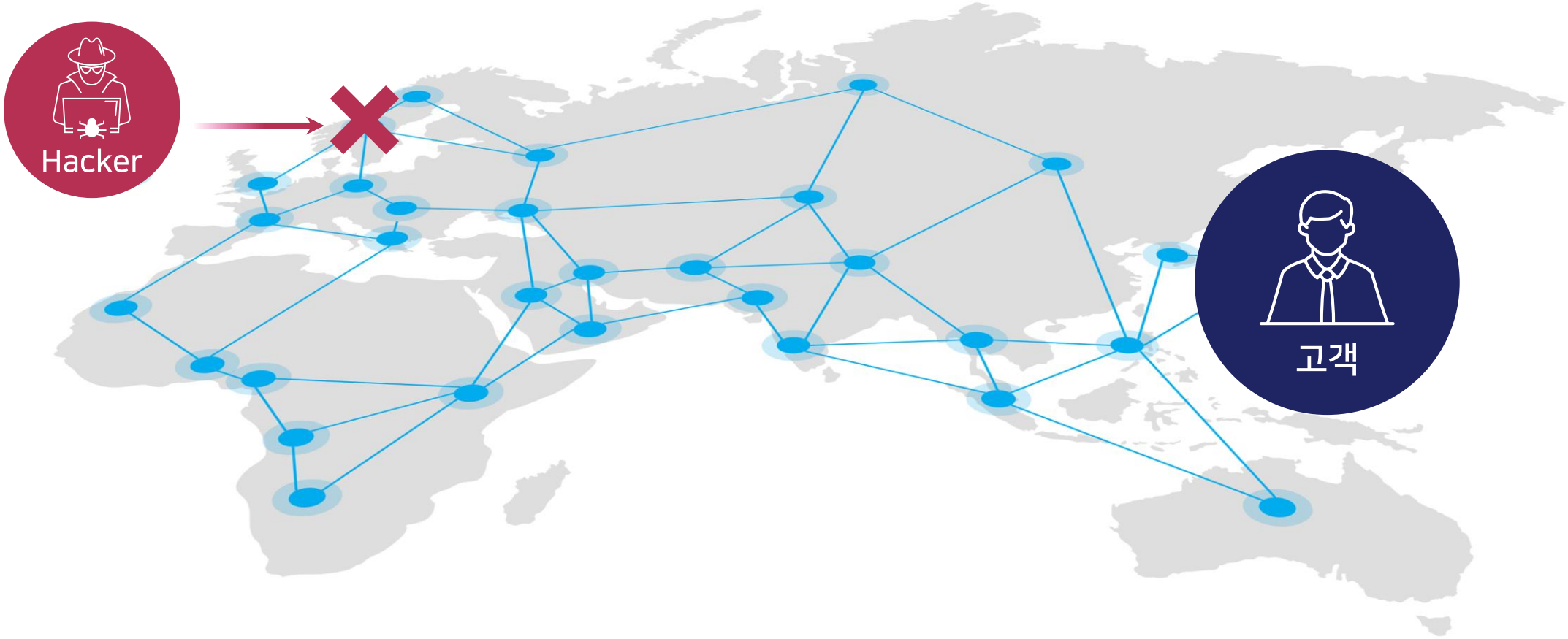


클라우드 기반 WAAP의 활용

클라우드 환경에서 특정 CSP에 보안 장비를 구축한다면,
Hacker의 공격이 고객 서비스 인프라까지 도달한 이후에 방어하는 On-Premise 방식과 차이가 없습니다.

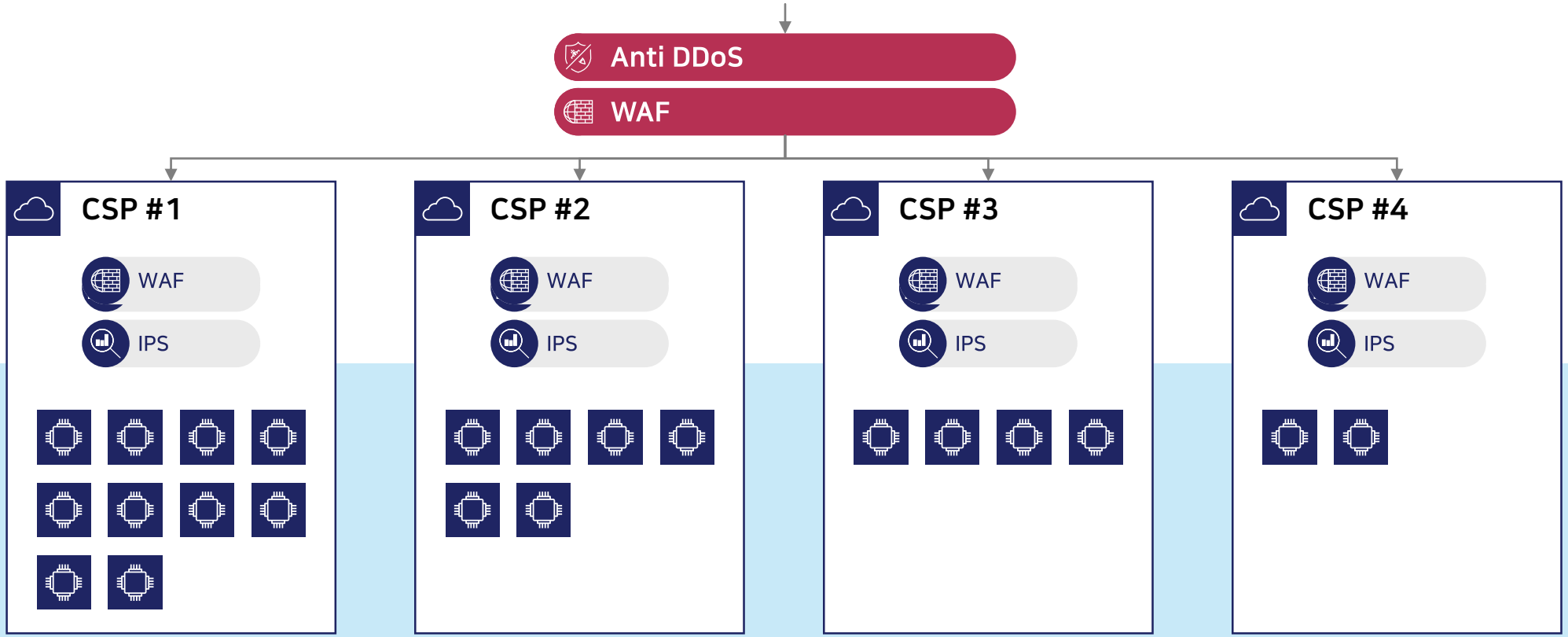
클라우드 기반 WAAP의 활용

반면 Cloud-based WAAP은 글로벌 통신 거점에 구축된 보안 장비가 현지에서 Hacker의 공격을 차단하는 방식입니다.
일종의 망 사업자와 보안 사업자가 합쳐진 개념입니다.



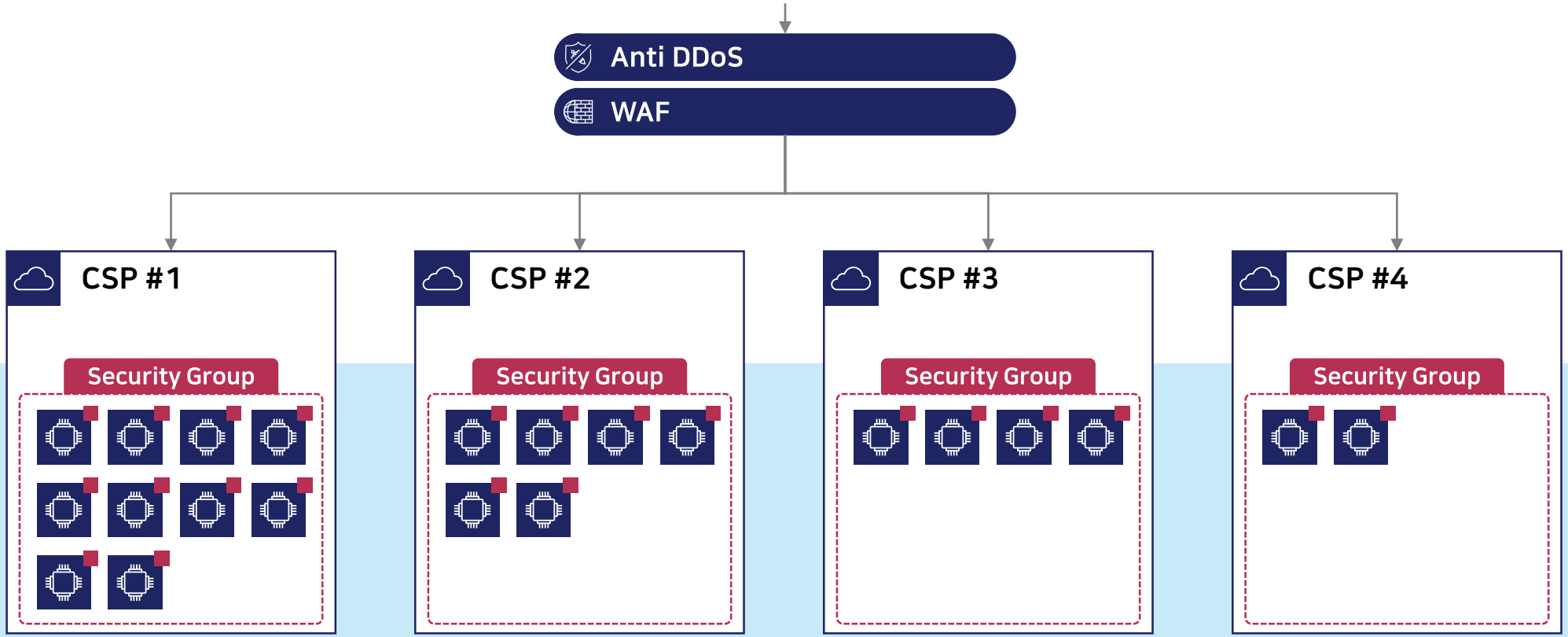
통합하기

Cloud-based WAAP은 글로벌 분산된 보안 거점을 통한 공격 방어가 용이하므로
삼성SDS는 CSP별 보안 구성에서 WAF와 Anti-DDoS를 삭제하고 통신 경로를 일원화 하였습니다.



분산하기

IPS는 삼성SDS가 다년간의 보안관제 서비스 노하우를 가지고 있는 Host 기반 IPS Agent 설치로 대체하였고
방화벽은 CSP의 Security Group으로 대체하되, 의료/금융 같은 업종은 법 제도에 따라 추후 도입하기로 하였습니다.



설계 완료

Cloud-based WAAP를 통해 고객이 어떤 CSP, 어떤 지역의 클라우드를 사용해도 Hacker의 공격을 효율적으로 방어할 수 있도록 보안 설계를 마쳤습니다.

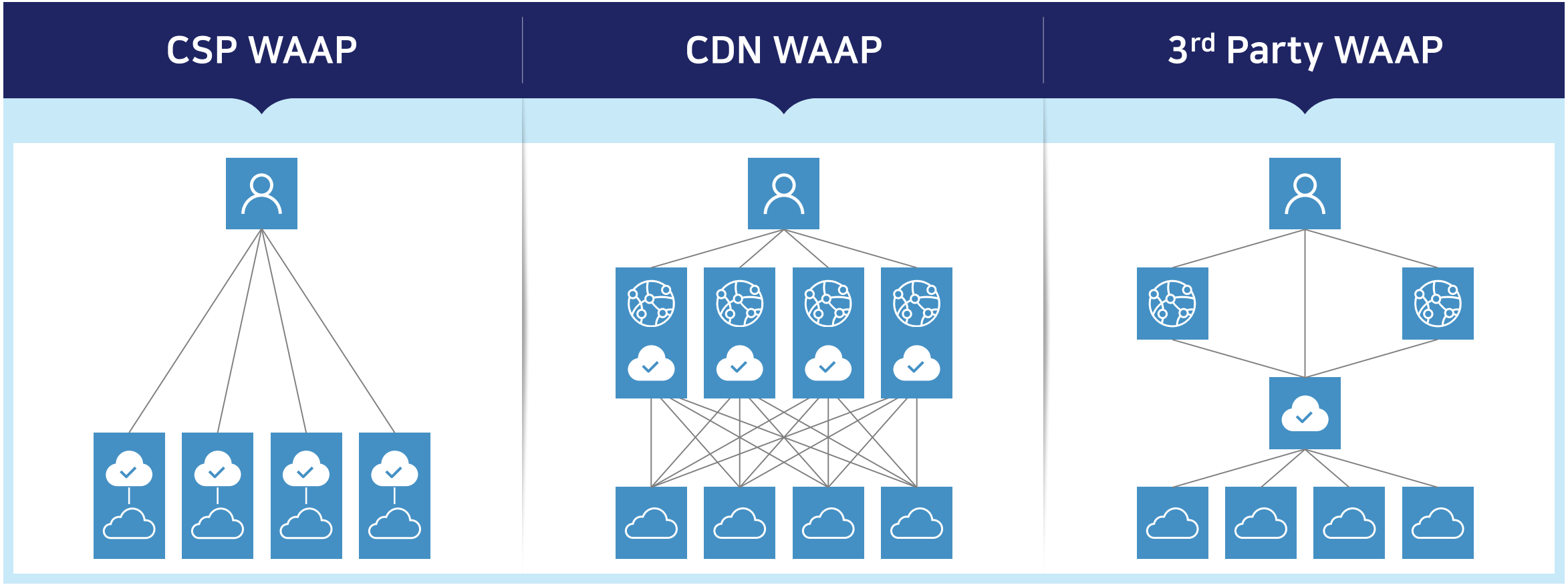
또 다른 고민의 시작

삼성SDS Cloud-based WAAP 서비스를 위한 WAAP 솔루션을 선정해야 했습니다.
여러 WAAP 사업자 중 최고를 선택하는 것도 중요하지만 고객의 상황에 최적화 가능한 솔루션이 필요했습니다.

CSP WAAP	CDN WAAP	3rd Party WAAP
amazon	Akamai	imperva
Microsoft	CLOUDFLARE	f5
ORACLE	Limelight NETWORKS	FORTINET
Google	CDNetworks	Barracuda. Your journey, secured.
		radware availability | performance | security

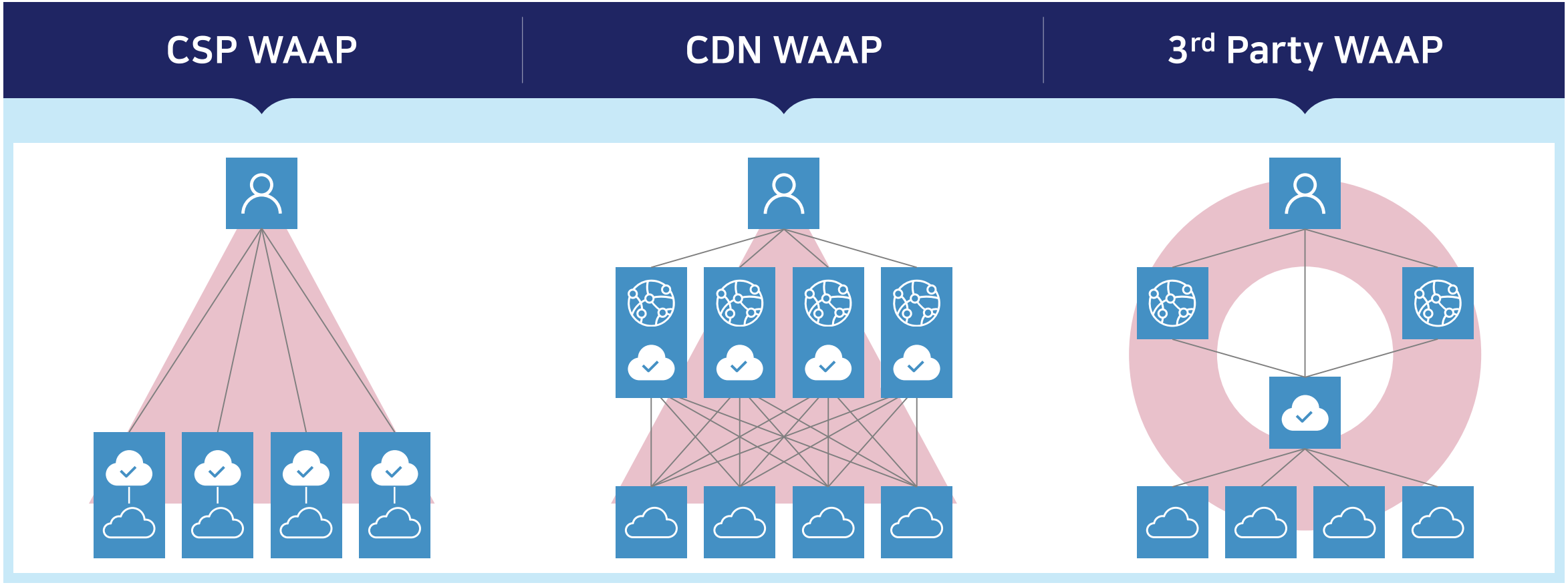
최적의 WAAP 선정하기

CSP, CDN 사업자, 3rd Party WAAP 모두가 장단점이 있었지만,
3rd Party WAAP 솔루션이 다양한 고객 환경에 따라 가장 탄력적인 아키텍쳐를 제공할 수 있었습니다.



표준과 예외

삼성SDS의 표준으로는 3rd Party의 WAAP 솔루션을 채택해서 모든 고객 환경에 WAAP 적용이 가능하도록 했습니다.
다만, 특정한 고객의 상황에 따라 CDN WAAP를 선별적으로 사용하기도 하였습니다.



결론

Cloud-based WAAP가 장점이 많지만 때론 Legacy 방식의 보안 아키텍처도 좋은 대안이 될 수 있습니다.
Legacy부터 클라우드까지 많은 경험과 노하우가 있는 삼성SDS가 도움이 되어드리겠습니다.

	Legacy	Cloud-based WAAP
용량	✔ 보안 솔루션이 설치된 VM의 성능과 수에 비례한 방어 용량	✔ 글로벌 각지에 분산 배치된 고용량 보안 인프라 활용
구성	✔ 각 CSP, 각 Region별 구축	✔ 전용 보안 장비 구축 필요 없음 ✔ 보안 서비스 필요 시 즉시 적용 가능
정책	✔ 고객의 정기/비정기 업데이트	✔ WAAP 사업자의 일괄 업데이트
비용	✔ 초기 투자 비용 소요 ✔ 사용량과 무관한 고정 비용 발생	✔ 서비스형 보안으로써 초기 구축 비용 없음 ✔ 사용량 기반의 과금

삼성SDS 차별화 포인트

POINT 01

클라우드 보안 전문성

- ✓ 국내 최초 클라우드 보안관제 개시
- ✓ 다수의 클라우드 보안 컨설팅 경험 보유

POINT 02

Application 보안 노하우

- ✓ 20년간의 Web Application 보안 정책 개발
- ✓ 관제 서비스 역량 보유

POINT 03

풍부한 WAAP 서비스 경험

- ✓ 다수의 고객, 다양한 클라우드 환경에 대한 WAAP 서비스 및 트러블슈팅 경험 보유


경계면 보안 아키텍쳐
Cloud-based
WAAP
권한 관리
아키텍쳐
Multi-account
아키텍쳐
내부 이상징후
탐지 체계
데이터 보안
아키텍쳐

Thank you

SAMSUNG SDS