CLOUD INSIGHT

클라우드 보안,

Cloud Security

9개 키워드로 완벽 정복

Part_2

BESPIN GLOBAL

HELPING YOU ADOPT CLOUD.

클라우드 보안,

9개 키워드로 완벽 정복 Part_2

요약

기업의 IT 보안 담당자들이 반드시 알아야 할 가이드입니다. 최신 클라우드 보안 개념부터 현재 가장 트렌디한 클라우드 보안 전략까지 다루고 있습니다. 클라우드 보안 아키텍처를 고민중이라면 이 문서를 반드시 숙지하셔야 합니다. 클라우드 보안 9개의 키워드 중 1편에서는 1~5를 다루고, 2편에서는 6~9를 알려 드립니다.

Contents

Part_1

01 클라우드 보안 아키텍처
02 클라우드 보안 아키텍트
03 클라우드 리스크 진단
04 네이티브 클라우드 공급자 보안
05 클라우드 보안 통제 브로커

Part_2

06 클라우드 보안 형상 관리
07 클라우드 워크로드 보호 플랫폼
08 보안 접근 서비스 엣지
09 클라우드 보안의 논리적 아키텍처

6

클라우드 보안 형상 관리

Cloud Security Posture Management

클라우드 보안 형상 관리(CSPM) 툴은 일반적으로 IaaS나 CSP가 제공하는 PaaS 서비스를 위한 클라우드 컨트롤 플레인 상의 보안 설정 진단을 넘어서서, 정책 위반시 이러한 공급자가 조치할 수 있는 능력 등 관리 기능을 제공합니다. 이들은 클라우드 오딧 및 운영 이벤트 검토를 통한 리스크 판별 및 알림 기능을 제공합니다. CSPM은 정의된 보안 프레임워크와 표준에 매핑된 시각화 및 리포팅 기능을 제공해, 컴플라이언스를 지원합니다.

CSPM 툴은 아래 기능을 지원합니다.

컴플라이언스 진단
베스트 프랙티스와 강화되는 지침에 기반해 구독과 배포 환경 설정을 검토합니다.
진단은 PCI DSS, HIPAA, 보안 규칙, NIST 사이버보안 프레임워크 등 주어진 표준에 따라 정의되는 경우가 많습니다.

운영 모니터링
이용하는 클라우드와 배포된 환경 소스로부터 로그 피드를 수집하고,
알림 기능을 제공합니다.

데브옵스 통합
플랫폼은 서비스 API를 노출하여 지속적 통합 및 배포(CI/CD)를 위한 데브옵스 자동화를 더 심화시킵니다. 예를 들면 리스크 해결을 위한 위한 세부 정보를 배포 전 설정 관리 프로세스에 다시 제공할 수 있습니다.

인시던트 대응
모니터링 및 알림과 연계하여 인시던트 관리 및 경감을 위한 기능을 제공합니다.

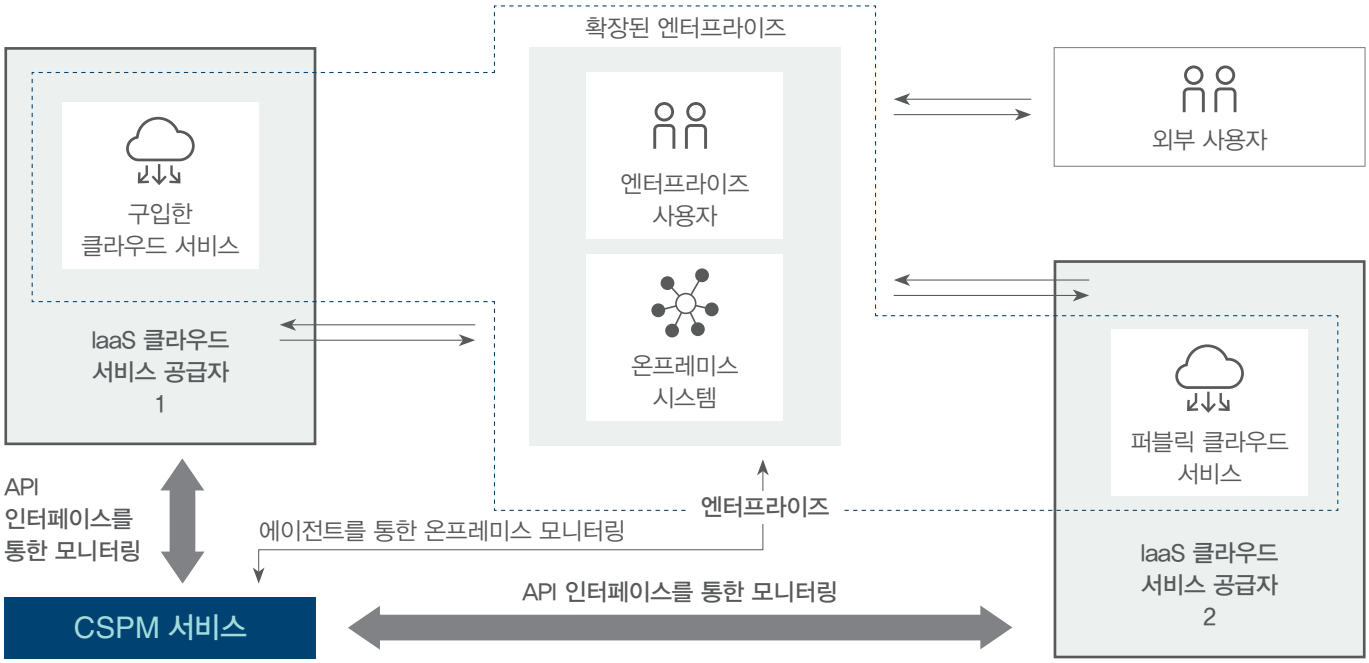
리스크 판별
모니터링, 진단, 컴플라이언스 정보를 종합해 클라우드 환경에서 리스크를 판별하고 우선순위화할 수 있는 방법을 제공합니다.

리스크 시각화
판별된 리스크를 쉽게 시각화할 수 있는 방법을 제공합니다. 리스크에 더 깊이 파고들어 중요도 낮은 정보와 세부사항까지 파악해 운영, 선별, 인시던트 대응을 지원할 수 있게 합니다.

표 6은 CSPM을 활용한 가장 일반적인 유스 케이스를 보여줍니다.

6
클라우드 보안 형상 관리
Cloud Security Posture Management

표6 _ CSPM의 일반적인 멀티클라우드 유즈케이스



Source : Gartner
720923_C

아키텍트들은 클라우드 네이티브한 데이터와 어플리케이션 통제를 승인하고 강화하기 위해 CSPM을 사용합니다. CSPM은 IaaS 환경의 대리 관리와 보안 통제를 가능하게 합니다. CSPM은 주어진 보안 리스크에 대한 알림을 제공하고, 어떤 경우에는 해결을 자동화할 수 있는 방법을 제공합니다. 또한 설정 이슈, 취약점, 위협, 그리고 실제 이벤트 사이의 리스크 측량을 실시간으로 제공합니다.

CSPM은 설정 이슈 및 베스트 프랙티스에서 벗어나는 부분을 발견해 워크로드 이슈와 잠재적인 공격 노출을 탐지합니다. 이는 보안 운영 센터와 인시던트 팀에 기술적인 인사이트를 제공합니다. 많은 툴들은 네이티브 모니터링 및 알림 툴과 상호작용하여 효과적인 인시던트 탐지 및 에스컬레이션을 제공합니다.

CSPM은 호스트/워크로드에서부터 클라우드 관리 레이어까지 IaaS 클라우드 배포의 올바른 설정을 가능하게 합니다. 많은 CSPM 시스템은 CSP 네이티브 보안 로그와 서드파티 보안 아웃풋을 처리해 더 심도 깊은 안정성을 제공합니다. 일부는 계정 플랫폼 또는 네이티브 클라우드 계정과 연동해 IaaS 클라우드 관리자 권한에 접근할 수 있는 특권 접근 통제를 제공합니다.

7 클라우드 워크로드 보호 플랫폼

Cloud Workload Protection Platforms

클라우드 워크로드 보호 플랫폼(CWPP)은 거의 인프라 워크로드에만 유일하게 집중하는 다양한 기능의 조합을 제공합니다. 벤더 솔루션들은 카테고리에 따라 다양합니다. 어떤 솔루션은 넓은 범위의 기능을 제공하지만, 어떤 솔루션들은 '컨테이너화'와 같은 하나의 보호 접근법이나 배포 패턴에만 집중합니다.

CWPP 벤더 서비스는 기업이 CSP가 네이티브로 제공하는 기능들이 일부 보안 요구사항을 해결하고 있다는 전제 하에, 기업의 IaaS 활용에 맞는 다양한 기능의 조합을 제공합니다. CWPP 기능과 벤더가 제공하는 기능을 이해한 후에, 적합한 툴을 선택하세요. 표 7은 CWPP 툴들의 분류에 따라 제공되는 기본 기능을 정리한 것입니다. 물론 여기 보이는 것 외에도 벤더들은 차별화된 서비스를 추가로 제공합니다.

표7 _ CWPP 종류와 기본 기능

공간 노출 영역 축소 | 실행 전 보호 | 실행 후 보호

CWPP의 핵심 기능	CWPP 변형						
	전체 영역	컨테이너	서버리스	메모리, 프로세스 무결성 보호	네트워크와 마이크로세그멘테이션	EDR	취약성, 견고화 및 구성 컴플라이언스
견고화 및 구성	■	■		■	■	■	■
호스트 기반 네트워크 방화벽	■	■			■		
마이크로세그멘테이션	■	■			■		
이용방지 및 메모리 보호	■			■			
취약성 점검	■	■					■
어플리케이션 통제	■	■	■	■	■		■
특권 계정 관리	■	■	■				
안티바이러스	■					■	
취약점 차폐	■			■			■
무결성 통제	■	■	■	■			■
사용자 행동 모니터링	■	■	■		■	■	■
침입 탐지/예방	■	■			■	■	
워크로드 EDR						■	
자동 복구	■	■			■	■	■

Source : Gartner
720923_C

8

보안 접근 서비스 엣지

Secure Access
Service Edge

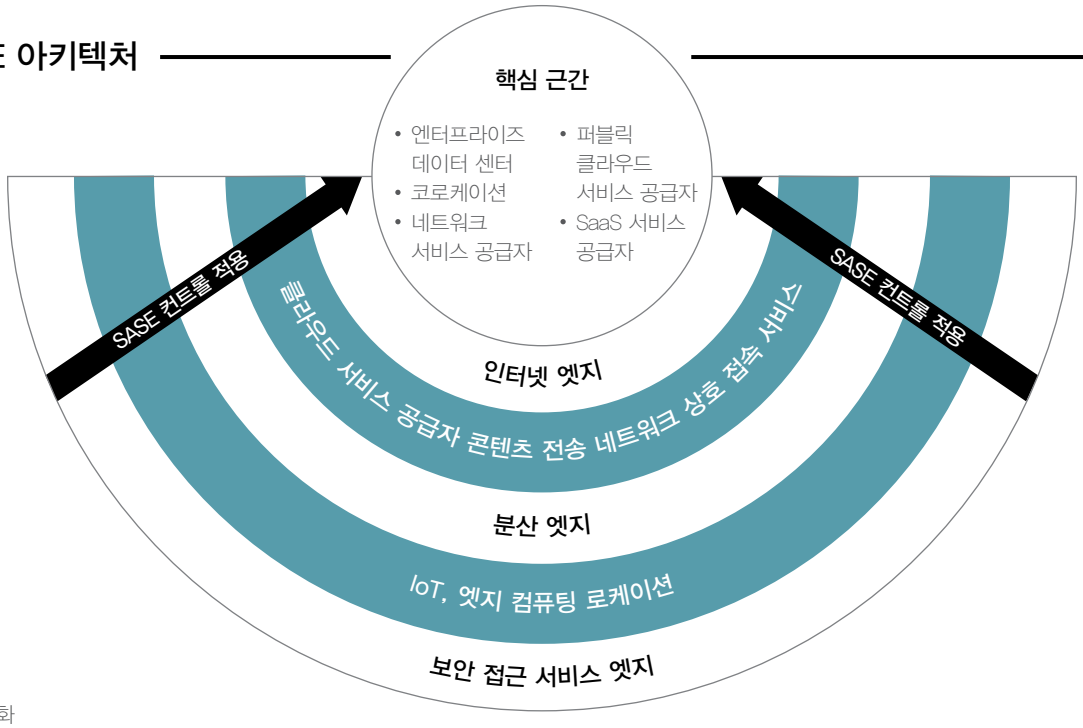
확장성, 유연성, 더 안전한 보안에 대한 요구에 따라 IT 아키텍처는 발전하고 있습니다. 저지연시간 및 WAN-엣지 요구사항과 같은 네트워크 챌린지도 IT 아키텍처의 변화를 부추기고 있습니다. 이렇게 다양한 요인들로 인해 SASE(보안 접근 서비스 엣지)라는 통합 서비스 모델이 등장하게 되었습니다. 클라우드 보안 아키텍트들은 이러한 기대 사항을 인지하고 있어야 하며, 클라우드와 분산 서비스가 성장함에 따라 SASE와 연동된 기능들을 도입해야 합니다.

두 가지 핵심 트렌드가 SASE 아키텍처로의 전환을 주도하고 있습니다.

1. 기업의 데이터가 매우 다양한 서비스 영역에 분산되어 있으며, 대부분 엔터프라이즈 데이터센터 밖으로 이동하고 있습니다. 앞으로 기업 데이터는 IaaS, PaaS와 SaaS를 포함한 모든 종류의 다양한 퍼블릭 클라우드 서비스에 저장되고 처리될 것입니다.

2. 사용자 경험을 개선하기 위해 사용자와 가까운 곳에서 데이터를 처리하는 게 점점 일반적인 일이 되어가고 있습니다. 데이터 분산이라는 첫 번째 트렌드를 고려했을 때, 이 트렌드는 기업이 데이터센터 중심의 중앙 집중 아키텍처에 의존하지 않고 더 효과적으로 트래픽 흐름을 관리하도록 요구합니다.

표8 _ SASE 아키텍처



네트워킹
- 방화벽
- 복원력
- 이중화
- 네트워크 암호화
- 소프트웨어 정의 안전선
- 트래픽 쉐이핑
- 와이파이 보호
- 대역폭 최적화
- DNS 보호
- VPN
- QoS
- 라우팅과 경로선택
- 네트워크 위협 탐지 및 방지

사용자 / 디바이스 / 어플리케이션에 따라 정의되는 맥락
계정/신원 | 신임/리스크 | 역할/권한 | 지리적 정보 | 디바이스

어플리케이션 보안
- 어플리케이션 방화벽
- 웹 어플리케이션 API 보호
- 사용자 및 개체 행동 분석
- 클라우드 앱 디스커버리
- 어플리케이션 위협 탐지 및 방지

서비스 강화
- 레이턴시 개선
- SaaS 가속화
- 비용 최적화

데이터 보안
- 데이터 유실 방지
- 캐싱
- 원격 브라우저 격리
- 난독화
- 데이터 디스커버리
- 지리적 제한

8

보안 접근 서비스 엣지

Secure Access

Service Edge

표 8은 일반적인 SASE의 기능들을 보여줍니다. 이 기능들은 엔드포인트에서 제공되며 사실상 계정 중심입니다. 이것이 특히 중요한 이유는 주어진 어플리케이션을 위해 어떤 클라우드 스타일을 선택하든, 기업이 항상 관리하고 제어해야 하는 것은 계정과 사람의 역할, 계정과 디바이스의 건전성이기 때문입니다. 핵심 서비스에 대한 접근은 사용자의 맥락적 상황(사람인지, 디바이스인지, 머신인지)에 따라 결정됩니다. 이 핵심 서비스들은 다층적이고 상호보완적인 보안 관리의 조합에 따라 접근 결정을 내립니다. 이 조합이 리스크 기반 접근을 결정한다고 볼 수 있습니다. 이들은 다음을 고려합니다.

⇨ 계정 및 신원 자체에 대한 정보
⇨ 허가와 권한을 포함한 유저와 어플리케이션 사이의 신뢰 관계
⇨ 기업 (접속의 맥락에 따른 실시간 평가를 포함)
⇨ 기술적인 보안 및 컴플라이언스 정책의 집행
⇨ 지리적인 제약
⇨ 연결하는 디바이스에 대한 정보

SASE의 핵심 기능은 네트워크, 애플리케이션, 데이터 보안 등 기존 영역에 분산됩니다. 또한 현대적인 분산 데이터를 더 효과적으로 관리하는 기능도 포함합니다. 서비스는 소프트웨어 정의 WAN(SD-WAN), SWG, CASB 그리고 제로트러스트 네트워크 액세스(ZTNA)를 포함하며, 암호화와 위협 탐지 모니터링을 포함해 전송 중인 데이터를 보호하는 기능을 하는 서비스형 방화벽(FWaaS)도 포함합니다. 권장하는 기능으로는 웹 어플리케이션과 API 보호 (WAAP), 원격 브라우저 격리, 재귀적 DNS, 네트워크 샌드박스를 포함합니다. 추가적인 운영 기능은 상황과 유즈케이스에 따라 다르며, 와이파이 핫스팟 보호, 네트워크 속임수, 레거시 VPN 지원, 오프라인 또는 캐시 상태의 보호를 제공하는 엣지 컴퓨팅 보호 등이 있을 수 있습니다. 향후 SASE가 데이터 맥락에 따른 API 기반 접근통제 등을 제공하면 SaaS 도입에 도움이 될 수 있으며, 관리되는 디바이스와 관리되지 않는 디바이스 모두 지원하는 기능이 향후 출시될 수 있습니다. SASE는 아직 범용적으로 사용되고 있진 않지만, 핵심 보안 문제를 해결하는 신규 기능들을 제공합니다.

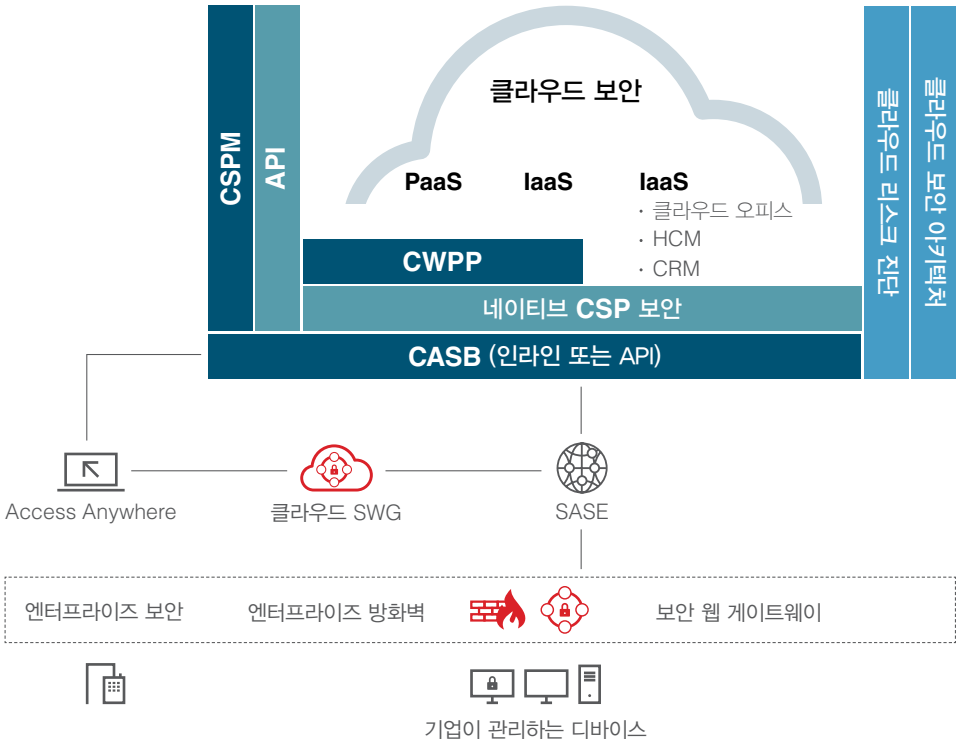
9

클라우드 보안의 논리적 아키텍처

Cloud Security
Logical Architecture

지금까지 모든 레이어와 컴포넌트를 다루었기 때문에, 이를 기반으로 논리적인 아키텍처를 설계하고 클라우드 보안의 모든 구성요소가 어떻게 짜맞추어지는지 확인할 수 있습니다. 일부 경우에는 온프레미스 EFW나 SWG를 여전히 제대로 구성해야 합니다. 오피스365 트래픽의 경우, 이러한 솔루션을 우회하여 바로 마이크로소프트로 트래픽을 라우팅해야 합니다. 이것이 API나 인라인 프록시와 같은 배포 옵션을 이해하는 게 클라우드 보안 솔루션 구축에 중요한 이유입니다. 표 9는 모든 가능한 클라우드 보안 솔루션과 프로세스를 결합했을 때의 논리적인 클라우드 보안 아키텍처를 보여줍니다.

표9 _ **클라우드 보안의 논리적 아키텍처**



Source : Gartner
720923_C

결론

Conclusion

클라우드 보안은 매우 복잡하며 기존 보안 아키텍처에 방대한 영향을 미칩니다. 좋은 소식은 클라우드 공급자들과 클라우드 보안 솔루션 모두 발전하고 있다는 것입니다. 클라우드 보안 아키텍처와 클라우드 보안 아키텍트 롤은 베스트 프랙티스, 경영진의 방침, 실제 현업 사례 등이 결정합니다.

클라우드 보안과 리스크 관리의 핵심 토픽은 매우 빠르게 바뀌고 있습니다. 기술 전문가들은 더 애자일한 프로세스에 따라 변화를 수용해야 클라우드 인프라를 최신 위협으로부터 지킬 수 있을 것입니다.

클라우드 보안 아키텍처 롤과 책임을 정해서 보안 전략을 이끌도록 하는 데서 시작하세요. 그 다음에 요구사항에 맞는 클라우드 네이티브와 서드파티 툴로 구성된 클라우드 보안 전략을 수립하세요.

다음으로, 하나의 IaaS 클라우드를 사용하는 기업이라면 IaaS, PaaS, SaaS 공급자가 제공하는 빌트인 보안 기능을 먼저 활용하세요. 이미 멀티클라우드 전략을 수립했거나 새로운 공급자를 사용하는 기업이라면, CASB, CSPM과 CWPP 같은 솔루션을 고려하세요. CASB가 SaaS와 IaaS를 위한 기능을 지원하기 때문에, 대부분의 기업은 CASB로 시작을 합니다. CASB는 아래와 같은 기능을 제공합니다.

⇨ 여러 개의 클라우드 어플리케이션에 걸쳐 모니터링, 정책 생성 및 위협 경감이 가능한 통합 대시보드 제공

⇨ 기존에 사용하는 SWG와 EFW 인프라와 연동해 쉐도우 IT 클라우드 앱 사용에 대한 가시성을 제공

⇨ 클라우드 앱 리스크 데이터베이스를 사용해 기본적인 클라우드 리스크 진단을 할 수 있는 유용한 툴

IaaS와 PaaS에 대한 더 심화된 요구사항을 정립하게 되면 CSPM 툴을 사용해 클라우드 컨트롤 플레인, 보안 구성, IaaS 보안 안전선에 대한 가시성을 확보하세요. 또 CWPP 벤더 툴을 사용해, 점점 컨테이너와 서버리스 기능이 추가되는 워크로드의 보안 구성에 대해 가시성과 컨트롤을 확보하세요.

CSPM 툴은 다음을 도와줍니다:

- 자동화된 보안 스캐닝과 복원
- 클라우드 침입의 가장 큰 원인인 고객의 잘못된 구성을 방지
- 클라우드 서비스 운영 모니터링

CWPP 툴은 다음을 도와줍니다:

- 컨테이너와 VM을 위한 보호
- 네트워크 분할 정책 생성과 모니터링
- 워크로드 구성 관리
- 어플리케이션 화이트리스트 작성
- 시스템 건전성 확인

심화된 솔루션을 도입하고 나면, SASE 도입을 고려하세요. 중장기적인 미래를 봤을 때 안정적이고 확장성있는 원격 액세스 아키텍처를 만드는 것이 좋습니다.

◇

CSPM과 CWPP 조건을 동시에 만족하는 유일한 솔루션은
팔로알토네트웍스(PaloAlto Networks)의 '프리즈마 클라우드(Prisma Cloud)'입니다.

베스핀글로벌은 팔로알토 네트웍스와 '클라우드 보안 서비스(MSSP)파트너십'을 맺고
'프리즈마'를 제공하고 있습니다. 클라우드 보안을 강화하는 완벽한 솔루션을 고민중이라면
지금 무료 상담을 신청하세요.

클라우드 보안 솔루션 무료 상담 신청하기

함께 읽어볼 만한 연관 콘텐츠

– 원격업무, 베스핀글로벌 End-to-end 화상솔루션으로 시작하세요!
– 지속적인 모니터링과 자동화로 이벤트 매니지먼트 개선하는 방법
– 인시던트 관리에 대한 확실한 안내서
– 2019 클라우드 보안 백서
– 다음에는 피해갈 수 있다! 클라우드 장애 대비를 위한 3가지 고려사항
– 퍼블릭 클라우드로의 전환. 문제는 보안?

“Helping You Adopt Cloud.”

클라우드 전문 인력 및 클라우드 관리 어떻게 시작해야 하나요?
클라우드 IT를 대한민국에서 가장 잘 아는 400여 명의 클라우드 전문가를
베스핀글로벌에서 만나실 수 있습니다.

Meet 베스핀글로벌 전문 컨설팅팀

클라우드의 도입을 고민하신다면 베스핀글로벌 컨설팅팀이
최적의 클라우드 컨설팅을 제공해 드립니다.

Meet 아시아 최고의 클라우드 운영팀, 베스핀글로벌 매니지드 서비스팀

클라우드 운영에 대한 노하우가 부족해 걱정이시라면
클라우드 서비스의 베테랑이 여러분의 클라우드를 관리해드립니다.

Meet OpsNow

클라우드 비용을 최대 80% 절감하고, 장애 대응 시간을 절반으로 줄일 수 있는
멀티-클라우드 관리 플랫폼 OpsNow를 만나보세요.

About Bespin Global

국내 최다 클라우드 인증 자격을 보유한 MSP
국내 유일 ISO 인증, ISMS 인증, GS인증을 확보한 MSP
가트너가 인정한 한·중·일 유일한 MSP

베스핀글로벌은 클라우드 IT를 위해 태어난 클라우드 매니지드 서비스 기업입니다.
클라우드 도입을 위한 전략컨 설팅, 클라우드 상에서 수많은 고객의 IT 자산을
안정적으로 운영하고 관리할 수 있는 서비스와 솔루션, 클라우드를 기반한 머신러닝과
빅데이터와 같은 최신 기술의 빠른 도입까지 클라우드로 할 수 있는 전 영역을
End-to-end로 제공합니다. 4년 연속 가트너 매직 쿼드런트 퍼블릭 클라우드 MSP 부문에
한·중·일 최초로 등재되었고, 포브스로부터 한국의 주목할 만한 유니콘으로
선정되기도 했습니다.

클라우드로 가기로 결정하였다면 누구와 함께 갈지를 선택해야 합니다.
처음부터 끝까지 믿을 만한 파트너를 찾는다면 베스핀글로벌이 정답입니다.

클라우드로 가기로 결정했다면
누구와 함께 갈지를 선택해야 합니다.

처음부터 끝까지 믿을만한 파트너를 찾는다면
베스핀글로벌이 정답입니다.

→ 베스핀글로벌 웹사이트
→ 서비스 문의

베스핀글로벌 소셜미디어
→ facebook
→ linkedin
→ youtube

BESPIN GLOBAL
HELPING YOU ADOPT CLOUD.