Could Security

(v1.0)

2023년 6월
안종석
james@jslab.kr

1

I. 클라우드 보안 트렌드 ---------- 3
II. 클라우드 인프라와 보안 ---------- 63
III. 클라우드 보안 솔루션과 비즈니스 ---------- 141

2

I. 클라우드 보안 트렌드

- 클라우드 보안 동향
- 클라우드 보안 제조사 사례
- 클라우드 보안 솔루션 사례

I. 클라우드 보안 트렌드

❖ 모든 시스템 또는 데이터 센터에 대한 대부분의 보안 개념은 클라우드 컴퓨팅에서도 동일

- **Cryptography** (암호화)
- **Access control** (액세스 제어)
- **Data and media sanitation** (데이터 및 미디어 보안)
- **Network security** (네트워크 보안)
- **Virtualization security** (가상화 보안)
- **Common threats** (일반적인 위협)

AAA : 인증(Authentication), 권한(Authorization), 계정관리(Accounting)
- 인증: 망,시스템 접근을 허용하기 전에 사용자의 신원을 검증
- 권한: 검증된 사용자에게 어떤 수준의 권한과 서비스를 허용
- 계정관리: 사용자의 자원에 대한 사용 정보를 모아서, 과금, 감사, 용량증설, 리포팅 등

Certified Cloud Security Professional

Source: Carter, Carter, Daniel (2022-11-24T22:58:59.000). CCSP Certified Cloud Security Professional All-in-One Exam Guide, Third Edition . McGraw Hill LLC. Kindle Edition.

I. 클라우드 보안 트렌드

❖ **PCI**(Payment Card Industry) **compliance:**

- **Level 1: Greater than 6 million credit card transactions a year**
- **Level 2: Between 1 million and 6 million credit card transactions a year**
- **Level 3: 20,000 to 1 million transactions a year**
- **Level 4: Greater than 20,000 transactions a year**

Your Level is:	Your business does:	You should:
4	- less than 20,000 eCommerce transactions per year - less than 1 million other transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
3	- 20,000 - 1 million transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
2	- 1-6 million transactions per year	- complete an annual risk assessment using an SAQ - conduct quarterly PCI scans
1	- 6 million+ transactions per year	- conduct an annual internal audit - conduct quarterly PCI scans

연간 2만건 미만의 온라인 거래 또는 최대 1백만 건의 거래 판매자. 유효성 검사에는 SAQ(또는 자체 평가 설문지), ASV(승인된 스캔 공급업체)의 분기별 네트워크 스캔, 규정 준수 증명 양식이 포함

판매자는 매년 2만~100만 건의 온라인 거래가 발생하며, 검증에는 SAQ, ASV에 의한 분기별 네트워크 스캔 및 규정 준수 증명 양식이 포함

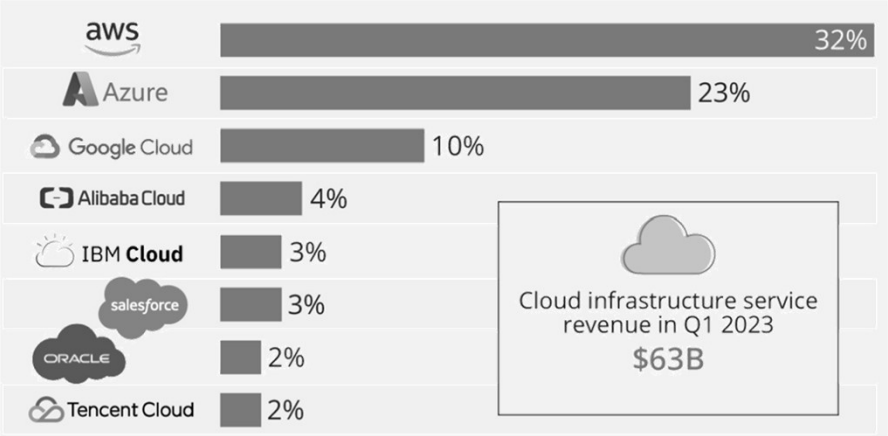
판매자는 매년 100만~600만 건의 온라인 거래가 발생하며, SAQ, ASV에 의한 분기별 네트워크 검사 및 규정 준수 증명 양식이 포함

모든 채널에서 연간 600만 건 이상의 거래가 발생하는 판매자 또는 데이터 유출이 발생한 모든 판매자

PCI-DSS: Payment Card Industry Data Security Standard
Source: Coombs, Ted. Cloud Security For Dummies (p. 124). Wiley. Kindle Edition

I. 클라우드 보안 트렌드

❖ **주요 클라우드 인프라 서비스 제공업체의 전 세계 시장 점유율** (Q1 2023)

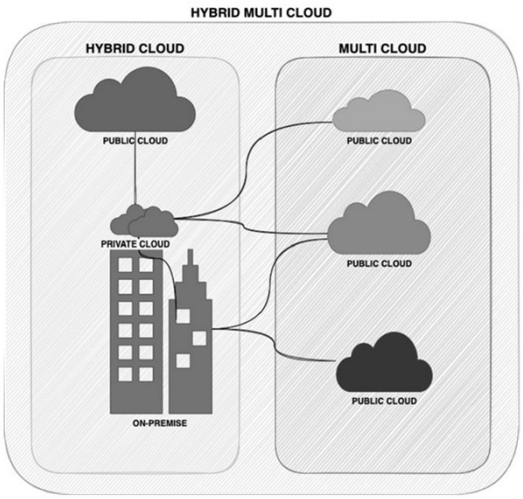


Source: https://www.researchandmarkets.com/reports/5738899/global-multi-cloud-security-market-offering

I. 클라우드 보안 트렌드

❖ **Cloud types (delivery models)**

- **Hybrid multi cloud**
  - On-premise
  - Private cloud
  - Hybrid cloud
  - Multi cloud

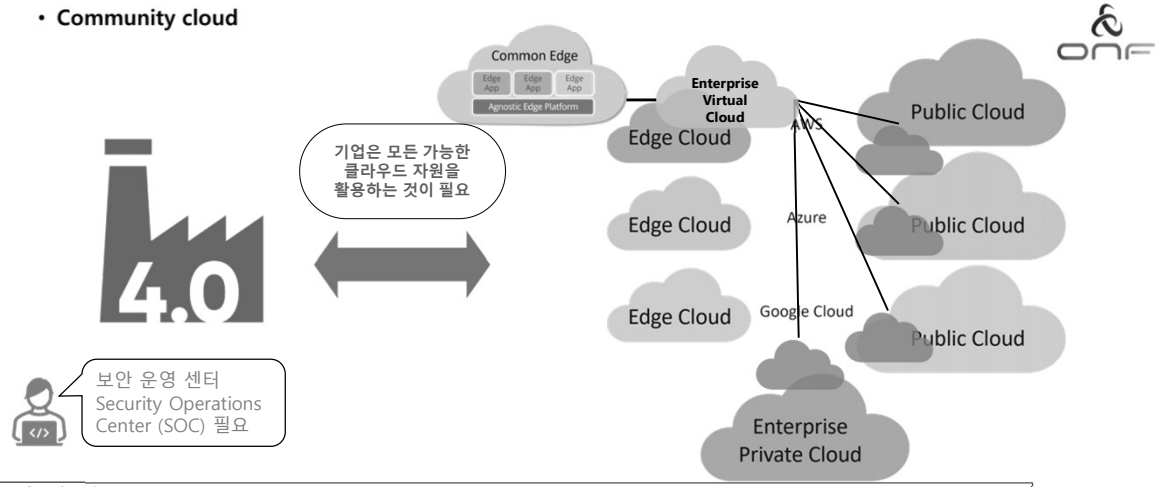


Source: Iyer, Sreekanth (2022-11-17T22:58:59.000). Hybrid Cloud Security Patterns: Leverage modern repeatable architecture patterns to secure your workloads on the cloud . Packt Publishing. Kindle Edition.

I. 클라우드 보안 트렌드

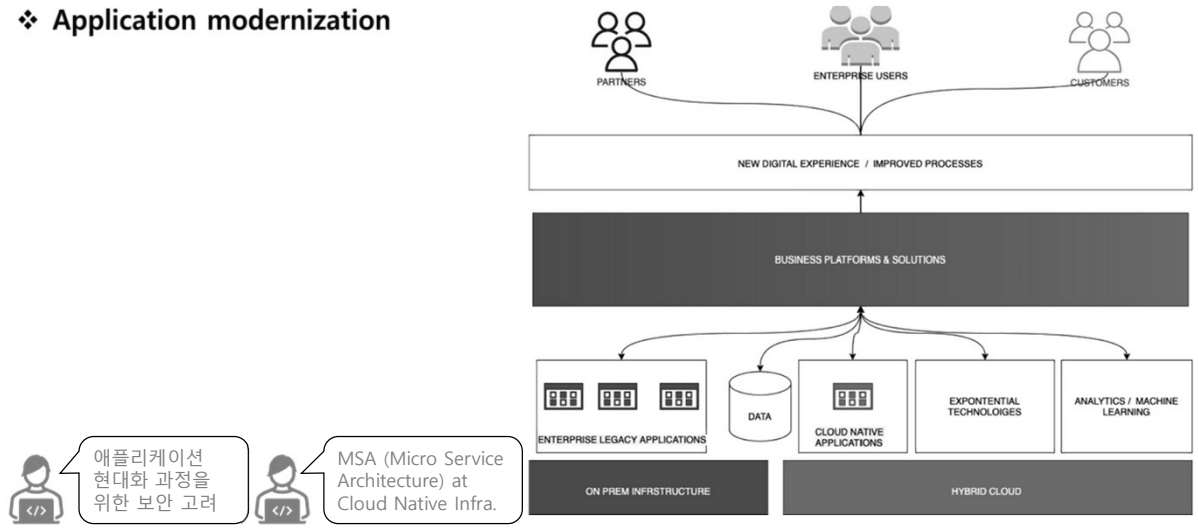
❖ **멀티클라우드는 뉴노멀 (ONF: Enterprise Multi-Cloud is the New Normal)**

- **Can't afford to be tied to just a single hyperscaler – 하나의 'Virtual Cloud' 필요**
- **Community cloud**



I. 클라우드 보안 트렌드

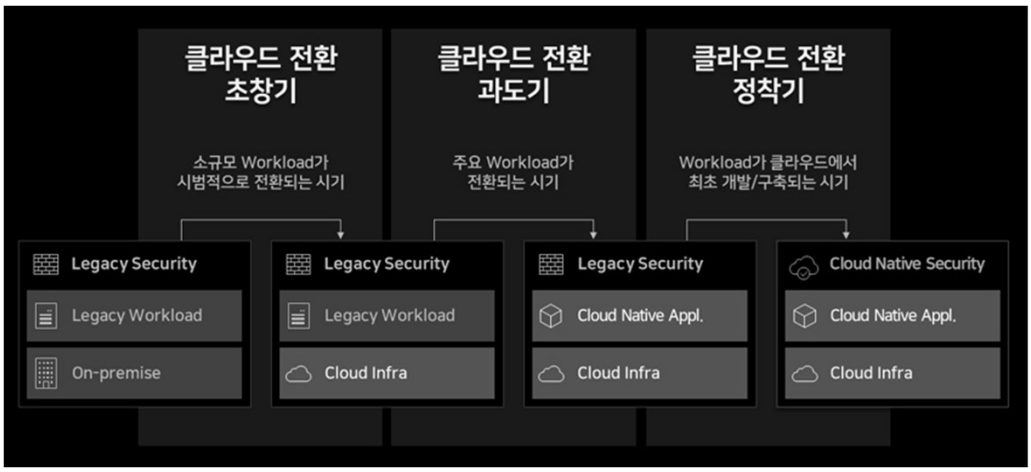
❖ **Application modernization**



Source: Iyer, Sreekanth (2022-11-17T22:58:59.000). Hybrid Cloud Security Patterns: Leverage modern repeatable architecture patterns to secure your workloads on the cloud . Packt Publishing. Kindle Edition.

I. 클라우드 보안 트렌드

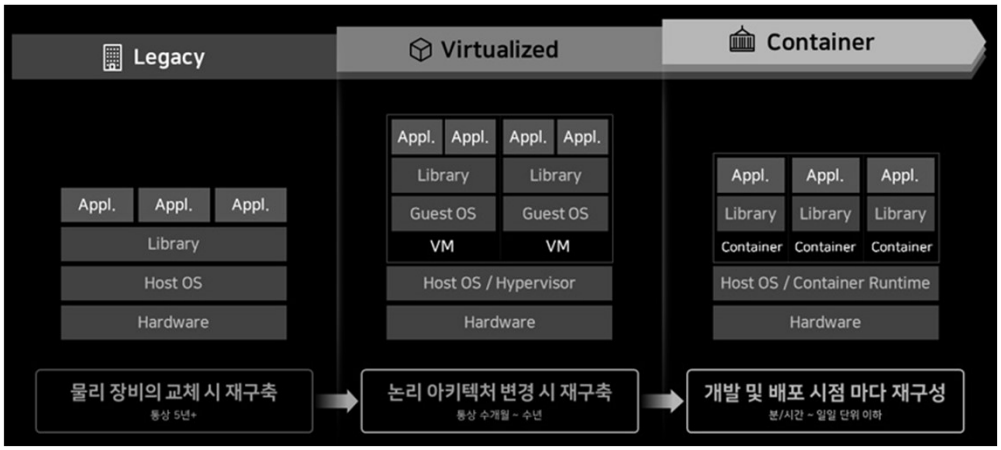
❖ **클라우드 보안의 단계적 접근**



Source: https://www.samsungsds.com/kr/insights/cloud_security.html

I. 클라우드 보안 트렌드

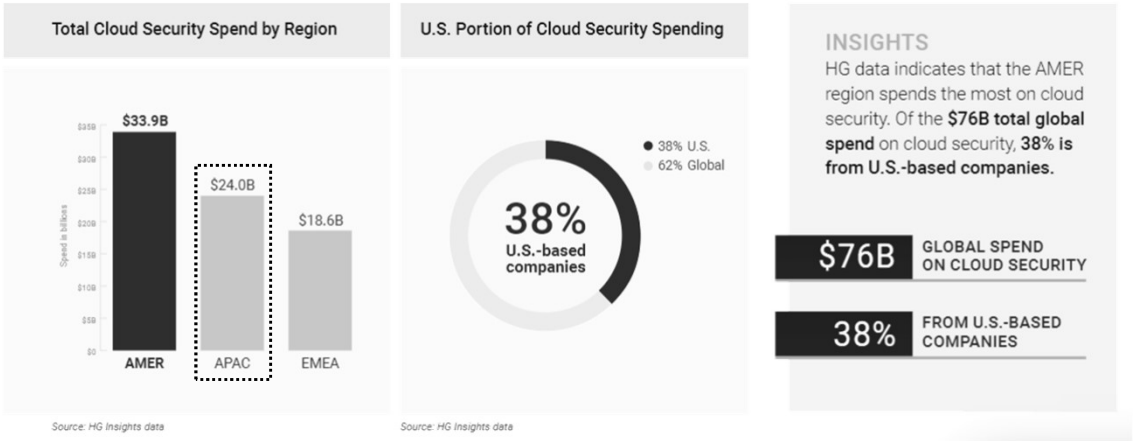
❖ 클라우드 인프라의 변화



Source: https://www.samsungsds.com/kr/insights/cloud_security.html

I. 클라우드 보안 트렌드

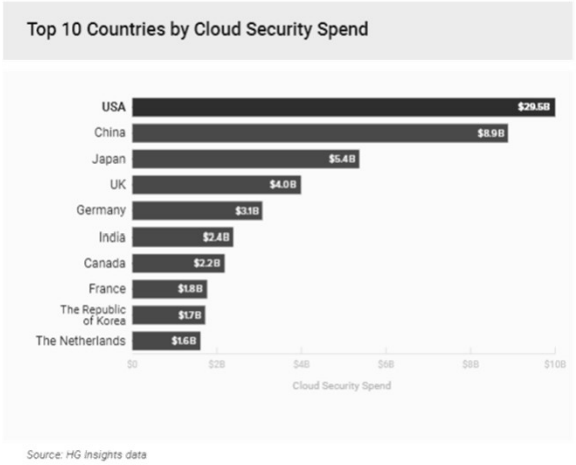
❖ **글로벌 클라우드 보안 시장 규모 및 전망** (2023)

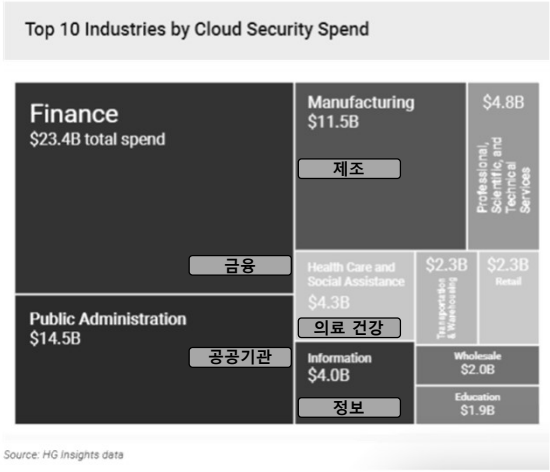


Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

I. 클라우드 보안 트렌드

❖ **Top 10 Countries and Industries by Cloud Security Spend** (2023)





Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

I. 클라우드 보안 트렌드

❖ **2021-2023 전세계 보안 분야별 사용자 지출**

표1. 2021-2023년 전 세계 정보 보안 및 리스크 관리 분야별 최종 사용자 지출(단위: 백만 달러)

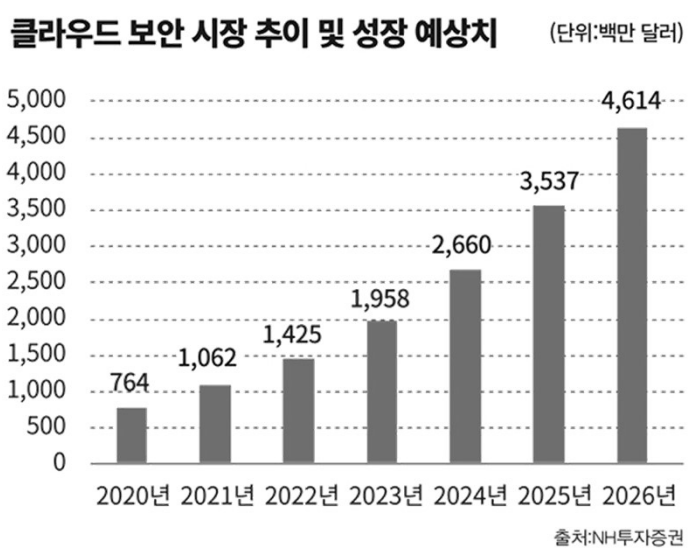
시장 분야	2021 지출	2021 성장률 (%)	2022 지출	2022 성장률(%)	2023 지출	2023 성장률(%)
애플리케이션 보안	4,963	20.8	6,018	21.3	7,503	24.7
클라우드 보안	4,323	36.3	5,276	22.0	6,688	26.8
데이터 개인 정보	1,140	14.2	1,264	10.8	1,477	16.9
데이터 보안	3,193	6.0	3,500	9.6	3,997	14.2
아이덴티티 액세스 관리(IAM)	15,865	22.3	18,019	13.6	20,746	15.1
인프라 보호	24,109	22.5	27,408	13.7	31,810	16.1
통합 리스크 관리(IRM)	5,647	15.4	6,221	10.1	7,034	13.1
네트워크 보안 장비	17,558	12.3	19,076	8.6	20,936	9.7
기타 정보 보안 소프트웨어	1,767	26.2	2,032	15.0	2,305	13.4
보안 서비스	71,081	9.2	71,684	0.8	76,468	6.7
소비자 보안 소프트웨어	8,103	13.7	8,659	6.9	9,374	8.3
총계	157,749.7	14.3	169,156.2	7.2	188,336.2	11.3

출처: 가트너 (2022년10월)

Source: https://zdnet.co.kr/view/?no=20221014164810

I. 클라우드 보안 트렌드

❖ 클라우드 보안 시장



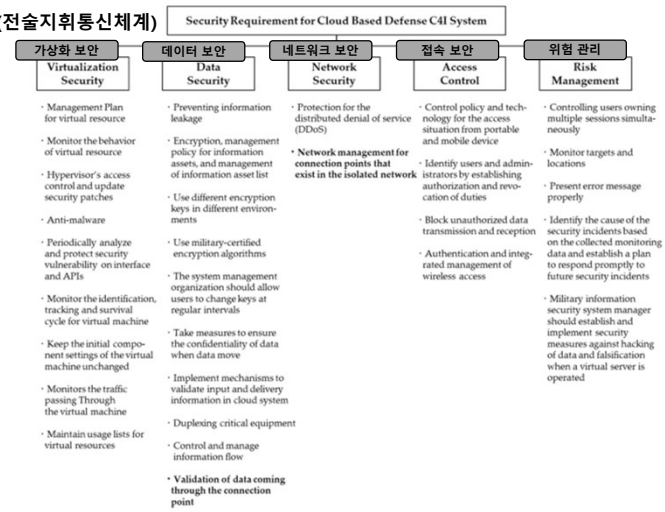
Source: https://www.econovill.com/news/articleView.html?idxno=585396

I. 클라우드 보안 트렌드

❖ Security requirements for cloud-based defense C4I system.

- Risk Management
- Access Control
- Network Security
- Data Security
- Virtualization Security
  - 가상자원 관리
  - 가상자원 모니터
  - 하이퍼바이저 보안
  - Anti-malware
  - 주기적 보안 분석
  - VM 모니터
  - VM 세팅 유지
  - VM 트래픽 모니터
  - 가상 자원 사용 관리

C4I 체계(전술지휘통신체계)

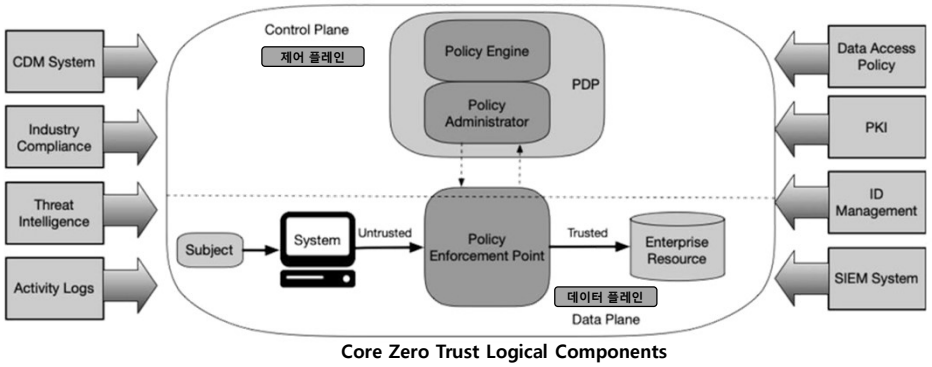


Source: https://www.mdpi.com/2071-1050/13/24/13827/htm

I. 클라우드 보안 트렌드

❖ NIST(National Institute of Standards and Technology), 미국 국립 표준 기술 연구소

• Logical Zero Trust Components: 800-207 Zero Trust Architecture



Core Zero Trust Logical Components

PDP: Policy decision point, PEP: Policy enforcement point

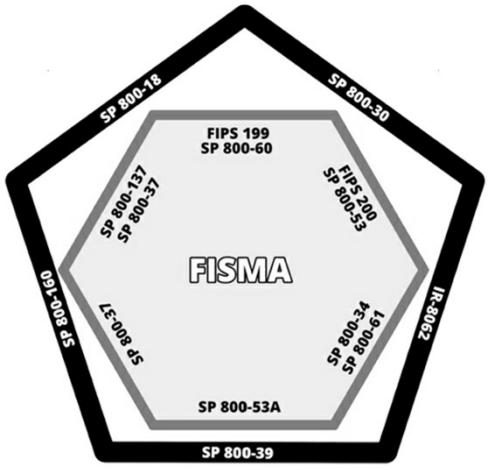
Source: https://www.techrepublic.com/article/zero-trust-security-a-cheat-sheet/

I. 클라우드 보안 트렌드

❖ Federal Information Security Modernization Act:

• FISMA is composed of a number of NIST publications.

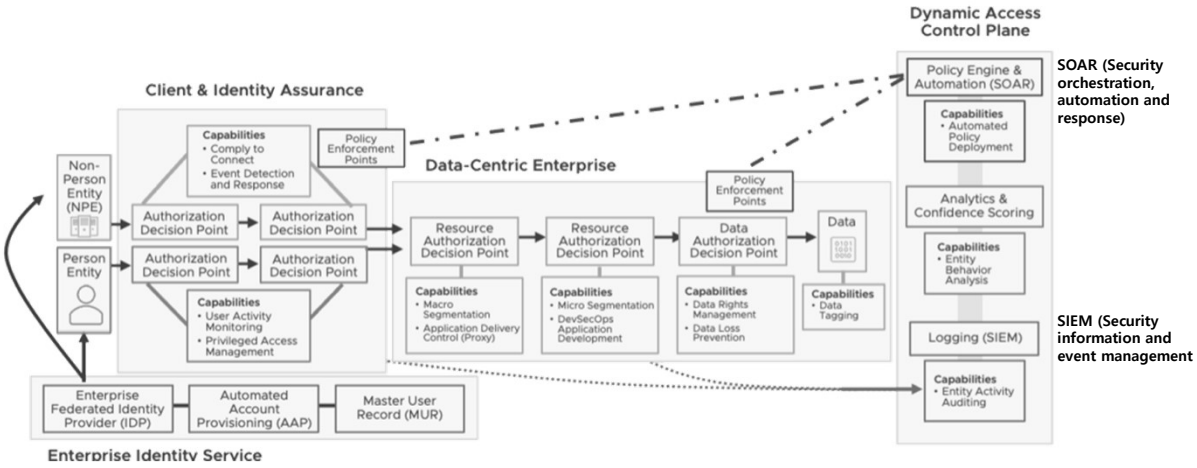
- FIPS-199: Categorization
- SP 800-60 Vol. 1 Rev. 1: Guide for Mapping Types of Information and Information Systems to Security Categories
- SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- SP 800-53A Rev. 5: Assessing Security and Privacy Controls in Information Systems and Organizations
- SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- SP 800-61 Rev. 2: Computer Security Incident Handling Guid
- SP 800-18 Rev. 1 : Guide for Developing Security Plans for Federal Information Systems



Source: Coombs, Ted. Cloud Security For Dummies (p. 307). Wiley. Kindle Edition.

I. 클라우드 보안 트렌드

❖ Zero – Trust Architecture 엔터프라이즈 (예)

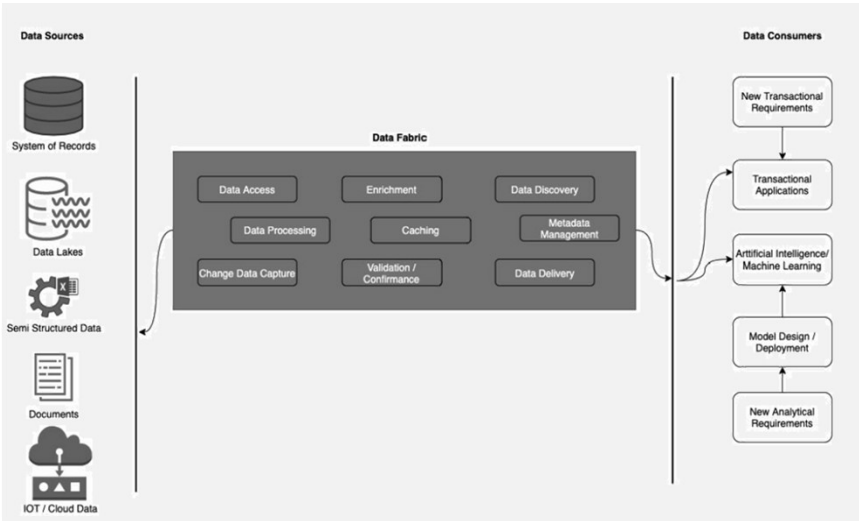


SOAR (Security orchestration, automation and response)

SIEM (Security information and event management

I. 클라우드 보안 트렌드

❖ The data fabric



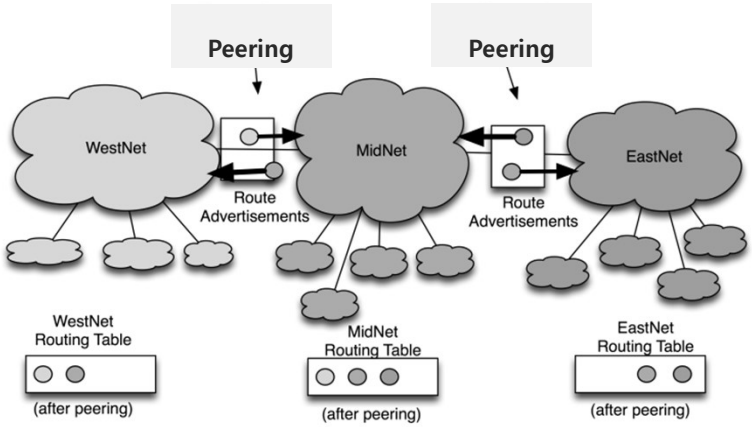
- 데이터웨어하우스
- 데이터레이크
- 레이크하우스

Source: Iyer, Sreekanth (2022-11-17T22:58:59.000). Hybrid Cloud Security Patterns: Leverage modern repeatable architecture patterns to secure your workloads on the cloud . Packt Publishing. Kindle Edition.

I. 클라우드 보안 트렌드

❖ 피어링 peering (1:1 연결)

• 피어링 내망을 경유해서 다른 망과 연결시켜주는 역할은 제외되기 때문에 WestNet과 EastNet은 MidNet을 경유해서 서로 통신할 수 없음 (즉, 피어링 관계에서는 피어링한 관계 내에서만 통신)

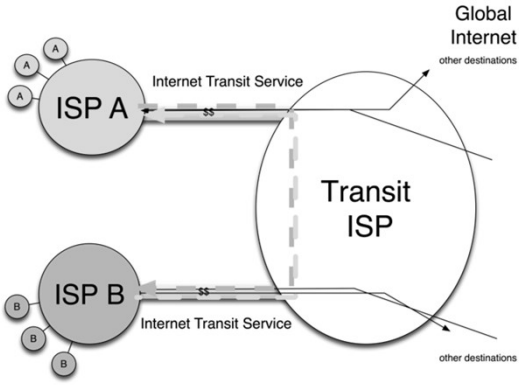


Source: https://m.clien.net/service/board/lecture/17610900

I. 클라우드 보안 트렌드

❖ 트랜짓 transit (1:1:N 연결)

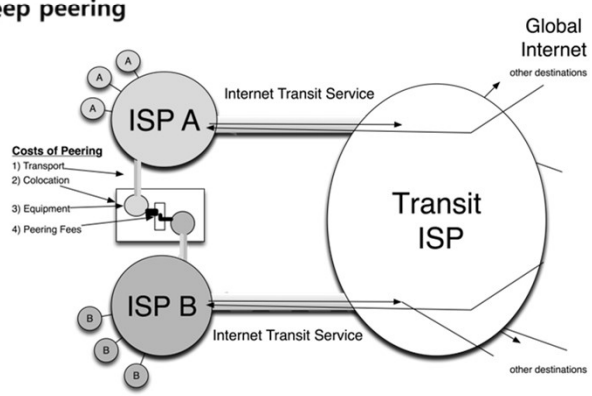
• 모든 망 운영자가 서로 피어링을 맺기에는 너무 비효율적 (n개의 망이 있다면, n*(n-1)/2개의 접속이 필요
• 트랜짓 서비스는 경유시켜주는 쪽이 서비스를 제공하는 것으로 트랜짓 서비스는 요금 발생



Source: https://m.clien.net/service/board/lecture/17610900

❖ 피어링 vs 트랜짓

- 피어링은 상대방하고만 1:1로 통신하기 위한 접속이고, 트랜짓은 상대방뿐만 아니라 상대방을 통해 다른 망과 통신하기 위한 접속
- 피어링은 무료일 수도 있고 유료일 수도 있지만, 유료라 하더라도 트랜짓보다는 저렴
- 무정산 피어링 settlement-free peering, bill-and-keep peering
- 유상 피어링 paid peering
- 트랜짓은 대역폭을 늘리기 어려움

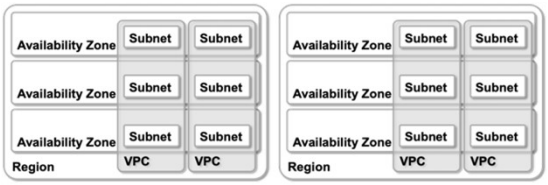


MCN 중앙 관리를 위한 트랜짓 고려

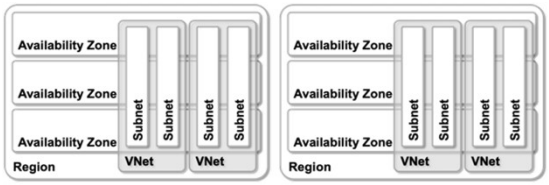
Source: https://m.clien.net/service/board/lecture/17610900

❖ Virtual Networks and Subnets in AWS, Azure, and GCP

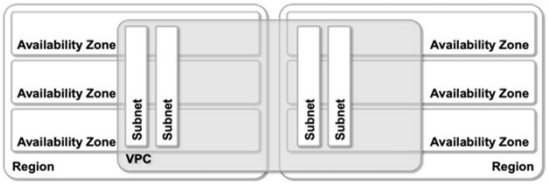
VPCs and subnets in AWS



VNet and subnets in Azure



GCP VPCs and subnets

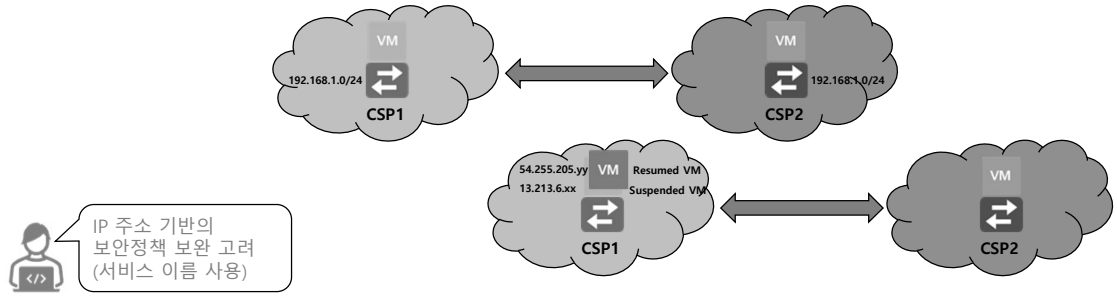


Source: https://blog.ipspace.net/2021/02/vpc-subnets-aws-azure-gcp.html

I. 클라우드 보안 트렌드

❖ Check point

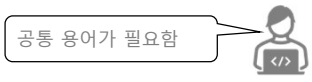
- 인프라 생성전에는 정확한 네트워크 정보를 얻기 어려움
- VPN Gateway를 활용해도 통신이 어려울 수 있고, Supernetting이 쉽지 않음
- Suspended → Resume 시 IP 주소 변경되어 통신 문제 발생 할 수 있음
- 원하는 규모의 IPv4 사설 주소 공간 확보가 어려 울 수 있음



Source: @ ETRI Conference 2022 '멀티클라우드 가상네트워크 기술' (김윤곤) 참조

I. 클라우드 보안 트렌드

❖ AWS vs. Azure vs. GCP: the key differences



Features	Amazon AWS	Microsoft Azure	Google GCP
Age	11 years old	5 years old	6 years old
Pricing	최소 60초 사용의 초당 요금제	분 단위 기준	분 단위 기준
Compute	EC2(Elastic Compute Cloud)는 모든 컴퓨팅 관리를 제공하고, 이 프로그램은 소유자가 직접 설계하거나 편의를 위해 미리 구성된 설정이 있는 가상 머신을 감독한다.	Microsoft Azure를 사용하면 가상 머신을 생성하고 가상 머신에 대한 확장 세트를 만들 수 있다.	GCP(Google 클라우드 플랫폼)의 일부인 GCE(Google 컴퓨트 엔진)도 비슷한 기능을 수행한다.
Storage	AWS는 할당된 일시적(단기) 비축을 제공한다. 인스턴스가 시작되자마자 제공, 인스턴스는 케이스가 끝날 때 삭제된다.	Azure는 ID 드라이브(일시적 용량)를 사용하며, 페이지 블롭 VM 기반 볼륨은 블록 스토리지(Microsoft의 선택)에 저장한다. 오브젝트 스토리지는 정사각형 블롭 (Square Blobs) 및 파일을 사용한다.	상대적으로 Google의 Cloud Platform은 짧은 비축과 지속적인 순환을 모두 제공한다. 객체 비축을 위해 GCP에는 Google Cloud Storage가 있다.

Source: Coombs, https://www.coursera.org/articles/aws-vs-azure-vs-google-cloud

❖ **AWS vs. Azure vs. GCP: Compute services compared**

Services	GCP	Azure	AWS
IaaS	Google Compute Engine	Virtual Machines	Amazon Elastic Compute Cloud
PaaS	Google App Engine	App Service and Cloud Services	AWS Elastic Beanstalk
Containers	Google Kubernetes Engine (GKE)	Azure Kubernetes Service (AKS)	Amazon Elastic Container Service (EKS)
Serverless Functions	Google Cloud Functions	Azure Functions	AWS Lambda

Source: Coombs, https://www.simform.com/blog/aws-vs-azure-vs-gcp/

❖ **AWS vs. Azure vs. GCP: Block Storage / Disk (2022)**

FEATURE	AWS	AZURE	GCP
Disk types	EBS Provisioned IOPS SSD, EBS General Purpose SSD, Throughput Optimized HDD, Cold HDD	Ultra disks, premium SSD, standard SSD, standard HDD	Persistent disks (HDD), SSD persistent disks
Redundancy	Single zone	Single zone or multi zone	Single zone or multi zone
Encryption at rest	Supported	Supported	Supported
Snapshots	Supported	Supported	Supported
Snapshot locality	Regional	Regional	Global
Disk attachment	Attached up to 16 instances in read-write mode	Attached up to 10 instances in read-only mode for SSDs only	Attached up to 10 instances in read-only mode
Attached disks per instance	Up to 40	Up to 64	Up to 128

Source: Coombs, https://docs.multy.dev/blog/compute-aws-vs-azure-vs-gcp/

I. 클라우드 보안 트렌드

❖ **AWS vs. Azure vs. GCP: Networking Services (2023)**

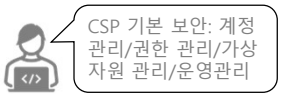
FEATURE	AWS	AZURE	GCP
Virtual Network	Amazon Virtual Private Cloud(VPC)	Virtual Networks (VNets)	Virtual Private Cloud
Elastic Load Balancer	Elastic Load Balancer	Azure Load Balancer	Google Cloud Load Balancing
Peering	Direct Connect	ExpressRoute	Google Cloud Interconnect
DNS	Amazon Route 53	Azure DNS	Google Cloud DNS

Source: Coombs, https://intellipaat.com/blog/aws-vs-azure-vs-google-cloud/ Updated on 31st Mar, 23

I. 클라우드 보안 트렌드

❖ **AWS vs. Azure vs. GCP: Security**

AWS	Azure	GCP
• **Data isolation through firewalls and granular IAM.** (방화벽과 세분화된 IAM을 통한 데이터 격리) • **AWS inspector for vulnerability assessment.** (취약성 평가를 위한 AWS 인스펙터) • **API activity monitoring.** (API 활동 모니터링) • **Guard Duty for threat intelligence.** (위협 인텔리전스를 위한 Guard Duty)	• **Central security system.** (중앙 보안 시스템) • **Anti-malware option for malware protection.** (맬웨어 방지를 위한 맬웨어 방지 옵션) • **256-bit AES encryption for Azure keys.** (Azure 키에 대한 256비트 AES 암호화) • **Penetration tests to test security measures.** (보안 조치를 테스트하기 위한 침투 테스트)	• **Security from privileged access attacks.** (권한 있는 액세스 공격으로부터 보안) • **Google KMS to manage cryptographic keys.** (암호화 키를 관리하는 Google KMS) • **Google IAM for granular access control.** (세분화된 액세스 제어를 위한 Google IAM) • **Google cloud security scanner to identify potential threats.** (잠재적 위협을 식별하는 Google 클라우드 보안 스캐너)



Source: Coombs, https://www.simform.com/blog/aws-vs-azure-vs-gcp/

I. 클라우드 보안 트렌드

❖ **AWS vs. Azure vs. GCP: cheat sheet**

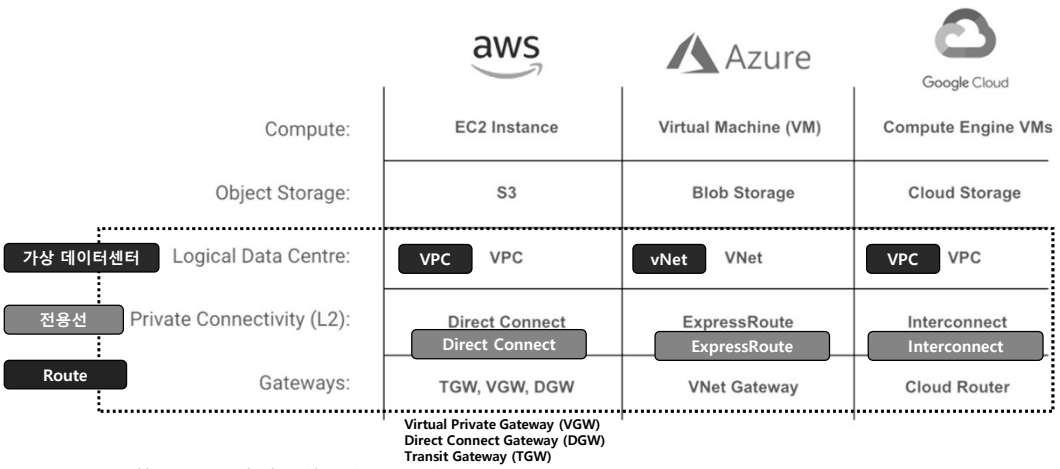
CSP와 보안 파트너의 관계 고려

	Amazon Web Services	Microsoft Azure	Google Cloud Platform
Regions	Global Infrastructure	Regions	Regions and Zones
Pricing	Cloud Services Pricing	Pricing	Pricing
Compute	EC2	Virtual Machines	Compute Engine
Serverless	Lambda	Functions	Cloud Functions
Containers	ECS	AKS	Kubernetes Engine
Machine Learning	SageMaker	Machine Learning	Cloud Machine Learning Engine
Cognitive Services	Comprehend	Cognitive Services	Cloud Natural Language
IoT	IoT Core	IoT Hub	Cloud IoT Core
Networking	Direct Connect	Virtual Network	Cloud Interconnect
Content Delivery	CloudFront	CDN	Cloud CDN
Big Data Analytics	Athena	Stream Analytics	Cloud Dataflow
Authentication and Access Management	IAM	Active Directory	Cloud IAM
Security	GuardDuty	Security Center	Cloud DLP
AR & VR	Sumerian	N/A	N/A
Virtual Private Cloud	VPC	N/A (Virtual Network)	Virtual Private Cloud
Support	Support	Support	Support
3rd Party Software and Services	Marketplace	Marketplace	Cloud Launcher

Source: Coombs, https://www.simform.com/blog/aws-vs-azure-vs-gcp/

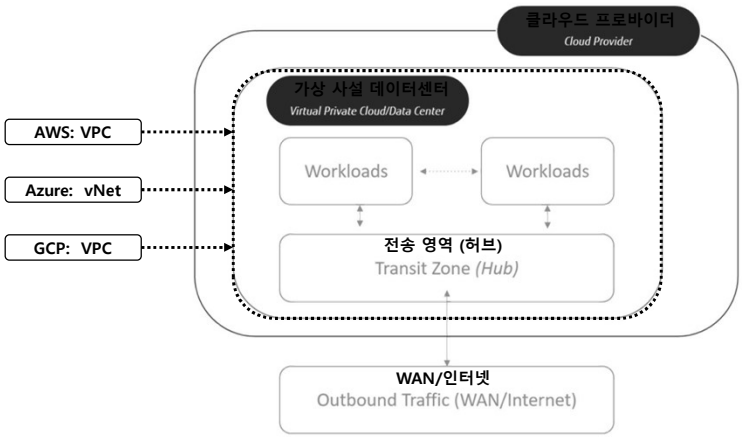
I. 클라우드 보안 트렌드

❖ **CSP 네트워크 용어 (terminology alignment)**



Source: https://www.megaport.com/blog/comparing-cloud-providers-private-connectivity/

❖ High-level diagram of a virtual private cloud/data center



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 74). Packt Publishing. Kindle Edition.

❖ IaaS Networking Services across AWS, Azure, GCP

Network Services/Function	AWS	Azure	Google
Network Administration	Account	Subscription	Project
Virtual Network	VPC & Subnets	VNET & Subnet	VPC and Sub-Network
DNS	Route 53	Traffic Manager	Cloud DNS
VPN	VGW	VPN Gateway	VPN Gateway
Peering	AWS Peering or DirectConnect	Azure Peering or ExpressRoute	Google Cloud Interconnect
Load Balancer	ELB	NLB	Cloud Load Balancer
Security	Sec Groups	Network Security Groups	Network ACLs
Storage	S3	Blob Storage	Cloud Storage
Notifications	SNS	Notification hubs	Cloud Messaging
Messaging	SQS	Batch	Pub/Stub
Logging	CloudTrail	Operational Insights	Cloud Logging
Monitoring	CloudWatch	Application Insights	Cloud Monitoring

Source: https://aviatrix.com/learn-center/answered-multi-cloud/how-to-do-multicloud-networking-abstraction-and-orchestration-across-aws-azure-and-google/

I. 클라우드 보안 트렌드

❖ The six CCSP(Certified Cloud Security Professional) domains and their weightings

CCSP Examination Weights

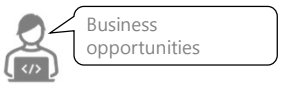
Domains	Weight
1. Cloud Concepts, Architecture, and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk, and Compliance	13%
Total:	100%

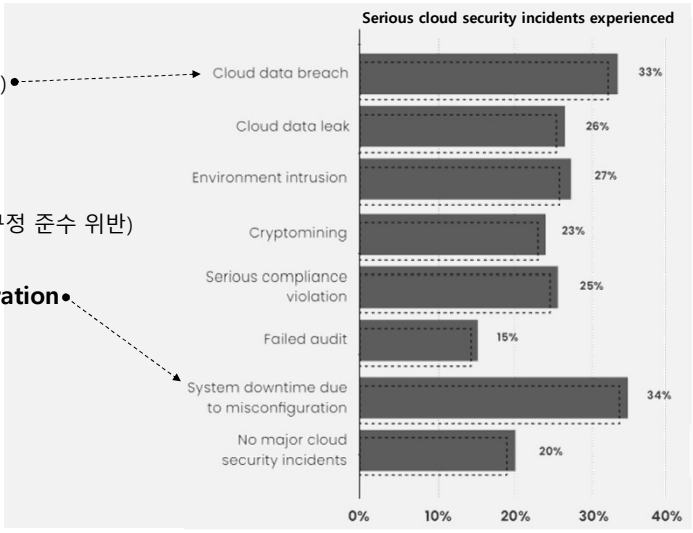
Source: Carter, Daniel (2022-11-24T22:58:59.000). CCSP Certified Cloud Security Professional All-in-One Exam Guide, Third Edition . McGraw Hill LLC. Kindle Edition.

I. 클라우드 보안 트렌드

❖ 심각한 클라우드 보안 사고 경험

- **Cloud data breach** (클라우드 데이터 침해)
- **Cloud data leak** (클라우드 데이터 유출)
- **Environment intrusion** (환경 침입)
- **Cryptomining** (암호화폐 채굴)
- **Serious compliance violation** (심각한 규정 준수 위반)
- **Failed audit** (감사 실패)
- **System downtime due to misconfiguration** (잘못된 구성으로 인한 시스템 다운타임)
- **No major cloud security incidents** (주요 클라우드 보안 사고 없음)



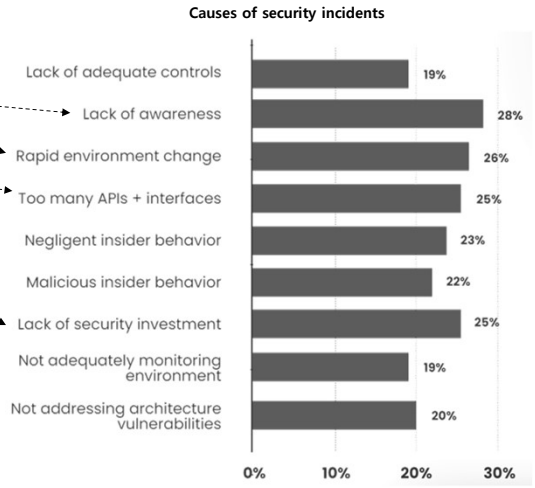


Source: https://resources.snyk.io/state-of-cloud-security , The State of Cloud Security Report 2022, synk

I. 클라우드 보안 트렌드

❖ **보안 사고의 원인** (Causes of security incidents)

- **Lack of adequate controls** (적절한 통제 부족)
- **Lack of awareness** (인식 부족)
- **Rapid environment change** (급격한 환경 변화)
- **Too many APIs + interfaces**
- **Negligent insider behavior** (부주의한 내부자 행동)
- **Malicious insider behavior** (악의적인 내부자 행동)
- **Lack of security investment** (보안 투자 부족)
- **Not adequately monitoring environment** (적절한 모니터링 환경 미비)
- **Not addressing architecture vulnerabilities** (아키텍처 취약점을 해결하지 않음)

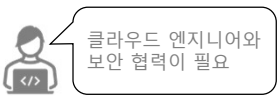


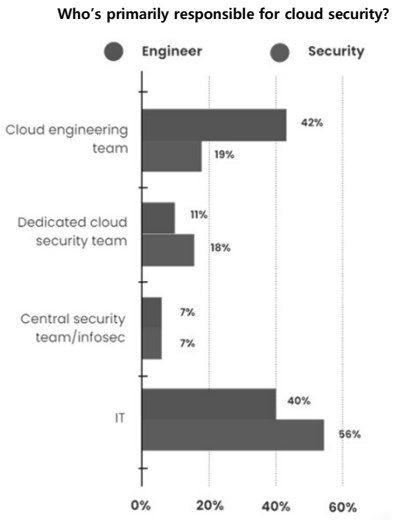
Source: https://resources.snyk.io/state-of-cloud-security , The State of Cloud Security Report 2022, synk

I. 클라우드 보안 트렌드

❖ **Who's primarily responsible for cloud security?**

- **Cloud engineering team**
- **Dedicated cloud security team**
- **Central security team/infosec**
- **IT**





Source: https://resources.snyk.io/state-of-cloud-security , The State of Cloud Security Report 2022, synk

I. 클라우드 보안 트렌드

❖ **Cloud security challenges**

- **응답자의 45%는 클라우드 보안 작업에 상당한 엔지니어링 리소스가 소요된다는 데 동의**

비효율적인 클라우드 보안 프로세스의 주요 영향 (조직 유형별)

Enterprises	보안팀 자원의 중요한 투자 Significant investment of security team resources
Startups	클라우드 엔지니어링 자원의 중요한 투자 Significant investment of cloud engineering resources
SMBs	클라우드 엔지니어링 자원의 중요한 투자 Significant investment of cloud engineering resources
Public sector	애플리케이션과 기능의 적용 지연 Application and feature deployment delays

Security Managed Service가 필요

Source: https://resources.snyk.io/state-of-cloud-security , The State of Cloud Security Report 2022, synk

I. 클라우드 보안 트렌드

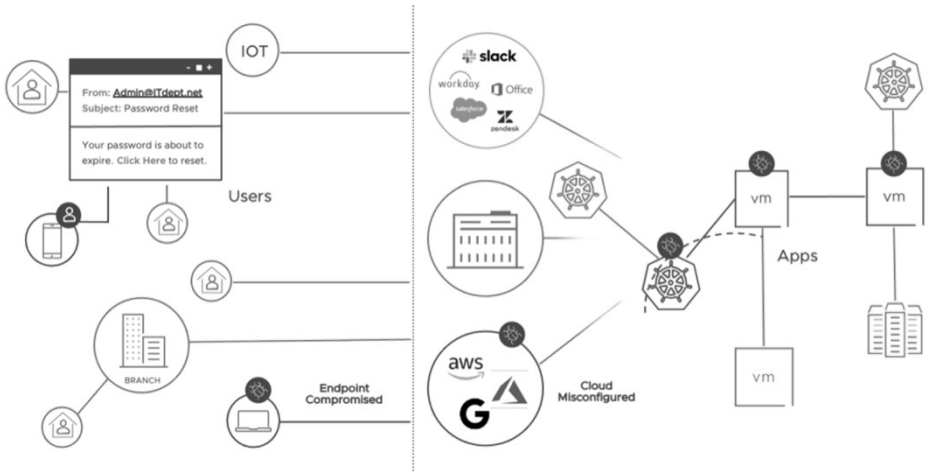
❖ **다양한 공격 표면**(Attack Surface), 2023

- **Massive growth in SaaS applications**
  (SaaS 애플리케이션의 큰 성장)
- **Software supply chain uncertainty**
  (소프트웨어 공급망의 불확실성)
- **Work-from home**
  (재택 근무)
- **IT / OT convergence & 5G**
  (IT/OT 융합 및 5G)
- **Rapid growth in cloud native services**
  (클라우드 네이티브 서비스의 급속한 성장)
- **Cloud native applications**
  (클라우드 네이티브 애플리케이션)

Source: https://www.trendmicro.com/en_gb/ciso/22/d/attack-surface-management.html

I. 클라우드 보안 트렌드

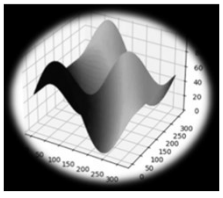
❖ 엔드포인트 침해 (Endpoint Compromised) 예



I. 클라우드 보안 트렌드

❖ **Attack Surface의 진화 공식**

- **Complex & Rapidly Evolving**
  - Changes in Infrastructure
  - Changes in User Behaviors
  - New Threats and Vulnerabilities
  - Speed of Business



$$as = [(i + u) * t]^s$$

Speed of Business 비즈니스의 속도

Changes in Infrastructure 인프라 변경

Changes in User Behaviors 사용자 행동 변경

New Threats and Vulnerabilities 새로운 위협과 취약점

Source: https://www.trendmicro.com/

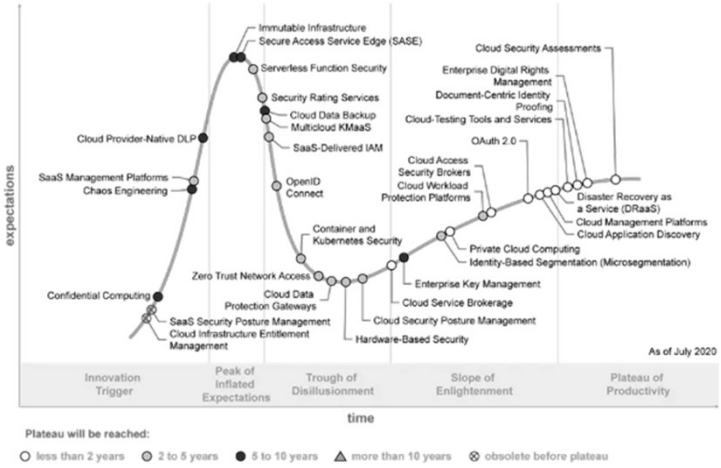
I. 클라우드 보안 트렌드

❖ **DevSecOps** (2022, Gartner)

Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

I. 클라우드 보안 트렌드

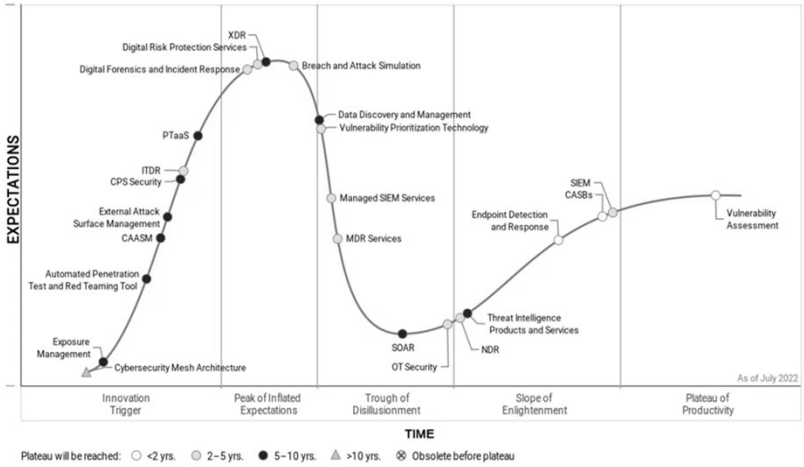
❖ Gartner Hype Cycle for Cloud Security, (2020)



Source: https://www.securityinfowatch.com/cybersecurity/press-release/21152886/gartner-multicloud-data-security-trends-noted-in-gartner-hype-cycle-for-cloud-security-2020

I. 클라우드 보안 트렌드

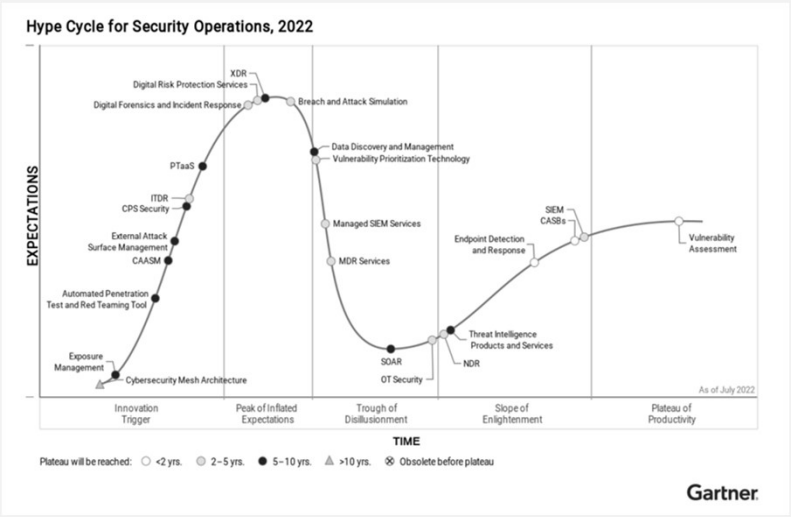
❖ Hype Cycle for Security Operations (Gartner 2022)



Source: https://cymulate.com/blog/gartner-hype-cycle-security-operations/

I. 클라우드 보안 트렌드

❖ Gartner's Hype Cycle For External Attack Surface Management (EASM)

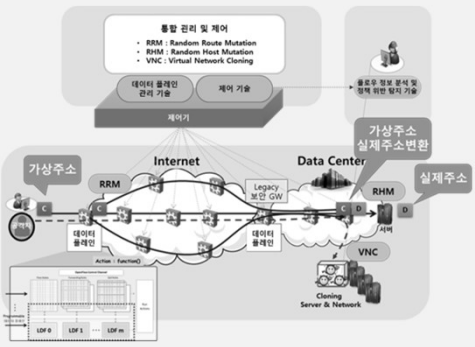


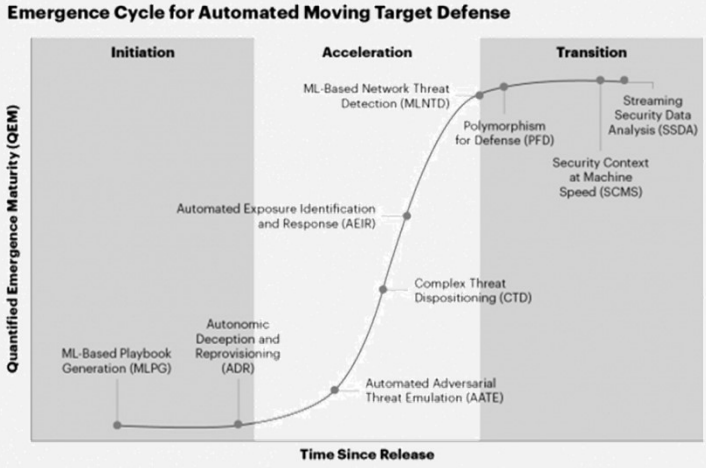
- CASB (Cloud Access Security Broker)
- EDR (Endpoint Detection and Response)
- MDR (Managed Detection and Response)
- NDR (Network Detection and Response)
- SOAR (Security orchestration, automation and response)
- SIEM (Security information and event management)
- XDR (Extended Detection and Response)

Source: https://www.firecompass.com/gartner-hype-cycle-easm/

I. 클라우드 보안 트렌드

❖ 가트너 **AMTD** (Automated Moving Target Defense) **기술 성장 단계**
❖ 출처 : 데이터넷(http://www.datanet.co.kr)



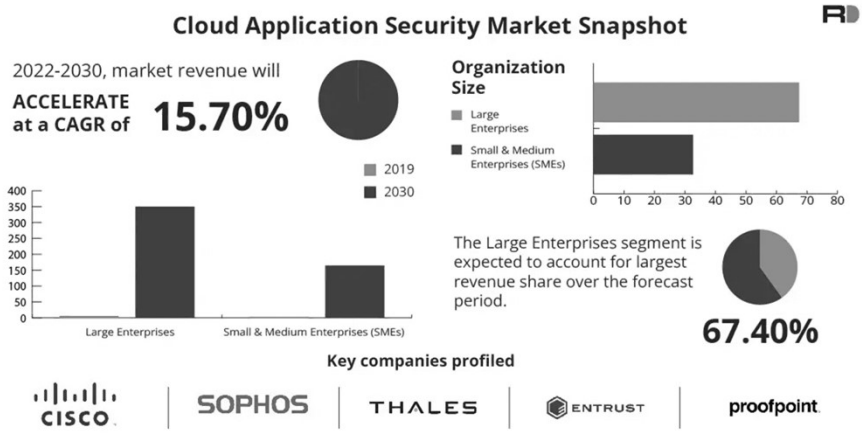


Source: http://www.datanet.co.kr/news/articleView.html?idxno=183297

47

I. 클라우드 보안 트렌드

❖ **Market Synopsis** (Global Market Insight)

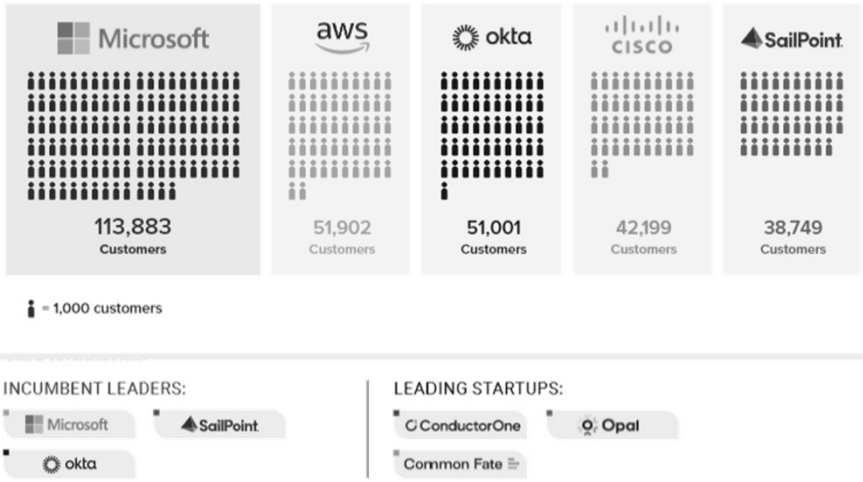


Source: https://www.reportsanddata.com/report-detail/cloud-application-security-market

48

I. 클라우드 보안 트렌드

❖ **Top IAM Providers**



- Identity and Access Management(IAM)

Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

I. 클라우드 보안 트렌드

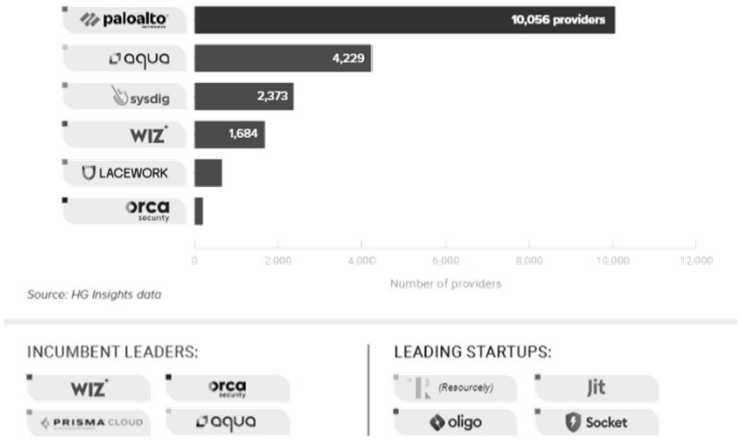
❖ **Top 10 cloud security companies (2022)**

1. **VMware:** Provider of multi-cloud services for all apps
2. **Palo Alto Networks:** Aiming to shape the cloud-centric future with technology
3. **CrowdStrike:** Cloud-delivered protection
4. **Trend Micro:** Its cyber security platform protecting 500,000+ organisations
5. **Check Point Software:** Cyber security solutions to governments and corporate enterprises
6. **Datadog:** Monitoring and security platform for cloud applications.
7. **Qualys:** Founded in 1999 as one of the first SaaS security companies, A founding member of CSA
8. **Proofpoint:** The first SaaS-based cybersecurity and compliance company
9. **Netskope:** Aiming to redefine cloud, data, and network security, The Netskope Intelligent SSE
10. **Lacework:** A data-driven security platform.

Intelligent Security Service Edge (SSE), Cloud Security Alliance (CSA)

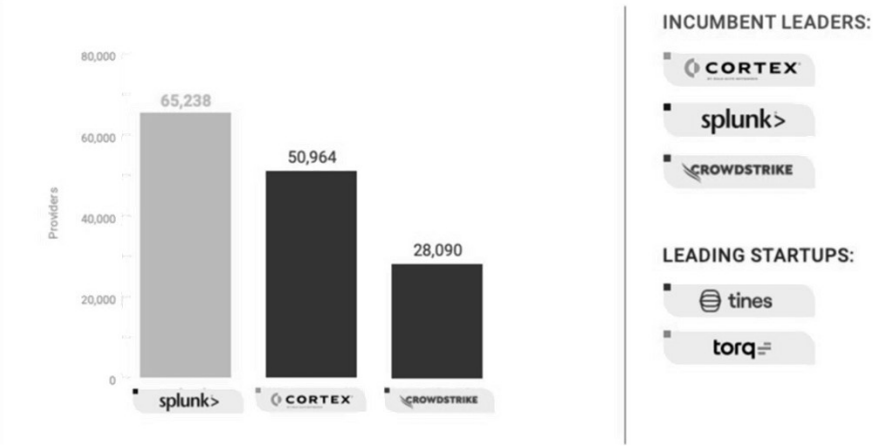
Source: https://www.getastra.com/blog/security-audit/best-cloud-security-companies/#Top_10_Best_Cloud_Security_Companies

❖ **Top Application Security Providers**



Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

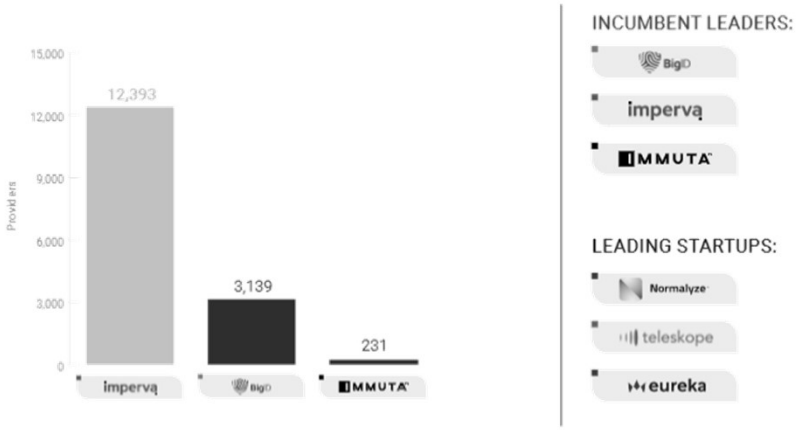
❖ **Top Security Automation Providers**



Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

I. 클라우드 보안 트렌드

❖ **Top Data Security Providers**

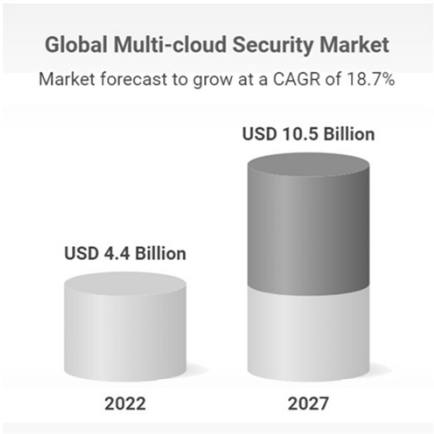


Source: https://hginsights.com/blog/2023-cloud-security-market-size-growth-forecast

I. 클라우드 보안 트렌드

❖ **Global Multi-cloud Security - Forecast to 2027 CAGR 18.7%** (Research and Market)

- **Market by**
  - **Offering (Solution and Services),**
  - **Cloud Model (IaaS, PaaS, and SaaS),**
  - **Application (Network, Endpoint),**
  - **Verticals (BFSI, Healthcare, IT and ITeS, Retail and eCommerce),**
  - **Organization Size Region**



Source: https://www.researchandmarkets.com/reports/5738899/global-multi-cloud-security-market-offering

I. 클라우드 보안 트렌드

❖ **Multi-cloud Security Market** (Global Market Insight)

Source: https://www.gminsights.com/industry-analysis/multi-cloud-security-market

I. 클라우드 보안 트렌드

❖ **Multi-cloud Security Market Ecosystem** (Market and Market)

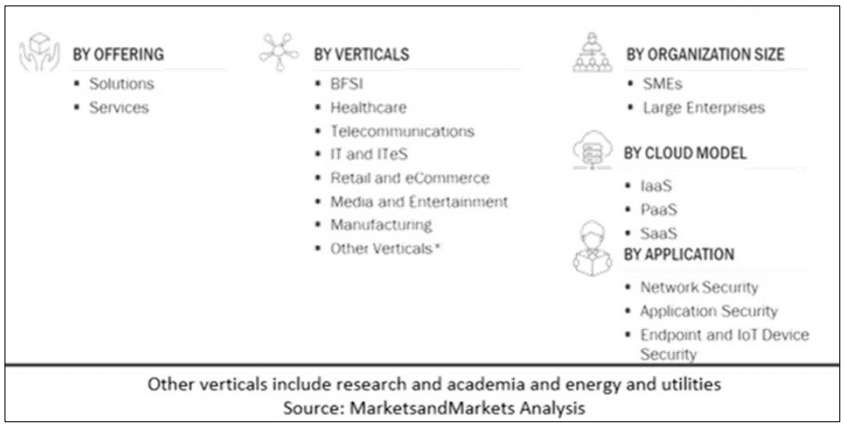
MULTI-CLOUD MANAGEMENT	CLOUD SECURITY	MULTI-CLOUD NETWORKING	ZERO TRUST SECURITY
▪ BMC Software ▪ CenturyLink ▪ Accenture ▪ VMware ▪ DoubleHorn ▪ RightScale ▪ CliQr ▪ Cloudyn ▪ Jamcracker ▪ Dell Technologies ▪ IBM ▪ Citrix ▪ UnityOneCloud ▪ SixSq ▪ Others	▪ Amazon Web Services ▪ Microsoft ▪ Check Point ▪ Google ▪ Palo Alto Networks ▪ McAfee ▪ IBM ▪ Zscaler ▪ Cisco ▪ Fortinet ▪ Sophos ▪ Forseeti ▪ Broadcom ▪ Trend Micro ▪ Tenable ▪ Forcepoint ▪ Netskope ▪ Imperva ▪ Proofpoint ▪ Others	▪ VMware ▪ Oracle ▪ F5 ▪ Cisco ▪ Nutanix ▪ Juniper ▪ Citrix ▪ Illumio ▪ Akamai ▪ Aviatrix ▪ Prosimo ▪ Infoblox ▪ Others	▪ Cisco ▪ Palo Alto Networks ▪ Okta ▪ Check Point ▪ Trend Micro ▪ IBM ▪ FireEye ▪ McAfee ▪ Forcepoint ▪ RSA Security ▪ Illumio ▪ Sophos ▪ Google ▪ Microsoft ▪ VMware ▪ Fortinet ▪ Cloudflare ▪ Others

Source: https://www.marketsandmarkets.com/Market-Reports/multi-cloud-security-market-231733464.html

I. 클라우드 보안 트렌드

❖ **Multi-cloud Security Market** (Market and Market)

- **By Offering**
- **By Verticals**
- **By Organization size**
- **By Cloud model**
- **By Application**

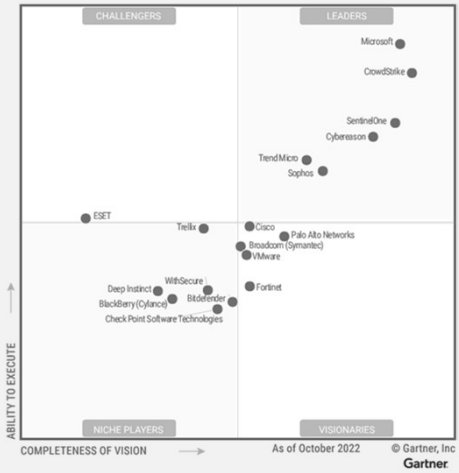


Source: https://www.marketsandmarkets.com/Market-Reports/multi-cloud-security-market-231733464.html

I. 클라우드 보안 트렌드

❖ **Magic Quadrant for Endpoint Protection Platform (Gartner, December 2022)**

- **Leaders:**
  - Microsoft
  - CrowdStrike
  - SentinalOne
  - Cybereason
  - TrendMicro
  - Sophos



Source: https://kr.sentinelone.com/lp/gartnermq/

I. 클라우드 보안 트렌드

❖ **Magic Quadrant for WAAP(Web Application and API Protection) (Gartner, August 2022)**

- **Leaders:**
  - Akamai,
  - Cloudflare,
  - Imperva

Source: https://www.gartner.com/doc/reprints?id=1-2B19DBZH&ct=220906&st=sb

I. 클라우드 보안 트렌드

❖ **Magic Magic Quadrant for Security Service Edge (Gartner 2023)**

- **Leaders:**
  - Netskope,
  - Zscaler,
  - Palo Alto Networks

Source: https://www.gartner.com/doc/reprints?id=1-2D7QDAX2&ct=230413&st=sb

I. 클라우드 보안 트렌드

❖ **Magic Quadrant for Application Performance Monitoring and Observability (Gartner 2022)**

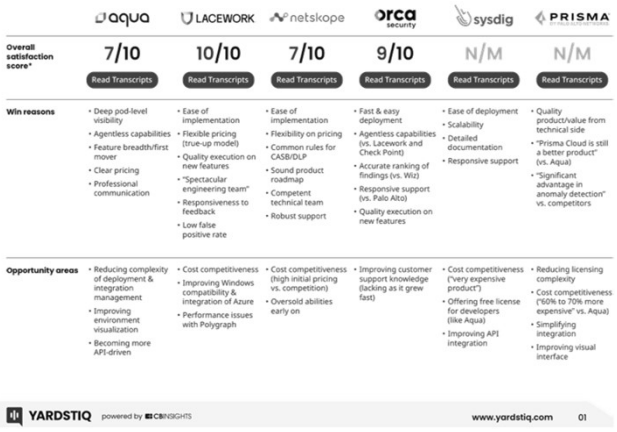
- **Leaders: Datadog, Dynatrace, New Relic, Honeycomb, IBM(Instana)**

Source: https://www.sumologic.com/brief/gartner-apm-and-observability-magic-quadrant/

I. 클라우드 보안 트렌드

❖ **Vendor Scorecard : Cloud Security**

- **Based on interviews with software buyers who recently evaluated cloud security solutions**



	aqua	LACEWORK	netskope	orca security	sysdig	PRISMA
Overall satisfaction score*	7/10	10/10	7/10	9/10	N/M	N/M
	Read Transcripts	Read Transcripts	Read Transcripts	Read Transcripts	Read Transcripts	Read Transcripts
Win reasons	• Deep pod-level visibility • Agentless capabilities • Feature breadth/first mover • Clear pricing • Professional communication	• Ease of implementation • Flexible pricing (true-up model) • Quality execution on new features • "Spectacular engineering team" • Responsiveness to feedback • Low false positive rate	• Ease of implementation • Flexibility on pricing • Common rules for CASB/DLP • Sound product roadmap • Competent technical team • Robust support	• Fast & easy deployment • Agentless capabilities (vs. Lacework and Check Point) • Accurate ranking of findings (vs. Wiz) • Responsive support (vs. Palo Alto) • Quality execution on new features	• Ease of deployment • Scalability • Detailed documentation • Responsive support	• Quality product/value from technical side • "Prisma Cloud is still a better product" (vs. Aqua) • "Significant advantage in anomaly detection" vs. competitors
Opportunity areas	• Reducing complexity of deployment & integration management • Improving environment visualization • Becoming more API-driven	• Cost competitiveness • Improving Windows compatibility & integration of Azure • Performance issues with Polygraph	• Cost competitiveness (high initial pricing vs. competition) • Oversold abilities early on	• Improving customer support knowledge (lacking as it grew fast)	• Cost competitiveness ("very expensive product") • Offering free license for developers (like Aqua) • Improving API integration	• Reducing licensing complexity • Cost competitiveness ("60% to 70% more expensive" vs. Aqua) • Simplifying integration • Improving visual interface

YARDSTIQ powered by CBINSIGHTS www.yardstiq.com 01

Source: https://www.cbinsights.com/reports/CB-Insights_Cloud-Security-Vendor-Scorecard.pdf?

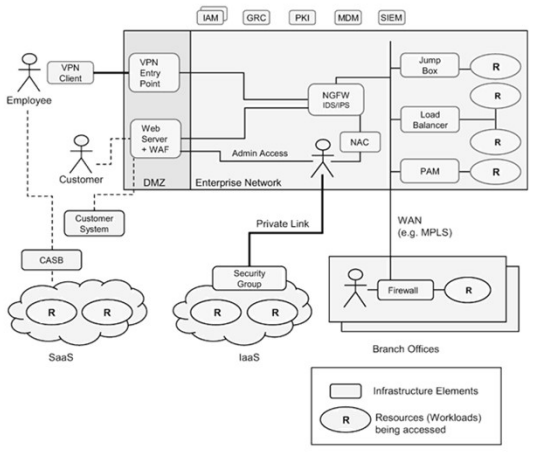
II. 클라우드 인프라 와 보안

- 클라우드 인프라 및 아키텍처
- 클라우드 아키텍처 모델
- 하이브리드/멀티클라우드 모델

II. 클라우드 인프라 와 보안

❖ **Representative Enterprise Architecture**

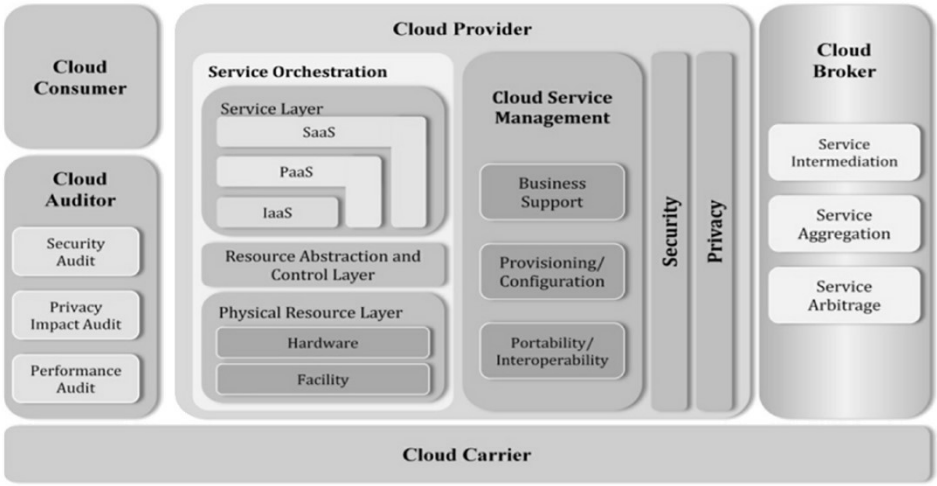
- **the US National Institute of Standards and Technologies (NIST) Zero Trust Architecture, from Special Publication 800-207.**
  - Identity and Access Management
  - Network Infrastructure (Firewalls, DNS, Load Balancers)
  - Jump Boxes
  - Privileged Access Management
  - Network Access Control
  - Intrusion Detection/Intrusion Prevention
  - Virtual Private Network
  - Next-Generation Firewalls
  - Security Information and Event Management
  - Web Server and Web Application Firewall
  - Infrastructure as a Service
  - Software as a Service and Cloud Access Security Brokers



Source: Garbis, Jason; Chapman, Jerry W. (2021-02-25T22:58:59.000). Zero Trust Security . Apress. Kindle Edition.

II. 클라우드 인프라 와 보안

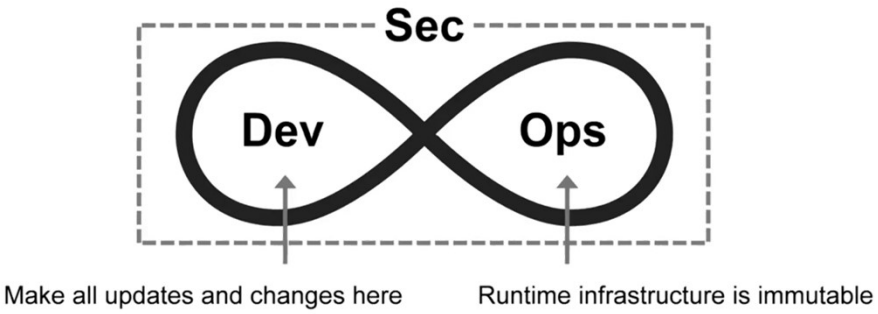
❖ **NIST 500-292 reference architecture example. (Source: NIST 500-292.)**



Source: Thompson, Graham; Thompson, Graham (2020-03-22T22:58:59.000). CCSK Certificate of Cloud Security Knowledge All-in-One Exam Guide . McGraw Hill LLC. Kindle Edition.

II. 클라우드 인프라 와 보안

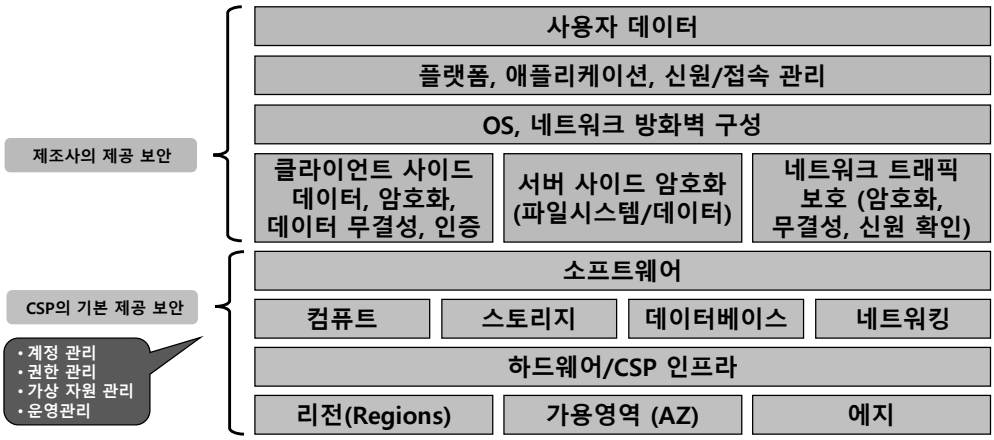
❖ **Immutable Infrastructure**



Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

II. 클라우드 인프라 와 보안

❖ 클라우드 보안을 위한 CSP와 제조사 (예)



II. 클라우드 인프라 와 보안

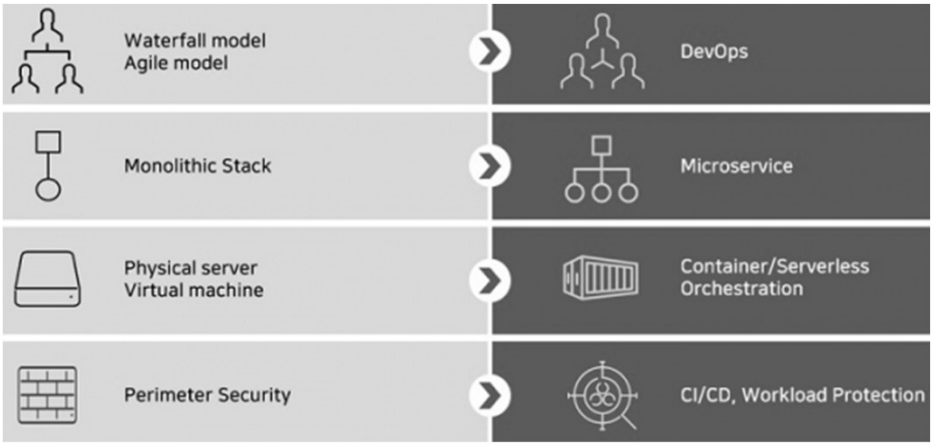
❖ CSP Native vs 3rd Party 보안 솔루션 비교

		비교 우위
비용 효율성	CSP Native는 초기 투자 비용이 없으며 사용한 만큼 지불 할 수 있음	CSP Native / 3rd Party ISV
가용성	CSP Native는 CSP가 SLA를 보장하며, 고객의 운영 부담이 낮음	CSP Native / 3rd Party ISV
탄력성	CSP Native는 사용량 증감에 따라 CSP가 자동으로 Resource를 조절함	CSP Native / 3rd Party ISV
도입 및 전환 속도	CSP Native 보안 기능은 구매 / 설치 등의 절차가 불필요함	CSP Native / 3rd Party ISV
Multi 클라우드	3rd Party ISV는 모든 CSP에 동일 솔루션 적용 및 관리 가능함	CSP Native / 3rd Party ISV
Hybrid 클라우드	3rd Party ISV는 On-premise까지 동일 솔루션 적용 및 관리 가능함	CSP Native / 3rd Party ISV
난이도 및 기술지원	3rd Party ISV는 각 솔루션 제조사의 기술지원을 받기 용이함	CSP Native / 3rd Party ISV

Source: https://www.samsungsds.com/kr/insights/cloud_security.html

II. 클라우드 인프라 와 보안

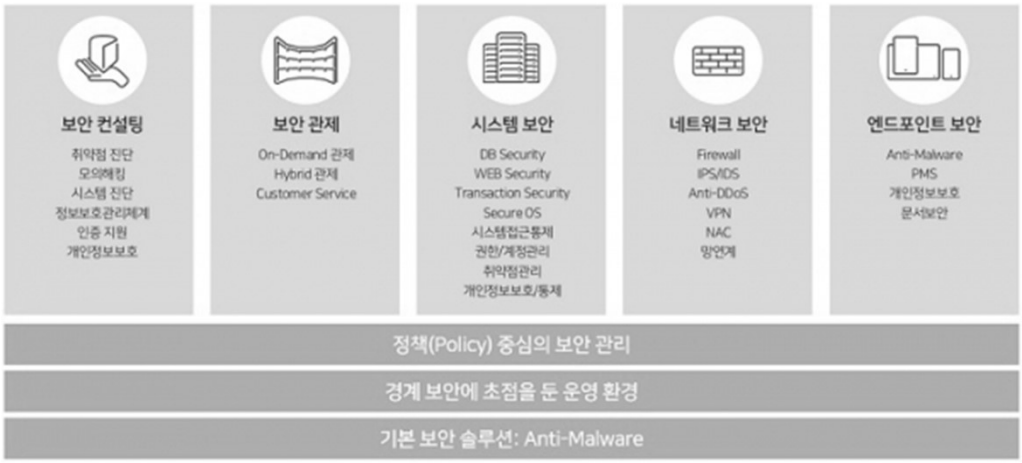
❖ 온프레미스와 클라우드의 차이



Source: https://www.datanet.co.kr/news/articleView.html?idxno=177045

II. 클라우드 인프라 와 보안

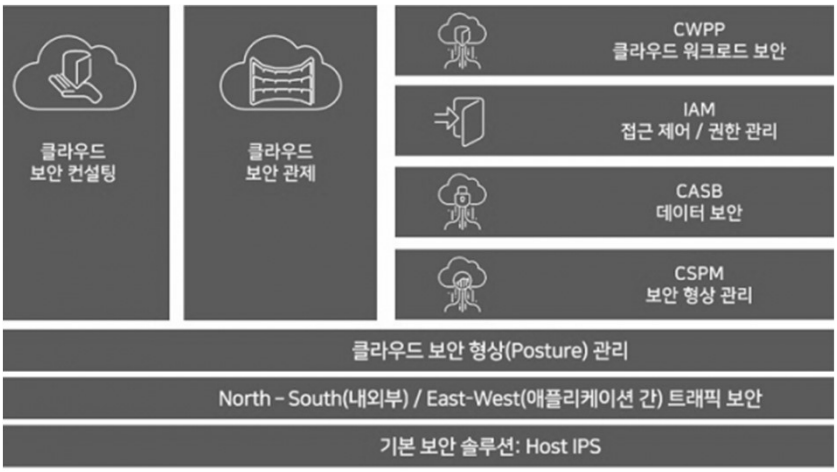
❖ 온프레미스와 온프레미스 보안 프레임워크



Source: https://www.datanet.co.kr/news/articleView.html?idxno=177045

II. 클라우드 인프라 와 보안

❖ 클라우드 보안 프레임워크



Source: https://www.datanet.co.kr/news/articleView.html?idxno=177045

II. 클라우드 인프라 와 보안

❖ 클라우드 보안 툴 역할과 보호영역

보안 툴	역할	보호 영역
클라우드 워크로드 보안 플랫폼 (CWPP: Cloud Workload Protection Platform)	클라우드 워크로드 보호	IaaS & PaaS
클라우드 보안 형상 관리 (CSPM: Cloud Security Posture Management)	IaaS와 PaaS에 걸쳐 잘못된 보안 구성 방지	IaaS & PaaS
클라우드 접근 보안 중개 (CASB: Cloud Access Security Broker)	클라우드 리소스 접근 제어 및 보안 정책 적용	SaaS
SaaS 관리 플랫폼 (SMP: SaaS Management Platform)	여러 SaaS 툴을 단일 플랫폼에서 관리	SaaS
SaaS 보안 형상 관리 (SSPM: SaaS Security Posture Management)	SaaS 애플리케이션 보안 형상 관리 및 리스크 평가	SaaS

Source: https://www.datanet.co.kr/news/articleView.html?idxno=177045

❖ 가트너의 클라우드 보안 주요 주제에 대한 다양한 적용 영역

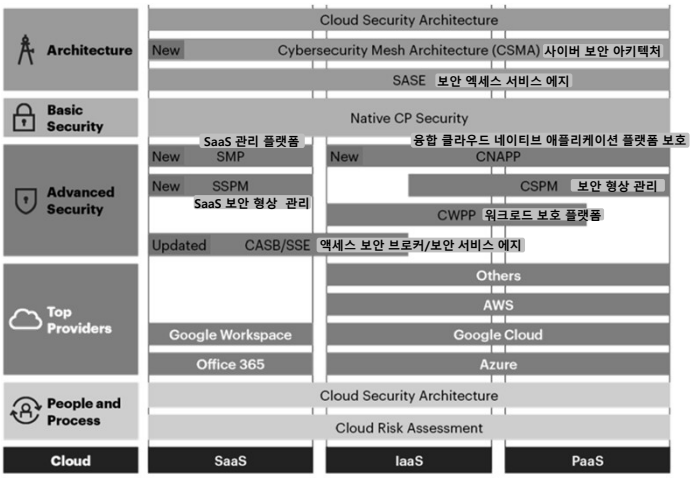
- **CSMA: Cybersecurity Mesh Architecture** (사이버 보안 아키텍처)
- **SASE: Secure Access Service Edge** (보안 액세스 서비스 에지)

- 계정 관리
- 권한 관리
- 가상 자원 관리
- 운영관리

클라우드 사업자의 기본 제공 보안

- **CASBs: Cloud Access Security Brokers** (액세스 보안 브로커)
- **SSE: Security Service Edge** (보안 서비스 에지)
- **CSPM: Cloud Security Posture Management** (보안 형상 관리)
- **CWPP: Cloud Workload Protection Platform** (워크로드 보호 플랫폼)
- **CNAPP: Combined Cloud-native Application Platform Protection** (융합 클라우드 네이티브 애플리케이션 플랫폼 보호)
- **SMP: SaaS Management Platform** (SaaS 관리 플랫폼)
- **SSPM: SaaS Security Posture Management** (SaaS 보안 형상 관리)

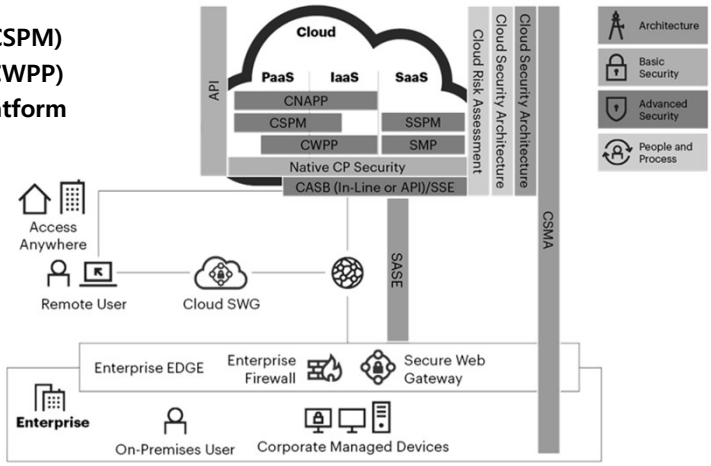
Offering	SMPs	CASBs	SSPMs
Centralizing administrative functions	Yes	No	Yes
Shadow IT discovery	Yes	Yes	Yes
Access control	Yes, to a limited extent	Yes	Yes
DLP	No	Yes	Yes
Packet filtering	No	Yes	No



Source: https://emtemp.gcom.cloud/ngw/eventassets/en/conferences/2023/secme10/documents/gartner_uae_sec_guide_to_cloud_security_concepts.pdf

❖ Cloud Security Logical Architecture

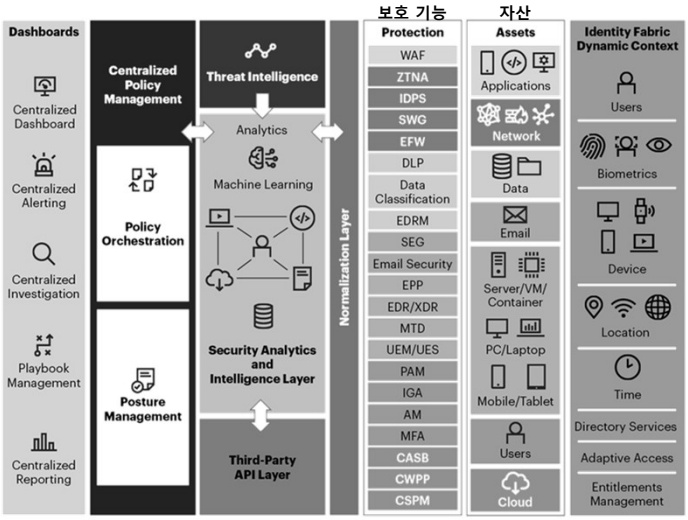
- **Cloud Access Security Brokers (CASBs)**
- **Cloud Security Posture Management (CSPM)**
- **Cloud Workload Protection Platform (CWPP)**
- **Combined Cloud-native Application Platform Protection (CNAPP)**



Source: Gartner

II. 클라우드 인프라 와 보안

❖ **Cybersecurity Mesh Architecture**

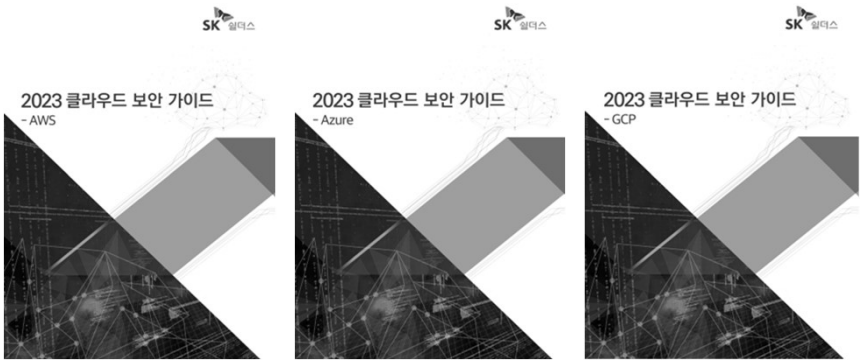


Source: Gartner

II. 클라우드 인프라 와 보안

❖ **Basic Security – Native CP Security**

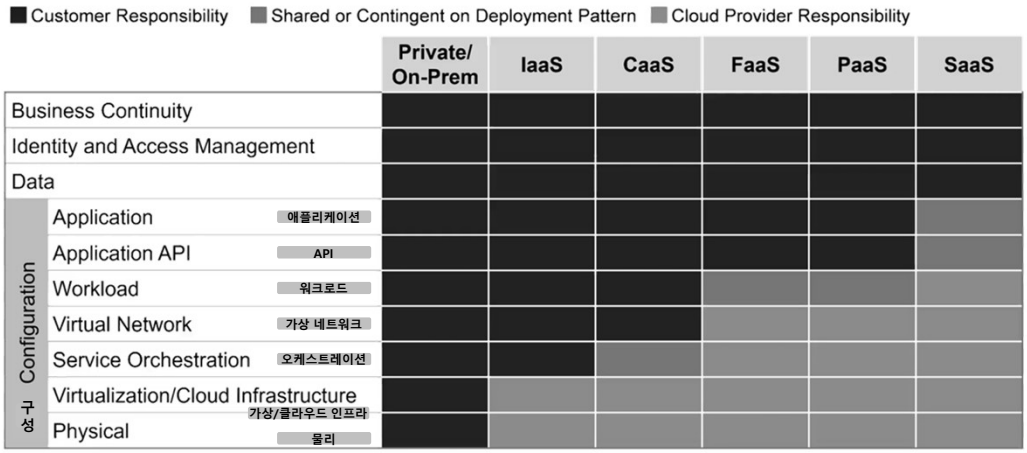
- 계정 관리
- 권한 관리
- 가상 자원 관리
- 운영관리



Source:

II. 클라우드 인프라 와 보안

❖ **The Nuances of Split Responsibility (클라우드 책임 분담의 차이)와 구성(Configuration)**

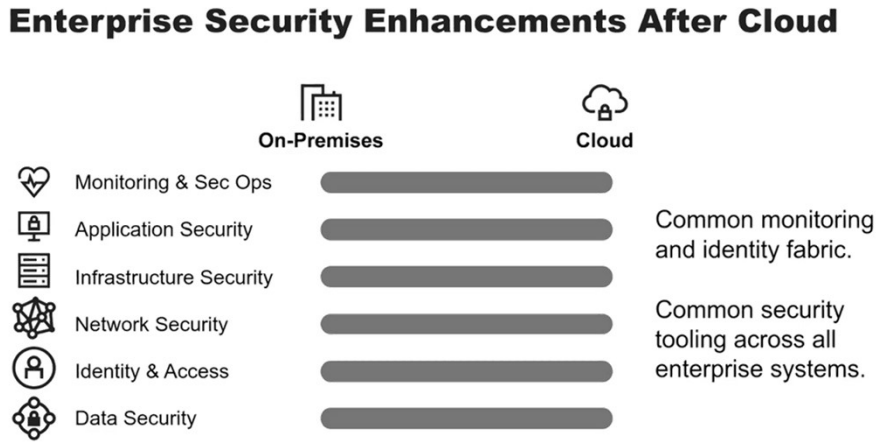


Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

Source: https://twitter.com/Gartner_inc/status/1534249589435518976

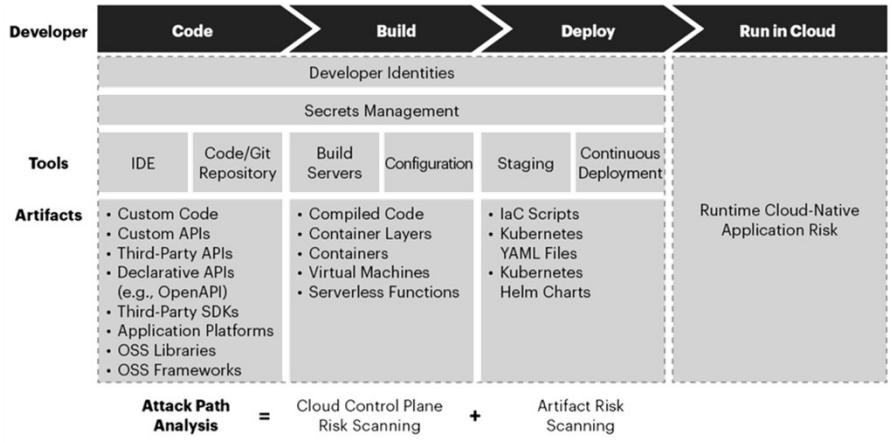
II. 클라우드 인프라 와 보안

❖ **The Nuances of Split Responsibility**



Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

❖ Code-to-Cloud Risk Visibility, Prioritization and Remediation.

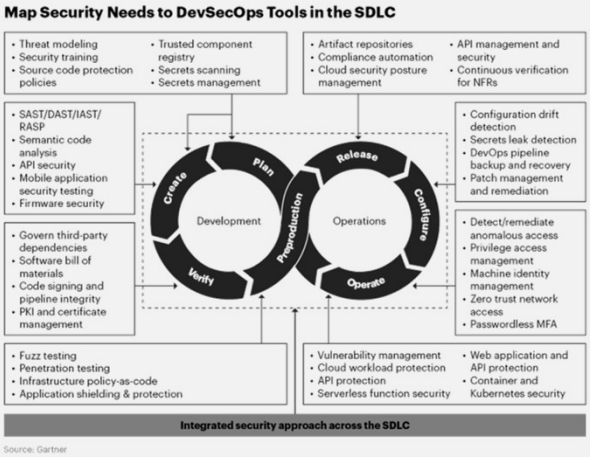


IDE = integrated development environment; OSS = open-source software

Source: https://www.uptycs.com/blog/6-takeaways-cnapp-gartner-market-guide-2023

❖ Software Development Life Cycle (SDLC)

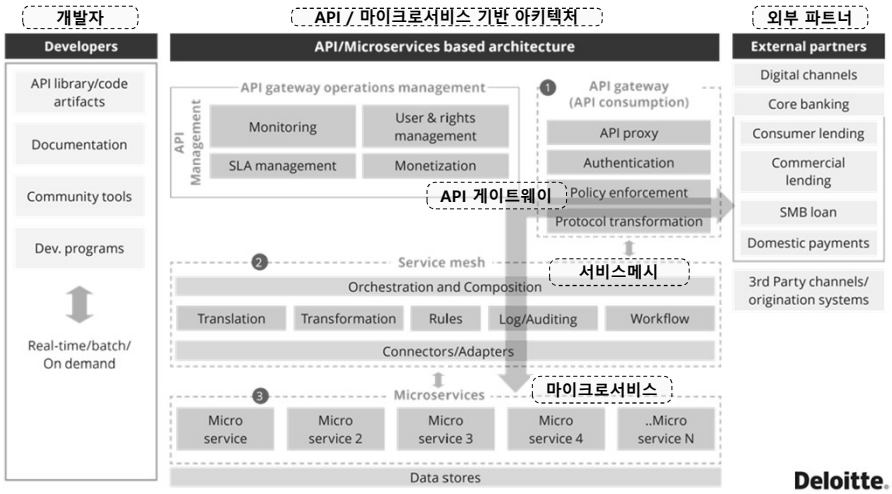
• Select DevSecOps Tools for Secure Software Delivery



Source: https://kr.sentinelone.com/lp/gartnermq/

II. 클라우드 인프라 와 보안

❖ Microservices-based architecture (예)



Source: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-enabling-platform-banking-pov.pdf

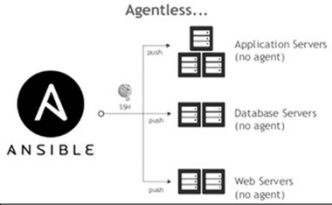
II. 클라우드 인프라 와 보안

❖ IaC(Infrastructure as Code): PXE 부팅 및 킥스타트 → Ansible → Terraform

Kickstart config

```
#Generated by Kickstart Configurator
#platform=x86

#System language
lang en_US
#Language modules to install
langsupport en_US
#System keyboard
keyboard us
#System mouse
mouse
#System timezone
timezone Asia/Seoul
#Root password
rootpw --iscrypted $1$U92SgeLPSIzOSEH9Ygs3o6wmnOe.Nw.
#Initial user
user jslab --fullname "JS Lab" --iscrypted --password $1$3RSoMDqy$WanSKHy3rzSqaSq5Z6D0S/
#Reboot after installation
reboot
#Use text mode install
text
#Install OS instead of upgrade
install
#Use CDROM installation media
cdrom
#System bootloader configuration
bootloader --location=mbr
#Clear the Master Boot Record
zerombr yes
#Partition clearing information
clearpart --all --initlabel
#Disk partitioning information
part swap --size 4096
part / --fstype ext4 --size 1 --grow
#System authorization infomation
auth  --useshadow  --enablemd5
#Network information
network --bootproto=dhcp --device=eth0
#Firewall configuration
firewall --disabled
#Do not configure the X Window System
skipx
```




```
# config file for ansible -- https://ansible.com/
# ===============================================

[defaults]

# some basic default values...

#inventory      = /etc/ansible/hosts
#library        = /usr/share/my_modules/
#module_utils   = /usr/share/my_module_utils/
#remote_tmp     = ~/.ansible/tmp
#local_tmp      = ~/.ansible/tmp
#plugin_filters_cfg = /etc/ansible/plugin_filters.yml
#forks          = 5
#poll_interval  = 15
#sudo_user      = root
#ask_sudo_pass = True
#ask_pass      = True
#transport      = smart
#remote_port    = 22
#module_lang    = C
#module_set_locale = False.
```

Ansible

```
terraform {
  required_providers {
    docker = {
      source  = "kreuzwerker/docker"
      version = "~> 3.0.1"
    }
  }
}

provider "docker" {}

resource "docker_image" "nginx" {
  name         = "nginx"
  keep_locally = false
}

resource "docker_container" "nginx" {
  image = docker_image.nginx.image_id
  name  = "tutorial"

  ports {
    internal = 80
    external = 8000
  }
}
```

Terraform

II. 클라우드 인프라 와 보안

❖ Terraform은 클라우드 및 온프레미스 리소스를 안전하고 효율적으로 빌드, 변경 및 버전 관리할 수 있는 코드 도구로서의 인프라 (IaC: Infrastructure as Code)

- Terraform은 인프라를 안전하고 효율적으로 구축, 변경 및 버전 관리하기 위한 도구
- 인프라는 고수준 구문을 사용하여 설명
- Terraform은 AWS에서 VPC, 서브넷, 보안 그룹 및 인스턴스와 같은 인프라의 프로비저닝에 사용

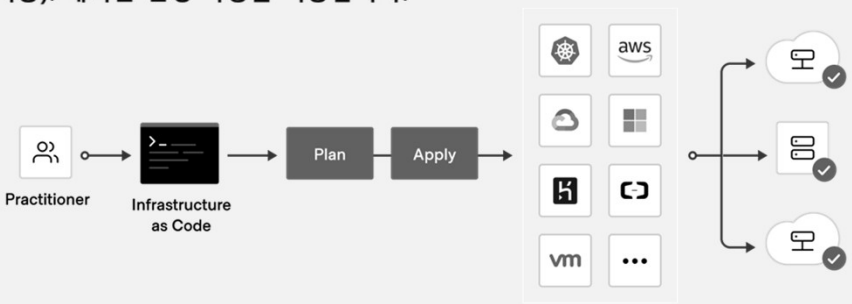
Terraform이 구성할 가장 중요한 것은 자원 (Resource)이다. (예)

```
resource "aws_instance" "web" {
    ami    = "ami-408c7f28"
    instance_type = "t2.micro"
```


II. 클라우드 인프라 와 보안

❖ 멀티클라우드를 위한 IaC (예: Terraform)

- Scope (범위): 프로젝트의 인프라를 식별합니다.
- Author (작성자): 인프라에 대한 구성을 작성합니다.
- Initialize (초기화): Terraform이 인프라를 관리하는 데 필요한 플러그인을 설치합니다.
- Plan (계획): 구성에 맞게 Terraform이 수행할 변경 사항을 미리 봅니다.
- Apply (적용): 계획한 변경 사항을 적용합니다.



Source: https://developer.hashicorp.com/terraform/tutorials/docker-get-started

II. 클라우드 인프라 와 보안

❖ Kubernetes and Helm (예: Deploying 5G)

- helm show values openverso/open5gs

II. 클라우드 인프라 와 보안

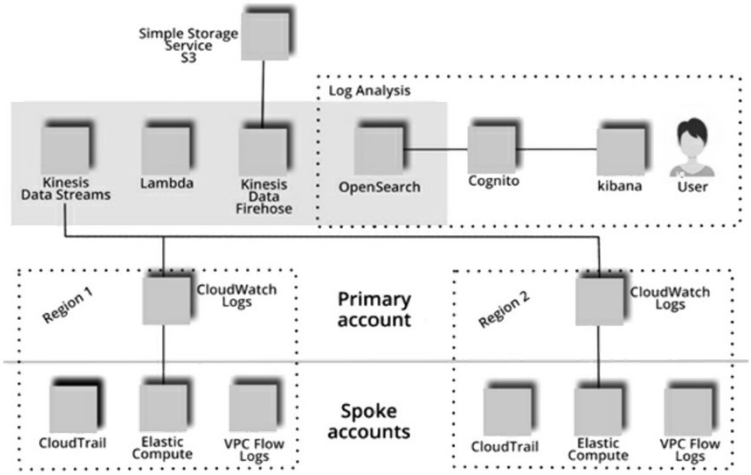
❖ AWS 보안, 자격 증명 및 규정 준수 서비스

카테고리	설명	AWS 서비스
ID 및 액세스 관리	• AWS 서비스 및 리소스에 대한 액세스와 ID를 안전하게 관리	• AWS Identity and Access Management(IAM)
	• 여러 AWS 계정과 애플리케이션에 대한 인력의 액세스 권한을 중앙에서 관리	• AWS IAM Identity Center(SSO의 후속 서비스)
	• 안전하고 매칠 없는 확장 가능한 고객 ID 및 액세스 관리 구현	• Amazon Cognito
	• 맞춤형 애플리케이션 내에서 세부 권한 및 권한 부여를 관리	• Amazon Verified Permissions(평가판)
	• 완전관리형 Microsoft Active Directory 서비스로 효율성 개선	• AWS Directory Service
	• 여러 계정에서 AWS 리소스를 간편하고 안전하게 공유	• AWS Resource Access Manager
	• AWS 리소스를 확장할 때 중앙 집중식으로 환경을 관리	• AWS Organizations
탐지	• AWS 보안 검사 자동화 및 보안 경고 중앙 집중화	• AWS Security Hub
	• 지능형 위협 탐지로 AWS 계정을 보호	• Amazon GuardDuty
	• 규모에 맞는 지속적인 자동 취약성 관리	• Amazon Inspector
	• 몇 단계로 보안 데이터를 자동으로 중앙 집중화	• Amazon Security Lake(평가판)
	• 리소스 구성에 대한 진단, 감사 및 평가	• AWS Config
	• AWS, 온프레미스 및 기타 클라우드에서 리소스 및 애플리케이션을 관측하고 모니터링	• Amazon CloudWatch
	• 사용자 활동 및 API 사용 추적	• AWS CloudTrail
	• IoT 디바이스 및 플릿에서 보안 관리	• AWS IoT Device Defender
네트워크 및 애플리케이션 보호	• 계정 전체의 방화벽 규칙을 중앙에서 구성하고 관리	• AWS Firewall Manager
	• VPC 전반에 네트워크 방화벽 보안 배포	• AWS Network Firewall
	• 관리형 DDoS 보호 기능을 통해 애플리케이션 가용성과 응답성을 최대화	• AWS Shield
	• VPN 없이 기업 애플리케이션에 대한 보안 액세스 제공	• AWS Verified Access(미리 보기)
	• 일반적인 익스플로잇으로부터 웹 애플리케이션 보호	• AWS Web Application Firewall(WAF)
	• VPC의 아웃바운드 DNS 트래픽 필터링 및 제어	• Amazon Route 53 Resolver DNS Firewall
데이터 보호	• 대규모로 민감한 데이터 검색 및 보호	• Amazon Macie
	• 데이터를 암호화하거나 디지털 서명할 때 사용하는 키를 생성 및 제어	• AWS Key Management Service(AWS KMS)
	• AWS의 단일 테넌트 하드웨어 보안 모듈(HSM) 관리	• AWS CloudHSM
	• AWS 서비스 및 연결된 리소스를 통해 SSL/TLS 인증서를 프로비저닝하고 관리	• AWS Certificate Manager
	• 리소스를 식별하고 데이터를 보호하기 위한 사설 인증서 생성	• AWS Private Certificate Authority
	• 보안 암호의 수명 주기를 중앙에서 관리	• AWS Secrets Manager
인시던트 대응	• 보안 데이터를 분석하고 시각화하여 잠재적 보안 문제 조사	• Amazon Detective
	• AWS로의 확장 가능하고 비용 효율적인 애플리케이션 복구	• AWS Elastic Disaster Recovery
규정 준수	• AWS의 규정 준수 보고서에 온디맨드 방식으로 액세스할 수 있도록 무료로 제공되는 셀프서비스 포털	• AWS Artifact
	• AWS 사용량을 지속적으로 감사하여 위험 및 규정 준수 평가를 간소화	• AWS Audit Manager

Source: https://aws.amazon.com/ko/products/security/

II. 클라우드 인프라 와 보안

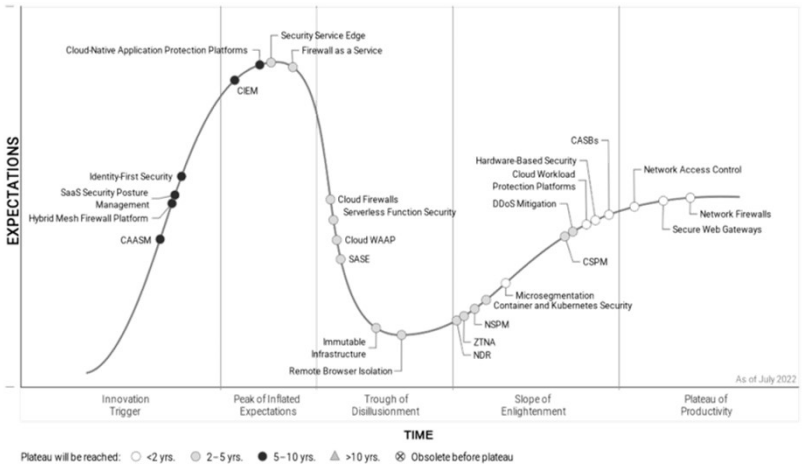
❖ **AWS suggested logging architecture.**



Source: Coombs, Ted. Cloud Security For Dummies (pp. 138-139). Wiley. Kindle Edition

II. 클라우드 인프라 와 보안

❖ **Hype Cycle for Workload and Network Security (Gartner 2022)**

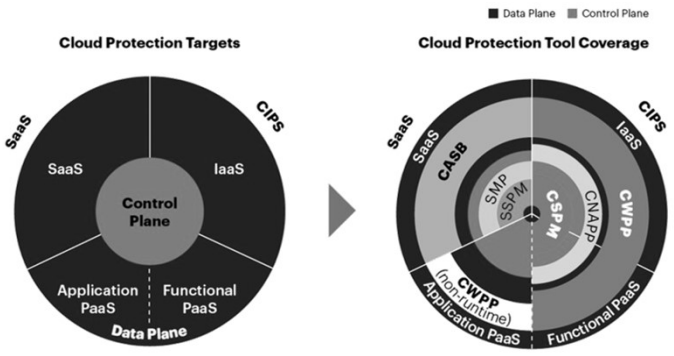


Source: https://www.illumio.com/blog/2022-gartner-hype-cycle-workload-network-security-microsegmentation-high-benefit-technology

❖ The Nuances of Split Responsibility

❖ Tool Coverage

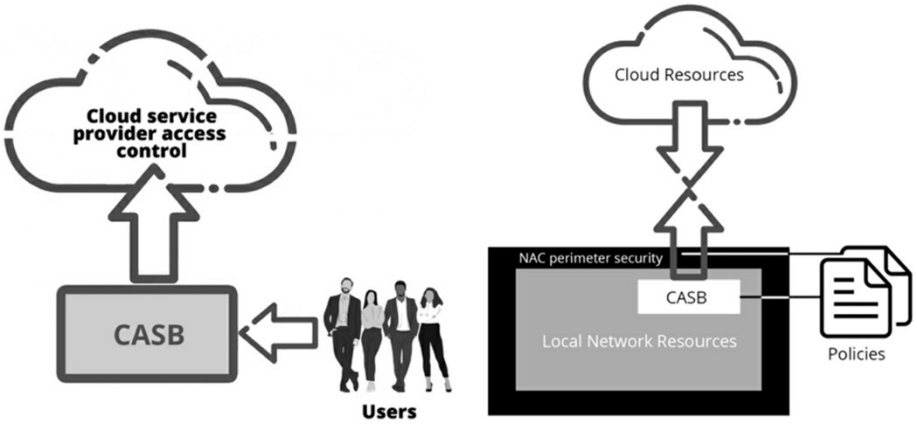
- **CASBs:** Cloud Access Security Brokers, (클라우드 액세스 보안 브로커)
- **CSPM:** Cloud Security Posture Management, (클라우드 보안 형상 관리)
- **CWPP:** Cloud Workload Protection Platform, (클라우드 워크로드 보호 플랫폼)
- **CNAPP:** Combined Cloud-native Application Platform Protection, (결합된 클라우드 네이티브 애플리케이션 플랫폼 보호)
- **SSPM:** SaaS Security Posture Management, (SaaS 보안 형상 관리)



Source: https://twitter.com/Gartner_inc/status/1534249589435518976

❖ CASB 시스템은 사용자와 클라우드 액세스 제어 시스템 사이에 위치

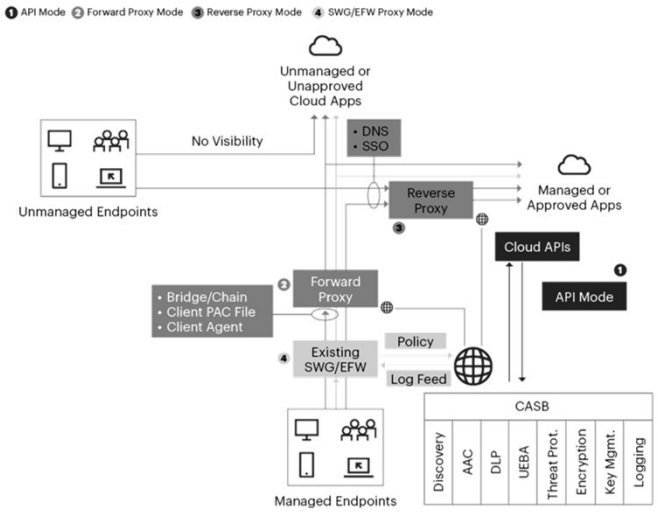
❖ 액세스 제어와 관련하여 NAC와 CASB 시스템은 동일한 정책을 가질 수 있다.



CASB (Cloud Access Security Broker)
Source: Coombs, Ted. Cloud Security For Dummies (p. 115). Wiley. Kindle Edition.

II. 클라우드 인프라 와 보안

❖ **CASB(Cloud Access Security Broker) Architectures**



The combination of CASB, SWG and ZTNA is called Security Service Edge (SSE):

- SWG(Secure Web Gateways)
- CASB(Cloud Access Security Broker)
- ZTNA(Zero Trust Network Access)

Source: Gartner

II. 클라우드 인프라 와 보안

❖ **Cloud Workload Protection Platform (CWPP)**

- **클라우드 워크로드 보호 플랫폼(CWPP)은 클라우드에서 운영과 관련된 워크로드를 관리**
- **네트워킹, 컴퓨팅, 스토리지가 포함**
- **클라우드 워크로드는 로컬 네트워크 환경의 동일한 서비스와는 다른 보안 요구 사항이 있음**
- **CWPP 시스템은 로컬 클라우드, 퍼블릭 클라우드 및 이 둘의 하이브리드를 포함하는 멀티클라우드 환경에서 이러한 워크로드를 관리.**
- **CWPP를 구현하면 여러 가지 이점**
  - CWPP 애플리케이션은 DevOps 개발 파이프라인에 통합
  - 개발하는 애플리케이션이 워크로드 보안을 위해 자동으로 구성
  - CWPP는 클라우드 애플리케이션이므로 다른 클라우드 솔루션과 동일한 이점을 누릴 수 있다.
  - 필요에 따라 확장 및 축소할 수 있으며 사용량에 따라 요금이 지불
  - 많은 클라우드 기반 보안 솔루션과 마찬가지로 온프레미스와 클라우드 모두에서 전체 네트워크를 감독하는 단일 액세스 지점을 제공함으로써 가시성을 확보할 수 있다.
  - 이러한 유형의 솔루션은 제로 트러스트 구현 및 AIOps와 같은 인공 지능 솔루션과 잘 어울린다

Source: Coombs, Ted. Cloud Security For Dummies (pp. 304-305). Wiley. Kindle Edition.

II. 클라우드 인프라 와 보안

❖ **Cloud security posture management (CSPM)**

- **CSPM으로 관리하기 클라우드 보안 태세 관리(CSPM)는 CWPP의 중요 부분**
- **잘못된 구성은 클라우드 보안의 주요 문제 중 하나이므로 구성 오류를 검사하기 위해서는 CSPM과 같은 시스템이 필요**
- **직접적인 오류 외에도 구성이 회사 보안 정책은 물론 회사에서 직면할 수 있는 모든 규정 준수 요구 사항과 일치하는지 확인**
- **구성 설정의 수가 관리할 수 없을 정도로 방대해졌기 때문에 자동화가 필요한 시점**
- **CSPM 시스템은 대부분의 구성 오류를 자동으로 찾아서 수정하므로 시스템의 보안을 강화할 수 있다.**
- **체크포인트(www.checkpoint.com)는 CWPP와 CSPM 솔루션을 모두 보유하고 있고, 클라우드가드 워크로드 보호 애플리케이션은 서버리스 및 컨테이너화된 클라우드 애플리케이션에 보안을 제공할 수 있다.**
- **맥아피는 제로 트러스트 철학에 따라 검색, 위험 평가, DevOps와의 통합 등 동일한 기능을 수행하는 MVISION 클라우드 네이티브 애플리케이션 플랫폼(CNAPP www.mcafee.com/enterprise/en-us/solutions/mvision.html)을 보유하고 있다.**
- **Aqua(www.aquasec.com)에서도 CNAPP 솔루션을 제공한다.**

Source: Coombs, Ted. Cloud Security For Dummies (pp. 304-305). Wiley. Kindle Edition.

II. 클라우드 인프라 와 보안

❖ **What Are the Factors Driving the Need for CSPM?**

1. **클라우드 컴퓨팅 도입이 증가:** 따라 기업은 점점 더 많은 클라우드 서비스를 사용하며 점점 더 복잡한 환경을 활용하고 있고, 더 많은 요구 사항을 충족하기 위해 클라우드 공급업체는 각각 고유한 구성 옵션이 있는 다양한 서비스를 제공하므로 이러한 구성이 보안에 미치는 영향을 모니터링하고 이해하기 어렵다.
2. **클라우드 확산으로 인한 클라우드 가시성 문제:** 기업은 일반적으로 클라우드 배포 및 서비스에 대한 완전한 가시성을 확보하지 못한다. 이는 많은 팀이 여러 공급업체에 걸쳐 새로운 클라우드 계정과 서비스를 설정할 수 있는 기능을 가지고 있기 때문이다.
3. **클라우드 인프라의 동적 특성:** 클라우드 서비스는 지속적으로 새로운 리소스를 추가하거나 제거하는 스케일아웃 기능을 제공한다.
4. **복잡한 환경은 보안 문제로 이어진다:** 기업이 멀티 클라우드 및 하이브리드 클라우드 전략을 채택함에 따라 적절한 보안을 위해 가시성이 매우 중요해졌다.
5. **셀프 서비스 IaaS 및 PaaS:** 셀프 서비스 기능을 사용하면 개발자가 계획 및 배포 단계에서 IT 및 보안 인력에 대한 의존도를 낮출 수 있지만 적절한 보안 및 가시성 범위를 제공하지는 못한다.
6. **보안 전문성 부족:** 개발자와 클라우드 운영팀이 암호화, 서비스 권한 부여, 키 관리와 같은 측면에 대한 위험 및 보안 결정을 내려야 한다. 실수나 잘못된 구성을 방지하기 위해 적절한 가시성과 제어 기능이 있어야 한다.
7. **적절한 도구 부재:** 기업이 데브옵스(DevOps)로 전환하는 동안 기존 보안 도구는 너무 느리고 번거로워 클라우드 리스크를 관리하기 어렵고, 팀은 규정 준수 및 보안 검사를 개발 파이프라인에 직접 통합해야 한다.

Source: https://www.aquasec.com/cloud-native-academy/cspm/gartner-cspm/

II. 클라우드 인프라 와 보안

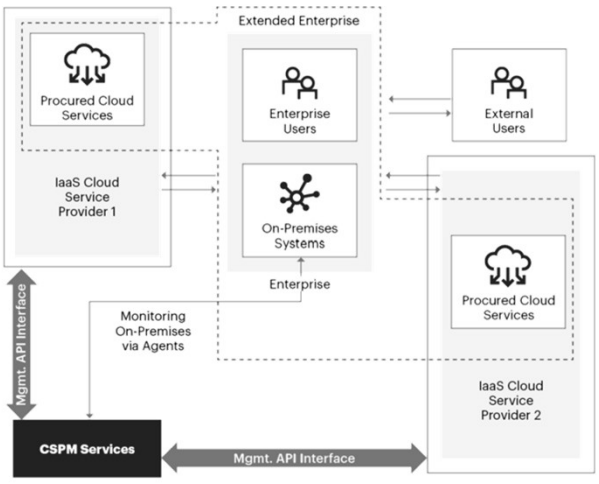
❖ How Does Cloud Security Posture Management(CSPM) Work?

- CSPM 도구는 클라우드 환경을 검사하고 모범 사례 및 알려진 보안 문제와 비교하는 방식으로 작동
- CSPM 도구는 보안 위험을 수정해야 할 때 클라우드 리소스 소유자에게 경고하고, 경우에 따라 자동화를 사용하여 부적절한 계정 권한을 취소하는 등 문제를 자동으로 해결
- CSPM은 일반적으로 클라우드 우선 전략을 채택하고 보안 모범 사례를 하이브리드 및 멀티 클라우드 환경으로 확장하려는 조직에서 사용
- CSPM은 원래 Amazon EC2 컴퓨팅 인스턴스와 같은 서비스형 인프라(IaaS) 클라우드 리소스를 보호하는 데 사용되었지만, 클라우드 데이터베이스와 같은 서비스형 플랫폼(PaaS)과 서비스형 소프트웨어(SaaS)의 잘못된 구성을 식별하는 데도 사용
- CSPM 솔루션은 여러 데이터 소스에 의존할 수 있고, 일반적으로 서비스 구성에 대한 가시성을 확보하기 위해 클라우드 제공업체 API에 액세스한다. 다른 소스에는 취약한 워크로드를 찾기 위해 이벤트의 클라우드 모니터링(예: AWS CloudTrail), 로그 분석 또는 클라우드 블록 스토리지 볼륨 분석이 포함
- 일부 CSPM 도구는 특정 클라우드 환경이나 서비스에 대해 정의된 모범 사례만 사용할 수 있는 반면, 다른 도구는 조직이 맞춤형 규정 준수 표준이나 정책을 지정할 수 있는 더 유연한 기능을 제공
- 특정 도구는 특정 클라우드 환경의 잘못된 구성을 감지하는 데 제한될 수 있고 여러 클라우드 계정에서 작동하지 않을 수 있으므로 도구를 선택할 때 이 점을 고려하는 것이 중요하고, 대부분의 CSPM 도구는 HIPAA, GDPR, PCI DSS를 비롯한 일반적인 규정 및 업계 표준에 따라 지속적인 규정 준수 검사를 지원

Source: https://www.aquasec.com/cloud-native-academy/cspm/gartner-cspm/

II. 클라우드 인프라 와 보안

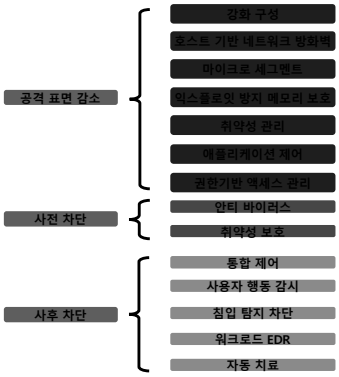
❖ Multicloud Use Case for CSPM



Source: Gartner

❖ **Types of Cloud Workload Protection Platforms(CWPP) and Their Minimum Capabilities**

클라우드 워크로드 보호 플랫폼(CWPP)



■ Attack Surface Reduction ■ Pre-Execution Protection ■ Post-Execution Protection

	공격 표면 감소	사전 차단		사후 차단				
				CWPP Variants				
CWPP's "DNA Markers"/Capabilities	Broad Spectrum	컨테이너 Container-Focused	서버리스 Serverless-Focused	메모리 Memory, Process Integrity Protection	ID Identity-Based Segmentation and Visibility	EDR EDR-Focused	취약성 Vulnerability, Hardening and Config. Compliance	앱제어 App. Control/ Desired State Enforcement
Hardening and Configuration	■	■		■			■	■
Host-Based Network Firewalling	■	■			■			
Microsegmentation	■	■			■			
Exploit Prevention and Memory Protection	■			■				
Vulnerability Management	■	■					■	■
Application Control	■	■	■	■	■		■	■
Privileged Access Management	■	■	■					
Antivirus	■					■		
Vulnerability Shielding	■			■			■	■
Integrity Control	■	■	■	■			■	■
User Behavior Monitoring	■	■	■		■	■	■	■
Intrusion Detection/ Prevention	■	■			■	■		
Workload EDR						■		
Autoremediation	■	■			■	■	■	■

Source: Gartner

Endpoint detection and response (EDR)

97

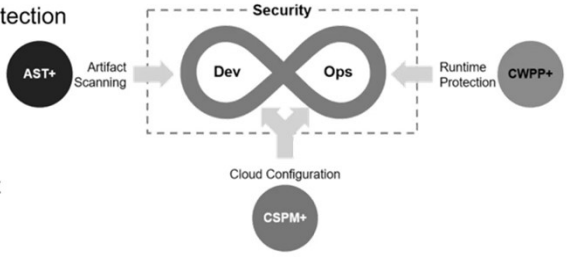
❖ **클라우드 네이티브를 위한 보안** (Evolving Security Approaches Cloud Native Applications)

- **CSPM: Cloud Security Posture Management** (클라우드 보안 형상 관리)
- **CWPP: Cloud Workload Protection Platform** (클라우드 워크로드 보호 플랫폼)
- **AST: Application Security Testing** (애플리케이션 보안 테스트)

클라우드 네이티브
애플리케이션 보호 플랫폼

Cloud-native application protection platforms needs to address:

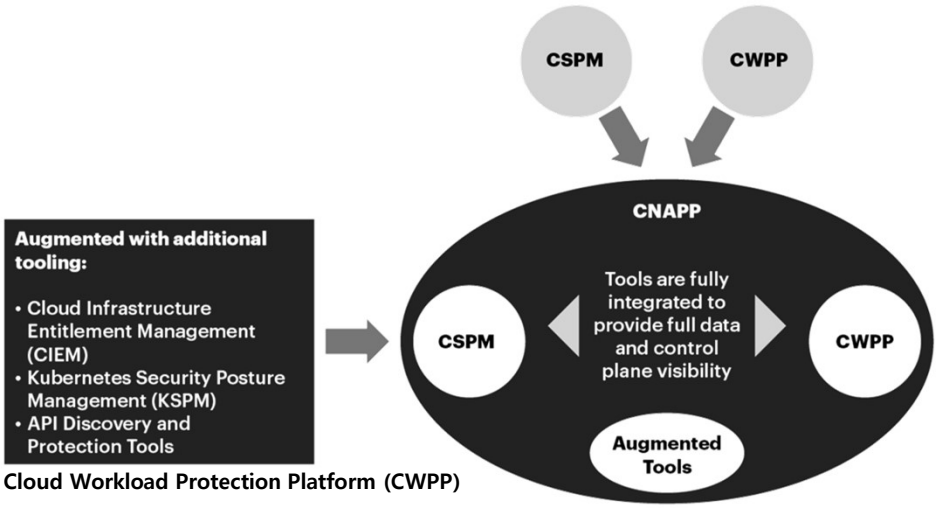
- **Runtime** Protection
- Cloud **Configuration**
- **Artifact** Scanning
- **DevSecOps** Enablement



Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

II. 클라우드 인프라 와 보안

❖ **Cloud-Native Application Platform Protection (CNAPP)**



Cloud Workload Protection Platform (CWPP)

Source: Gartner

II. 클라우드 인프라 와 보안

❖ **The Cloud Native Application Protection Platform (CNAPP)**

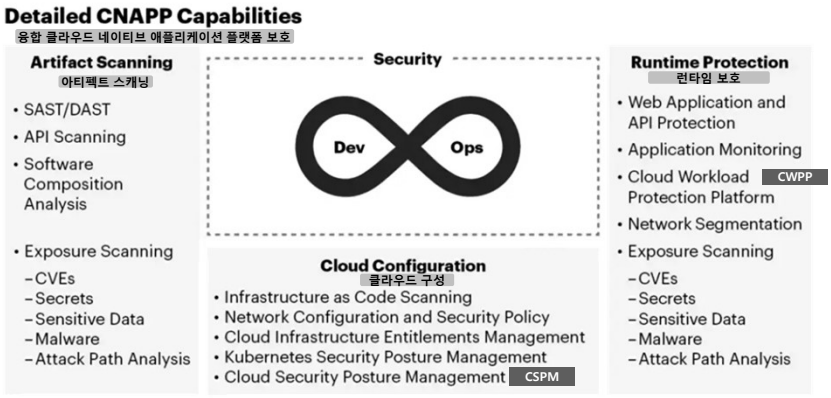
- **Artifact scanning:** 아티팩트란 소프트웨어 프로그램, 라이브러리, 압축된 아카이브 파일 또는 애플리케이션 배포에 사용되는 기타 파일을 의미
- **Cloud Workload Protection Platform (CWPP)**
- **Cloud Infrastructure Entitlements Management (CIEM):**
- **Cloud Security Posture Management (CSPM):** 이 기능은 구성 설정을 적용할 때 취약성을 보호하고 사람의 실수로부터 보호.
- **Kubernetes Security Posture Management (KSPM):**

Source: Coombs, Ted. Cloud Security For Dummies (p. 304). Wiley. Kindle Edition.

II. 클라우드 인프라 와 보안

❖ **The all in-one Cloud Security Solution CNAPP** (Gartner)

• **CNAPP: Cloud-Native Application Protection Platform** (융합 클라우드 네이티브 애플리케이션 보호 플랫폼)

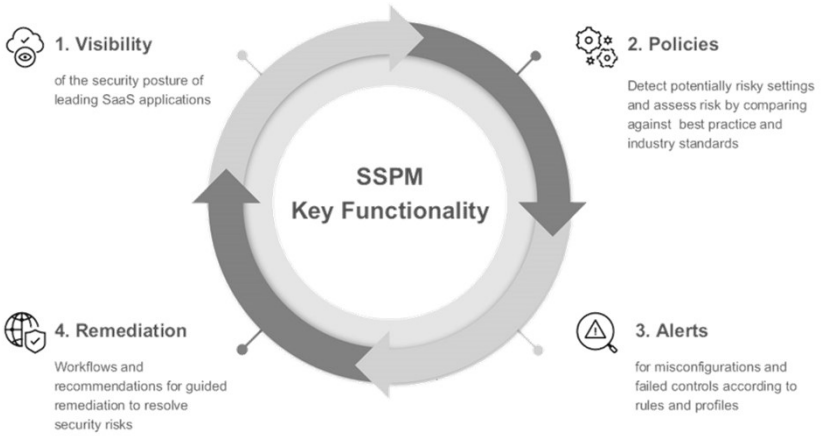


Static application security testing (SAST), Dynamic application security testing (DAST)

Source: https://medium.com/geekculture/the-all-in-one-cloud-security-solution-cnapp-according-to-gartner-3ef52e75b65d

II. 클라우드 인프라 와 보안

❖ **What is SaaS Security Posture Management (SSPM)**

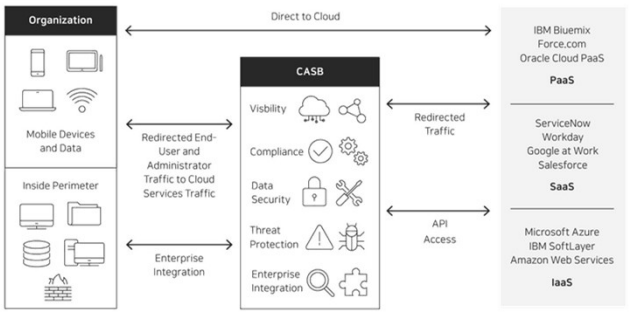


Source: https://www.netskope.com/security-defined/what-is-sspm#:~:text=On%20a%20simpler%20note%2C%20think,policies%20and%2For%20regulatory%20standards.

II. 클라우드 인프라 와 보안

❖ **CASB** (Cloud Access Security Broker)

- 이용자와 클라우스 서비스 사이에 위치하여 독립적으로 보안 기능을 수행하는 솔루션
- 에이전트, 어플라이언스(Appliance), API 등 다양한 형태로 제공
- 클라우드 서비스 이용에 대한 가시성, 접근제어, 내부정보 유출방지(DLP), 이상탐지, 로깅(Logging), 감사(Audit) 등의 보안 기능을 수행
- 일반적인 CASB는 API를 통해 보안 기능을 제공하며 클라우드 서비스에 특화된 정교한 보안 정책을 제공하며, 신규 서비스에 대한 지속적인 지원이 필요

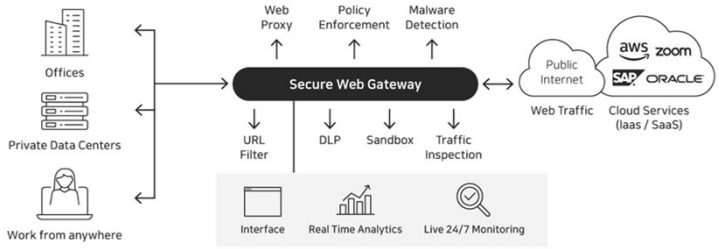


Source: CASB – 클라우드 접속 보안 브로커, ITFIND

II. 클라우드 인프라 와 보안

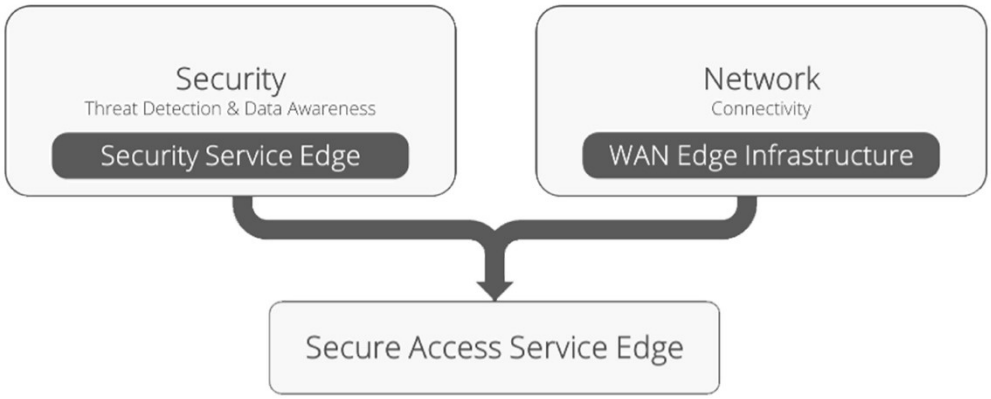
❖ **SWG (Secure Web Gateway)**

- 사용자와 클라우드 사이에 위치하며, 웹에 특화된 보안 정책을 제공
- 데이터 유출 방지, 안티바이러스, URL 필터링, HTTPS 검사, 애플리케이션 제어 등의 보안 기능을 제공
- 웹 콘텐츠가 내부에 도달하기 전에 이를 선별하고 필터링 (모든 트래픽이 SWG를 경유)
- 독립적으로 실행되거나 또는 SASE의 일부로 배포되어 사용될 수 있다. SWG와 CASB는 제공하는 보안 기능의 수준(Granular) 과 범위(Coverage) 차이가 있으나 SASE 또는 SSE(Secure Service Edge) 등의 모델에서는 통합된 형태로 제공



Source: How Secure Web Gateway Works, Toolbox

❖ SASE: Secure Access Service Edge (보안 엑세스 서비스 에지)



Source: Gartner 2023

❖ SASE is composed of both network and security principles.

TWO SIDES OF SASE

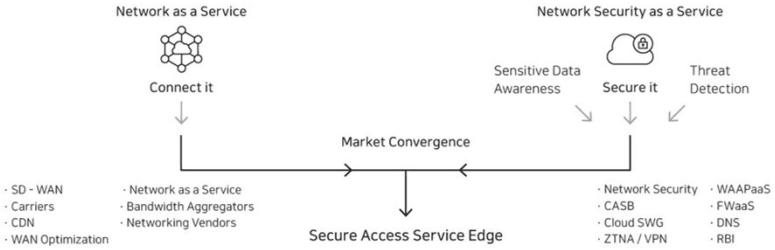
NETWORK	SECURITY
SD-WAN ROUTING DYNAMIC PATH SELECTION LATENCY OPTIMIZATION NaaS	WAN SECURITY BROWSING PROTECTION SaaS SECURITY WEB SECURITY REMOTE ACCESS FWaaS IoT SECURITY

SASE, known as the Security Service Edge (SSE).

Source: Coombs, Ted. Cloud Security For Dummies (p. 298). Wiley. Kindle Edition.

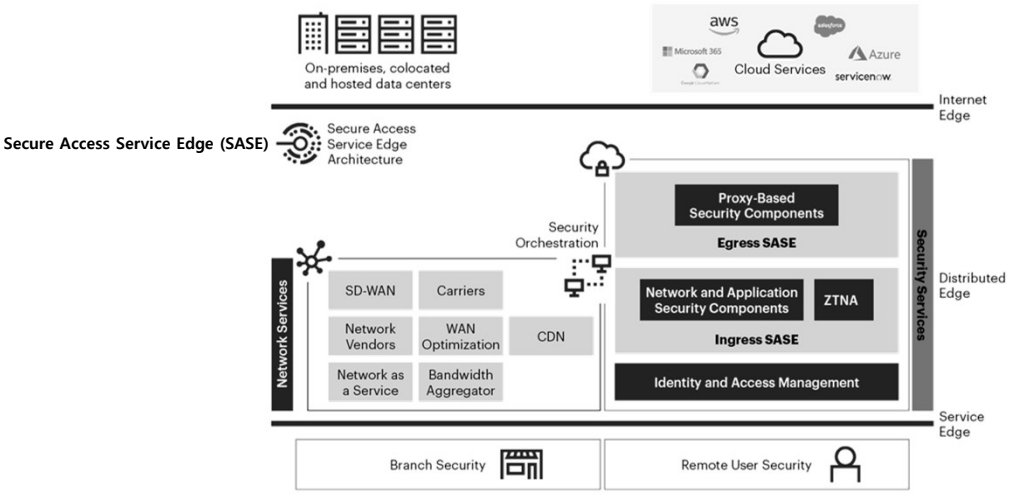
❖ SASE (Secure Access & Service Edge, 새시)

- 2019년 가트너(Gartner)가 제시한 새로운 개념으로 네트워크와 보안이 통합하는 아키텍처
- SASE는 WAN(Wide Area Network)과 CASB, FWaaS(Firewall as a Service), SDP, SWG 등의 보안서비스를 단일 클라우드 또는 플랫폼으로 통합하여 제공
- 가트너는 이를 통해 다양한 네트워크 환경 및 보안 서비스 구축에 대한 유연성을 확보하면서 비용과 복잡성을 감소시킬 수 있다고 예상
- 모든 연결과 컨텐츠를 SASE에서 검사하는 것으로 가시성과 보안성을 동시에 확보할 수 있다고 기대



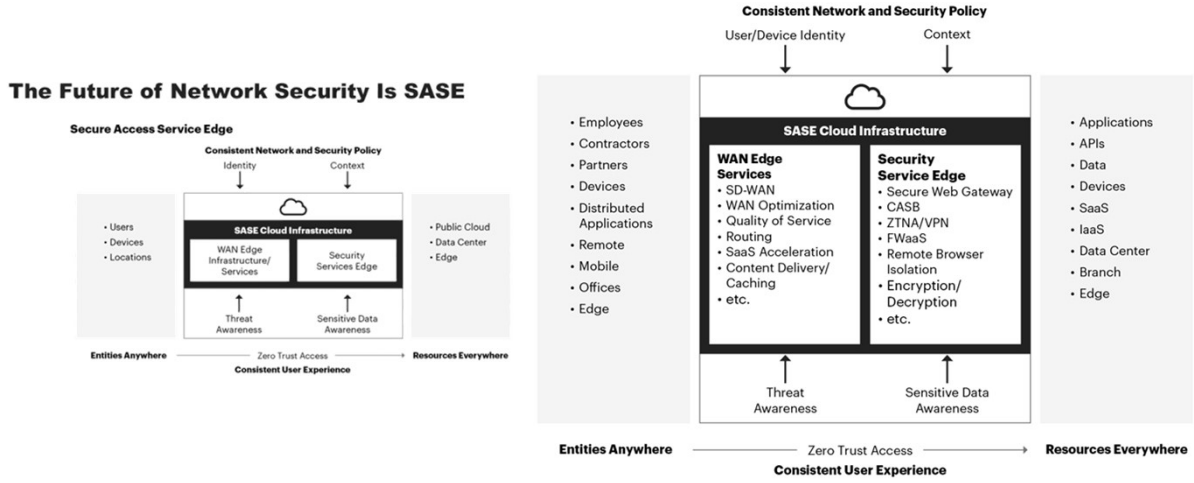
Source: SASE Convergence – The Future of Network is in the Cloud, Gartner

❖ 가트너의 SASE 아키텍처 구성 요소



Source: Gartner

❖ SASE Detailed View



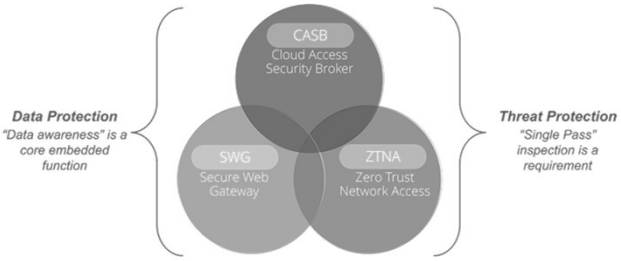
Source: Gartner

❖ The Leading SASE(Secure Access Service Edge) Vendors

Source: https://investianalystnewsletter.substack.com/p/sase-breakdown-a-deep-dive-and-the

❖ **What is the SSE(Security Service Edge)?:** 2021년 초에 가트너가 처음 소개한 보안 서비스 에지(SSE)는 단일 공급업체의 클라우드 중심 통합 솔루션으로 웹, 클라우드 서비스, 서비스형 소프트웨어 및 비공개 애플리케이션에 대한 엔터프라이즈 액세스를 보호하여 디지털 혁신을 가속화하고 성능 향상과 성장을 수용할 수 있는 클라우드 및 네트워킹 보안 구축에 필수적인 구성 요소로 간주된다. Gartner에 따르면 SSE는 주로 클라우드 기반 서비스로 제공되며 온프레미스 또는 에이전트 기반 구성 요소의 하이브리드를 포함할 수 있습니다. SSE 클라우드 기반 구성 요소 및 기능은 다음과 같다:

- **액세스 제어**
- **위협 방어**
- **데이터 보안**
- **보안 모니터링**
- **네트워크 기반 및 API 기반 통합을 통해 적용하는 허용 가능한 사용 제어**

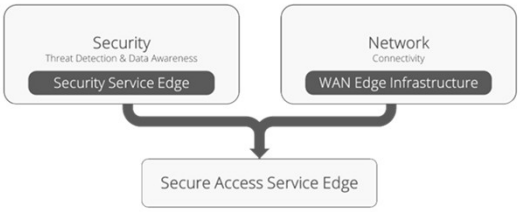


Source: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-sse.html

111

❖ **What's the difference between SASE and SSE?:**

- **보안 액세스 서비스 에지(SASE)는 네트워킹 및 보안 기술을 단일 클라우드 제공 플랫폼으로 통합하여 안전하고 빠른 클라우드 전환을 가능하게 하는 기술이고, SASE의 차세대 진화에서 고도로 통합된 광역 네트워크(WAN) 에지 인프라 플랫폼과 고도로 통합된 보안 플랫폼인 보안 서비스 에지(SSE)를 결합하는 두 가지 공급업체 접근 방식을 소개한다.**
- **보안 서비스 에지(SSE)는 웹, 클라우드 서비스, 프라이빗 애플리케이션에 대한 액세스를 보호하기 위해 보안 웹 게이트웨이(SWG), 클라우드 액세스 보안 브로커(CASB), 제로 트러스트 네트워크 액세스(ZTNA)를 비롯한 모든 보안 서비스를 통합하는 SASE의 보안 구성 요소이다. SASE 프레임워크의 네트워킹 구성 요소인 WAN 엣지 인프라는 네트워크 아키텍처를 혁신하여 보다 효율적인 클라우드 직접 연결을 지원함으로써 네트워크 연결 요소에 중점을 둔다.**



Source: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-sse.html

112

❖ **What's the difference between SASE and SSE?:**

- **SASE 프레임워크 내에서 네트워킹과 보안은 모두 통합된 방식으로 소비되며 클라우드 서비스로 제공됩니다. SSE는 WAN 엣지 인프라와 통합되어 완벽한 SASE 플랫폼을 구현합니다. SSE 보안 서비스에는 다음이 포함된다:**
  - ✓ **클라우드 접속 보안 브로커(CASB):** 기업이 민감한 자산을 클라우드로 이전할 때 사용자와 클라우드 서비스 제공업체 사이의 중개자 역할을 수행하여 데이터 가시성, 보안, 규정 준수의 격차를 해소하고 기존 온프레미스 인프라에서 보안 정책을 확장하며 클라우드 전용 콘텐츠에 대한 새로운 정책을 만들 수 있도록 지원한다. SSE 모델에 통합된 CASB는 서비스형 소프트웨어(SaaS) 리스크를 자동으로 검색 및 제어하며, 실시간 위협 방지를 위해 사용자 및 엔티티 행동 분석(UEBA) 및 인공 지능(AI) 기능을 활용하면서 데이터, 멀웨어 및 정책 위반에 대한 SaaS 애플리케이션을 검사하는 API 기반 보안 프로세스 역할을 한다.
  - ✓ **보안 웹 게이트웨이(SWG):** 승인되지 않은 트래픽이 기업 네트워크에 침입하는 것을 방지하는 체크포인트 역할을 하는 사이버 장벽이다. SWG는 사용자가 승인된 안전한 웹사이트에 접속할 수 있도록 하고 URL 필터링, 웹 가시성, 악성 콘텐츠 검사, 웹 액세스 제어와 같은 보호 기능을 실행하면서 사용자와 웹사이트를 연결하여 웹 기반 위협으로부터 사용자를 보호한다.
  - ✓ **제로 트러스트 네트워크 액세스(ZTNA):** 모든 원격 위치 및 디바이스에서 클라우드 및 기업 데이터 센터에서 호스팅되는 비공개 애플리케이션에 대한 안전한 제로 트러스트 액세스를 제공하기 위해 세분화된 적응형 및 상황 인식 정책을 시행한다. ZTNA는 보안 경계를 동적인 정책 기반의 클라우드 제공 에지로 전환하여 디지털 혁신의 접속 요구 사항을 지원하는 SASE의 핵심 요소로 작용한다.
  - ✓ **데이터 손실 방지(DLP):** 저장 중이거나 사용 중이거나 네트워크에서 이동 중인 개체(일반적으로 파일)에 포함된 정보 콘텐츠를 정책 기반으로 분류할 수 있도록 지원한다. DLP 도구는 이러한 정책을 실시간으로 적용하여 민감한 데이터 요소에 필요한 보호를 확장하고 조직의 정책에 따라 특히 조직 외부에서 이러한 정보에 대한 액세스 및 흐름을 제한하는 데 사용된다.
  - ✓ **원격 브라우저 격리(RBI):** 격리된 클라우드 환경 내에서 웹 브라우징 활동을 포함하는 강력한 형태의 웹 위협 보호 기능이다. RBI는 웹사이트에 숨겨져 있을 수 있는 멀웨어나 악성 코드로부터 사용자를 보호하고 악성 코드가 최종 사용자의 디바이스에 접근할 수 있는 기회를 제거한다.
  - ✓ **서비스형 방화벽(FWaaS):** 인터넷에서 데이터와 애플리케이션을 보호하는 클라우드 기반 방화벽 솔루션입니다. SSE는 FWaaS를 활용하여 온사이트 데이터 센터, 클라우드 인프라, 지사, 모바일 사용자 등 다양한 소스에서 발생하는 트래픽을 집계한다. 또한 FWaaS는 모든 위치와 사용자에 걸쳐 일관된 애플리케이션 및 보안 정책 적용을 제공하는 동시에 완벽한 네트워크 가시성과 제어 기능을 제공한다.

Source: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-sse.html

❖ **What are the benefits of SSE?:** 원격 근무 인력과 고객 기반에 대한 요구가 증가함에 따라 기업들은 보안 전략의 복잡성을 줄이는 동시에 보안과 사용자 경험을 개선해야 하는 과제를 안고 있다. 보안 서비스 에지(SSE) 통합 기술은 엔드포인트 보호의 복잡성을 줄이면서 기업 전체의 클라우드 서비스 보안을 강화하는 데 효과적인 것으로 입증되었다. 완전한 SSE 전략은 기업에게 온사이트와 원격에서 직원과 이해관계자에게 혜택을 제공하는 포괄적인 보안 기술 세트를 제공한다.

- **전 세계 어디서나 애플리케이션, 툴, 데이터, 리소스에 대한 직접적이고 안전한 인터넷 액세스, 무단 액세스, 데이터, 위험, 위협에 대한 처리 트래픽 감소, 무단 액세스, 데이터 위험, 위협에 대한 처리 트래픽 개선, 데이터 센터를 통해 트래픽을 다시 라우팅할 필요성 제거**
- **모든 사용자, 모든 기기, 어디서나 애플리케이션 리소스에 접속할 때 웹, 클라우드, 프라이빗 앱에 더 빠르고 안전하며 효율적으로 연결합니다.**
- **네트워크에 접속하는 사용자의 행동 모니터링 및 추적**
- **클라우드 내 및 모든 웹 대상에서 위협 방어, 클라우드 네이티브 공격과 지능형 멀웨어 모두 탐지**
- **인터넷, 클라우드 내, 클라우드 간 이동을 통한 데이터 보호**
- **사용자 ID, 컨텍스트, 최소 권한 액세스를 기반으로 데이터 및 애플리케이션에 대한 안전한 제로 트러스트 액세스 지원**

Source: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-sse.html

II. 클라우드 인프라 와 보안

❖ **Magic Quadrant for Security Service Edge(SSE)**

- **Netskope**
- **Zscaler**
- **Palo Alto Networks**
- **Cisco**
- **Skyhigh Security**
- **Force Point**
- **Lockout**
- **Broadcom**
- **iboss**
- **Cloudflare**

Source: Gartner 2023

Figure 1: Magic Quadrant for Security Service Edge

Source: Gartner

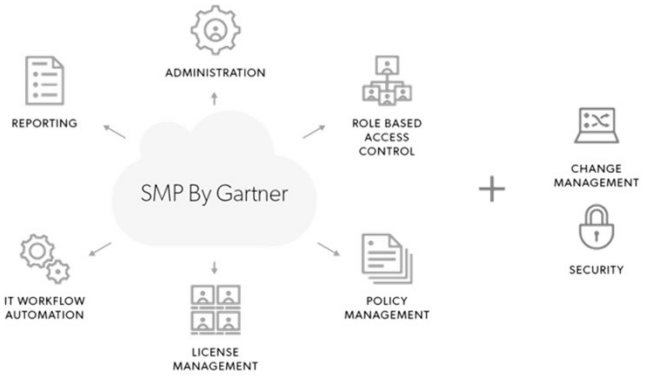
II. 클라우드 인프라 와 보안

❖ **What is a SaaS management platform (SMP)?:** SaaS 관리 플랫폼(SMP)은 서비스형 소프트웨어(SaaS) 애플리케이션에 대한 관리, 사용 및 보안 정보를 중앙 집중화하며, SMP는 다음 3개의 주기능을 제공한다.

- **애플리케이션 검색:** SMP는 ID 및 액세스 관리(IAM) 서비스부터 브라우저 확장에 이르기까지 다양한 소스를 사용하여 현재 사용 중인 모든 SaaS 애플리케이션을 추적한다. 또한 이러한 애플리케이션을 사용하는 사용자와 사용 빈도에 대한 정보를 집계한다.
- **애플리케이션 관리:** SMP는 SaaS 애플리케이션의 관리 기능을 중앙 집중화한다. 이를 통해 라이선스 관리, 사용자 오프보딩 및 온보딩, 애플리케이션 내 사용자 그룹 생성 및 관리와 같은 IT 작업을 간소화할 수 있다.
- **보안 및 규정 준수:** SMP를 통해 기업은 데이터 보호, 액세스 제어 및 기타 보안 설정을 중앙 집중화할 수 있습니다. IT 팀은 이러한 정보를 얻기 위해 각 SaaS 애플리케이션을 방문할 필요 없이 SMP를 제어 센터로 사용할 수 있습니다.

Source: https://www.cloudflare.com/en-gb/learning/cloud/what-is-smp/

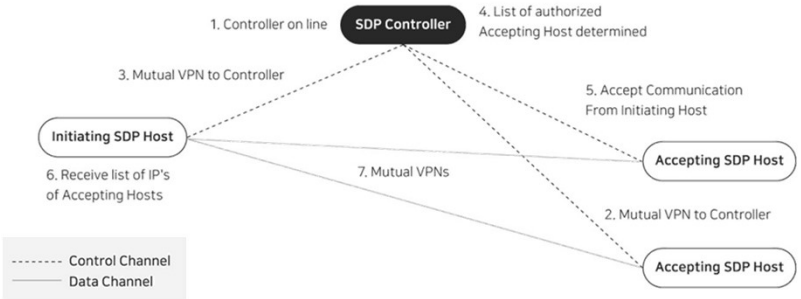
❖ What is a SaaS management platform (SMP)?



Source: https://www.cloudeagle.ai/blogs/choosing-the-best-saas-management-platform

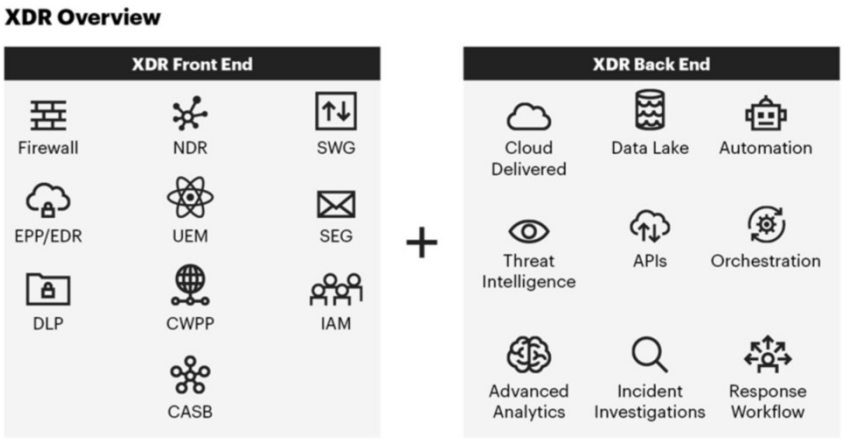
❖ **SDP** (Software Defined Perimeter, 소프트웨어 정의 경계)

- **CSA(Cloud Security Alliance)가 추진하는 접근통제를 위한 프레임워크**
- **SDP는 컨트롤러, 게이트웨이(또는 서버), 클라이언트로 구성하여 경계를 설정 기반으로 접근통제**
- **기존의 '선 연결, 후 인증' 방식에 비해 SDP는 '선 인증, 후 연결' 방식으로 인증 결과에 따라 연결이 제한**
- **이러한 특징으로 권한이 없는 사용자(인증 실패자)는 연결 대상을 확인조차 할 수 없는 상태가 되어 SDP를 '블랙 클라우드(Black Cloud)' 기술 이라고 부르기도 함.**



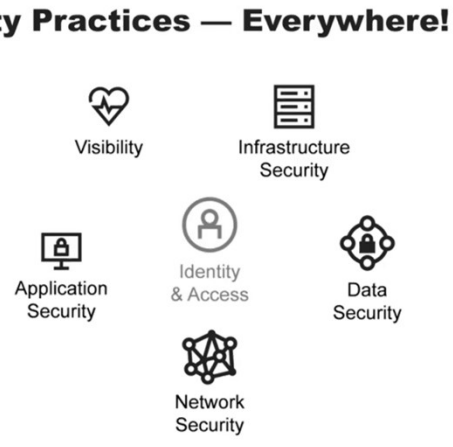
Source: SDP 아키텍쳐, SDP Specification 1.0, CSA

❖ XDR Overview

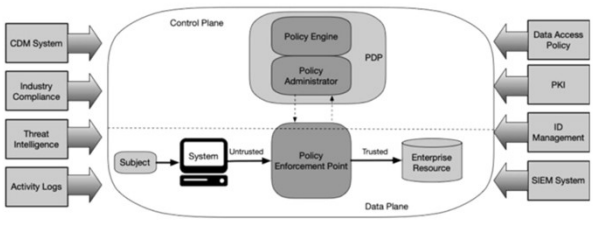


Source: https://www.gartner.com/doc/reprints?id=1-28124RDS&ct=211111&st=sb

❖ Zero Trust Architecture



❖ NIST(National Institute of Standards and Technology), 미국 국립 표준 기술 연구소
• Logical Zero Trust Components: 800-207 Zero Trust Architecture

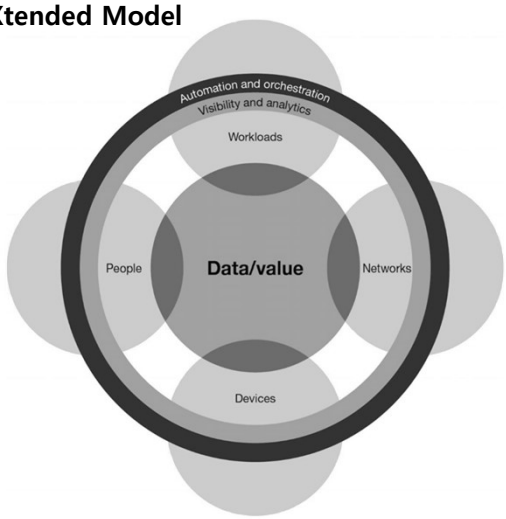


Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

II. 클라우드 인프라 와 보안

❖ **제로트러스트 확장 생태계: Forrester Zero Trust eXtended Model**

- **Data/value**
- **Visibility and analysis**
- **Automation and orchestration**
- **People / Workload / Network / Device**

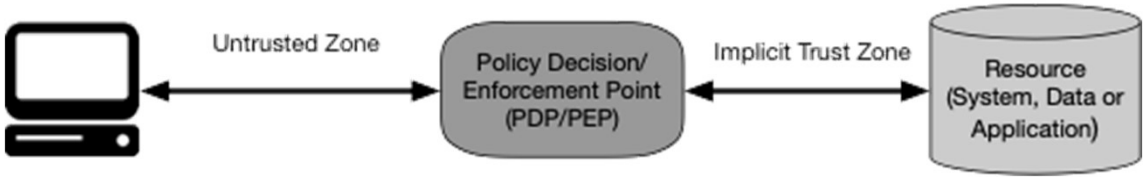


Source: The Zero Trust eXtended Ecosystem: Data, Forrester Research, Inc., August 11, 2020

II. 클라우드 인프라 와 보안

❖ **Zero Trust Access** (제로 트러스트 엑세스)

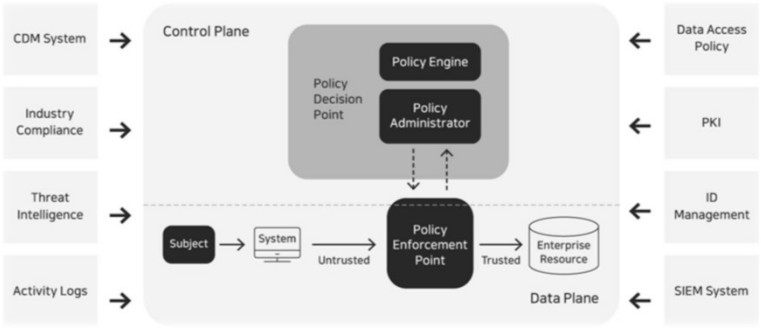
- **PDP: Policy decision point**
- **PEP: Policy enforcement point**



Source: NIST(National Institute of Standards and Technology), 미국 국립 표준 기술 연구소, Special Publication 800-207

❖ 제로트러스트 아키텍처(ZTA)

- 제로트러스트 아키텍처(ZTA)의 시작은 '누구(Components)' 를 어떻게 누락 없이 탐지하고 식별할 수 있는지의 가시성(Visibility)의 확보'
- 조직활동에 참여하는 모든 자산(Asset)이라고 할 수 있으며 구성원(사람)을 포함하여 서버, 네트워크 장비, 어플리케이션뿐만 아니라 정책, 워크플로우, 네트워크 연결 등 모든 것이 포함



Source: Core Zero Trust Logical Components, Zero Trust Architecture, NIST

❖ ZTNA Anywhere

- So as we shift to hybrid work, we are hoping that vendors get out in front of this problem with expanded/new offerings. Think of it as ZTNA Anywhere or Universal ZTNA.

From Zero Trust Network Access to Universal Zero Trust Network Access

Source: https://blogs.gartner.com/andrew-lerner/2022/03/08/ztna-anywhere/

II. 클라우드 인프라 와 보안

❖ **Security Operations Center (SOC)**

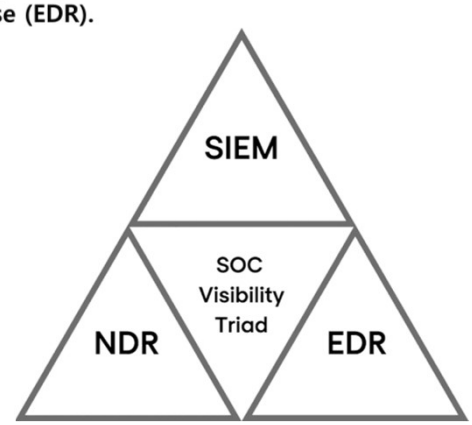
- 보안 운영 센터(SOC)는 조직의 컴퓨터 시스템과 네트워크에 대한 사이버 보안 위협을 모니터링, 탐지, 대응 및 완화하는 중앙 집중식 팀
- 다양한 도구와 기술을 사용하여 보안 데이터를 수집 및 분석하고, 잠재적인 위협을 식별하며, 조직을 보호하기 위한 조치를 취한다.
- SOC는 일반 데이터 보호 규정(GDPR)과 같은 업계 규정을 준수하는 데도 도움이 될 수 있다
  - ✓ 피싱 공격
  - ✓ 랜섬웨어 공격
  - ✓ 데이터 유출
  - ✓ 서비스 거부 공격
  - ✓ 멀웨어 감염
- SOC에는 일반적인 구성 요소
  - ✓ 보안 분석가 팀
  - ✓ 일련의 보안 도구 및 기술
  - ✓ 위협을 모니터링, 탐지 및 대응하기 위한 프로세스

Source: https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/

II. 클라우드 인프라 와 보안

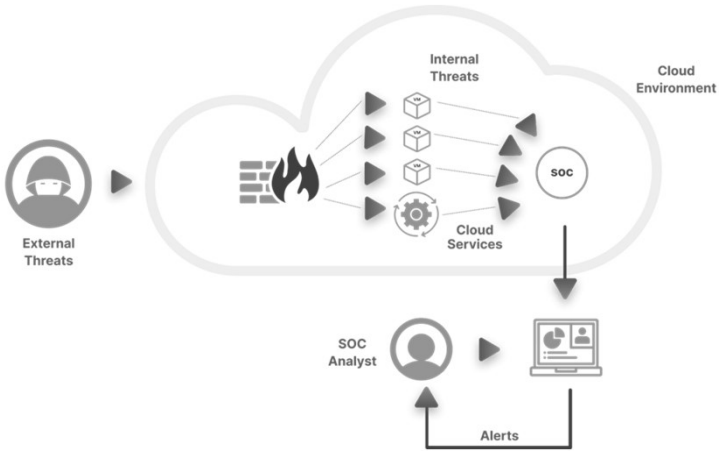
❖ **Three core elements of the SOC visibility triad.**

- 보안 정보 및 이벤트 관리를 통한 사용자 및 엔터티 행동 (SIEM으로 알려진 보안 전략)
- 네트워크 탐지 및 대응, Network detection and response (NDR).
- 엔드포인트 탐지 및 대응, Endpoint detection and response (EDR).



Source: https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/

❖ C-SOC: Protect your Multi-Cloud environments from internal and external threats.

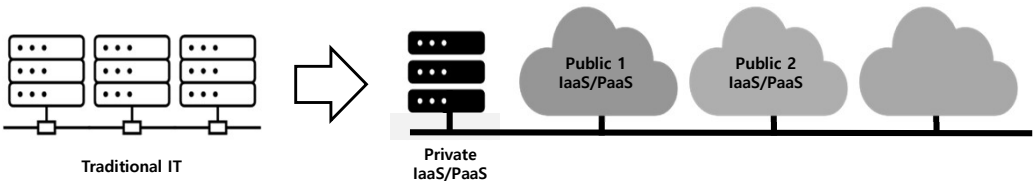


C-SOC (Cloud Security Operations Center)

Source: https://www.axiomio.com/cloudsoc

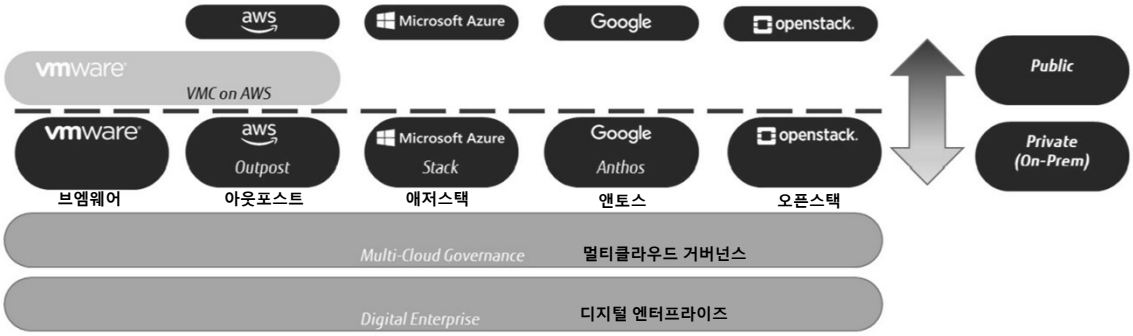
❖ **클라우드 운영 모델의 변화**

- **Run:** 전용 인프라 → 클라우드 상의 스케줄링
- **Connect:** 고정 IP 주소 → 서비스 기반 유동 IP
- **Secure:** IP 주소 기반 보안 정책 → Identity 기반
- **Provisioning:** 전용 서버 → 요청 기반 용량



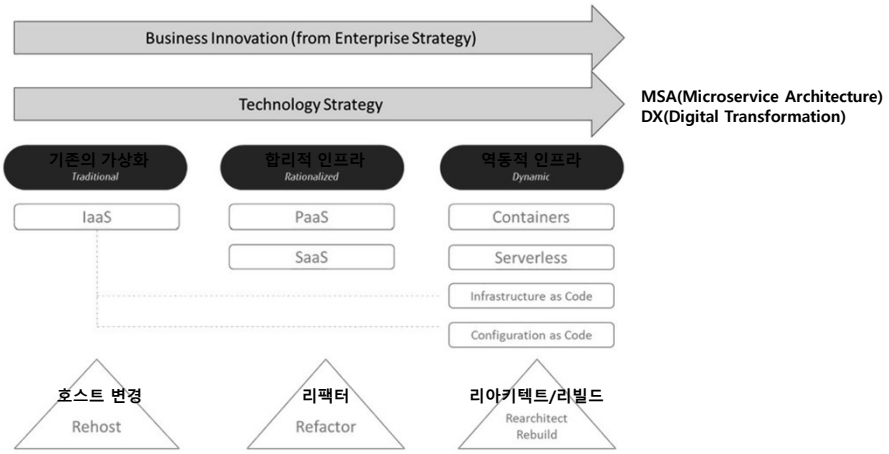
❖ 주요 멀티클라우드 플레이어 (Main players in the field)

- Public: AWS, Azure, Google, OpenStack, (VMware)
- Private(On-Prem): VMware, Outpost(AWS), Azure Stack, Anthos(Google), OpenStack



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 48). Packt Publishing. Kindle Edition.

❖ Technology strategy following business innovation



Source: Mulder, Jeroen. Multi-Cloud Architecture and Governance: Leverage Azure, AWS, GCP, and VMware vSphere to build effective multi-cloud solutions (p. 83). Packt Publishing. Kindle Edition.

II. 클라우드 인프라 와 보안

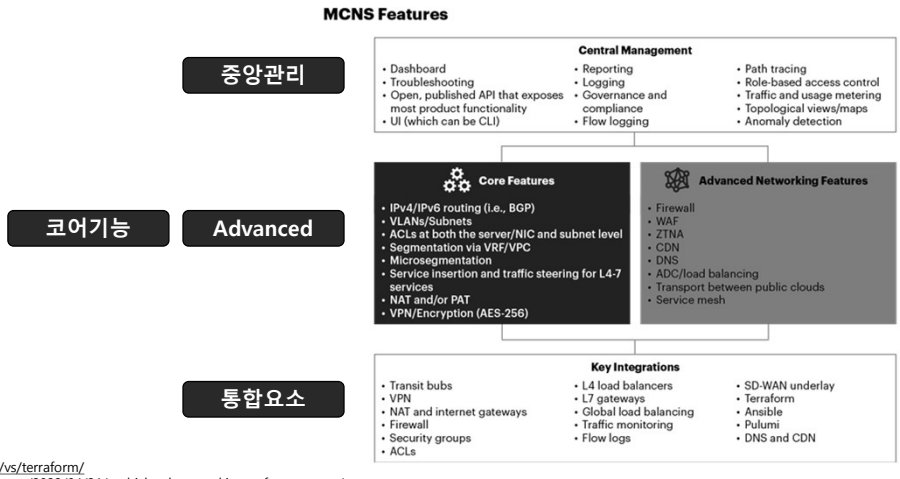
❖ 멀티클라우드 장점 - Benefts of Multi-Cloud

- Cost-effective service with optimum satisfaction — 비용
- One out of many alternatives to choose the best in Class Services — 선택의 범위
- Availability — 가용성
- Avoiding Vendor Lock-in — 벤더 락인 회피
- Data Privacy and Compliance — 데이터 보안 준수
- Proximity/Low Latency — 지연
- Disaster Recovery — 재난 복구
- Data Management — 데이터 관리

Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

II. 클라우드 인프라 와 보안

❖ 가트너(예): Multicloud Networking Software (MCNS)

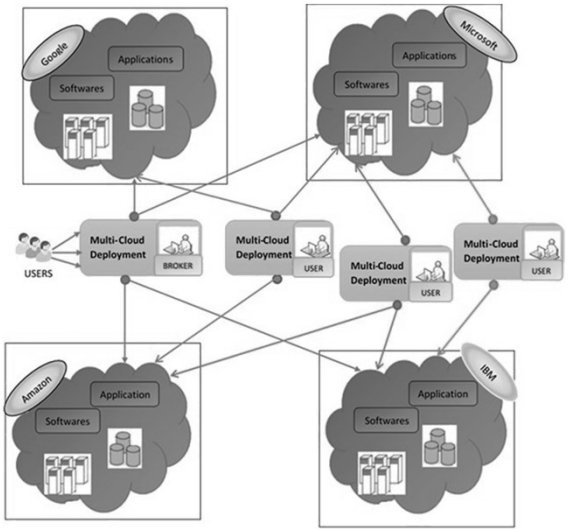


Source: https://www.pulumi.com/docs/intro/vs/terraform/
Source: https://blogs.gartner.com/andrew-lerner/2022/04/21/multicloud-networking-software-mcns/

❖ 멀티클라우드 환경 - Multi-cloud environment

- **Cloud Aggregators**
- **Cloud Integrators**
- **Cloud Customizers**

Cloud aggregators are high-level consultants or architects who bring together multiple **cloud** services and offer them as a combined package to customers.



Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

❖ 제조사의 멀티클라우드 (예): Multi-Cloud Network (Cisco Cloud Network Controller)

- **Intra-cloud connectivity:** Extend segments across regions, Automate route propagation across virtual networks, Automate L4-L7 service insertion
- **Inter-cloud connectivity:** Automate route propagation across clouds, Extend routing domains and segments across Clouds, Automate L4-L7 service insertion
- **Hybrid cloud connectivity:** Automate Overlay connectivity for different types of Underlays, Extend routing domains and segments between On Premises and Cloud sites, Enable consistent networking and visibility between On Premises and Cloud
- **External network connectivity:** Standards-based IP connectivity to any network, Secure connectivity to external network spanning datacenters and branches.
- **L4-L7 service insertion:** Automate firewall and load balancer insertion, Automatically update routing and security policy to insert L4-L7 services, Integrate with third-party L4-L7 services and cloud native L4-L7 services
- **Brownfield VPC onboarding:** Safe and fast migration and rollback, Ability to use Cloud Network Controller with brownfield environments

Source: https://blogs.cisco.com/datacenter/modernize-your-multi-cloud-network-with-cisco-cloud-network-controller

II. 클라우드 인프라 와 보안

❖ 멀티클라우드 환경의 도전

• Challenges in multi-cloud environment

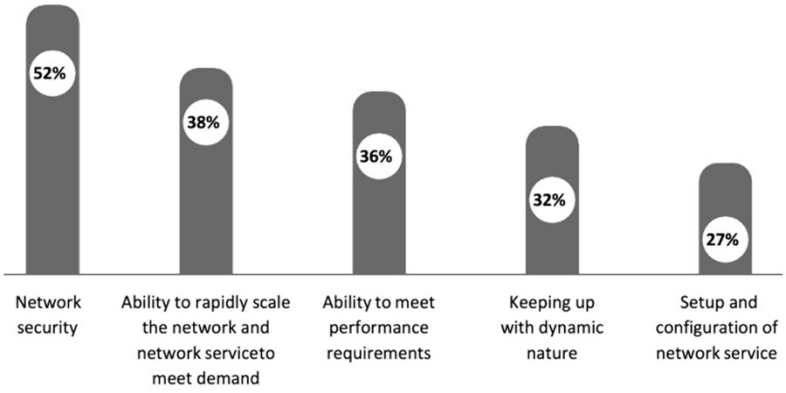
Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

II. 클라우드 인프라 와 보안

❖ 멀티클라우드 네트워킹의 도전 - Challenges of Multi-cloud networking

• Top five network challenges in modern multi-cloud environments

✓네트워크 보안
✓네트워크의 신속한 스케일 요구
✓성능 요구
✓클라우드 특징 다이나믹 지원
✓네트워크 서비스 구성

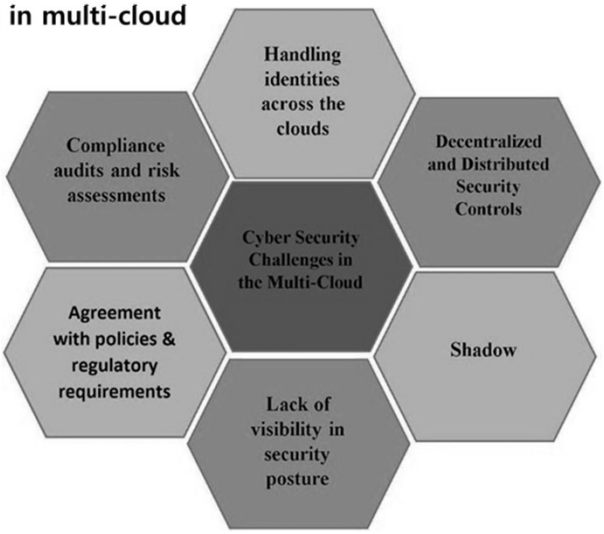


Source: https://www.wipro.com/infrastructure/the-strategy-to-build-secure-multi-cloud-networking/

II. 클라우드 인프라 와 보안

❖ 사이버보안 도전 - Cyber security challenges in multi-cloud

- 준수 (Compliance)
- 정책 (Policy)
- 가시화 (Visibility)
- 음영 (Shadow)
- 탈중앙 제어 (Decentralized)
- 클라우드간 ID (Identity)



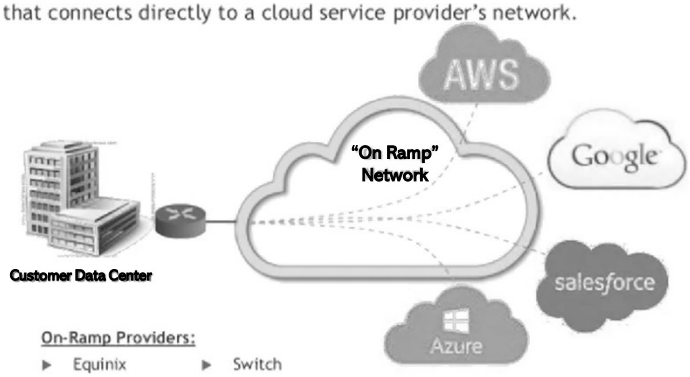
Source: 'Operationalizing Multi-Cloud Environments', Technologies, Tools and Use Cases, B. S. Rajeshwari, Pethuru Raj, Ramkumar Thirunavukarasu (2022)

II. 클라우드 인프라 와 보안

❖ 온램프 서비스 - Cloud "On-Ramp" Service Providers

- Equinix
- CoreSite
- Digital Realty
- Switch
- Cologix
- Megaport

▶ Cloud On Ramp Services provide a connection service within a data center that connects directly to a cloud service provider's network.



On-Ramp Providers:

- ▶ Equinix
- ▶ CoreSite
- ▶ Digital Realty
- ▶ Switch
- ▶ Cologix
- ▶ Megaport

Source: Joseph Primicerio

❖ 제조사의 멀티클라우드 (예): F5의 Distributed Cloud Mesh vs. Other Multi-Cloud Solutions

Features	Other solutions	Distributed Cloud Mesh
Consolidated L3-L7 networking + security service	x	v
Multi-tenancy + self-service for NetOps and DevOps	x	v
Multi-layer security	x	v
App-to-app connections without exposing the underlying network	x	v
Global physical network	x	v
Automation assistance for NetOps	v	v
Security service insertion	v	v
Observability and analytics	External	v
Lifecycle management	Controller	SaaS

Source: https://www.f5.com/cloud/use-cases/multi-cloud-networking

❖ MCNS (Multicloud Networking Software) 제조사

제조사	제품/서비스 또는 플랫폼
Alkira	Cloud Networking
Arrcus	Arrcus Multi-Cloud Networking (MCN)
Arista Networks	Any Cloud Platform
Aviatrix	Aviatrix Cloud Network Platform
Cohesive Networks	VNS3
Cisco	Cisco Cloud Services Router 1000V (CSR1kv), Cisco Catalyst 8000V Edge Software, Cisco Cloud APIC
F5	F5 Distributed Cloud Platform
Prosimo	AXI Platform
VMware	NSX Cloud

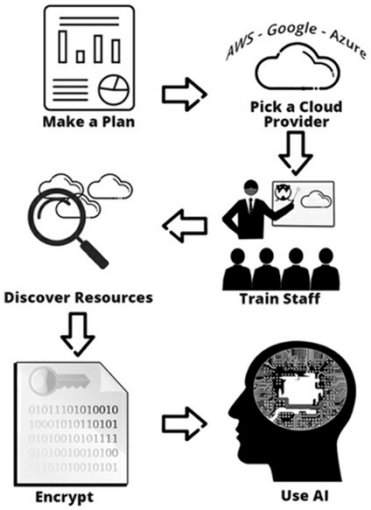
Source: https://www.gartner.com/doc/reprints?id=1-29S4R0C1&ct=220419&st=sb

III. 클라우드 보안 솔루션과 비즈니스

- 클라우드 트렌드 와 비즈니스
- 클라우드 네이티브 보안 도입
- 클라우드 보안 및 비즈니스 전략

❖ **An infographic of important steps to cloud security success.**

- **Make a Plan**
- **Pick a Cloud Provider**
- **Train Staff**
- **Discover Resources**
- **Encrypt**
- **Use AI**



Source: Coombs, Ted. Cloud Security For Dummies (p. 313). Wiley. Kindle Edition.

III. 클라우드 보안 솔루션과 비즈니스

- **AIOps will detect, prioritize, assign, diagnose, resolve, and self-improve, getting smarter all the time.**

Source: Coombs, Ted. Cloud Security For Dummies (p. 147). Wiley. Kindle Edition. .

III. 클라우드 보안 솔루션과 비즈니스

- **오픈 소스 보안 사용 많은 사이버 보안 방어 애플리케이션이 시중에 나와 있지만, 때로는 클라우드 리소스를 보호하기 위해 자체 애플리케이션을 구현하고 싶을 수도 있다. 처음부터 시작할 필요는 없으며, 필요에 따라 설치 및 수정할 수 있는 오픈 소스 프로젝트가 많이 있다.**
- **https://code.nsa.gov에서 NSA가 공개한 오픈 소스 프로젝트를 사용하여 오픈 소스 보안 개발을 시작할 수 있다.**
- **GitHub에서 수백 개의 오픈 소스 프로젝트를 찾을 수도 있다. 예를 들어, AWS 버킷을 위한 편리한 안티바이러스 프로젝트는 https://github.com/widdix/aws-s3-virusscan에서 찾을 수 있다. 이 특정 프로젝트의 홈페이지(https://bucketav.com)로 이동하면 이 프로젝트의 상용 버전에 대한 가격을 확인할 수 있습니다. 제약 조건에 따라 두 가지 중 하나를 선택할 수 있다.**

Source: Coombs, Ted. Cloud Security For Dummies (p. 142). Wiley. Kindle Edition. .

III. 클라우드 보안 솔루션과 비즈니스

❖ **클라우드 보안에 중점을 둔 보안 및 위험 관리 기술 전문가는 다음을 수행해야 한다.**

- **클라우드 보안 전략을 정의하고 식별된 요구사항에 따라 타사 도구로 보강된 클라우드 네이티브 제공업체의 도구를 선호하는 것부터 시작**
- **클라우드 보안 아키텍처 역할을 정립하고 모범 사례를 정의하여 민첩성을 유지하며 프로세스 기반 제어를 민첩하게 정의**
- **클라우드 앱 위험 기능에 클라우드 액세스 보안 브로커(CASB)를 사용하여 클라우드 위험 평가를 자동화하고 속도를 높힌다**
- **CASB를 사용하여 승인된 클라우드 앱의 중요한 데이터를 보호하고 승인되지 않은 클라우드 앱에 대한 가시성과 세분화된 액세스 제어를 제공**
- **클라우드 보안 태세 관리(CSPM), 클라우드 워크로드 보호 플랫폼(CWPP) 및 결합된 클라우드 네이티브 애플리케이션 플랫폼 보호(CNAPP) 공급업체 도구를 배포하여 여러 클라우드에서 IaaS 및 PaaS 가시성 및 워크로드 인사이트를 개선**
  - Cloud Access Security Brokers (CASBs)
  - Cloud Security Posture Management (CSPM)
  - Cloud Workload Protection Platform (CWPP)
  - Combined Cloud-native Application Platform Protection (CNAPP)

Source: Guide to Cloud Security Concepts (Gartner, September 2021)

III. 클라우드 보안 솔루션과 비즈니스

❖ **Getting that Stamp of Approval**

- **CCSK(The Certificate of Cloud Security Knowledge):** 클라우드 보안 지식 자격증(CCSK)은 클라우드 보안 전문가로 좋은 일자리를 얻고자 하는 사람과 이미 이 분야에서 일하고 있는 사람의 경력을 향상시키는 데 도움이 될 수 있다. (https://cloudsecurityalliance.org/education).
- **CISA (Certified Security Information Systems Auditor):** CISA 과정은 정보 보안 감사 관행의 필수 사항을 다루는 ISACA www.isaca.org 과정
- **CRISC (Certified Risk and Information Systems Control):** 이 자격증은 IT 위험 관리에 중점을 둡니다. 이 자격증은 위험을 식별, 분석, 평가, 평가, 우선순위 지정 및 대응하기 위한 모범 사례의 토대를 구축합니다. 이 인증 프로그램에 대한 자세한 내용은 https://www.isaca.org/credentialing/crisc 참조
- **CCAK (Certificate of Cloud Auditing Knowledge):** 이 과정에서는 클라우드 감사에 대한 필수 사항을 배울 수 있다. 규정 준수 요구 사항으로 인해 보안 감사를 받아야 하는 기업은 이러한 감사를 처리할 수 있는 숙련된 인력을 확보하고 싶을 것이다. 감사에 실패하면 회사에 심각한 결과를 초래할 수 있다.
- **Advanced Cloud Security Practitioner:** 고급 클라우드 보안 실무자 교육은 기본적으로 표준 실습 교육에서 확장된 CCSK 교육이다.
- **GDPR Lead Auditor and Consultant**

Source: Coombs, Ted. Cloud Security For Dummies (p. 317). Wiley. Kindle Edition

III. 클라우드 보안 솔루션과 비즈니스

❖ **Security Frameworks (1 of 2)**

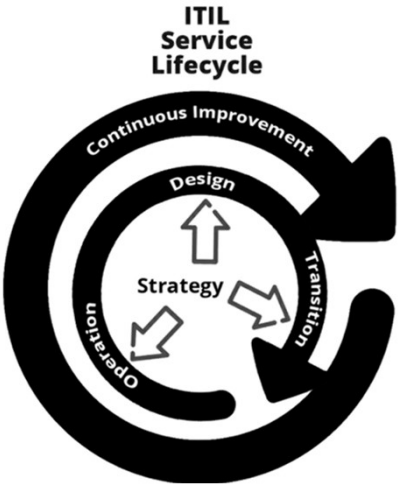
- **Control Objectives for Information and Related Technology (COBIT):** Isaca framework (www.isaca.org)
- **Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT)** www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf
- **Federal Risk and Authorization Management Program (FEDRAMP):** https://marketplace.fedramp.gov/#!/products
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** www.priv.gc.ca/biens-assets/compliance-framework/en/index
- **Payment Card Industry — Data Security Standard (PCI–DSS):** https://cio-wiki.org/wiki/Payment_Card_Industry_Data_Security_Standard_(PCI_DSS).
- **The Gramm-Leach-Bliley Act (GLBA)**
- **Security Controls Framework (SCF)**
- **DFARS 252.204-7012/ NIST 800-171**
- **Sherwood Applied Business Security Architecture, or SABSA:** https://sabsa.org 기업의 목표 달성을 위한 요구 사항과 균형을 맞추면서 정보 보안을 달성하기 위한 프레임워크 및 방법론이며, COBIT만큼 산업 중립적이지는 않지만 은행, 원자력 발전, 정부, 정보 통신 회사 등 보안 목표가 중요한 조직에서 사용하고 있다.

Source: Guide to Cloud Security Concepts (Gartner, September 2021)

III. 클라우드 보안 솔루션과 비즈니스

❖ **Security Frameworks (2 of 2)**

- **ISO/IEC 27000 Series: www.cisecurity.org/controls**
- **CIS Benchmarks: https://learn.cisecurity.org/benchmarks.**
- **ISO/IEC 15048, more commonly known as the Common Criteria: https://commoncriteriaportal.org/index.cfm?**
- **FDA regulations on electronic records and signatures: The particular regulation, 21 CFR Part II (often just called Part II)**
- **The Information Technology Infrastructure Library (ITIL)**



Source: Coombs, Ted. Cloud Security For Dummies (p. 297). Wiley. Kindle Edition.

III. 클라우드 보안 솔루션과 비즈니스

❖ **Enterprise Security Architecture - SABSA**

- **SABSA는 비즈니스 목표를 추적 가능하게 지원하는 엔터프라이즈 및 솔루션 수준에서 비즈니스 중심의 위험 및 기회 중심 보안 아키텍처를 개발하기 위한 입증된 방법론**
- **SABSA는 기업의 요구 사항을 완벽하게 충족하고 보안 서비스가 비즈니스 및 IT 관리 인프라의 필수적인 부분으로 설계, 제공 및 지원되도록 보장 (저작권이 보호되지만 SABSA는 상용 제품이 아닌 공개 사용 방법론)**
- **SABSA는 독립적으로 사용되거나 전체적인 통합 엔터프라이즈 솔루션으로 사용되는 일련의 통합 프레임워크, 모델, 방법 및 프로세스로 구성되며 다음을 포함:**
  - Business Requirements Engineering Framework (known as Attributes Profiling)
  - Risk and Opportunity Management Framework
  - Policy Architecture Framework
  - Security Services-Oriented Architecture Framework
  - Governance Framework
  - Security Domain Framework
  - Through-life Security Service Management & Performance Management Framework

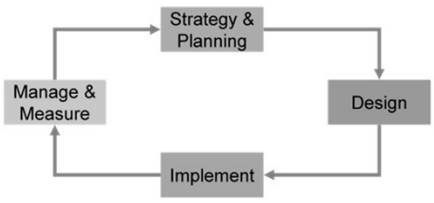
Source: https://sabsa.org/sabsa-executive-summary/, "Sherwood Applied Business Security Architecture(SABSA)" as it was first developed by John Sherwood.

III. 클라우드 보안 솔루션과 비즈니스

❖ **Enterprise Security Architecture - SABSA**

SABSA Key Features, Advantages & Benefits Summary

Business View	Contextual Architecture
Architect's View	Conceptual Architecture
Designer's View	Logical Architecture
Builder's View	Physical Architecture
Tradesman's View	Component Architecture
Manager's View	Management Architecture

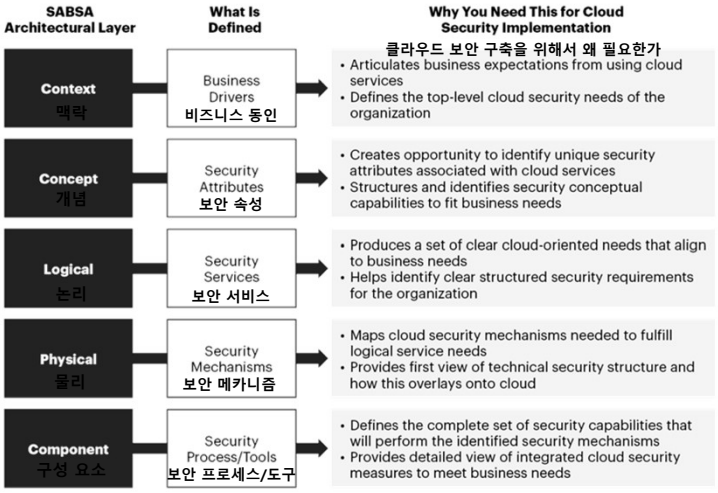


Feature	Advantage	Benefits							
		Chairman & Board	CEO	CFO	COO	CRO	CIO	CISO	CTO & Architects
비즈니스 중심 Business Driven	Value – assured	Protects shareholder value	Protects corporate reputation	Ensures efficient return on investment	Focuses on performance management	Enables flexible fit with industry regulations	Enables a digital information-age business	Facilitates alignment of security strategy with business goals	Leverages the full power of information technology
위험 중심 Risk focused	Prioritized & proportional responses	Optimizes shareholder risk & aligns with risk appetite	Meet corporate governance requirements	Improves predictability & consistency	Enables process improvement	Supports enterprise risk management	Identifies information exploitation opportunities	Facilitates prioritization of security & risk – control solutions	Manages information system risk
포괄적인 Comprehensive	Scalable scope	Addresses all shareholder concerns	Meets enterprise wide requirements	Supports scalable, granular budgeting	Provides end-to-end process coverage	Enables a fully integrated risk control strategy	Sustains through-life information architecture	Ensures all business concerns regarding security & control are addressed	Applies at any level of project size or complexity
모듈식 Modular	Agility for ease of implementation & management	Ensures flexibility to meet dynamic market & economic conditions	Enables fast time to market with business solutions	Facilitates effective management of both development & operational costs	Integrates with legacy environments	Enables incrementally increasing maturity	Enables technology neutral information management strategies	Enables a project-focused approach to security & control development	Provides a holistic architectural approach
오픈소스 Open Source *	Free use, open source, global standard	Guarantees 'escrow' & perpetuity of return on investment	Provides assurance through industry standard	Eliminates expensive on-going license fees	Simplifies recruitment & training	Provides global acceptability for auditors & regulatory supervisors	Provides a future-proof strategic framework for information management	Provides a sustainable framework for integration of other security standards	Avoids vendor dependence & lock-in
감사 가능 Auditable	Demonstrates compliance to relevant authorities	Demonstrates compliance to regulators & external auditors	Ensures a smooth & successful external & regulatory audit process	Minimizes cost of management time dealing with audit processes	Minimizes adverse effect of audits on performance targets	Ensures that compliance risk is effectively managed	Facilitates smooth & successful internal audits of information systems & processes	Supports security & risk review processes	Improves relationship & interactions with auditors & security reviewers
투명한 Transparent	Two-way traceability	Supports market transparency & disclosure	Provides a clear view of where expenditure is made & what value is returned	Enables full audit ability for effectiveness of expenditure	Measures efficiency & effectiveness of processes & resource deployment	Demonstrates 'current state' and 'desired state' of compliance levels	Encourages fully integrated people – process – technology solutions	Provides traceability of implementation of business-aligned security requirements	Verifies justification & completeness of technical solutions.

Source: https://sabsa.org/sabsa-executive-summary/, "Sherwood Applied Business Security Architecture(SABSA)" as it was first developed by John Sherwood.

III. 클라우드 보안 솔루션과 비즈니스

❖ **SABSA 보안 아키텍처 계층과 클라우드 보안을 위한 가치**



Source: Gartner

III. 클라우드 보안 솔루션과 비즈니스

❖ **SABSA 보안 아키텍처 계층과 클라우드 보안을 위한 가치**

SABSA Layer	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual (맥락)	Business goals and decisions	Business risks	Business meta-processes	Business governance	Business geography	Business time dependence
Conceptual (개념적)	Business value and knowledge strategy	Risk management strategy and objectives	Strategies for process assurance	Security and risk governance; trust framework	Domain framework	Time management framework
Logical (논리적)	Information assets	Risk management policies	Process maps and services	Trust relationships	Domain maps	Calendar and timetable
Physical (물리적)	Data assets	Risk management practices	Process mechanisms	Human interface	Infrastructure	Processing schedule
Component (구성요소)	Component assets	Risk management components and standards	Process components and standards	Human entities: components and standards	Locator components and standards	Step timing and sequencing components and standards
Management (관리)	Delivery and continuity management	Operational risk management	Process delivery management	Governance, relationship and personal management	Environment management	Time and performance management

Source: Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures

III. 클라우드 보안 솔루션과 비즈니스

❖ 10 Top Cloud Security Companies in 2023

1. Fidelis: Best for DevSecOps
2. Skyhigh: Best Security Service Edge
3. Lacework: Best CNAP Platform
4. Qualys: Best for Compliance
5. Palo Alto: Best for Cloud Workload Protection
6. Symantec: Best for CASB
7. Tenable: Best for Vulnerability Management
8. Trend Micro: Best for Hybrid Cloud Security
9. Netskope: Best Overall Cloud Security
10. Zscaler: Best for Advanced Threat Protection

11. Methodology and cloud security buying considerations

Source: https://www.esecurityplanet.com/products/cloud-security-companies/

III. 클라우드 보안 솔루션과 비즈니스

❖ Cloud Security Best Practices

- Understand Your Shared Responsibility Model
- Ask Your Cloud Provider Detailed Security Questions
- Deploy an Identity and Access Management Solution
- Train Your Staff
- Establish and Enforce Cloud Security Policies
- Encrypt Data in Motion and At Rest
- Use Intrusion Detection and Prevention Technology
- Double-Check Your Compliance Requirements
- Consider a CASB or Cloud Security Solution
- Conduct Audits, Pentesting and Vulnerability Testing
- Enable Security Logs
- Understand and Mitigate Misconfigurations

- 공유 책임 모델 이해
- 클라우드 제공업체에 자세한 보안 질문하기
- ID 및 액세스 관리 솔루션 배포
- 직원 교육
- 클라우드 보안 정책 수립 및 시행
- 이동 중 및 미사용 데이터 암호화
- 침입 탐지 및 방지 기술 사용
- 규정 준수 요건 재확인
- CASB 또는 클라우드 보안 솔루션 고려
- 감사, 펜테스팅 및 취약성 테스트 수행
- 보안 로그 사용
- 잘못된 구성 이해 및 완화

Source: https://www.esecurityplanet.com/cloud/cloud-security-best-practices/

III. 클라우드 보안 솔루션과 비즈니스

❖ Top 10 Cloud Security Companies (2023)

1. Astra Security
2. Palo Alto Networks
3. Qualys
4. Symantec
5. Intruder
6. LookOut
7. Sophos
8. Detectify
9. Probely
10. Lacework

Source: https://www.fortunebusinessinsights.com/cloud-security-market-102427

III. 클라우드 보안 솔루션과 비즈니스

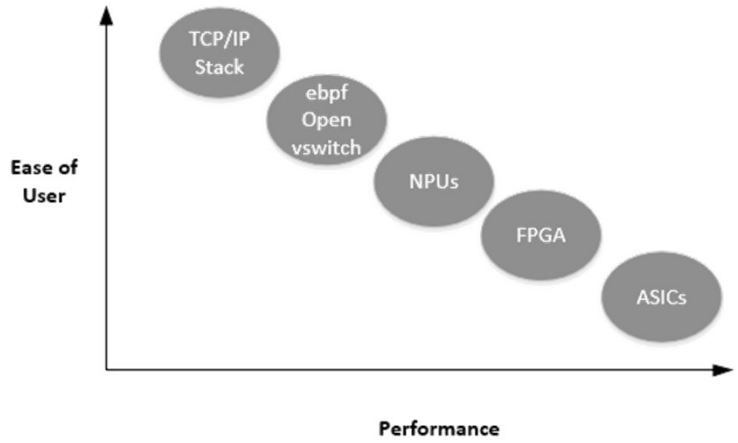
❖ The 20 Coolest Cloud Security Companies Of The 2023 Cloud 100s

1. Aqua Security
2. Check Point Software Technologies
3. Ermetic
4. Fortinet
5. Illumio
6. Imperva
7. Lacework
8. Laminar
9. Netskope
10. Orca Security
11. Palo Alto Networks
12. Proofpoint
13. Qualys
14. Securonix
15. Semperis
16. Skyhigh Security
17. Sophos
18. Trellix
19. Trend Micro
20. Zscaler

Source: https://www.crn.com/news/security/the-20-coolest-cloud-security-companies-of-the-2023-cloud-100/1

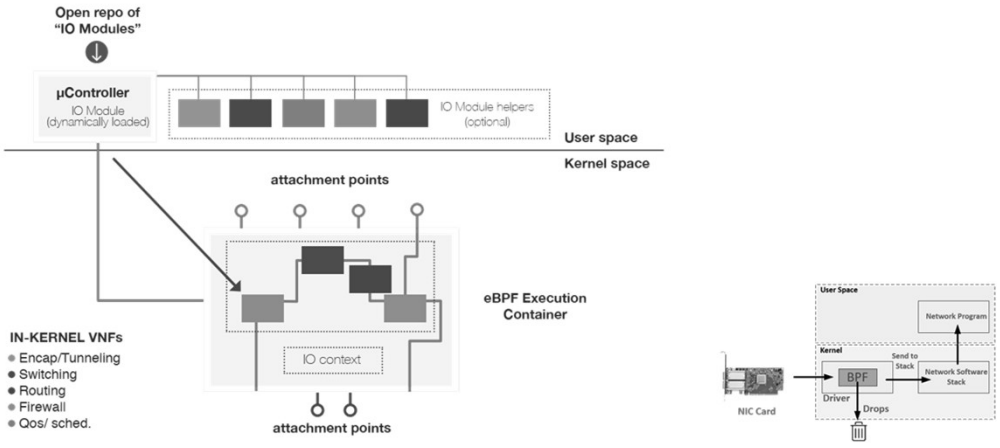
III. 클라우드 보안 솔루션과 비즈니스

❖ 클라우드 네트워킹/보안을 위한 상능 강화 플랫폼 변화

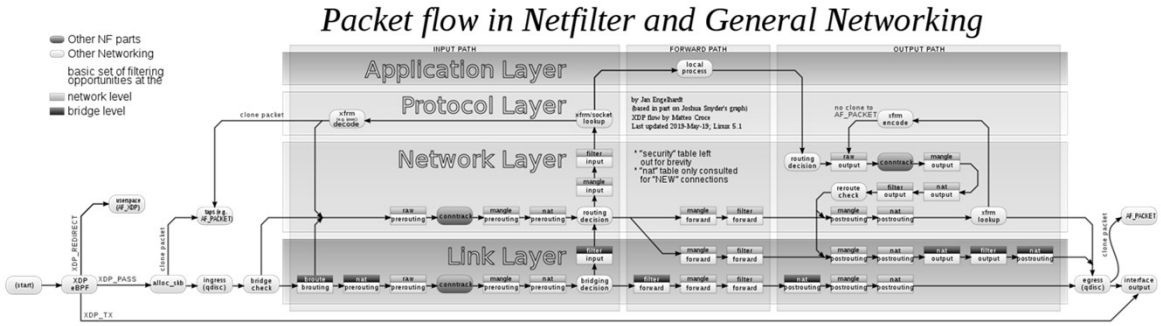


III. 클라우드 보안 솔루션과 비즈니스

❖ **eBPF Framework for Networking**
(by IO Visor, retrieved from iovisor.org)



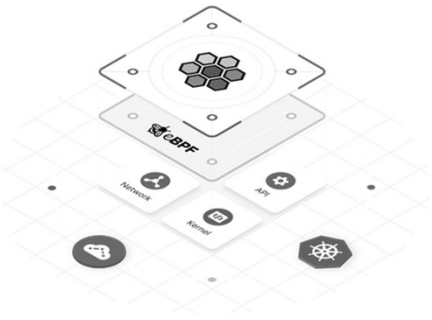
❖ **Offload Layers by eBPF**

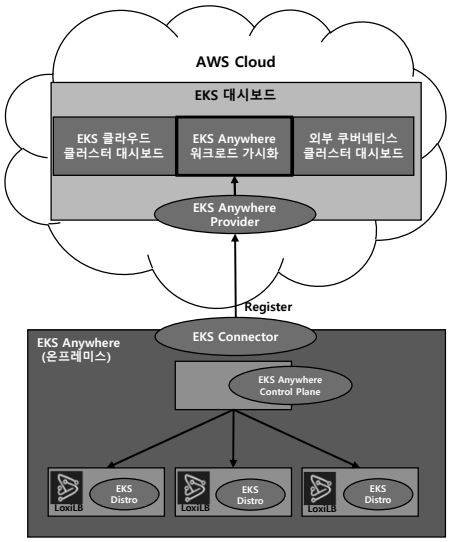


Source: https://medium.com/simplestaking/integrating-an-ebpf-based-firewall-into-the-tezedge-node-with-multipass-validations-769d4c6ccd93

❖ **eBPF 사용 (예): AWS EKS Anywhere**

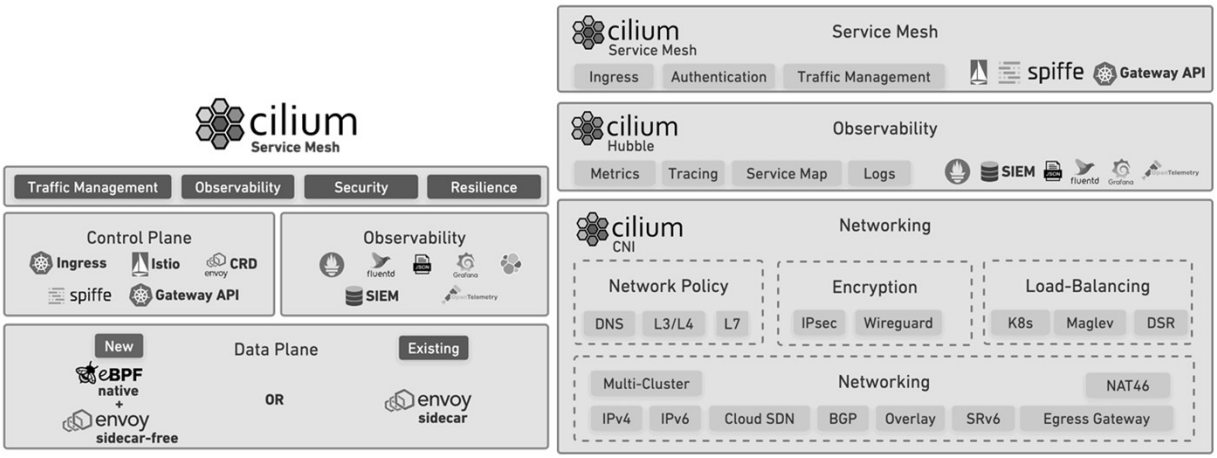
- **Cilium (eBPF)**
- **MetalLB or LoxiLB (eBPF)**





Source: https://cilium.io/

❖ eBPF 사용 (예): Cilium 1.12 Major Features



Source: https://www.cncf.io/blog/2022/07/20/cilium-1-12-ga-cilium-service-mesh-and-other-major-new-features-for-enterprise-kubernetes/

❖ eBPF 사용 (예): Calico Project

- Calico's eBPF dataplane

Factor	Standard Linux Dataplane	eBPF dataplane
Throughput	Designed for 10GBit+	Designed for 40GBit+
First packet latency	Low (kube-proxy service latency is bigger factor)	Lower
Subsequent packet latency	Low	Lower
Preserves source IP within cluster	Yes	Yes
Preserves external source IP	Only with externalTrafficPolicy: Local	Yes
Direct Server Return	Not supported	Supported (requires compatible underlying network)
Connection tracking	Linux kernel's conntrack table (size can be adjusted)	BPF map (fixed size)
Policy rules	Mapped to iptables rules	Mapped to BPF instructions
Policy selectors	Mapped to IP sets	Mapped to BPF maps
Kubernetes services	kube-proxy iptables or IPVS mode	BPF program and maps
IPIP	Supported	Supported (no performance advantage due to kernel limitations)
VXLAN	Supported	Supported
Wireguard	Supported (IPv4 and IPv6)	Supported (IPv4)
Other routing	Supported	Supported
Supports third party CNI plugins	Yes (compatible plugins only)	Yes (compatible plugins only)
Compatible with other iptables rules	Yes (can write rules above or below other rules)	Partial; iptables bypassed for workload traffic
Host endpoint policy	Supported	Supported
Enterprise version	Available	Available
XDP DoS Protection	Supported	Supported
IPv6	Supported	Not supported (yet)

Source: https://projectcalico.docs.tigera.io/maintenance/ebpf/enabling-ebpf

III. 클라우드 보안 솔루션과 비즈니스

❖ NSX Distributed Firewall & IDS/IPS is running on the NVIDIA DPU (vSphere 8)

- Acceleration Next Generation Firwalls
- Hardware-Accelerated Intrinsic Security and the Cloud Servers

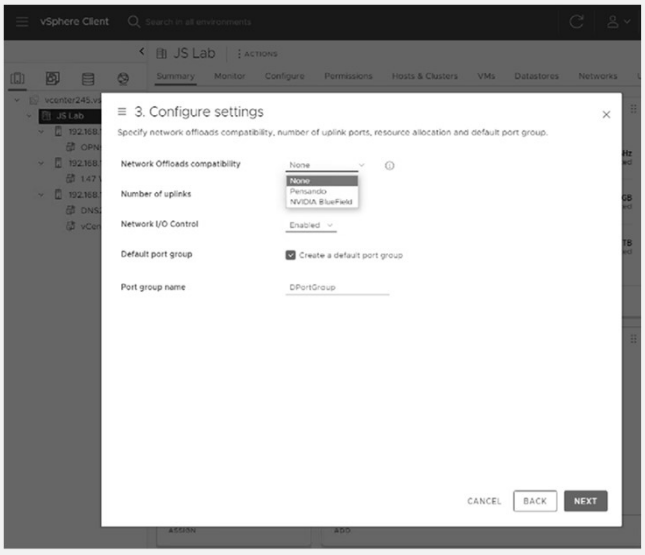
NVIDIA Accelerated Switching and Packet Processing (ASAP2) with Deep-Packet-Inspection technology enables seamless offload of packet filtering, steering, crypto, stateful connection tracking and L4-L7 inspection to the DPU Hardware

Source: https://www.storagereview.com/news/dell-poweredge-servers-with-nvidia-dpus-gpus-and-vmware-vsphere-8-announced

III. 클라우드 보안 솔루션과 비즈니스

❖ vSphere 8, vDS and NSX will allow using DPU Network Offloading

- vSphere 버전 8.0의 Distributed Switch 및 NSX를 사용하면 네트워크 서비스가 DPU로 오프로드되므로 x86 CPU 오버헤드 없이 네트워크 성능을 향상할 수 있다.



III. 클라우드 보안 솔루션과 비즈니스

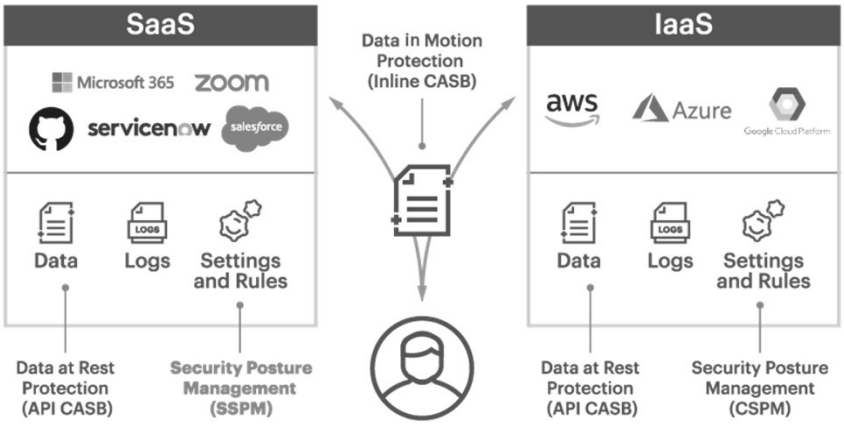
❖ **How to deploy and manage SASE?:** 기업이 효과적인 SASE 솔루션을 구축하기 위해 취할 수 있는 두 가지 방향이 있다.

- **단일 공급업체 접근 방식:** WAN 엣지 인프라와 SSE 솔루션을 결합한 단일 공급업체 제품을 평가하고 참여합니다. 이 접근 방식은 운영을 간소화하여 조직의 SASE 요구 사항을 충족할 수 있지만, SSE 공급업체만이 제공할 수 있는 고급 보안 기능을 포기해야 할 수도 있다. 장기적으로 고급 보안 기능의 부족을 메우기 위해 보안 공급업체 솔루션을 추가로 구입해야 하는 경우 비용이 더 많이 들 수 있다.
- **두 공급업체 접근 방식:** 동급 최강의 WAN 엣지 인프라 솔루션과 통합 제품 내에서 CASB, SWG, ZTNA, RBI, FWaaS 구성 요소를 융합하는 SSE 보안 솔루션을 제공하는 두 공급업체 솔루션을 평가하고 참여한다. 이 두 공급업체 접근 방식은 장기적으로 시스템 배포, 관리, 유지보수를 간소화하고 효율화한다.

Source: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/what-is-sse.html

III. 클라우드 보안 솔루션과 비즈니스

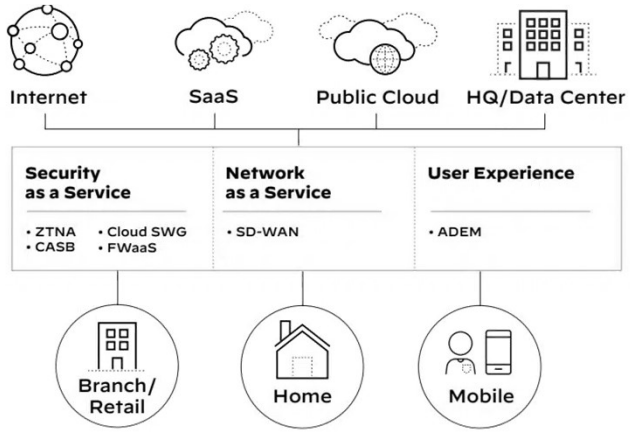
❖ **Netskope: Detects overly permissive settings**



Source: https://www.netskope.com/security-defined/what-is-sspm#:~:text=On%20a%20simpler%20note%2C%20think,policies%20and%2For%20regulatory%20standards.

III. 클라우드 보안 솔루션과 비즈니스

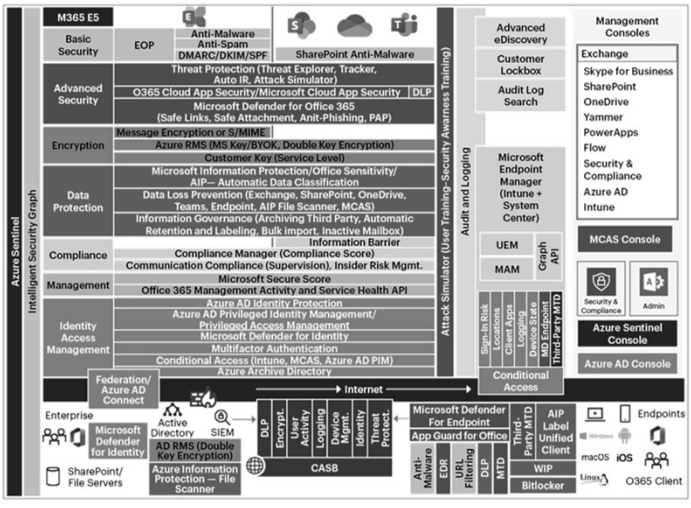
❖ Palo Alto Networks Prisma Access architecture



Source: https://www.comparitech.com/net-admin/best-zero-trust-security-vendors/

III. 클라우드 보안 솔루션과 비즈니스

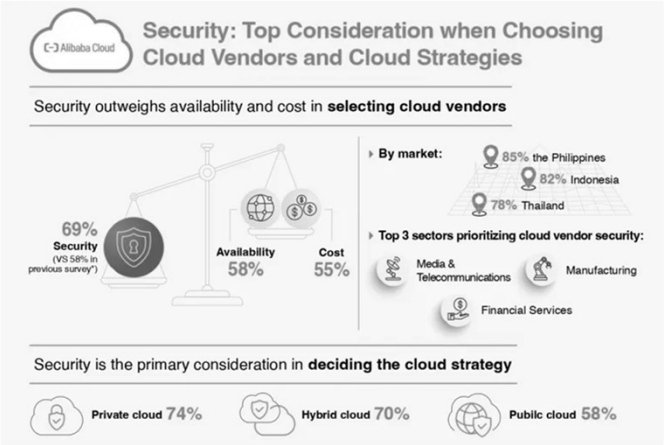
❖ Microsoft 365 Native Security Tools



Source: Gartner

III. 클라우드 보안 솔루션과 비즈니스

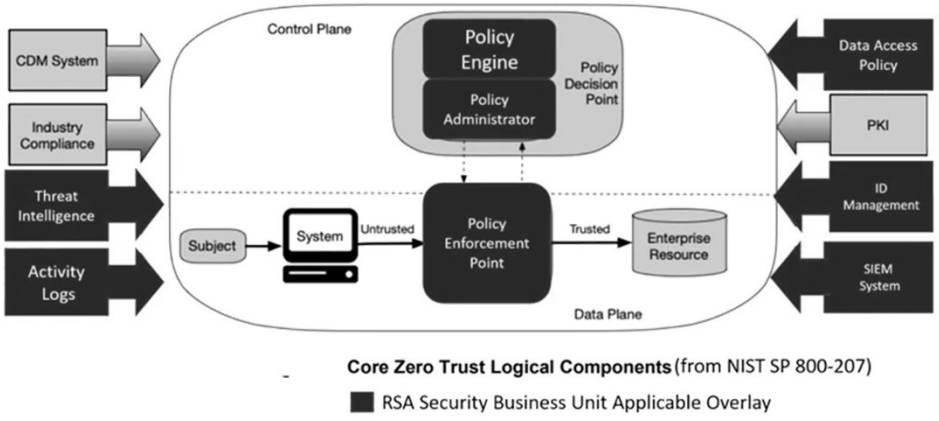
❖ 알리바바: 'CSP 선택의 가장 큰 결정 요인으로 가용성 및 비용보다 보안이 더 중요한 이유'



Source: https://www.press.in.th/cloud-vendor-selection/

III. 클라우드 보안 솔루션과 비즈니스

❖ RSA Security Business Unit Applicable Overlay



Core Zero Trust Logical Components (from NIST SP 800-207)

RSA Security Business Unit Applicable Overlay

Source: https://www.rsa.com/zero-trust/what-is-zero-trust/

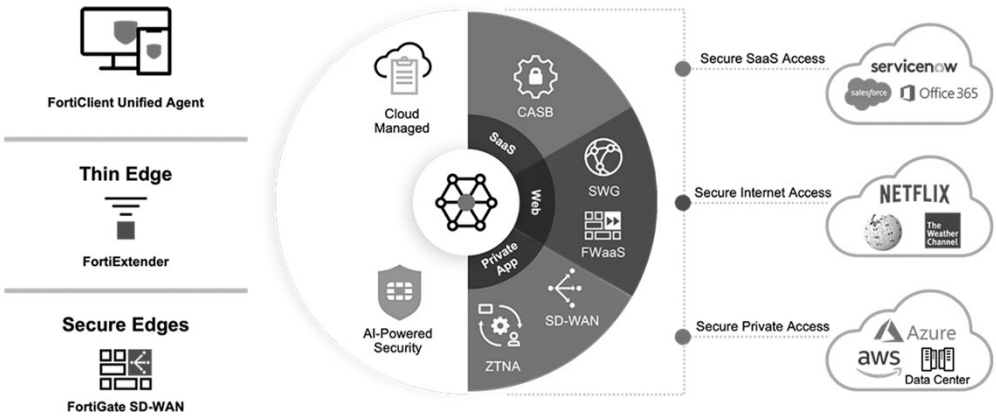
III. 클라우드 보안 솔루션과 비즈니스

❖ 포티넷: Fortinet SASE

Cloud Access Security Broker (CASB), Zero-Trust Network Access (ZTNA), Secure Web Gateway (SWG)
Source: Modified, Fortinet SASE

III. 클라우드 보안 솔루션과 비즈니스

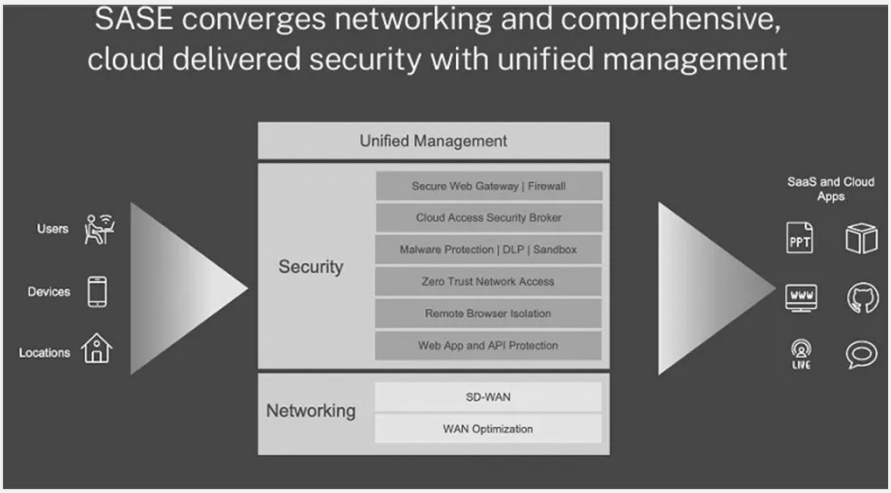
❖ 포티넷: Cloud-Delivered Enterprise-Grade Security Everywhere (FortiSASE)



Source: https://www.fortinet.com/products/sase

III. 클라우드 보안 솔루션과 비즈니스

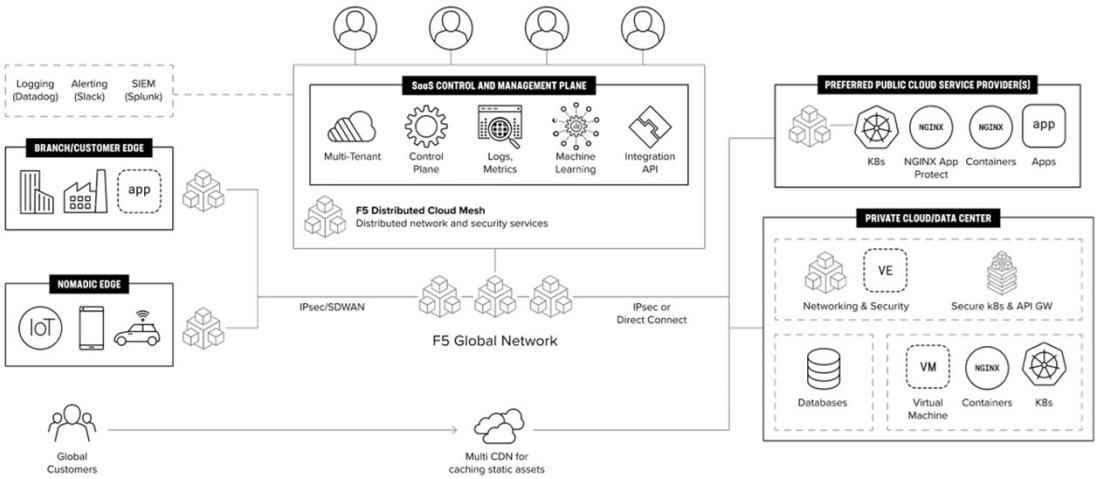
❖ **Citrix SASE**



Source: Citrix SASE

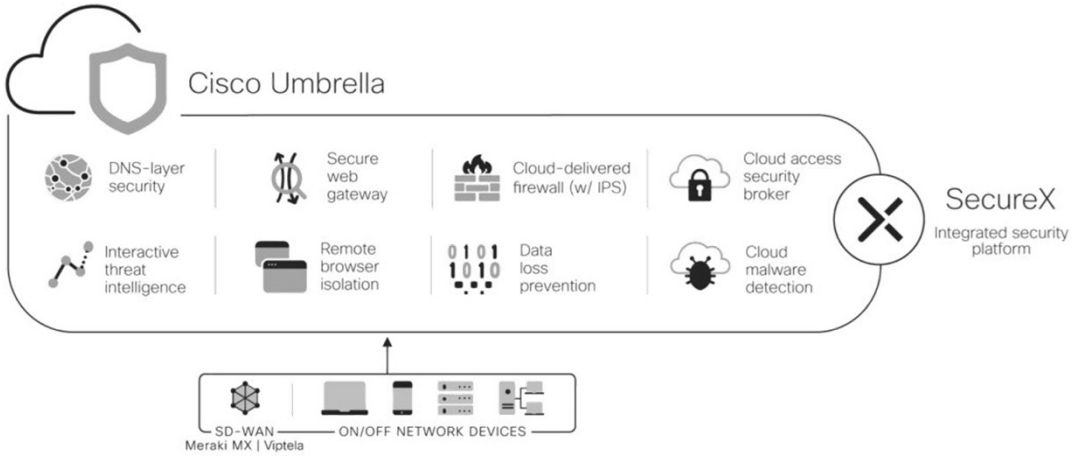
III. 클라우드 보안 솔루션과 비즈니스

❖ **F5: 멀티 클라우드 네트워킹 서비스 인프라 플랫폼 구축 (SaaS)**



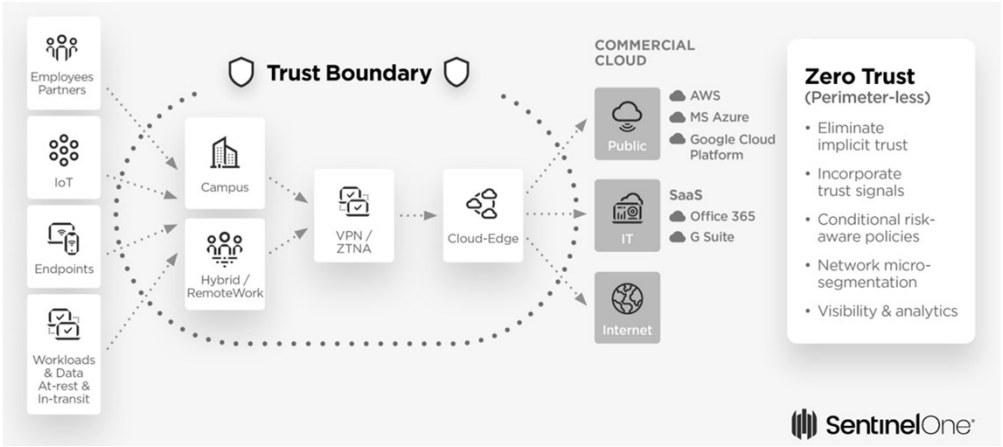
Source: https://www.f5.com/solutions/use-cases/multi-cloud-networking

❖ **Cisco Security Cloud Designed to be Industry's Most Open Platform** (Cisco)



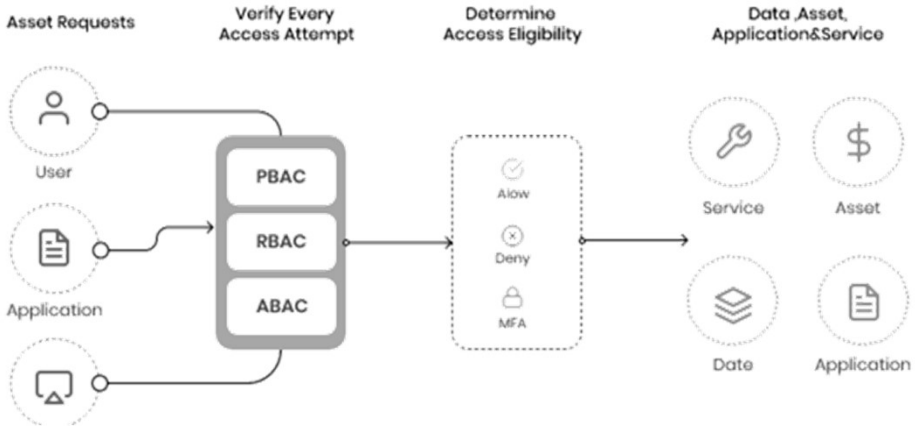
Source: https://www.storagereview.com/news/cisco-security-cloud-designed-to-be-industrys-most-open-platform

❖ **Sentinelone: Zero – Trust Security**



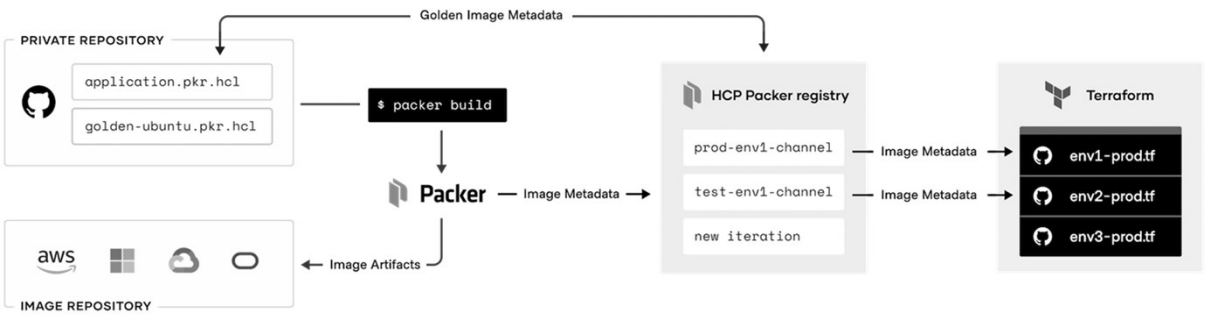
Source: https://www.sentinelone.com/cybersecurity-101/zero-trust-architecture/

❖ **Corsha: Zero – Trust Architecture**



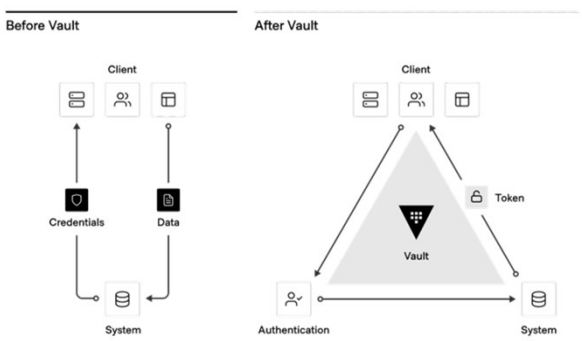
Source: https://corsha.com/nist-800-207-zero-trust-architecture

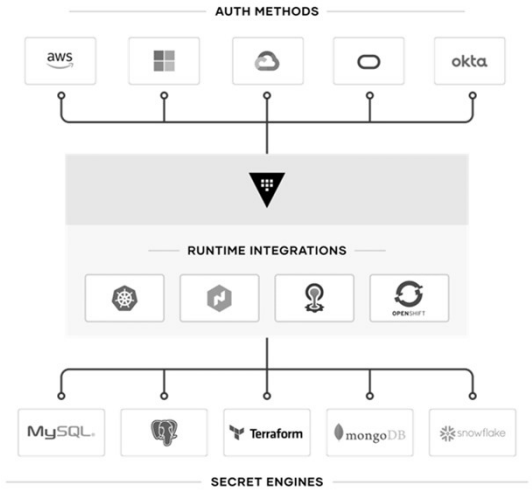
❖ **Build Automated Images with HashiCorp Packer** (HashiCorp)



Source: https://www.hashicorp.com/cloud-operating-model

❖ **Manage Secrets and Protect Data with HashiCorp Vault** (HashiCorp)

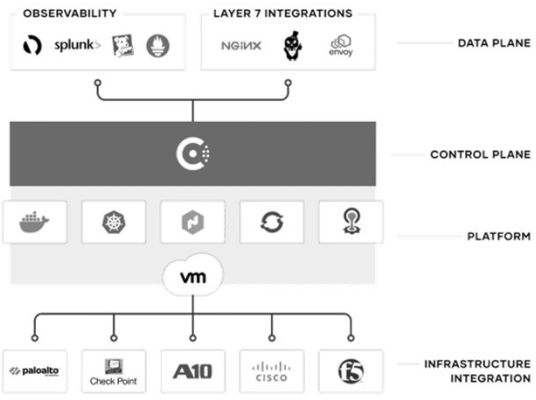




Source: https://www.hashicorp.com/cloud-operating-model

❖ **Zero Trust Networking with Service Mesh and API Gateway** (HashiCorp)

- **Consul은 서비스 네트워킹을 위한 광범위한 에코시스템을 지원하는 단일 컨트롤 플레인을 제공.**



Source: https://www.hashicorp.com/cloud-operating-model

❖ HashiCorp(해시코프) 볼트(Vault) 및 쿠버네티스 통합을 위한 지원 방법 비교

- Sidecar
- CSI
- Vault

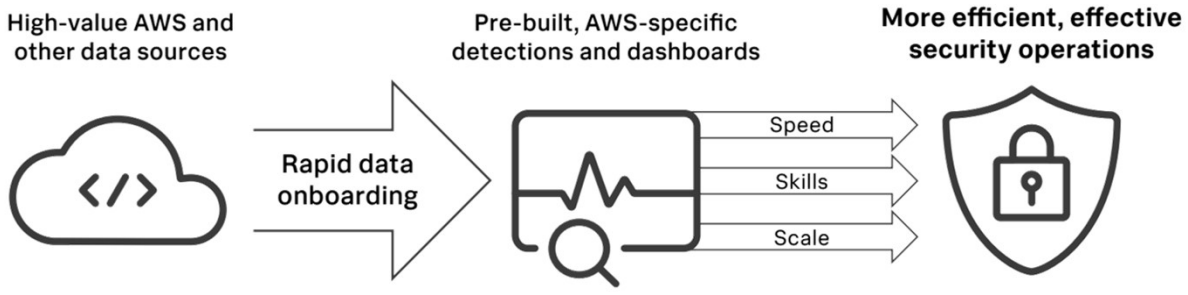
	Sidecar	CSI	Vault Operator
Secret projection	Shared Memory Volume Environment Variable*	Ephemeral Disk Environment Variables Kubernetes Secrets	Kubernetes Secrets, Kubernetes Secret Volumes, Environment Variables
Secret scope	Global	Global	Global
Secret types	All Vault Secret Engines (Static & Dynamic)	All Vault Secret Engines (Static & Dynamic)	All Vault Secret Engines (Static & Dynamic)
Secret templating	✓	×	Not for Beta, more than likely for GA
Secret size limit	Vault w/Consul Backend: 512 KB (Default) No Limit Vault w/ Integrated Storage Backend: 1 MiB (Default) No Limit	Vault w/Consul Backend: 512 KB (Default) No Limit Vault w/ Integrated Storage Backend: 1 MiB (Default) No Limit	Vault w/Consul Backend: 512 KB (Default) No Limit Vault w/ Integrated Storage Backend: 1 MiB (Default) No Limit
Secret definitions	Vault CLI / API /UI	Vault CLI / API /UI	Vault CLI / API
Encryption	Yes (at rest and in-transit)	Yes (at rest and in-transit)	In transit via TLS, at-rest ** only if 'etcd' storage is encrypted.

	Sidecar	CSI	Vault Operator
Secret rotation	✓	×	✓
Secret caching	✓	×	✓
Auditability	✓	✓	✓
Deployment method	1 Shared K8s Cluster Service + 1 Sidecar Container	Daemonset	Kubernetes Deployment
Vault agent support	✓	×	×
Helm support	✓	✓	✓
Customer Support	×	×	✓
Kubernetes Secrets drift detection and automation remediation	×	×	✓

Source: Carter, Daniel (2022-11-24T22:58:59.000). CCSP Certified Cloud Security Professional All-in-One Exam Guide, Third Edition . McGraw Hill LLC. Kindle Edition.

❖ Splunk Security Analytics for AWS

- 몇 주 이상 걸리지 않고 구독 후 몇 시간 내에 인사이트를 얻을 수 있다.
- IAM, 네트워크 및 기타 보안 데이터에 대해 사전 구축된 AWS 전용 대시보드 및 탐색.
- Splunk의 위협 연구 팀이 만든 도구와 가이드를 통해 동적 조사 기능을 제공

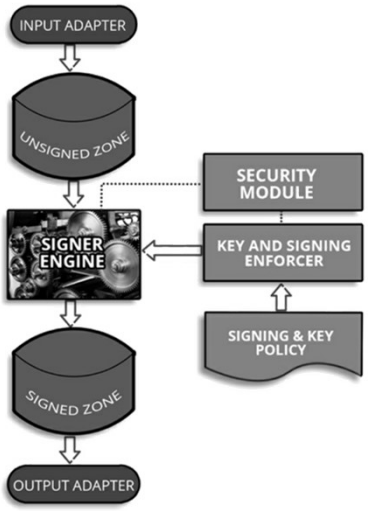


Source: https://www.splunk.com/en_us/pdfs/resources/product-brief/Splunk-Splunk-Security-Analytics-for-AWS-PB-106-web.pdf

III. 클라우드 보안 솔루션과 비즈니스

❖ **OpenDNSSEC(www.opendnssec.org):**

- DNSSEC 키와 영역 서명을 유지 관리하는 오픈 소스 애플리케이션
- 데이터 출처 인증: 여기에는 정보가 실제로 권한이 부여된 영역에서 온 것인지 확인하는 작업이 포함됩니다. 인증에 실패하면 확인자는 공격이 있는 것으로 간주하고 시도를 무시
- 데이터 무결성 보호: 여기에는 데이터가 도중에 변경되지 않았는지 확인하는 것이 포함됩니다. 이는 데이터가 서명되어 있고 키를 사용하여 확인할 수 있기 때문에 가능
- 애플리케이션은 서명되지 않은 영역을 가져와 필요한 디지털 서명 및 기타 DNSSEC 레코드를 추가하는 방식으로 작동함
- 이 정보가 영역에 추가되면 해당 영역을 관리하는 권한 있는 네임 서버로 전송함



Source: Coombs, Ted. Cloud Security For Dummies (p. 257). Wiley. Kindle Edition.

III. 클라우드 보안 솔루션과 비즈니스

❖ **HSM(Hardware Security Modules) 제품 평가:**

- HSM을 선택할 때는 어떤 클라우드 서비스 제공업체를 사용하든 상관없이 제대로 작동하는지 확인해야 한다.
- 안전하고 빠르며 확장 가능한 HSM을 찾는다
- 시장이 제한되어 있기 때문에 선택할 수 있는 HSM 공급업체가 몇 개 밖에 없다. 다음은 가장 잘 알려진 업체들이다:
  - nShield: www.entrust.com/digital-security/hsm/products/nshield-hsms/nshield-connect
  - Thales Group: https://cpl.thalesgroup.com/encryption/hardware-security-modules
  - PKI Solutions: www.pkisolutions.com

❖ **클라우드 HSM 사용의 몇 가지 이점:**

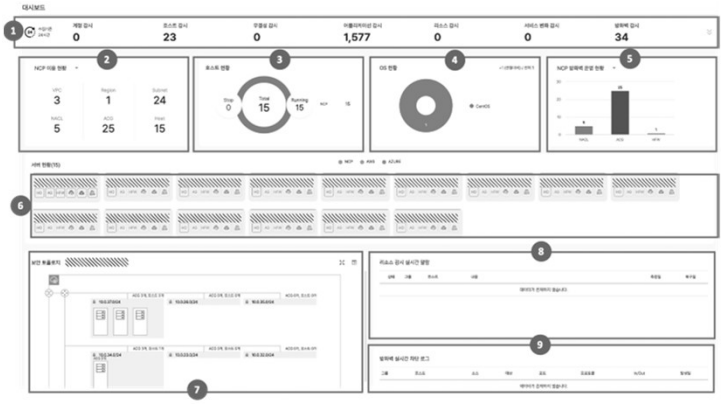
- **Increased security**
- **Scalability**
- **Reduced management requirements**
- **The reassurance that comes from not having your device in a vulnerable building**

Source: Coombs, Ted. Cloud Security For Dummies (p. 258). Wiley. Kindle Edition.

❖ 네이버클라우드: 클라우드 보안 형상관리 서비스 'Cloud Security Watcher'

- 네이티브 클라우드 보안 형상관리 서비스 (Cloud Security Posture Management, CSPM)
- 자산 가시성 확보, 보안 규정 준수 평가, 위협 교정 지원, 멀티 클라우드 통합 관리

영역	설명
① 24시간 변동 현황 모니터링	대시보드 상단에 배치된 메뉴
② 이용 현황	사용 중인 클라우드 서비스에서 그룹, 클라우드, 리전 정보, VPC/VNet, 서브넷 등 이용 현황
③ 호스트 현황	사용 중인 클라우드 서비스의 전체 호스트 현황
④ OS 현황	사용 중인 클라우드 서비스에 설치된 OS 현황
⑤ 방화벽 운영 현황	사용 중인 클라우드 서비스의 전체 방화벽 운영 현황
⑥ 서버 현황	클라우드 서비스 내 등록된 서버 현황
⑦ 보안 토폴로지	호스트의 네트워크별 정보를 기반으로 생성된 토폴로지
⑧ 리소스 감시 실시간 알람	클라우드 서비스 내 등록된 호스트들에 대한 정책 설정 시 지정한 임계치별 호스트 상태의 위험, 주의가 발생된 내역
⑨ 방화벽 실시간 차단 로그	클라우드 서비스 내 등록된 호스트들의 방화벽 차단에 발생한 최근 알람 리스트



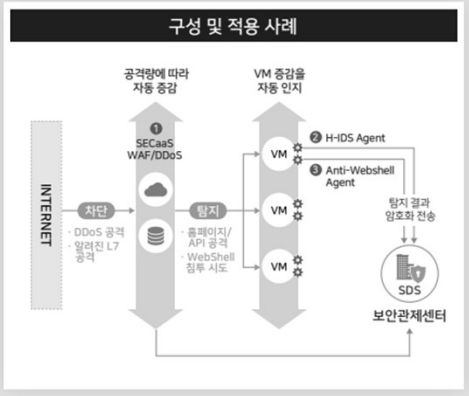
Source: https://guide.ncloud-docs.com/beta/docs/csw-use

❖ 삼성SDS: 클라우드 보안관제 서비스

클라우드 보안서비스 Use Case

클라우드 보안관제

보안관제 대상이 상시 변경되는
동적인 클라우드 특성을 감안한
보안관제 서비스



제공 사항

❶ SECaaS WAF/DDoS
- DDoS, L7 공격이 고객의 VM에 도달하기 이전에 사전 차단
- 공격량에 따라 SECaaS 규모가 자동 증감

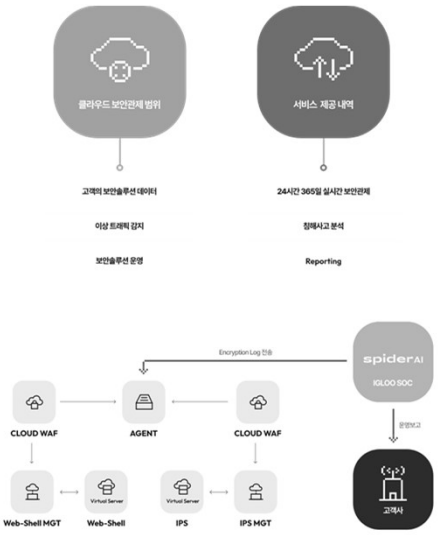
❷ Host-based IDS (Agent 포함)
- 홈페이지/API 대상 공격을 탐지하고 탐지 결과를 SECaaS에 반영하여 차단

❸ Anti-Webshell (Agent 포함)
- Web shell (해킹도구)의 업로드 시도를 탐지 및 검역

Source: https://www.samsungsds.com/kr/cloud-security/cloud-security.html

III. 클라우드 보안 솔루션과 비즈니스

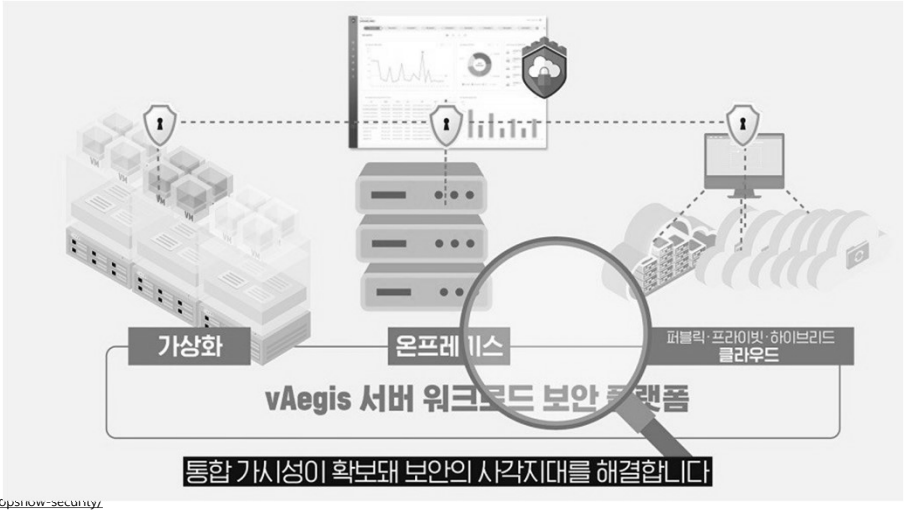
❖ 이글루: 클라우드 보안관제 서비스



Source: https://www.igloo.co.kr/service/cloud-security/

III. 클라우드 보안 솔루션과 비즈니스

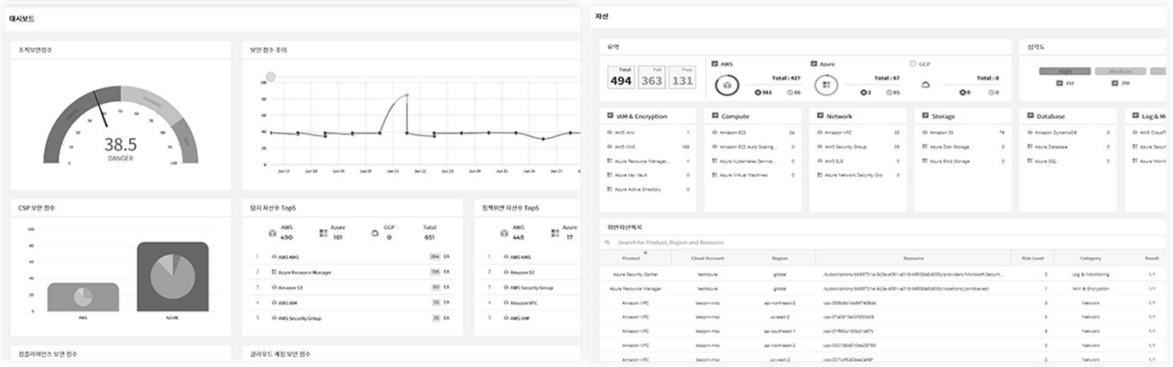
❖ SGA 솔루션즈: 클라우드 워크로드 프로텍션 플랫폼(CWPP) SGA솔루션즈 'vAegis'



Source: https://www.opsnow.com/products/opsnow-security/

III. 클라우드 보안 솔루션과 비즈니스

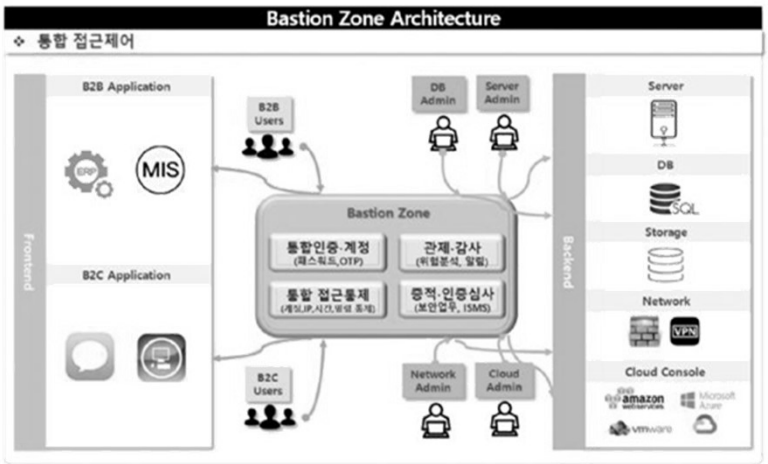
❖ OpsNow Security (SaaS): 클라우드 보안 형상 관리, 멀티 클라우드 환경 지원, 보안 담당자 특화 솔루션, 클라우드 보안 정책 가이드, 국내·외 컴플라이언스 지원



Source: https://www.opsnow.com/products/opsnow-security/

III. 클라우드 보안 솔루션과 비즈니스

❖ 메가존: Hybrid-Multi Cloud를 위한 배스천 존 아키텍처 (통합 접근 제어)

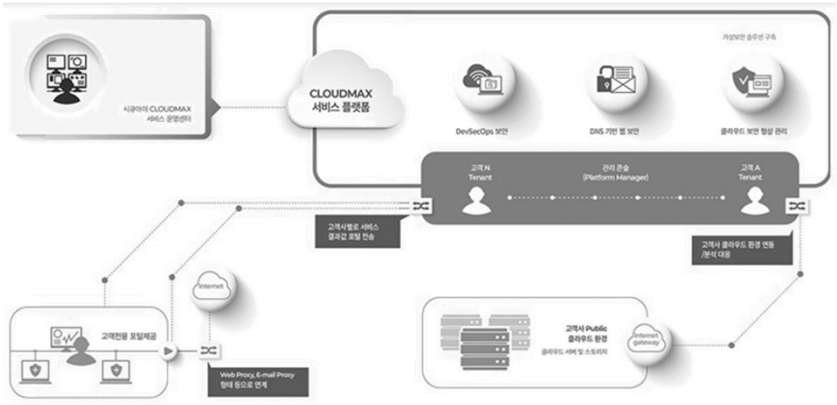


Source: https://www.opsnow.com/products/opsnow-security/

III. 클라우드 보안 솔루션과 비즈니스

❖ 시큐아이: 플랫폼 기반 '클라우드맥스' 클라우드 보안

- 데브섹옵스(DevSecOps) 보안
- DNS 기반 웹보안
- 워크 로드 보안
- 클라우드 보안 형상 관리



Source: https://www.kcloudnews.co.kr/news/articleView.html?idxno=775

191

III. 클라우드 보안 솔루션과 비즈니스

❖ 진앤현시큐리티: 클라우드(Cloud) 보안 및 ZTNA 보안솔루션

SECUCALL

Security Solution Integration&Operation

네트워크보안 통합구축

- 구축형 보안제품 판매
  - 국산보안제품
  - 외산보안제품
  - 클라우드CWPP보안제품
- 보안제품 통합 유지보수
- 보안운용인력 파견
- 보안통합유지보수

원격보안관제

- 보안장비 운용
- 탐지/분석
- 침해 대응
- 결과보고
- 정책 업데이트
- 현황관제

네트워크 보안

보안01 시스템 통합 구축

보안 02 통합 유지보수/ 인력파견

SECUMOM

클라우드 보안/ 보안통제 솔루션 제조

클라우드 보안 사업

- 표준 템플릿에 의한 보안점검
- 자산관리 / 시스템 무결성보증
- 애플리케이션 제어 및 관리 보안통제 (Security_Group)
- CSPM (Cloud Security Posture Management)
- CWPP (Cloud Workload Protection Platform)

보안운용업무 자동화 사업

- 사고 대응 내역을 기록하고 조직 내에 공유하여 차후 신속한 의사결정
- SOA (SOC의 보안업무 자동화)
- SRIP (보안 이벤트 자동대응)
- TIP (외부위협 정보이용 관제)

차세대 보안 솔루션 사업

- 사용자와 단말 내부 행위를 모니터링하고 위협 탐지
- 대용량 트래픽 네트워크단 보안통제
- BAS (SOC의 보안업무 자동화)
- AI 기반 이상징후 탐지/경보
- CTI (Cyber Threat Intelligence)

SECULINKS

제로 트러스트 보안 연결/연계 솔루션 제조

시큐링스 SDP

- 보안원격연결 솔루션

시큐링스 CASB

- 클라우드 접근 보안 중계 솔루션

시큐링스 IDCS

- 초고속 망연계 솔루션

시큐링스 ITDS

- 지능형 트래픽분석 솔루션

시큐링스 Cloud Box

- 시스템 접근제어 솔루션

Source: http://jinnhyunsecurity.com/?page_id=131

192

III. 클라우드 보안 솔루션과 비즈니스

❖ LG유플러스, 기업 고객 위한 SECaaS 'U+클라우드보안팩'

• "중소기업·소상공인 대상 시장"

Source: https://www.kcloudnews.co.kr/news/articleView.html?idxno=775

III. 클라우드 보안 솔루션과 비즈니스

❖ **Multi-Cloud Security Threats** (Couchbase)

- 통합 관리 및 거버넌스 부족
- 사일로, 인력 제약, 교육 격차
- 위치에 관계없이 워크로드를 보호
- 상호 운용성 부족
- 잘못된 구성 또는 구성 변동
- 환경 전반의 가시성 부족
- 일관된 액세스 제어 유지
- 섀도 IT

Source: https://www.couchbase.com/blog/multicloud-security/

III. 클라우드 보안 솔루션과 비즈니스

❖ **Multi-Cloud Security Threats** (Couchbase)

- **통합 관리 및 거버넌스 부족:** 여러 클라우드 환경 전반에서 보안 정책, 액세스 제어 및 모니터링을 관리하는 것은 특히 통합 거버넌스가 마련되어 있지 않은 경우 어려울 수 있다.
- **사일로, 인력 제약, 교육 격차:** 사일로, 인력 제약, 교육 격차 등으로 인해 여러 클라우드 환경의 보안 정책과 절차가 일관되지 않을 수 있다. 이러한 불일치로 인해 사이버 공격에 노출되고 보안 사고에 효과적으로 대응하기 어려울 수 있다.
- **워크로드의 위치에 관계없이 워크로드 보호:** 워크로드의 위치에 관계없이 워크로드를 보호하는 것이 중요합니다. 이를 위해서는 모든 클라우드 환경에서 일관된 보안 정책과 액세스 제어를 구현해야 한다.
- **상호 운용성 부족:** 클라우드 제공업체마다 서로 다른 API와 프로토콜을 사용하므로 상호 운용성 문제가 발생할 수 있다. 적절한 통합이 이루어지지 않으면 모든 환경에서 보안 정책이 일관되게 적용되지 않을 수 있다.
- **잘못된 구성 또는 구성 변동:** 한 클라우드 환경의 변경 사항이 모든 환경에 복제되지 않은 경우 잘못된 구성 또는 구성 변동이 발생할 수 있다. 이는 보안 취약점으로 이어질 수 있으며 일관된 보안 태세를 유지하기 어렵게 만들 수 있다.
- **환경 전반의 가시성 부족:** 적절한 모니터링 및 가시성 도구가 없으면 모든 클라우드 환경에서 보안 인시던트를 탐지하기가 어려울 수 있다. 이는 대응 지연과 피해 증가로 이어질 수 있다.
- **일관된 액세스 제어 유지:** 모든 클라우드 환경에서 액세스 제어를 일관성 있게 유지하는 것이 중요하다. 일관성이란 강력한 인증 및 권한 부여 정책을 적용하고 액세스 권한을 정기적으로 검토하는 것을 의미한다.
- **섀도 IT:** 섀도 IT는 비즈니스 부서에서 IT 승인 없이 클라우드 서비스를 사용할 때 발생할 수 있다. 이는 보안 취약점으로 이어질 수 있으며 모든 환경에서 일관된 보안 태세를 유지하기 어렵게 만들 수 있다.

Source: https://www.couchbase.com/blog/multicloud-security/

III. 클라우드 보안 솔루션과 비즈니스

❖ **Developing a Multi-Cloud Security Strategy** (Couchbase)

- **중요 자산 및 데이터 식별:** 보호가 필요한 중요 자산과 데이터를 식별하는 것부터 시작해야 하며, 중요 자산에는 민감한 고객 정보, 재무 데이터, 지적 재산, 기타 유출 시 조직에 심각한 피해를 입힐 수 있는 독점 정보 등이 포함
- **위험 및 위협 평가:** 중요 자산을 식별한 후에는 해당 자산에 대한 잠재적 위험과 위협을 평가하며, 위험 평가에는 내부 위협, 외부 위협, 공급망 공격 등 위협 환경을 고려하고 인프라 및 애플리케이션의 취약점을 파악하는 것이 포함
- **보안 프레임워크 선택:** 조직의 목표와 규정 준수 요건에 맞는 보안 프레임워크를 선택하며, 널리 사용되는 프레임워크에는 미국 국립표준기술연구소(NIST)의 사이버 보안 프레임워크, PCI DSS(결제 카드 업계 데이터 보안 표준), ISO 27001 등이 있다.
- **보안 제어를 구현:** 선택한 프레임워크에 부합하는 보안 제어를 구현하여 식별된 위험과 위협을 완화하며, 이러한 보안 제어에는 ID 및 액세스 관리, 네트워크 세분화, 암호화, 데이터 손실 방지 및 보안 모니터링이 포함될 수 있다.
- **모니터링 및 테스트:** 멀티클라우드 보안 전략이 효과적이고 최신 상태인지 확인하기 위해 정기적으로 모니터링하고 테스트하며, 모니터링 및 테스트에는 정기적인 취약성 평가, 침투 테스트, 보안 감사 수행이 포함된다.
- **인시던트 대응 계획:** 보안 인시던트 발생 시 취해야 할 단계를 간략하게 설명하는 인시던트 대응 계획을 개발하며, 이 계획에는 대응 팀을 파악하고, 역할과 책임을 정의하고, 커뮤니케이션 채널을 구축하는 것이 포함되어야 한다.
- **정기적인 보안 테스트:** 보안 전략을 정기적으로 테스트하여 취약점을 파악하고 보안 제어의 효과를 평가하며, 침투 테스트 및 취약성 평가를 수행하여 멀티클라우드 환경의 취약점을 파악한다.
- **보안 트렌드에 대한 최신 정보 파악:** 업계의 최신 보안 동향과 위협에 대한 최신 정보를 파악하며, 보안 커뮤니티에 참여하고, 컨퍼런스에 참석하고, 업계 보고서를 읽으며 최신 정보를 파악하고 그에 따라 전략을 조정한다.

Source: https://www.couchbase.com/blog/multicloud-security/

III. 클라우드 보안 솔루션과 비즈니스

❖ **Multi-Cloud Security Best Practices** (Couchbase)

- **통합 관리 및 거버넌스 플랫폼을 사용:** 통합 관리 및 거버넌스 플랫폼을 사용하면 모든 클라우드 공급업체에 일관된 정책을 적용하고, 규정 준수 보고를 간소화하며, 잘못된 구성의 위험을 줄일 수 있다.
- **포괄적인 ID 및 액세스 관리(IAM) 전략 구현:** 포괄적인 IAM 전략에는 역할 기반 액세스 제어, 다단계 인증, 사용자 계정의 중앙 집중식 관리가 포함된다.
- **미사용 및 전송 중인 데이터에 암호화를 사용:** 암호화는 중요한 데이터를 무단 액세스로부터 보호하기 때문에 멀티클라우드 보안의 중요한 구성 요소이다.
- **로그 및 이벤트 모니터링 및 분석:** 로그와 이벤트를 모니터링하여 보안 인시던트를 감지하고 신속하게 대응하여 위험을 완화할 수 있다.
- **정기적으로 취약성 평가 및 자동화된 모의 침투 테스트를 수행:** 취약성 평가와 침투 테스트는 인프라와 애플리케이션의 잠재적 취약성을 식별하는 데 도움이 되므로 멀티클라우드 보안의 중요한 구성 요소이다.

Source: https://www.couchbase.com/blog/multicloud-security/

III. 클라우드 보안 솔루션과 비즈니스

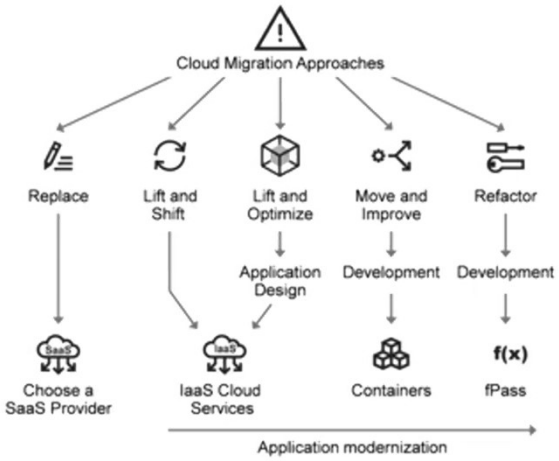
❖ **Multi-Cloud Security Challenges** (Couchbase)

- **복잡성:** 멀티클라우드 보안은 복잡할 수 있으며, 특히 여러 클라우드 제공업체가 자체 보안 프로토콜과 정책을 가지고 있는 경우 더욱 그렇다. 이로 인해 모든 클라우드에서 보안 태세를 종합적으로 파악하기가 어려울 수 있다.
- **통합:** 통합은 멀티클라우드 보안의 주요 과제이다. 보안 위협을 모니터링, 탐지 및 대응하기 위해 보안 도구 및 프로세스가 각 클라우드 제공업체의 API와 통합되도록 해야 한다.
- **규정 준수:** 여러 클라우드 제공업체를 사용하면 서로 다른 규제 요건을 준수하는 것이 어려울 수 있다. 개인 식별 정보(PII) 또는 결제 카드 정보와 같은 민감한 데이터를 처리하는 것이 복잡해질 수 있다.
- **기술 격차:** 멀티 클라우드 보안 전략을 구현하려면 다양한 클라우드 제공업체의 보안 프로토콜에 대한 전문 기술과 지식이 필요하다. 이러한 전문 지식을 갖춘 사내 직원이 없을 경우, 강력한 보안 태세를 개발하고 유지하는 데 어려움을 겪을 수 있다.
- **비용:** 여러 클라우드에서 보안을 관리하려면 비용이 많이 들 수 있다. 여러 클라우드에서 보안을 관리하기 위해 추가 도구와 리소스에 투자해야 할 수 있으며, 이는 전체 IT 비용을 증가시킬 수 있다.

Source: https://www.couchbase.com/blog/multicloud-security/

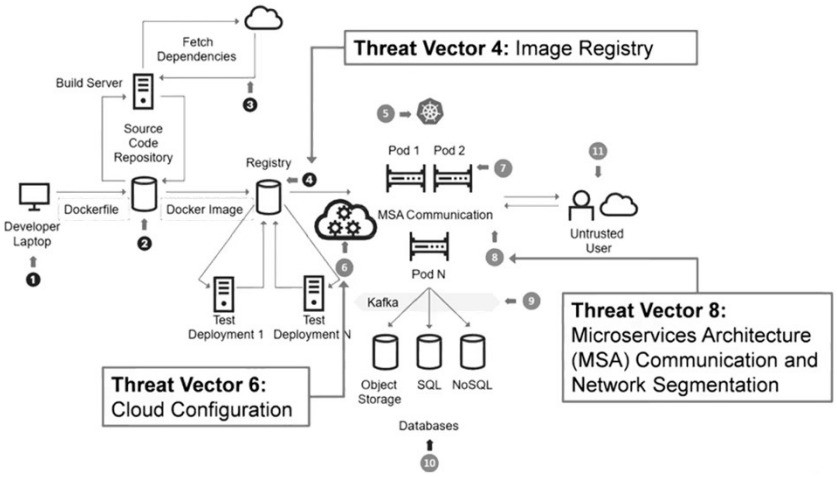
❖ **Digital Transformation Creates New Security Exposures**

- **Cloud Migration for Application Modernization**
  - Replace → SaaS
  - Lift and Shift → IaaS
  - Lift and Optimize → Application Design → IaaS
  - Move and Improve → Development ➔ Containers
  - Refactor → Development → fPass



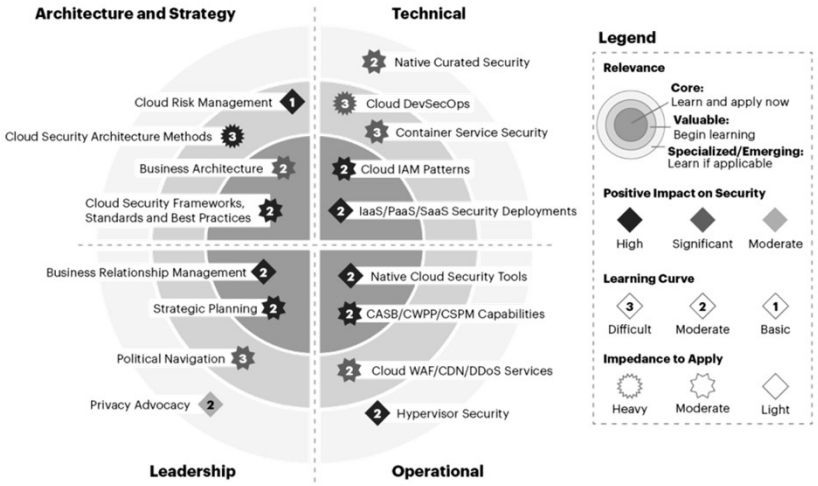
Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

❖ **New Security Threats – Container Example**



Source: Gartner - https://webinar.gartner.com/429960/agenda/session/1033381?login=ML

❖ 클라우드 보안 아키텍처 기술 범위 (Cloud Security Architecture Skills Scope)



Source: Gartner

THANK YOU