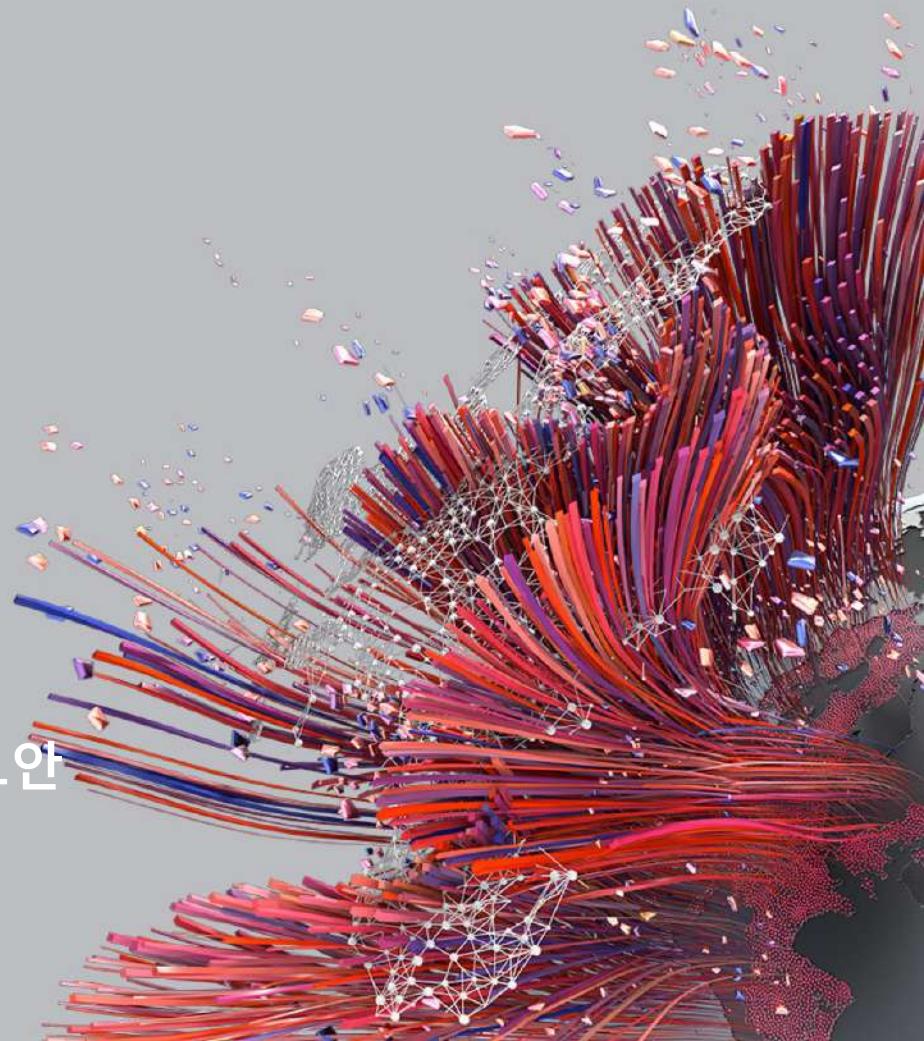
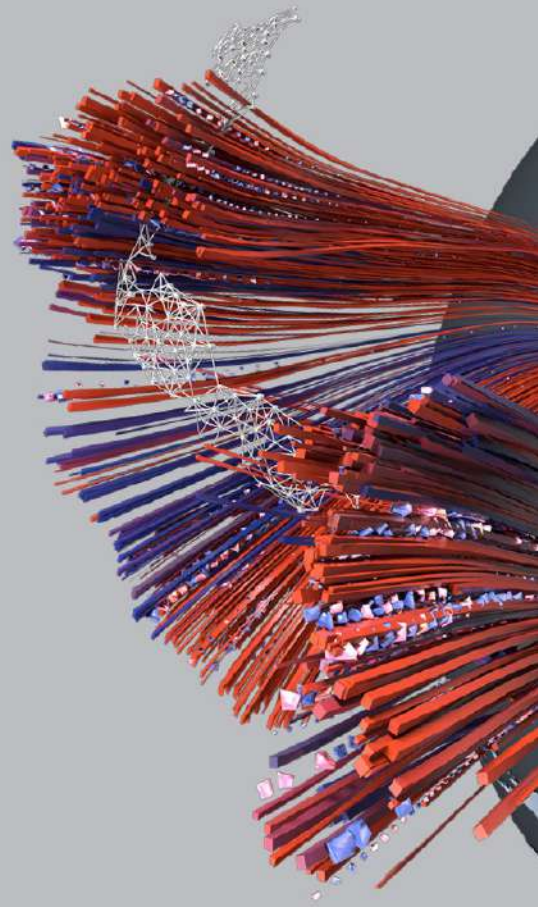


기업의 클라우드 보안은 워크로드 보안으로부터

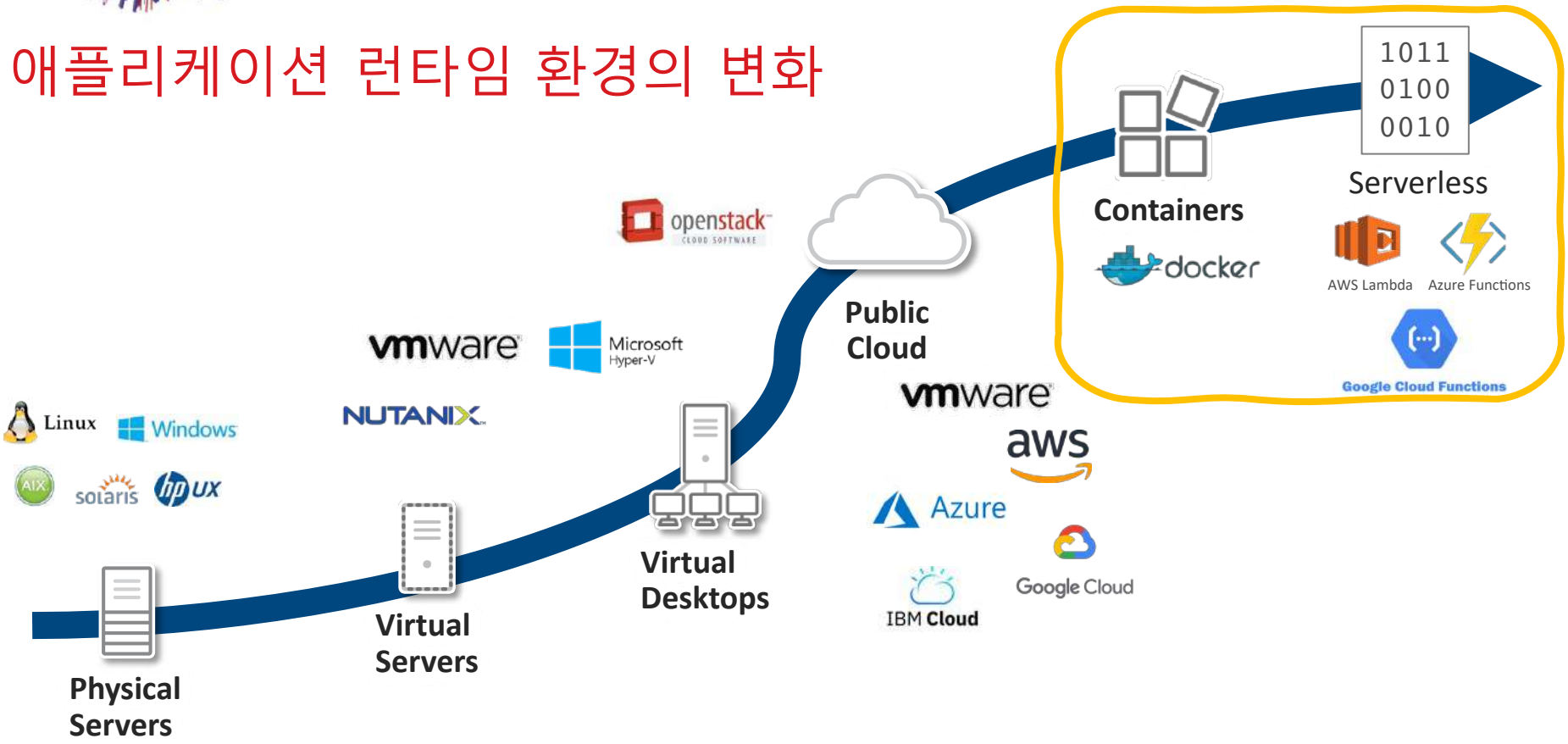
가장 쉽고 효과적인 클라우드 워크로드 보안

장 성 민
Trend Micro

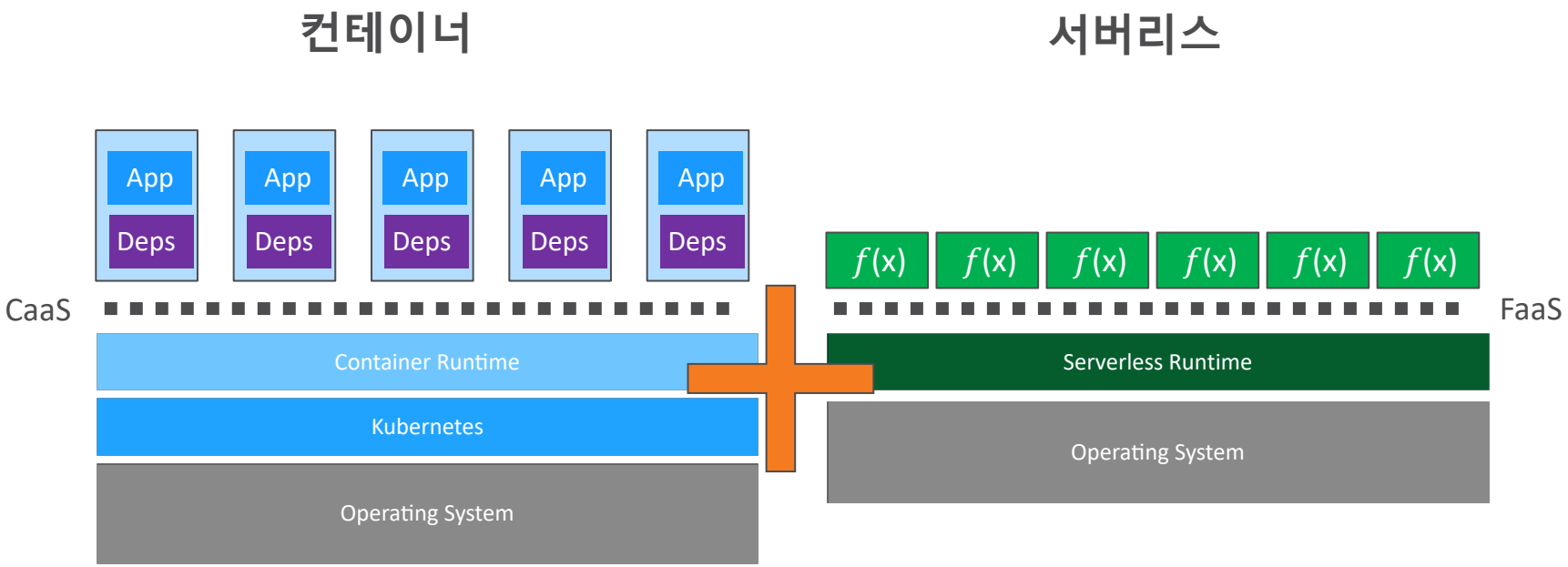


클라우드 네이티브 애플리케이션으로의 진화

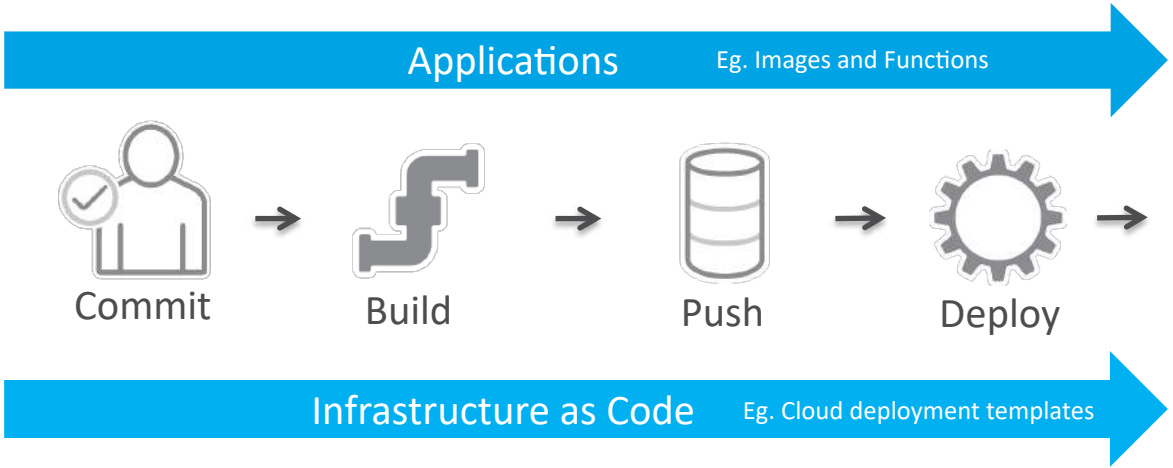
애플리케이션 런타임 환경의 변화

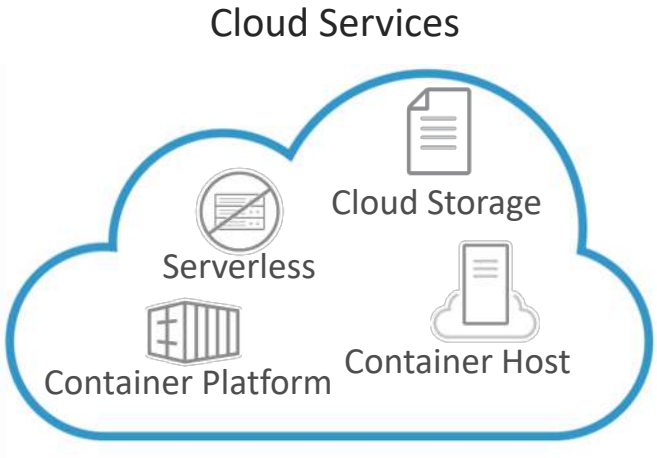


새로운 애플리케이션 런타임 환경



클라우드 네이티브 애플리케이션





클라우드 네이티브 애플리케이션의 보안 고려사항

- 취약한 소스 코드
- 악성코드
- 기밀정보, 키 정보
- 규정위반

- 잘못된 클라우드 서비스 설정을 노리는 익스플로잇
- 클라우드스토리지에 악성코드 업로드

Applications

Commit → Build → Push → Deploy

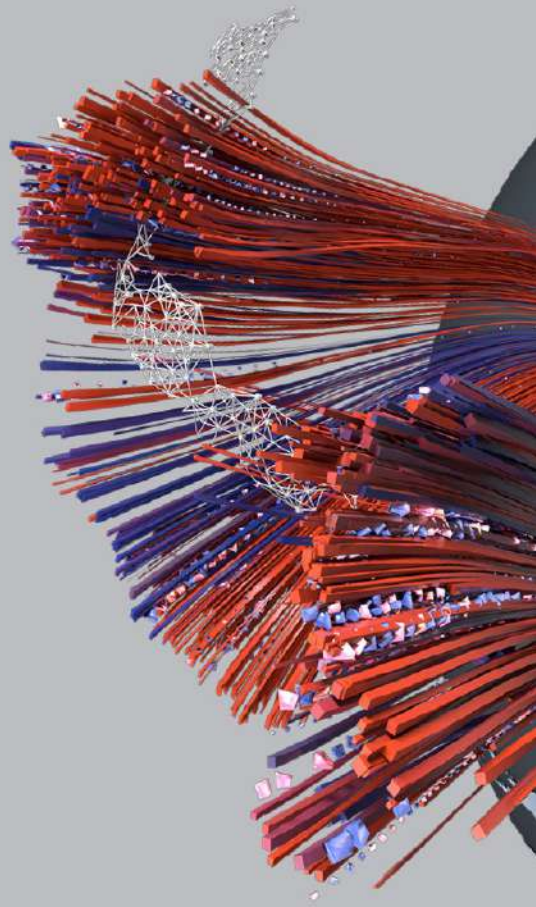
Infrastructure as Code

- 잘못된(오류) 설정

Cloud Services

Cloud Storage
Serverless
Container Platform
Container Host

- Serverless 애플리케이션 공격
- 컨테이너 플랫폼 서비스에 대한 공격
- 컨테이너 호스트에 대한 공격



클라우드 워크로드 보안부터!!

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | 무결성 모니터링 | 애플리케이션제어

취약점 방어(Virtual Patching)

IDS / IPS → OS &애플리케이션 취약점 보호

Web 애플리케이션 보호

애플리케이션 제어 → 애플리케이션 가시화 & 통제

IPv4, IPv6, Port, Protocol 제어 ← 방화벽

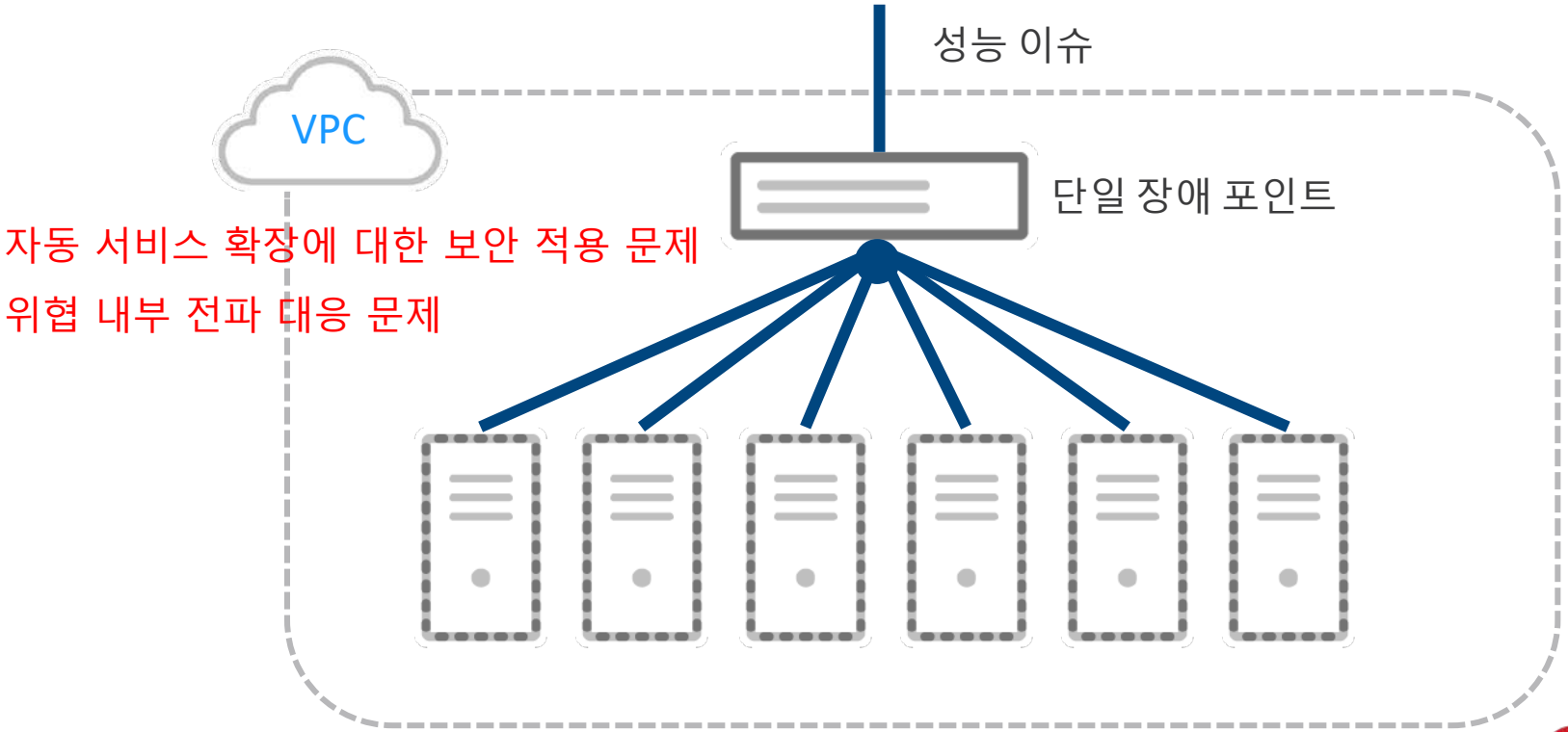
안티 멀웨어 (백신) → 악성 코드 공격에서 보호

중요한 보안 이벤트를 로그에서 효율적으로 발견 ← 로그 감사 Log Inspection

무결성 모니터링 Integrity Monitoring → 디렉토리, 파일, 레지스트리,속성, 통신포트 등의 이상 변경 감지

응용프로그램 제어 Application Control → 불법 애플리케이션 차단

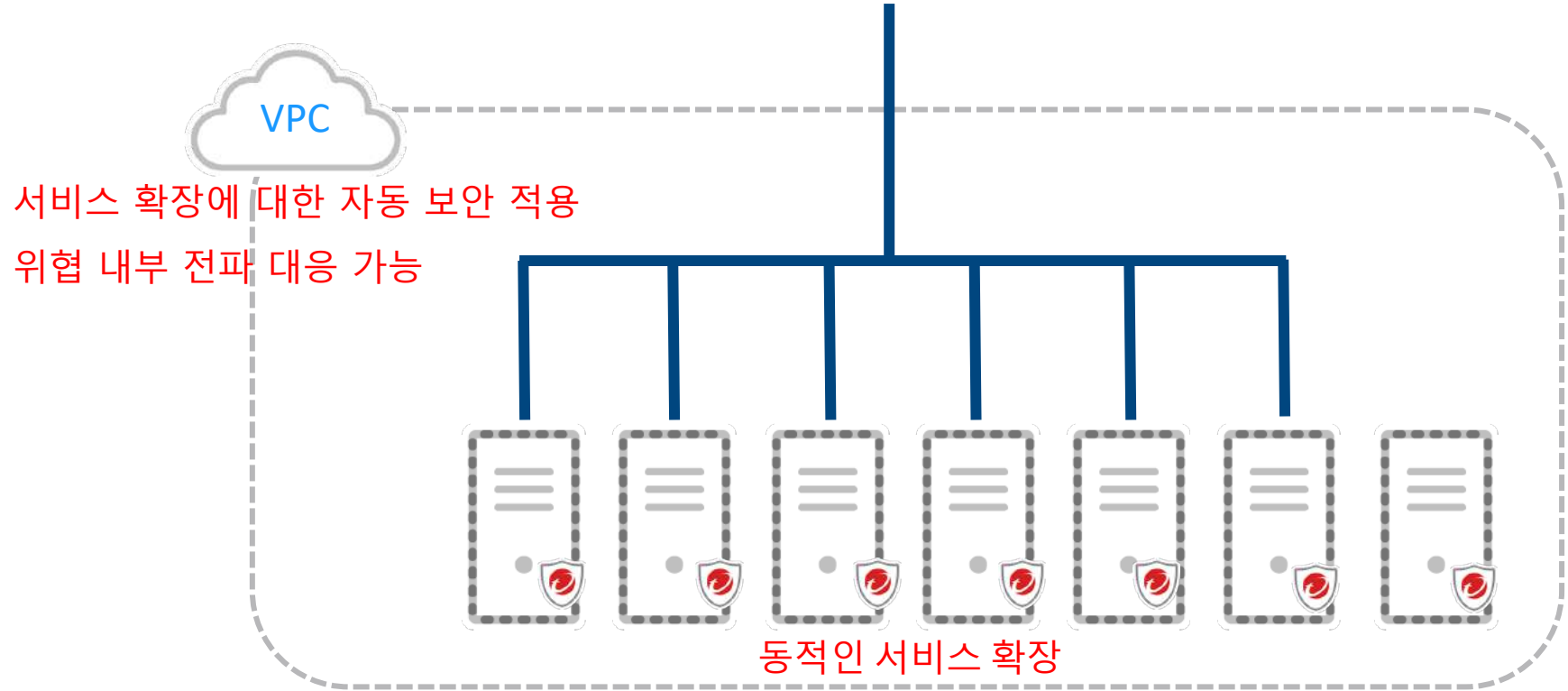
동적인 워크로드 보호 – 자동화된 보안



자동 서비스 확장에 대한 보안 적용 문제

위협 내부 전파 대응 문제

동적인 워크로드 보호 – 자동화된 보안



제로데이 취약점 대응 – Shared Responsibility Model

Docker

Jenkins

solarwinds

Sunburst

Erebus

GhostCat [CVE-2020-1938]

Exchange

Hafnium

Heartbleed

WannaCry

The Apache Software Foundation
http://www.apache.org/

Struts™ 2

Zerologon

Windows

TREND MICRO

취약점을 이용한 익스플로잇 방어

EXPLOIT DATABASE

Verified Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2021-03-23	⬇		✓	Codiad 2.8.4 - Remote Code Execution (Authenticated)	WebApps	Multiple	WangYihang
2021-03-23	⬇		✗	Elodea Event Collector 4.9.3 - 'ElodeaEventCollectorService' Unquoted Service Path	Local	Windows	Alan Mondragon
2021-03-23	⬇		✗	ActivIdentity 8.2 - 'ac.sharedstore' Unquoted Service Path	Local	Windows	SamAlucard
2021-03-23	⬇		✗	ELAN Touchpad 15.2.13.1_X64_WHQL - 'ETDService' Unquoted Service Path	Local	Windows	SamAlucard
2021-03-23	⬇		✗	Hi-Rez Studios 5.1.6.3 - 'HiPatchService' Unquoted Service Path	Local	Windows	Ekrem Can Kök
2021-03-23	⬇		✗	Hotel And Lodge Management System 1.0 - 'Customer Details' Stored XSS	WebApps	PHP	Jitendra Kumar Tripathi
2021-03-23	⬇		✗	MyBB 1.8.25 - Poll Vote Count SQL Injection	WebApps	PHP	SivertPL
2021-03-22	⬇		✗	OSAS Traverse Extension 11 - 'travextensionhostsvc' Unquoted Service Path	Local	Windows	Johnny Tech
2021-03-22	⬇		✗	ProFTPD 1.3.7a - Remote Denial of Service	DoS	Multiple	xynmaps
2021-03-22	⬇		✗	MyBB 1.8.25 - Chained Remote Command Execution	WebApps	PHP	SivertPL
2021-03-22	⬇		✗	KZTech/JatonTec/Neotel JT3500V 4G LTE CPE 2.0.1 - Weak Default WiFi Password Algorithm	Remote	Hardware	LiquidWorm
2021-03-22	⬇		✗	MacPaw Encrypto 1.0.1 - 'Encrypto Service' Unquoted Service Path	Local	Windows	Ismael Nava
2021-03-22	⬇		✗	WordPress Plugin Delightful Downloads Jquery File Tree 1.6.6 - Path Traversal	WebApps	PHP	Nicholas Ferreira
2021-03-22	⬇		✗	Winpakpro 4.8 - 'WPCommandFileService' Unquoted Service Path	Local	Windows	Alan Mondragon
2021-03-22	⬇		✗	Winpakpro 4.8 - 'ScheduleService' Unquoted Service Path	Local	Windows	Alan Mondragon

Showing 1 to 15 of 43,889 entries

FIRST PREVIOUS 1 2 3 4 5 ... 2926 NEXT LAST

취약점 방어(가상패치) - Shared Responsibility Model

침입방지

네트워크와
애플리케이션에
대한 위협 방어

취약점 스캔

자동화된 취약점 감사
및 방어 룰 적용

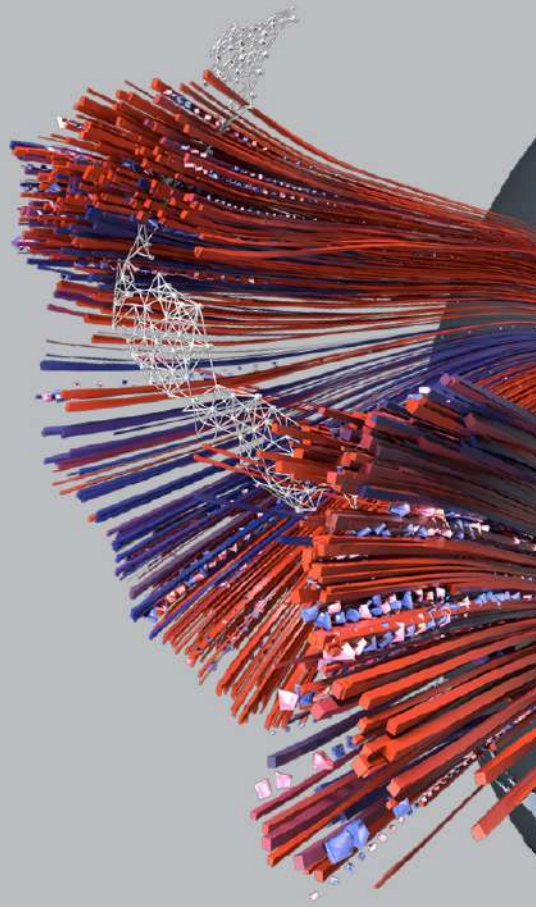
OS와 애플리케이션 취약점 차단

랜섬웨어 C&C 접속 탐지 및 차단

긴급 패치에 대한 비용 감소

EOS 시스템과 애플리케이션 보호

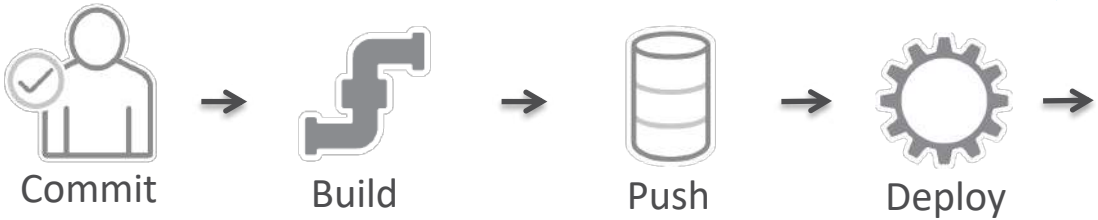
DevOps 보안 적용도 필수 !!!



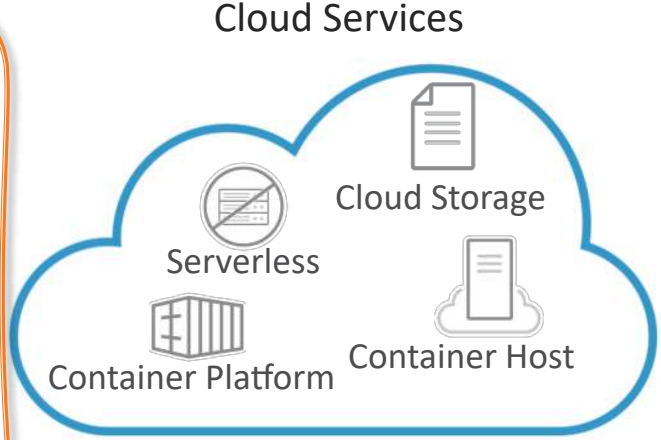
DevOps 파이프라인에 보안 적용

애플리케이션 빌드 파이프 라인에서 보안 적용

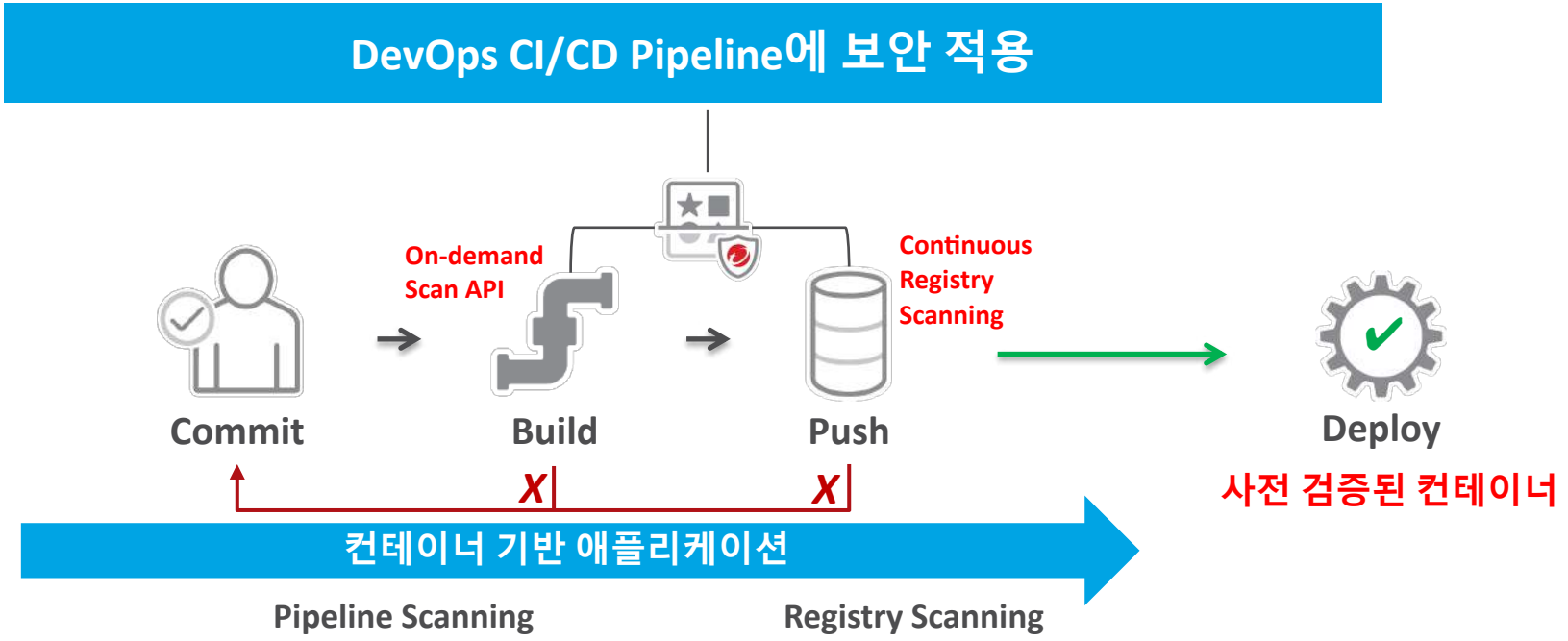
Applications — Eg. Images and Functions

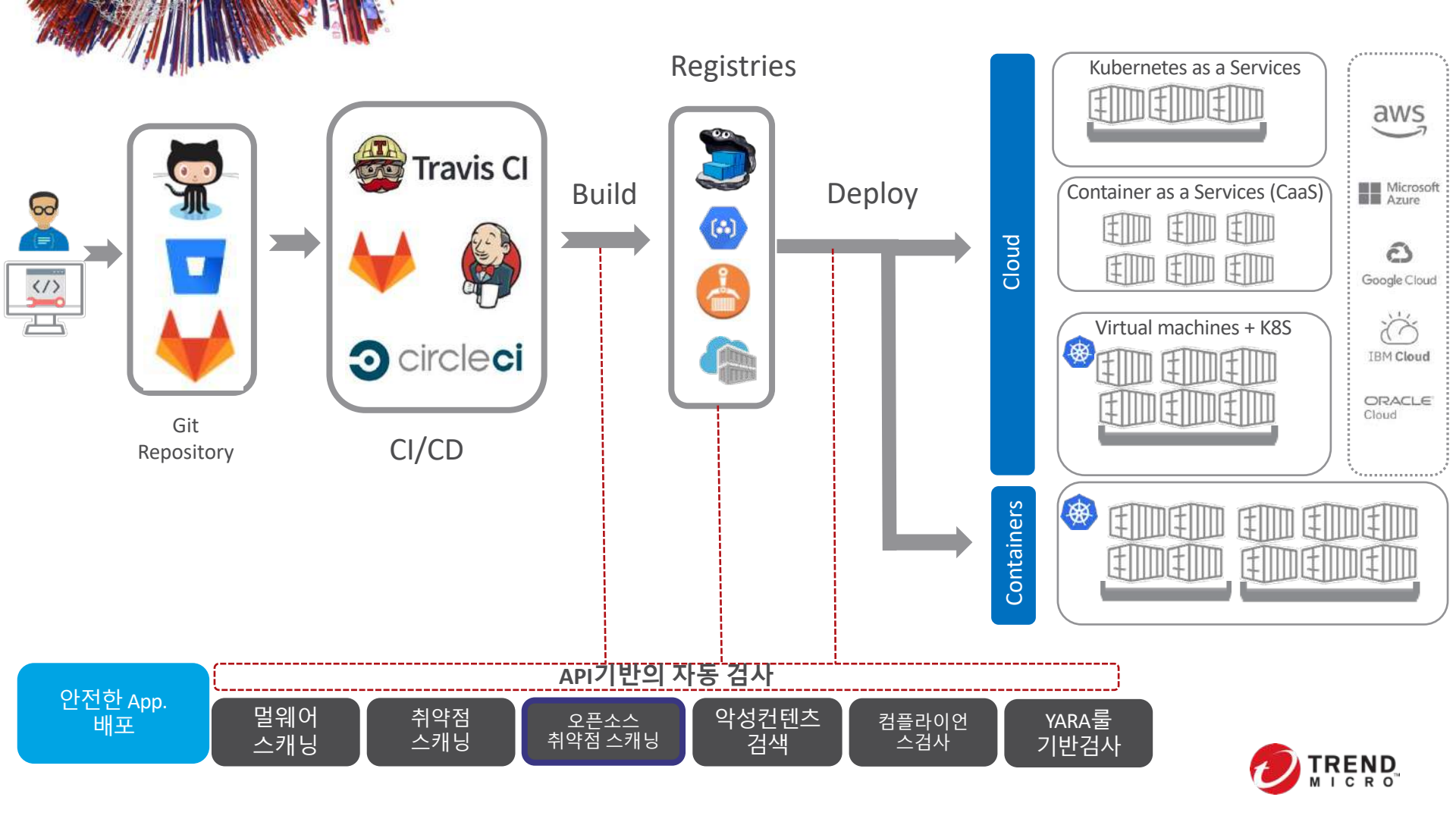


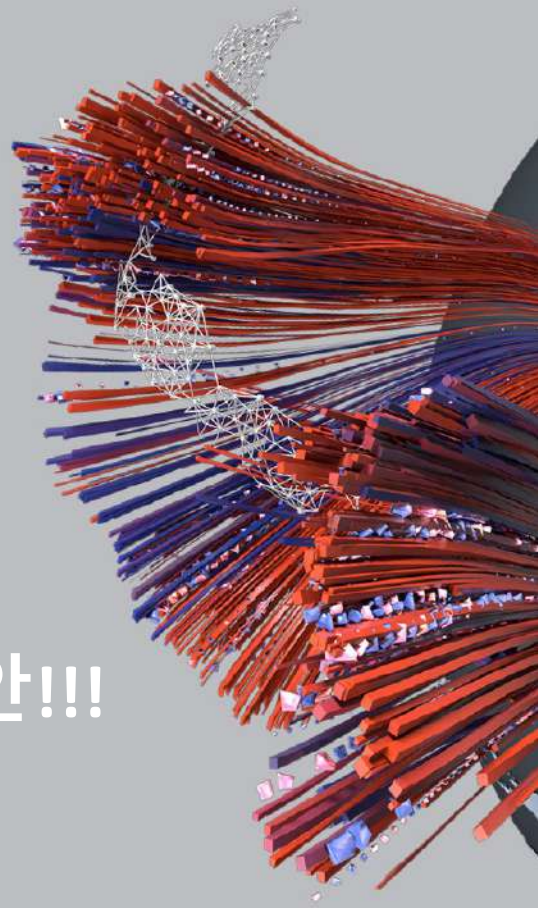
Infrastructure as Code — Eg. Cloud deployment templates



CI/CD 파이프라인에 보안 적용

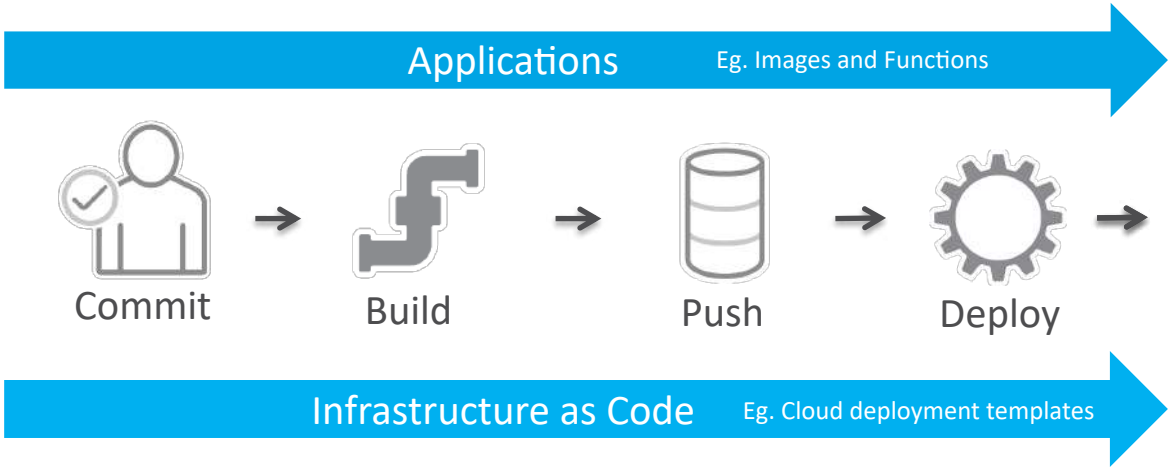


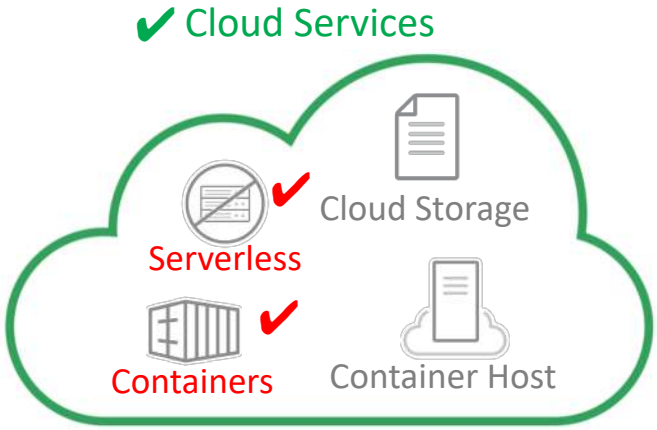

Registries
Travis CI
circleci
Git
Repository
CI/CD
Build
Deploy
Cloud
Containers
Kubernetes as a Services
Container as a Services (CaaS)
Virtual machines + K8S
aws
Microsoft Azure
Google Cloud
IBM Cloud
ORACLE Cloud
안전한 App. 배포
API기반의 자동 검사
멀웨어 스캐닝
취약점 스캐닝
오픈소스 취약점 스캐닝
악성컨텐츠 검색
컴플라이언 스검사
YARA룰 기반검사
TREND MICRO



세째, 새로운 애플리리케이션 런타임 보안!!!
- CaaS, Serverless 보안

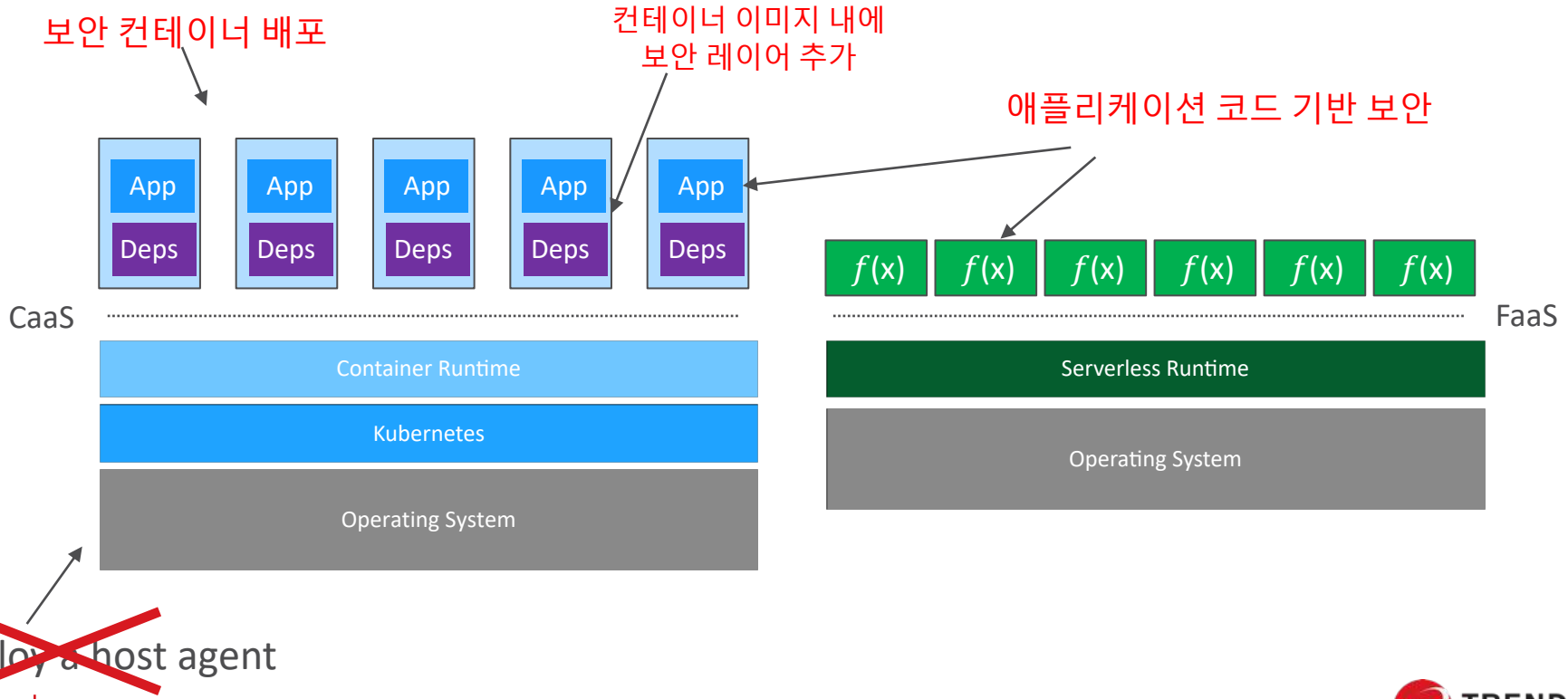
새로운 애플리케이션 런타임 환경 보안



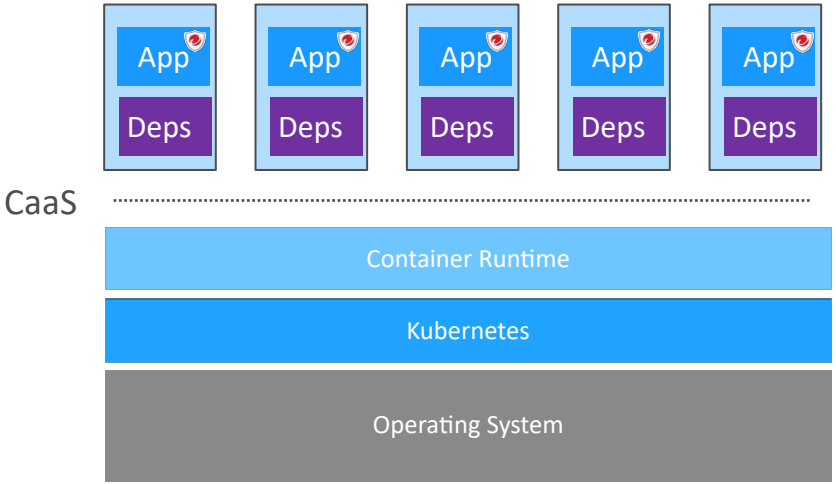


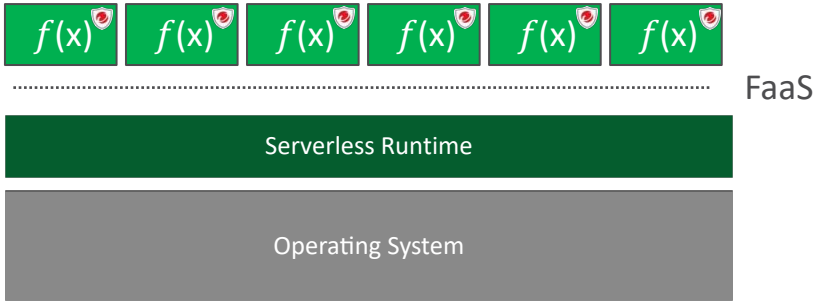
- 컨테이너 플랫폼 보호
- 서버리스 애플리케이션 보호

컨테이너 플랫폼 & 서버리스 애플리케이션 보안

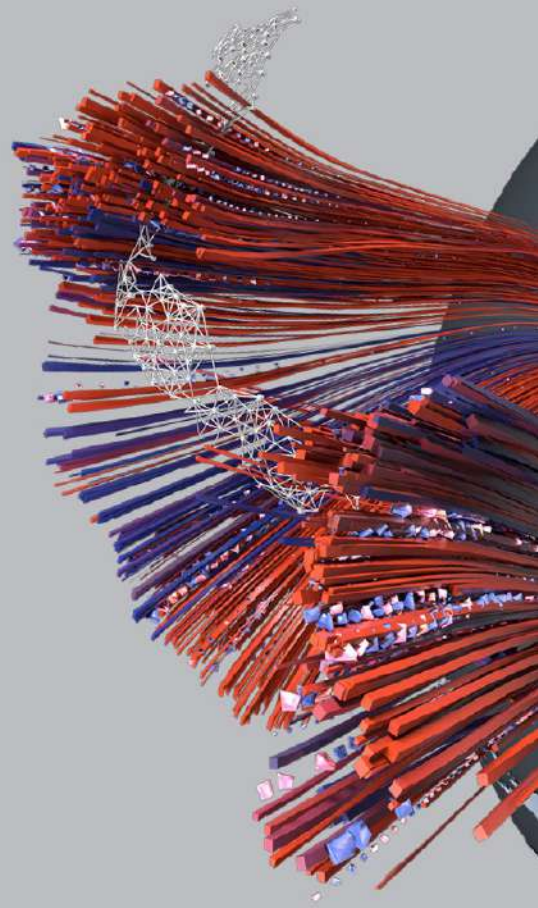


RASP(Runtime Application Self-Protection)





- 앱 일관성
- 개발 친화적이고 빠른 보안 적용
- 정확성
- API 보안
- 효율적인 자원 & 비용 관리
- 유연성

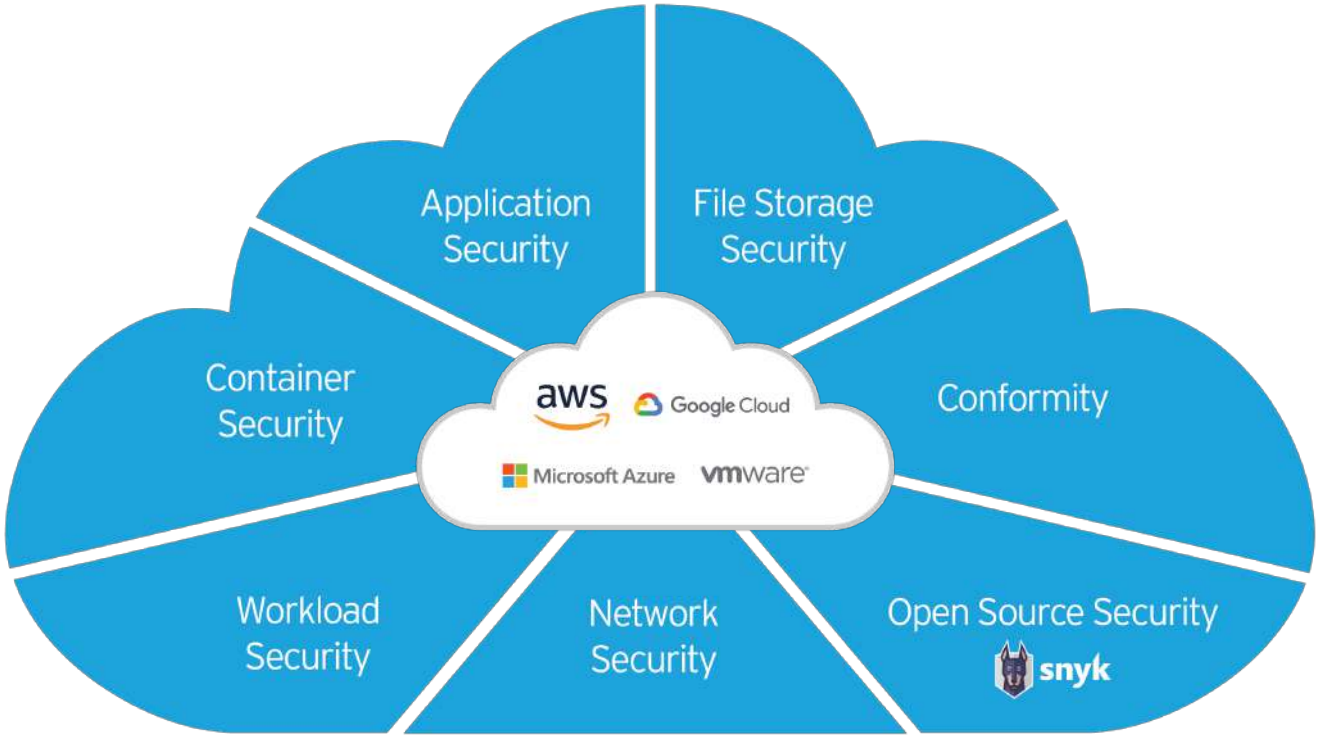


Trend Micro Cloud One

Trend Micro Cloud One™

Security Services Platform for Cloud Builders

Trend Micro cloud one



TREND MICRO

Cloud One™ Workload Security – Deep Security

Environments


Containers


Cloud


Virtual Server


Data Center

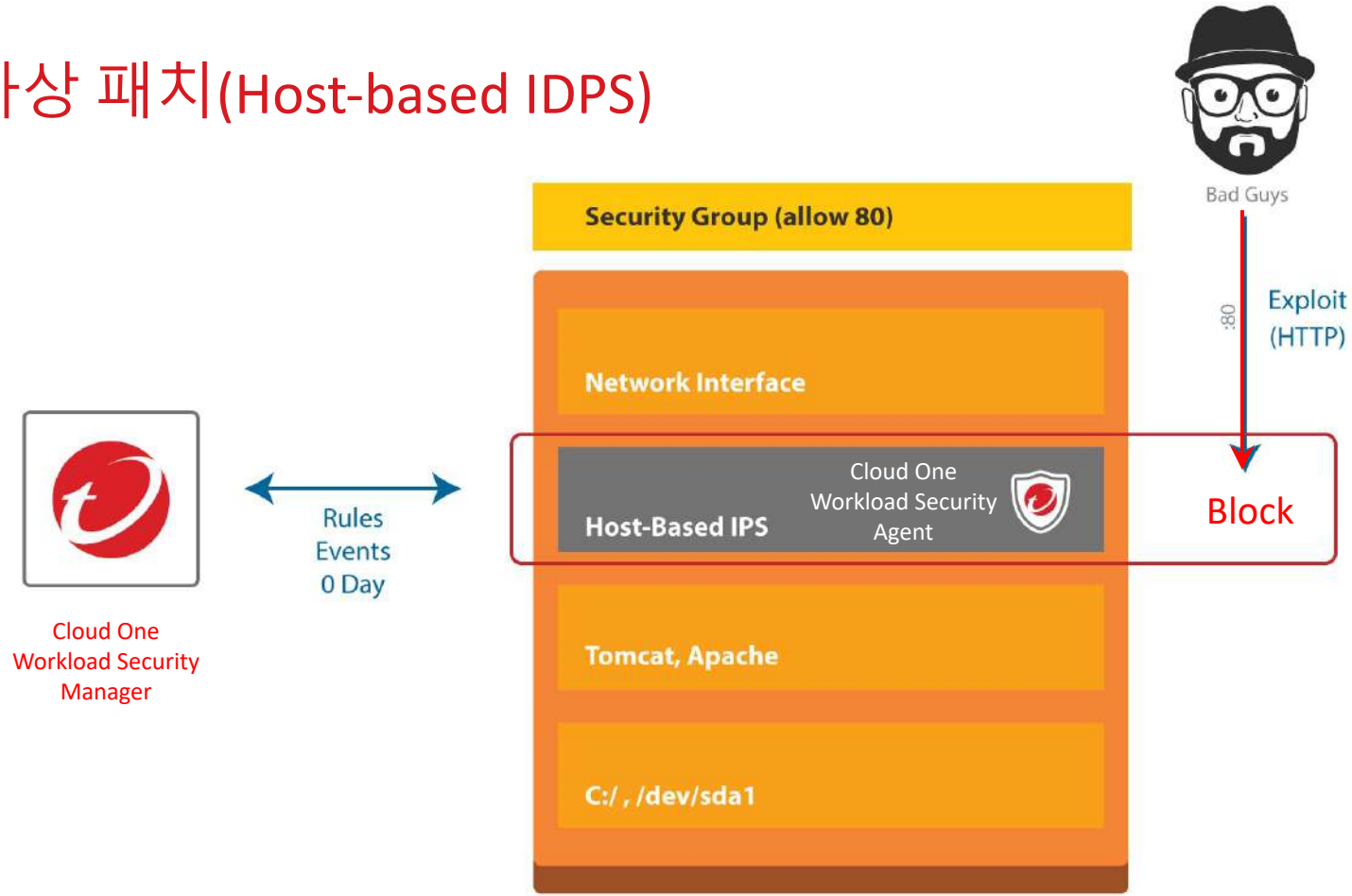
API & Integrations

Platforms

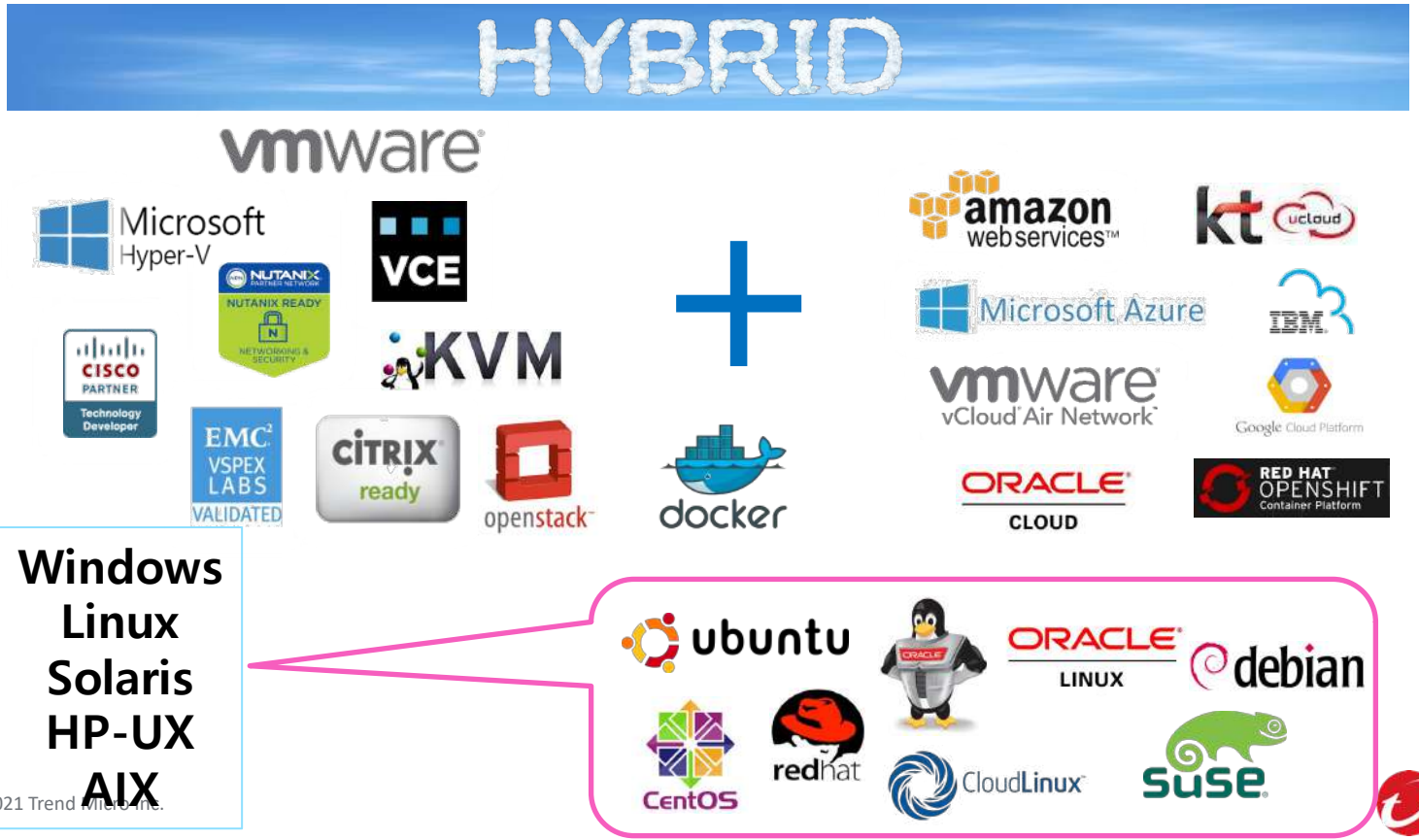
- 호스트 기반 보안 & 침해 대응
  - 취약점 (IDS/IPS) & 측면 이동탐지, 방화벽
  - 무결성 모니터링, 애플리케이션 제어 & 로그 감사
  - 멀웨어 & 랜섬웨어 (행위 & 머신러닝)
- 배포 자동화, API 통합
- 가장 광범위한 플랫폼과 클라우드 환경 지원

클라우드 워크로드, 컨테이너 및 서버에 대한 런타임 워크로드 보안

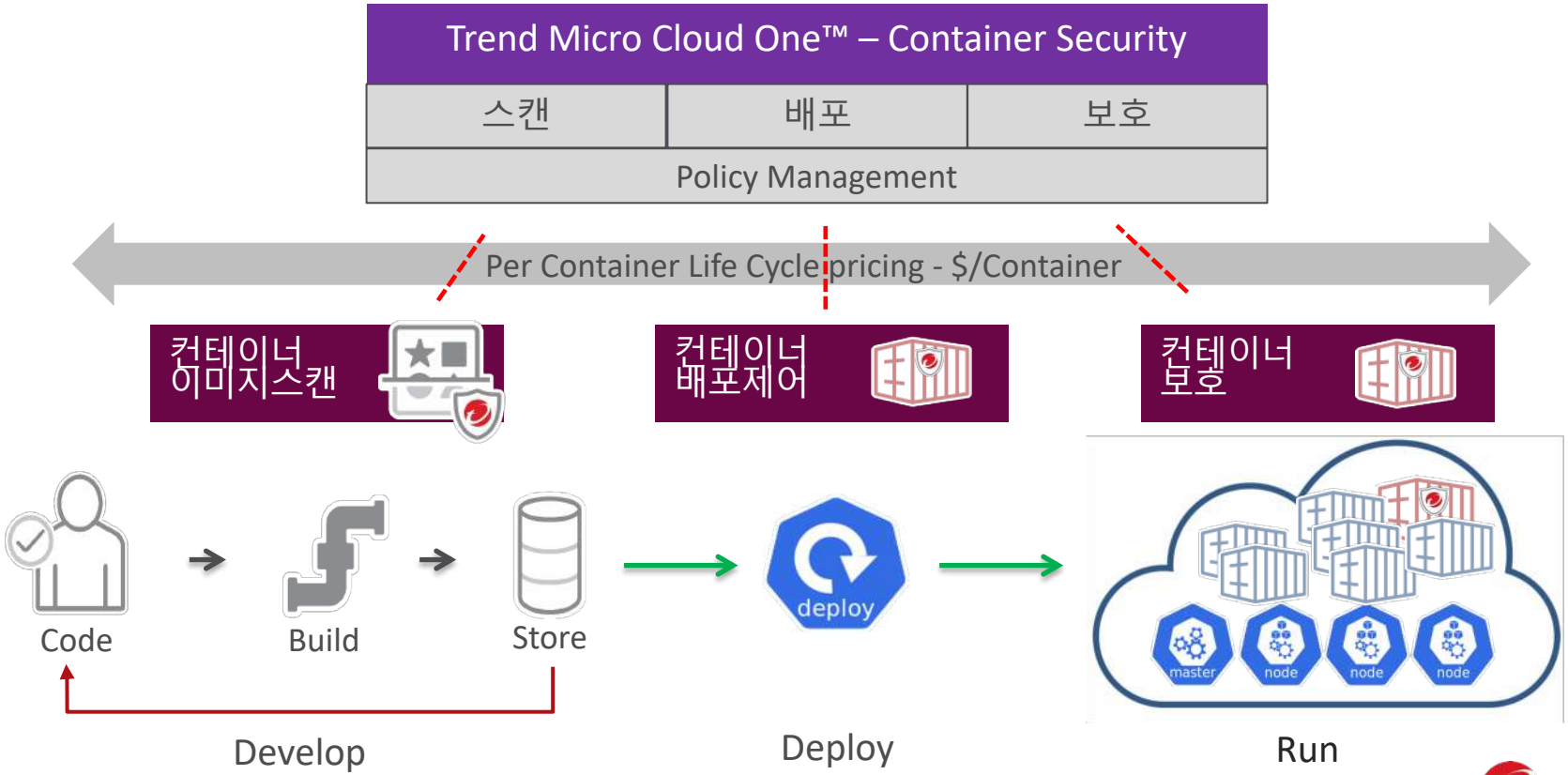
가상 패치(Host-based IDPS)



Cloud One™ Workload Security- 가장 많은 클라우드, 플랫폼 지원

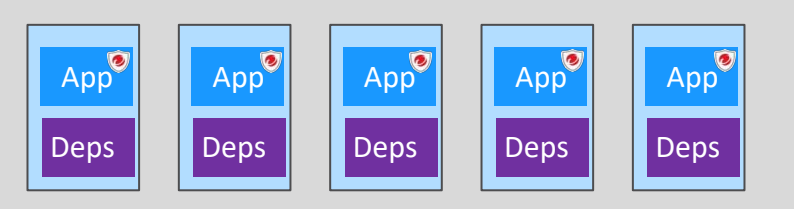


Cloud One™ Container Security



Cloud One™ Application Security

Containers



Kubernetes

OpenShift

Pivotal PKS

AWS EKS

Azure AKS

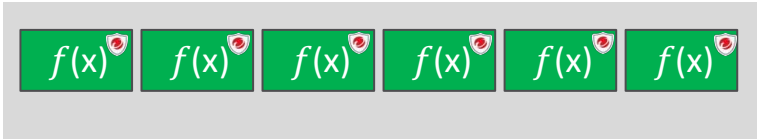
Google GKE

AWS Fargate

Azure Container Instances

Cloud Run

Serverless Functions



AWS Lambda

Azure Functions*

Google Functions*

aws

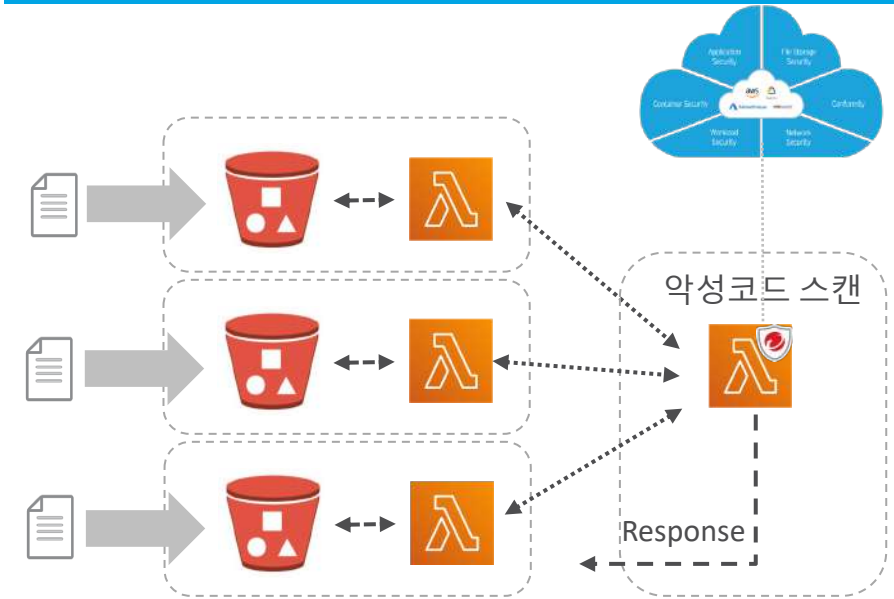
Google Cloud Platform

Azure

TREND MICRO

Cloud One™ File Storage Security

Trend Micro Cloud One File Storage Security

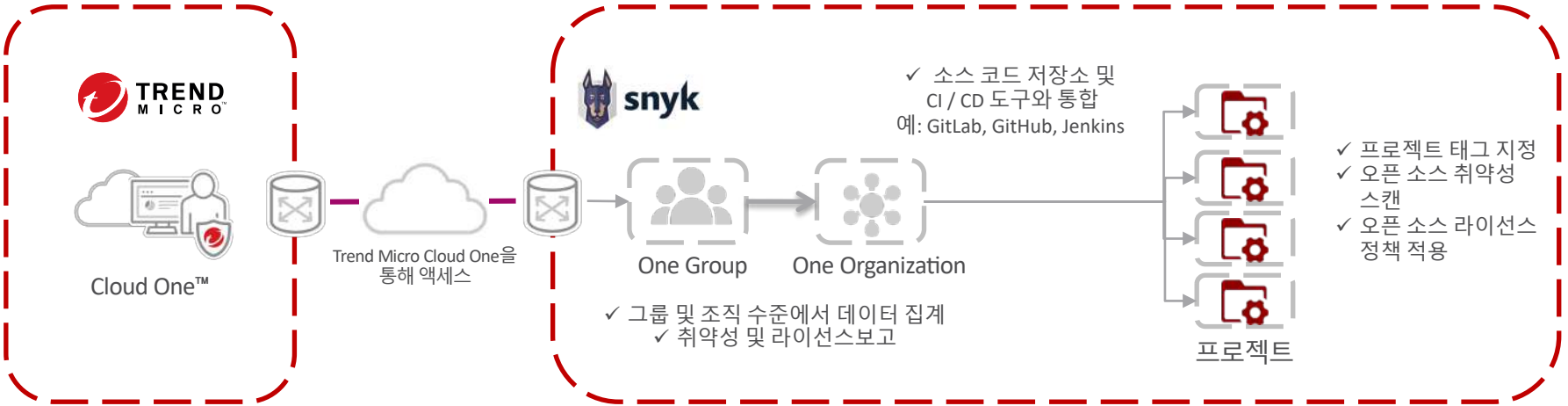


- 악성코드 스캐너 배포
- 최고의 악성코드 대응 기술
  - 파일 평판
  - 신/변종 탐지
  - 머신러닝
- 새로운 개체 자동 스캔
- 버킷 격리
- 상세 탐지 로그

*Planned

클라우드 스토리지 서비스를 위한 악성코드 검사

Cloud One™ – Open Source Security by Snyk



Open Source 취약점 & 라이선스 검사

Cloud One™ Conformity

자동 점검

빌드 파이프라인에서 런타임에 이르기까지 모범사례 및 규정 준수, 표준 준수 여부를 지속적으로 점검

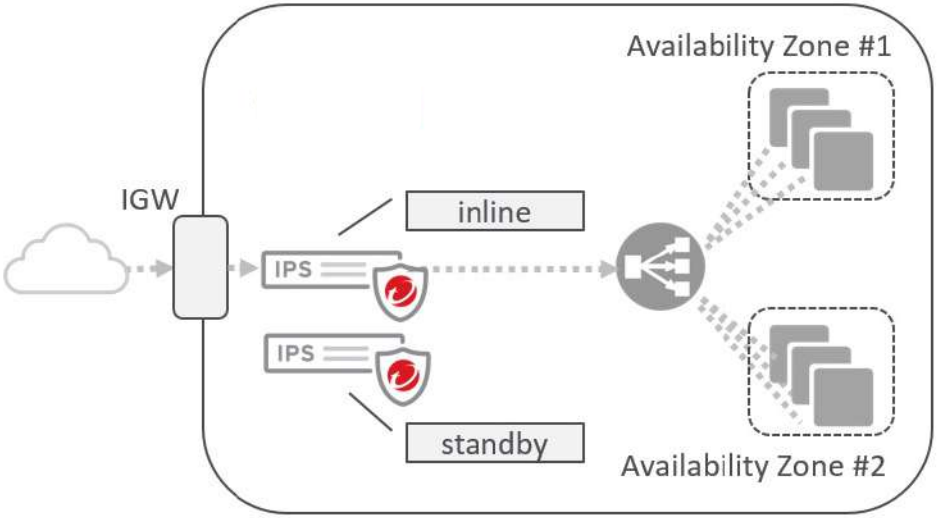
자동 교정

자동 교정 및 개발 워크플로우와의 통합으로 문제를 더 빠르게 해결

- AWS & Azure에서 100개 이상의 서비스 지원
- 클라우드 구성을 위한 600개 이상의 모범 사례 룰
- 규정 준수: AWS Well Architected Framework, PCI, HIPAA, NIST, GDPR, CIS, ISO-27001, User-defined
- 자동 교정 기능이 있는 70개 이상의 제어 기능이 포함된 단계별 교정 프로세스 지원

클라우드 인프라의 안전한 구성에 대한 보안관리 및 감사

Cloud One™ Network Security



- 네트워크 환경에 최적화 (AWS Transit Gateway, GWLB)
- 취약점에 대한 가상 패치, 위협 및 C&C 트래픽 탐지 및 차단
- 네트워크 구성의 변경을 최소화하여 빠르게 인라인 구성 가능한 유연한 구성
- 단일 인스턴스로 최대 10Gbps의 네트워크 성능 지원

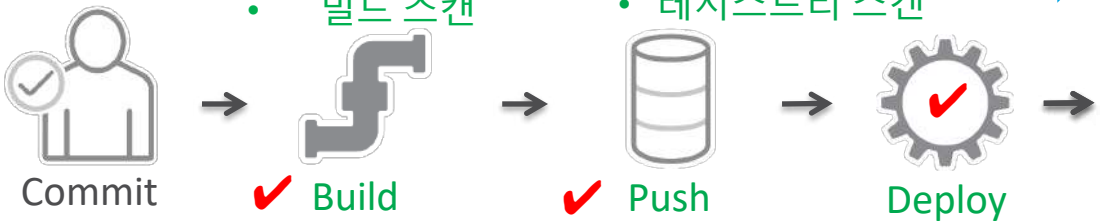
전체 VPC 와 클라우드 네트워크 세그먼트를 신속하게 보호

멀티 | 하이브리드 클라우드 보안 - Cloud One™

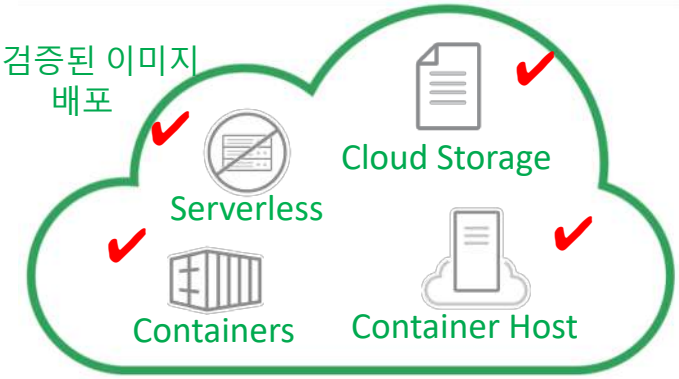
- 취약점 감지 및 수정
- 악성코드 탐지
- 비밀 / 키 찾기
- 규정 준수 평가

- 잘못된 구성으로 부터 보호
- 악성 파일 업로드 차단

Applications Eg. Images and Functions



- 빌드 스캔
- 레지스트리 스캔
- 검증된 이미지 배포

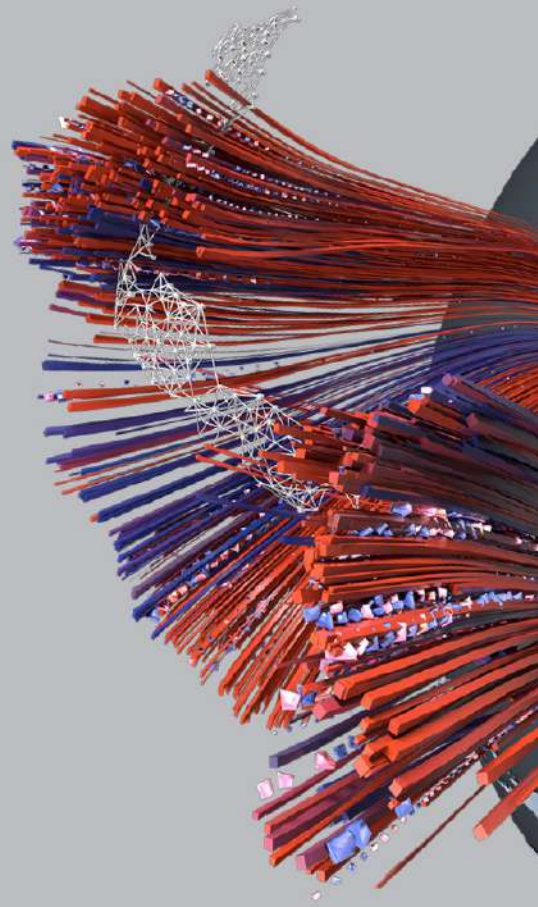


Infrastructure as Code Eg. Cloud deployment templates

- 클라우드 리소스 구성 검증
- 자동 수정

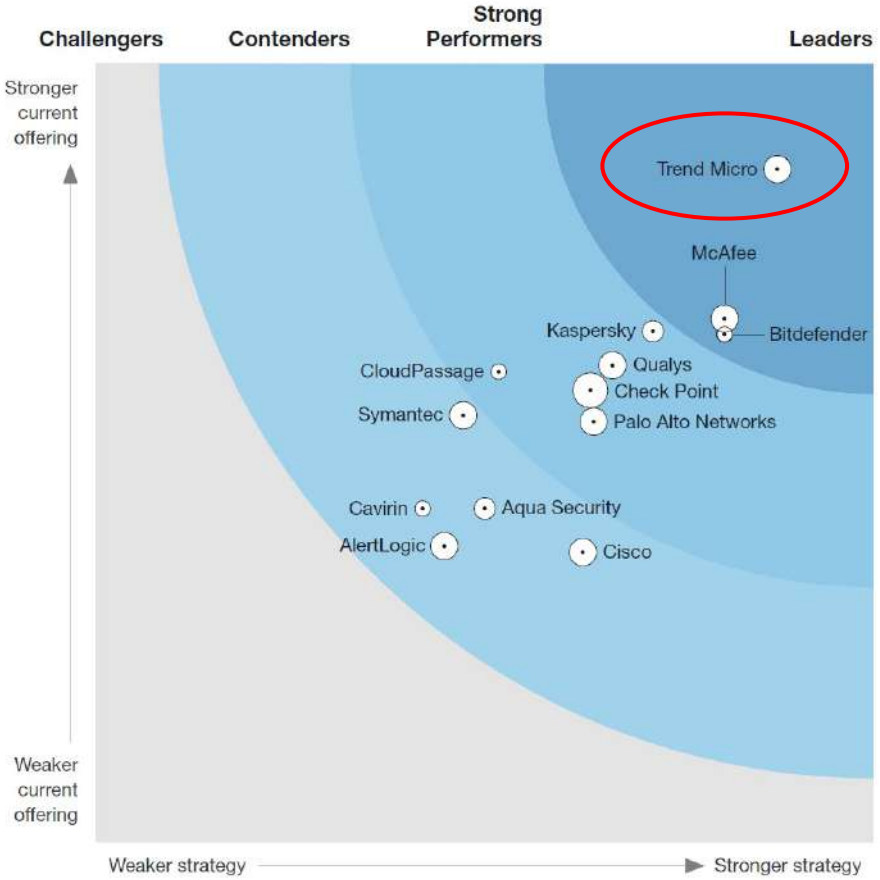
- 컨테이너 호스트 보호
- 컨테이너 플랫폼 보호
- 서버리스 애플리케이션 보호

클라우드 보안 리더



The Forrester Wave™: Cloud Workload Security, Q4 2019 에서 제품과 전략 부문에서 최고 점수로 최상위 리더 선정

FORRESTER®



Source: The Forrester Wave™: Cloud Workload Security, Q4 2019
by Andras Cser with Merritt Maxim, Matthew Flug, and Peggy Dostie

Free Report Available Here:
https://resources.trendmicro.com/Forrester-Cloud-Workload-Leadership-Report.html

TREND MICRO

Gartner®

Market Guide for Cloud Workload Protection Platforms

7 of 7

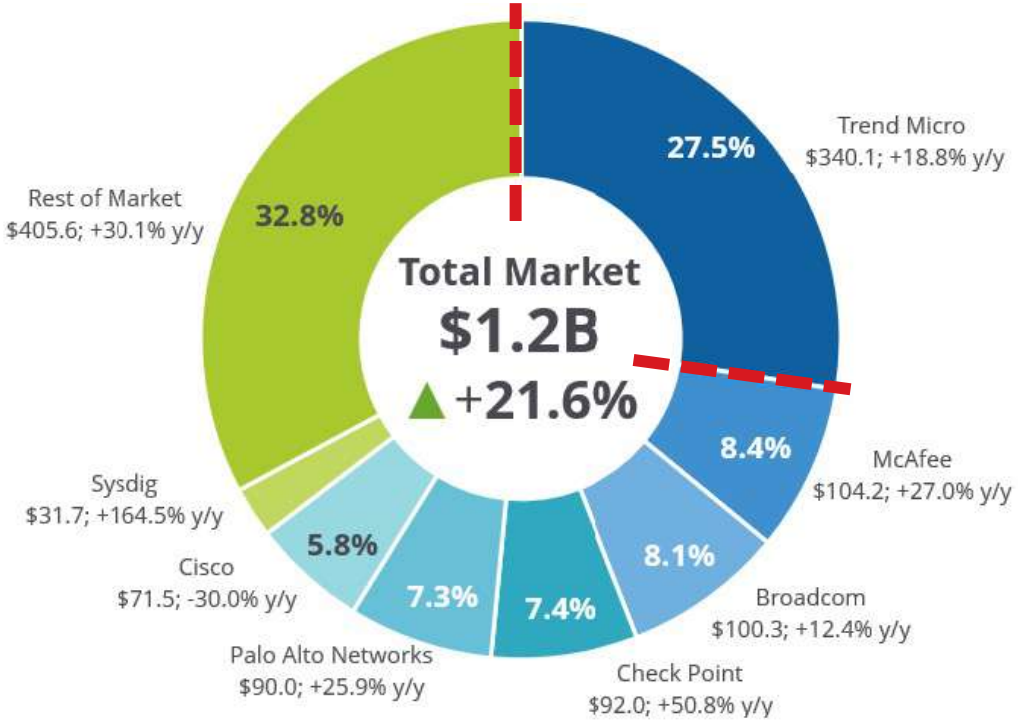
Core Controls*

Trend Micro가 모든 보안 공급업체 중 가장 많은
클라우드 보안 제어 및 기준을 제공함*

Based on Trend Micro's assessment of Gartner 2019 Market Guide for Cloud Workload Protection Platforms; April 2019 | G00356240 | Neil MacDonald.

TREND MICRO

CWPP #1 Market Share



하이브리드 클라우드
워크로드 보안 시장

점유율 1위 27.5%

IDC ANALYZE THE FUTURE

Source: IDC, Worldwide Hybrid Cloud Workload Security Market Shares, 2020: Time to Shift Left, June 2021

TREND MICRO

TREND MICRO™

THE ART OF CYBERSECURITY

The global shift of Trend Micro customers from on-premises to SaaS-based security. **Created with real data by artist Brendan Dawes.**