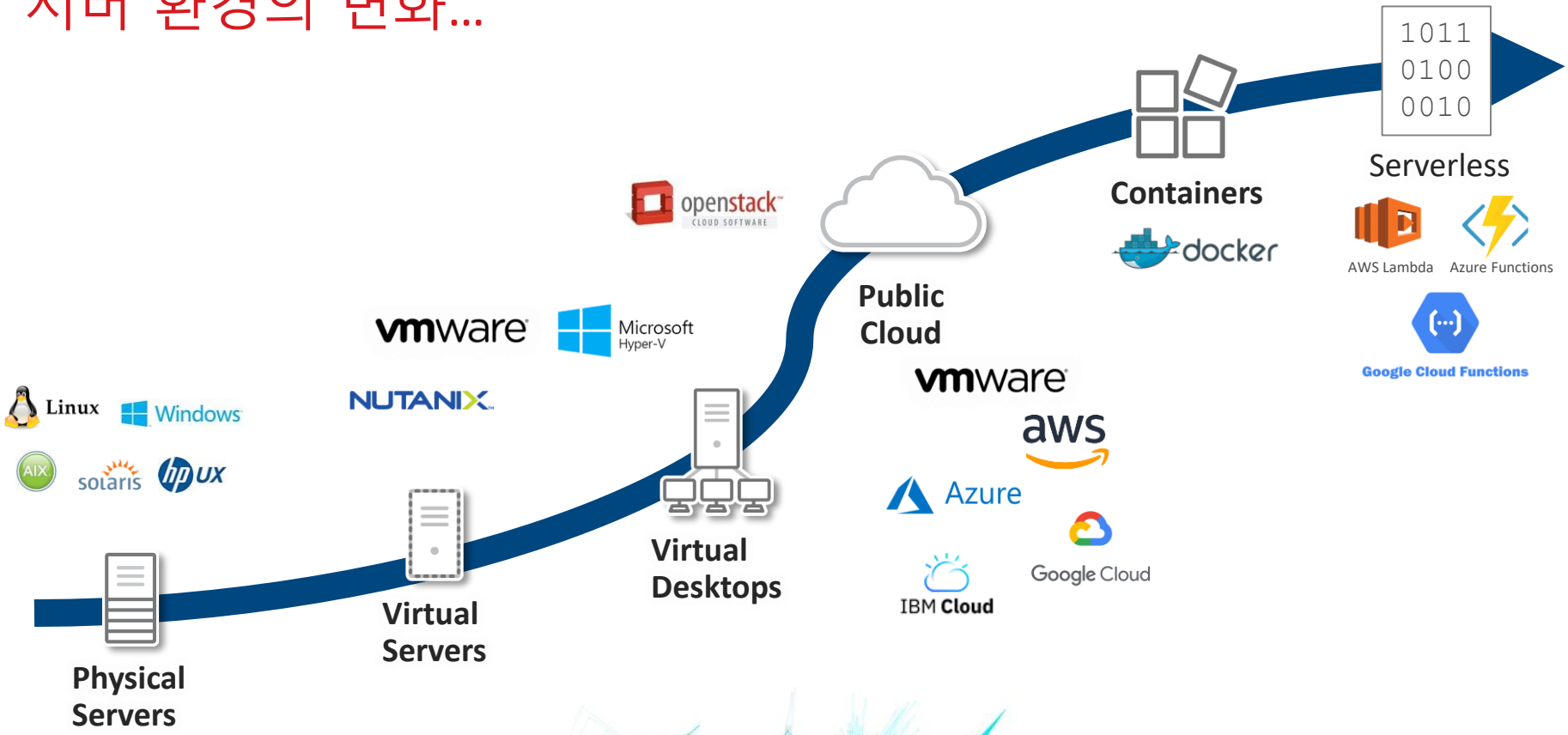
DevOps를 위한 CI/CD 파이프라인 보호

효과적인 DevSecOps 구현

TREND MICRO

서버 환경의 변화...



애플리케이션, 서비스 환경의 변화…

It’s a Hybrid Cloud World

Existing Applications = Cash Cow

New Applications = Growth

Physical Servers

Virtual Servers

Cloud Instances

Containers

Serverless

Data Centers

Cloud

TREND MICRO

애플리케이션, 서비스 환경의 변화…

ESG Whitepaper, Leveraging the Agility of DevOps Processes to Secure Hybrid Clouds, 2018

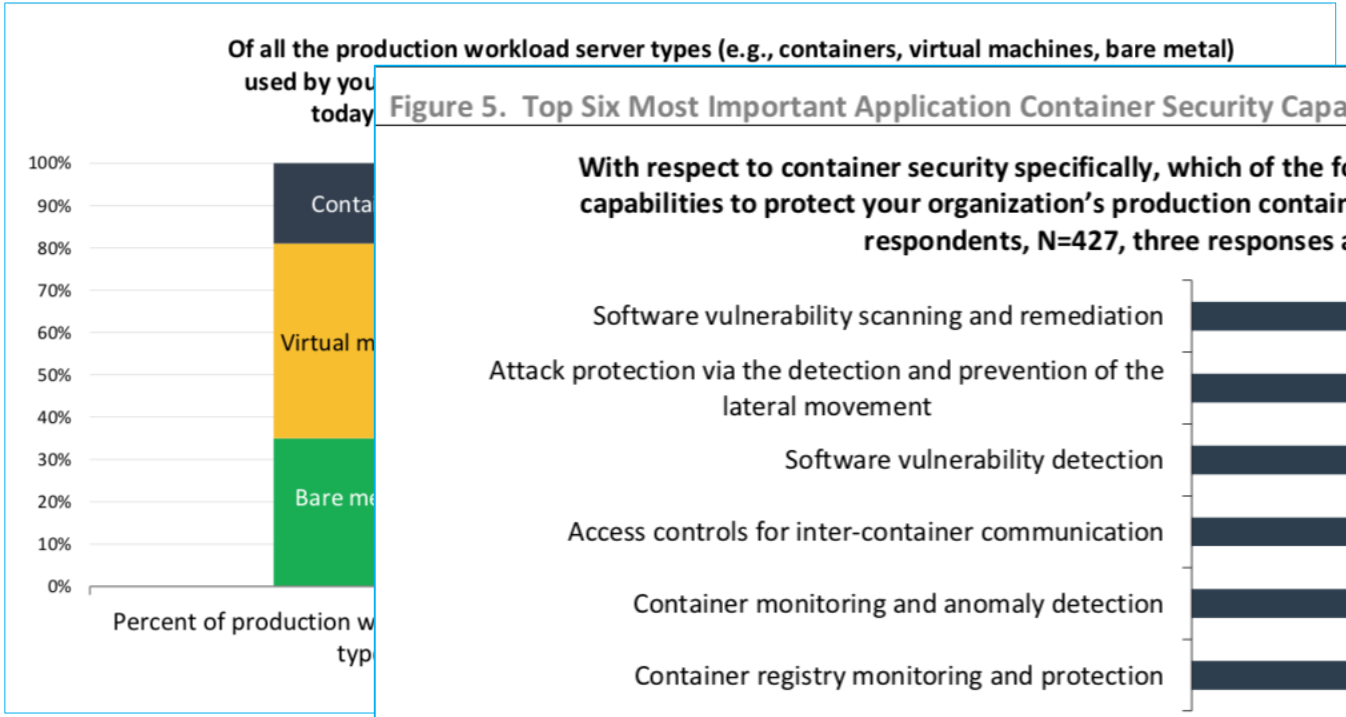
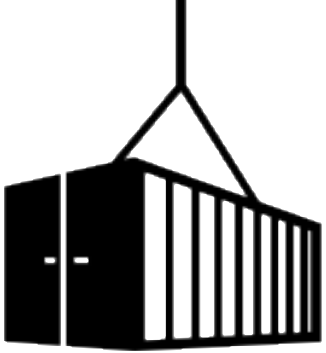


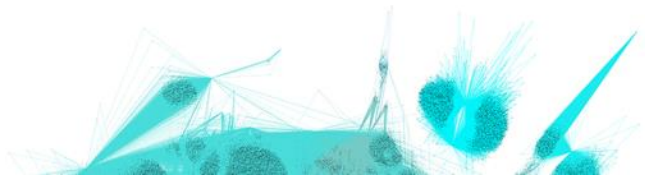
Figure 5. Top Six Most Important Application Container Security Capabilities

With respect to container security specifically, which of the following are the most important capabilities to protect your organization's production containerized applications? (Percent of respondents, N=427, three responses accepted)

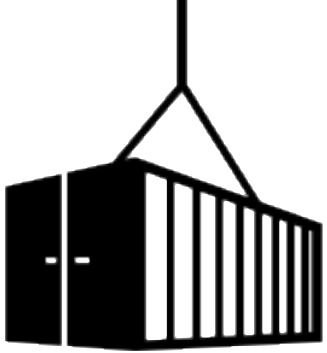
Source: Enterprise Strategy Group

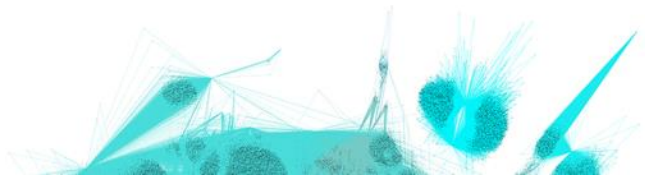
컨테이너 기반 애플리케이션 증가



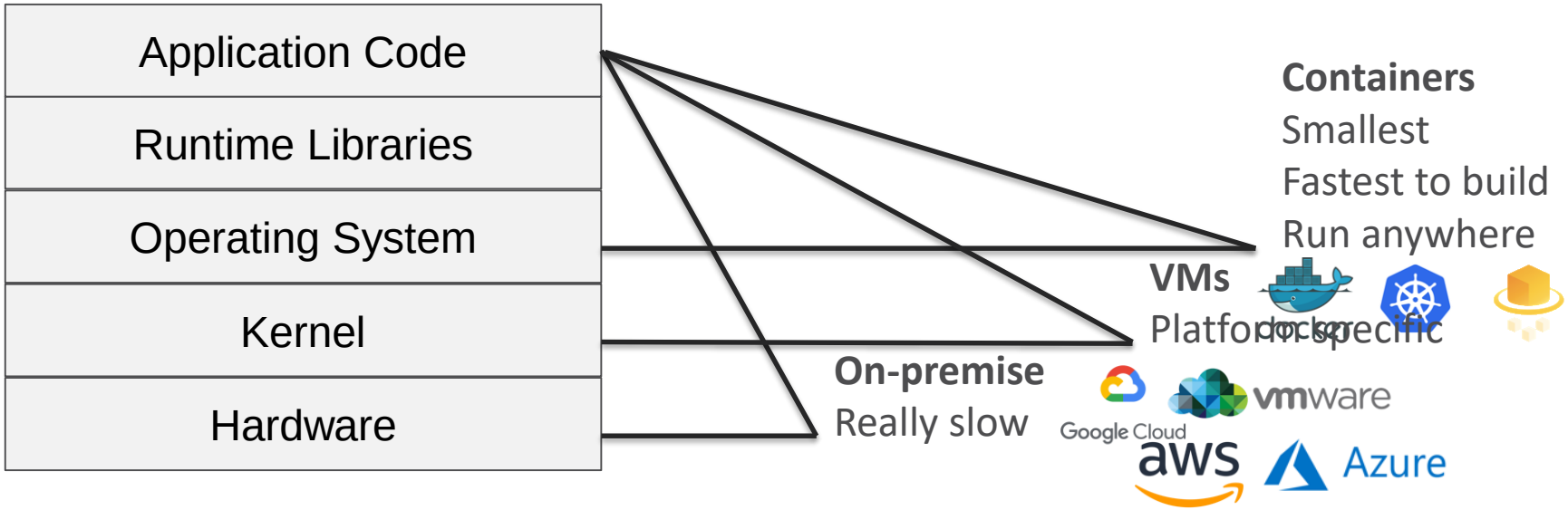


컨테이너 기반 애플리케이션 증가





컨테이너 기반 애플리케이션의 장점



보안 요구사항 for 하이브리드 클라우드

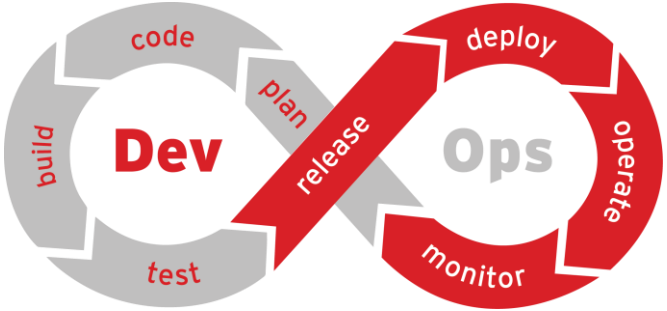
Pipeline Management & Deployment

GitHub
Jenkins
ANSIBLE
CHEF
puppet
SALTSTACK
kubernetes
PowerShell
AWS OpsWorks

IT Service Management

slack
Jira Software
now
Amazon SNS

Automation With Pipeline & Workload Security



Environments

aws
Azure
Google Cloud
docker
RED HAT OPENSHIFT
vmware

Monitoring Tools

New Relic.
AWS CloudTrail
AWS Config

TREND MICRO

DevOps

계획되지 않은 작업을 유발 - **보안 및 규정 준수 요구 사항 증가**

보안이 **시간을 늦추고...**

클라우드 or 배포 모델에 **최적화되지 않거나 호환되지 않는** 보안 도구

PAIN!

규정을 준수하고 보안 요구 사항을 충족시키기 위해 다시 작업하는 데 **너무 많은 시간 낭비**

PAIN!

보안 구현이 어렵고 자동화 되지 않아 **Time -to-Market 목표를 달성하지 못함**

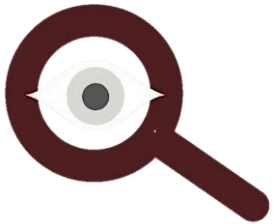
PAIN!

다양한 클라우드 환경지원과 높은 보안성 때문에 **작업을 간소화 할 수 없음**

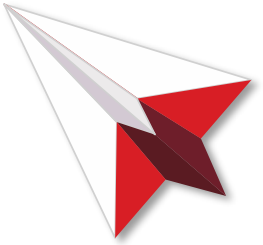
TREND MICRO

클라우드 네이티브 보안

Visibility



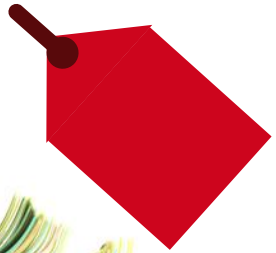
Agility



Sec
Dev Ops

Compliance

Purchasing



클라우드 네이티브 보안

DevOps Wants To…

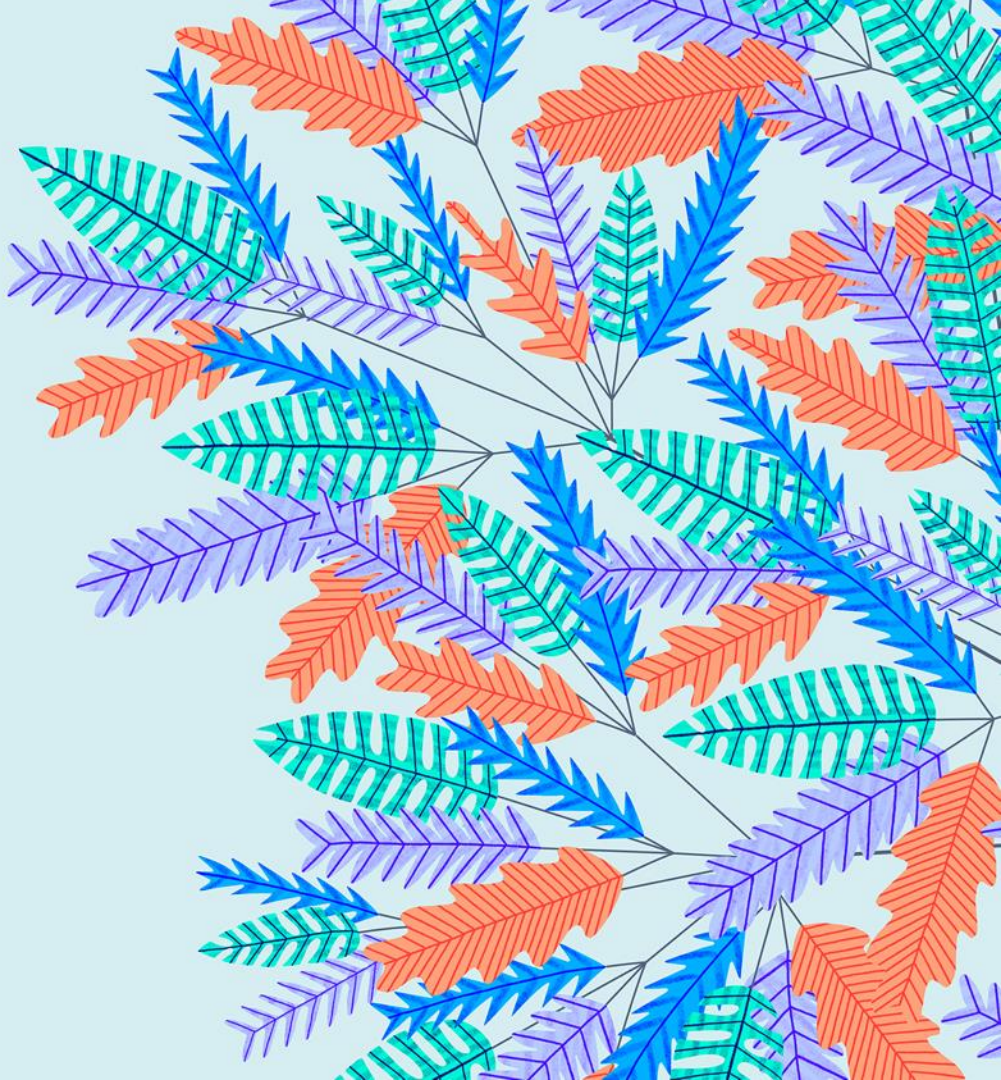
안전한 이미지 빌드
빌드 이미지에 대한 보안성 체크

빠른 이미지 배포
이미지에 대한 보안성 체크로 인한 속도저하 없어야

어디서나 이미지 실행
다양한 클라우드, 도커환경에서 실행 가능

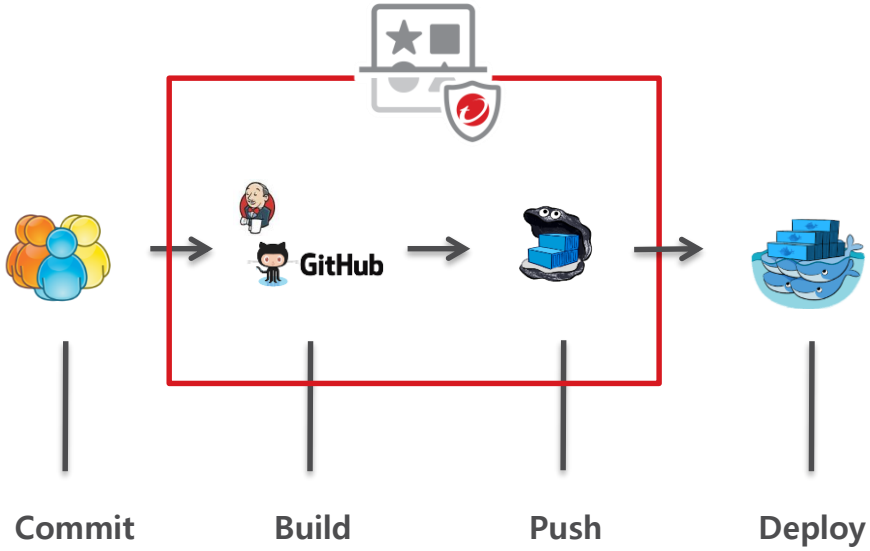
TREND MICRO™

Deep Security Smart Check



Deep Security Smart Check

도커 컨테이너 Build Pipeline 원활한 보안 적용

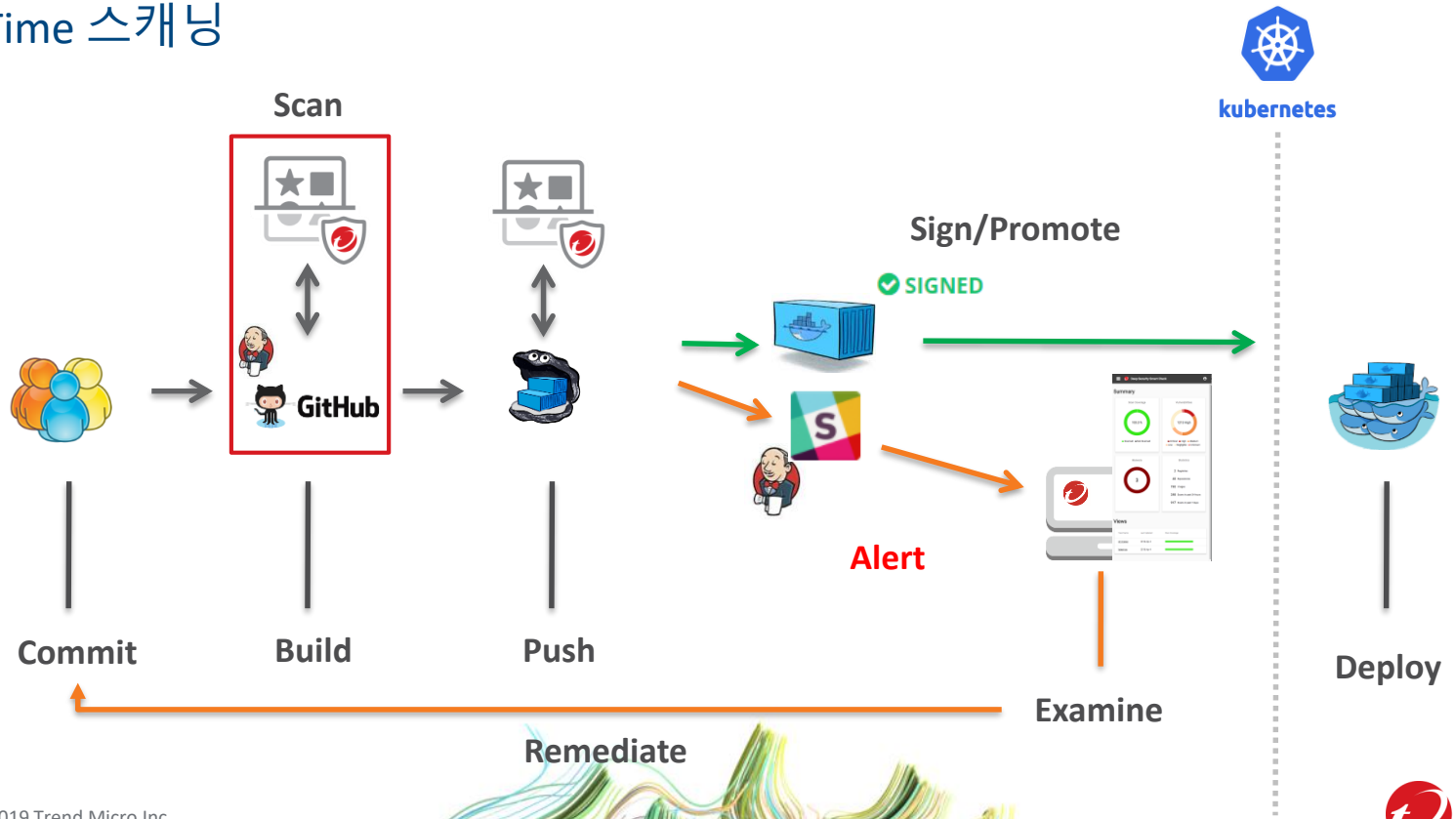


- 취약점 검사
  - 로컬 및 원격 익스플로잇
- 멀웨어 탐지
  - 패턴기반 + 머신러닝(Pre-excution)
- 지속적인 스캔(Continuous Scan)
- 스캔 상세 로그
- 자동화

Runtime을 위한 안전한 이미지 보장

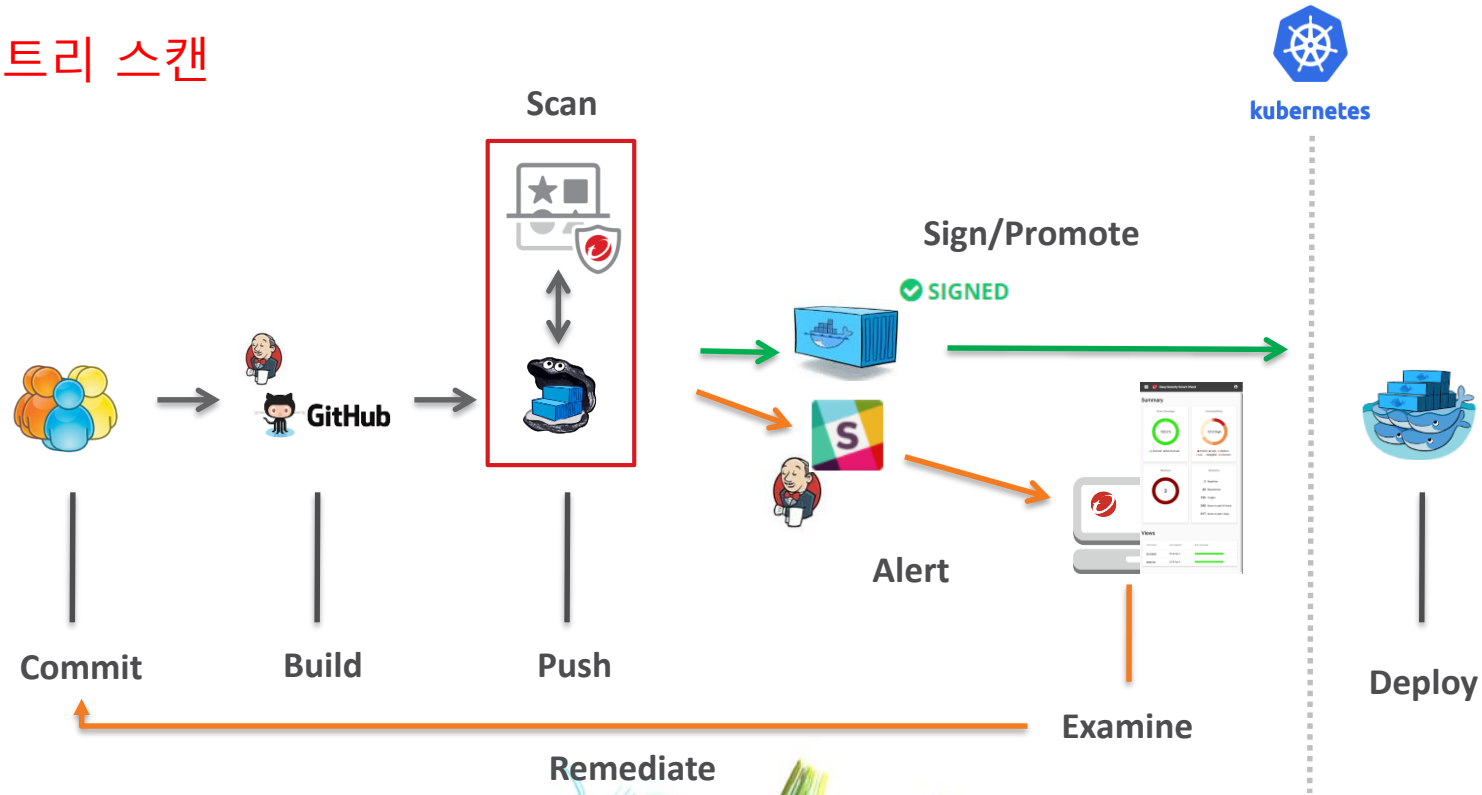
CI/CD Pipeline 통합

Build Time 스캐닝



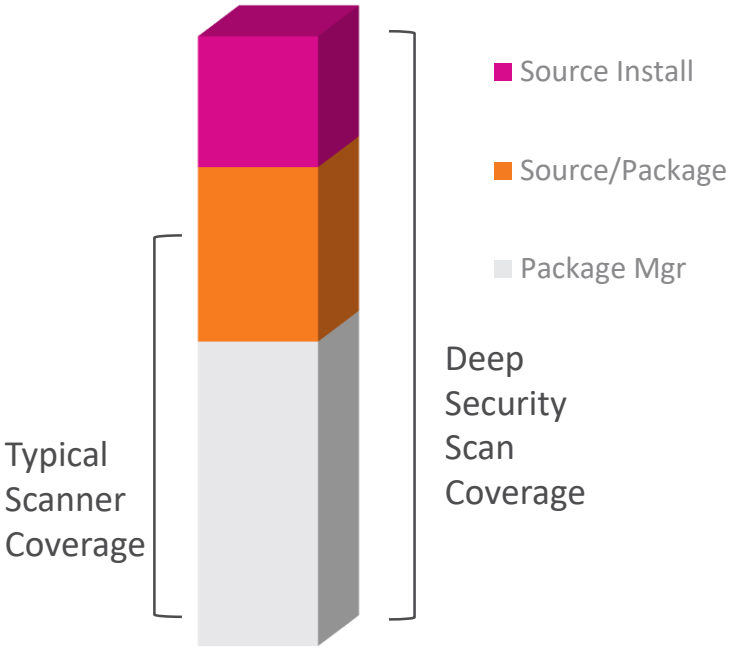
CI/CD Pipeline 통합

레지스트리 스캔

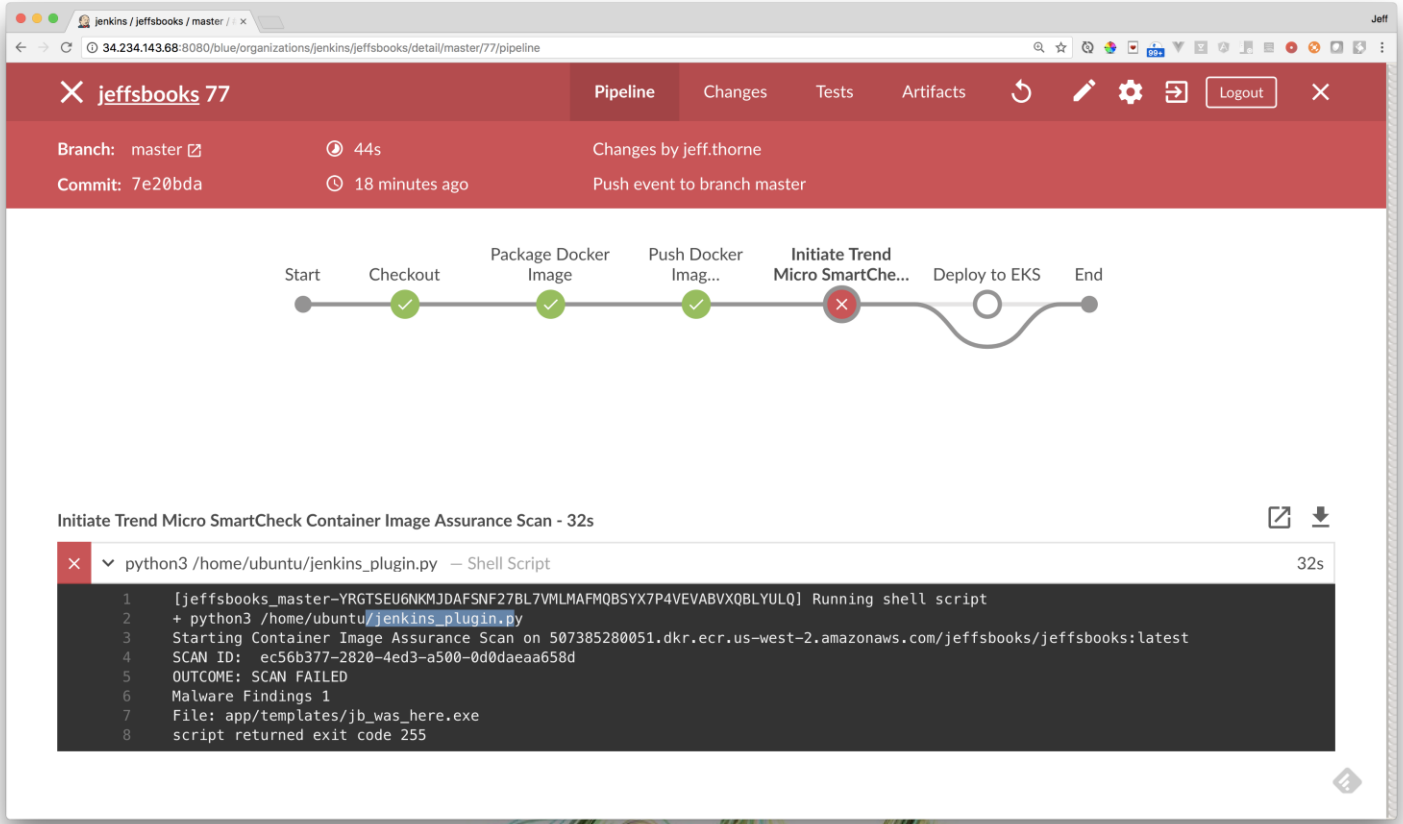


취약점 스캔 범위

- 보안, 컴플라이언스 검사
- 로컬/원격 취약점 검사
- 위협인텔리전스 기반 실시간 위협 검사
- 패키지 관리 애플리케이션 감지
- + 애플리케이션 감지 기능
  - Wordpress
  - Drupal
  - Fluentd
  - PostgreSQL
  - Ruby
  - Tomcat



Jenkins Pipeline 통합



“DevOps” & “개발팀” 을 위한 이미지 문제점 상세정보 제공

이미지에서 위험도가 높고 취약점을 내포한 패키지 정보

패치는 가능여부

취약점 상세 정보

상세 패치 정보

Deep Security Smart Check

Vulnerabilities:

Legend:

- Fix available in newer version
- Fixed in a subsequent layer

Package	Severity	Vulnerabilities
glibc 2.19-18+deb8u9	high	CVE-2014-9761, CVE-2017-1000366, CVE-2017-1000408, CVE-2017-16997, CVE-2017-8804, CVE-2018-1000001, CVE-2018-6485
	medium	CVE-2016-10228, CVE-2017-1000409, CVE-2017-12132, CVE-2017-12133
	low	CVE-2015-5180, CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2018-11236, CVE-2018-11237
	negligible	CVE-2010-4051, CVE-2010-4052, CVE-2010-4756, CVE-2015-8985
	unknown	CVE-2017-18269
ncurses 5.9+20140913-1	high	CVE-2017-10684, CVE-2017-10685
	medium	CVE-2017-11112, CVE-2017-11113, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-16879
	low	CVE-2018-10754

CVE-2017-12132

debian

Name	CVE-2017-12132
Description	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, bugtraq, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, Mageia, GitHub code/issues, web search, more)
NVD severity	medium (attack range: remote)
Debian Bugs	870650

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
eglibc (PTS)	wheezy	2.13-38+deb7u10	vulnerable
	wheezy (security)	2.13-38+deb7u12	vulnerable
glibc (PTS)	jessie (security), jessie	2.19-18+deb8u10	vulnerable
	stretch	2.24-11+deb9u3	vulnerable
	stretch (security)	2.24-11+deb9u1	vulnerable
	buster, sid	2.27-3	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
eglibc	source	(unstable)	(unfixed)	medium		
glibc	source	(unstable)	2.25-1	medium		870650
glibc	source	experimental	2.25-0experimental1	medium		

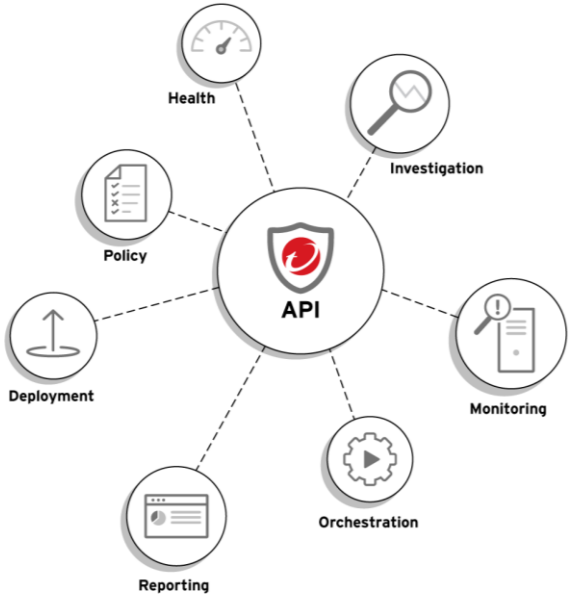
Notes

```
[stretch] - glibc <no-dsa> (Minor issue)
[jessie] - glibc <no-dsa> (Minor issue)
[wheezy] - eglibc <no-dsa> (Minor issue)
https://sourceware.org/bugzilla/show_bug.cgi?id=21361
https://sourceware.org/git/gitweb.cgi?p=glibc.git;h=e14a27723cc3a154d67f3f26e
https://arxiv.org/pdf/1205.4011.pdf
```


TREND MICRO

자동화로 DevOps 파이프라인에서 보안 적용

"보안은 개발에 대한 방해물로 간주되었지만 더 이상은 아닙니다. 우리 팀은 보안이 환경에 내장되어 있음을 잘 알고 있습니다. 보안 팀은 클라우드 운영의 효율성을 높이는 데 도움을 주고 있습니다"- Infor DevOps team



자동화된 보안 - 정책 생성 및 업데이트

배포 자동화 – 전체 워크로드에 보안 적용

모니터링 자동화 – 전체 워크로드의 운영 및 보안 상태

오케스트레이션 자동화 - 파이프 라인 도구, SOAR 도구통합

보고 자동화 - 맞춤형 컴플라이언스 리포트 및 SEIM 통합

파이프라인 & 워크로드 보안 자동화

Pipeline 관리 & 배포 도구

GitHub
Jenkins
ANSIBLE
CHEF
SALTSTACK
puppet
AWS OpsWorks
PowerShell
kubernetes

환경 & 레지스트리

AWS
vmware
docker

관리 & 서비스 도구

slack
now
Jira Software
Amazon SNS
ELK Stack

SIEM 솔루션

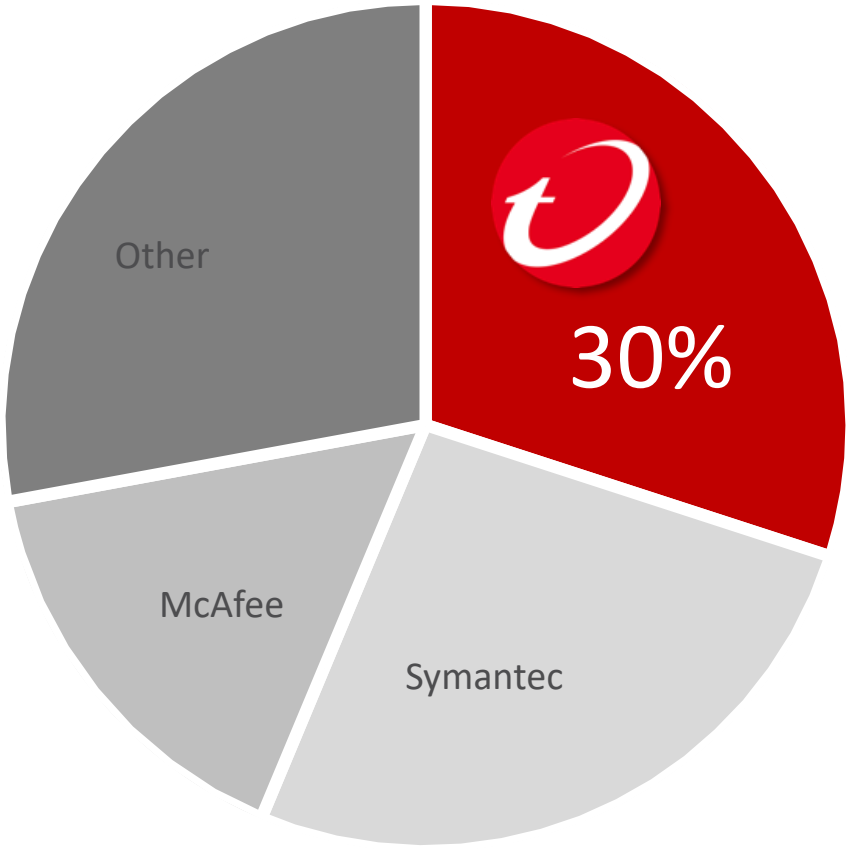
splunk>
sumologic
ArcSight
IBM Radar


Gartner
2018
Market Guide for
Cloud Workload
Protection Platforms
23 of 26
capabilities &
considerations
Trend Micro delivers the
most cloud security
controls of all security
vendors evaluated

The MARKET LEADER

in server security for 8 straight years

IDC
Analyze the Future



Source: IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116

TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**