하이브리드 데이터센터를 위한 마이크로세그멘테이션

vARMOUR

vARMOUR AT A GLANCE

2011
FOUNDED IN US

150
EMPLOYEES

$29B
MARKET OPPORTUNITY

24
PATENTS

FINANCIAL SERVICES | SERVICE PROVIDERS | CRITICAL INFRASTRUCTURE

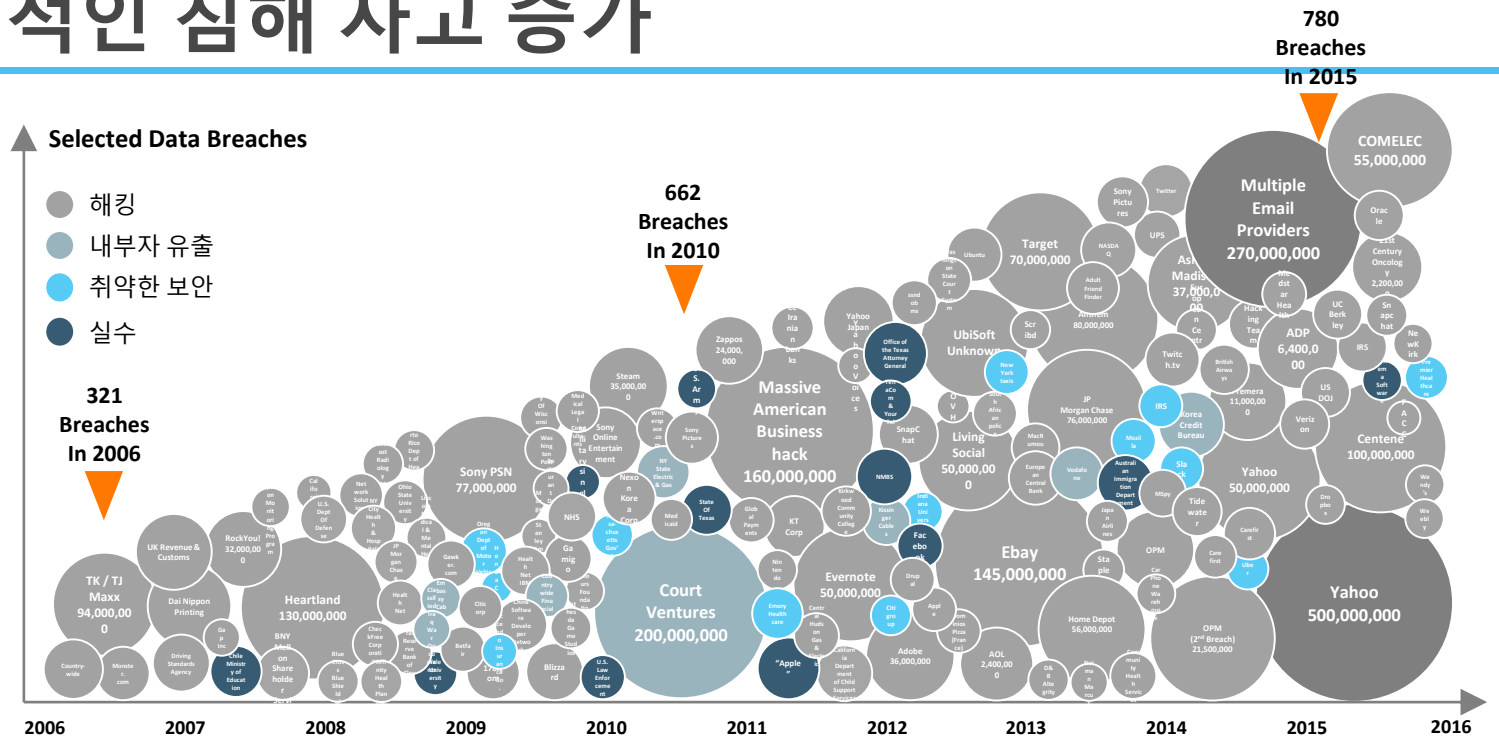
$82.4M
FUNDING

24
PATENTS PENDING

1
HOUR
TO DOWNLOAD,
INSTALL & SEGMENT

400+
USERS*

지속적인 침해 사고 증가



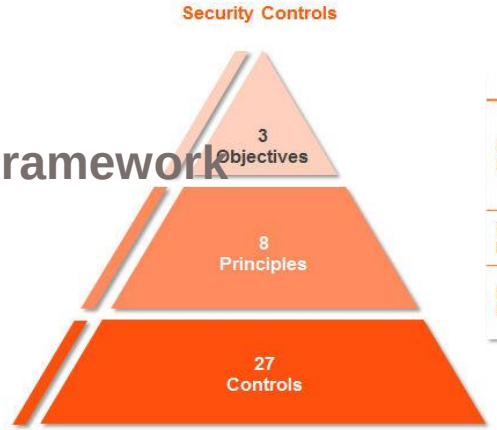
지속적인 공격과 위협으로 2009년 이후 사이버 보안 지출 두 배 이상 증가

Source: Identity Force, DataBreaches.net, IdTheftCentre, informationisbeautiful.net, press news reports and Risk Based Security (Data Breach QuickView report, February 2014) TIA's 2010-2017 ICT Market Review and Forecast

국제 보안 정책 환경 변화

- 유럽 개인정보보호법
  (GDPR-General Data Protection Regulation)
- 2018.05.25부터 시행

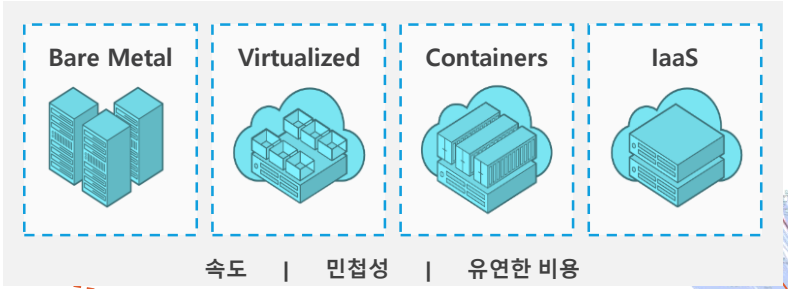
- Customer Security Controls Framework
  SWIFT 2017년 3월 발표
- 2018년 1월부터 감사 시행

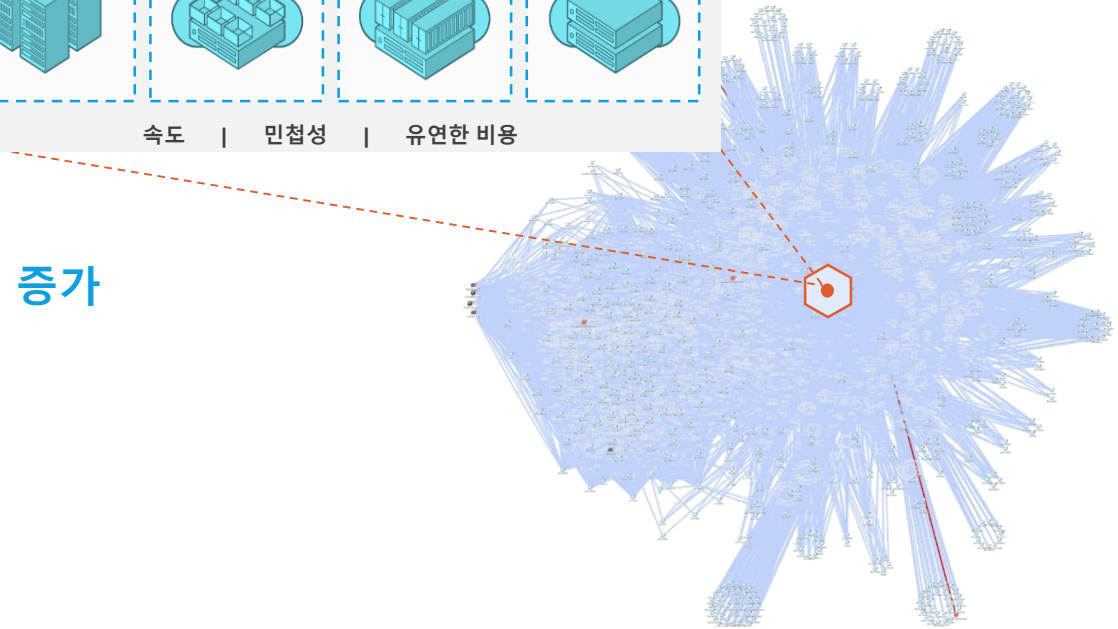


SWIFT Customer Security Controls Framework

Secure Your Environment	1.	Restrict Internet access
	2.	Protect critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

데이터센터 환경 변화

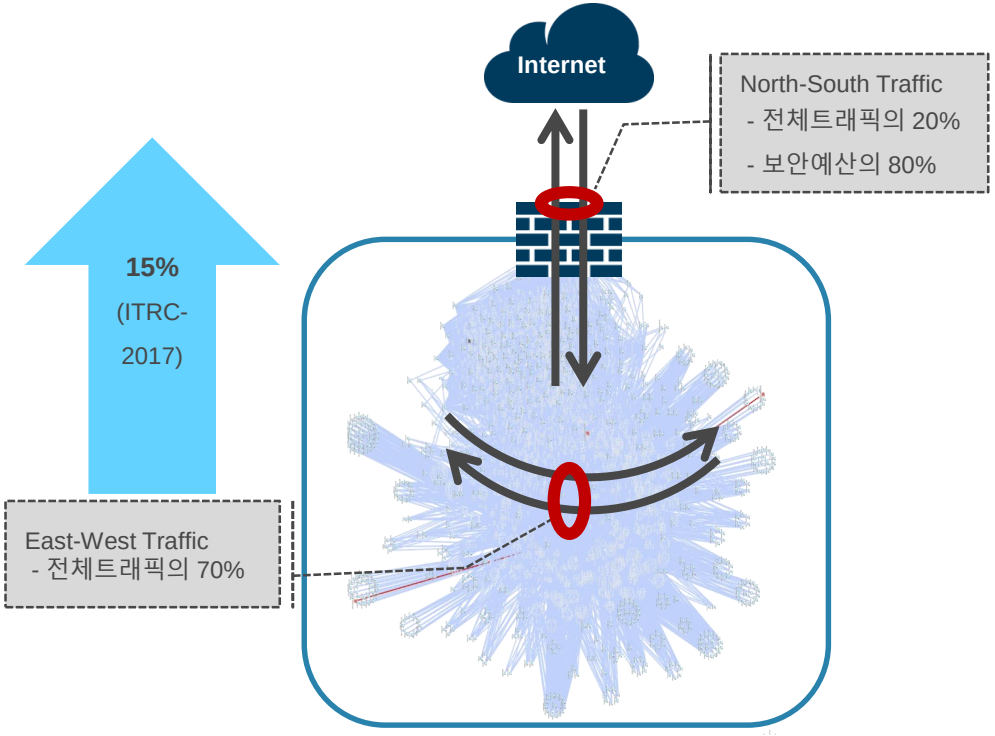




- **하이브리드 클라우드 환경의 증가**
  - **베어메탈/가상서버/컨테이너 등**
- **대용량의 내부 트래픽 발생**
  - 내부 East-West 트래픽 증가
- **관리의 애로사항 증가**
  - 혼재 환경과 내부 트래픽 증가에 따른 보안 위협 요소 증가

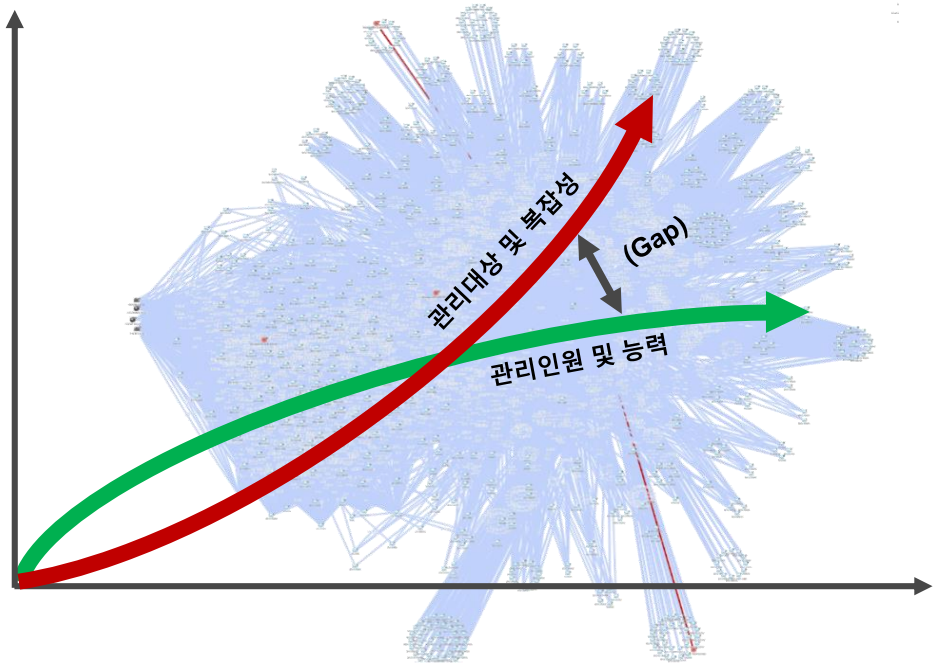
데이터센터 환경 변화

- 다양한 인프라가 혼재된 환경
  - 베어메탈/가상서버/컨테이너 등
- **대용량의 내부 트래픽 발생**
  - **내부 East-West 트래픽 증가**
- 관리의 애로사항 증가
  - 혼재 환경과 내부 트래픽 증가에 따른 보안 위협 요소 증가



데이터센터 환경 변화

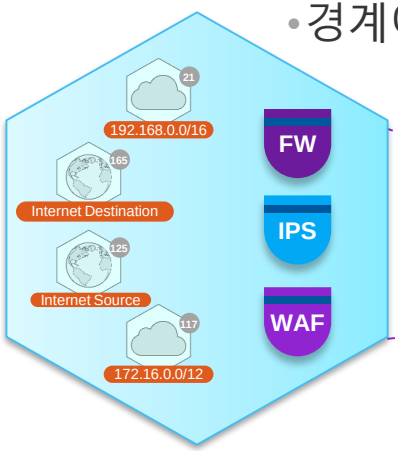
- 다양한 인프라가 혼재된 환경
  - 베어메탈/가상서버/컨테이너 등
- 대용량의 내부 트래픽 발생
  - 내부 East-West 트래픽 증가
- **관리의 애로사항 증가**
  - **혼재 환경과 내부 트래픽 증가에 따른 보안 위협 요소 증가**

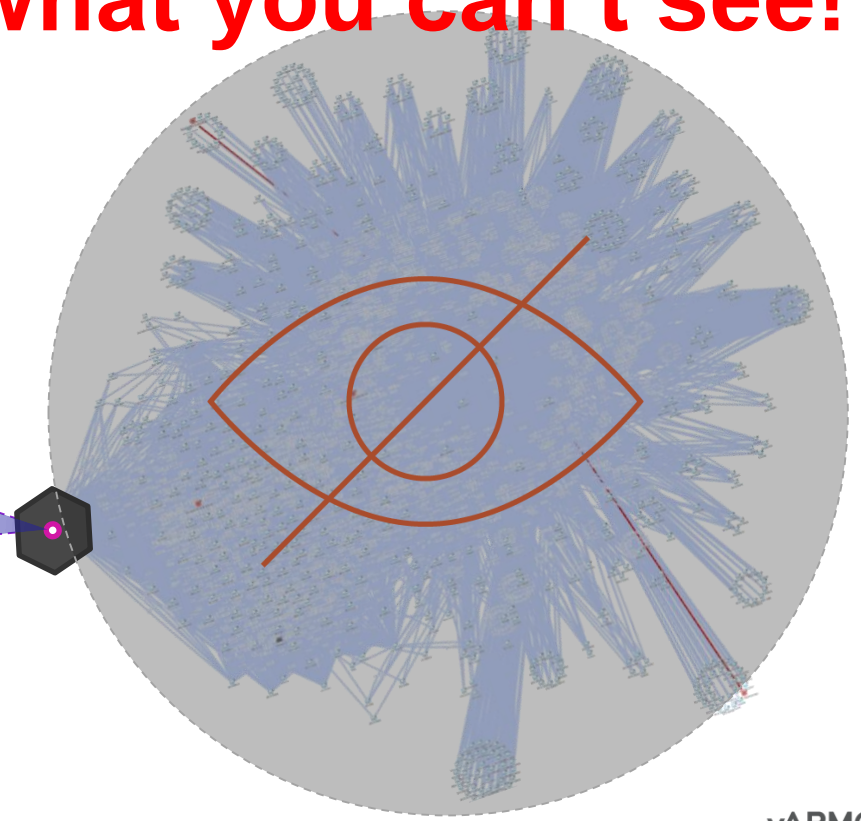


기존 보안시스템의 한계

You can’t secure what you can’t see!

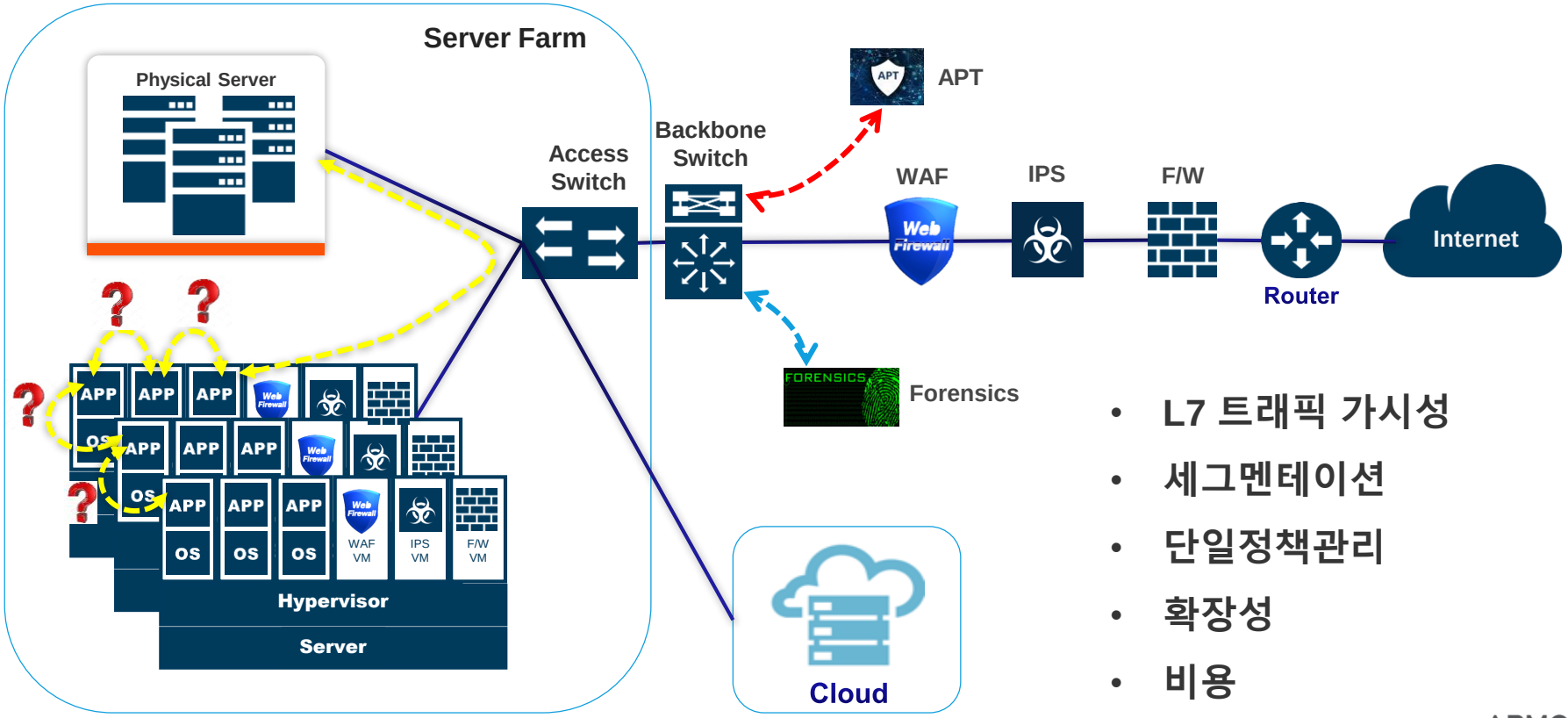
- 경계에 집중 보안





기존 보안시스템의 한계

하이브리드 환경에서 가상환경에 대한 보안적용 방안의 한계



- L7 트래픽 가시성
- 세그멘테이션
- 단일정책관리
- 확장성
- 비용

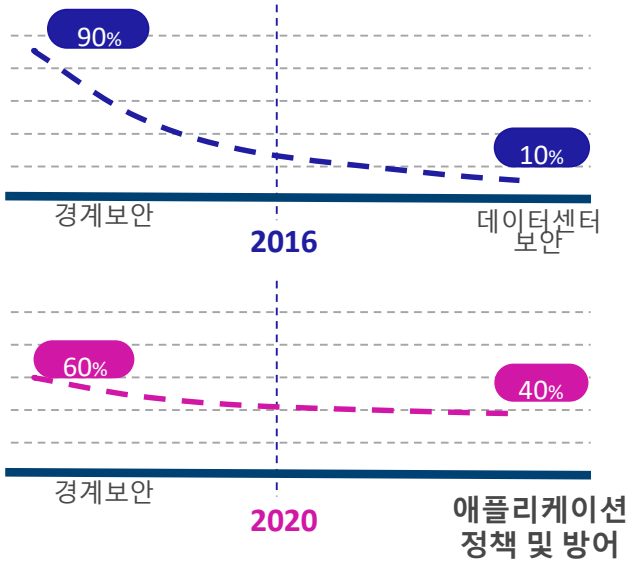
빠르게 성장하고 있는 마이크로세그멘테이션 보안

애플리케이션 정책 및 보호는 마이크로세그멘테이션과 같이 높은 우선 순위 해결

Gartner says top security priority

- 대부분의 IDC는 아직 마이크로세그먼테이션 기능 및 **가상 자산을 분할하고 보호해야 할 필요성을 인지하지 못하고** 있으며, 게다가 **기존은 낮은 효율성과 확장성을 기반으로 운용**하고 있기 때문에 마이크로 세그먼테이션은 가상화 된 데이터 센터의 **보안에서 최우선 과제**가 되었습니다.
- 기관 및 회사는 다양한 보안 제품을 운용중이며 이로 인해 복잡한 인프라를 갖추고 있습니다. **마이크로세그멘테이션을 구현하는 새로운 솔루션은 3th Party 제품과 경쟁하지 않고 통합**되어야 합니다. "
- 가상화 데이터센터에서 마이크로세그멘테이션을 위한 제품 비교
- **Published:** 29 June 2017
- Gartner, Inc.

SDDC에서 변화되는 보안투자



총 시장 규모 : 3조원 규모

년평균 성장율 : ~12%

Source: IDC, Frost & Sullivan.

자산에 대한 인식 변환

클라우드 환경에서 관리 대상의 모든 애플리케이션을 자산으로 인식

IP 기반 하드웨어

네트워크 장비

서버 장비

보안 장비

네트워크 레벨의 트래픽 가시성

소프트웨어

웹

애플리케이션

워크로드

DB

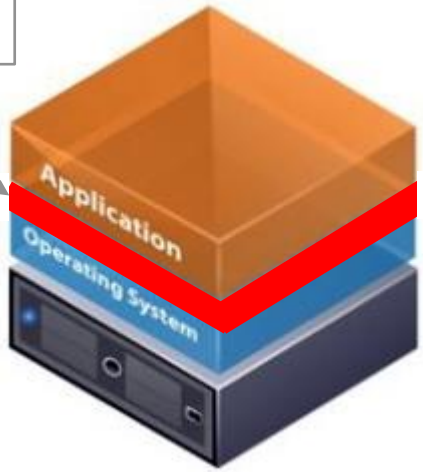
애플리케이션 레벨의 트래픽 가시성

가상화 환경에서 보안 적용 이슈

하이브리드 환경에서의 보안 적용 시 성능에 대한 이슈 증가

AV, DRM, DLP, 서버보안, 자산관리 SW 등

보안 및
관리 솔루션



단일 시스템 단일 리소스 점유

Agent or S/W…?

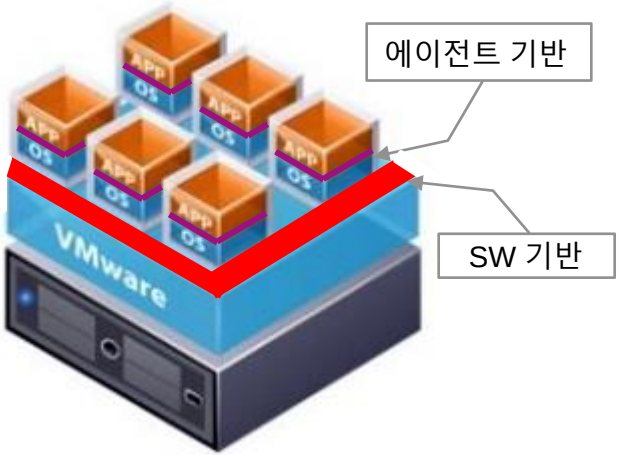
AV, DRM, DLP, 서버보안, 자산관리 SW 등

+

F/W, IPS, WAF, VM관리 SW 등

에이전트 기반

SW 기반



단일 시스템 복수 리소스 점유

향후 보안 이슈 사례

SWIFT 고객 보안 통제 프레임워크

1. 보안 영역에 속한 모든 구성 요소와 통신 식별
2. 모든 구성 요소가 매핑되고 외부와의 모든 연결에 대한 흐름을 명확하게 이해
3. 매핑이 완료된 후 관리자는 규정에 따라 정책 세분화 및 시행
4. 모든 데이터 감사부서에 제공

SWIFT Customer Security Controls Framework

Secure Your Environment	1.	Restrict Internet access
	2.	Protect critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

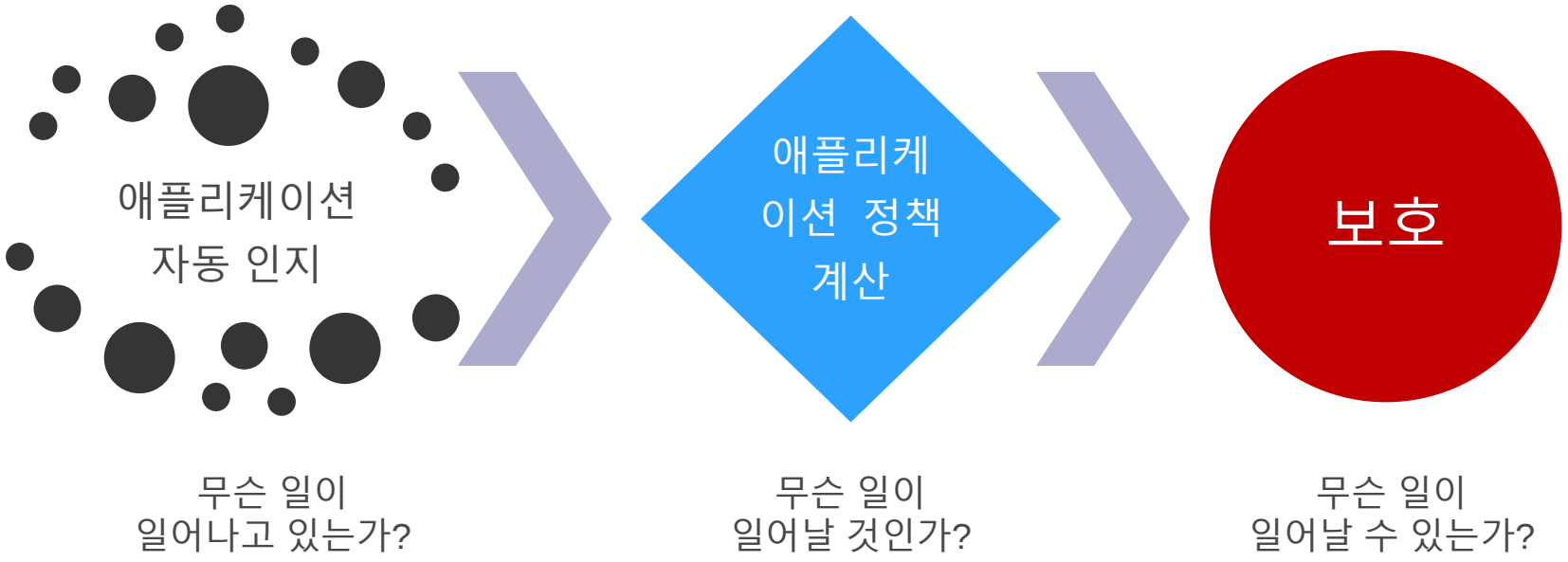
네트워크를 세분화하여 일반IT에서 SWIFT 관련 서버에 대한 접근 제한

vARMOUR

- 하이브리드 클라우드 및 데이터센터에 통합 보안 서비스를 제공하는 최초의 분산 플랫폼
- 가상화 환경에 특화되어 애플리케이션 및 트래픽에 대한 가시성 제공 및 제어를 하는 마이크로세그멘테이션 기반 L7 방화벽

애플리케이션 정의 보안

하이브리드 환경에서의 애플리케이션 가시성 및 제어

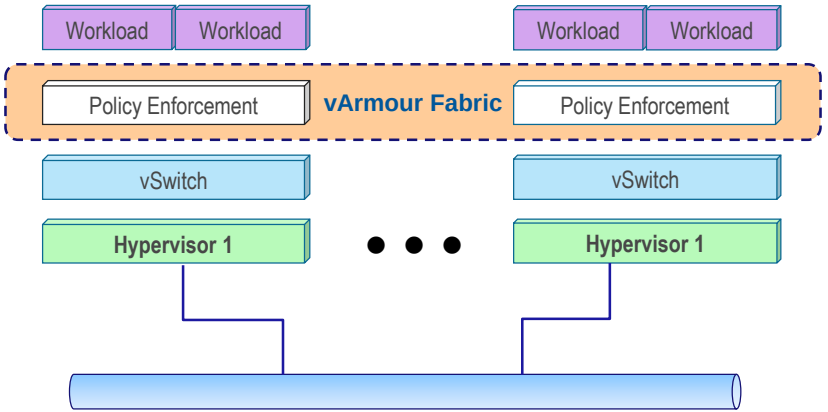


심플 – 애플리케이션 중심 – 하이브리드 클라우드 보안

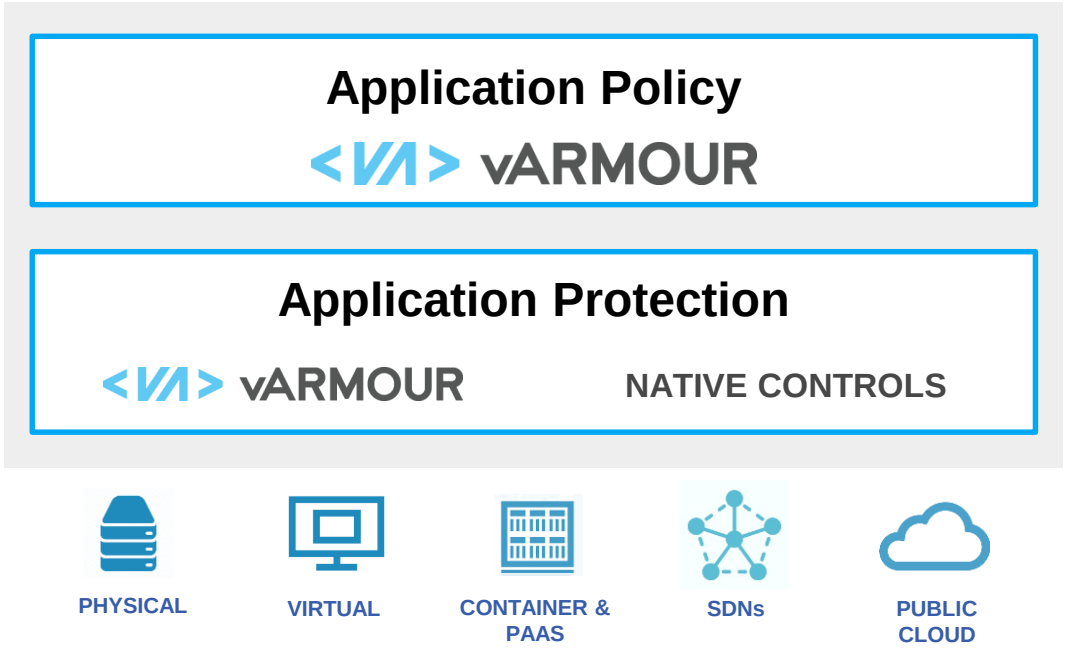
vArmour DSS 개요

vArmour DSS 는 데이터센터 및 클라우드 시스템 전반에 걸쳐 적용되는 소프트웨어 기반의 분산보안시스템으로 애플리케이션 레벨의 가시성 제공 및 중앙 집중 정책 제어를 제공.

- 네트워크 변경 필요 없음
- 애플리케이션 인식 마이크로세그멘테이션
- 중앙 집중 관리
- 전체 7계층 트래픽에 대한 가시성 제공
- API-중심 통합
- 최소(60분 이내)의 설치 시간



vArmour 정책 관리 및 적용



애플리케이션 정책 서비스 관리:

멀티 클라우드 전반에 걸친 애플리케이션 및 데이터의 가시성 제공 및 제어

Application Policy – Key Questions

1 **누가 중요한 애플리케이션 및 데이터를 사용하고 있는가?**

- 모든 애플리케이션에서 가장 민감한 요소는 모니터링 및 보안솔루션과 떨어져 있는 것
- 클라우드와 컨테이너는 가시성 및 제어의 문제 내포

2 **중요 시스템에 대한 오용을 막을 수 있는가?**

- 침입 방지는 권한이 없거나 악의적인 사용자를 예방하는 것을 의미
- 보안 정책은 VLAN이나 IP주소가 아닌 애플리케이션과 사용자에 대한 정책

3 **하이브리드 클라우드 환경에서 애플리케이션을 보고 제어 할 수 있는가?**

- 애플리케이션은 더 이상 고정되어 있지 않고 클라우드로 확장 또는 마이그레이션
- 애플리케이션 상호 의존성은 클라우드 환경에서 더 복잡

주요 관점

침입을 방지하려면 공격자가 목표로 하는 자산,
즉 중요한 **애플리케이션과 데이터에 대한 가시성 및 제어**가 필요하다.

중요 애플리케이션에 대한 사용 및 오용 이해

중요 자산 보기…

Critical Apps

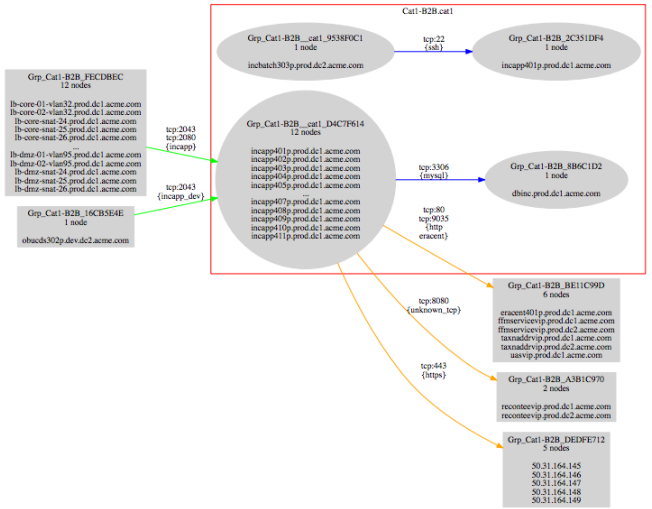
Finance/billing; critical systems (e.g. EPIC; SWIFT; SCADA; etc)

Critical Data

Data repositories: Databases; fileshares; etc

Critical IT Systems

Active Directory; Domain Controllers; DNS; NMS; etc



상호 연결 관계로 애플리케이션 시각화

– 일부 유효한 경우 일부 유효하지 않음

…누가 사용하고 있는가?

Users

Internal or external users; grouped by access

External apps

Third party systems; other apps in the environment

Vulnerable systems

Vulnerable communications; unpatched / old systems

Application Protection – Key Questions

1

데이터센터 내부의 횡적(East-West) 트래픽을 어떻게 제어할 것인가?

- 데이터센터 내에서 증가되는 횡적 트래픽
- 만약 경계에서 침입되어지면, 내부의 횡적 이동을 통제할 방법이 전무

2

데이터센터 내부의 공격 표면을 어떻게 줄일 것인가?

- 대부분의 침입은 중요하지 않은 자산에서 발생하여 내부로 확산
- 공격자가 가장 선호하는 것인 인접해 있는 대형 네트워크

3

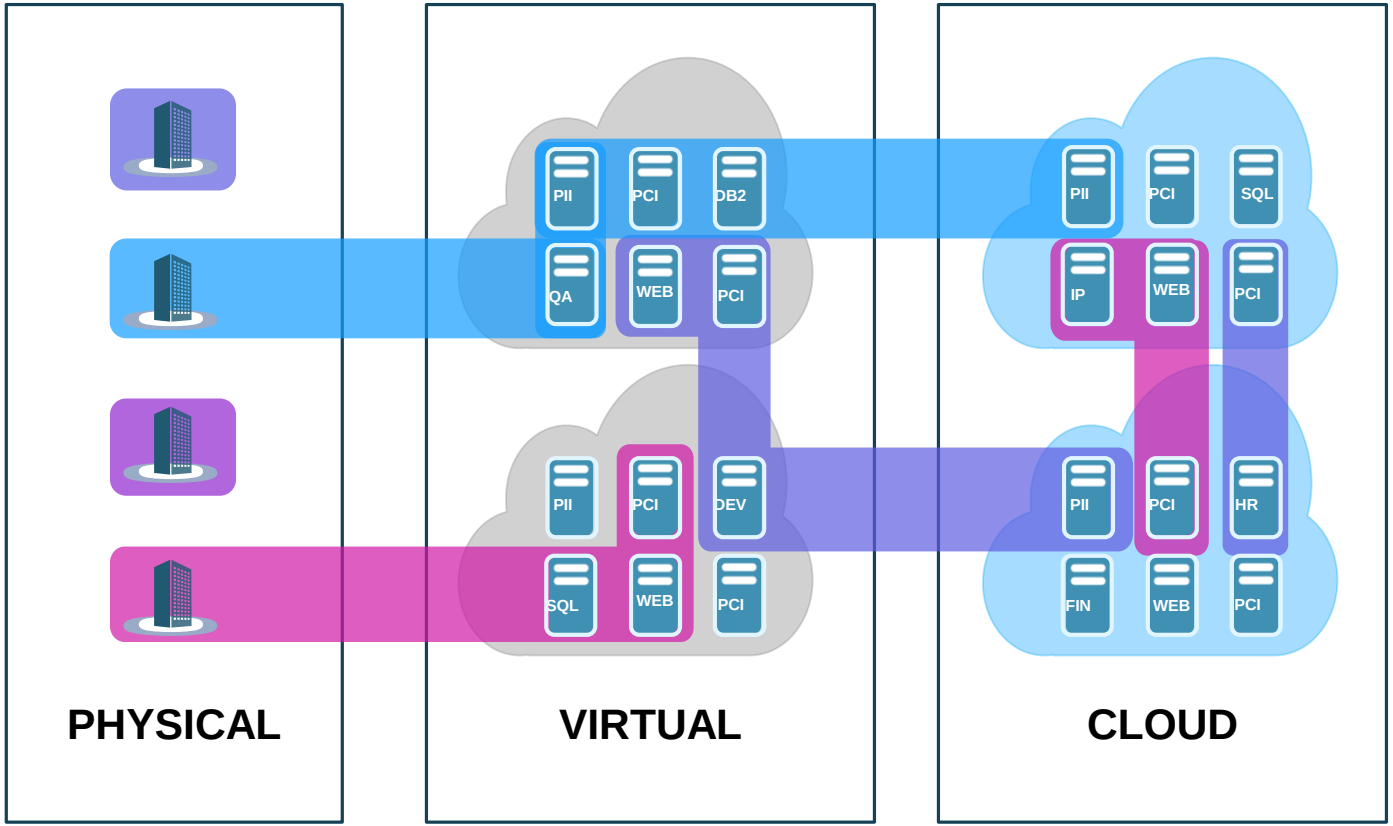
워크로드 레벨에서 간편한 보안정책을 어떻게 적용할 것인가?

- 기업의 컴퓨팅 설치공간이 프라이빗 DC에서 클라우드로 확대되고 있음
- 워크로드가 이동할 때 정책 변화가 필요 없는 간편한 정책

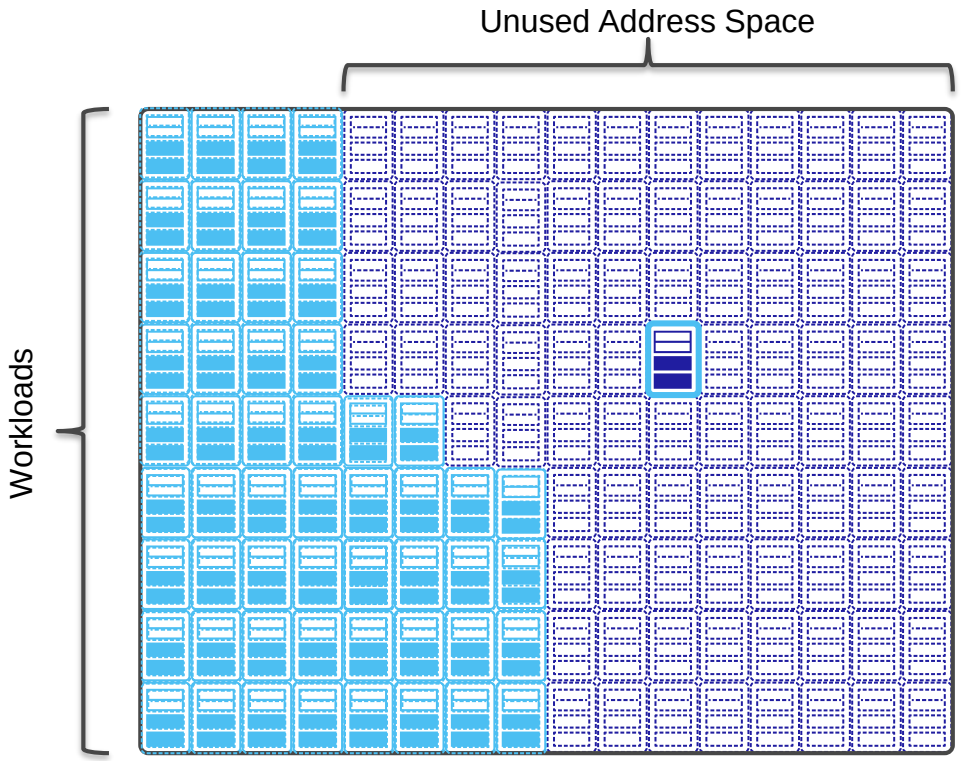
주요 관점

워크로드 레벨에서 횡적 트래픽을 제어하고 정책을 적용할 수 있는 소프트웨어 기반의 확장 가능한 보안솔루션으로 기존 **경계 보안 스타일에 대한 보완**이 필요하다.

마이크로세그멘테이션 보안 정책

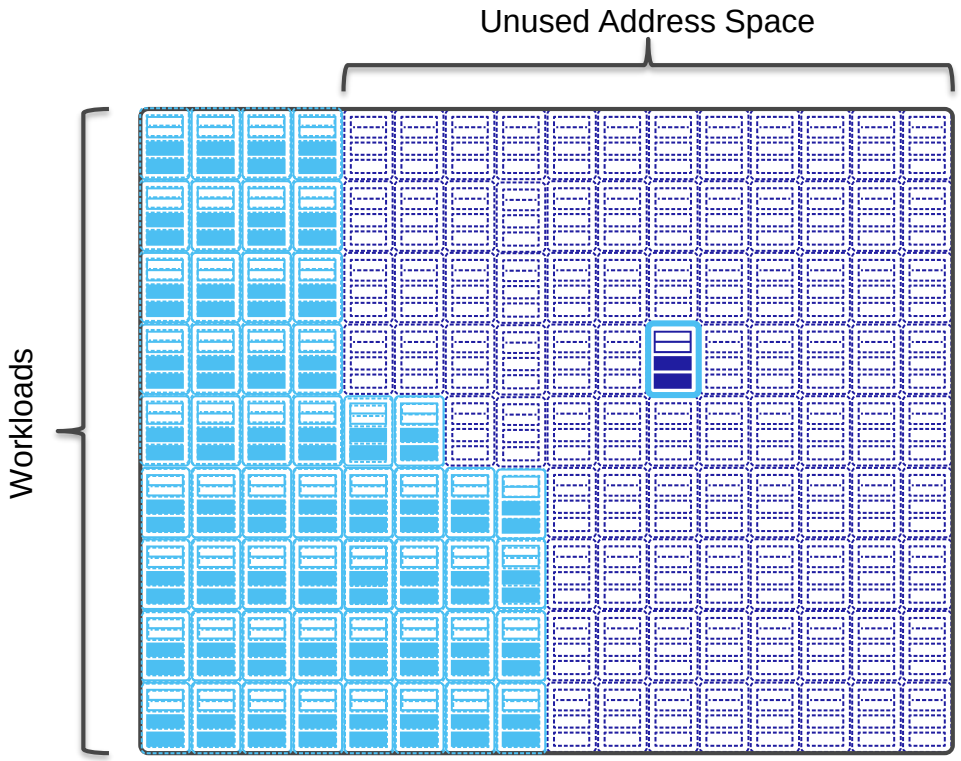


능동적인 탐지를 위한 디셉션 서비스



- vArmour 패브릭은 데이터센터 빈공간에 대한 접속을 제어
- 트랜스패어런트한 트래픽 라우팅은 단일 디셉션을 수천 또는 수만개처럼 보이게 속임

능동적인 탐지를 위한 디셉션 서비스



- **단순화(Simple)**
  - vArmour를 통합 배포, 관리, 경고 및 분석
  - DSS 관리를 위한 DSS 단일 디셉션 포인트
- **확장성(Scalable)**
  - 단일 인스턴스에서 대규모 디셉션 범위 적용
  - 통합된 탐지, 분석 및 대응은 워크로드 단순화
- **보안(Secure)**
  - vArmour 패브릭에 의한 악용으로부터 보호
  - 데이터센터 통신에 대한 완벽한 L7 가시성 제공

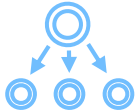
vArmour 정책 관리 및 적용 정리

멀티 클라우드 기술은 데이터센터와 클라우드 내의 워크로드 및 애플리케이션을 보호

Application Policy

DISCOVER

ILLUSTRATE



ORCHESTRATE

APPLICATION DISCOVERY: 복잡한 환경 전반에 걸쳐 애플리케이션 및 데이터에 대한 가시성 제공

USE AND MISUSE ILLUSTRATION ILLUSTRATE: 중요한 애플리케이션을 사용하거나 오용하는 것을 표시

ORCHESTRATE MULTIPLE FABRICS: 데이터센터 및 클라우드 환경 전반에 걸쳐 정책 조율

SEGMENT

DECEIVE

ENFORCE

Application Protection

SEGMENT: 기존 환경(가상 및 Physical) 뿐만 아니라 클라우드기반에서 분산 방화벽뿐만 아니라 마이크로 세그멘테이션을 가능하게 함

DECEIVE: 매우 정확한 디셉션 기술로 지능화된 적과 대응

ENFORCE: 동적 정책 시행으로 실시간 환경 변화에 대응

자동화된 사이클로서의 애플리케이션 보안

애플리케이션 검색

사용 및 오용 평가

애플리케이션 보안 정책

주요 애플리케이션에 대한 사용 및 오용 이해

정책 계산

예방 및 탐지 정책의 자동화 모델

정책 오케스트레이션 (측정, 테스트, 배포)

애플리케이션 보호 - 마이크로세그멘테이션

모든 워크로드에 대한 강화된 애플리케이션 정책

세분화

기만

적용

PHYSICAL

PRIVATE CLOUD

CONTAINER & PAAS

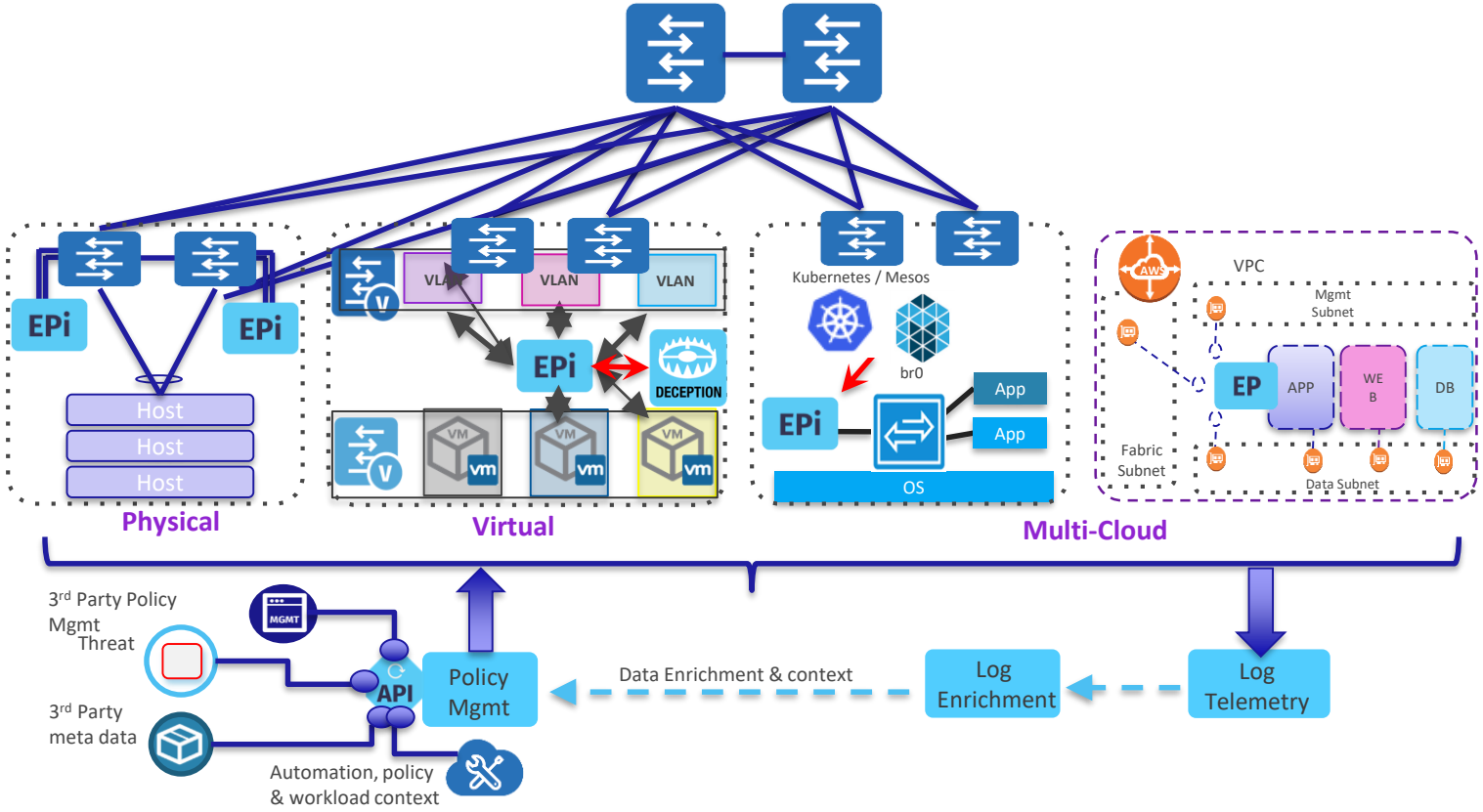
PUBLIC CLOUD

SDN

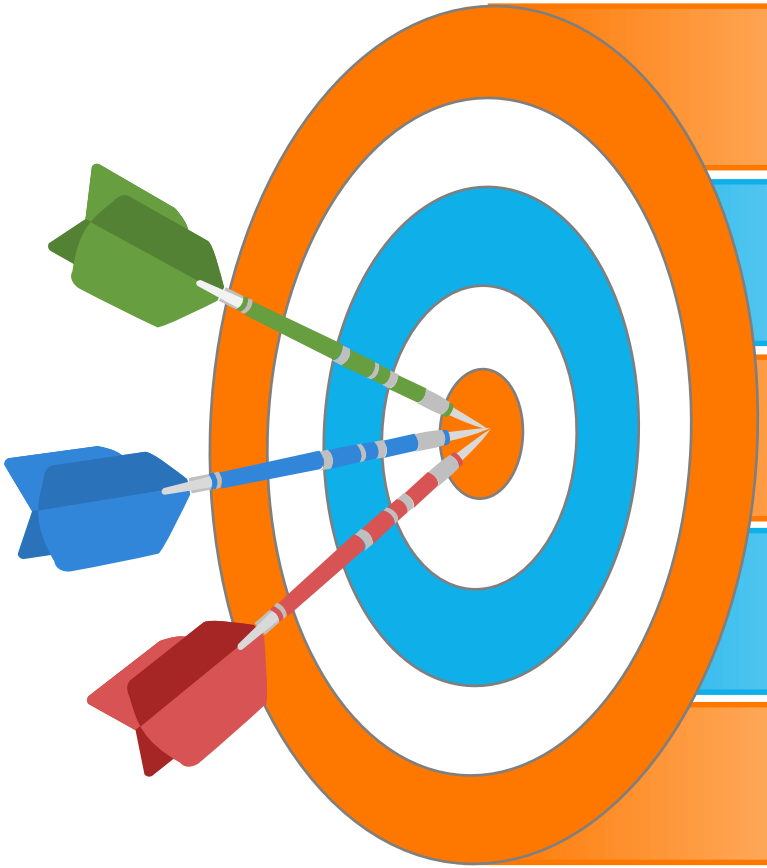
vArmour DSS FABRIC

NATIVE CLOUD CONTROLS

데이터센터 및 클라우드 기반 vArmour 적용



vArmour 특징



애플리케이션 중심 정책

SWIFT 지불과 EPIC 전자의무기록 같은 애플리케이션 가시화 및 제어(예를) vs. IP 주소 및 포트

멀티클라우드 환경 적용

베어메탈/물리적 워크로드/컨테이너 등을 포함하는 온-프레미스 및 클라우드 환경을 위한 싱글 포인트 가시성 및 제어

에이전트리스 제어 기능

스테이트풀 L7 네트워크 세그멘테이션은 에이전트를 사용 할 수 없는 규정을 준수 하면서 기존의 방화벽을 대체 가능

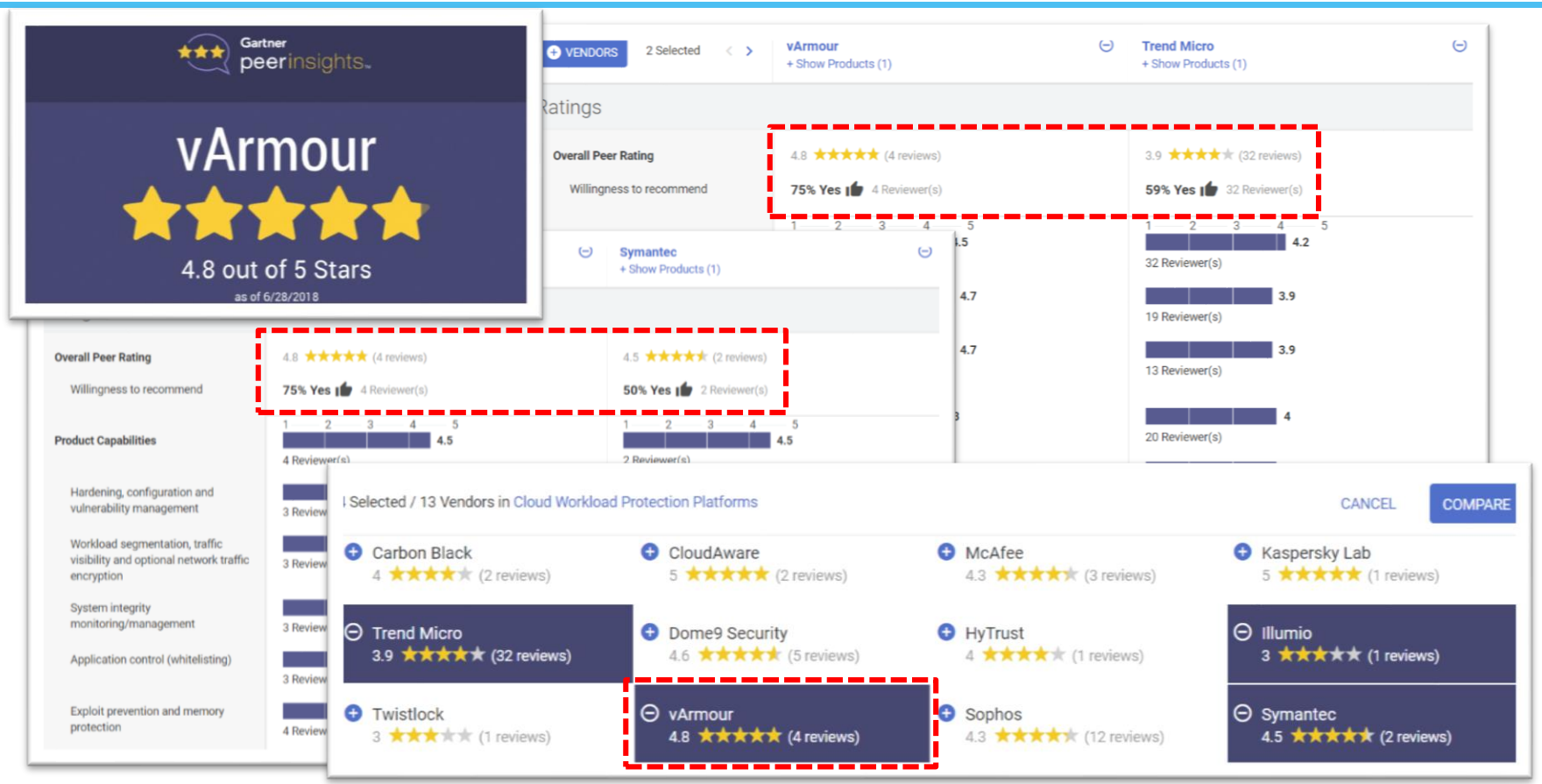
클라우드 확장성

유일한 스테이트플 L7 제품으로 단일 패브릭에서 100,000 워크로드 까지 확장 가능하며, 단일 시스템의 경우 시스템당 백만으로 확장(수평 확장).

빠른 가치 획득

수분 안에 다운로드하여 설치하고 애플리케이션을 인지 가능하며 템플릿을 사용하여 즉시 보안 정책 구축 가능

Gartner 비교 평가



출처:https://www.gartner.com/reviews/market/cloud-workload-protection-platforms/vendor/vArmour

vARMOUR