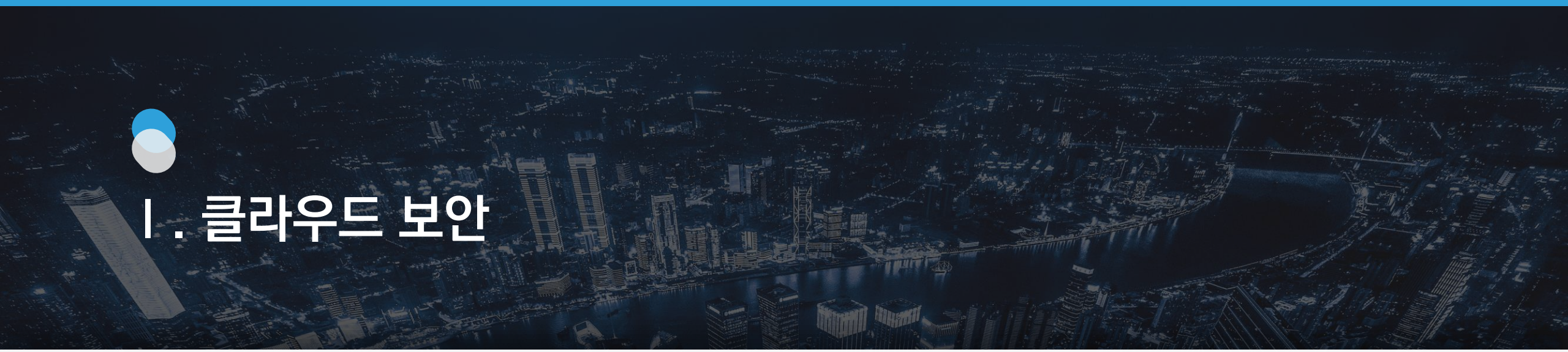
클라우드 워크로드를 보호하는 최적의 보안 전략

2022. 04. 22.

CONTENTS



Ⅰ. 클라우드 보안

1. 클라우드 동향
2. 클라우드 서비스의 명암
3. 기존 보안 위협과 클라우드 보안 위협
4. 클라우드 보안 위협
5. 클라우드 보안 사고 사례
6. 클라우드 워크로드 보안 전략
7. 클라우드 보안 기술 트렌드
8. 하이브리드 클라우드 환경에서 통합 보안 필요성
9. vAegis 솔루션의 필요성

1. 클라우드 동향

기업규모가 커질수록 하이브리드 클라우드를 사용하며, '보안'이 클라우드 산업 활성화의 큰 저해 요인

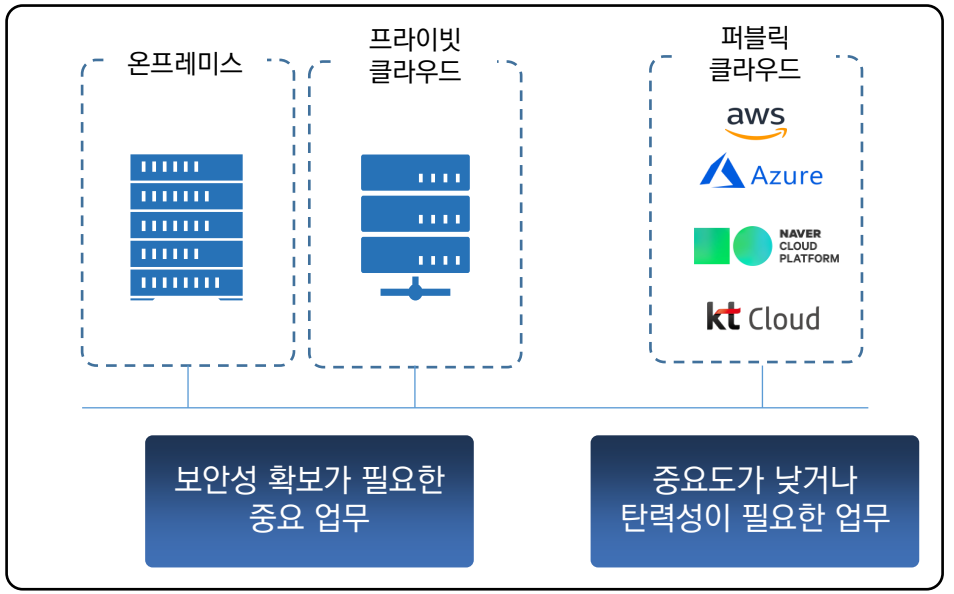
클라우드 제공 형태별 매출 비중

[단위 : %]

구분		퍼블릭 클라우드	프라이빗 클라우드	하이브리드 클라우드
전체		36.8	13.1	50.2
종사자 수	1 ~ 9인	78.9	9.6	11.6
	10 ~ 29인	40.7	21.8	37.5
	30 ~ 99인	40.0	21.2	38.8
	100 ~ 299인	0.6	23.3	46.1
	300인 이상	32.6	3.8	63.5
기업 규모	대기업	29.4	3.8	66.7
	중견기업	40.2	12.5	47.4
	중소기업	42.6	21.9	35.5
서비스 모델	IaaS	48.33	19.8	31.9
	PaaS	23.8	38.0	38.2
	SaaS	39.4	6.0	54.5
	CMS	3.3	1.9	94.8
	기타	63.4	34.6	2.0

['2021 클라우드 산업 실태 조사'- 과학기술정보통신부]

국내 클라우드 시장은 하이브리드가 주도



※ 하이브리드 클라우드 : 1개 이상의 퍼블릭 클라우드와 자체 인프라(프라이빗 클라우드) 또는 온프레미스가 조합된 환경
※ CMS(Content Management System) : 컨텐츠 관리 시스템으로 기업이 디지털 컨텐츠를 관리하기 위해 사용하는 소프트웨어 시스템 또는 플랫폼

2. 클라우드 서비스의 명암

클라우드는 기존 IT환경에 비해 많은 장점을 갖지만 클라우드의 환경에 따른 새로운 보안 위협에 노출

유연한 IT 인프라 관리

클라우드는 IT 인프라를 실시간으로 자유롭게
조정할 수 있기 때문에 인프라 부족 또는 과도한 인프라 도입의
문제점이 발생하지 않음

신속한 인프라 도입

클라우드 서비스 가입 후 몇 분 내로
인프라를 도입해 서비스 구축 가능

간편한 글로벌 서비스

수 많은 클라우드 사업자가 전 세계 주요 대륙에
데이터 센터를 보유하고 있어 미리 구축한 데이터 센터를 활용

예상치 못한 트래픽 폭주 대응

'오토스케일링' 기술을 통해
자동으로 상황에 맞춰 인프라를 조절해 트래픽 관리

장애 없는 서비스

클라우드 사업자는 많은 데이터센터와
가상화 기술을 활용해 장애 없는 서비스를 보장

빅데이터, 인공지능(AI) 서비스 확장

머신러닝과 AI는 데이터가 중요한데 클라우드는
필요한 데이터를 쉽게 모을 수 있기에 AI를 고도화 하는데 유용

UP
DOWN

보안 취약점

- 비 인가된 접근
- 클라우드 어플리케이션 가시성
- 어플리케이션 API 취약성
- 시스템 취약성
- 컴플라이언스 이슈
- 휴먼 에러(관리자의 실수)

"2023년까지 최소 99%의 클라우드 보안 실패는 고객사 잘못에 의한 것"

"2021년까지 기업 50%는 관리자 실수로 인해 중요 정보가 인터넷에 노출될 것"

[가트너]

67.5%

클라우드 보안 솔루션 사용 안함

11.3%

보안 사고 유무 확인 안함

[데이터넷]

3. 기존 보안 위협과 클라우드 보안 위협

기존 IT환경의 보안 위협을 그대로 가지며, 클라우드의 특수한 환경에 따른 새로운 보안 위협 내포

분류	보안 위협	관련 기관					
		Gartner	RSA	CSA	NIST	ITU-T X.1601	ENSIA
기존 보안 위협	□ 데이터 손실 및 유출 위협 - 데이터 백업관리, 외부 저장장치 관리, 삭제 관리 미흡	●		●	●	●	●
	□ 데이터 변조 위협 - 데이터 암호화 및 키 관리 미흡	●	●			●	●
	□ 인증 및 권한 관리 위협 - 사용자 계정정보 유출, 권한 관리 미흡	●	●	●	●	●	●
	□ 시스템 및 네트워크 보안 취약점 - 악성코드, OS 보안취약점, 가상 네트워크 취약점		●	●	●	●	
	□ 서비스 장애 - 재난관리, 클라우드 서비스 제공업체의 폐업 및 합병	●	●		●	●	●
	□ 내부자 관리 실수 - 통합 정책 관리 미흡, 법령 및 규정 준수 미흡	●	●	●	●	●	●
	□ 시스템 악용 - 클라우드 자원 활용한 피싱, 봇넷 악용	●	●	●			
클라우드 고유 보안 위협	□ 하이퍼바이저 취약점 - 취약한 하이퍼바이저 활용 VM 피해	●		●	●	●	
	□ VM 내부 공격 - VM간 패킷 스니핑, 악성코드 전파, 내부 영역 침입탐지 어려움	●		●	●	●	
	□ 안전하지 않은 API - CSI에서 제공한 API에 취약점 존재 시 정보 유출, 서비스 장애 발생			●	●	●	

※ CSA(Cloud Security Alliance): 클라우드 보안 협회
※ ITU-T X.1601: ITU-T(ITU Telecommunication Standardization Sector; 국제전기통신연합 전기통신표준화 부문), X.1601은 클라우드 컴퓨팅 보안 프레임워크 표준문서
※ NIST(National Institute of Standards and Technology): 미국 표준기술연구소
※ ENSIA(European Union Agency for Network and Information Security): 유럽 연합 네트워크 및 정보보안 기구

4. 클라우드 보안 위협

클라우드의 복잡성은 공격자가 숨을 수 있는 완벽한 장소

데이터 유출

데이터는 사이버 공격의 주요 대상
인터넷을 통해 접근할 수 있는 데이터는 잘못된 구성이나 이용에 가장 취약

잘못된 구성 및 부적절한 변경 관리

클라우드 기반 리소스는 매우 복잡하고 동적이어서 구성하기가 어려움

클라우드 보안 아키텍처 및 전략 부족

클라우드에서 데이터와 애플리케이션을 운용하면서 클라우드에 맞지 않는 보안 인프라와 전략을 사용

ID, 자격 증명, 액세스 및 키 관리 부족

서버실과 건물 같은 물리적 리소스, 데이터와 시스템 관리, 액세스 관리가 미흡해 초래되는 위협

계정 하이재킹

피싱이 더욱 효과적이고 표적화

내부자 위협

신뢰하고 있는 내부자로부터 초래되는 위협

안전하지 못한 인터페이스와 API

사용자 인터페이스와 API의 취약점은 공격자에게 사용자나 직원의 계정을 쉽게 훔칠 수 있는 경로 제공

취약한 제어 영역

관리자가 인프라의 논리, 보안, 검증을 완전하게 통제 및 관리하지 못할 때 제어 영역이 취약

메타스트럭처와 어플리스트럭처 실패

메타스트럭처에는 시스템 보호 방식에 대한 보안 정보가 들어 있으며,
API 호출을 통해 이런 정보를 공개하는데, API는 고객이 승인되지 않은 액세스를 감지하도록 도움을 주지만 로그나 감사 시스템 데이터 같이 아주 민감한 정보도 포함

클라우드 사용과 관련된 가시성이 제한되는 문제

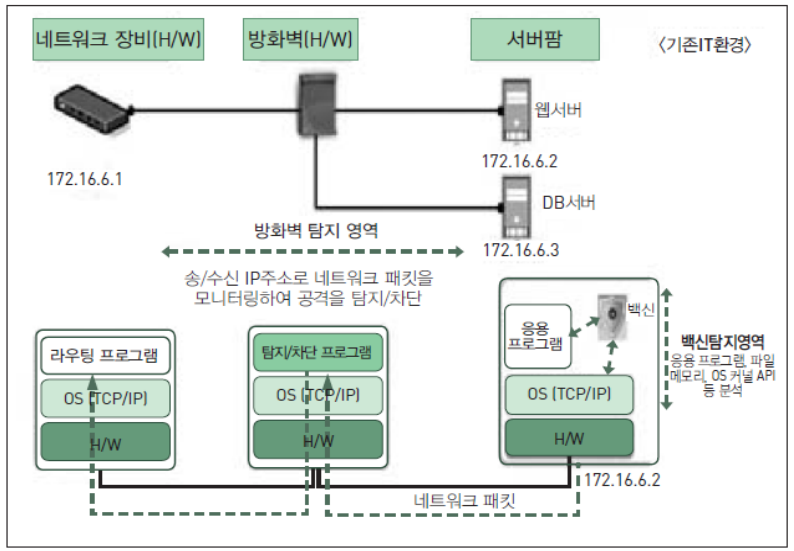
허가 받지 않은 앱을 사용하는 문제, 허가된 앱을 오용하는 문제

※ 메타스트럭처(Metastructure): 클라우드 서비스 업체와 고객의 경계선
※ 어플리스트럭처(Applistructure): 어플리케이션과 기술 인프라의 병합

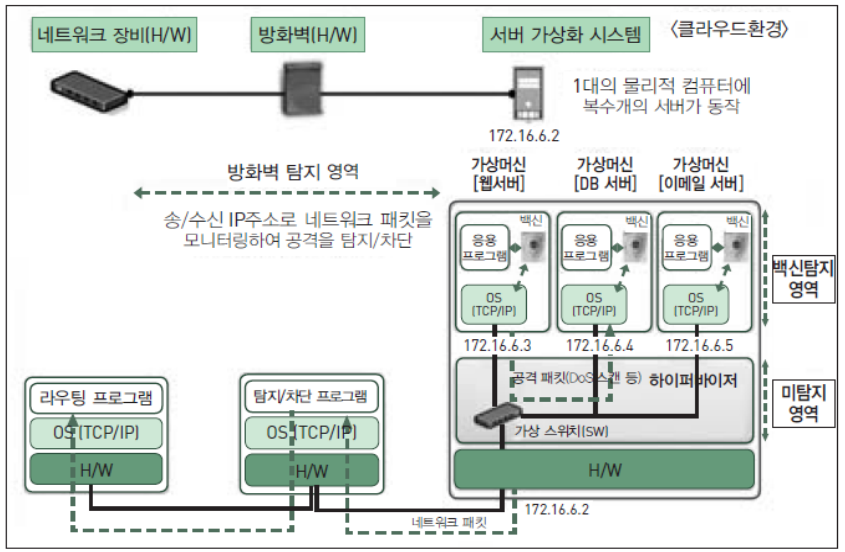
['클라우드에 대한 주요 위협'- CSA(Cloud Security Alliance)]

4. 클라우드 보안 위협

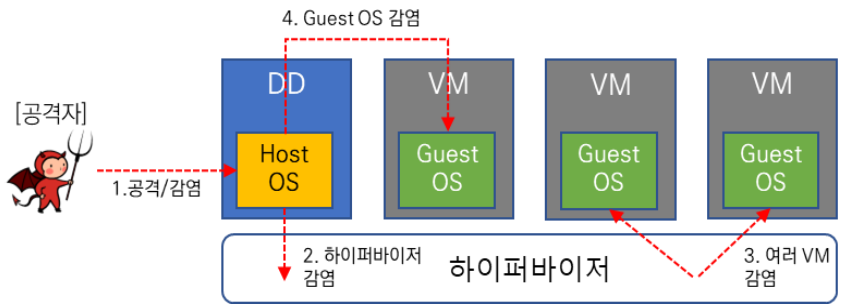
클라우드의 복잡성은 공격자가 숨을 수 있는 완벽한 장소

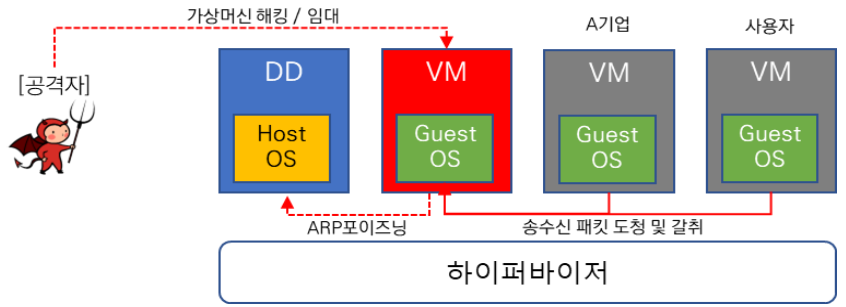


기존IT 환경



클라우드 환경





※ ARP 포이즈닝: 서버에 잘못된 MAC 주소 정보를 보내 해당 ARP 캐시테이블을 오염시키는 것으로 ARP 프로토콜의 내용의 검증을 확인하지 않는 프로토콜 자체의 취약점을 이용한 공격 기법. ARP Spoofing을 하기 위한 선행 단계로 많이 사용

※ ARP Spoofing: 오염된 ARP 캐시테이블을 이용해 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법

5. 클라우드 보안 사고 사례

보안 사고에서 주요 대상은 데이터(정보)

미국의 대형 은행, Capital One 개인정보 유출 사고

- 2019년 7월 19일, 약 1억 건의 신용카드 소지자와 미국 내 신청자 및 캐나다에서 6만 건의 개인 정보를 도난
- WAF(Web Application Firewall)를 잘못 구성
- 공격자는 잘못 구성된 WAF를 사용하여 액세스 토큰을 생성
- 그런 다음 액세스 토큰을 사용하여 AWS 스토리지에서 데이터를 가져옴
- 고객 정보가 포함된 700 개의 폴더와 데이터 패킷이 외부 위치로 복사

인도 혼다 자동차 민감 정보 유출 사고

- 2018년 5월 30일, 독일의 보안 회사 Kromtech Security는 인도의 혼다 자동차에서 아마존 AWS S3 버킷이 인터넷에 노출되어 있다는 보고서를 발표
- 2개의 S3 버킷에는 Honda Connect를 다운로드 해 설치한 사용자의 개인 정보(이름, 전화번호, 성별, 비밀번호, 이메일 주소 등)가 포함
- S3 버킷은 최소 3개월 이상 노출

국내 클라우드 정보 유출 사례

사업자명	유출 건수	내용	조치
야놀자	• 52,132	접근권한 관리 미흡	• 과징금 5,690만원 • 과태료 3,000만원
스타일쉐어	• 6,400,001		• 과징금 9,470만원 • 과태료 1,600만원
집꾸미기	• 183,323		• 과징금 2,830만원 • 과태료 2,200만원
스퀘어랩	• 419,028		• 과징금 540만원 • 과태료 1,500만원
골드스푼	• 130,000		• 과징금 1억 2,979만원 • 과태료 1,860만원

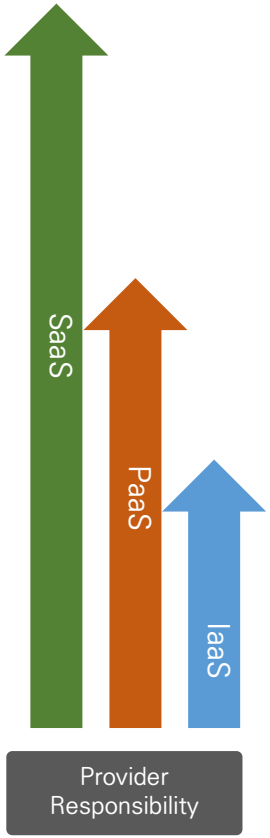
※ AWS S3: 내구성과 확장성이 뛰어난 스토리지 서비스
※ 버킷: Amazon S3에 저장된 객체에 대한 컨테이너

6. 클라우드 환경에서의 사용자 책임

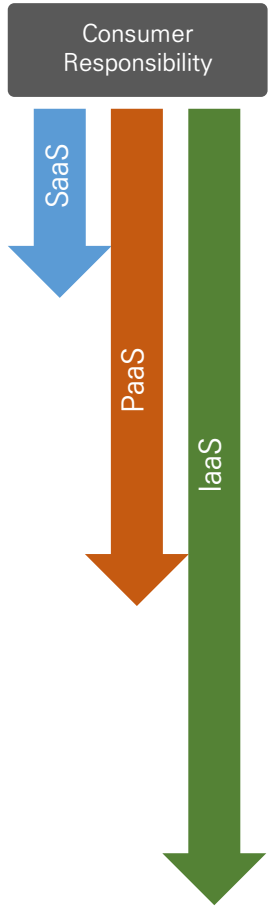
클라우드 환경에서 보안은 책임 공유 모델로 사용자(고객사)의 책임 존재

“ 클라우드에 저장된 데이터에 대한 기본 책임은 서비스 제공자가 아닌 사용자 ”

[클라우드 책임 공유 모델((Shared Responsibility Model)]



On-Premises	IaaS	PaaS	SaaS
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Application	Application	Application	Application
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical



7. 클라우드 보안 기술 트렌드

클라우드 접근 보안 중계, 클라우드 워크로드 보안 플랫폼, 클라우드 보안 형상관리가 중심

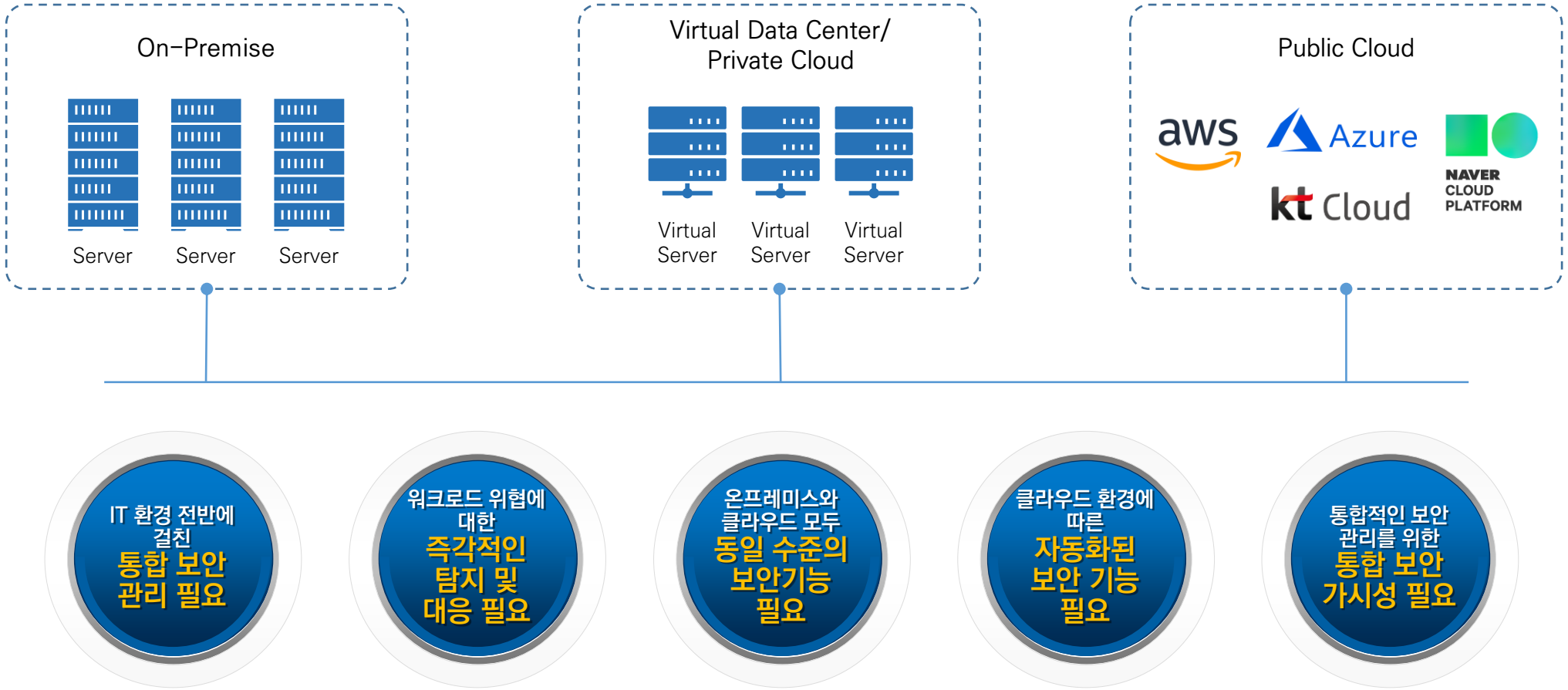
항 목	CASB (Cloud Access Security Broker)	**CWPP** **(Cloud Workload Protection Platform)**	CSPM (Cloud Security Posture Management)
설명	• 클라우드 접근 보안 중계	• 클라우드 워크로드 보호 플랫폼 (클라우드 보안의 가장 기본)	• 클라우드 보안 형상 관리
주요 기능	• 클라우드 및 애플리케이션에 대해 가시화 • 사용자 접근 통제를 적용	• **하이브리드 및 멀티 클라우드 환경에서 서버 워크로드를 보호**	• 클라우드 서비스의 위험평가 및 관리
영역별 구분	• SaaS 보안에 중점 • 일부 기능이 IaaS 까지 확대	• 온프레미스, 가상 머신(VM), 컨테이너, 서버리스 등 워크로드에 대해 가시성과 보안 제공	• IaaS, PassS 클라우드 스택 전반의 보안평가 • IaaS, PassS 클라우드 컴플라이언스 모니터링
핵심 기능	• DLP 및 장치, 데이터의 중요도에 따른 액세스 제어 등의 데이터 보호 • 업/다운로드 데이터 감지 및 Zero-day 위협 탐지 • SSO 연동 및 위험 로그인 감시를 위한 다중 인증 지원 기능 • 클라우드 앱 사용 관련 모니터링	• 보안 강화 및 설정/취약점 관리 • 네트워크 방화벽, 가시성 확보 및 마이크로세그멘테이션 • 시스템 무결성 보장 • 어플리케이션 제어 • 익스플로잇 예방 및 메모리 보호 • 서버 워크로드 EDR, 행위 모니터링 및 위협 탐지 • 호스트 기반 침입탐지 시스템 • 안티 멀웨어	• 컴플라이언스 진단 • 운영 모니터링 • 데브옵스 통합 • 인시던트 대응 • 리스크 판별 • 리스크 시각화
대표 벤더	• 오라클 (팔레라) • IBM (그래비던트) • 마이크로소프트 (아달롬) • 시만텍 (스카이큐어) • 맥아피 (스카이하이 네트웍스)	• 트렌드마이크로 • 맥아피 (CASB) • 캐스퍼스키 • 브로드컴 (시만텍) • 비트디펜더 • 팔로알토네트웍스 (CSPM) • 안랩 (CPP, Cloud Protection Platform)	• 체크포인트 (돔나인) • 팔로알토네트웍스 (에비던트아이오, 레드락) • 소포스 (아비드시큐어)

※ 워크로드(Workload): 리소스에서 실행할 수 있는 특정한 어플리케이션, 서비스, 기능 또는 특정한 작업량, 가상머신, 데이터베이스, 컨테이너, Hadoop 노드 및 어플리케이션이 모두 클라우드 워크로드로 간주
※ 마이크로 세그멘테이션(Microsegmentation): IT 환경을 통제 가능한 구역으로 분할해 각 워크로드를 상호 안전하게 격리하는 동시에 네트워크 보호를 더 세분화함으로써 승인되지 않은 횡적 이동 문제에 대처

8. 하이브리드 클라우드 환경에서 통합 보안 필요성

온프레미스에서 클라우드까지 넓어지면서 하이브리드 환경에서 통합 보안 관리 및 대응 필요

하이브리드 클라우드 환경에서는 방어해야 할 위협표면이 증가하였고, 클라우드 특성에 따른 보안 위협은 빠르게 전파/확산되어 기존의 전통적인 보안 솔루션으로 탐지/대응이 불가하므로 **“하이브리드 환경에서의 통합 보안 솔루션”**이 필요



9. CWPP 솔루션의 필요성

기존 IT 환경과 클라우드 환경을 아우르는 통합보안 솔루션 필요

분류	보안 위협
기존 보안 위협	데이터 손실 및 유출 위협
	데이터 변조 위협
	인증 및 권한 관리 위협
	시스템 및 네트워크 보안 취약점
	서비스 장애
	내부자 관리 실수
	시스템 악용
클라우드 고유 보안 위협	하이퍼바이저 취약점
	VM 내부 공격
	안전하지 않은 API

01 하이브리드 클라우드 환경의 통합 보안 필요

IT환경이 기존 온프레미스에서 클라우드 환경까지 확장에 따른 하이브리드 환경에서의 보안 가시성 확보와 신속한 대응 필요

- 기존 온프레미스 환경과 클라우드 환경에서 동일한 보안 수준 제공 필요
- 이원화 보안 관리가 아닌 통합 보안 관리를 통한 가시성 확보 필요

02 클라우드에서의 워크로드 보안 필요

유동적으로 운영되는 클라우드 서버에 대한 가시성 확보가 중요하며, 효율성 향상과 안정적인 서버 운영 필요

- 기존 온프레미스 서버와 동일한 보안 수준 필요
- 클라우드의 특수한 환경인 오토스케일링에 대응 필요

03 클라우드에서의 네트워크 보안 필요

클라우드 환경에서 종적(North-south)이 아닌 횡적(East-west) 트래픽 통제 필요

- 클라우드 서버간, 어플리케이션 간의 통신이 빈번하게 발생하며 이러한 특성은 악성 행위의 확산에 노출되므로 이에 대한 대응 필요

II. CWPP 제품 소개

1. 워크로드 통합 보안 플랫폼
2. 제품 구성
3. 주요 기능
4. vAegis 특장점

1. 워크로드 통합 보안 플랫폼

vAegis는 서버 워크로드 보호에 최적화된 다양한 보안기능을 제공하는 보안 플랫폼

“ 하이브리드 환경에서의 **서버 워크로드 통합 보안 플랫폼** ”

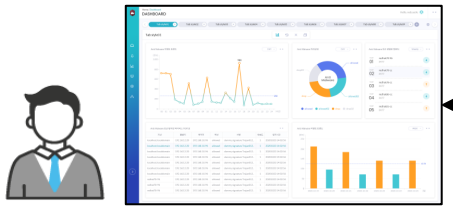
vAegis는 기존 보안 솔루션은 클라우드에 대해 한정된 가시성 제공을 넘어 IT 인프라 전반에 걸쳐
통합적인 가시성을 제공하고 다양하고 강력한 통합 보안 기능을 제공하여
서버 워크로드 통합 보안 플랫폼으로서 효율적이고 높은 성능을 제공합니다.

[하이브리드 환경 전반의 통합 보안]

2. 제품 구성

보안기능을 수행하는 Agent, 정책/로그관리를 수행하는 Management Server, 관리 UI인 Manager로 구성

[vAegis Manager]



[vAegis Management Server]

- 보안 정책 관리
- 자원(시스템) 관리
- 로그 수집/관리
- 이벤트 생성
- 패턴 업데이트

온프레미스

[vAegis Agent]

- Host IPS
- Anti-Malware
- Firewall
- 무결성 감시
- Application Control
- 로그 관리

Virtual Server / Cloud

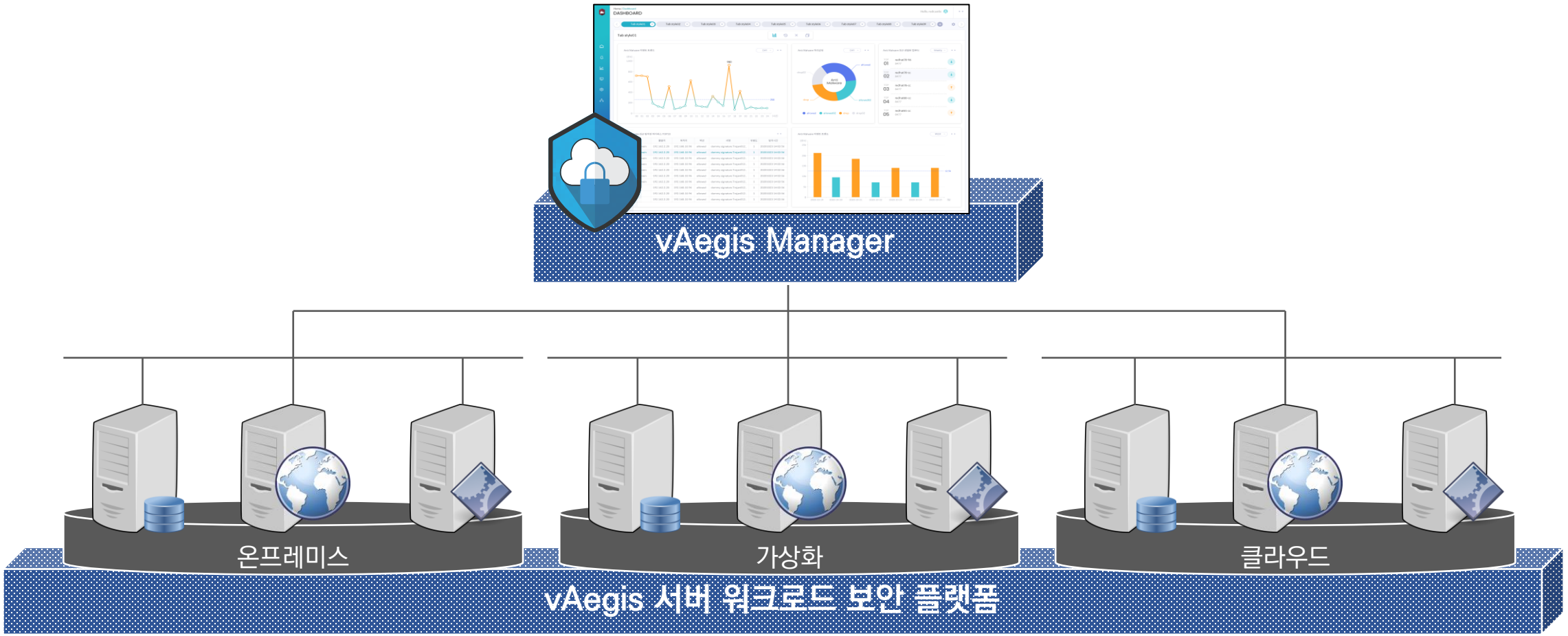
[vAegis Agent]

- Host IPS
- Anti-Malware
- Firewall
- 무결성 감시
- Application Control
- 로그 관리

3. 주요 기능 - 통합 대시보드 및 관리/대응

vAegis Manager를 통한 하이브리드 환경의 통합 가시성 제공 및 통합 보안 관리

✓ 온프레미스, 가상화 환경 및 클라우드 환경 전반의 서버 워크로드에 대한 통합된 가시성 제공 및 통합 보안 관리 기능 제공

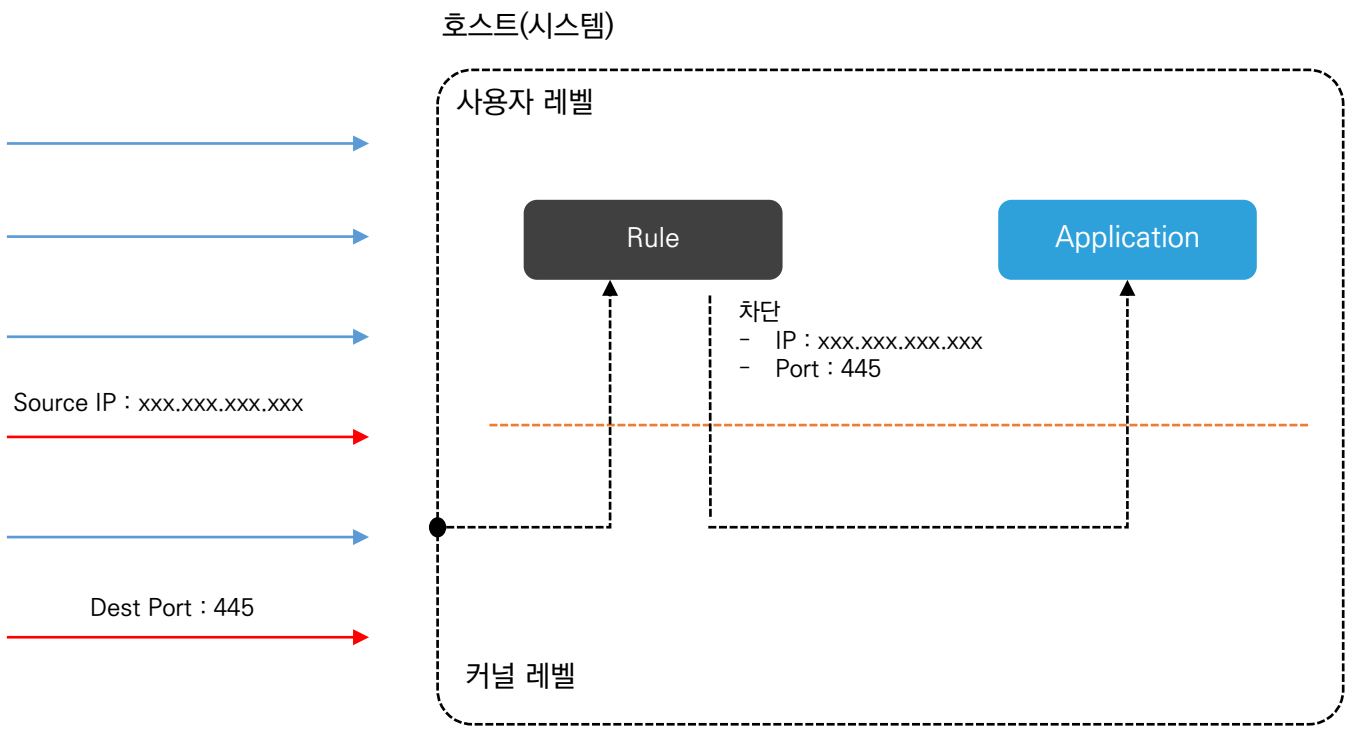


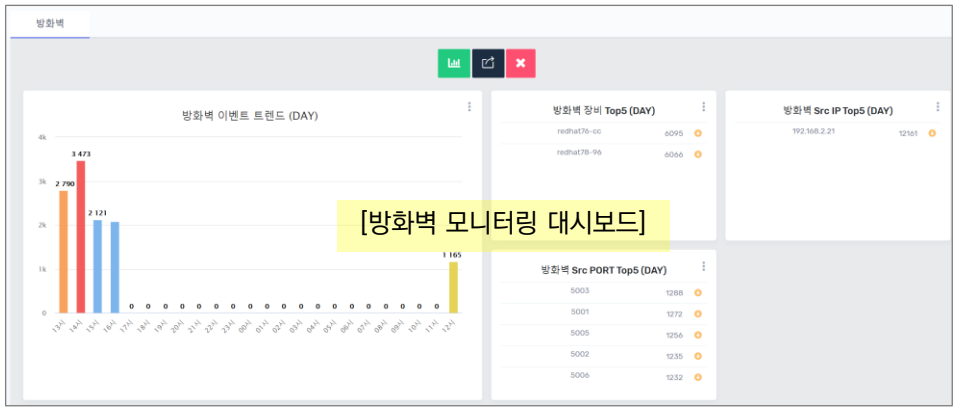
3. 주요 기능 – Firewall

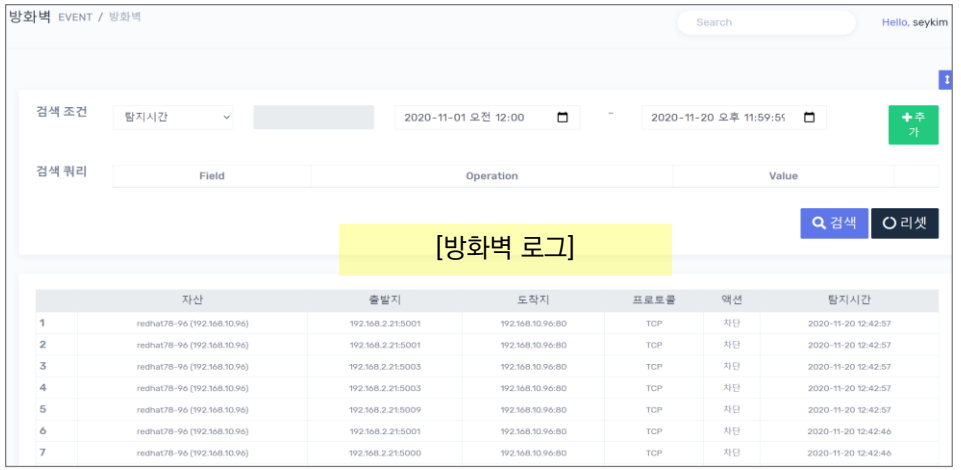
Inbound/Outbound 모든 IP 및 포트를 통제하여 서버에 대한 무단 접근 차단

✓ 워크로드 별로 방화벽을 제공하고 가시성 확보

- 진화된 Netfilter를 사용하여 커널 레벨에서 방화벽 정책에 따른 접근통제 기능 제공







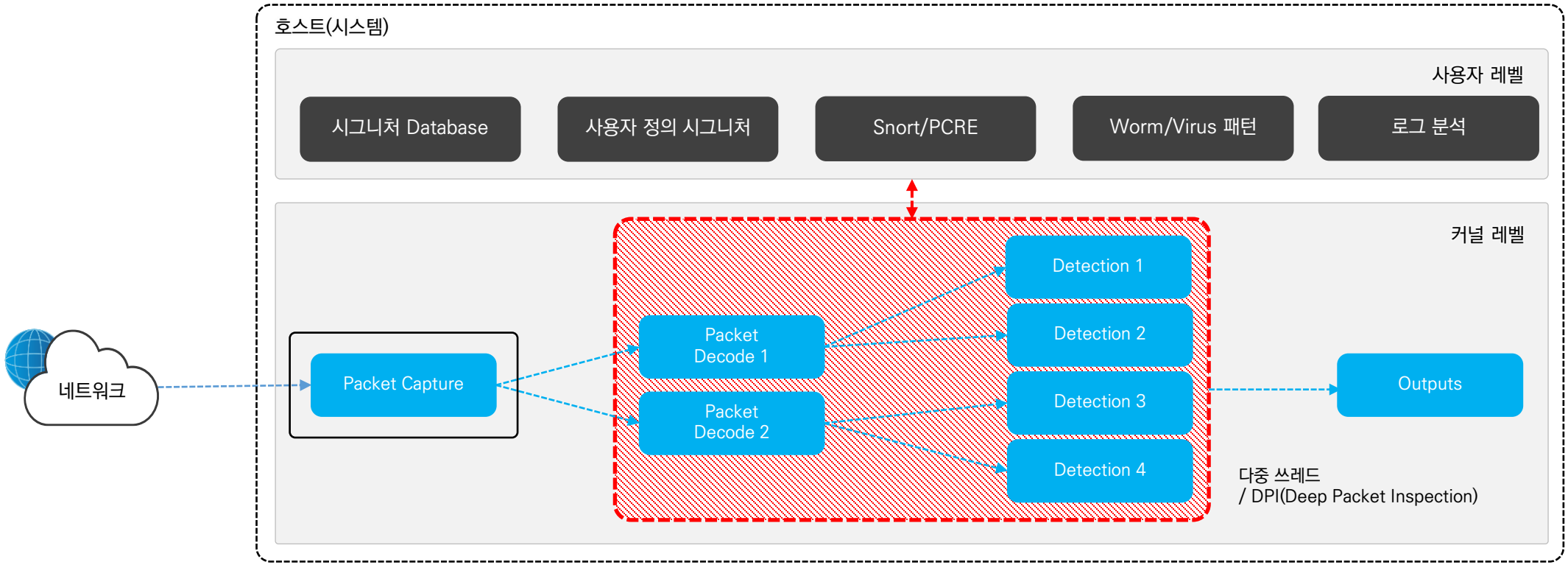
에스지에이솔루션즈(주)

3. 주요 기능 - Host IPS

다중 쓰레드 방식으로 동작하며 악의적인 패킷 탐지 및 차단하고 DPI를 지원하는 호스트 기반 IPS

✓ 네트워크 공격 방어 및 제로데이 취약점 공격 대응

- 오픈소스 기반의 Sourcefire사의 Snort 룰 호환/지원하고, DPI(Deep Packet Inspection) 데이터 저장 기능을 제공
- SQL Injection, Cross-Site Scripting과 같은 웹 어플리케이션 공격에 대한 탐지 및 차단 제공, CVE 취약점 탐지/차단/로깅하고 C&C 서버 콜백 통신 차단 기능 제공



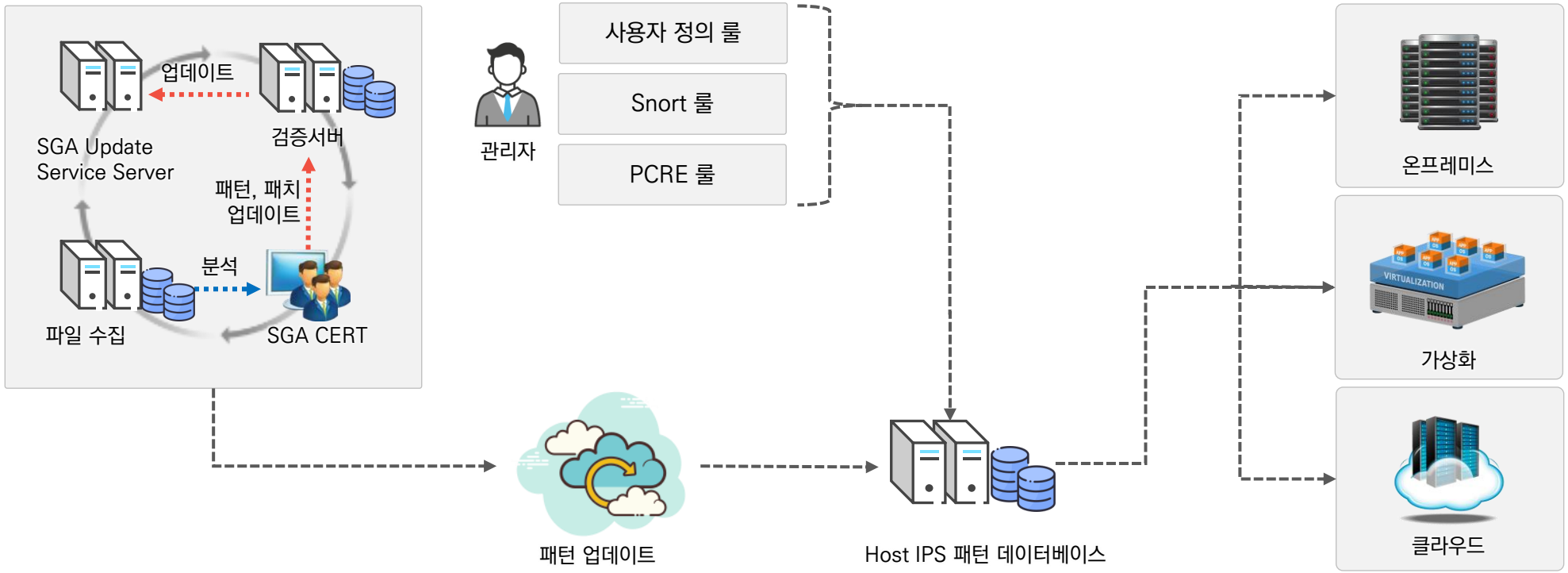
※ DPI(Deep Packet Inspection): 네트워크에서 전송되는 패킷의 헤더와 페이로드 내 정보를 분석하는 콘텐츠 내용 분석 기술. OSI 7 Layer까지 분석이 가능하며, 사전에 정의한 룰 기반 패킷의 패턴 분석 가능

3. 주요 기능 - Host IPS

시스템의 최적화된 IPS 패턴 자동 업데이트 및 Snort 룰과 PCRE 지원

✓ 다양하게 제공되는 탐지 룰 기능을 통한 다양한 공격에 대응

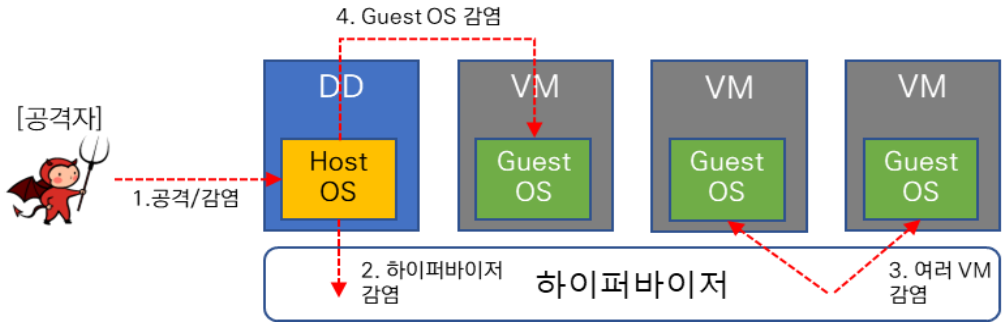
- IPS 패턴 자동 업데이트 혹은 관리자의 수동 업데이트 지원
- Snort 룰(패턴)을 호환/지원하여 관리자의 편의성 제공
- PCRE(Perl Compatible Expressions)를 지원하여 하나의 패턴으로 다수의 공격을 탐지하여 보안성 강화와 편의성 제공



※ PCRE (Perl Compatible Regular Expressions): Perl 프로그래밍 언어의 정규 표현식으로 복잡한 탐지 룰 생성 지원

3. 주요 기능 - Host IPS 필요성

HIPS(Host IPS)는 동적인 워크로드 간의 보안 취약점의 내부 전파를 탐지하고 차단



하이퍼바이저 감염 위험

가상화 시스템 내 하이퍼바이저가 취약할 경우 이를 활용하는 여러 개의 가상머신(VM)이 동시에 피해

가상 머신 공격 경로

사용자의 가상머신들이 상호 연결되어 내부의 가상머신에서 다른 가상머신으로의 패킷스니핑, 해킹, DDoS 공격, 악성코드 전파 등의 공격 경로가 존재

공격자의 익명성

가상환경에서는 공격자가 식별이 어려워 기존 네트워크 보안기술(방화벽, NIPS)로는 가상화 내부 영역에 대한 침입탐지가 어려움

가상 머신의 이동성

가상화 환경에서는 물리적 플랫폼 간 가상머신의 이동이 용이하여 이로 인한 감염이 확산되는 문제 발생

종적 통신 탐지 기반의 기존 네트워크 IPS로는 클라우드 특성의
횡적 통신 즉 워크로드 간의 악의적 행위(트래픽) 탐지 불가

워크로드 간의 보안 취약점, 악성코드 등의 전파 및 확산 방지

호스트 IPS는 각 서버의 용도별, 어플리케이션 별 등에 따라 다양한 정책 설정

오탐 시에 호스트 IPS는 해당 서버만 영향을 주므로 적용된 서버에 정책만 수정

워크로드 내 OS 취약점이나 어플리케이션의 보안 취약점 점검 지원

제로데이 취약점 대응 가능

Auto Scaling 지원

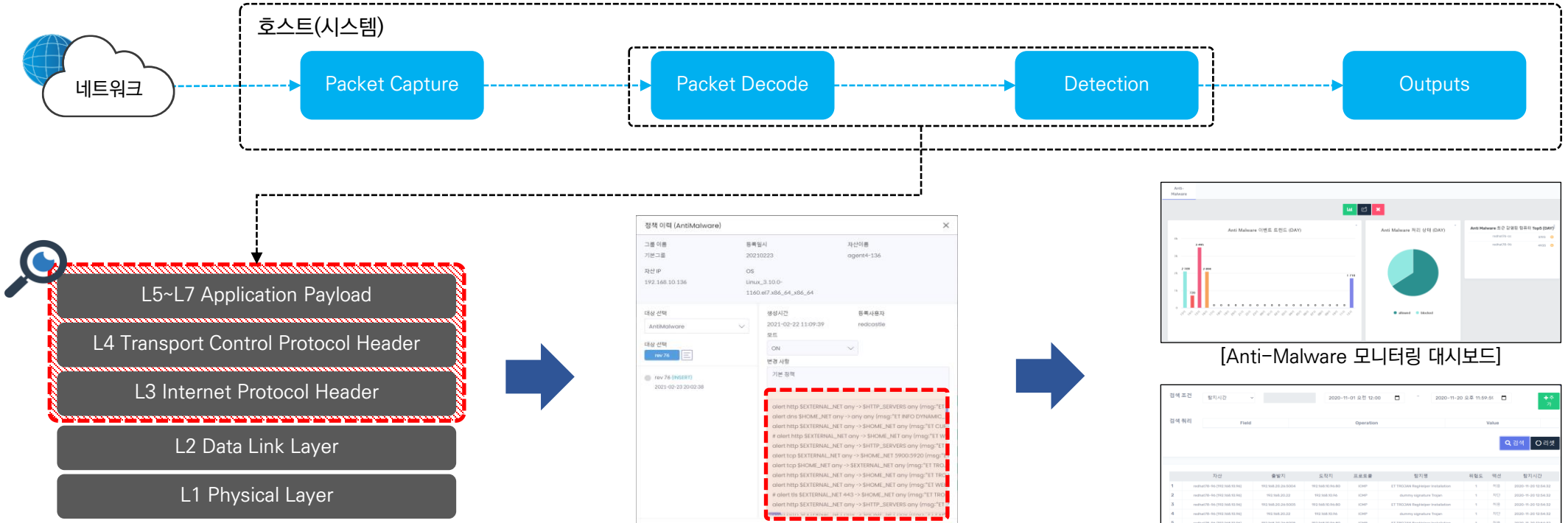
※ 종적 네트워크(North-South Network) : 데이터 센터와 클라이언트, 네트워크 상의 데이터 센터 외부와 통신하는 트래픽

※ 횡적 네트워크(East-West Network) : 데이터 센서 내부에서 발생되는 트래픽으로 서버와 서버 간의 트래픽

3. 주요 기능 - Anti-Malware

고성능 네트워크 패킷 분석과 자동화 된 프로토콜 감지 기능을 사용하여 실시간 악성코드 탐지

✓ 시그니처(패턴) 기반으로 Malware를 탐지하여 보안 컴플라이언스 충족
- 알려진 악성 소스에 대한 주소에 대해 악성 트래픽에 플래그를 지정할 수 있는 IP 평판 기능 제공
- Worm, Trojan 그리고 일반적인 Malware 뿐만 아니라 랜섬웨어 탐지 및 차단 기능 제공



[Anti-Malware 탐지 룰 정의]

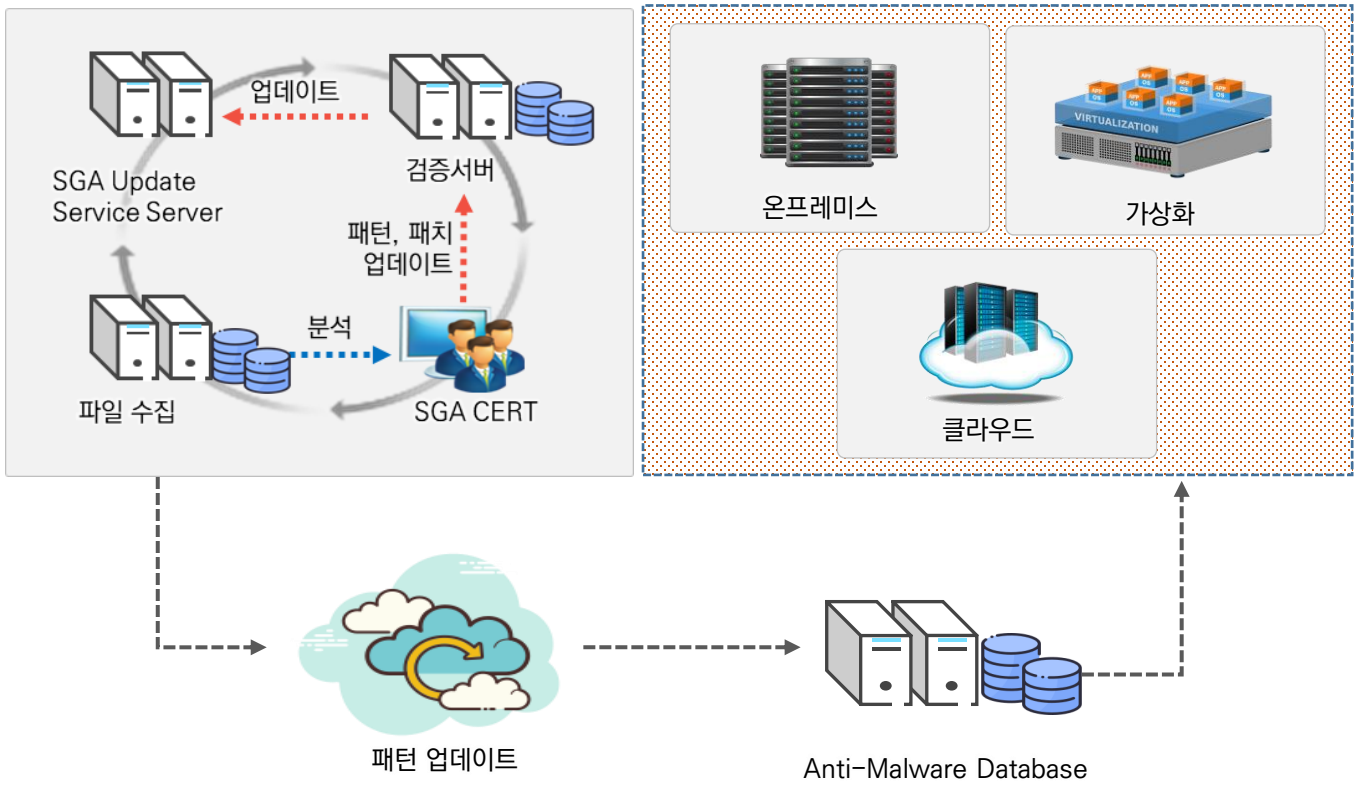
[Anti-Malware 모니터링 대시보드]

[Anti-Malware 이벤트]

3. 주요 기능 - Anti-Malware

Linux 및 Windows 서버 등 플랫폼 기반에서 MS Office 매크로 바이러스, 웜, 트로이목마 등 멀웨어 탐지하고 차단

✓ 시그니처(패턴) 기반으로 Malware를 탐지하여 보안 컴플라이언스 충족
- Zip, RAR, 7zip, ARJ, Tar, Gzip, IMG 등 다양한 아카이브 형식에 대한 기본 지원
- UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack으로 압축되고 SUE, Y0da Cryptor 지원
- 압축 및 난독화 된 ELF 실행 파일 및 휴대용 실행 파일(PE)에 대한 지원



유포 및 차단

- Virus Chaser for Linux는 서버의 악성코드 방역을 위한 솔루션
- 서버에서 PC로 악성코드 확산을 막아주며, PC의 악성코드 유입을 차단

CLI를 통한 동적 사용

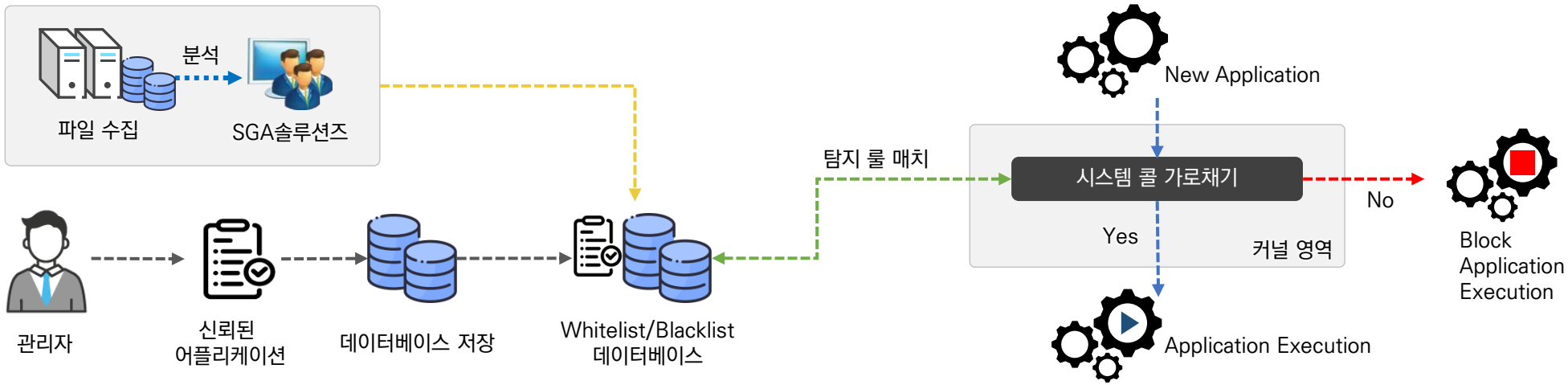
- CLI 명령어를 통한 스캔과 업데이트 기능을 제공
- 스캔 시 제외할 경로 및 확장자를 등록함으로써 효율적인 스캔 작업을 수행

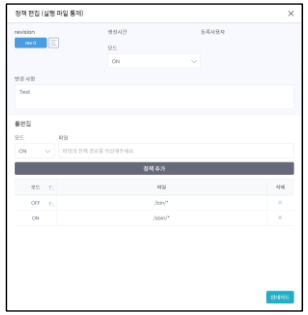
3. 주요 기능 - Application Control

운영체제 커널 레벨에서 화이트/블랙리스트 모두 지원하여 강력한 보안 기능 제공

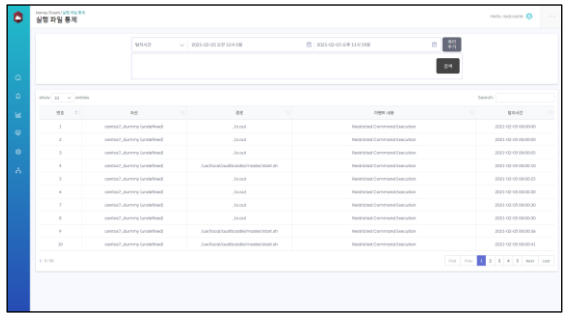
✓ 제로트러스트 관점에서 화이트리스트/블랙리스트 기반으로 어플리케이션 실행을 제어

- 화이트리스트 기반으로 신뢰된 어플리케이션만 실행하거나 또는 블랙리스트 기반으로 실행 차단 어플리케이션 설정으로 보안성을 강화하여 안정적인 IT 서비스 제공





[어플리케이션 통제 정책 설정]



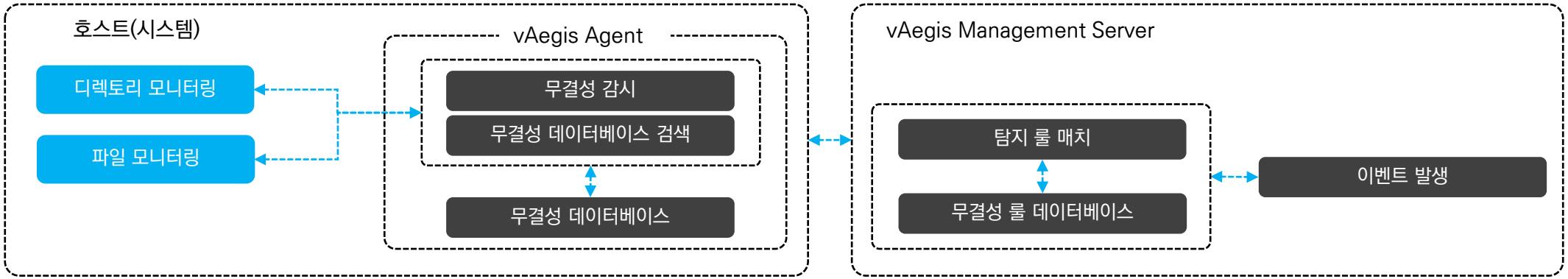
[어플리케이션 통제 위반 로그 조회]

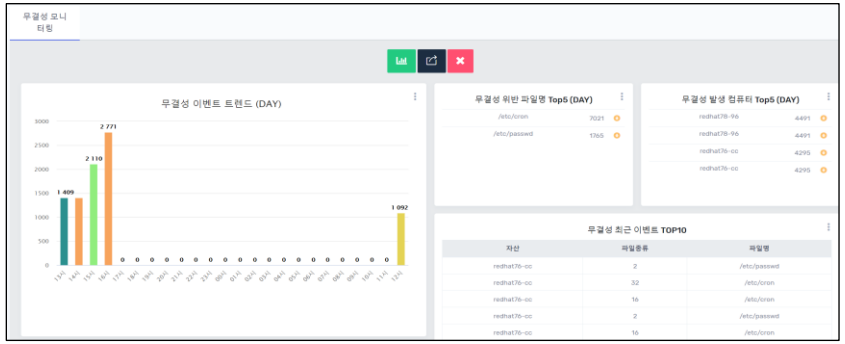
3. 주요 기능 - 무결성 감시

디렉토리, 파일 등 운영체제 바이너리 파일 및 어플리케이션 주요 파일에 대한 무결성 탐지

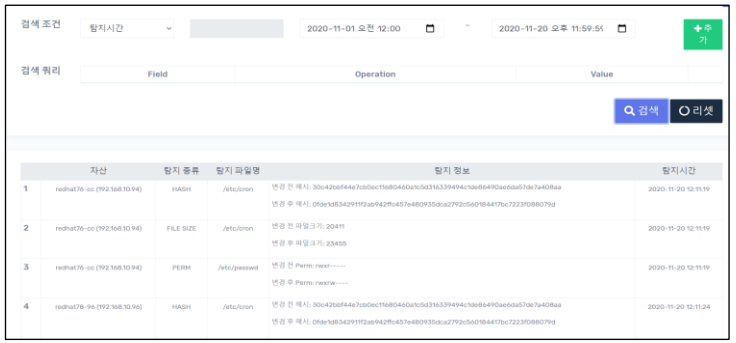
✓ 워크로드가 부팅/구동된 상태에서 시스템 파일이나 구성에 대한 무결성을 실시간으로 모니터링

- 디렉토리와 파일 대한 속성(권한, 크기 등), 내용 그리고 날짜 등을 암호 해시함수인 SHA-256을 사용하여 데이터베이스에 저장하고, 디렉토리와 파일에 대하여 주기적 모니터링하여 데이터베이스와 비교하여 수정 사항 발생 시 로깅하고 그 수정 사항을 관리자에게 경고 이벤트를 보냄





[무결성 감시 대시보드]



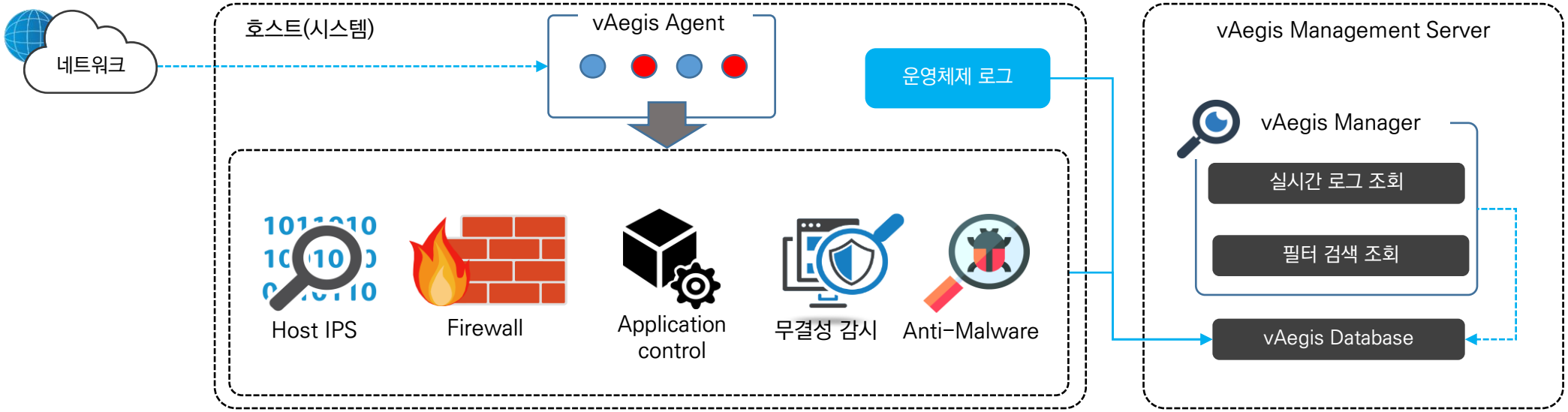
[무결성 감시 검색 조회]

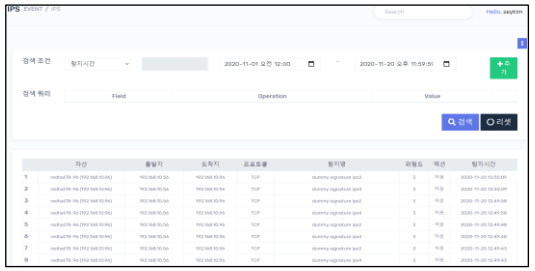
3. 주요 기능 - 로그 관리

운영체제 로그 및 보안 로그를 수집/저장하고 다양한 필터를 통한 분석 및 조회

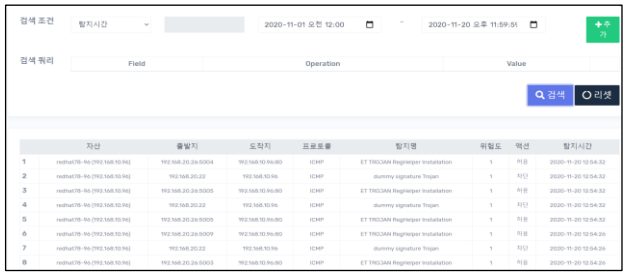
✓ 하이브리드 환경에서 로그를 통합 수집 및 관리

- 시스템에서 발생하는 운영체제 로그 및 vAegis 보안정책(Rule Set)을 위반하는 보안 로그를 수집하고 분석하는 기능 제공





[Host IPS 로그 검색 조회]

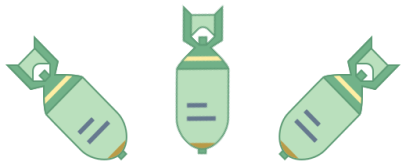


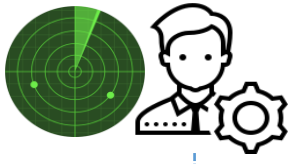
[Anti-Malware 로그 검색 조회]

[무결성 감시 로그 검색 조회]

4. vAegis 특장점

온프레미스 환경을 포함하여 가상화, 클라우드 환경에서 동일한 보안 환경 제공





SGA솔루션즈
위협침해행위 분석

시그니처(패턴) 수시/정기 업데이트

Firewall	• 공격 표면 방어, 내부 확산 방지, DDoS 방어
Host IPS	• 네트워크 트래픽 분석 공격 탐지/차단 • 제로데이 취약점 공격 방어
Anti-Malware	• 시그니처 기반 Malware를 탐지/차단 • 보안 컴플라이언스 충족
Application Control	• 제로트러스트 관점에서 화이트리스트/ 블랙리스트 기반의 어플리케이션 실행 통제
무결성 감시	• 시스템 파일, 구성에 대한 무결성 실시간 감시
로그 관리	• 주요 이벤트 식별 및 처리

온프레미스 

가상화 

클라우드 

동일한 보안 환경 제공

• vAegis는 개별 환경에 국한되지 않고 기존의 온프레미스 환경을 포함하여 가상화 및 클라우드 환경까지 IT 환경 전반에 걸쳐 동일한 보안 환경 제공

일원화된 보안 기능

• vAegis는 단일 Agent를 통하여 Firewall/Host IPS 기능의 네트워크 보안부터 Anti-Malware/Application Control, 무결성 감시 기능의 시스템 내부 보안까지 일원화된 보안 기능 제공

제로데이 취약점 대응

• vAegis는 유입되는 네트워크 트래픽을 분석하여 탐지 및 대응하는 호스트 기반의 IPS 기능을 통하여 제로데이 취약점으로 부터 서버를 보호

IT 서비스 연속성 제공

• vAegis는 IT 보안 강화를 통한 시스템의 안정적인 운영으로 지속적인 IT 서비스를 가능하게 하고 보안 위협으로부터 사전 대응 및 실시간 대응으로 잠재적인 보안 위협 제거

Ⅲ. 클라우드 워크로드 보안 전략

1. CWPP 운용 시 Security Hole
2. 서버보안 운용 시 CWPP Security Hole 제거
3. 서버보안(Secure OS)
4. 서버보안(Secure OS)과 CWPP 주요 기능
5. 서버보안(Secure OS)과 CWPP 동시 운용 시 이슈
6. 클라우드 플랫폼에서 보안 극대화

1. CWPP 운용 시 Security Hole

CWPP의 주요 보안 기능은 알려진 패턴 기반 탐지 및 대응

CWPP 주요 기능

하이브리드 및 멀티 클라우드 환경에서 서버 워크로드를 보호하기 위한 보안 플랫폼

☑ 서버 방화벽
- 세분화된 방화벽을 구축하고 가시성을 확보

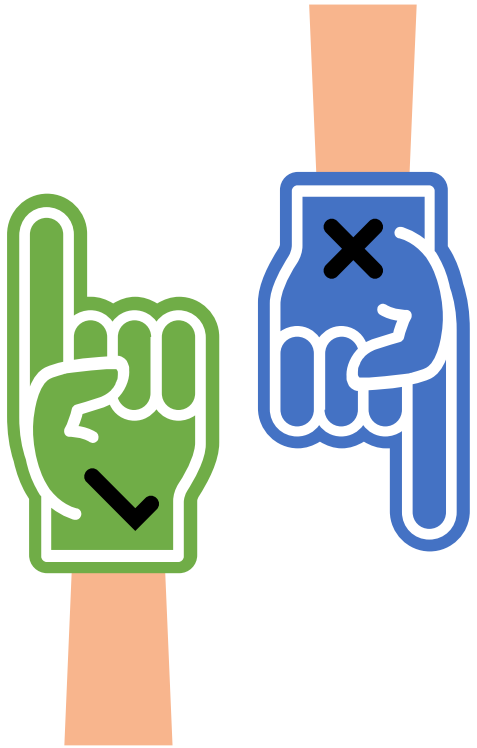
☑ Host IPS
- 네트워크 트래픽 분석하여 공격 탐지 및 차단

☑ Anti-Malware
- 시그니처 가반으로 멀웨어 탐지 및 차단

☑ 애플리케이션 통제
- 화이트리스트 기반으로 애플리케이션 실행 제어

☑ 무결성 검사
- 중요 파일/폴더, 프로세스 등 이 변경 됨을 감지하여 통보

☑ 로그 감사
- 많은 보안 감사 로그 중에서 중요한 이벤트 검색 기능을 제공하고 위험도별 분류 기능 제공



CWPP의 Security Hole

CWPP의 주요 보안 기능은 알려진 패턴(시그니처) 기반으로 탐지 및 대응

☒ IPS, Anti-Malware는 알려진 패턴(시그니처) 기반 보안 기능
- 신규 및 변종 공격에 대응 불가
- APT 공격의 지능적인 공격에 대응 불가

☒ 내부자 통제 기능 부재
- 슈퍼 유저 권한 탈취 공격에 대한 대응 불가
- 내부자의 악의적인 행위 대응 불가
- 내부자의 Human Error 대응 불가

☒ 무결성 검사는 파일 변조 차단 불가
- 변경에 대한 감지만 제공하여 시스템 주요 바이너리 파일 및 어플리케이션 설정 파일 등에 대한 변조 차단 불가
- 정상 업데이트와 변조 행위 식별 불가로 위협 행위에 대한 대응 불가

2. 서버보안 운용 시 CWPP Security Hole 제거

커널 레벨에서 보안 정책 기반의 우회가 불가능한 강력한 접근 통제

CWPP의 Security Hole

CWPP의 주요 보안 기능은 알려진 패턴(시그니처) 기반으로 탐지 및 대응

☒ IPS, Anti-Malware는 알려진 패턴(시그니처) 기반 보안 기능

- 신규 및 변종 공격에 대응 불가
- APT 공격의 지능적인 공격에 대응 불가

☒ 내부자 통제 기능 부재

- 슈퍼 유저 권한 탈취 공격에 대한 대응 불가
- 내부자의 악의적인 행위 대응 불가
- 내부자의 Human Error 대응 불가

☒ 무결성 검사는 파일 변조 차단 불가

- 변경에 대한 감지만 제공하여 시스템 주요 바이너리 파일 및 애필리케이션 설정 파일 등에 대한 변조 차단 불가
- 시스템 업데이트와 변조 행위 식별 불가로 위협 행위에 대한 대응 불가

서버보안(RedCastle) 대응

보안 정책을 기반으로 행위가 발생했을때 커널에서 system-call을 hooking하여 참조 모니터방식으로 허용 여부를 결정함으로써 기존 위협이든 신•변종의 보안 위협과 내부자의 행위 모두 통제 가능

☑ 인가된 행위 또는 비 인가된 행위를 사전에 식별하지 않고 사전에 설정된 보안 정책에 따라 접근 허용 여부를 결정하여 신•변종의 보안 위협과 APT 공격의 지능적인 보안 위협에 대응

☑ 모든 행위는 커널에서 system-call을 hooking함으로써 우회 접근•실행 등의 모든 행위 차단

☑ 서버보안 RedCastle은 슈퍼 유저 또한 일반 사용자와 동일하게 보안 정책 적용의 대상으로 간주하여 슈퍼 유저의 권한이 탈취된 보안 위협일지라도 보안 정책에 따라 통제

☑ 내부자의 악의적인 행위나 Human Error도 보안 정책에 따라 통제

☑ 단순히 무결성 검사가 아닌 커널에서의 파일 변조 행위를 사전에 차단하여 시스템 바이너리 파일 및 애플리케이션 설정 파일 등의 변조 방지

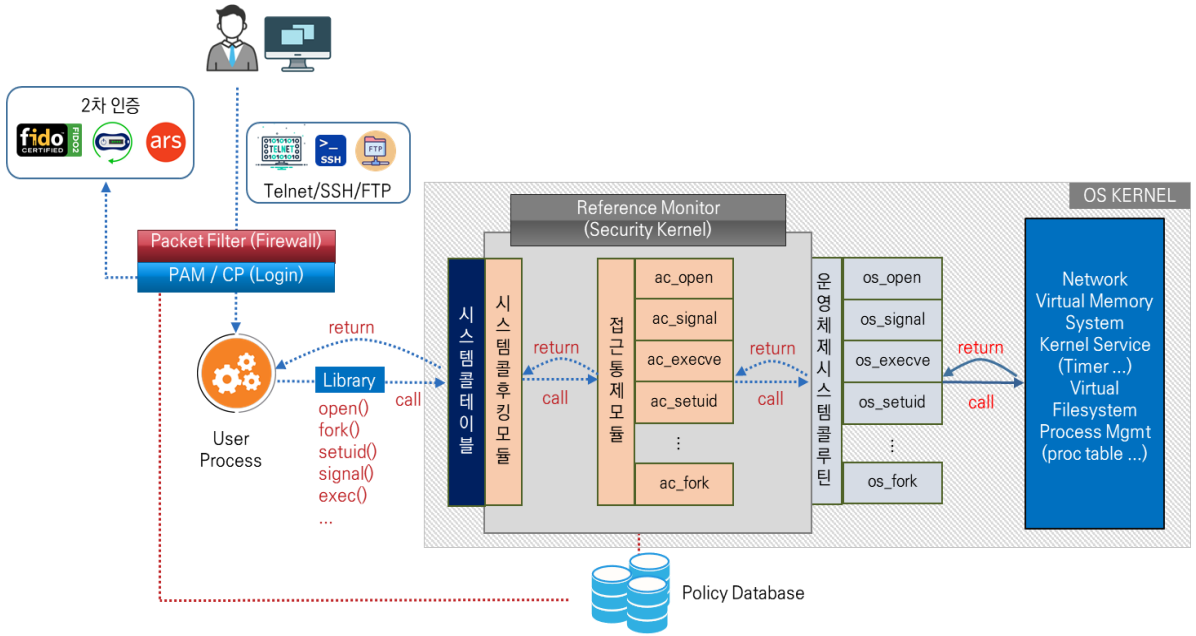
☑ 시스템 업데이트나 변조 행위 등을 식별할 필요없이 설정된 보안 정책에 따른 허용 여부만 결정함으로써 강력한 보안 기능 제공

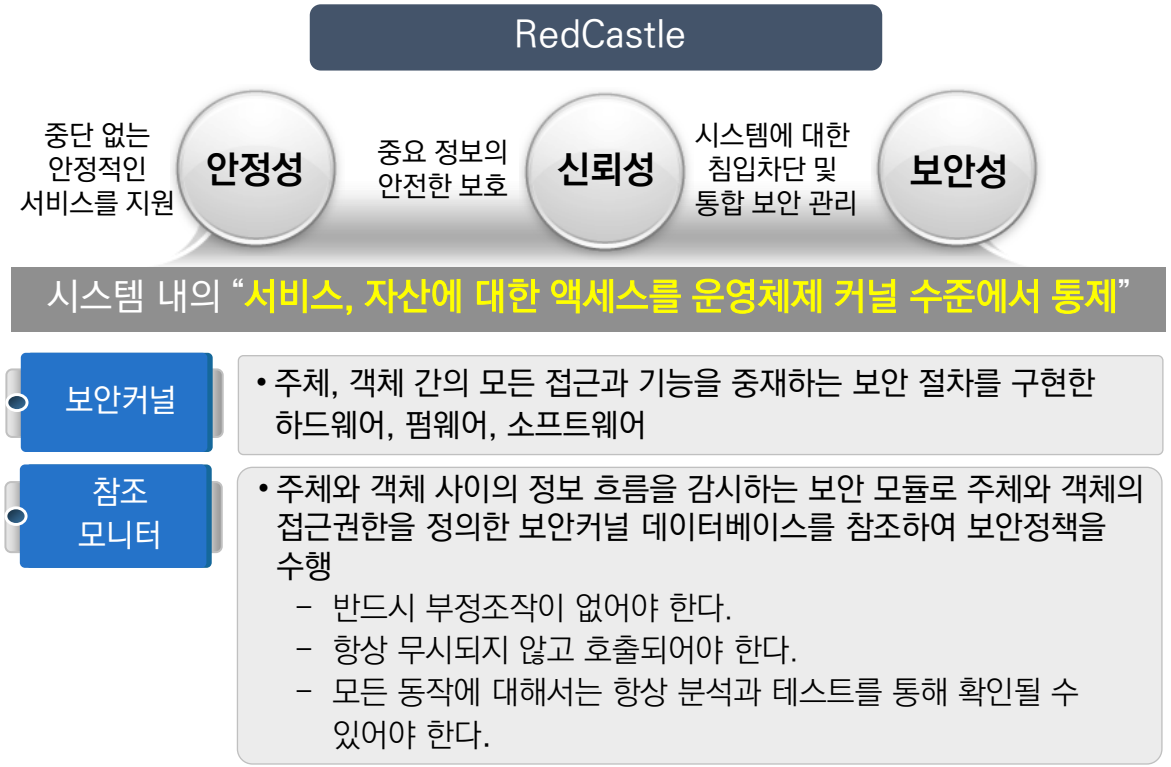
3. 서버보안(Secure OS)

운영체제 커널에서 시스템 콜을 가로채어 레퍼런스 모니터(정책비교) 방식으로 시스템의 주요 자원(파일, 프로세스 등)에 대한 접근 통제

"사이버 공격의 주 대상인 **시스템의 마지막 보안 퍼즐**"

패턴(시그니처)기반의 보안 솔루션들이 놓치는 공격을 **운영체제의 커널 레벨에서 보안 정책 기반으로 사용자의 행위 통제기능**을 구현하여 공격행위를 효과적으로 탐지하고 차단 기능 제공하여 **시스템의 마지막 보안 플랫폼**으로서 효율적이고 높은 성능을 제공합니다.



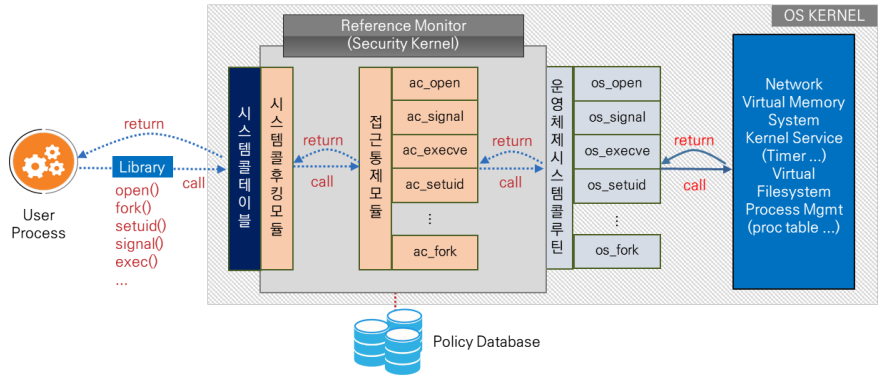


4. 서버보안(Secure OS)과 CWPP 주요 기능

IT 환경의 흐름에 따른 태생적인 다름은 있으나, 기본적인 보호 대상은 같다.

서버보안(Secure OS)

시스템 운영체제의 **커널 레벨에서 보안 정책기반으로 시스템 내의 주요 자산에 대하여 접근을 통제**하는 기능을 구현하여 전통적인 패턴 기반의 보안 솔루션들이 탐지/차단하지 못하는 공격행위를 효과적으로 탐지하고 차단하는 보안 솔루션



[Secure OS 기본 구조]

외부 접근 통제

- 방화벽
- 네트워크 바인드 통제
- 로그인 통제
- 경유 통제
- 공유 폴더 접근 통제

내부 접근 통제

- 명령어 실행 통제 / 파일 접근 통제
- 계정 이동 통제
- 파일 무결성 감시
- SetuID 파일 통제
- 프로세스 kill 통제

로그 관리

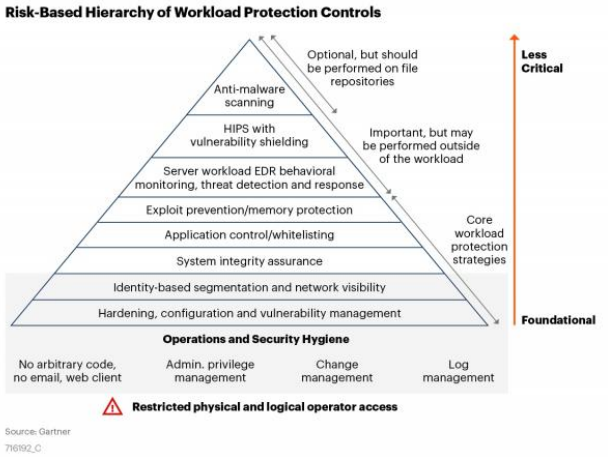
- TTY/커널기반 사용자 추적
- 보안 이벤트 실시간 모니터
- 보안 보고서

관리 기능

- 보안 정책 백업 및 복구
- 보안 정책 배포
- 시스템 계정 관리

CWPP(Cloud Workload Protection Platform)

하이브리드 및 멀티 클라우드 환경에서 서버 워크로드를 보호하기 위한 보안 플랫폼 (가트너)



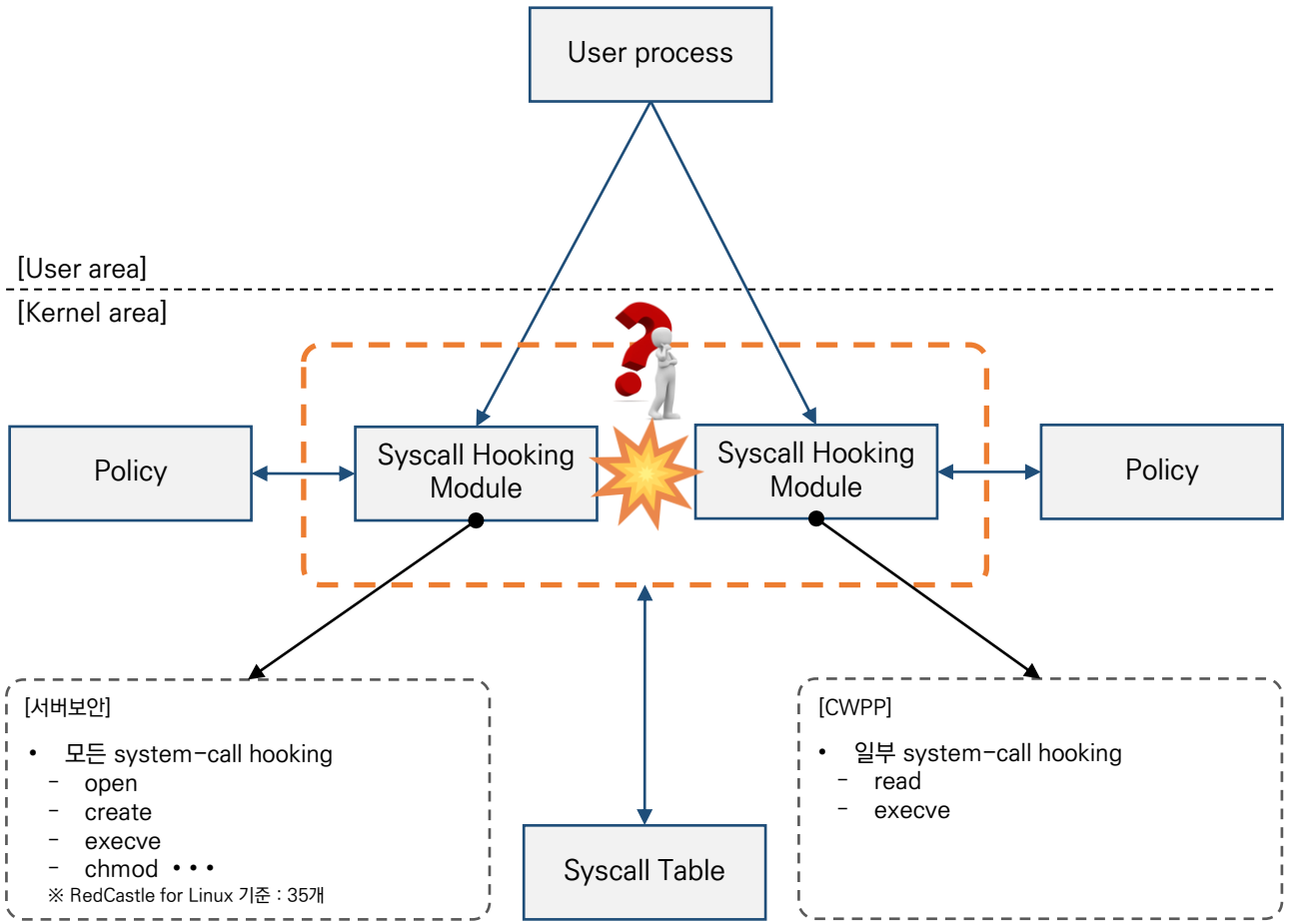
[CWPP 위험기반 계층 구조]

CWPP 주요 기능 (가트너)

- 보안 강화 및 설정/취약점 관리(Hardening, Configuration and Vulnerability Management)
- 네트워크 방화벽, 가시성 확보 및 마이크로세그멘테이션(Network Firewalling, Visibility and Microsegmentation)
- 시스템 무결성 보장(System Integrity Assurance)
- 애플리케이션 제어(Application Control/Whitelisting)
- 익스플로잇 예방 및 메모리 보호(Exploit Prevention/Memory Protection)
- 서버 워크로드 EDR, 행위 모니터링 및 위협 탐지·대응(Server Workload EDR, Behavioral Monitoring and Threat Detection/Response)
- 호스트 기반 침입 탐지 시스템(Host-Based IPS With Vulnerability Shielding)
- 안티 멀웨어(Anti-malware Scanning)

5. 서버보안(Secure OS)과 CWPP 동시 운용 시 이슈

서버보안과 CWPP 모두 커널 레벨에서 시스템 콜 후킹(System-Call Hooking)



서버보안과 CWPP 모두 커널 레벨에서 system-call hooking

- 서버보안
  - 명령어 실행통제, 파일접근 통제, 프로세스 kill 통제 등의 보안 기능을 수행하기 위해 커널에서 system-call hooking 사용
- CWPP
  - Anti-Malware, 애플리케이션 통제의 보안 기능을 수행하기 위해 커널에서 system-call hooking 사용

서버보안과 CWPP 동시 운용 시 문제점

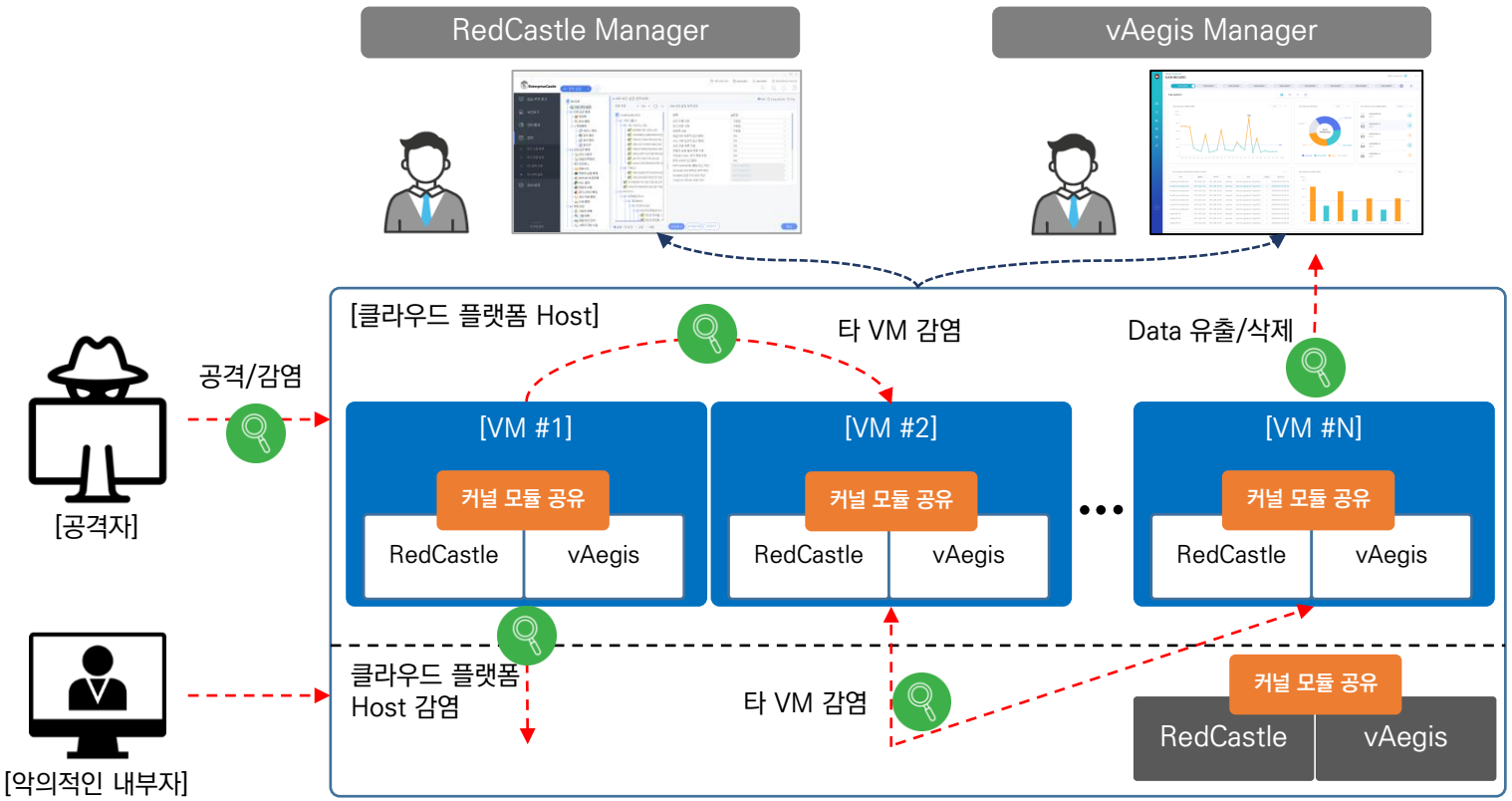
- 서버보안과 CWPP에서 서로 system-call hooking
  - ➤ 커널 패닉 등의 시스템 장애 발생 / 보안 기능 비정상 동작

서버보안과 CWPP 중 하나의 보안 솔루션만 운용 가능

6. 클라우드 플랫폼에서 보안 극대화 전략

vAegis는 Secure OS인 RedCastle과 동시 운용으로 멀티 보안 플랫폼 구성

유연성 보장 | 비용절감 | 알려진 보안 위협 차단 | 시그니처 기반 보안 강화 | **IT 서비스 연속성/안전성 보장** | 정책 기반 보안 강화 | 알려지지 않은 보안 위협 차단 | 우회 접근 /실행 차단 | 내부자 위협 차단



RedCastle

- 방화벽
- 네트워크 바인드 통제
- 로그인 통제
- 경유 통제
- 공유 폴더 접근 통제
- 명령어 실행 통제 / 파일 접근 통제
- 계정 이동 통제
- 파일 무결성 감시
- SetuID 파일 통제
- 프로세스 kill 통제

vAegis

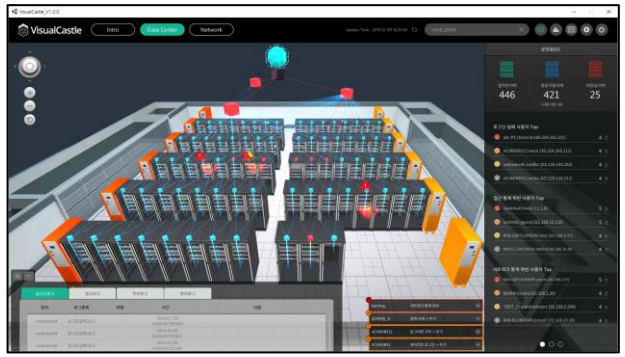
- Host IPS
- Application Control
- Anti-Malware
- Firewall (RedCastle 기능 중 선택)
- 무결성 감시 (RedCastle 기능 중 선택)

6. 클라우드 플랫폼에서 보안 극대화 전략

3D 시각화 솔루션 VisualAegis 연동

“ 하이브리드 환경에 최적화된 보안 **3D 시각화 솔루션** ”

복잡/다양한 클라우드 환경에서 **보안 상황을 시각적으로 강화**해 주는 보안 가시성 확보를 통해 진화하는 보안 위협으로 부터
빠르고 효율적으로 대응을 가능케하는 **보안 시각화 솔루션**



✓ 3D 통합 보안 모니터링
- 운영 중인 IDC나 서버룸 또는 클라우드의 내부 구성을 3D로 재현하여 쉽게 확인할 수 있는 직관적인 UI 제공

✓ 통합 보안 관리/직관적 대응
- 시스템 로그, 보안로그, 시스템 상태에 대해 시각적으로 확인하고 직관적으로 대응 가능

✓ 경로분석/사용자 행위 추적
- 서버에 접근하는 사용자의 접근 경로를 분석, 토폴로지 Map으로 표현하여 직관성을 제공하고, 사용자의 모든 행위를 동영상처럼 재연 가능한 감사 기능 제공

✓ 로그의 통합 관리
- 이기종 다중 운영체제에 대한 시스템 로그와 보안 로그를 중앙에서 통합 수집/관리

Thank You !

The most reliable index, secured by SGA Solutions