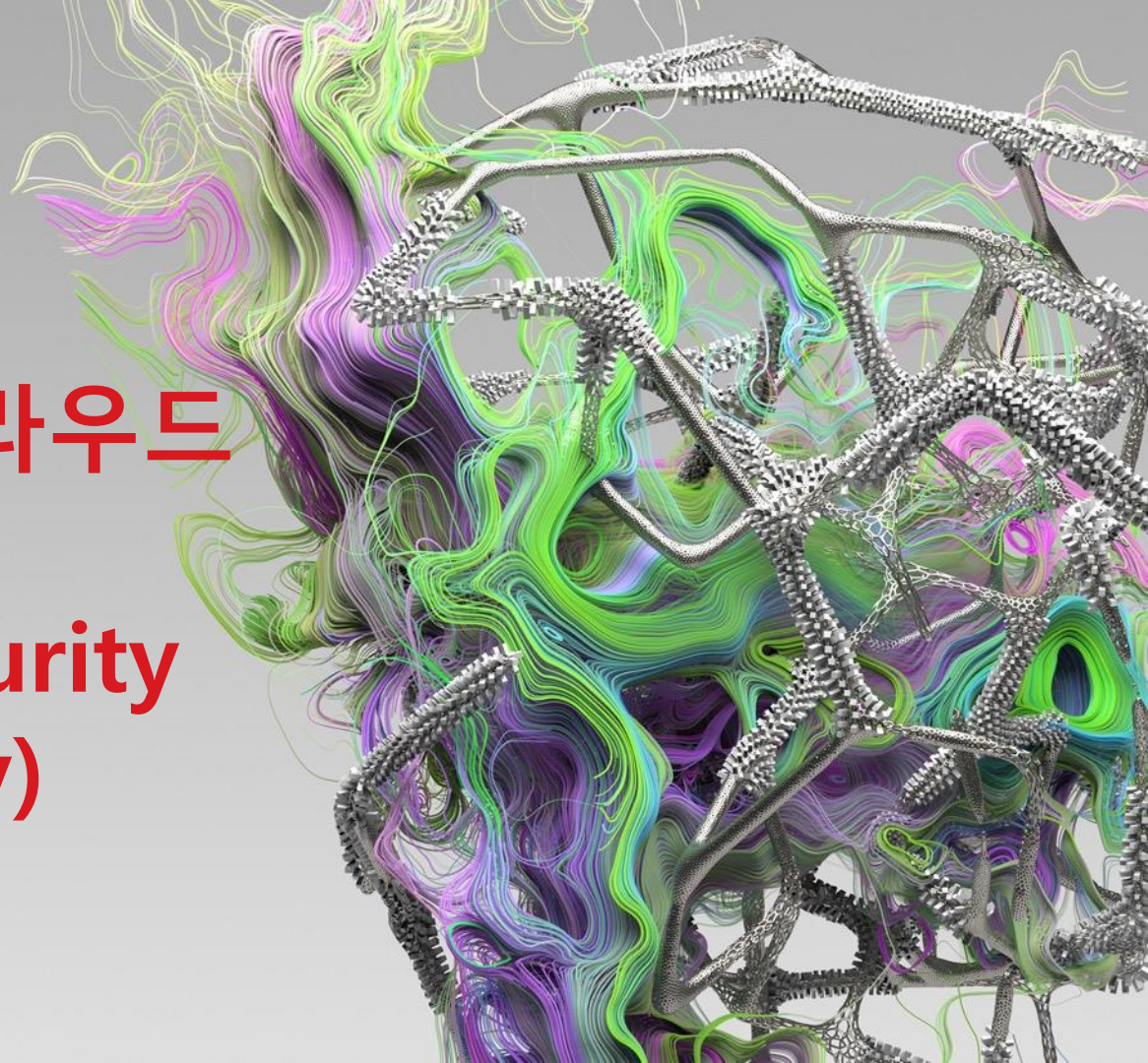
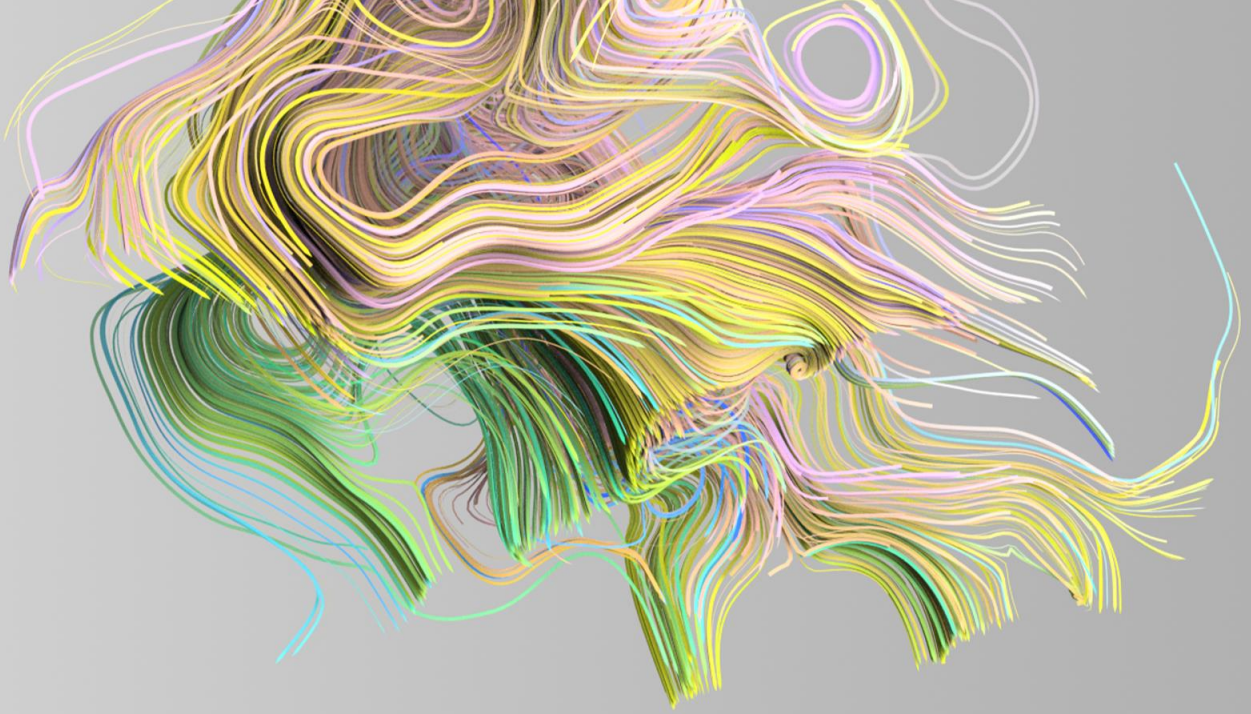
하이브리드 클라우드 보안을 위한 Workload Security (Deep Security)

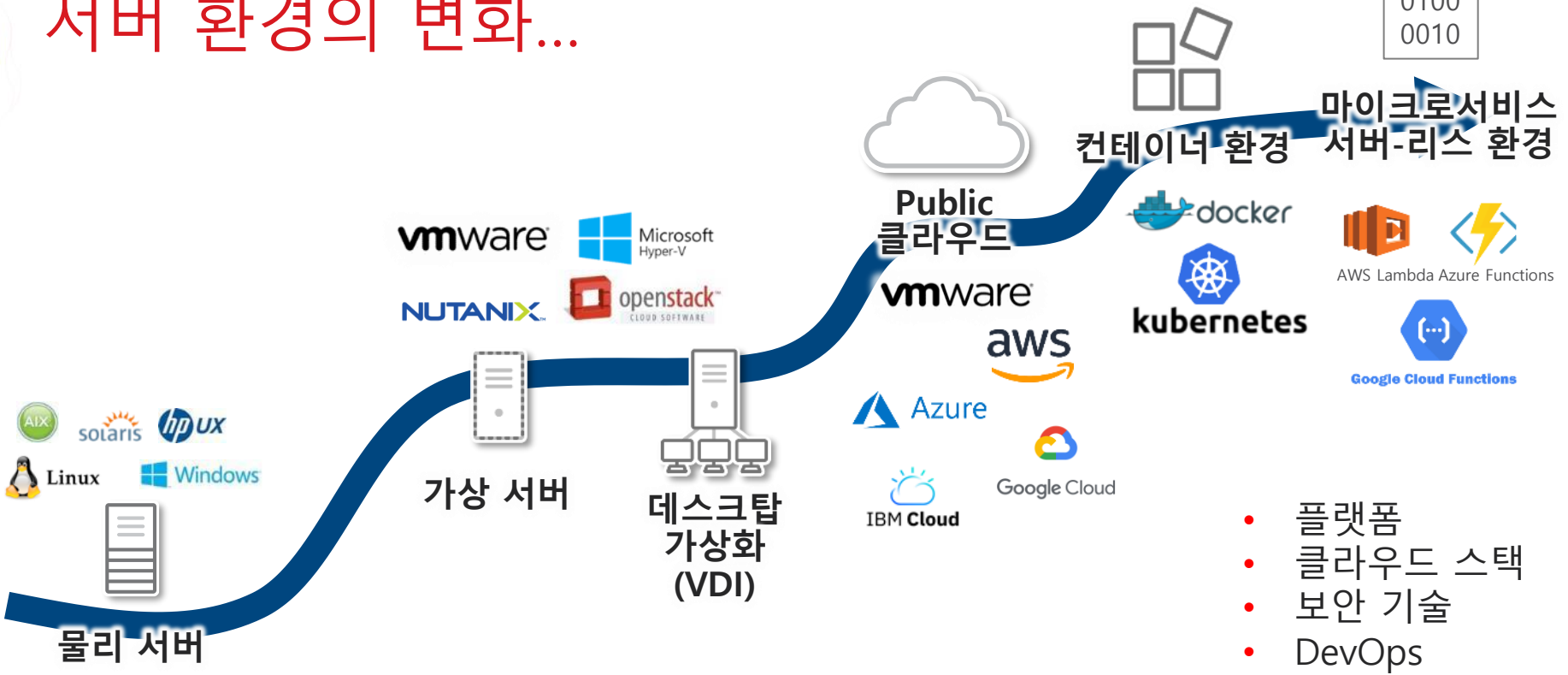
Trend Micro





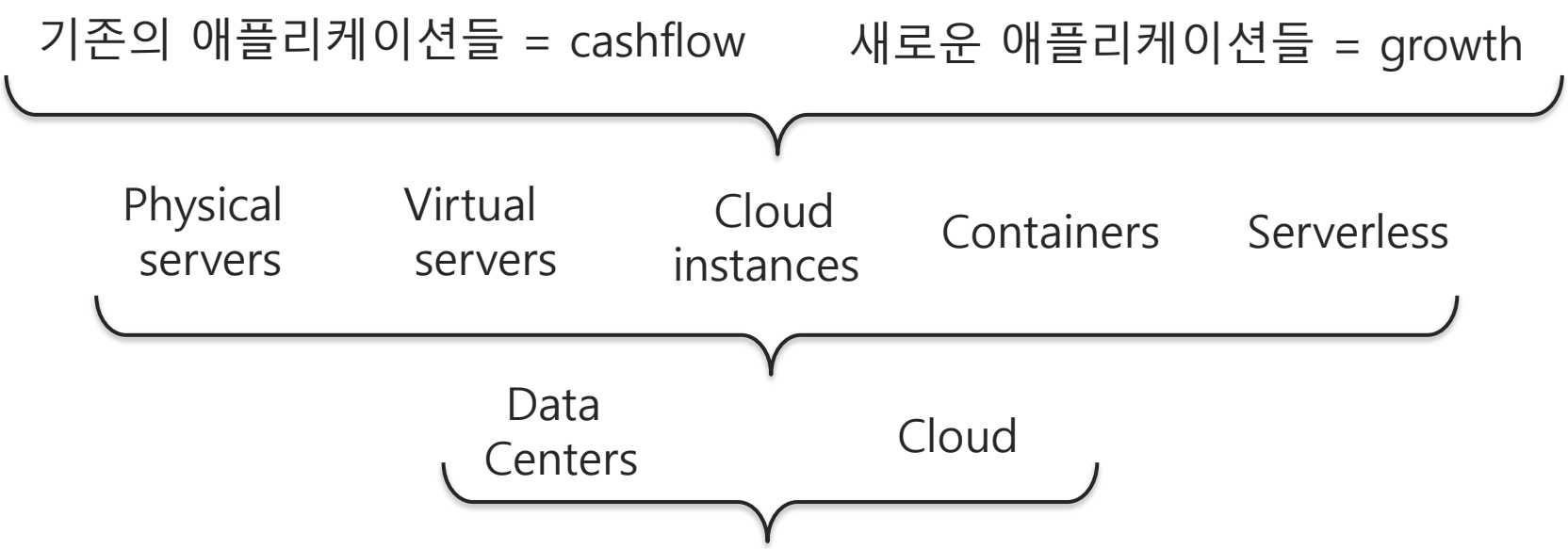
하이브리드 클라우드 보안?

서버 환경의 변화...



- 플랫폼
- 클라우드 스택
- 보안 기술
- DevOps
- DevSecOps

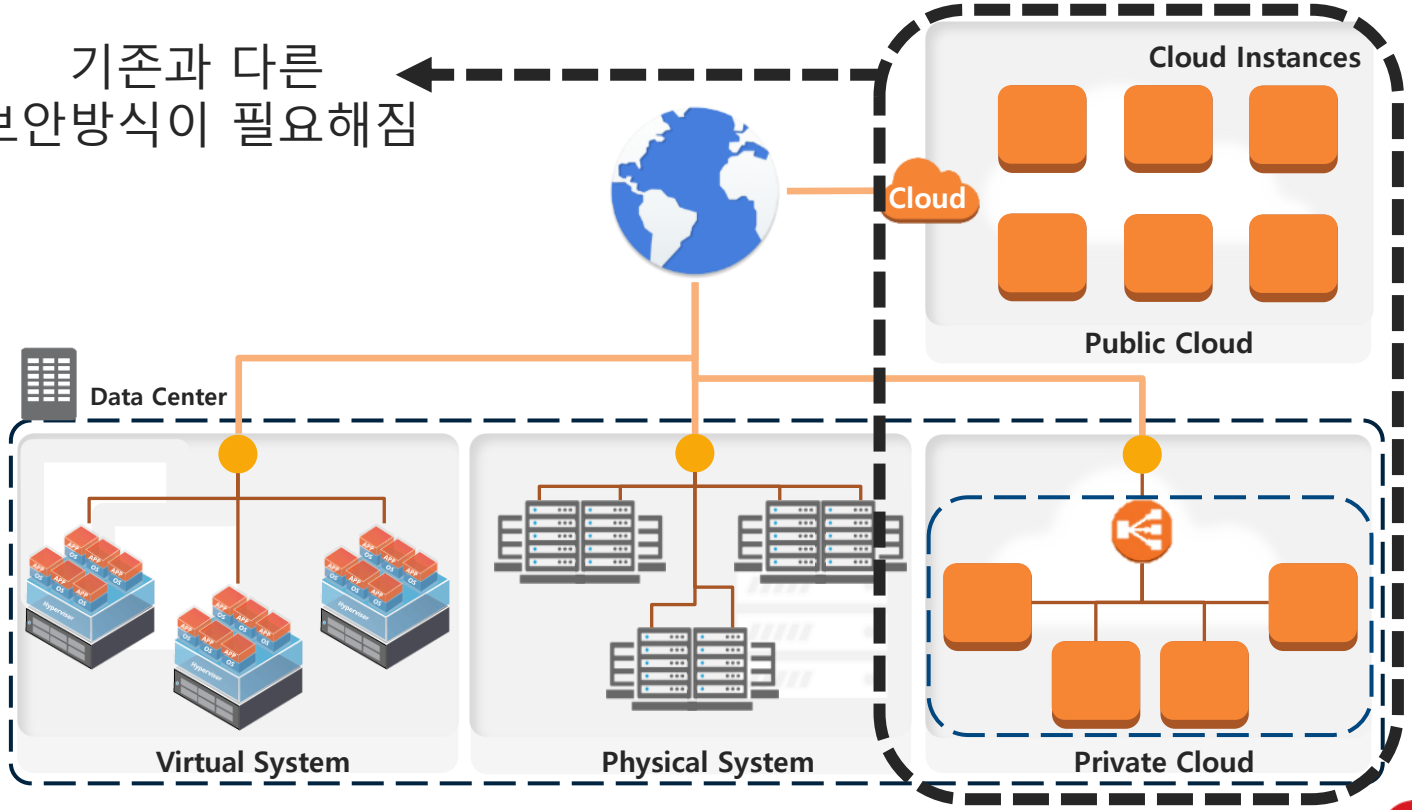
변화하고 있는 애플리케이션



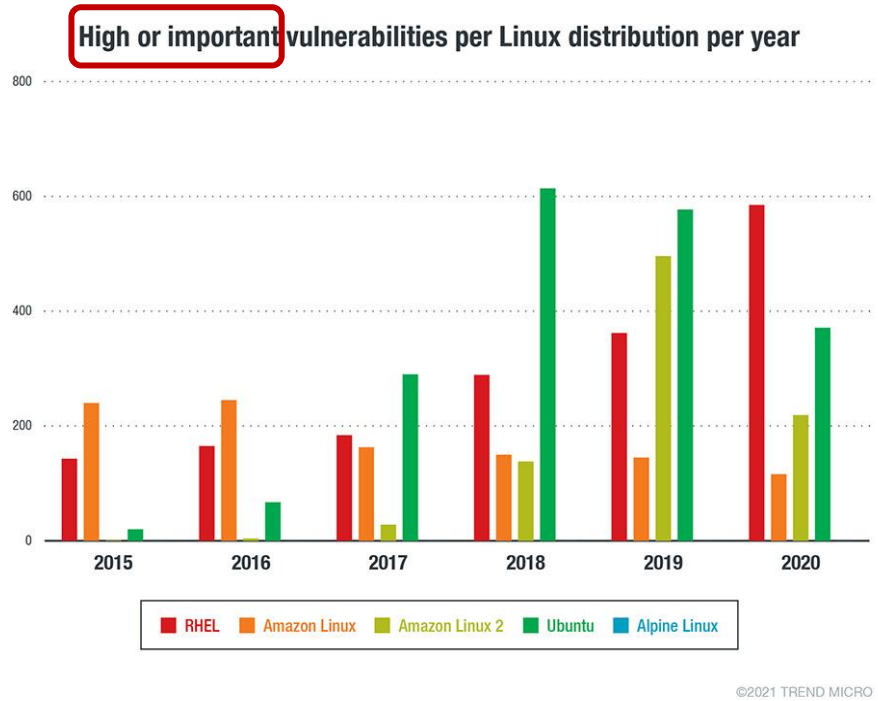
하이브리드 인프라 보안 및 운영

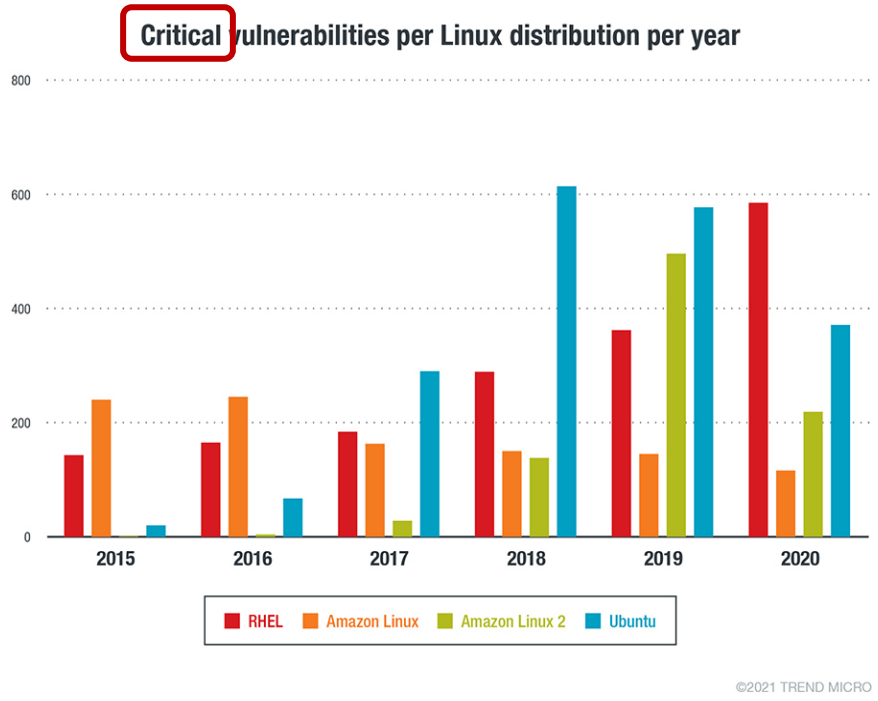
클라우드 보안 구현 방향

기존과 다른
보안방식이 필요해짐



Linux OS 취약점 증가





Sourced by Trend Micro Research Center, 2021

지속적으로 발생하는 취약점 들

Heartbleed

WannaCry

Erebus

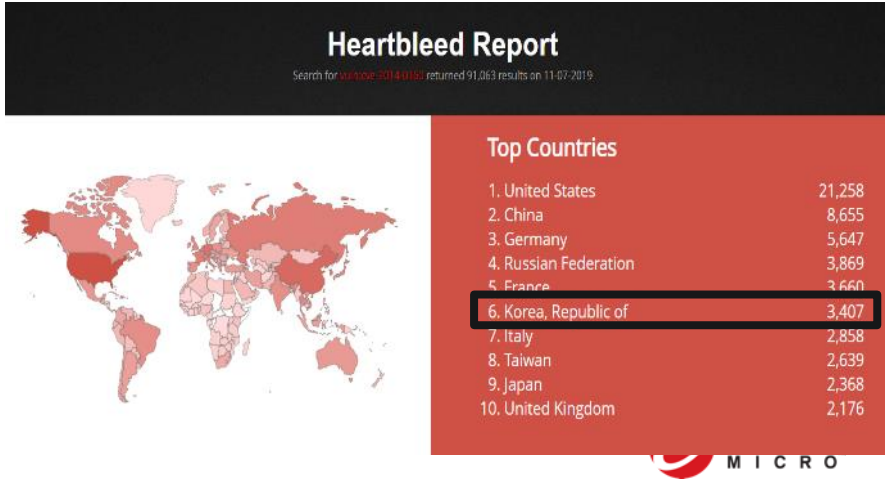
ZERO DAY INITIATIVE

Trend Micro ZDI detected 1449 vulnerabilities in 2018. This powers unmatched timeliness for virtual patches.

runC

kubernetes

The Apache Software Foundation
http://www.apache.org/
Struts™ 2



Windows

보안요구사항 - 하이브리드 클라우드

강력한 보안

악성코드방어 뿐만 아니라 **취약점 방어**, 허가되지 않은 **접근 제어**

일관된 보안 관리

다양한 환경에 동일한 보안정책관리, 하나의 보안관리 시점 제공

자동화된 보안관리

DevOps 파이프라인에 부담이 되지않는 **자동화된 보안**

하이브리드 클라우드를 위한 보안 적용범위

Build Pipeline

Image Scanning

Vulnerability Scanning

Malware Detection

Sweeping & Hunting

Runtime

Network Security

Intrusion Prevention

Firewall

Vulnerability Scanning

System Security

Application Control

Integrity Monitoring

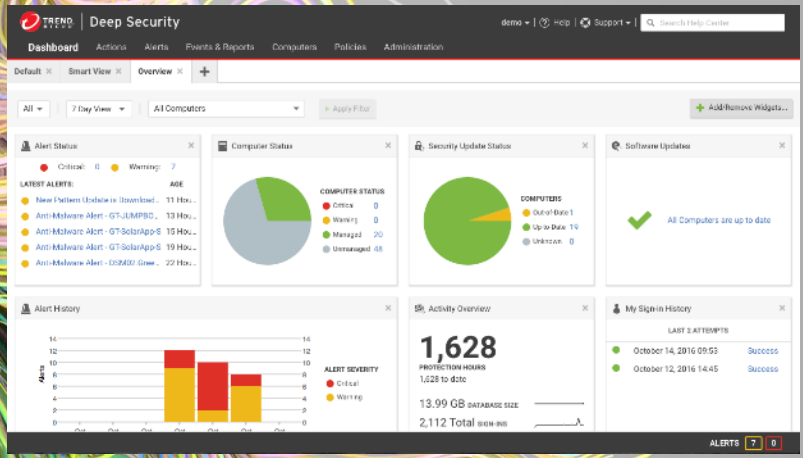
Log Inspection

Malware Prevention

Anti-Malware

Behavioral Analysis

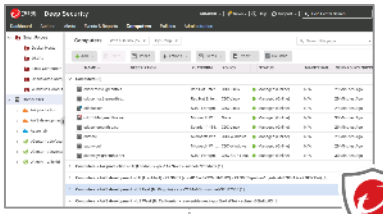
Sandbox Analysis



Workload Security (Deep Security)

Cloud One – Workload(Deep) Security

(#1 클라우드 네이티브 보안솔루션)



Workload Security
(Deep Security)

Data Center

vmware

NUTANIX

Microsoft Hyper-V

Public Cloud

aws

Azure

Google Cloud

Containers

docker

kubernetes

RED HAT OPENSHIFT

TREND MICRO

하이브리드 클라우드 보안 Workload(Deep) Security

Container Security

Pre-deployment

Image Scanning

Vulnerability Scanning | Malware Detection | Sweeping & Hunting

Continuous image scanning for malware & vulnerabilities

Workload(Deep) Security

Network Security

Intrusion Prevention | Firewall | Vulnerability Scanning

Stop network attacks, shield vulnerable applications & servers

Runtime / Deployed

System Security

Application Control | Integrity Monitoring | Log Inspection

Lock down systems & detect suspicious activity

Malware Prevention

Anti-Malware | Behavioral Analysis & Machine Learning | Sandbox Analysis

Stop malware & targeted attacks

Environments

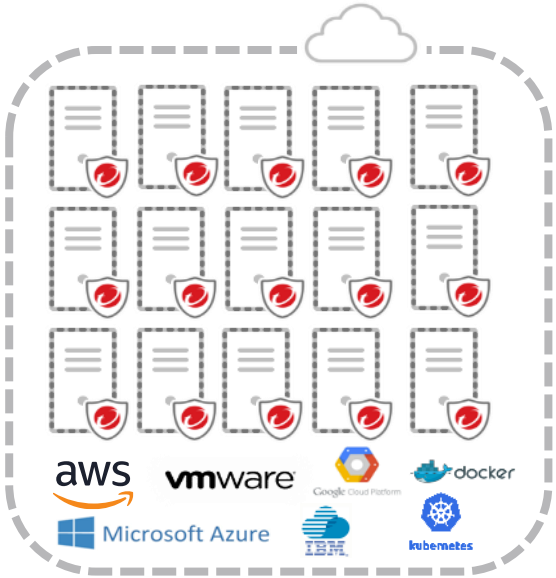
Platforms

API & Integrations

하이브리드 클라우드를 위한 보안 요구 사항

Hybrid Cloud Security

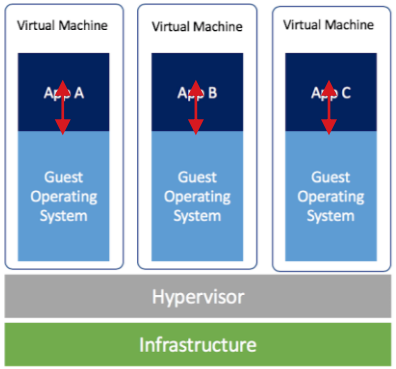
물리, 가상, 클라우드 및 컨테이너 배포에 대한 완전한 가시성을 갖춘 **단일 보안 관리 콘솔**

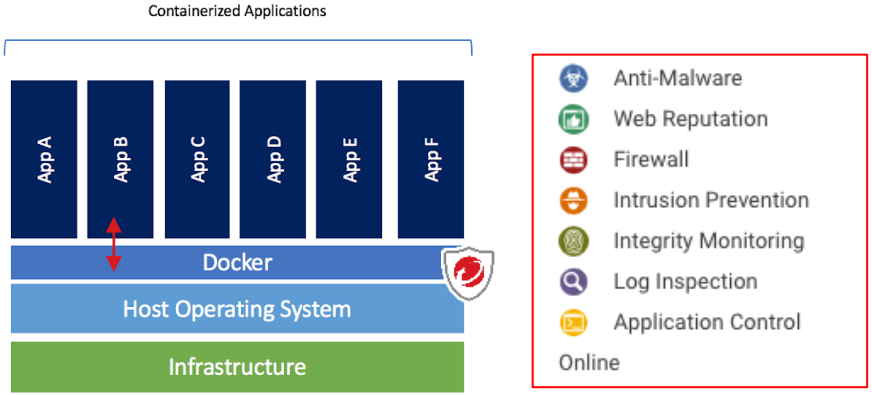


TREND MICRO

Workload(Deep) Security – 도커 호스트 보호

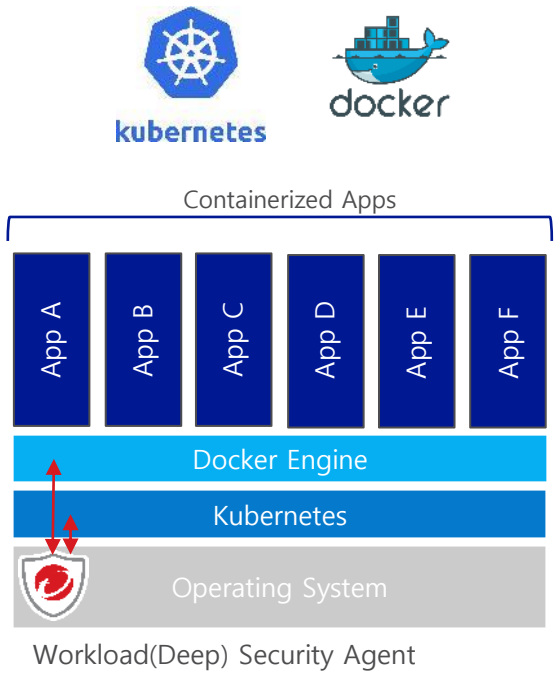
- Docker에서 실행되는 컨테이너 애플리케이션은 호스트 커널 공유
- 도커 호스트가 손상되면 모든 컨테이너 공격 가능



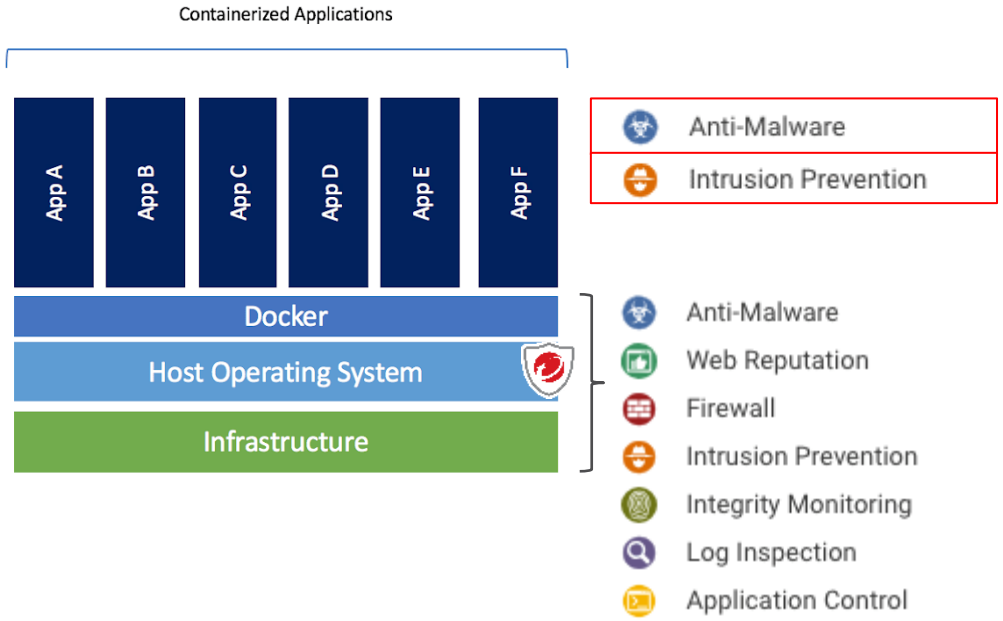


Workload(Deep) Security – 쿠버네티스, 도커 보호

- 도커 & 쿠버네티스 주요 오브젝트 모니터링
  - 도커, 쿠버네티스 자동 감지
  - 소프트웨어 업/다운 그레이드, 삭제
  - 실행파일 속성 변경
  - 실행중인 프로세스, 데몬
    - etcd, Kubelet, Kube-apiserver
  - 주요 설정 파일
    - Config, certs, keys, yaml files
  - Iptables 룰
  - 주요 디렉토리 접근 권한



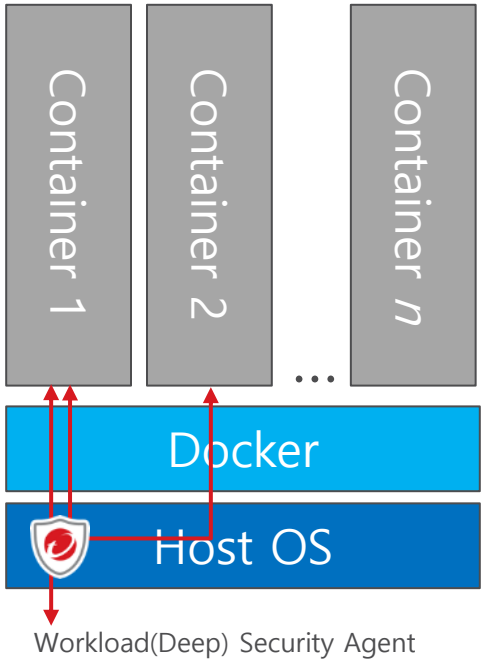
Workload(Deep) Security – 컨테이너 내부로 보호기능 확장



- 컨테이너 응용프로그램 보호
- 실시간 Anti-Malware (AM) 검사를 통해 악성 코드로부터 보호
- IPS로 애플리케이션 취약점을 이용한 공격으로 부터 보호
- 무결성 모니터링기능으로 컨테이너 변조 실시간 감지

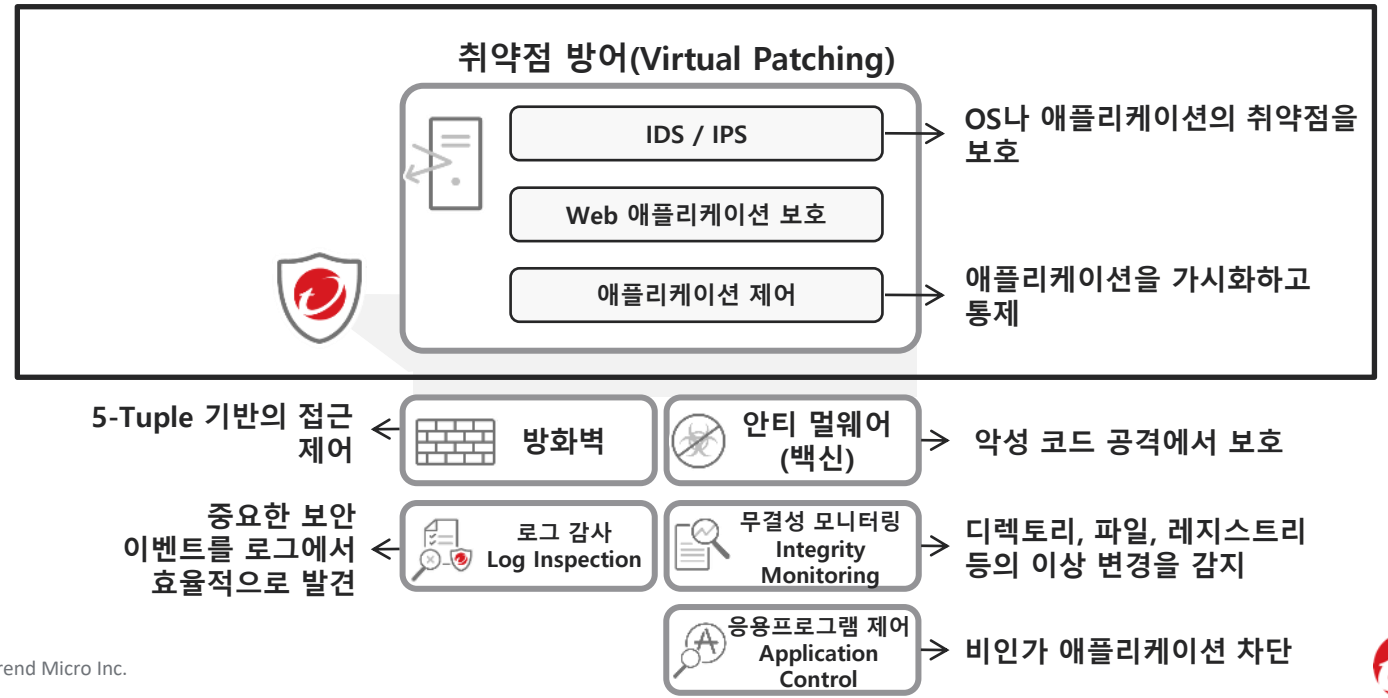
Workload(Deep) Security – 컨테이너 내부로 보호기능 확장

- 컨테이너 간의 트래픽을 검사하도록 DSA를 구성 가능
- "Scan Container Network Traffic" 옵션을 활성화
  - 네트워크 트래픽 후킹 접점이 컨테이너 인터페이스의 로컬로 이동됨
  - 컨테이너 간 "East-West" 트래픽을 포함한 모든 컨테이너 트래픽을 검색
  - 도커 포트 매핑의 영향을 받지 않는 탐지 정확도



Workload(Deep) Security - 통합서버보안

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



Anti-Malware (백신)

안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어

안티 멀웨어 (백신)

실시간 검색
예약 검색
수동 검색
동작 감지 기능에 의한 자기 방어 기능

[Web 평판(Reputation) 서비스]

Web 평판은?
Web에서 위협의 출처 인 악성 URL에 대한 액세스를 미연에 차단합니다.
트렌드 마이크로의 노하우가 담긴 'Smart Protection Network "기능의 하나입니다.

백신 기능

- 악성코드와 스파이웨어/그레이웨어를 탐지하고 치료
- 운영체제에 따라서 지원 기능이 다름

클라우드 패턴 사용

- 파일 평판 조회(WRS)와 웹 평판 조회(WRS)에 클라우드 패턴 방식을 사용

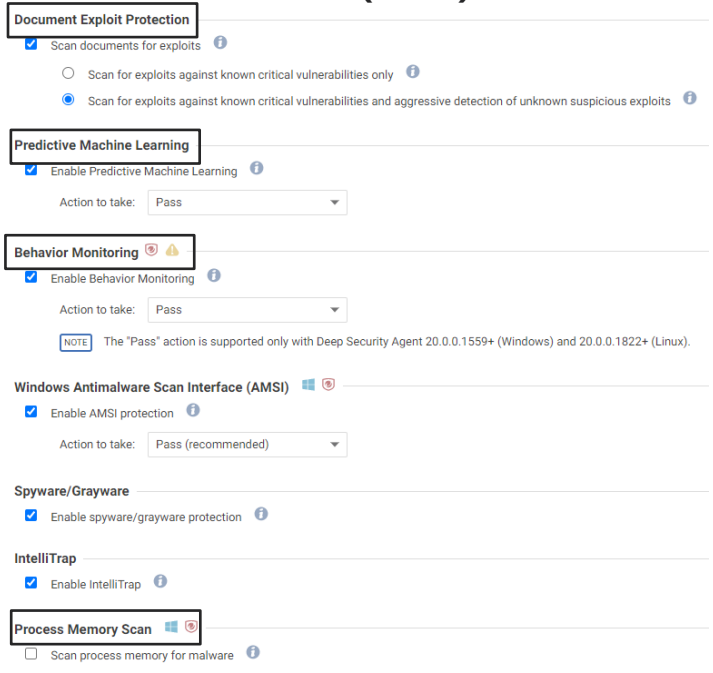
다양한 백신 옵션 설정

- 검색 제외 설정, 격리된 악성코드 복원 및 다운로드, 수동/예약 검색 시 CPU사용량 제한, 압축파일 검색 레벨 등 다양한 백신 정책을 설정

Anti-Malware (백신)

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | 무결성 모니터링 | 응용 프로그램 제어

안티 멀웨어 (백신)



Document Exploit Protection

- 문서 취약점을 가진 문서 파일 탐지
- 문서 취약점이 탐지된 문서파일을 Deep Discovery Analyzer(DDAN)로 전송

Predictive Machine Learning

- 머신러닝 기능으로 신종 악성코드 탐지 & 차단

동작 모니터링 - 랜섬웨어 대응

- 랜섬웨어의 암호화 행위 탐지
- 암호화 행위를 시도하는 프로세스를 강제 종료

실시간 메모리 검색

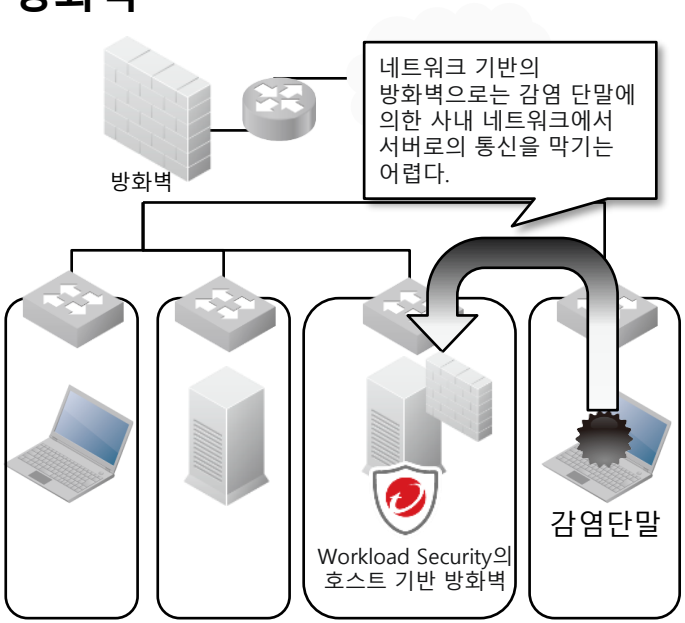
- 메모리 공간에서 실행되는 의심스러운 프로세스를 차단

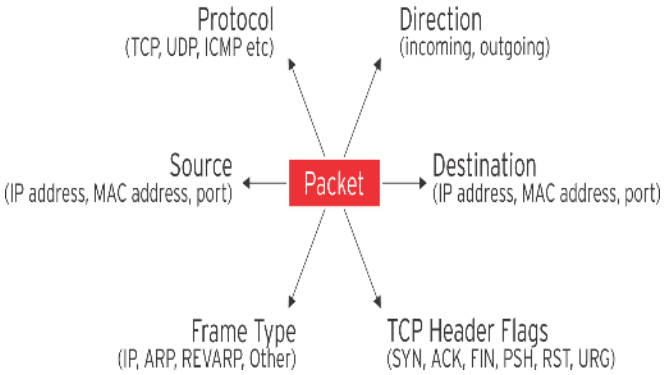
TREND MICRO

Firewall (방화벽)

안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어

방화벽





침입방지 (가상 패치 기능)

안티 멀웨어 (백신) | 방화벽 | **침입 방어 (취약점 방어)** | 로그 감사 | 무결성 모니터링 | 응용 프로그램 제어

- OS 나 응용 프로그램의 취약점 (보안 취약점)을 통한 공격 패킷을 탐지하고 방어하는 기능 (**가상패치**)

가상패치는? 취약성을 수정하는 보안 패치를 설치하는 대신 취약성을 악용하는 공격을 차단하고 가상 패치의 역할을 제공합니다.

포인트 1 : 소프트웨어 코드 레벨에서의 수정을 실시하지 않기 때문에 **실행중인 시스템에 영향이 적다.**

포인트 2: Windows와 Linux 같은 OS뿐 아니라 다양한 애플리케이션의 가상패치가 트렌드 마이크로로부터 제공된다.

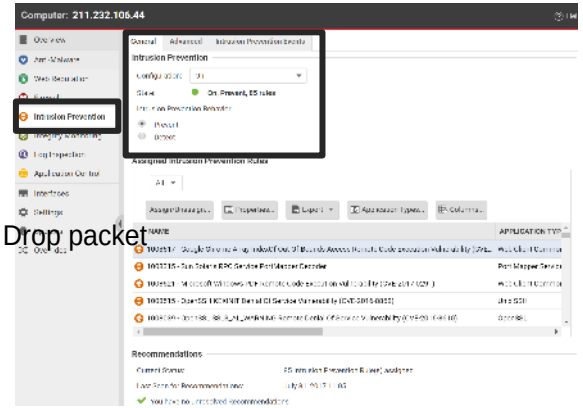
트렌드 마이크로로부터 제공되는 침입 차단 규칙 외 커스텀 규칙을 작성할 수도 있습니다.

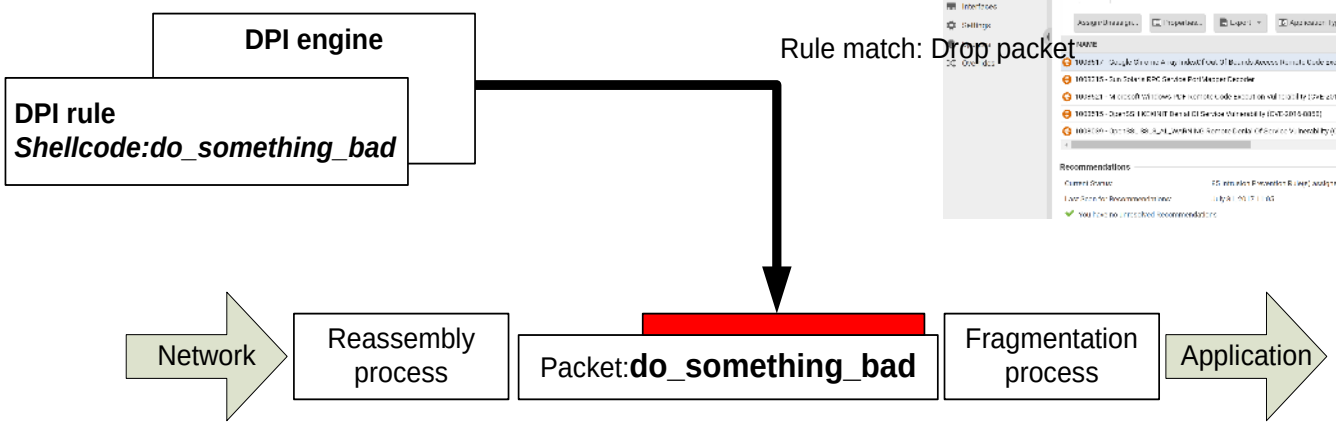
가상 패치는 일시적 보호를 목적으로 한 것으로, 근본적인 해결을 위해서는 보안 패치를 설치할 필요가 있습니다.

침입방지 (가상 패치 기능)

안티 멀웨어 (백신)	방화벽	**침입 방어 (취약점 방어)**	로그 감사	무결성 모니터링	응용 프로그램 제어

- 침입 방지 동작 방식
  - Application Control (패킷 기반)
  - IDS / IPS
  - Web Application Protection

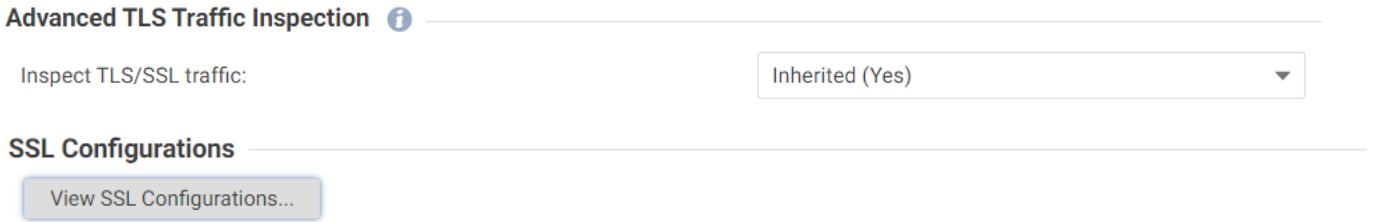




침입방지 (암호화 트래픽 분석 지원)

안티 멀웨어 (백신) | 방화벽 | **침입 방어 (취약점 방어)** | 로그 감사 | 무결성 모니터링 | 응용 프로그램 제어

- SSL 암호화 트래픽 분석 지원



  - **Advanced TLS Traffic inspection**
  - 에이전트(DSA)에서 windows의 iis, exchange, rdp나 Linux의 nginx, apache와 같은 앱의 TLS 통신을 통한 인증서 및 키를 가져와서 TLS 검사를 제공

  - 지원하지 않는 OS, 에이전트 버전 등의 환경에는 기존과 같이 인증서를 에이전트에 수동 적용하여 SSL 트래픽을 분석하는 **SSL Configurations** 설정 방법으로 지원

권장 스캔 (룰 자동 선별, 자동 룰 적용)

수집하는 정보

- 설치 프로그램 정보
- 파일 정보
- 실행되는 프로세스
- 환경 변수
- 열려있는 포트
- 레지스트리 (Windows 만 해당)
- 서비스 (Windows만 해당)

↓

- 응용 프로그램 버전
- 보안 패치의 적용 상황

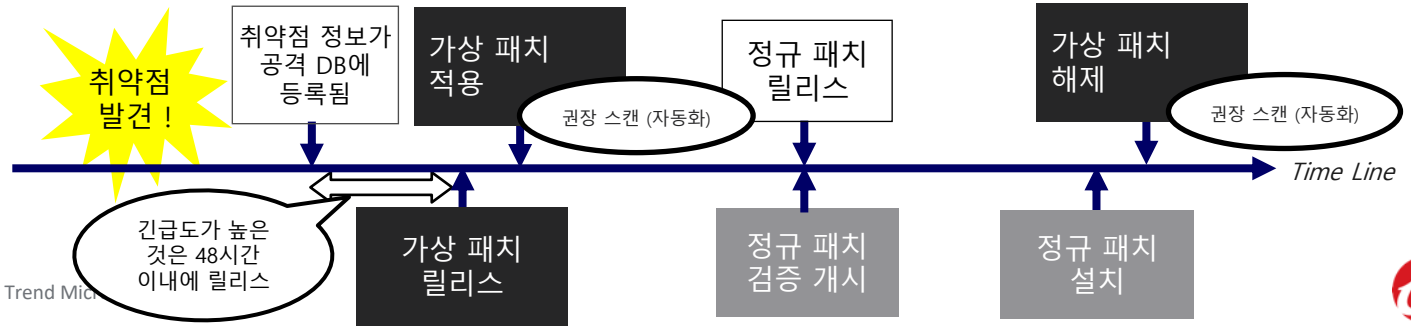
↓

권장하는 룰의 선별 자동 적용

권장 스캔 (룰 자동 선별, 자동 룰 적용)

권장스캔	서버에 설치된 Deep Security Agent가 서버에 설치된 애플리케이션의 정보를 수집하고 필요한 가상 패치를 자동 선택/적용

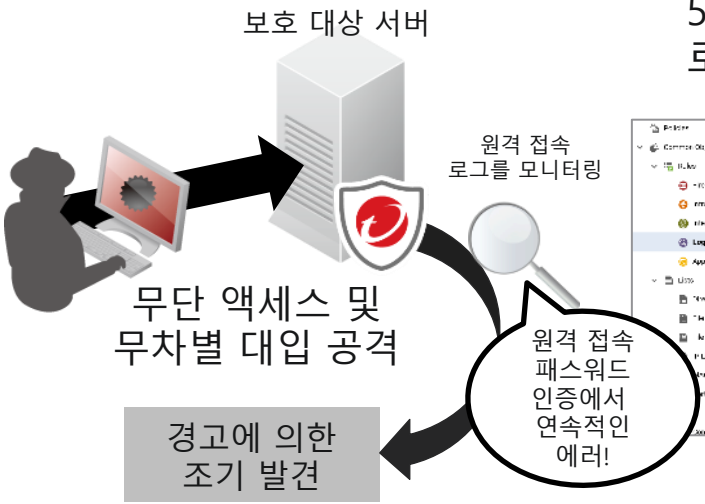
권장 스캔을 이용한 패치 관리



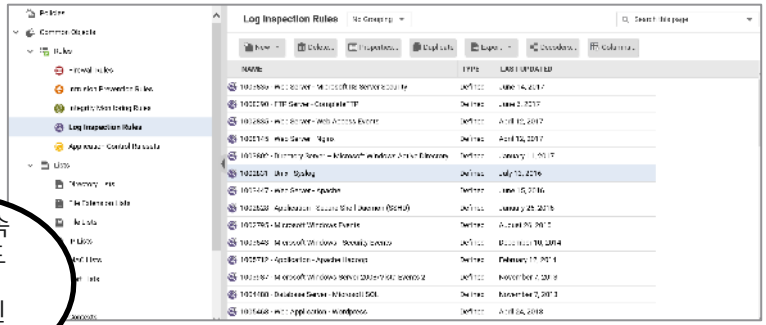
Log Inspection (로그 감사)

안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어

로그 감사



- 주요 OS, DB, Application에 대한 54개의 로그 프로파일을 이용한 로그 감사 설정 기능 제공

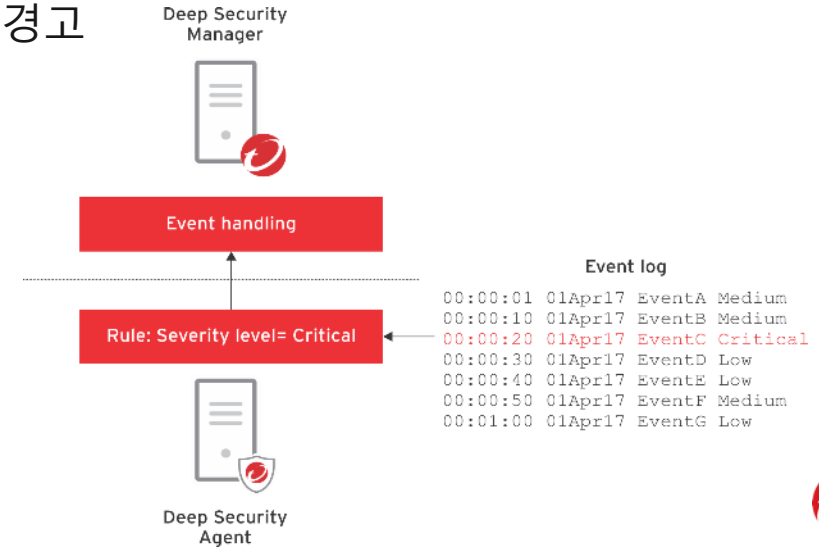


OS 이벤트 로그, Syslog 외에 Web 서버나 DB 등의 로그를 모니터링 할 수 있습니다.

Log Inspection (로그 감사)

안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어

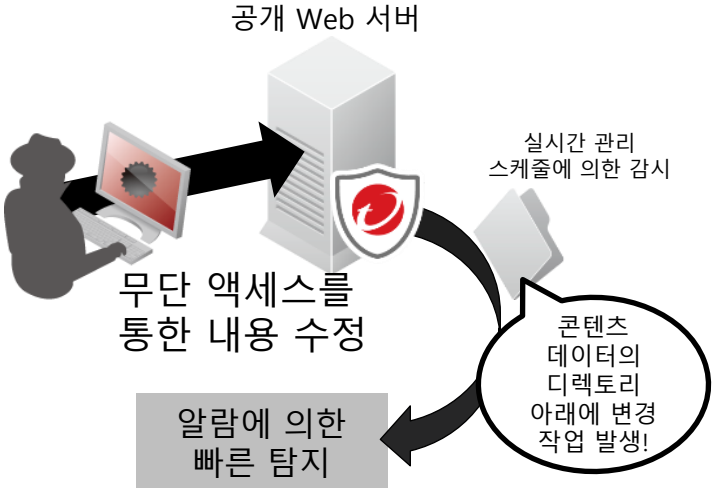
- OS, Application 로그까지 모니터링 하여 서버에 접근한 공격에 대해 모니터링 제공
- 서버나 애플리케이션에서 발생하는 로그를 모니터링 하는 기능으로 위협이 될만한 의심스러운 이벤트/메시지 발생시 경고

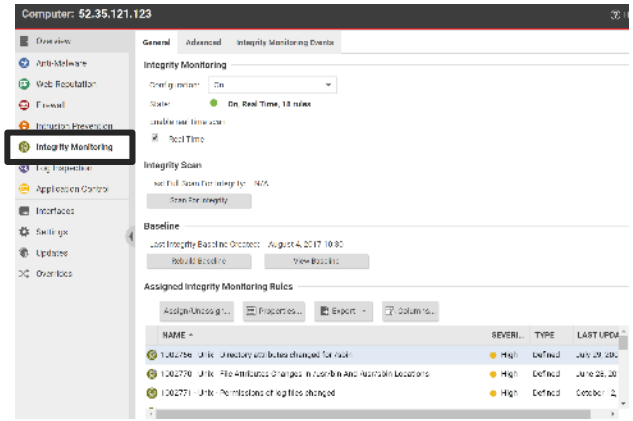


Integrity Monitoring (무결성 모니터링)

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | **무결성 모니터링** | 응용 프로그램 제어

무결성 모니터링

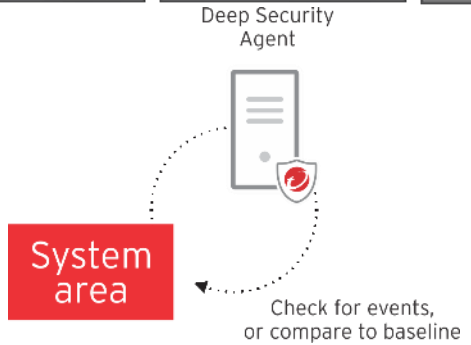




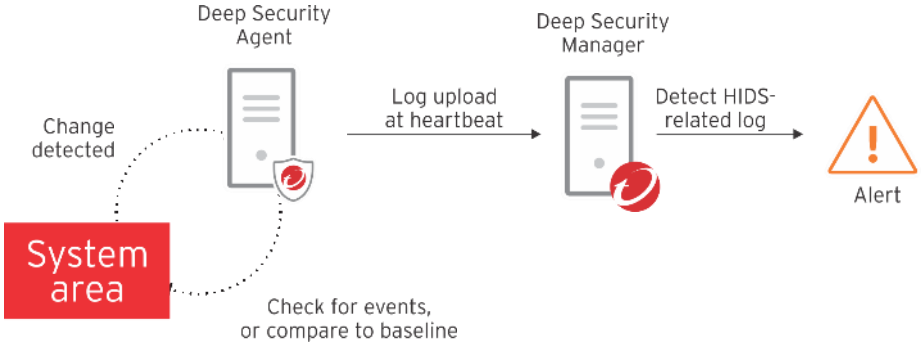
파일 (파일 속성 포함), 디렉토리, 레지스트리,
프로세스 등의 변화를 감지 할 수 있습니다.

Integrity Monitoring (무결성 모니터링)

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | **무결성 모니터링** | 응용 프로그램 제어

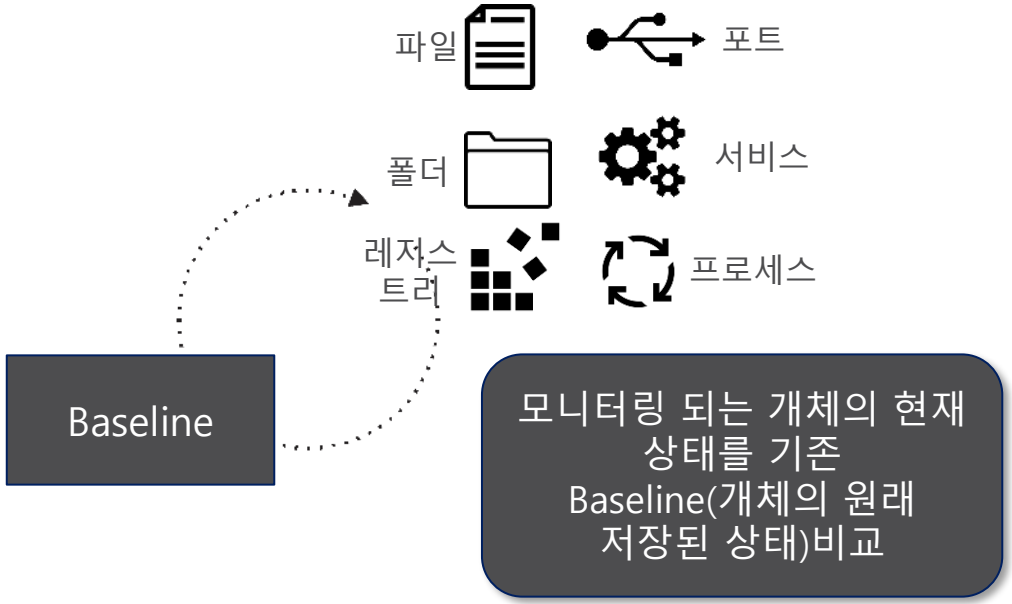


- Windows 레지스트리와 같은 파일 및 중요 시스템 영역에 대한 변경 사항을 탐지
- 이전에 기록한 기준과 비교하여 탐지 수행
- 사전 정의된 무결성 모니터링 규칙 및 새로운 규칙을 DSA 로 적용



Integrity Monitoring (무결성 모니터링)

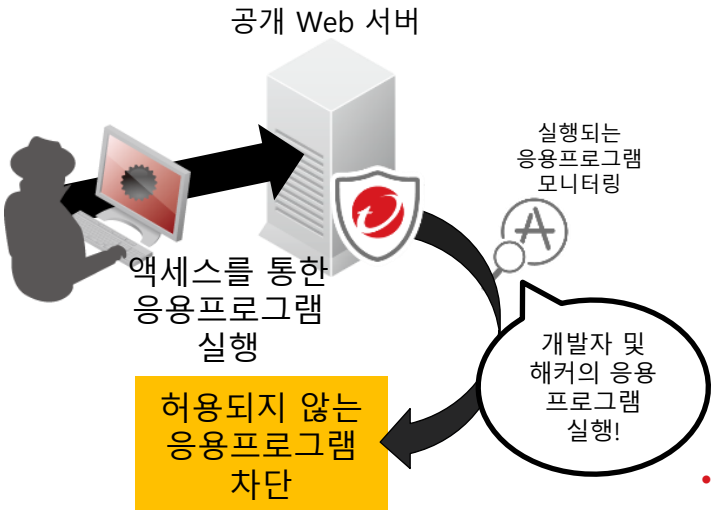
안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어



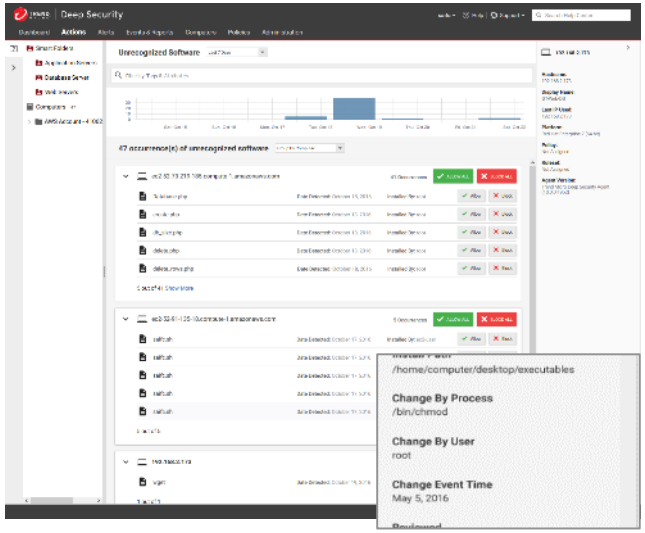
Application Control (응용 프로그램 제어)

안티 멀웨어 (백신) | 방화벽 | 침입 방어 (취약점 방어) | 로그 감사 | 무결성 모니터링 | **응용 프로그램 제어**

응용 프로그램 제어



- 일반 실행 파일의 바이너리와 라이브러리 외에 Java, PHP, Python 등 주요 Web 어플리케이션 프레임 워크에도 대응



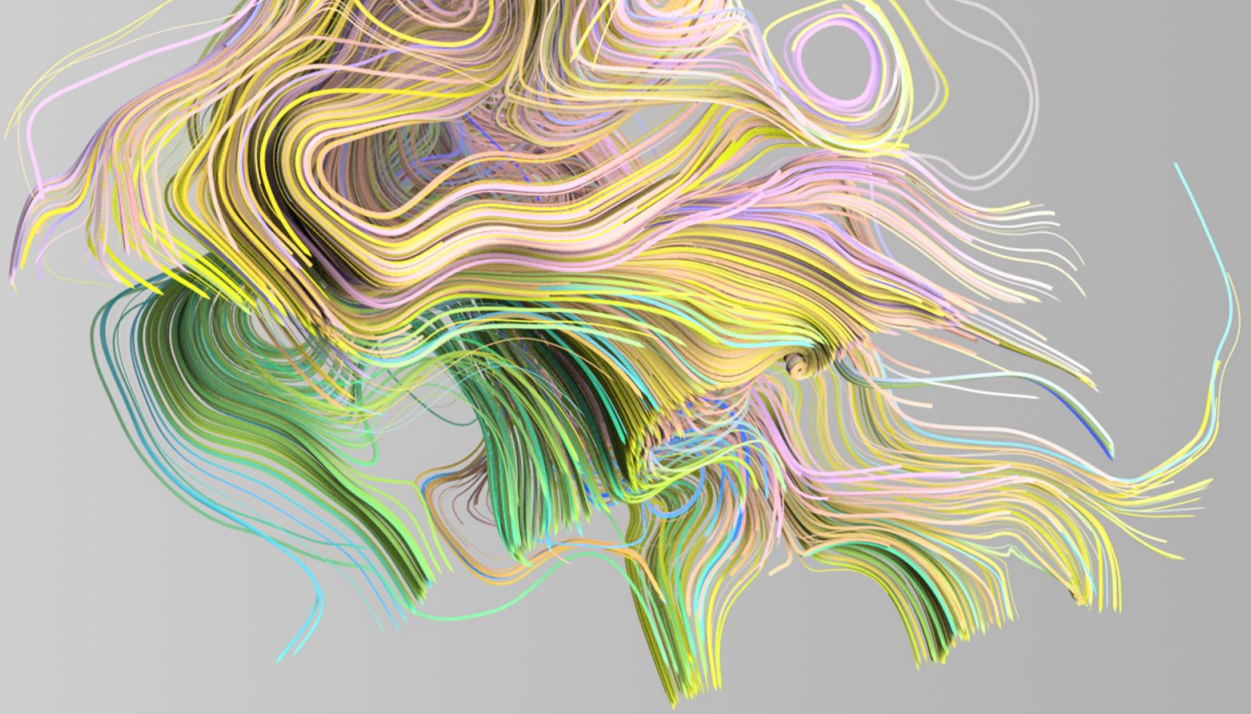
- DSA 호스트에서 실행되는 응용 프로그램을 모니터링
  - 화이트리스트 / 블랙리스트 방식 운영 가능
  - **탐지**(로그) 또는 **블록** 선택 가능

Application Control (응용 프로그램 제어)

안티 멀웨어 (백신)	방화벽	침입 방어 (취약점 방어)	로그 감사	무결성 모니터링	응용 프로그램 제어

- 응용프로그램 제어 동작 방법

- Agent 에서 변경사항을 지속적으로 모니터링
  - 기준 인벤토리 : ac.db 파일
- Workload(Deep) Security Agent는 소프트웨어에 대한 쓰기 작업 검색
- 인벤토리에 있는 원본 파일의 해시를 새 파일 및 변경된 파일의 해시 비교



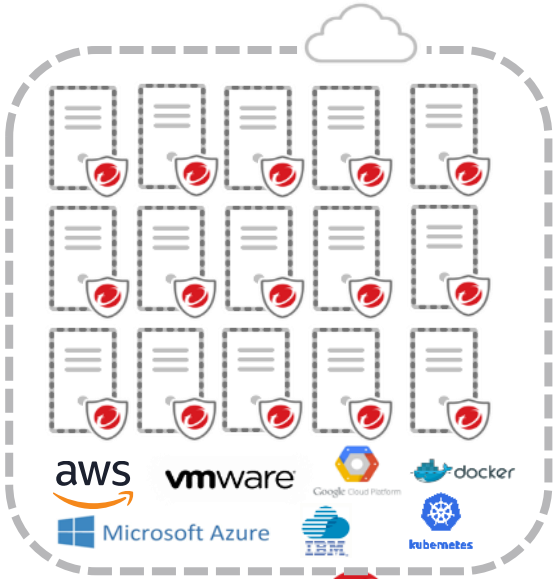
Workload(Deep) Security 구성

Cloud One – Workload(Deep) Security

Workload(Deep) Security Manager

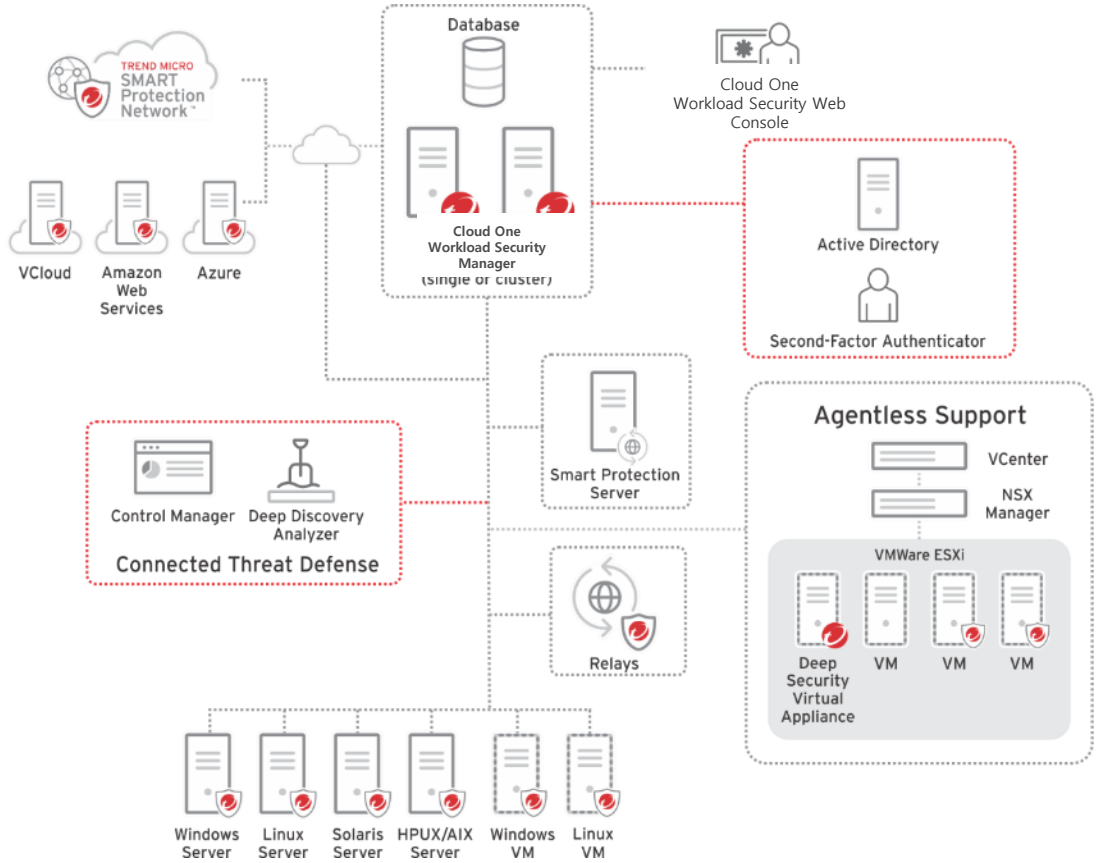
Hybrid Cloud
구성 지원 가능

물리, 가상, 클라우드 및
컨테이너 보호 **단일**
보안 관리 콘솔



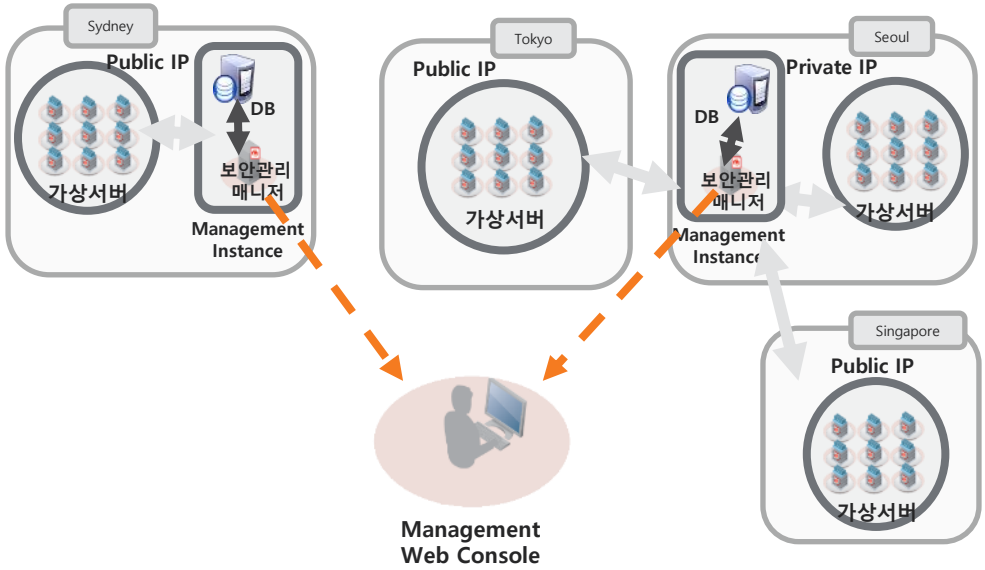
TREND MICRO

Workload(Deep) Security 컴포넌트 구성



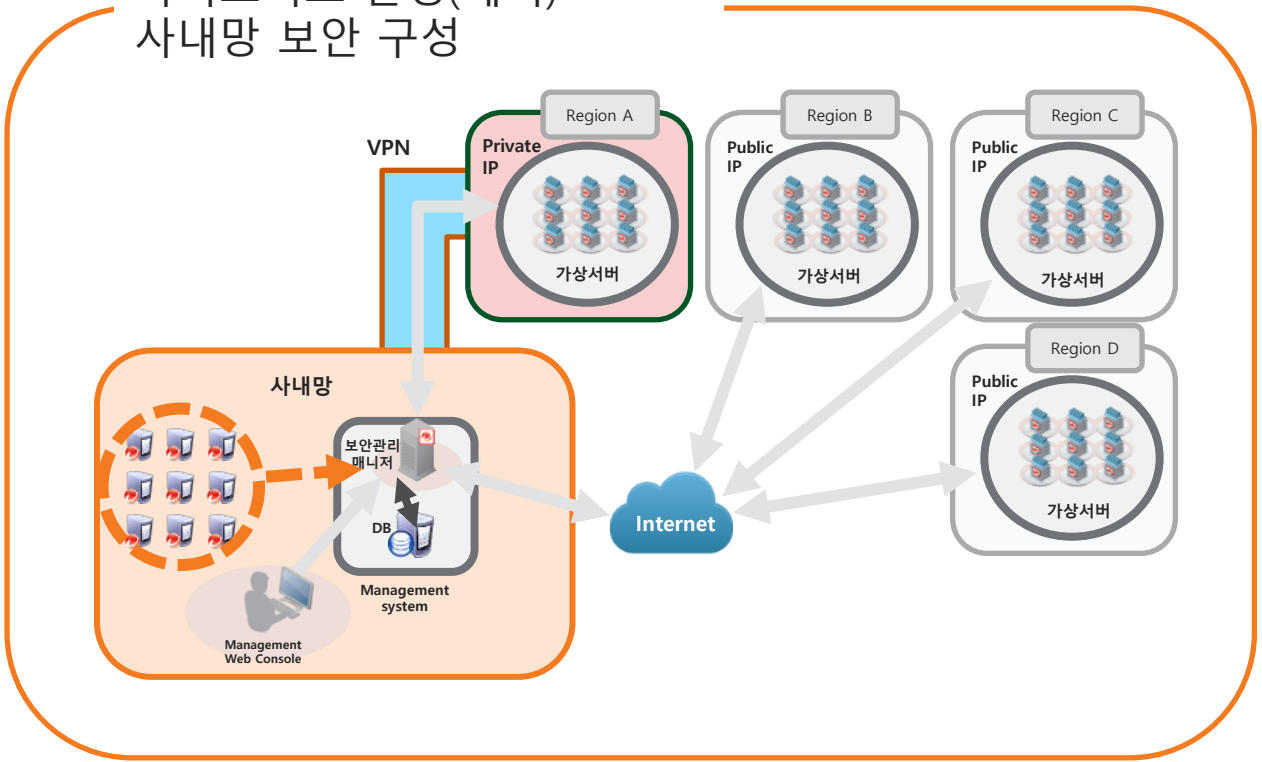
클라우드 환경 Workload(Deep) Security 구성

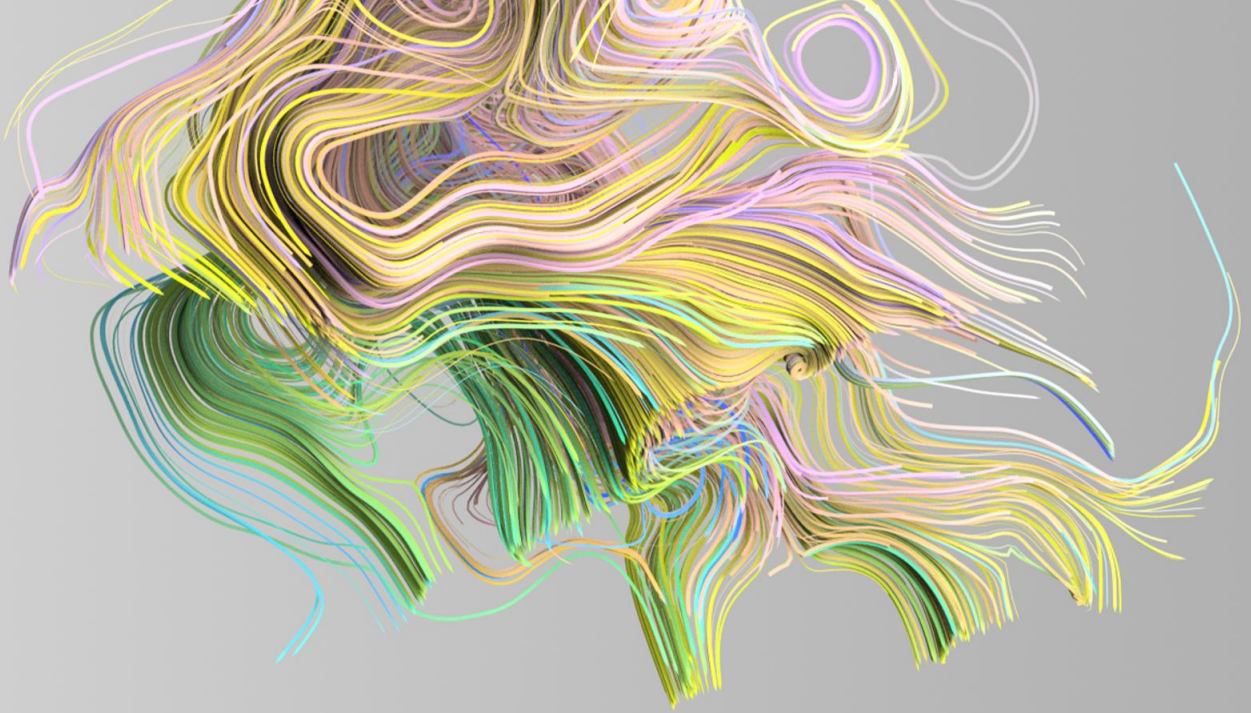
클라우드 환경(예시)
지역 별 연결 보안 구성



멀티, 하이브리드 클라우드 환경 구성

하이브리드 환경(예시)
사내망 보안 구성





Workload Security (Deep Security) 도입 사례

국내 고객 사례 (Workload Security, Deep Security 도입)

- 국내 500+ 이상의 고객사에 Cloud 및 Data 센터 서버 보안 제품 판매

금융

기업

국내 고객 사례 (Workload Security, Deep Security 도입)

- 중앙부처와 주요 기관 및 지자체에서 운영중

중앙부처

- 책임운영기관 행정안전부 국가정보자원관리원
- 대한민국 국방부 Ministry of National Defense
- 외교부
- 기획재정부
- 문화체육관광부
- 중소벤처기업부
- 해양수산부
- 보건복지부
- 교육부
- 환경부
- 과학기술정보통신부
- 행정안전부
- 고용노동부
- 산업통상자원부
- 국토교통부
- 국민권익위원회 Anti-Corruption & Civil Rights Commission
- 방송통신위원회 Korea Communications Commission
- 국가보훈처
- 인사혁신처
- 공정거래위원회
- 법제처
- 원자력안전위원회
- 금융위원회
- 통계청
- 국무조정실 국무총리비서실

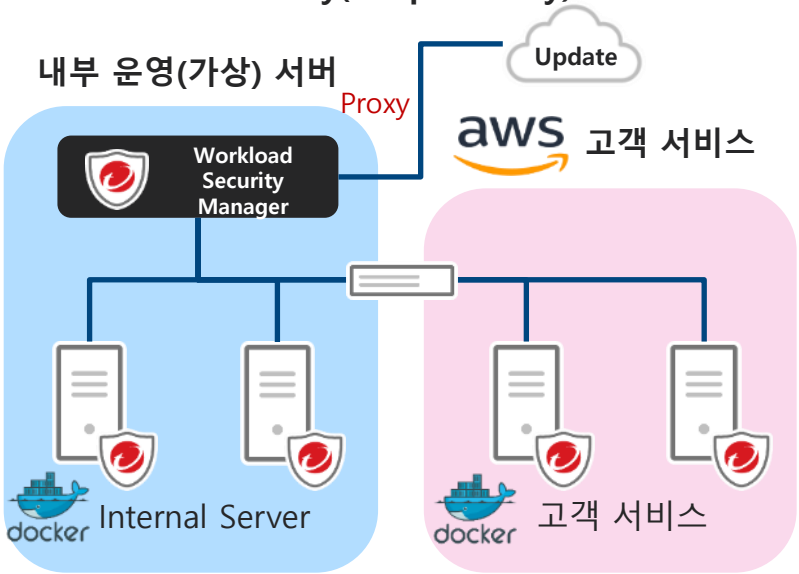
공공기관

- 소방청 National Fire Agency
- 우정사업본부 KOREA POST
- 감사원
- 민주평화통일자문회의 The Peaceful Unification Advisory Council
- KIC 한국투자공사 Korea Investment Corporation
- KERIS 한국교육학술정보원
- KOTI 한국교통연구원 THE KOREA TRANSPORT INSTITUTE
- 국가인권위원회
- 서울특별시
- ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute
- 국립암센터 NATIONAL CANCER CENTER
- BEPA 부산경제진흥원 Busan Economic Promotion Agency
- KID 보험개발원 Korea Insurance Development Institute
- KISA 한국인터넷진흥원
- nipa 정보통신산업진흥원 National IT Industry Promotion Agency
- 한국소비자원 Korea Consumer Agency
- 부산국제영화제
- 양산시
- 안양시

도입 사례 - A사

내용	Workload Security(Deep Security) 를 구축하여 내부 업무 서버 및 AWS 서비스 환경의 보안 적용
적용 범위	내부 가상 서버 및 AWS에 적용

Workload Security(Deep Security)적용 구성도

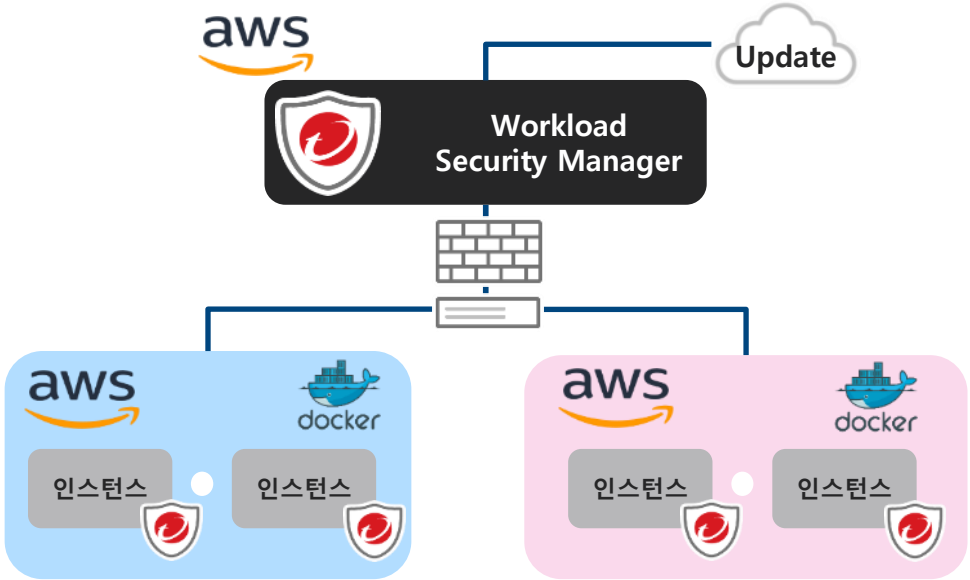


적용 내용	XXX 에서는 내부 가상환경 및 AWS에서 보안을 적용하기 위해 Workload Security(Deep Security) 도입하여 효율적으로 보안 강화
사용 기능	모든 보안 모듈 적용 (AM, FW, IDS/IPS, LI, IM)
구성 설명	내부 업무용으로 사용하는 가상환경 및 고객 서비스(AWS) 를 DS를 통해 회사 보안 정책에 맞게 적용하여 안전하게 보호 DSA를 통하여 탐지된 이벤트 들은 SIEM 장비로 Syslog를 발송하여 통합 모니터링을 통하여 분석 후 처리

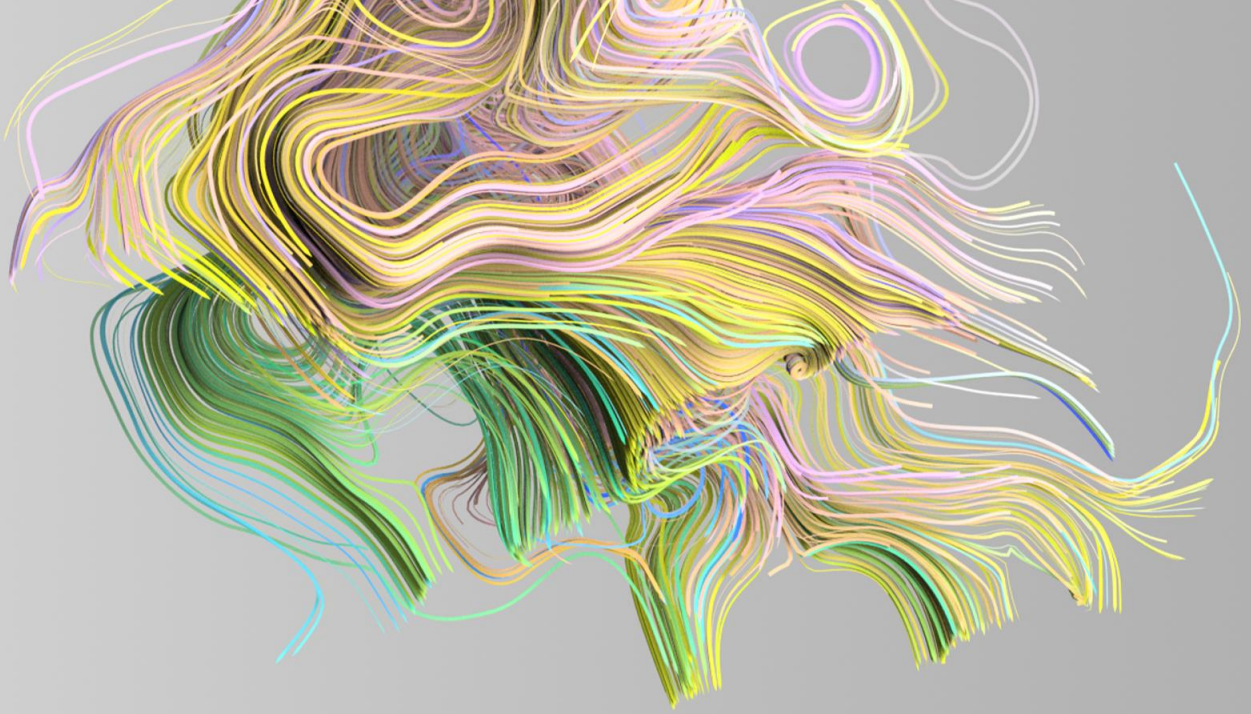
도입 사례 - B사

내용	Workload Security(Deep Security) 를 구축하여 AWS 환경의 업무 서버들의 보안 적용
적용 범위	모든 AWS 서버에 적용

Workload Security(Deep Security) 적용 구성도



적용 내용	AWS에서 보안을 적용하기 위해 Workload Security(Deep Security) 도입하여 효율적으로 보안 강화
사용 기능	IPS/IDS 보안 모듈 적용
구성 설명	외부 서비스(AWS) 를 DS를 통해 회사 보안 정책에 맞게 적용하여 안전하게 보호 DSA를 통하여 탐지된 이벤트 들은 SIEM 장비로 Syslog를 발송하여 SOC 에서 분석 후 처리



Trend Micro Cloud Security Vision

Compliance 대응

PCI

PCI DSS Requirement	Responsibility
Install and maintain a firewall configuration to protect cardholder data	Shared
Do not use vendor-supplied defaults for passwords or other security parameters	Shared
Protect stored cardholder data	Shared
Encrypt transmission of cardholder data	User
[illegible]arly update anti-virus software	User
[illegible]aintain secure systems and applications	Shared
[illegible]s to cardholder data by business need to know	Shared
Assign a unique ID to each person with computer access	Shared
Restrict physical access to cardholder data	Cloud Provider
Track and monitor all access to network resources and cardholder data	Shared
Regularly test security systems and processes	Shared
Maintain a policy that addresses info security for all personnel	Shared

8 of 12 requirements

SANS

SANS/CIS TOP 20 CRITICAL SECURITY CONTROLS	
1. Inventory of Authorized & Unauthorized Devices	11. Secure Configurations for Network Devices
2. Inventory of Authorized & Unauthorized Software	12. Boundary Defense
3. Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	13. Data Protection
4. Continuous Vulnerability Assessment & Remediation	14. Controlled Access Based on the Need t[illegible]
5. Controlled Use of Administrative Privileges	15. Wireless Access Control
6. Maintenance, Monitoring, & Analysis of Audit Logs	16. Account Monitoring & Control
7. Email and Web Browser Protections	17. Security Skills Assessment & Appropriate Training to Fill Gaps
8. Malware Defenses	18. Application Software Security
9. Limitation and Control of Network Ports, Protocols, and Services	19. Incident Response Management
10. Data Recovery Capability	20. Penetration Tests & Red Team Exercises

10 of 20 requirements

OWASP

	OWASP TOP 10	DEEP SECURITY COVERAGE
A1	Injection	IPS; generic protection
A2	Broken Authentication and Session Management	Not covered
A3	Cross-Site Scripting (XSS)	IPS; generic protection
[illegible]	[illegible]irect Object References	Not covered; attack can't be distinguished from normal traffic
[illegible]	[illegible]isconfiguration	IPS; coverage for specific vulnerabilities
[illegible]	[illegible]Data Exposure	IPS; ensure crypto weaknesses are not exploited
[illegible]	[illegible]unction Level Access Control	Not covered; attack can't be distinguished from normal traffic
A8	Cross-site Request Forgery (CSRF)	Not covered; attack can't be distinguished from normal traffic
A9	Using Known Vulnerable Components	IPS; various rules
A10	Unvalidated Redirects and Forwards	IPS on a case-by-case basis based on specific CVE Ex: Microsoft .NET Framework Forms Authentication URI Spoofing (CVE-2011-3415)

6 of 10 requirements

TREND MICRO

최고의 보안 위협 인텔리전스 보유

Cyber Threats | Vulnerabilities & Exploits | Targeted Attacks | AI & ML | IoT | OT / IIoT | Cybercriminal Undergrounds | Future Threat Landscape

클라우드 및 컨테이너 연구팀:

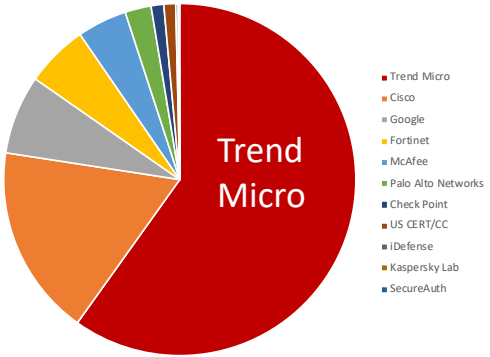
Kubernetes API Server
서비스 거부 취약점 (DoS)

Apache Tomcat 원격 코드 실행 취약점

Kubernetes API Proxy Request
처리 권한 상승 취약점

전 세계 450명의 본사 연구원 10,000명의 지사 연구원

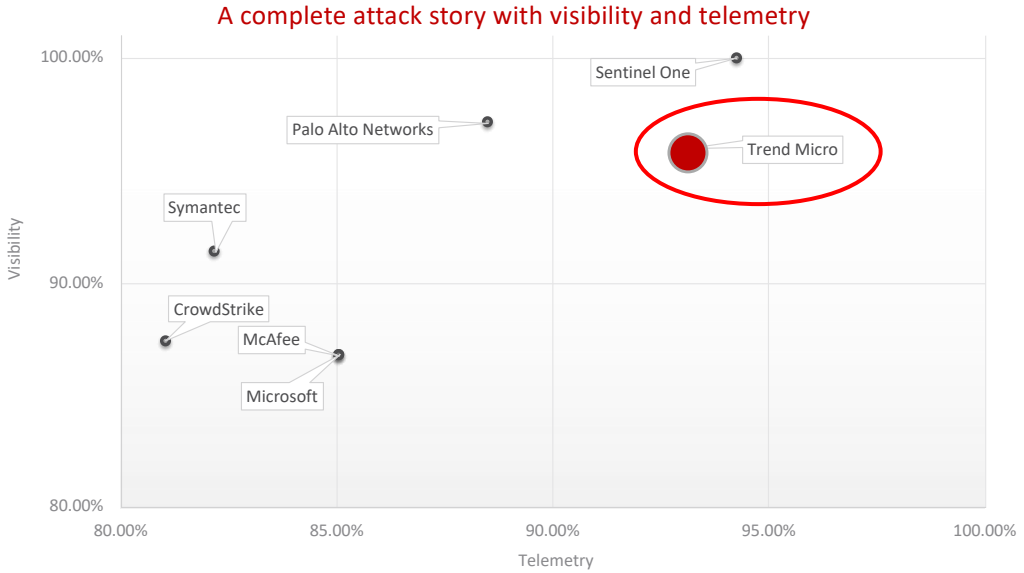
취약성 공개 분야의 마켓 리더



TREND MICRO | research

Carbanak & FIN7

Tradecraft and operational flows in two simulated breaches



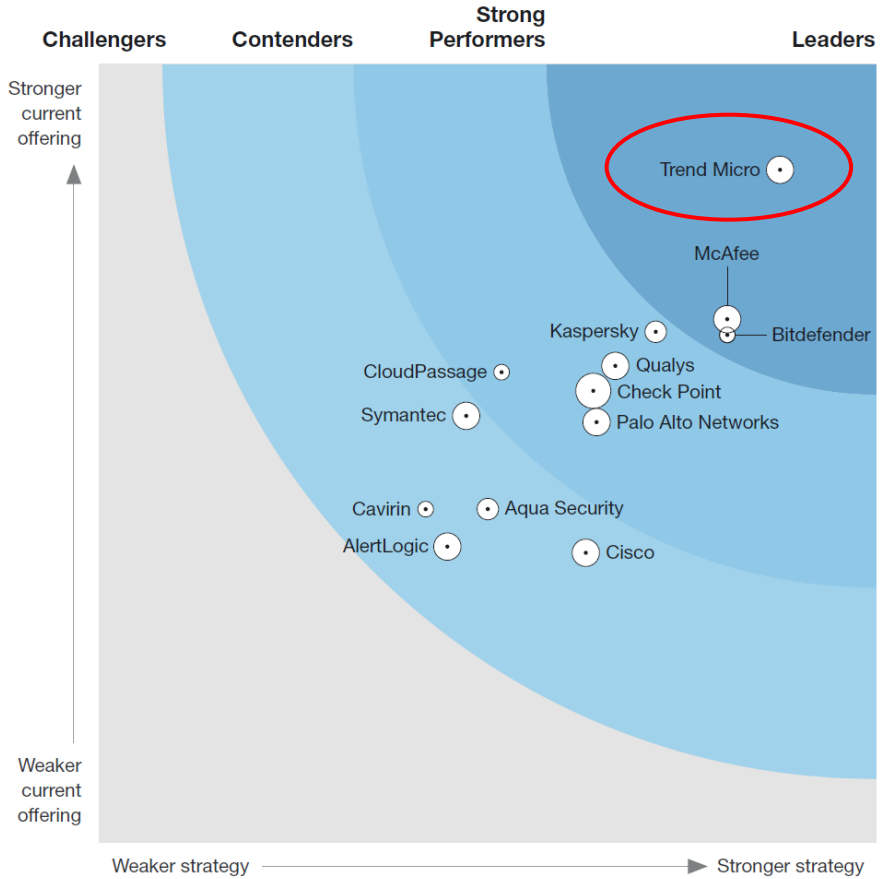
조직은 경고 피로 없이 높은 신뢰도 탐지를 원합니다.

- 가시성 & 텔레메트리 Top 3 순위
- Linux 공격의 100 % 탐지
- 더 나은 조사를 위한 고도로 강화 된 텔레메트리

Data Source: MITRE, 2021

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

FORRESTER®



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

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

Gartner®

2021년 클라우드 워크로드 보호 플랫폼 마켓 가이드

8 of 8

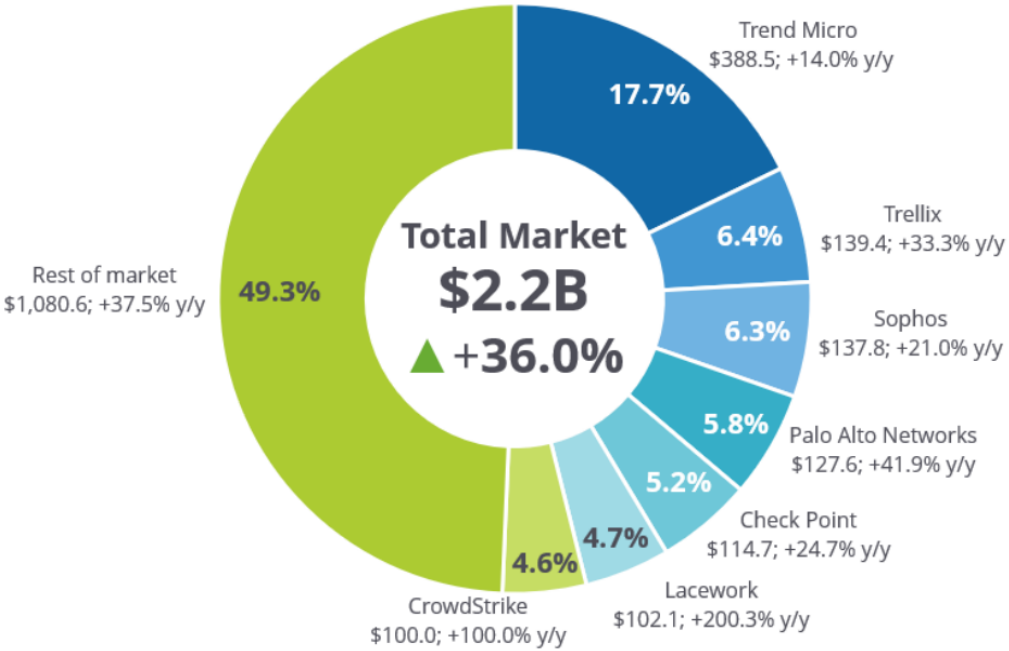
Recommendations*

*Based on Trend Micro's assessment of Gartner 2021 Market Guide for Cloud Workload Protection Platforms/ Neil MacDonald & Tom Croll, July 12, 2021.

TREND MICRO™

CWPP #1 Market Share

Worldwide Cloud Workload Security 2021 Share Snapshot



Note: 2021 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2022

하이브리드 클라우드
워크로드 보안 시장

점유율 1위 17.7%

TREND MICRO™

THE ART OF CYBERSECURITY

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