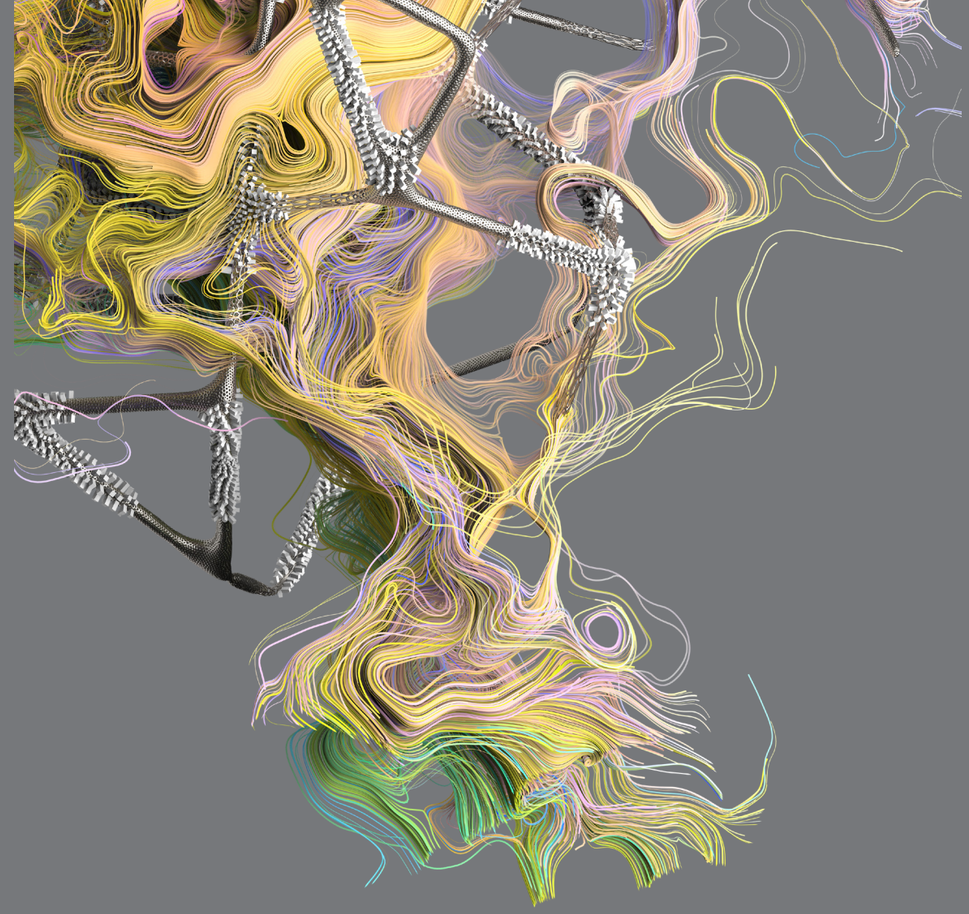
트렌드마이크로

서울시 강남구 영동대로 416 KT&G 타워 3층 (우 06176) TEL. 02-561-0990 FAX. 02-561-0660

http://www.trendmicro.co.kr

TREND MICRO

Securing Your Connected World



TREND MICRO

SOLUTION GUIDE

트렌드마이크로 솔루션 가이드

트렌드마이크로

글로벌 정보보안의 선두주자

트렌드마이크로는 글로벌 클라우드 보안 분야의 선두기업으로 고객사의 데이터센터, 클라우드 환경, 네트워크 및 엔드포인트 환경에 맞는 다양한 솔루션을 제공하는 다국적 정보보안 솔루션 벤더입니다. 전세계 60여개국에 7,000여명의 직원을 통해 50만 고객사와 250만 이상의 엔드포인트를 보호하며 다양한 글로벌 보안 위협 서비스로 제공하고 있습니다. 12년 연속 전세계 서버 보안 시장점유율 1위라는 업계 위상을 통해 클라우드 보안의 선두적인 입지를 다지고 있습니다

HYBRID CLOUD SECURITY SOLUTION

Gartner
클라우드 워크로드 보안
플랫폼을 위한 마켓 가이드
26개 중 23개 항목 충족
2019년

FORRESTER®
클라우드 워크로드 보안
제품 및 전략 범주
최상위 점수 획득
2019년

IDC
하이브리드 클라우드
워크로드 보안 시장
점유율 1위
2019년

NETWORK DEFENSE SOLUTION

ZERO DAY INITIATIVE
업계 최고
제로데이 취약점 방어

NSS LABS
데이터 유출 방지 시스템
5년 연속 “추천” 등급
2018년

NSS LABS
차세대 IPS “추천” 등급
2018년

USER PROTECTION SOLUTION

FORRESTER®
Endpoint Security Suites
리더그룹
2019년

Gartner
Endpoint Protection Platforms
리더그룹
2019년

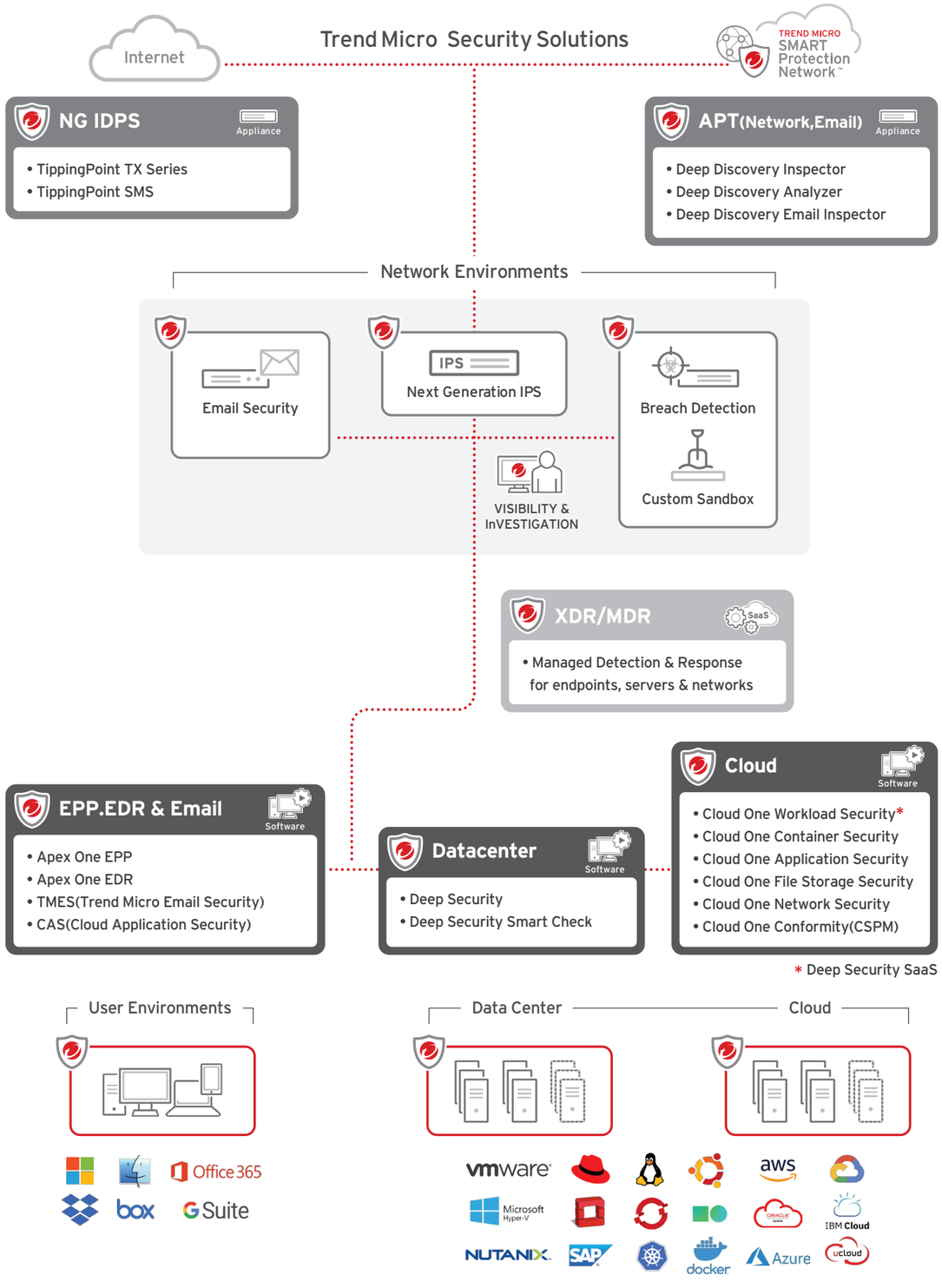
FORRESTER®
Enterprise Email Security
리더그룹
2019년

FORRESTER®
Enterprise Detection and
Response 리더그룹
2019년

트렌드마이크로 리서치

트렌드마이크로 리서치는 보안 분야에서 신뢰할 수 있는 글로벌 리더로서 전세계적으로 50만개 이상의 기업 및 기관을 보호하는 솔루션을 구축하고 있습니다. 2016년 이후 18억건 이상의 랜섬웨어 공격을 차단하고 있으며 5개 대륙에 걸쳐 15개의 위협 리서치 센터를 운영하고 주7일/24시간 보안 위협에 대응합니다. 제로데이 이니셔티브(ZDI) 프로그램을 통한 취약점 발견 및 공개하여 기업 및 소프트웨어 제공 벤더에 제공하고 있습니다.

솔루션 구성도

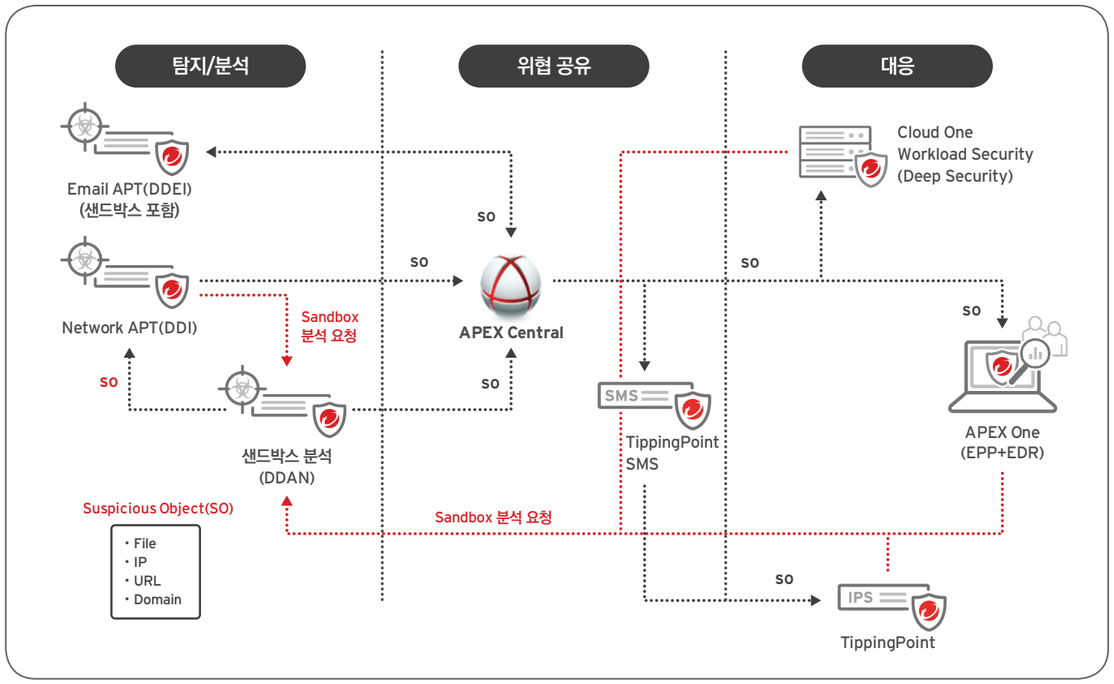


Connected Threat Defense

표적형 사이버 공격 대응을 위한 다계층 연동 보안 솔루션

알려지지 않은 위협에 대해서 트렌드마이크로 솔루션 간의 유기적인 위협 공유 메커니즘를 이용하여 빠르게 대응할 수 있도록 합니다. 트렌드마이크로 본사 R&D팀의 개입없이 기업에 최적화된 위협 대응 패턴을 실시간으로 생성, 공유, 적용하여 차단합니다.

CTD 위협 대응 프로세스



CTD 위협 대응 예

1 탐지
Deep Discovery™ Inspector의 의심스러운 파일 탐지

2 분석
Deep Discovery Analyzer 분석 후 패턴 파일(사용자 정의 시그니처)를 작성하여 Apex Central™에 전달

자동연계

4 차단
Apex One™ 알려지지 않은 위협 차단, 격리

3 위협·공유
Apex Central™에서 모든 클라이언트에 전달

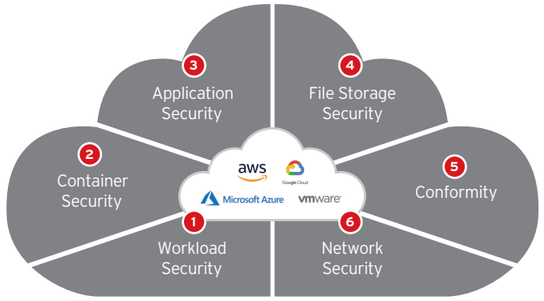
Connected Threat Defense™ 지원제품

제품명	역할			
	탐지	분석	연계	차단
APEX Central™			●	
Apex One™				●
Trend Micro Deep Security™	●			●
Deep Discovery™ Inspector	●	●		
Deep Discovery™ Email Inspector	●	●		●
Deep Discovery™ Analyzer		●		
TippingPoint T/TX 시리즈	●			●
Trend Micro Cloud App Security™	●	●		●

Cloud One

클라우드 환경을 위한 클라우드 인프라보안 서비스 플랫폼

Trend Micro Cloud One™ 은 클라우드 환경에 최적화된 보안 서비스 플랫폼으로 고객의 클라우드 환경을 위한 업계 최고의 보안 기능을 제공합니다. 고객의 안전한 클라우드 마이그레이션을 위해서 6가지 클라우드 네이티브 보안 기능을 제공합니다. 가상화 및 클라우드환경에서 DevOps, 컨테이너, 서버리스 보안에 이르기까지 클라우드 보안을 자동화되고 다양한 환경에 유연한 올인원 솔루션입니다.



1 **Trend Micro Cloud One™ – Workload Security**
클라우드 워크로드(virtual, physical, cloud and containers)를 위한 런타임 보안

2 **Trend Micro Cloud One™ – Container Security**
DevOps 빌드파이프 라인내의 빌드 이미지 스캐닝

3 **Trend Micro Cloud One™ – Application Security**
서버리스, API, 애플리케이션 보안

4 **Trend Micro Cloud One™ – File Storage Security**
클라우드 파일과 오브젝트 스토리지 서비스 보안

5 **Trend Micro Cloud One™ – Conformity**
CSPM(Cloud security and compliance posture management)

6 **Trend Micro Cloud One™ – Network Security**
클라우드 네트워크 보안(IPS)

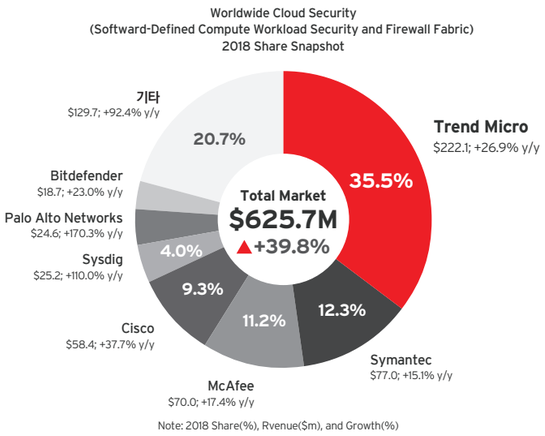
Cloud One™ 특장점

· 자동화된 보안
코드 레벨의 보안을 통해 DevOps 팀은 보안을 빌드 파이프 라인에 구현할 수 있으며, 자동 검색 및 배포, 빠른 시작 템플릿 및 기본 제공 자동화 기능을 이용하여 클라우드 환경을 보호하고 규정 준수 요구 사항을 신속하게 충족합니다.

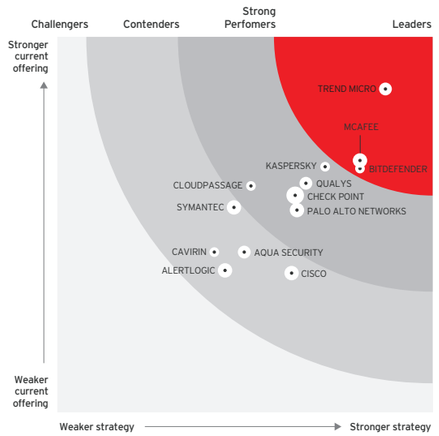
· 멀티 플랫폼
고객이 선택한 광범위한 플랫폼 지원을 통해 하이브리드 클라우드, 다중 클라우드 및 다중 서비스 환경에 대한 보안 뿐만 아니라 고객의 애플리케이션을 보호합니다.

· 올인원 솔루션(All-in-One)
클라우드 보안 요구사항을 충족하고 관리하는데 필요한 모든 도구와 깊이 있는 보안 기능을 제공하는 하나의 플랫폼입니다.

IDC 하이브리드 클라우드 워크로드 보안 시장 점유율 1위(2019년)



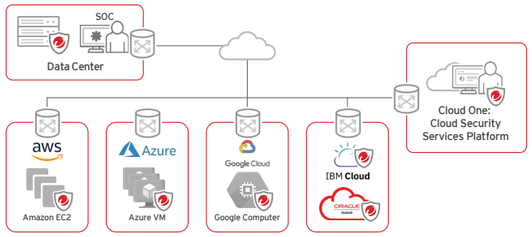
FORRESTER® 클라우드 워크로드 보안 제품 및 전략 범주 최상위 점수 획득(2019년)



Cloud One - Workload Security / Deep Security

클라우드 워크로드(물리, 가상, 클라우드 및 컨테이너)를 위한 런타임 보안

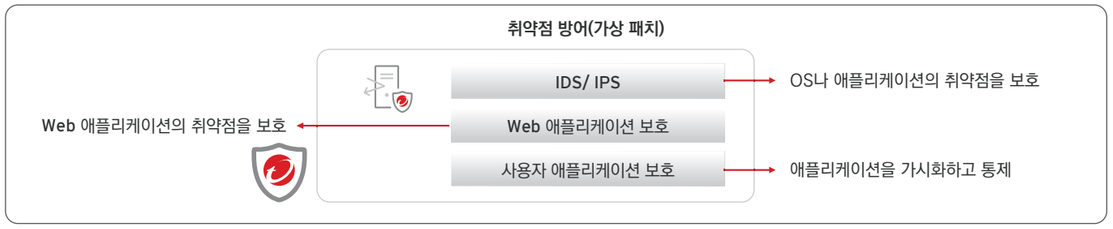
AWS, Azure, GCP, KT Cloud, Naver Cloud, NHN Toastd 및 각종 퍼블릭 클라우드 환경에서 자동으로 워크로드를 검색하여 클라우드의 동적 워크로드를 완벽하게 보호합니다. Cloud One Workload Security로 구동되는 하이브리드 클라우드 보안 솔루션은 물리적, 가상, 클라우드와 컨테이너 환경에서 다양한 워크로드와 기업의 애플리케이션에 대한 효과적인 보호 기능을 제공합니다.



올인원 보안

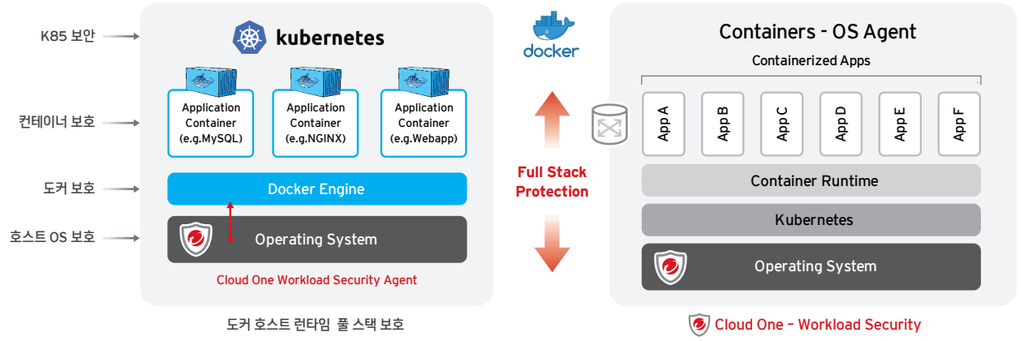
- 글로벌 위협 인텔리전스 기반의 신종/변종 랜섬웨어 방어
- 호스트 서버별 별도의 보안 정책 적용 및 통합보안관리 기능
- 취약점 방어를 위한 가상패치 기능
- 실시간 바이러스 스캔 기능
- 불법 애플리케이션 실행차단 기능
- 내부측면이동 차단 및 C&C 트래픽 차단

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



도커 + 컨테이너 호스트 런타임 풀 스택 보호

Cloud One Workload Security는 컨테이너환경에 대한 런타임 보호 기능을 제공합니다. 도커+컨테이너 호스트, 컨테이너 플랫폼 (Docker®), 오케스트레이터 (Kubernetes®), 컨테이너 자체와 컨테이너화 된 애플리케이션에 대한 공격을 탐지하고 차단합니다. Cloud One Workload Security에 포함된 API를 이용하여 보안팀은 자동화된 프로세스로 컨테이너를 보호하고 제어할 수 있습니다.

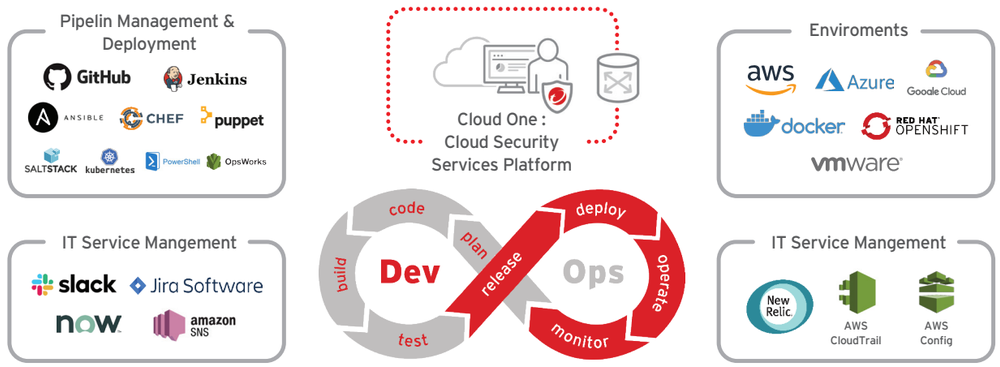


도커 호스트 런타임 풀 스택 보호

Cloud One - Workload Security

DevOps 파이프라인에서 자동화된 워크로드 보안 구현 가능

고객의 멀티, 하이브리드 클라우드 환경에서 워크로드를 구성하기 위해서 사용하고 있는 DevOps 도구, 관리도구, 모니터링 도구와 Cloud One Workload Security을 API 수준으로 통합하여 고객의 애플리케이션을 손쉽게 보호할 수 있습니다.



통합 서버 보안/리눅스 보안 - Deep Security

Deep Security는 번거롭고 복잡한 리눅스 서버 보안 작업을 엔드포인트 기반으로 자동화시켜 운영상의 편리함을 추가한 솔루션으로, 2004년부터 각종 리눅스 배포판과 커널을 지원하고 있습니다. 또한 물리 서버는 물론 가상화 서버, AWS 등 클라우드 서버까지 지원함으로써 국내 글로벌 IT 기업들이 보유한 수만 대의 리눅스 서버 보안에 적용되고 있습니다.

지원 OS | 리눅스

redhat · CentOS · Linux Amazon Cloud · SUSE · ubuntu · CloudLinux · ORACLE LINUX

특장점

- 클라우드 플랫폼 API 통합 (AWS, Azure외)
- Docker + Container 환경에 대한 보안 가능
- 엔터프라이즈의 AWS 보안 표준, 국내 최다 사용 서버 통합 보안 제품
- 클라우드 환경에 적합한 호스트기반 보안 제공
- 하이브리드 클라우드 보안 통합 (클라우드, 가상화, 물리환경) 관리
- VMware vCloud 및 NSX 보안을 통한 자동화
- 보안 솔루션 통합 (AV, IPS/IDS, F/W, LI, IM, AC)
- 가장 많은 플랫폼 지원 (Linux, Windows, Unix)
- 각종 보안 컴플리언스 만족 (PCI-DDS, HIPPA, HITECH)
- 국제CC 최고등급, EAL2+ (구 EAL4+)

지원 플랫폼

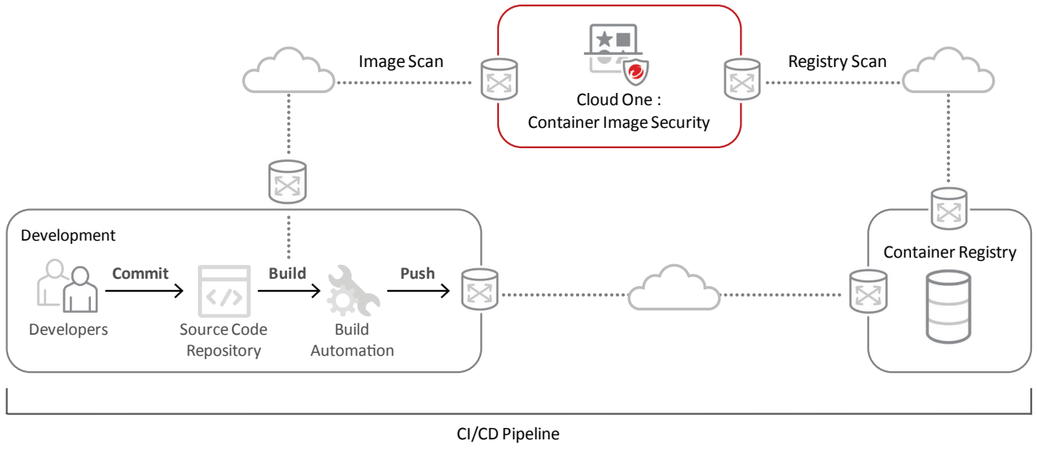
vmware · Microsoft Hyper-V · NUTANIX · CISCO PARTNER Technology Developer · VCE · CITRIX ready · KVM · EMC VSPEX LABS VALIDATED · openstack · docker

aws · IBM · kt ucloud · NHN TOAST · Microsoft Azure · NAVER CLOUD PLATFORM · vmware · Google Cloud · ORACLE CLOUD · RED HAT OPENSHIFT Container Platform

Cloud One – Container Security

CI/CD 파이프라인을 위한 자동화된 컨테이너 이미지, 레지스트리 스캔

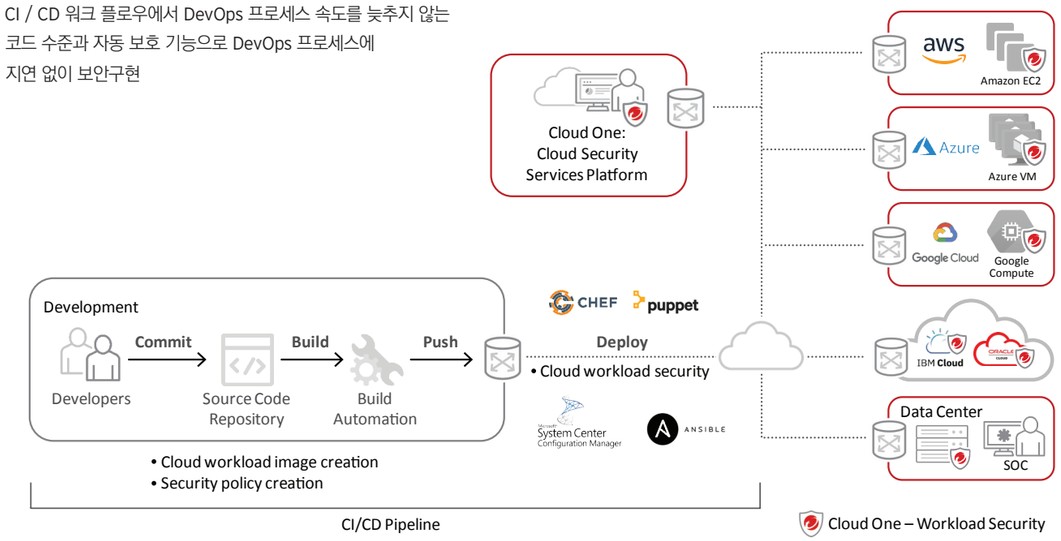
멀웨어, 취약점과 컴플라이언스 위배를 탐지하며 빌드 파이프 라인과 레지스트리의 자동화된 이미지 검색 기능을 제공합니다. Container Security를 통해 DevOps 팀은 기업의 애플리케이션 배포를 지속적으로 제공하고 빌드 주기에 영향을 주지 않고 배포 전 컨테이너의 안정성을 보장할 수 있도록 도와줍니다.



Cloud One Container Security 구성

특장점

- 배포전에 컨테이너 이미지에 대한 익스플로잇 보호
- 컨테이너 이미지 빌드 파이프라인과 레지스트리 검색을 통하여 멀웨어, 취약점과 내부정보 유출로 부터 보호
- 응용 프로그램 배포 전 위협 탐지
- CI / CD 워크 플로우에서 DevOps 프로세스 속도를 늦추지 않는 코드 수준과 자동 보호 기능으로 DevOps 프로세스에 지연 없이 보안구현
- CloudOne – Workload Security와 통합되어 런타임 컨테이너 보호 기능 제공하여 컨테이너 이미지 보안을 위한 Full Time Cycle Container Protection 제공

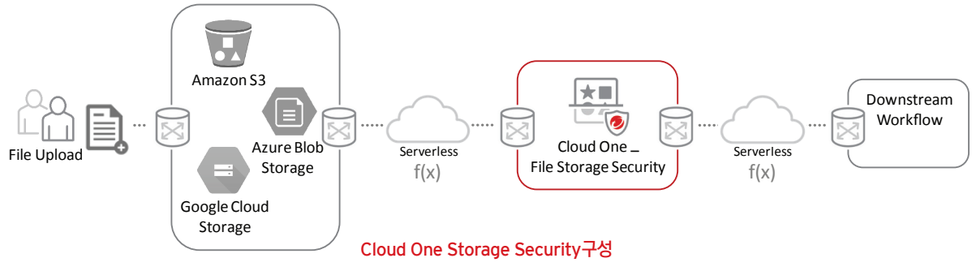


Cloud One Container Security와 Cloud One Workload Security 연동을 통한 클라우드 워크로드 보안

Cloud One – File Storage Security

클라우드 파일 & 오브젝트 스토리지 서비스 보안

다양한 클라우드 스토리지 플랫폼(Amazon S3, Azure Blob, Google Cloud Storage)을 지원하며 클라우드 스토리지 서비스에 대한 멀웨어를 실시간으로 탐지하여 대응할 수 있도록 지원합니다.



Cloud One Storage Security구성

특장점

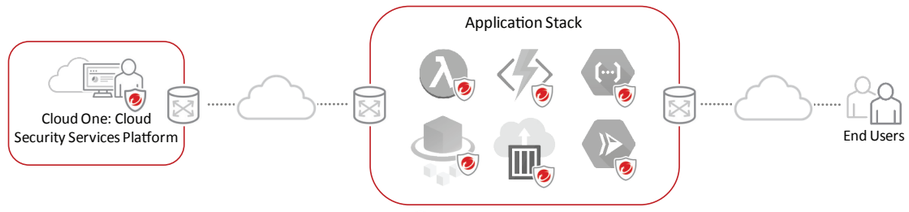
멀웨어 검사로 클라우드 파일에 대한 위협 벡터 감소

- 평판기반 악성파일 탐지 : 멀웨어 패턴기반의 알려진 악성 파일 차단
- 변종 악성코드 방어 : 이전 악성코드 정보와 알고리즘 분석 정보를 이용한 난독화된 변종 악성 코드로부터 보호
- 머신 러닝 : 머신 러닝 알고리즘을 사용하여 알려지지 않은 신종 악성코드 및 제로 데이 위협 분석

Cloud One – Application Security

컨테이너, 서버리스 및 다양한 클라우드 플랫폼에 구축된 애플리케이션과 API에 대한 위협 탐지와 보호

클라우드 환경의 새로운 서비스(Serverless)를 사용하는 애플리케이션을 위협으로부터 보호합니다. 사용자 애플리케이션에 통합해야하는 SDK와 달리 Application Security는 런타임에 애플리케이션 자체로 부트스트랩 됩니다. Cloud One Application Security는 최신 클라우드 애플리케이션 아키텍처에 최적화되어 기업의 애플리케이션을 원치 않는 행위로부터 실시간으로 즉시 차단하여 데이터와 기업의 비즈니스 로직을 보호합니다.



특장점

- SQLi를 포함하여 OWASP 10 런타임 위협 탐지와 보호
- RCE (원격 명령 실행) 위협 탐지
- Injection과 기타 자동 공격 차단
- 모든 공격 인스턴스에 대한 완벽한 모니터링과 차단 제공
- 코드 취약성에 대한 진단 정보 제공
- 공격자의 신원 및 공격 방법에 대한 정보 제공
- 1분 안에 구현 가능 – 애플리케이션 소스 코드 변경 필요 없음

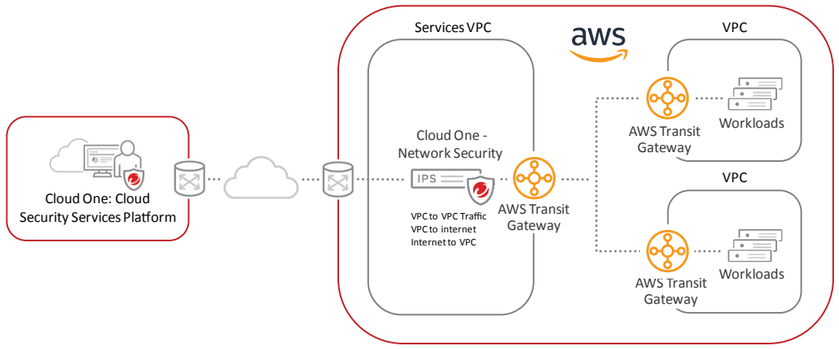
위협 대응

위협	탐지	보호
Open Redirect	✔	✔
Remote Command Execution (RCE)	✔	✔
Illegal File Access	✔	✔
SQL Injection	✔	✔
Antivirus/Anti-Malware Scanning of File Uploads	✔	✔
Malicious Payload	✔	✔

Cloud One – Network Security

클라우드용 Tipping Point

클라우드 네트워크 보안 구현을 단순하고 쉽게 구성할 수 있도록 지원하며 송수신 트래픽 검사를 기반으로 VPC(가상 사설 클라우드)와 클라우드 네트워크에 대해 자동화된 보안기능으로 클라우드 네트워크를 보호 할 수 있습니다. Cloud One Network Security는 AWS Transit Gateway의 효율성과 확장성을 이용하여 신속하고 간단한 배포를 제공하며 고객의 VPC와 온프레미스 네트워크를 연결할 때 효율성을 극대화 합니다.



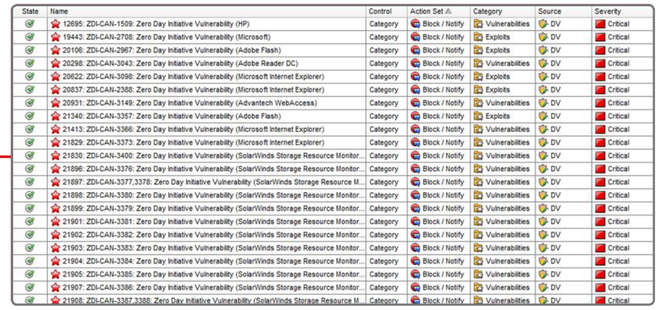
Cloud One Network Security 구성

Zero Day Initiative

Vulnerability-generic(보안취약점 방어) 기반의 필터(룰) 적용

ZERO DAY INITIATIVE

보안 패치가 존재하지 않는
보안 취약점에 대한 공격 가시성 및 사전 방어.
Trend Micro에서는 해당 시그니처에
"ZDI-CAN" 으로 구분해서 제공



State	Name	Control	Action Set	Category	Source	Severity
	12695: ZDI-CAN-1509: Zero Day Initiative Vulnerability (HP)	Category	Block / Notify	Vulnerabilities	DV	Critical
	19443: ZDI-CAN-2708: Zero Day Initiative Vulnerability (Microsoft)	Category	Block / Notify	Exploits	DV	Critical
	20106: ZDI-CAN-2967: Zero Day Initiative Vulnerability (Adobe Flash)	Category	Block / Notify	Exploits	DV	Critical
	20298: ZDI-CAN-3043: Zero Day Initiative Vulnerability (Adobe Reader DC)	Category	Block / Notify	Vulnerabilities	DV	Critical
	20622: ZDI-CAN-3098: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Exploits	DV	Critical
	20837: ZDI-CAN-2388: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Exploits	DV	Critical
	20931: ZDI-CAN-3148: Zero Day Initiative Vulnerability (Advantech WebAccess)	Category	Block / Notify	Vulnerabilities	DV	Critical
	21340: ZDI-CAN-3357: Zero Day Initiative Vulnerability (Adobe Flash)	Category	Block / Notify	Exploits	DV	Critical
	21413: ZDI-CAN-3366: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Vulnerabilities	DV	Critical
	21829: ZDI-CAN-3373: Zero Day Initiative Vulnerability (Microsoft Internet Explorer)	Category	Block / Notify	Vulnerabilities	DV	Critical
	21830: ZDI-CAN-3400: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21896: ZDI-CAN-3376: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21897: ZDI-CAN-3377,3378: Zero Day Initiative Vulnerability (SolarWinds Storage Resource M...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21898: ZDI-CAN-3380: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21899: ZDI-CAN-3379: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21901: ZDI-CAN-3381: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21902: ZDI-CAN-3382: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21903: ZDI-CAN-3383: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21904: ZDI-CAN-3384: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21905: ZDI-CAN-3385: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21907: ZDI-CAN-3386: Zero Day Initiative Vulnerability (SolarWinds Storage Resource Monitor...	Category	Block / Notify	Vulnerabilities	DV	Critical
	21908: ZDI-CAN-3387,3388: Zero Day Initiative Vulnerability (SolarWinds Storage Resource M...	Category	Block / Notify	Vulnerabilities	DV	Critical

ZDI 기반의 사전에 알지 못하는(Unknown) 보안 취약점 필터(룰)

특장점

Transparent

- Flow 기반 엔진
- 경계 없는 Deep Packet Inspection
- 서비스 중단 없이 인라인 구성 적용 및 해제

Fewer Moving Pieces

- 네트워크 환경에 맞게 효과적으로 In/Out 트래픽 검사
- 단일 EC2 VPC / Instance로 Load Balancer 불필요

Flexible

- AWS Transit-Gateway를 통해 인라인 형태로 초기 구성
- 유연한 라이선스 체계 지원

Cloud One – Conformity

Cloud Security Posture Management

다양한 클라우드 인프라에 대한 규정 준수 프레임 워크를 사용하여 클라우드 계정 내의 리소스 설정을 자동으로 검사하여 잘못된 설정으로 발생할 수 있는 위협으로 부터 기업의 클라우드 환경을 안전하게 보호할 수 있도록 지원합니다.

주요 기능

aws partner network
Advanced Technology Partner
Security Competency
Cloud Management Tools Competency

aws partner network
WINNER
Technology Partner of the Year 2019

특장점

자동화된 보안 & 컴플라이언스 검사

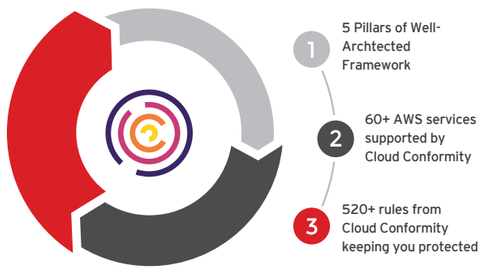
- 컴플라이언스 표준 (PCI, GDPR, HIPAA, NIST 등)과 클라우드 보안 모범 사례 규칙을 이용한 클라우드 인프라에 대한 보안 사항과 컴플라이언스 준수 상태 검사

클라우드 환경에 대한 Knowledge Base 기반 탐지

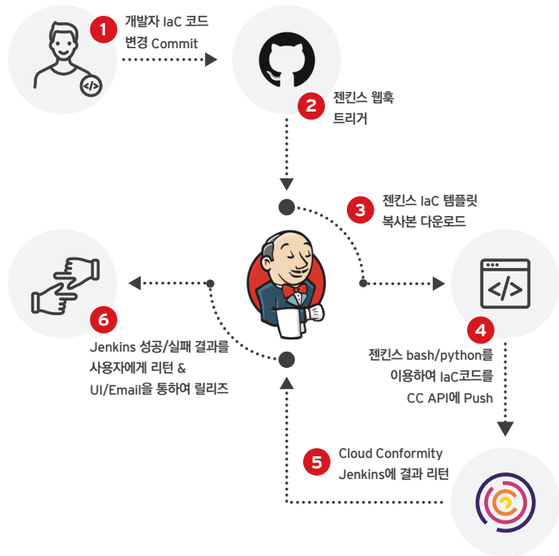
- 600가지 이상의 Knowledge base를 기반으로 클라우드 인프라에 대한 설정 검사

단순한 모니터링 프로세스

- 전체 멀티 클라우드 인프라에 대한 명확한 가시성 제공과 다양한 필터 조합으로 상세 점검 보고서 제공



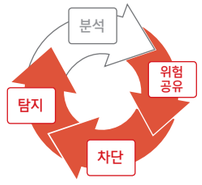
AWS Well-Architected Framework 지원



AWS CloudFormation Template Scanner

TippingPoint TX

NGIDPS(Next Generation Intrusion Detection & Prevention System)
단일 장비 최대 40Gbps성능을 제공하는 글로벌 NGIDPS 최상위 솔루션

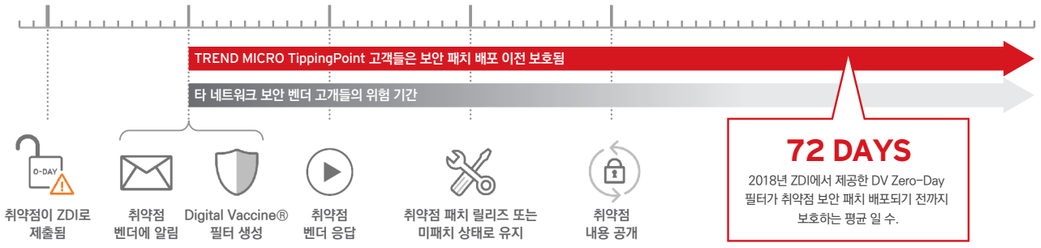


Zero Day Initiative

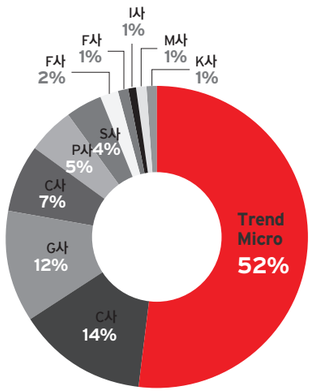
글로벌 최고의 취약점 발견 보고 연구기관 ZDI(Zero Day Initiative) 의 제로데이취약점을 이용하여 트렌드마이크로 고객들을 제로 데이 취약점으로부터 가장 먼저 보호할 수 있습니다.

- Vulnerability-generic(보안취약점 방어) 기반의 시그니처(룰) 제공
- 선제적인 대응이 가능하도록 알려지지 않은/알려진 보안취약점 방어 기반의 필터 룰을 신속하게 제공

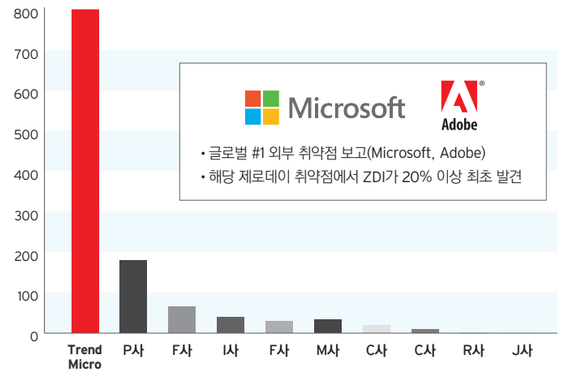
ZERO DAY INITIATIVE
LEADER in Global Vulnerability Research and Discovery SINCE 2007
FROST & SULLIVAN



글로벌 취약점 리서치



2018년 HIS Markit의
공공 사이버보안 취약점 마켓 보고서



(2006년 ~ 현재)
마이크로소프트 취약점 발견수에 대한 보안 인텔리전스

2019 NSS Labs NG IPS Test

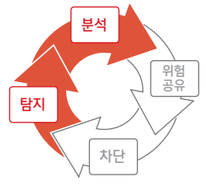
NSS LABS RECOMMENDED

Vendor	Security Effectiveness		Value(TCO per Protected Mbps)		Overall Rating
Trend Micro TippingPoint 8200TX Appliance v5.1.0.49751 + Deep Discovery Analyzer v6.1.0.114 + OfficeScan v12.0.5024	96.2%	Avobe Average	$40	Avobe Average	Recommended
Trend Micro TippingPoint 8400TX Appliance v5.1.0.4965 & Tren Micro Smart Protection fo Endpoints v12.0.5024	92.1%	Avobe Average	$28	Avobe Average	Recommended

<NSS Lab's 2019 Recommendations: An Analysis of Breach Prevention Systems>

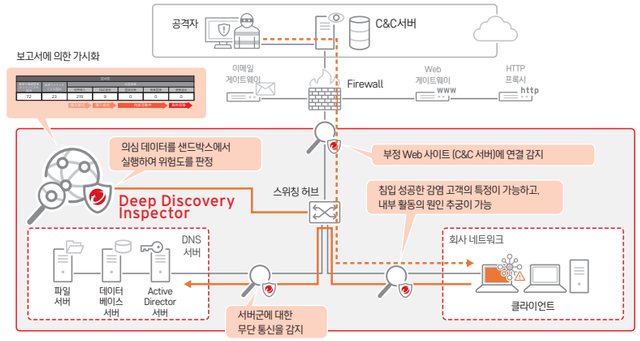
Deep Discovery Inspector

Network APT 탐지



표적형 공격과 제로 데이 공격을 네트워크의 행동에서 찾아 조기에 대처하고 심각한 피해를 사전에 방어하기 위한 제품입니다.
불법적인 파일 및 통신을 탐지하는 것 외에도 공격 초기 단계부터 내부 확산 및 외부와의 통신까지 다양한 공격 단계에서 관리 도구를 악용하는 공격을 발견합니다.

시스템 구성도



내부트래픽 검사

PsExec.exe의 실행 등 일반 관리자가 사용하는 한 문제가 없는 명령도 공격에 악용될 수 있습니다.
Deep Discovery Inspector는 관리자 권한을 탈취한 후, 수행되는 작업 등을 다각적으로 분석하여 이상을 감지합니다.

인터넷 트래픽 검사

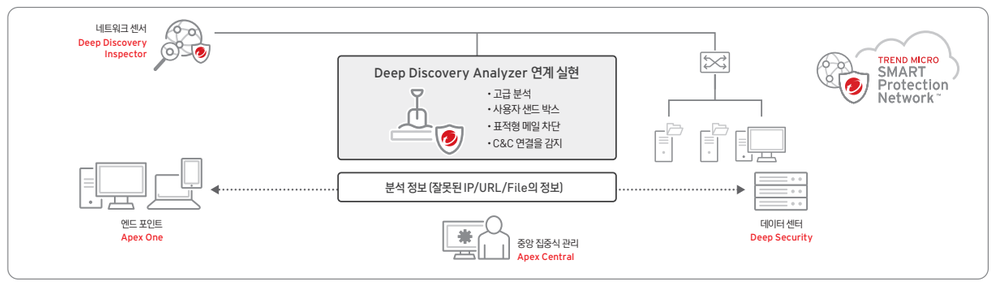
업계 최다 100개이상의 트래픽에 포함된 위협을 탐지합니다.

Deep Discovery Analyzer

Network ATP 분석

Deep Discovery Analyzer는 Trend Micro의 웹, 이메일, 엔드포인트 및 서버 보호 제품과 함께 샌드박스 분석 기능을 추가할 수 있습니다. 표적형 공격, 제로 데이 공격 및 신,변종 랜섬웨어 공격에 대한 대응책으로 운영 환경의 큰 변경 없이도 Trend Micro 제품을 통해 보안을 강화할 수 있습니다. Deep Discovery Analyzer는 분석 기능 외에도 다른 Trend Micro 제품에 사용할 수 있는 시그니처를 자동으로 생성하고 공유합니다. 또한 수동 분석 기능이 있어 고객이 직접 수집한 위협의심 정보를 분석하는데 사용이 가능합니다.

시스템 구성도



맞춤형 샌드박스

'맞춤형 샌드박스'에 의해 한국어를 비롯해 고객의 실제 환경에서 사용되는 OS나 소프트웨어를 이용한 환경을 구축. 실제 환경에 가까운 이미지에서 분석이 가능합니다.

Trend Micro 솔루션과의 연계

트렌드 마이크로의 각 솔루션과 연계하여 각 제품에서 발견 된 의심 파일을 분석합니다.

타사 솔루션과의 연계

ICAP 연계를 지원하고 ICAP 클라이언트 기능을 구현한 Web 프록시 제품 등의 파일이나 URL을 받았다. 사용자 샌드박스에서 분석하고 결과를 피드백합니다.

수동으로 분석

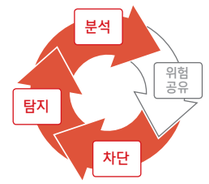
관리 화면에서 분석하려는 파일 URL을 샌드박스로 전송하면 분석이 있습니다.

Mac 파일 분석

macho와 class 등 Mac에서 사용되는 파일 형식도 샌드박스 분석이 가능합니다.

Deep Discovery Email Inspector

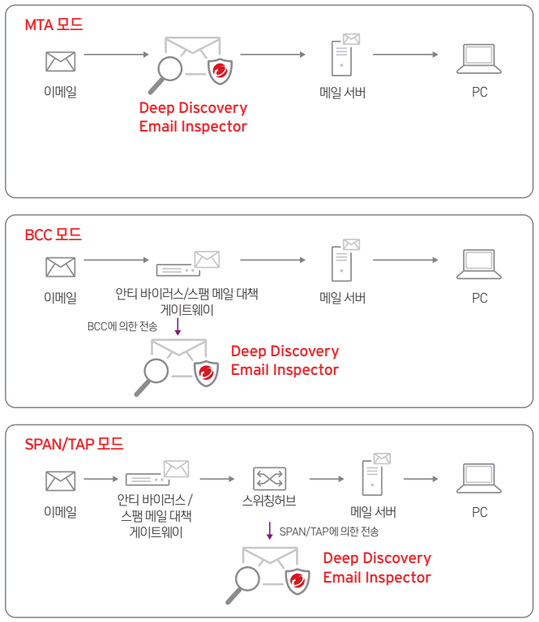
E-Mail APT



Connected Threat Defense™ 지원

표적형 메일 공격이나 랜섬웨어 메일 공격도 차단하는 메일 보안에 특화된 제품입니다. 이러한 공격에 대해 최신 탐지 기술과 샌드박스에 추가로 암호가 있는 파일도 지원하는 것으로 문제를 해결합니다. 이메일을 제어 할 수 있는 MTA 모드 뿐만 아니라 탐지모드로 기존 시스템 구성에 영향을 주지 않는 유연한 도입도 가능합니다.

시스템 구성도



위협에 대응하는 기술

- 암호로 압축 파일도 메일 본문에서 암호를 자동으로 검색하고 분석
- Advanced Threat Scan Engine（ATSE） 이 패턴 감지 할 수 없는 악성 파일이나 문서 취약점 공격 코드를 탐지
- 메일 본문 중의 URL을 분석하여 Web 평판 통해 트렌드마이크로가 매일 업데이트하는 악성 URL 데이터베이스와 비교
- 사용자 샌드박스에 의해 고객의 실제 환경을 재현하고 고객을 노리는 고유의 공격을 탐지

유연한 운용성

- 악성 이메일 탐지 시 즉시 차단 및 첨부 파일 격리, 본문에 경고 메시지 삽입 등을 선택 설정 가능
- 검색 목록에서 드롭 다운으로 자세한 내용을 검색, 첨부 파일 미리보기 등 원활한 관리·운용이 가능

도입 환경에 맞게 설치

- 악성 메일을 차단하는 MTA 모드(인라인)와 감지 모니터링 주체의 BCC 모드 ,TAP 모드에서 설치가 가능
- 게이트웨이 옵션 사용하여 기존의 DDEI 기능 이외에 스팸차단 대책 등의 게이트웨이 기능을 함께 제공 가능

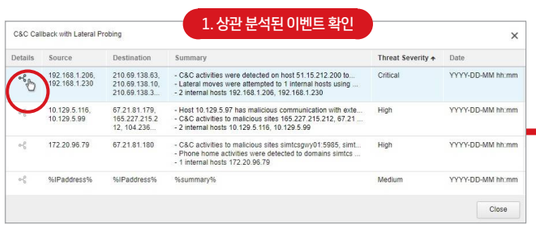
Deep Discovery Network Analytics

Network ATP 상관관계 분석

Network APT솔루션에 운영효율성을 더해주는 상관관계 분석을 제공하여 숨겨진 공격 탐지와 공격에 대한 상관관계 분석을 제공합니다.

특장점

- Deep Discovery Inspector에서 탐지 이벤트, 네트워크 메타데이터 연동
- 상관관계 맵(Map)과 탐지 이벤트/트랜젝션 정보 제공
- 개별 위협 이벤트 간의 연계정보와 상관관계 시각화



APEX One

차세대 엔드포인트 보안

머신러닝 기술을 적용한 고급 위협 보호 백신 기술과 애플리케이션제어, 취약점 방어와 함께 EDR기능까지 사용할 수 있는 올인원 싱글에이전트 엔드포인트 보안 솔루션입니다.

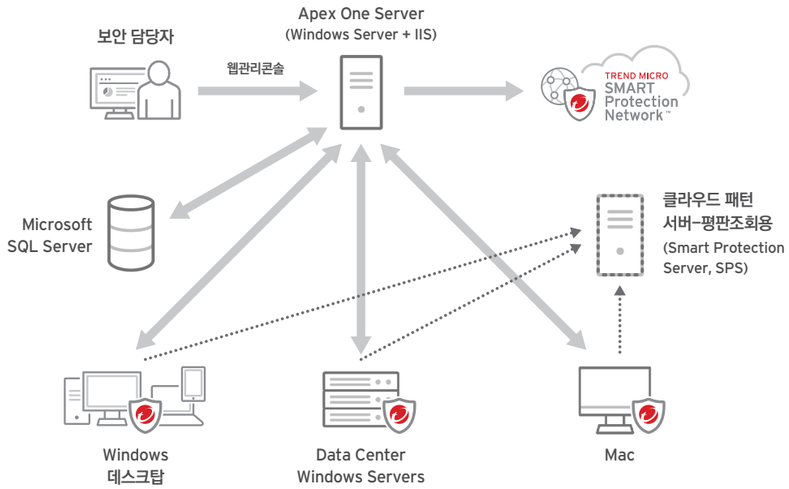
APEX One™ 주요기능

- 실행 전 & 런타임 머신러닝
- 가상패치
- 애플리케이션 제어
- 변종 랜섬웨어 차단
- IOA 동적 기반 분석
- 장치 제어
- C&C 차단
- 에이전트 격리 파일 격리
- 파일 평판 웹 평판

+ 추가 서비스

- EDR
- 클라우드 샌드박스
- XDR/MDR

APEX One™ 구성



보호 대상

- 물리 PC 엔드포인트
- 가상머신 엔드포인트
- 윈도우 PC 및 서버 메일
- Mac 컴퓨터
- POS, ATM 엔드포인트

위협 탐지 기능

- 머신러닝(파일 DNA 지문 분석, 런타임 머신러닝)
- 동작 모니터링(파일리스, 스크립트, 인젝션, 랜섬웨어, 브라우저 위협 대응
- 파일 평판
- 웹 평판
- 센서스(Census) 체크
- 침입 방지(호스트 방화벽, 익스플로잇 방지)
- 취약점 방어(가상패치)
- C&C 차단
- DLP, 장치 제어
- 샌드박스 및 A.P.T 탐지 연동
- EDR(Endpoint Detection and Response)

APEX One EDR

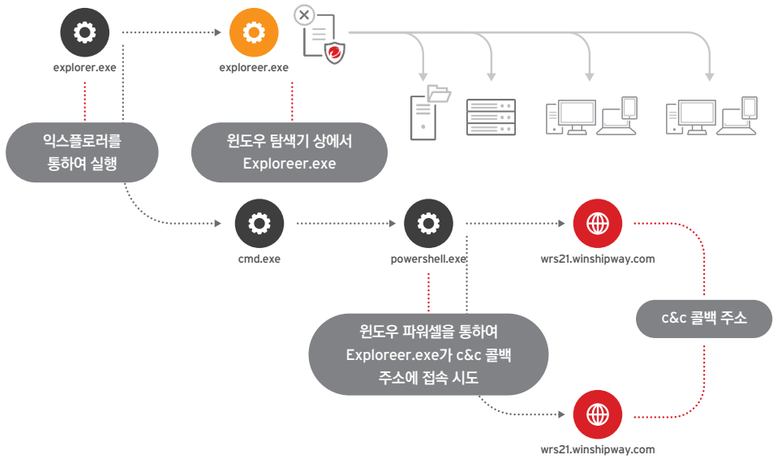
Endpoint Detection and Response

Apex One™ 에이전트에 통합된 EDR(Endpoint Detection and Response)은 위협의 근원을 탐색하고, 새로운 위협을 추적할 수 있도록 하는 고급 탐지와 분석을 가능하게 하고 최적의 대응방법을 제공합니다.

특장점

- 자동화 된 EDR 프로세스
- 위협 분석 통찰력과 풀 가시성
- 올인원 솔루션

RCA(Root Cause Analysis) 제공



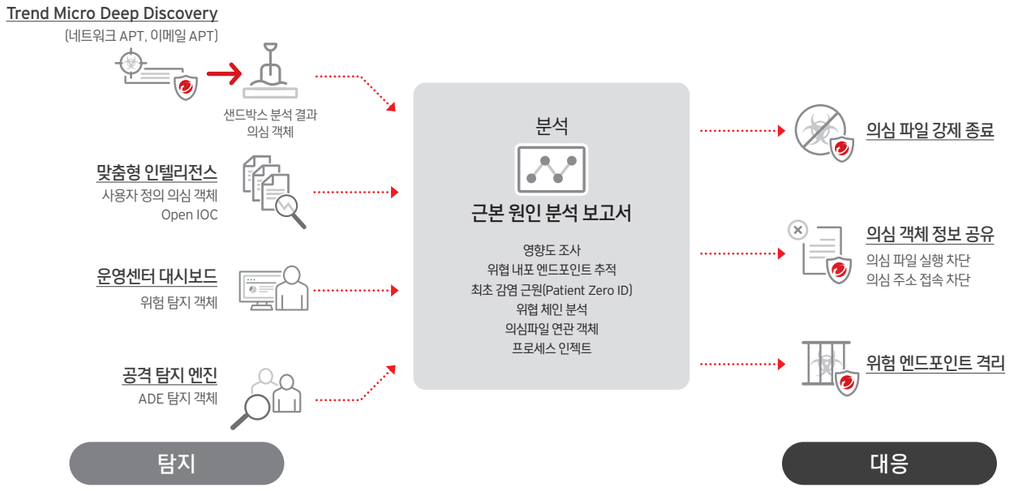
보호 대상

- Microsoft® Windows®
- MacOS*

주요 기능

- IOC 스위핑
- IOA 헌팅
- RCA분석
- 영향력 있는 탐지 분석
- 신속한 대응
- API 연동 지원

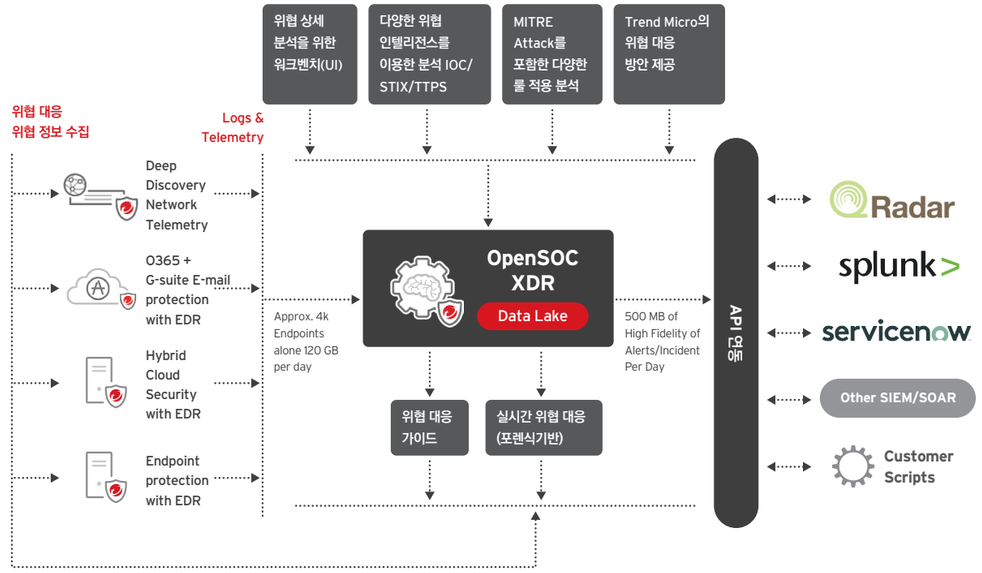
APEX One EDR 워크플로우



XDR/MDR

Managed Detection and Response Service

Trend Micro XDR/MDR는 서비스는 전자 메일, 엔드 포인트, 서버, 클라우드 워크로드 및 네트워크에서 위협을 탐지하고 대응하여 기업이 위협을 완화하는 동시에 고객의 보안팀의 위협대응에 대한 부담을 덜어줍니다. 이는 특허 받은 빅 데이터 인공 지능 (AI) 기술과 전문가 위협 인텔리전스를 사용하여 공격 전에 위협을 탐지하는 데 도움이 됩니다. 세부적인 근본 원인 분석(RCA)을 통해 공격의 범위와 확산을 파악하고 선제적인 대응 계획을 제공합니다.



Trend Micro XDR/MDR

특장점

AI 및 전문가 보안 분석

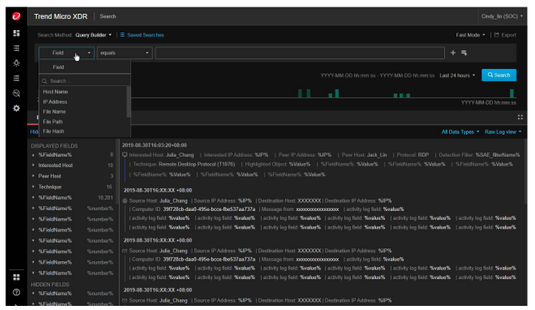
- 탐지율을 높이기 위한 기본 위협 전문 글로벌 위협 인텔리전스

엔트포인트를 뛰어넘는 모든 레이어 모니터링

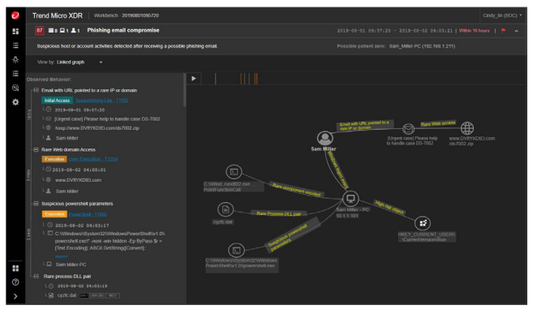
- 다중 계층(Cross-Layer) 에 걸친 위협 탐지와 대응

완벽한 가시성 제공

- 적은 리소스로 더 빠르게 대응할 수 있는 단일 플랫폼



빅데이터기반의 위협 검색



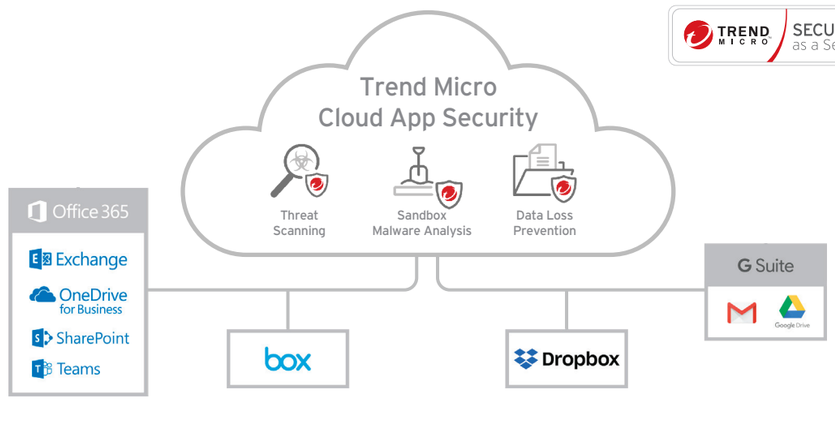
RCA(Root Cause Analysis)

Cloud App Security

Trend Micro Cloud App Security™를 사용하면 보안을 유지하면서 클라우드 서비스의 효율성을 극대화 할 수 있습니다.
유입되는 내부 Office 365 및 G Suite 전자메일에 대하여 고급 멀웨어 및 기타 위협으로부터 보호하고 Box, Dropbox, Google 드라이브, SharePoint® Online 및 OneDrive® for Business를 비롯한 다양한 클라우드 파일 공유 서비스에 대하여 보안을 적용합니다. Cloud App Security는 전자 메일 트래픽의 경로 변경이나 웹 프록시 설정없이 모든 사용자 기능을 유지하면서 API를 사용하여 Office 365 및 G Suite 그리고 기타 서비스와 직접 통합됩니다.

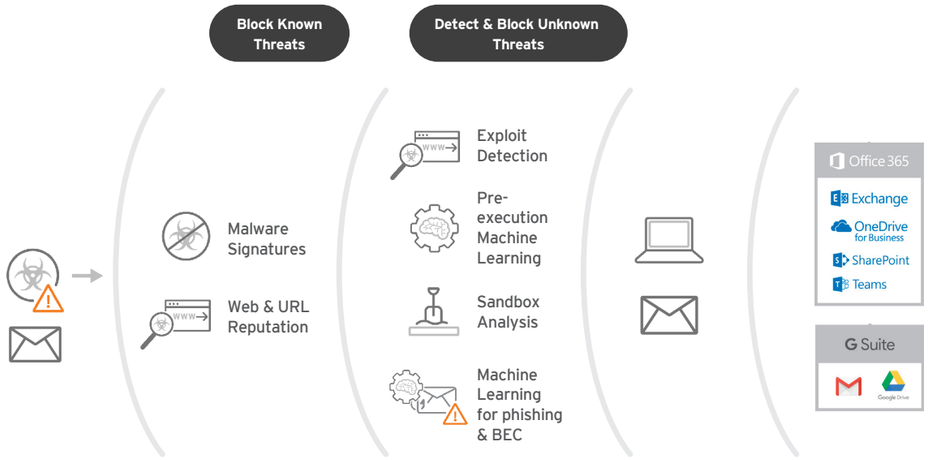
Connected Threat Defense™

제품 구성



주요 기능

- Office 365 및 G Suite 전자메일에 대한 피싱(Phishing) 차단과 메일 내 신종/변종 악성코드차단
- 관리자와사용자 환경에 최적화된 클라우드 애플리케이션 보안
- 애플리케이션, 장비 구성변경없이 자동 배포

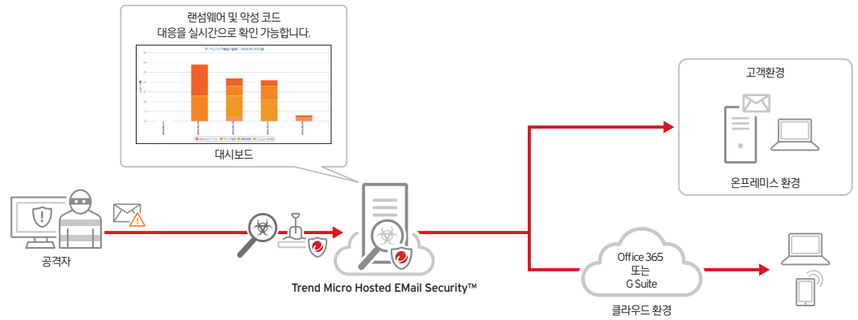


EMail Security

표적형 메일 공격과 기업이나 조직을 노리는 공격이 고도화·다양화되고 있으며 새로운 위협에 대응할 수 있는 솔루션이 필요합니다. 기존의 '이메일 바이러스·스팸 메일 대응'에서 '표적형 메일 공격 대응'에 클라우드 이메일 보안을 제안합니다.

TREND MICRO SECURITY as a Service

제품구성



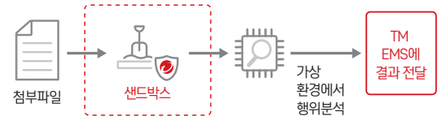
특장점

고급 표적형 메일 공격에 의한 침입을 방지

- APT 공격에 최초로 이용되는 표적형 메일 공격에 대해 "클라우드 샌드박스"를 사용한 동적 분석을 통해 알려지지 않은 위협 탐지
- 본문 등의 악성 프로그램을 다운로드 위험성이 있는 의심 URL 차단
- 유연한 설정이 가능하며 관리가 쉬운 스팸 메일 대책
- 판정이 어려운 스팸 방어 뿐만 아니라 오탐이 적고 다층 검사를 실시하여 최종 사용자가 격리 정책에 대한 유연성 제공
- Office365, G Suite 환경 지원

클라우드 샌드박스

- 트렌드마이크로 "클라우드 샌드박스"는 소프트웨어 등의 실행 환경을 클라우드에서 에뮬레이션 (가상 실행)하여 지금까지 감지 할 수 없었던 알려지지 않은 위협을 탐지·차단



비즈니스 이메일 사기(BEC) 대응

- 기업 내부 임직원 행세를 이용하는 BEC 대응
- 머신러닝기반 BEC 탐지

기능

요약		상세기능
	바이러스·스팸·피싱 메일 차단	바이러스 검색 등 규칙을 조합 보내는 메일 수신 메일에 대한 보안 위험을 탐지지/처리의 설정이 가능합니다。
	그레이(Gray) 메일 대응	이메일 마케팅 등 기업의 정책에 의해 결정이 갈라지는 그레이 구간의 메일을 대응합니다.
	고급 위협 검색	패턴 기반의 검색 및 추론 검색을 결합하여 표적형 메일 공격에 사용되는 문서의 공격 코드 및 기타 위협을 감지하고 필요에 따라 클라우드 샌드박스에 보냅니다.
	클라우드 샌드박스	ATSE에서 감지 의심스러운 이메일 첨부 파일과 URL을 필요에 따라 트렌드마이크로가 관리하는 클라우드 샌드박스에서 실행하고 행동을 분석할 수 있는 동적 분석 기능을 제공합니다. 표적형 메일 공격에 대한 대응을 보다 고도화 할 수 있습니다.
	소셜 엔지니어링 공격 대책	소셜 엔지니어링 공격 방지를 실행하면 스팸 검색 엔진에 의해 메일이 송수신 될 때마다 메일 각 부분(메일 헤더, 제목, 본문, 첨부 파일 및 SMTP 프로토콜 정보 등)에서 의심스러운 활동이 검색됩니다.
	콘텐츠 필터링	사전에 설정된 규칙이 준비되어 있으며, 키워드, 용어, 첨부 파일의 특성 및 기타 필터 규칙에 따라 이메일 메시지와 첨부 파일을 필터링 할 수 있습니다. 관리자는 기본 규칙을 수정하거나 새 규칙을 만들 수 있습니다.
	최종 사용자 격리	최종 사용자 격리 콘솔을 이용하여 각 최종 사용자는 격리된 스팸 메일 처리(재전송/삭제) 및 개별 승인 된 발신자 목록에 추가 실시할 수 있습니다.