화이트리스트 기반의 적응형 서버보안솔루션

mp(Malicious Process)Protect

(주) 굿데이아이티

Agenda

01 제안 배경

02 제품 소개

03 주요 기능

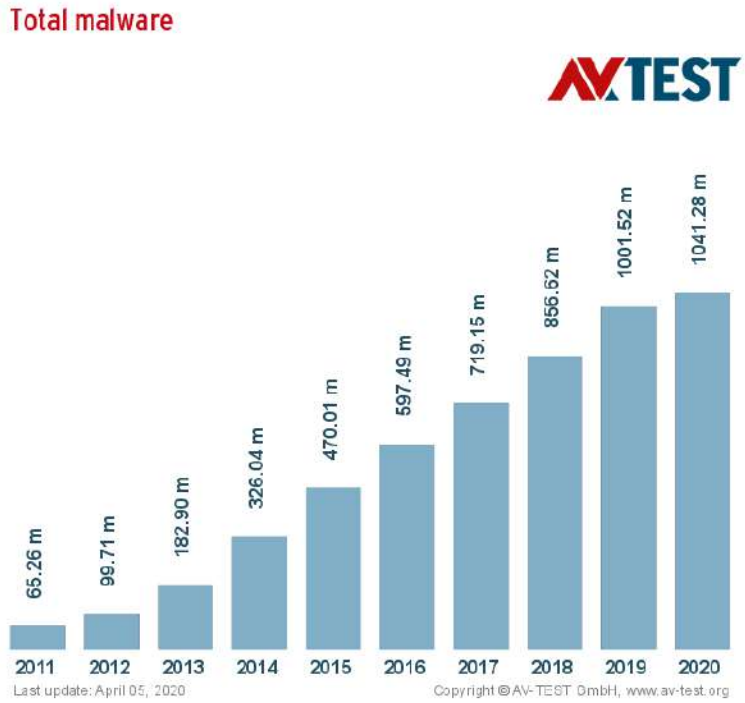
04 Case Study

01

제안 배경

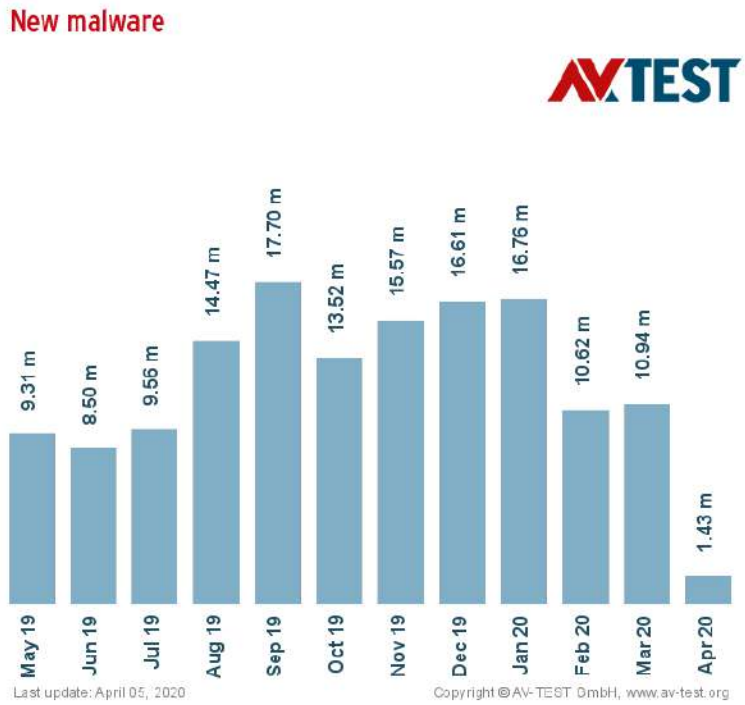
1. 보안 위협의 증가
2. 기존 대응방식의 한계
3. 차세대 서버 보안솔루션의 필요성
4. 기술적 배경 및 방향

1. 보안 위협의 증가



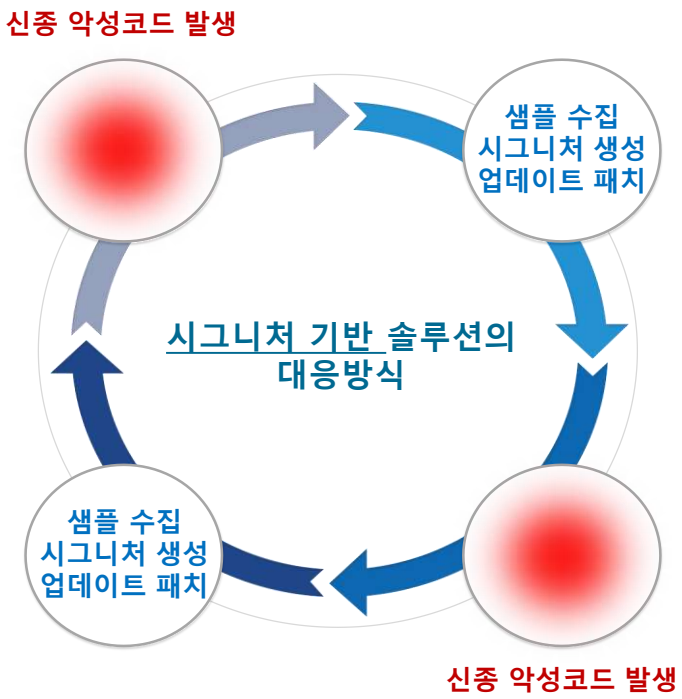
- 시스템 및 어플리케이션의 다양성과 복잡성에 따른, **악성코드의 지속적인 증가 (2020년 기준 약 10억 개 이상)**
- 주요 정부기관 및 기업 등에 치밀하고, 조직화된 형태로 목적에 따른 표적 공격(Targeted Attack)이 이루어 짐
- 공격의 80%는 범죄를 목적으로 하며, 해킹사고의 81%는 공격자가 몇 분만에 공격을 성공시킴
- 해킹사고 후 **67%가 수주 또는 수개월 동안 감지되지 않으며, 제 3자에 의해 보고**되고 있음

2-1. 기존 대응방식의 한계



- 기존 보안 환경을 우회하는 형태로 진화하고 있는 **신·변종 악성코드의 지속적인 출현**
- 시그니처(Signature) 기반, 룰 기반(Rule-based)의 보안 시스템은 신/변종 악성코드 탐지가 어렵고, 분석 및 대응을 위해 평균 5 ~ 14일까지 소요
- 약 30 ~ 40%의 Malware는 Time/Event 기반으로 Sandbox를 인지한 뒤, 이를 우회하는 공격을 수행

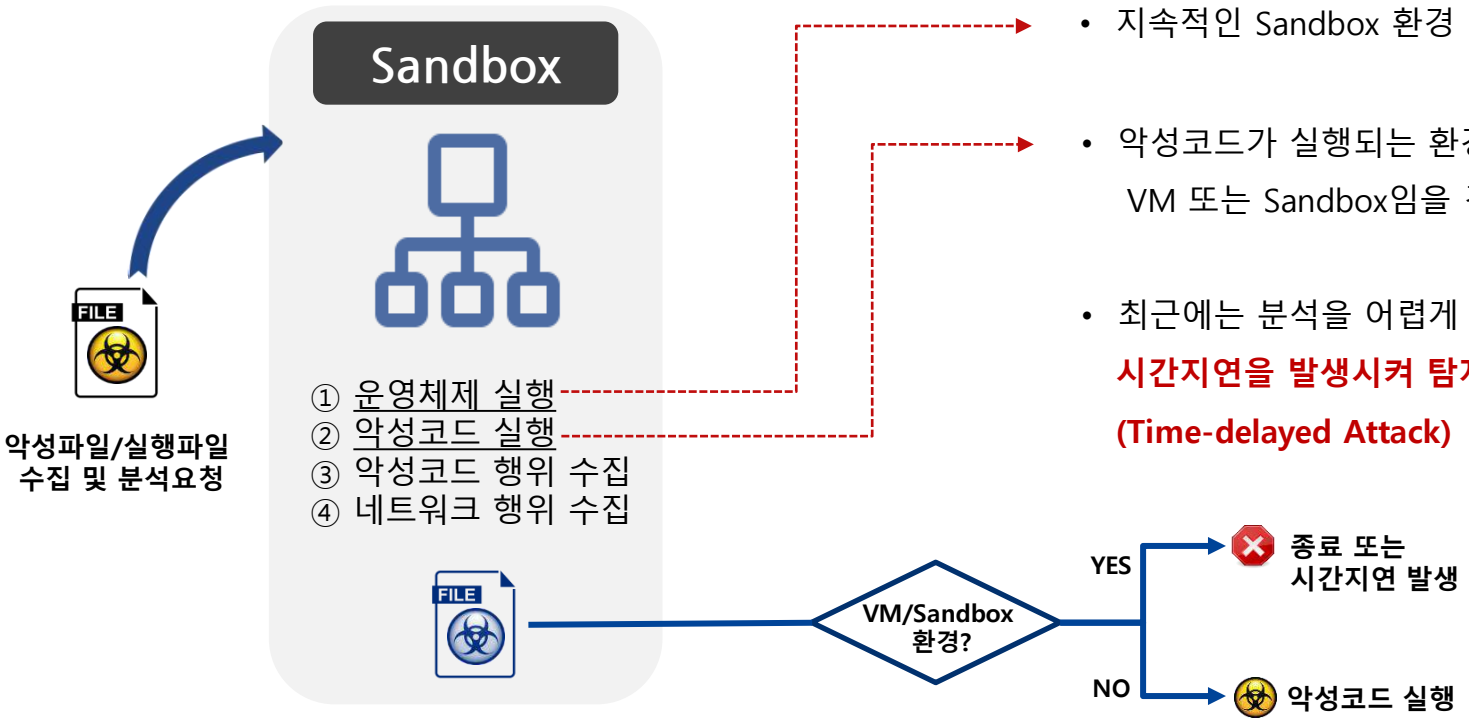
2-2. 기존 대응방식의 한계



- 악성코드에 대응하기 위한 시그니처 생성속도가 신종 악성코드의 출현 속도를 따라가지 못하면서 **제로-데이 공격에 대한 시간증가와 사후처리에 대한 한계점**이 존재하고 있음

반복적인 해킹사고 발생..

2-3. 기존 대응방식의 한계



- 지속적인 Sandbox 환경 업데이트 필요
- 악성코드가 실행되는 환경을 검사하여 VM 또는 Sandbox임을 감지하고 **실행종료**
- 최근에는 분석을 어렵게 만들기 위해 **시간지연을 발생시켜 탐지를 어렵게 함 (Time-delayed Attack)**

샌드박스 우회 가능..

3. 차세대 서버 보안솔루션의 필요성

환경 변화에 따른 필요성

- 복잡하고 고도화되는 융합산업에 대한 보안위협의 증가에 대응할 수 있는 신기술 필요
- IoT 기기 등 다양한 환경의 스마트 서비스 서버들에 대한 포괄적인 보안체계 마련
- 폭증하는 서비스 서버들에 대한 통합보안 과제방안 마련
- 공공/기업들의 스마트 서비스 등이 클라우드 환경으로 전환함에 따른 보안대책

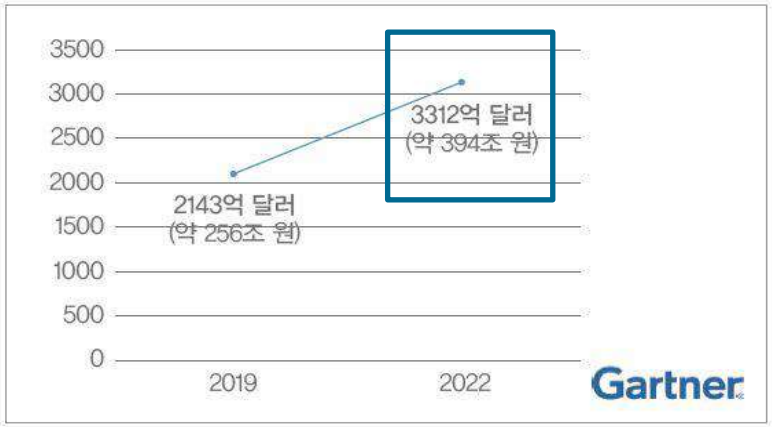
보안 위협에 따른 필요성

- 알려진 + **알려지지 않은 악성코드(Unknown)** 모두를 차단하는 새로운 접근방식 필요
- 알려지지 않은 악성코드에 대한 분석정보 및 위험성 제공
- 보안 담당자의 업무 부담을 줄이기 위한 자동 차단 및 분석 필요

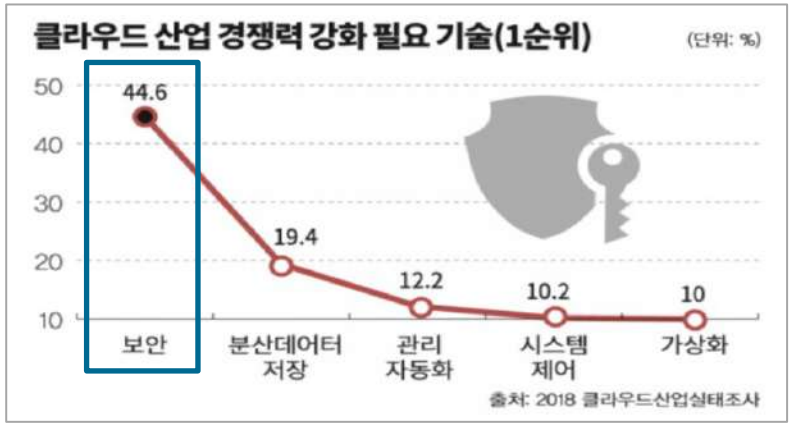
3. 차세대 서버 보안솔루션의 필요성

클라우드 환경전환에 따른 주요 이슈

- 복잡성 증대 : 멀티 클라우드, 하이브리드 클라우드 등
- 가시성 부재 : 사용자가 클라우드 운영 및 보안에서 배제
- 새로운 위협 : 오픈 운영환경에서 예상하지 못하는 다양한 위협이 존재
- 네트워크 백본형 보안장비들의 기능과 역할의 한계

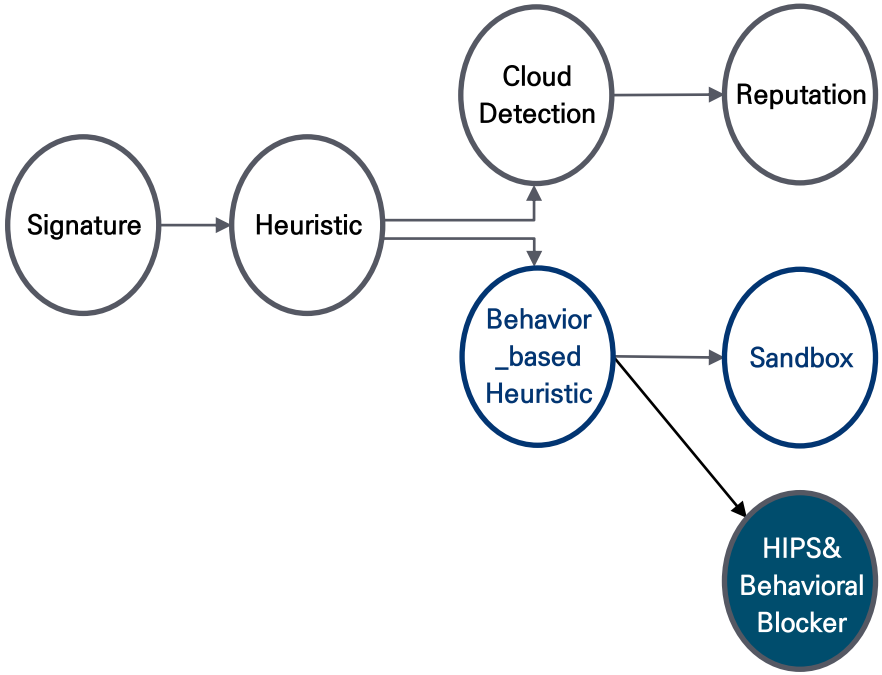


퍼블릭 클라우드 서비스 시장 규모(자료: 가트너)



4. 기술적 배경 및 방향

HIPS & Behavioral Blocker의 개념을 융합서버 보안기술에 적용



탐지방식	설명	제품
Signature	프로그램 서명을 확인하여 탐지 및 차단	백신 소프트웨어
Cloud reputation	의심파일을 분석서버로 보내 분석 후 판단결과를 통보	
Sandbox	의심파일을 보호된 영역에서 작동시켜 탐지 후 차단	파이어아이, 트렌드마이크로 등
HIPS	프로그램의 이벤트(프로세스의 행동)를 감시하고 분석하여 이벤트 실행을 차단	카스퍼스키, 코모도 등
Behavioral Blocker	HIPS와 동일하나 이벤트를 점수화하여 일정점수가 초과되면 차단	SONAR (노턴)

▶ HIPS & Behavioral Blocker의 개념을 PC에서 서버로 적용 (윈도우, 리눅스, 클라우드 컴퓨팅 환경 지원)

02

제품 소개

1. 제품 개요
2. 제품 특징
3. 구성 방식
4. 구조 및 동작원리
5. 사용 환경

1-1. 제품 개요

mpProtect

mp(Malicious Process)Protect는 화이트리스트 기반의 "알려진+알려지지 않은" 악성 프로세스를 신속하게 차단하고, 머신러닝으로 이상징후를 탐지하는 행위기반의 적응형 서버보안 솔루션입니다.

화이트리스트 기반의
프로세스 관리

" 알려진+알려지지 않은"
악성코드 제어

클라우드 분석 시스템
분석정보 제공

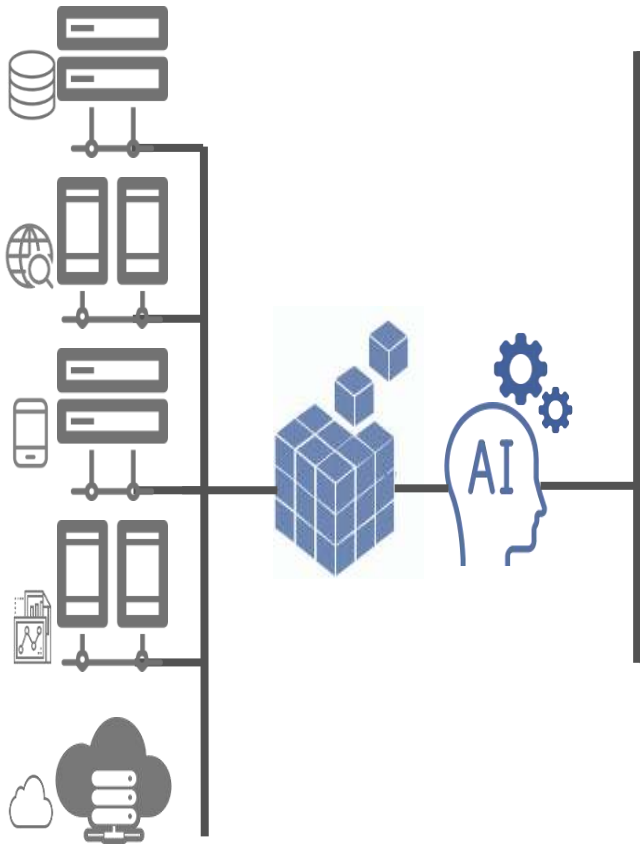
머신러닝 기반의 프로세스
이상징후 탐지

- ✓ 서버환경에 최적화된 화이트리스트 기반관리
- ✓ "알려진+알려지지 않은" 악성코드 탐지 및 실행 차단
- ✓ 탐지 프로세스 분석정보 및 위험도 제공(분석 시스템)
- ✓ 머신러닝 기반 다양한 모델의 프로세스 이상징후 탐지
- ✓ 중앙 집중 관리 및 제어
- ✓ 경량 에이전트 및 자원 점유 최소화

1-2. 제품 개요

mp(Malicious Process)Protect는 악성 프로세스 방어를 위한 빠른 탐지뿐만 아니라, 화이트리스트 기반의 관리로 선제적 대응 후 담당자에게 알림을 제공합니다.

2. 제품 특징



레퍼런스(whitelist) 관리

사전에 프로세스 whitelist 수집 및 실시간 프로세스 whitelist update를 통해 다양한 공격에 효율적으로 대응

중요 프로세스 보호

중요 프로세스에 대한 임의 종료 방지,
정상 프로세스의 임의 삭제 시 차단 및 통지

자동 실행차단

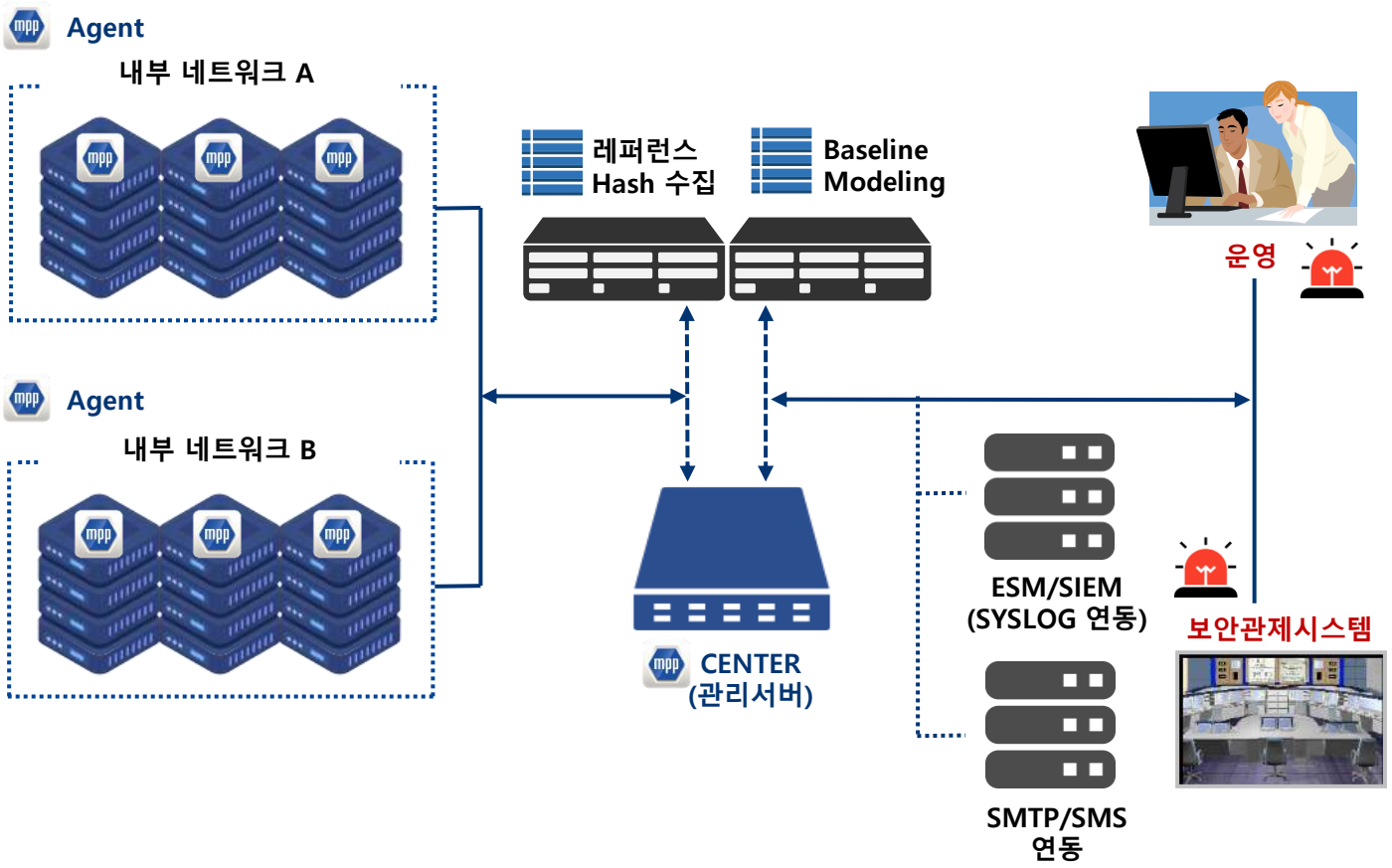
악의적으로 판명된 프로세스를 목록화 하여
해당프로세스 발생시 즉시 실행 차단

이상징후 탐지(Baseline Modeling)

머신러닝 기반의 프로세스의 자원 사용량 체크 및 이력을 주기적으로 수집하여, 정상 운영범위 (Baseline)를 모델링 후 임계치 설정을 통해 이상징후 탐지

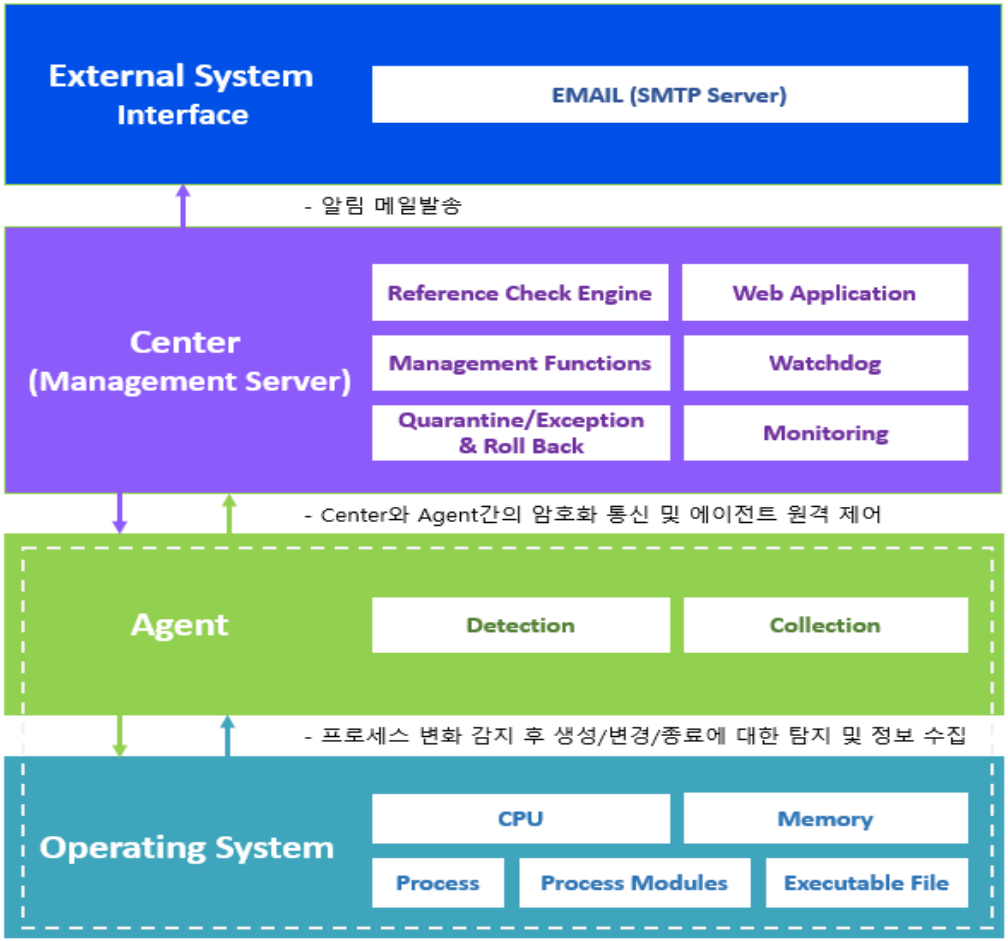
3. 구성 방식

mp(Malicious Process)Protect는 서버에 설치되는 에이전트와 중앙 관리를 하는 센터 서버로 구성되며, 관리자는 웹매니저(브라우저)를 통해 관리를 하게 됩니다.



4. 구조 및 동작원리

mp(Malicious Process)Protect는 OS에 에이전트가 설치되어 탐지 및 수집을 수행합니다. 센터서버는 에이전트들의 상단에 위치하며, 내부적으로 Reference Check Engine과 Web Application이 운영되고 있습니다.



5. 사용 환경

MPP CENTER

CENTER
(관리서버)

- **운영체제** : CentOS 7
- **웹 매니저(브라우저)** : Internet Explorer 9 이상, 크롬, 파이어폭스

MPP AGENT

Agent

[Windows]

- Windows Server 2000, 2003, 2008/R2, 2012/R2, 2016
- Windows Embedded standard 2009, 7
- Windows Embedded POSReady 2009, 7
- Windows Embedded 8.1

[Linux]

- RHEL 4 이상, CentOS, SuSE, Ubuntu

[Cloud OS]

- Windows, Linux

03

주요 기능

1. 기능 요약
2. 레퍼런스(whitelist) 수집기반 탐지
3. 알려지지 않은 프로세스 탐지 및 처리
4. 알려지지 않은 프로세스 분석정보
5. 실행 중인 프로세스 정보 확인
6. 머신러닝 기반의 Baseline Modeling
7. 연동기능
8. 대시보드

1. 기능 요약

프로세스 탐지

- ✓ 신규/변경/종료 프로세스 탐지
- ✓ 악성 프로세스 실행 차단
- ✓ 이상징후 탐지 (머신러닝 시스템 연동)

프로세스 정보

- ✓ 실행 중 프로세스 정보 확인
- ✓ 중요 프로세스 관리
- ✓ 프로세스 종료 이력
- ✓ 실행파일 분석 (클라우드 분석시스템 연동)

관리기능

- ✓ CENTER 관리 (관리서버)
- ✓ 에이전트 관리
- ✓ 레퍼런스 관리
- ✓ 업데이트 관리

부가기능

- ✓ SYSLOG 전송
- ✓ EMAIL/SMS 탐지내역 전송
- ✓ Scale In/Out 자동지원 (가상화 환경)

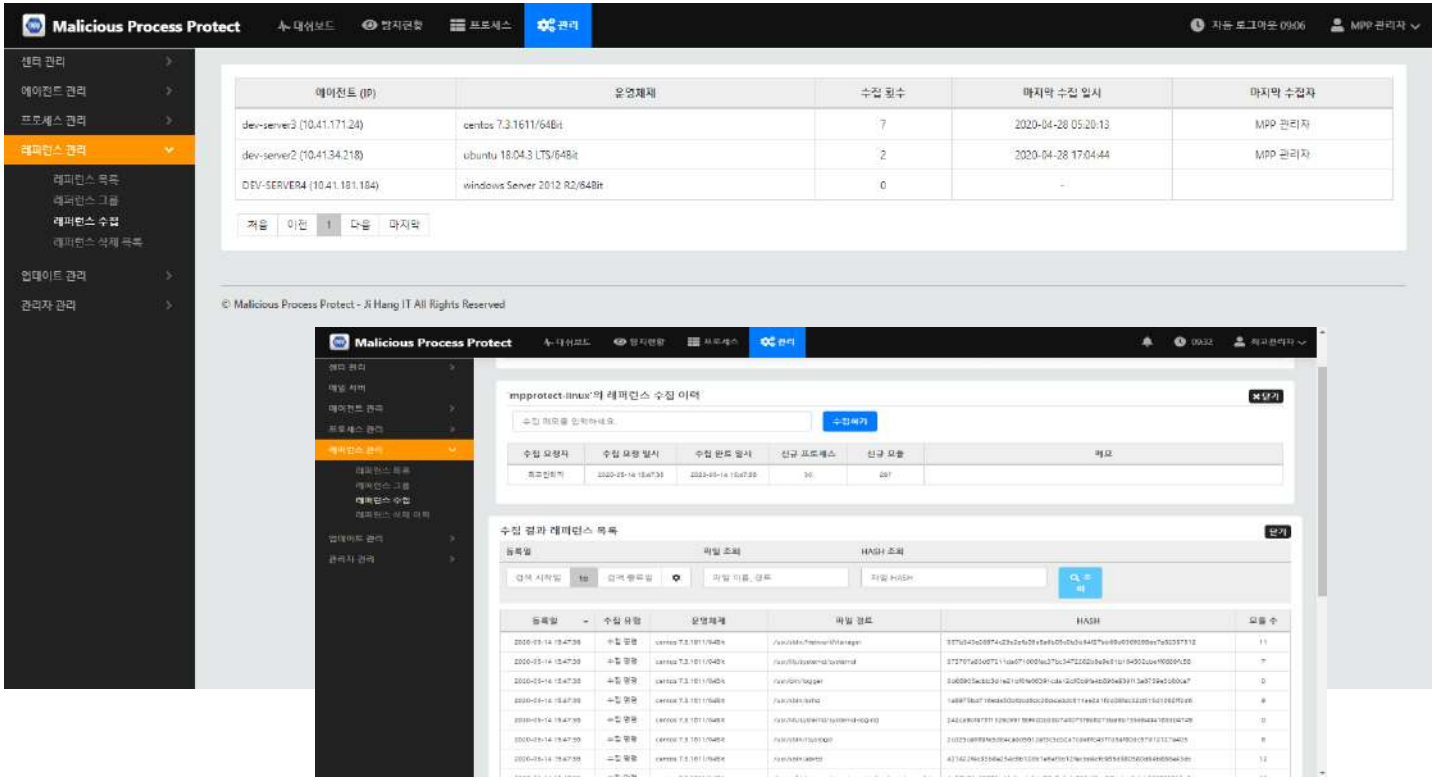
2. 레퍼런스 수집기반 탐지

합법적 프로세스를 보호하기 위한 화이트리스트 관리 기반 제공

화이트리스트 관리 기반은 사전에 정상적인 프로세스의 해시값을 수집한 뒤, 실시간 탐지과정에서 발견되는 프로세스와 비교하여 실행 차단 또는 수동검역 하거나, 정상일 경우 화이트리스트로 등록하는 관리 방식입니다.

탐지 전 프로세스
해시값 수집

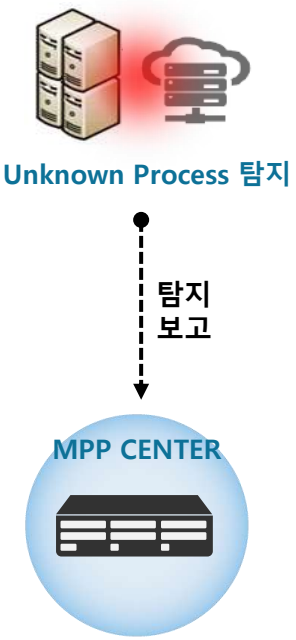
실시간
프로세스 탐지

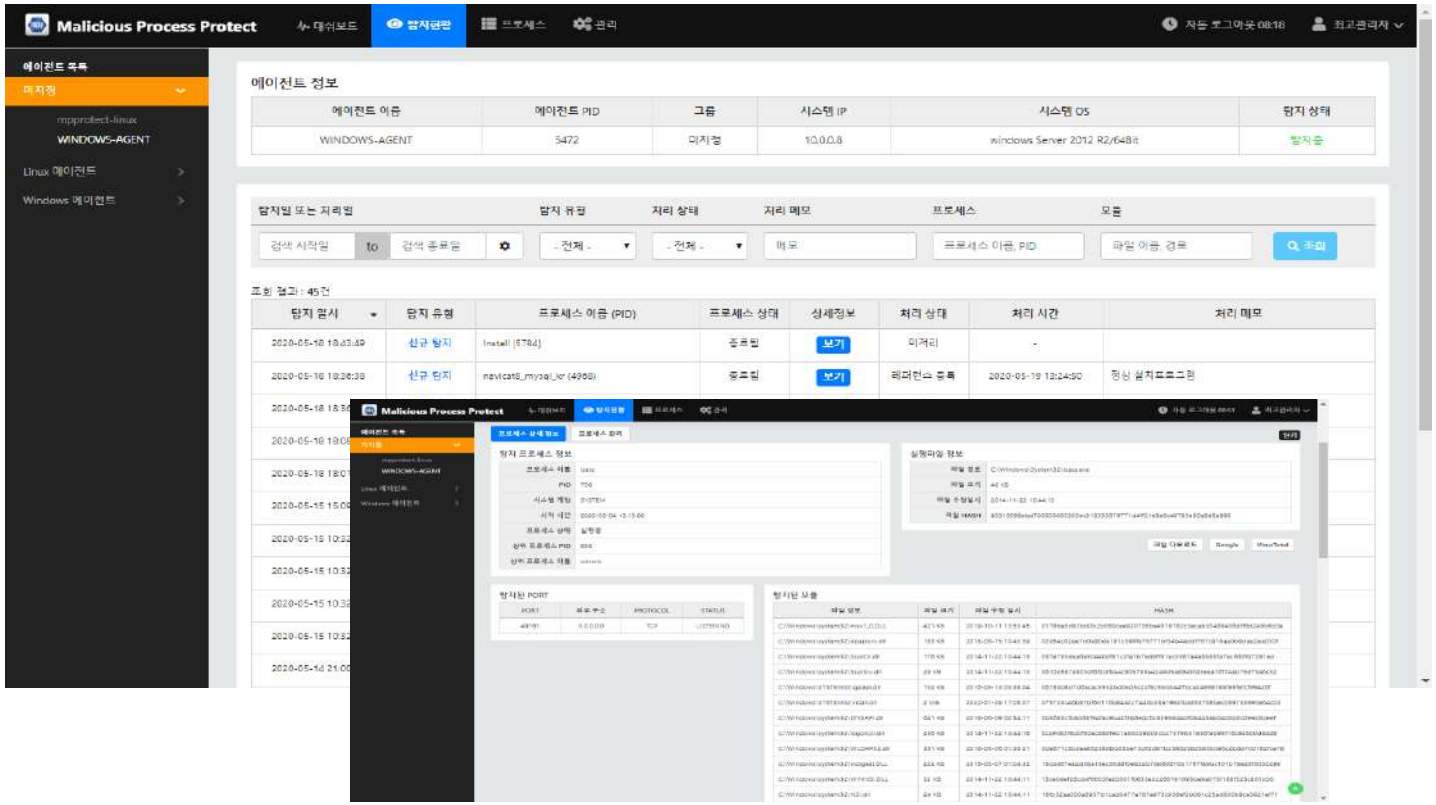


3. 알려지지 않은 프로세스 탐지 및 처리

알려지지 않은 프로세스 탐지 및 처리

알려지지 않은 새로운 프로세스가 탐지 될 경우, 실시간으로 관리자에게 탐지 내용을 전송하여 알리고, 관리자는 분석정보를 통해 검역 또는 예외 처리를 합니다.

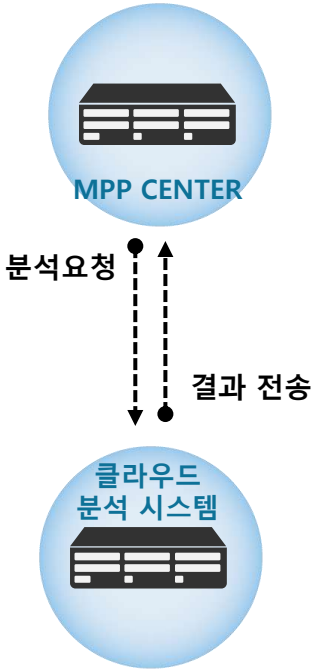


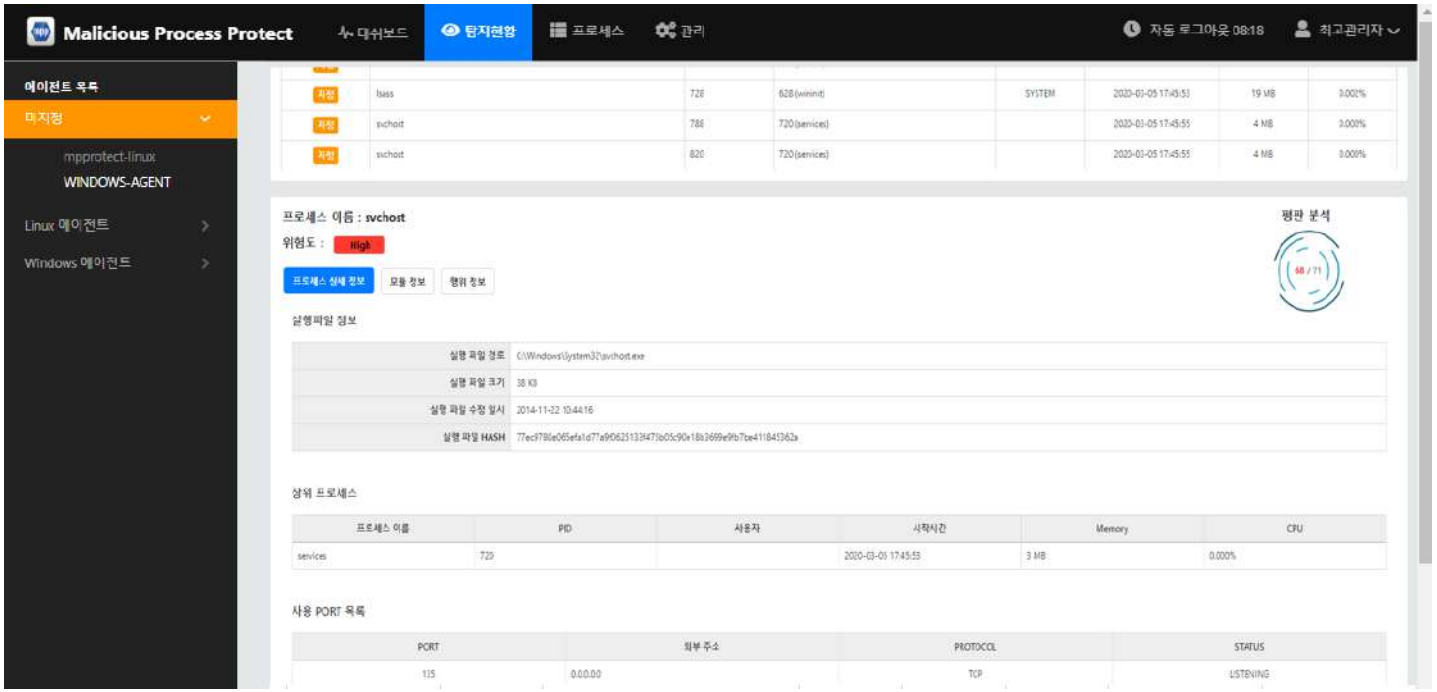


4. 알려지지 않은 프로세스 분석정보

알려지지 않은 프로세스 파일 분석

클라우드 분석 시스템 연동을 통해 알려지지 않은 악성 파일에 대한 정적/동적 분석 및 평판 기반 분석정보를 제공합니다.

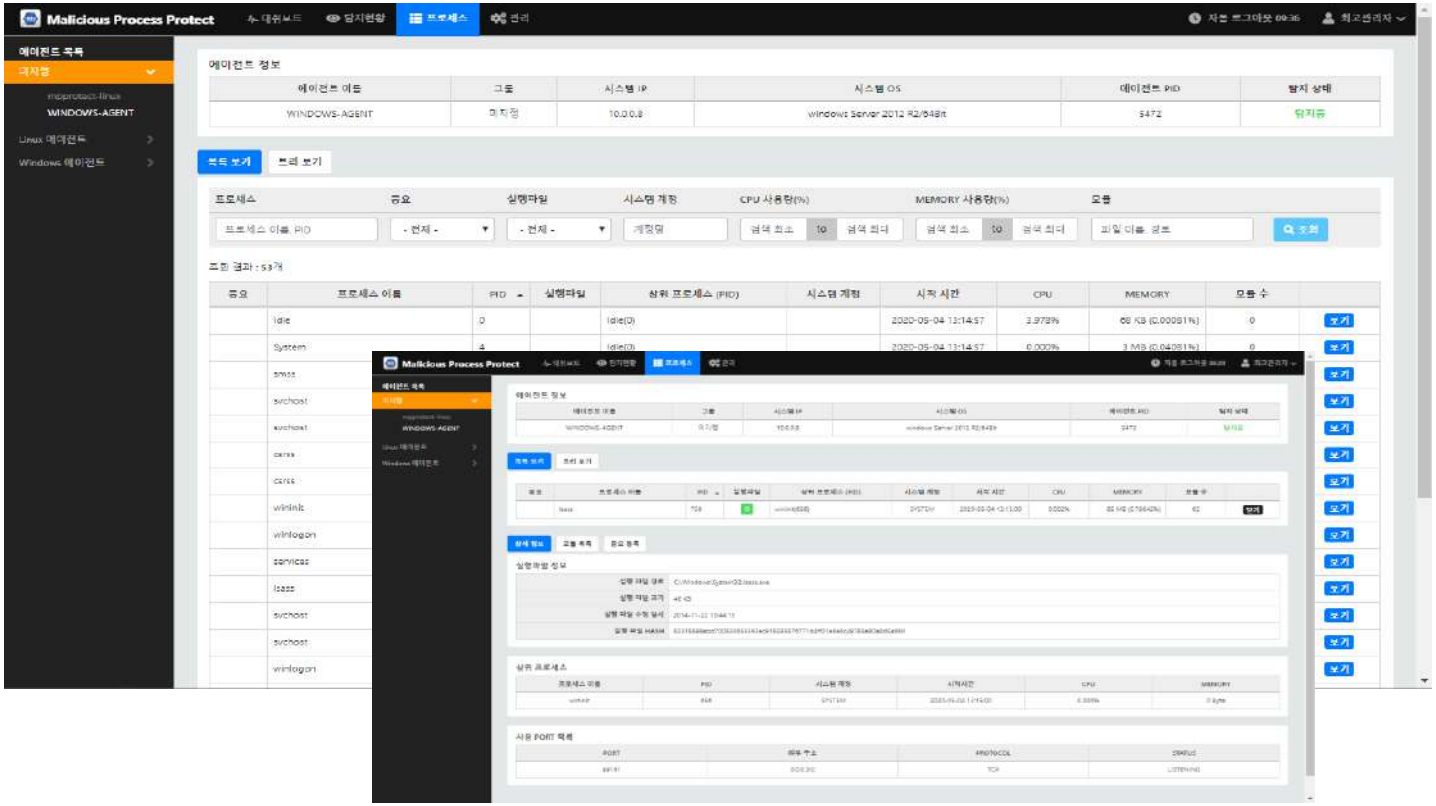




5. 실행중인 프로세스 정보 제공

실행중인 프로세스 정보 수집

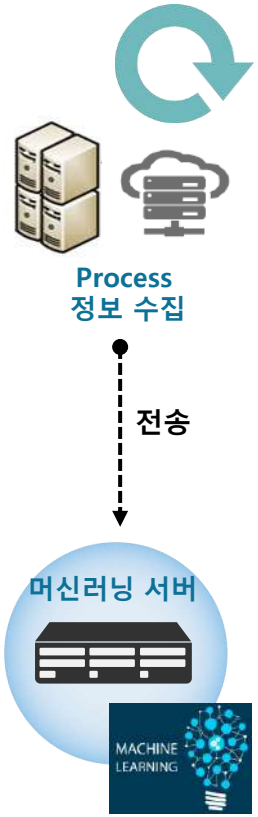
서버내 실행중인 프로세스의 정보를 제공하고, 프로세스의 CPU, MEMORY를 수집하여 머신러닝과 연동 후 이상징후를 탐지합니다. 또한, 중요 프로세스 등록을 통해 프로세스 임의 종료 시, 종료탐지로 관리자에게 통보합니다.

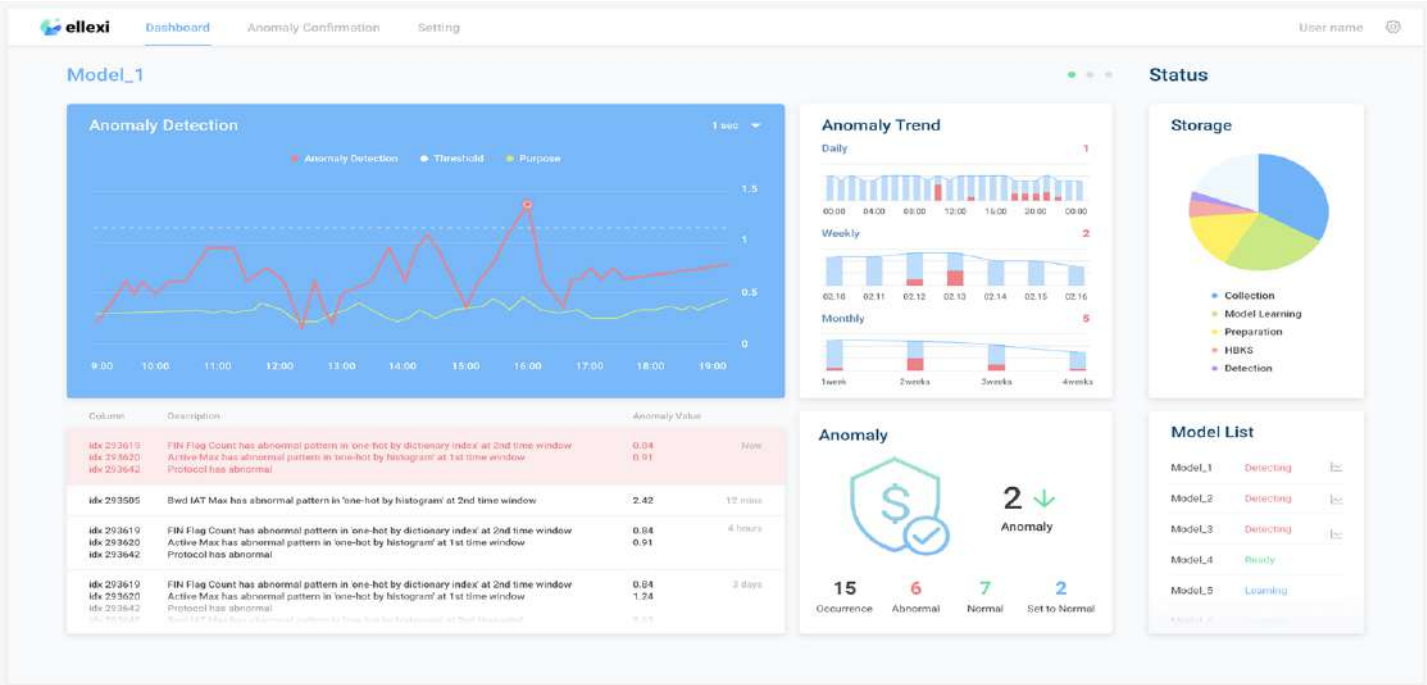


6. 머신러닝 기반의 Baseline Modeling

머신러닝 연동을 통한 프로세스 이상징후 탐지

동작중인 프로세스의 리소스 사용량 및 프로세스 특성 정보를 수집하여 머신러닝 기반으로 이상징후를 탐지하고 시각화하여 관리자에게 정보를 제공합니다.

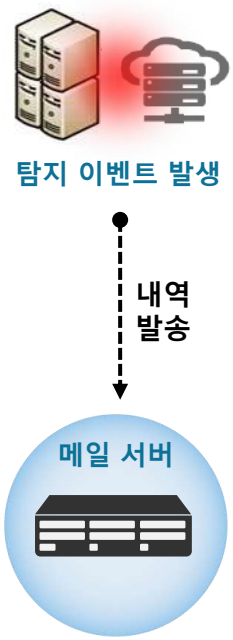


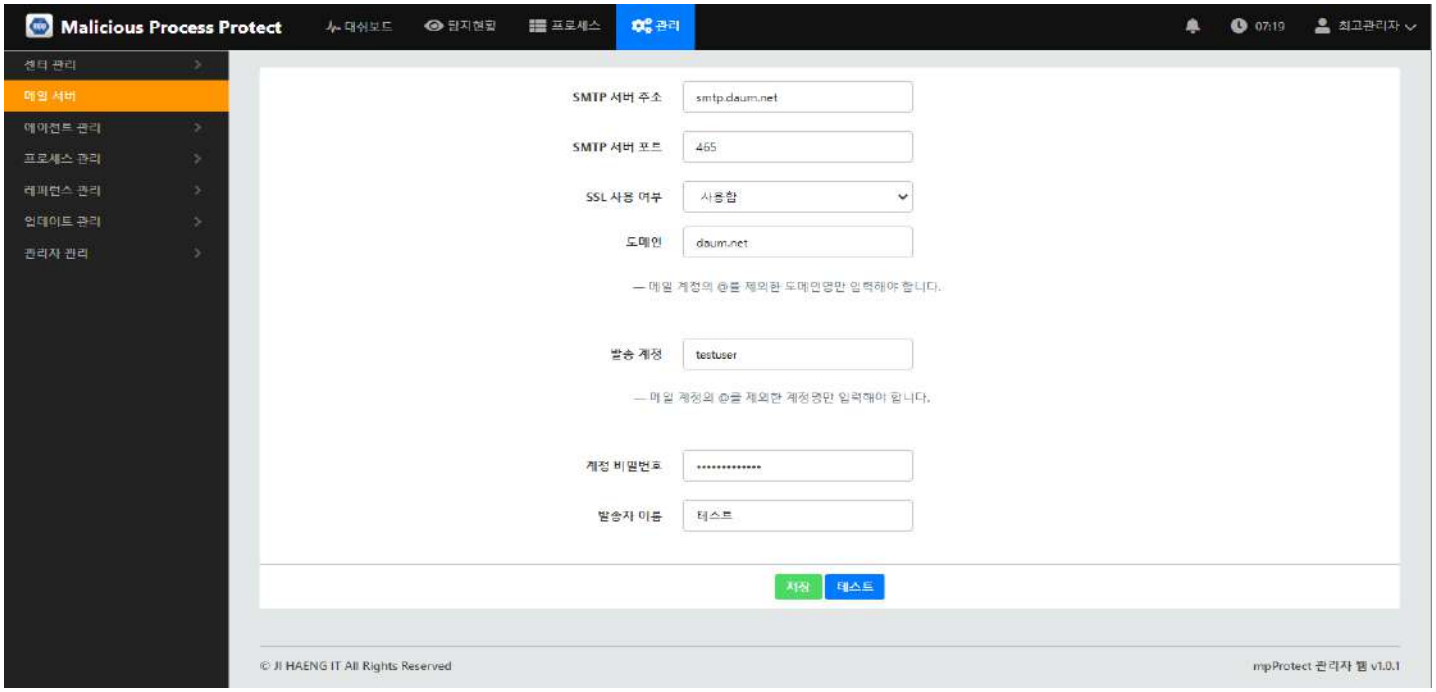


7. 연동 기능

연동을 통한 탐지로그 전송

SMTP 설정 및 SMS, MAIL DB 설정을 통해 탐지내역을 관리자에게 전송이 가능하며, 로그 수집서버(ESM, SIEM)와의 연동을 통해 전체 또는 유형별 SYSLOG 전송을 합니다.

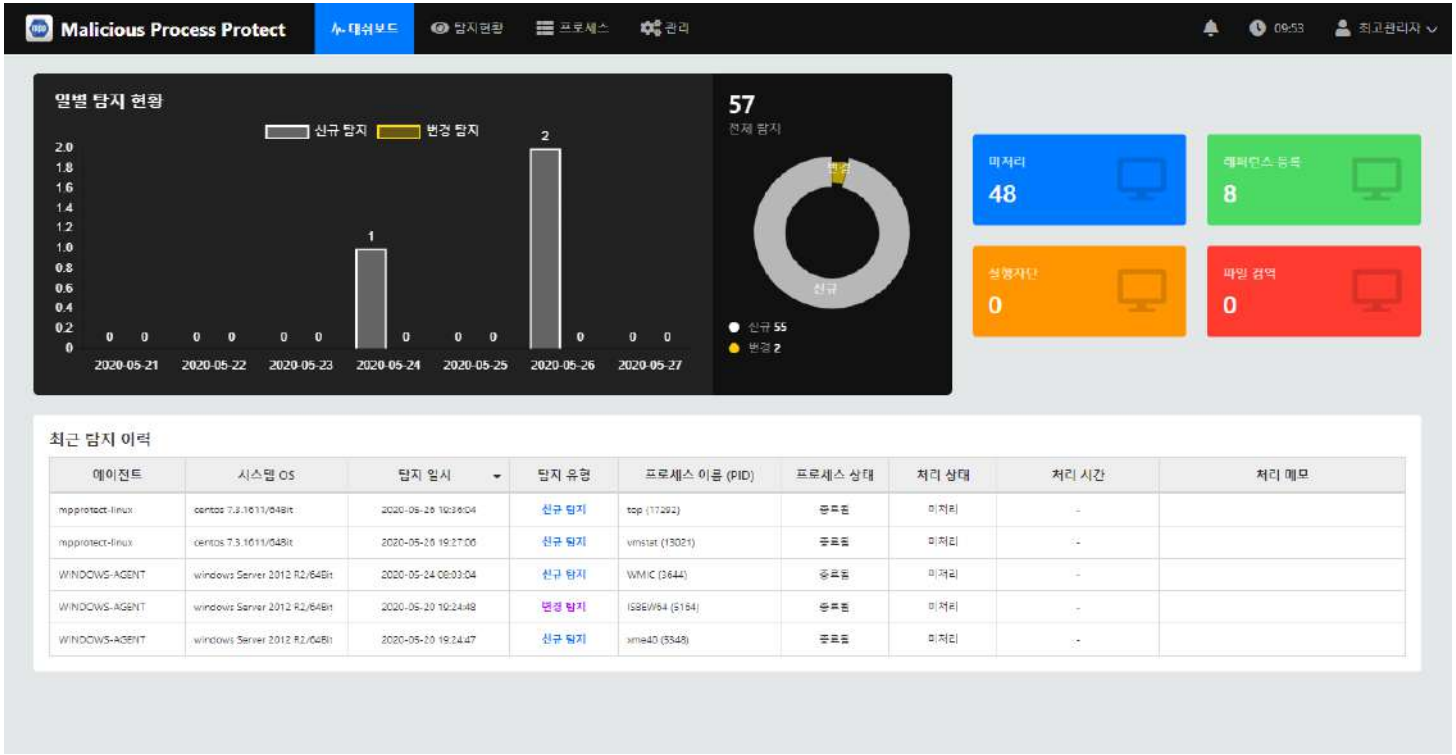




8. 대시보드

대시보드 화면

탐지 및 주요 이벤트를 중심으로 관리자가 쉽게 볼 수 있는 대시보드를 제공합니다.



04

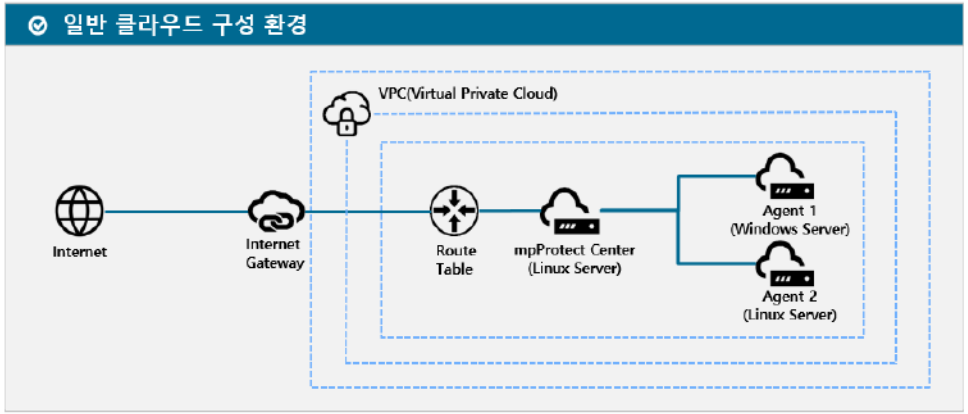
Case Study

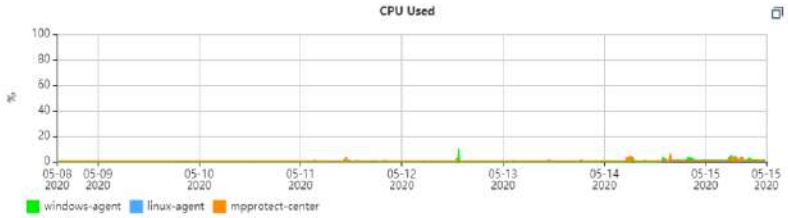
1. MPP for Cloud Service
2. MPP for Edge Computing
3. MPP for Cyber Security Monitoring

클라우드(Public & Private) 환경에 최적화 된 화이트리스트 기반의 프로세스 보안 솔루션

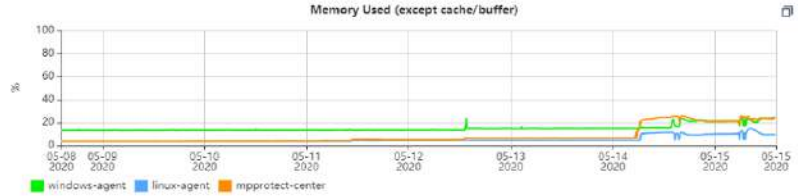
화이트리스트 기반의 프로세스 보안솔루션인 mp(Malicious Process)Protect는 특히 클라우드 환경에 적합한 솔루션으로 기능 및 운용의 안정성에 대한 검증 후 N클라우드 마켓플레이스에 등록되어 있습니다.

클라우드 구성환경에 따라 공용 혹은 전용의 관리서버를 제공하며 초경량 에이전트를 VM에 설치하여 간단한 설정만으로 운영이 가능하며 리소스 점유를 최소화한 초경량 솔루션입니다.

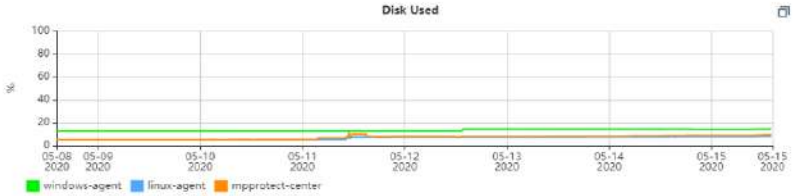




CPU 전체 평균 약 3%이하 사용



레퍼런스 수집 시, 메모리가 증가하였으나 점유율은 양호



DISK 사용량 양호

2. MPP for Edge Computing

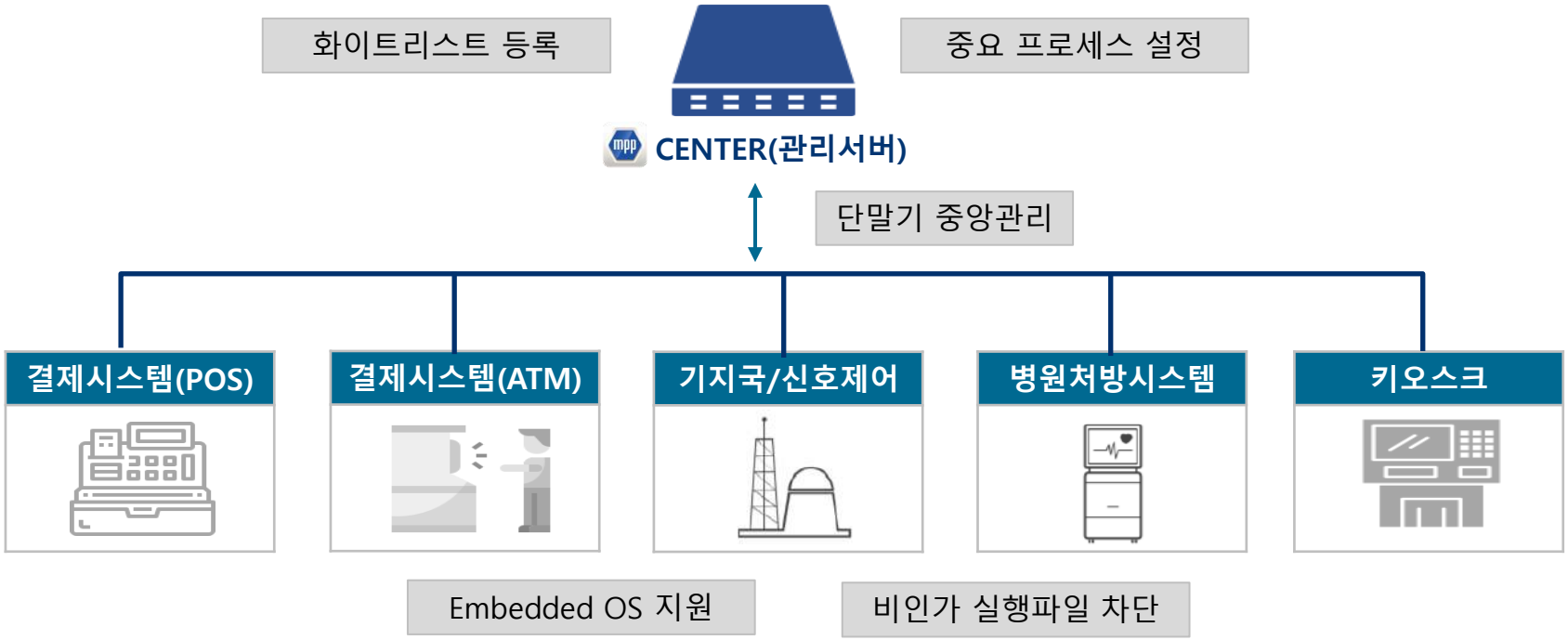
특수한 서비스를 목적으로 하는 Edge Computing에 적합

POS(Point-Of-Sales)를 비롯한 특수목적 시스템은 운영환경과 보안요구사항이 일반적인 시스템과 다르고 처리되는 정보의 기밀성과 무결성을 훼손하는 다양한 종류의 악의적인 공격과 보안 위협에 노출되어 있습니다

또한 대부분 제한된 시스템 자원에서 운용되기 때문에 보안 뿐만 아니라 시스템 가용성이 반드시 고려되어야 합니다.

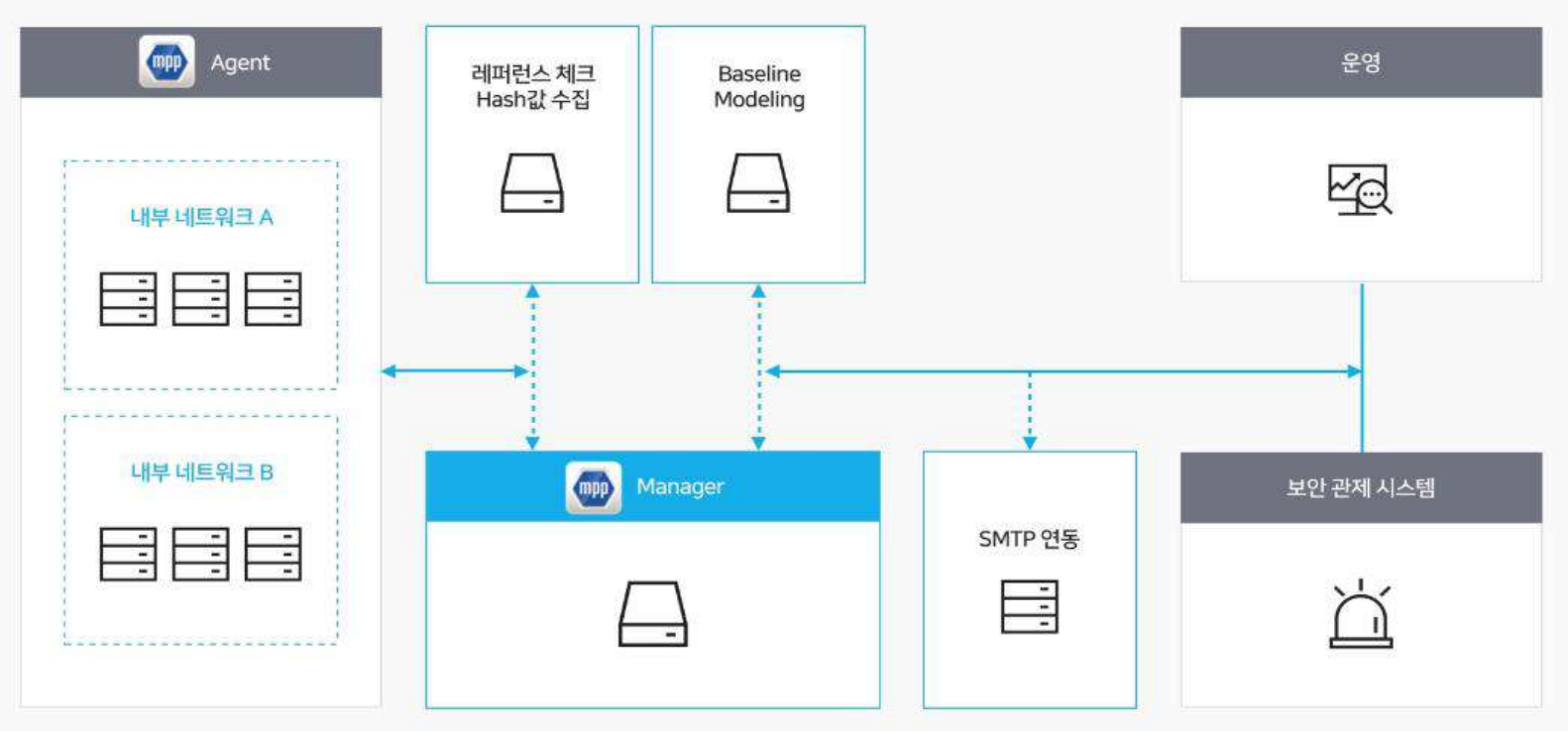
mp(Malicious Process)Protect는 이러한 특수목적 시스템에 최적화 된 화이트리스트 기반의 프로세스 보안솔루션 입니다.

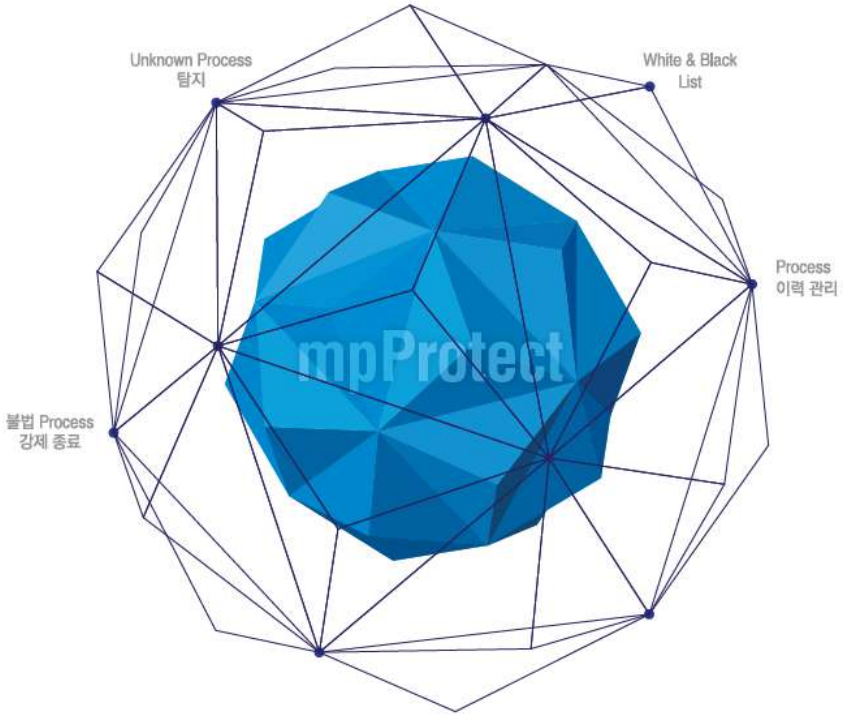
결제시스템(POS), ATM, 키오스크 등과 같은 제한된 시스템 자원에서 리소스 부담을 최소화 하고 특수한 서비스 프로그램 외 프로세스를 차단하여 안정적인 서비스를 보장합니다.



통합보안관제의 프로세스 보안 서비스

mp(Malicious Process)Protect는 레퍼런스 수집기능을 통해 해당 시스템의 화이트리스트 수집 후 지정된 프로세스 외 프로세스 실행 시, 이를 탐지/차단하고 보안관제 시스템에 통지합니다. 또한 중앙집중관리를 통해 다수의 서버를 제어할 수 있으며 장비의 현재상태 및 정보도 확인할 수 있습니다. (리소스, ON/OFF, 서버정보 등)





감사합니다.

(주) 굿데이아이티

- 주소: 서울시 금천구 가산디지털2로 115 대륭테크노타운3차 706호
- TEL: 1544-9293 Fax: 02-6008-1068
- 대표 문의: gdit@gdit.kr
- 영업 문의: sales@gdit.kr
- 기술 문의: tect@gdit.kr