kt cloud

안티랜섬웨어/EDR

Capture

Capture

소닉월과 센티널원의 협업으로 탄생한 EDR/XDR 솔루션으로 리눅스 운영체제에서 알려지지 않은 악성코드 분석과 헌팅을 통해 위협을 예방하고 행위기반의 AI 엔진이 랜섬웨어 및 각종 악성코드로부터 시스템을 보호하는 서버용 보안 솔루션입니다.

서비스 개요

최신 엔드포인트 보호 기능

- 최신 엔드포인트 보호 기능은 엔드포인트가 어디에 있든 최신 위협에 대한 보안 기능을 제공하도록 설계되었습니다.

EDR 기술을 통한 업계 최고의 차세대 백신

- 효과적인 위협 보호 기능을 제공하는 면에서 탁월할 뿐만 아니라 SonicWall 플랫폼과의 시너지 효과를 통해 네트워크 안팎에서 가시성과 보호 기능을 강화할 수 있습니다.

공격 실행 전 차단

- 랜섬웨어, 알려진 악성코드 및 알려지지 않은 악성코드, 메모리 익스플로잇 공격 등으로부터 보호

애플리케이션 취약성에 대한 가시성

- 취약한 애플리케이션, 그 심각도 및 이유 파악

서비스 주요 기능

- 리눅스 운영체제를 탑재한 물리서버 또는 클라우드 서비스를 이용하는 고객이 지능협 위협을 대응
- 차세대 행동 기반의 멀웨어 방어 시스템 (악성코드 실행 되지 전 또는 실행 중 차단/격리)
- 소닉월 CAPTURE ATP 서비스 + 센티널원 차세대 멀웨어 방어 기술
- 다양한 리눅스 운영체제 지원
- 다양한 로그 파일 저장 (/opt/sentinalone/log/)
- 고객사에 적합한 정책 운영 (예외처리 등)
- 평판 시스템 : 센티널원 클라우드를 통한 평판 분석
- 보안 원격 셸 감시
- MITRE Engenuity ATT & CK Evaluation 지원 및 제로데이 공격 방어
- 딥 파일 검사 : 디스크에 저장된 악성 파일을 검사하는 AI 엔진
- 고급 머신 러닝을 이용한 행위기반의 AI 엔진
- 익스플로잇 및 CLI 익스플로잇 등의 파일리스 공격 방어
- 주문형 수동 검사
- 위협에 대한 예방 및 방어에 촛점 : kill, 삭제, 격리
- 서비스 신청시 전용 설치 스크립트 제공 (.sh 파일), 쉽고 빠른 설치

서비스 요금

요금옵션명	단위	요금(VAT별도)	비고
CAPTURE for 리눅스 리눅스 운영체제용	1 (OS별)	57,000 원/월	수량 단위는 리눅스 OS 1개 기준입니다
원격기술지원 기술지원 서비스	1회 (1시간)	200,000 원/회	1회(1시간) 원격지원 서비스 요금입니다 (평일기준 10:00~17:00) 원격지원 도구를 사용한 원격지원 서비스를 제공합니다
방문기술지원 기술지원 서비스	1회	협의 필요	지역과 시간에 따라 방문기술지원비 협의가로 산정해 드립니다.

서비스 문의 | (주)소프트메일 sales@softmail.co.kr | 1661-9331 (보안코드 89)