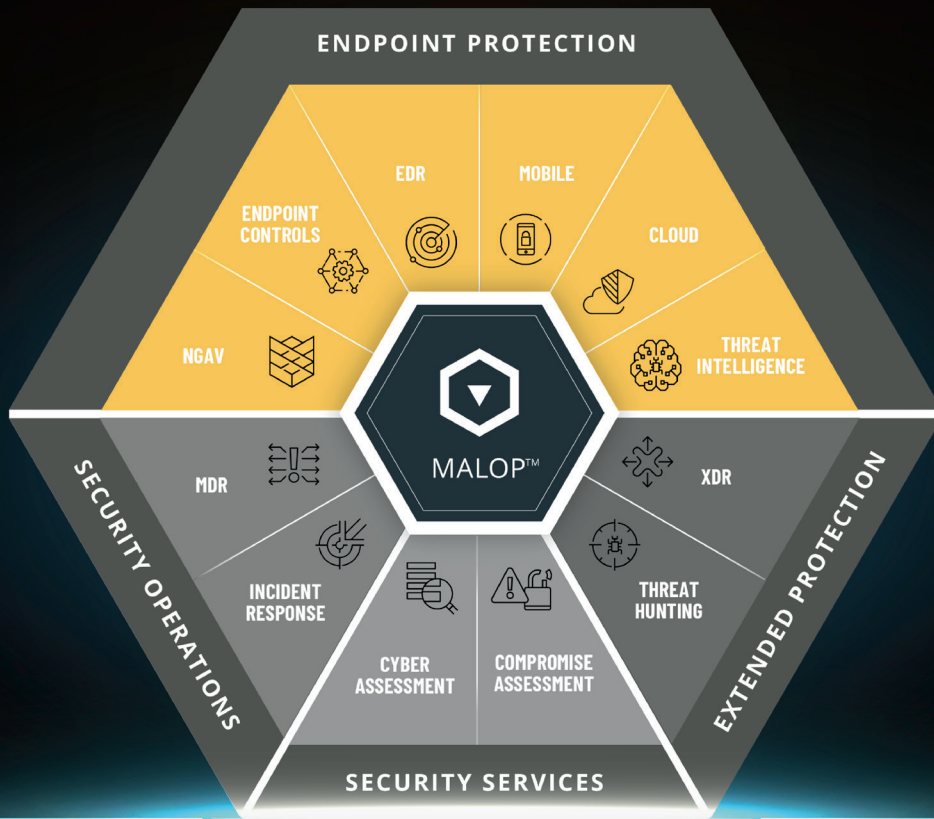


랜섬웨어 대응: 어떻게 준비하고 계신가요?

두산은 글로벌 계열사 모든 엔드 포인트와 서버에 Cybereason의 EDR과 IBM의 MDR를 도입하여 사이버 보안 공격에 대응하고 있습니다.

CYBEREASON DEFENSE PLATFORM



SUPPORTED SYSTEMS



DEPLOYMENT OPTIONS

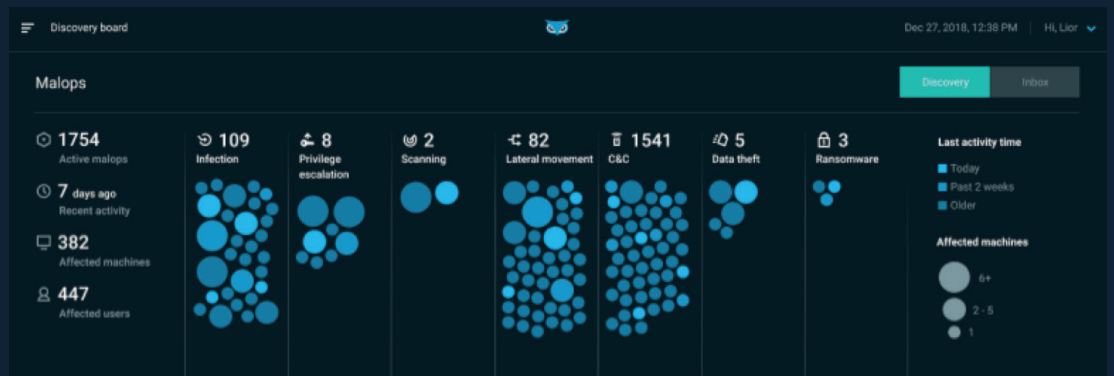


Cybereason의 EDR은 한 눈에 공격 상황을 파악해서 즉각적인 대응을 할 수 있고,



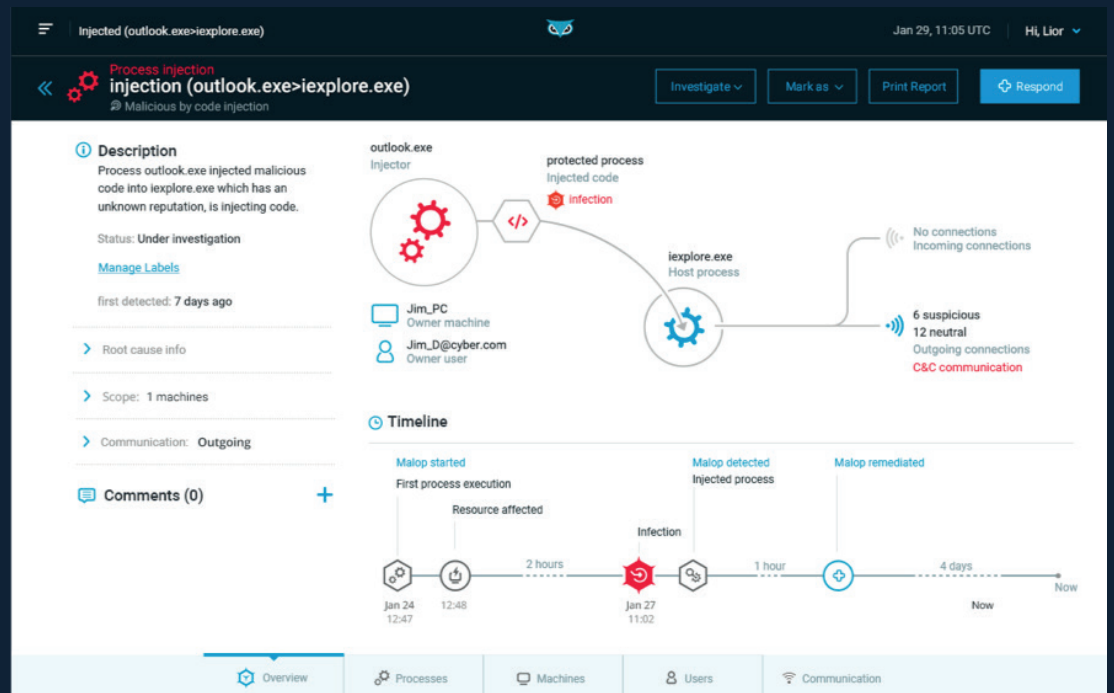
한 눈에 공격 상황에 대한 빠른 인지

탐지된 공격을 유형에 따라 분류하고, 버블 형태로 감염의 규모(크기)와 경과 시간(색)을 표시하여 한눈에 탐지 현황을 파악할 수 있습니다.



실시간으로 공격 현황에 대한 차별화된 가시성 제공

탐지 원인과 단말, 사용자 정보, 통신 내역 등이 가시적으로 변환되어 표시되며 타임라인을 통해 시간 단위의 조사 활동이 가능합니다.

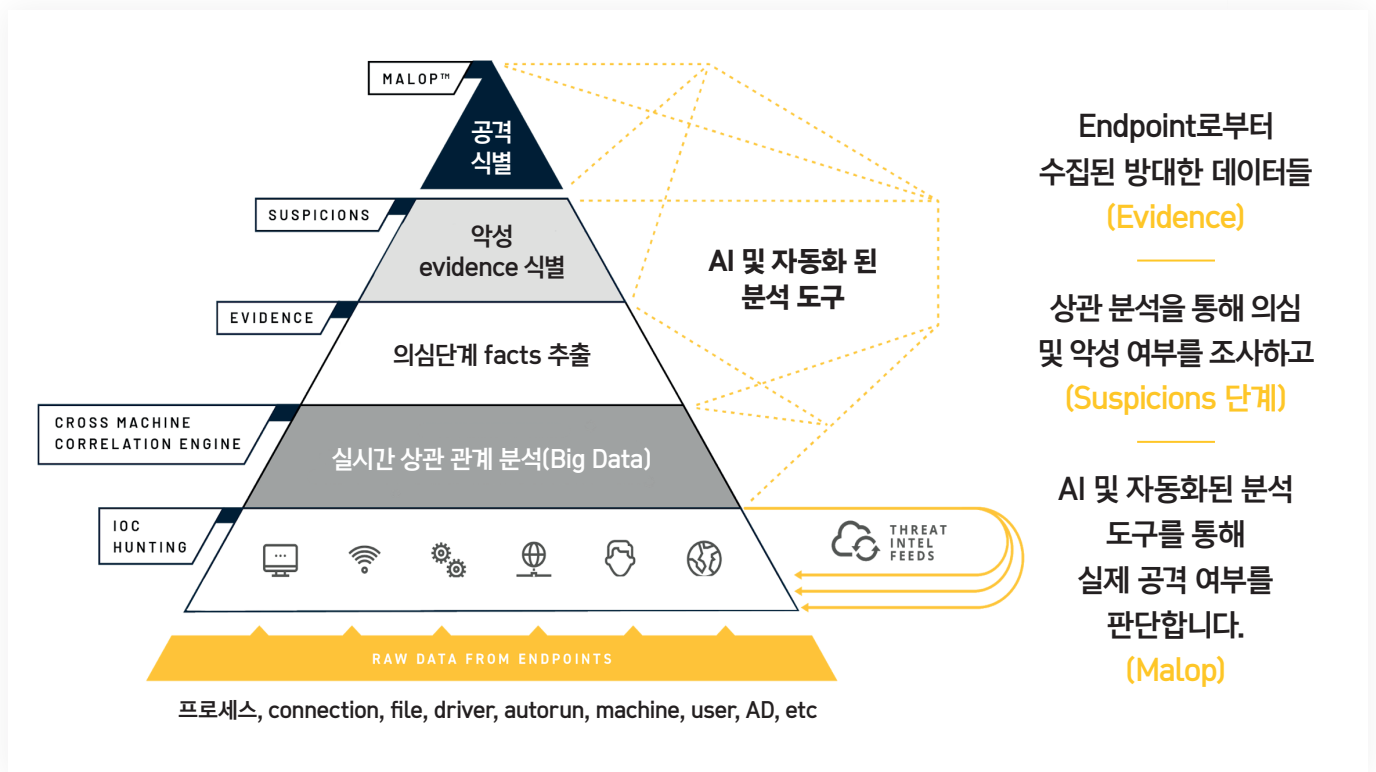




알려지지 않은 위협까지 대응 가능한 Multi-layered 방어를 가능하게 합니다.

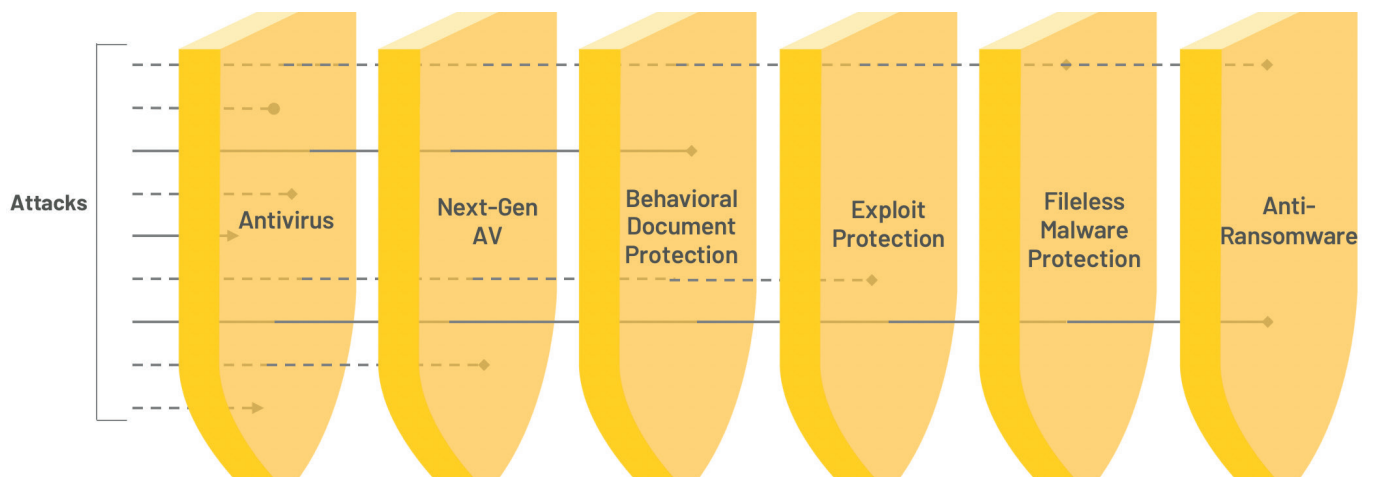


방대한 엔드포인트 데이터 기반 행위 분석으로 공격 식별



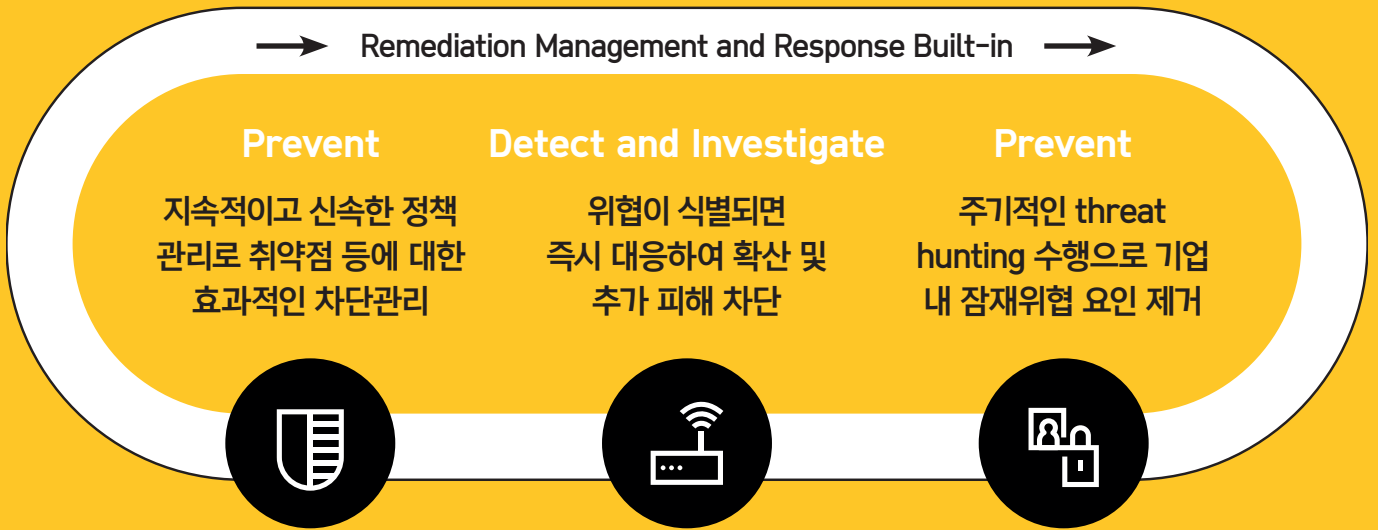
알려지지 않은 위협까지 대응 가능한 Multi-layered 방어력

피해가 발생하기 전에 이상 행위 분석, Machine Learning 기반으로 속임수, Fileless Malware 및 랜섬웨어 공격 등을 방지합니다.



IBM MDR은 AI 기반 자동화와 전문가 분석의 시너지로 강력한 위협방어체계를 제공합니다.

1 전문가 서비스를 통한 24/7 위협 탐지 및 대응



2 글로벌 위협 인텔리전스 + AI 기반 자동화 + 전문가 주도 선제적 위협 추적 및 대응 = 강력한 위협 방어 체계 구축

