DocStory

랜섬웨어 팬더믹 대응 솔루션

Endpoint Data Protection

에스엠테크놀러지(주)

랜섬웨어 피해 현황은?

위험 경보

- 지난해 전 세계 랜섬웨어 공격이 3억463만 건으로 2019년(1억8790만건) 대비 62%증가
- 올해는 6월말까지 이미 지난해 랜섬웨어 공격 건수를 넘어섬
- 다크웹에 공공기관 임직원정보 90%이상 유출되어 이를 통한 피해 증가 예상

2021.05 미국 콜로니얼 파이프라인
- 최대 송유관 업체
- 다크사이드(DarkSide)
- 연료 공급 차질
- 500만달러 지불

2021.05 미국 JBS
- 세계 최대 육가공 업체 브라질 JBS의 미국지사
- 레빌(Revil)
- 공장 일시 중단
- 1100만달러 지불

2021.07 미국 카세야
- IT보안관리 서비스 업체
- 레빌(Revil)
- 고객사 1500여 곳 피해
- 1100만달러 비트코인 지불

랜섬웨어 팬데믹

영국의 「이코노미스트」는 디지털 마피아와 랜섬웨어 위탁 개발 서비스가 횡행하는 전 세계 사이버 세상의 현주소를 「랜섬웨어 팬데믹(pandemic 감염병 대유행)」이라 진단

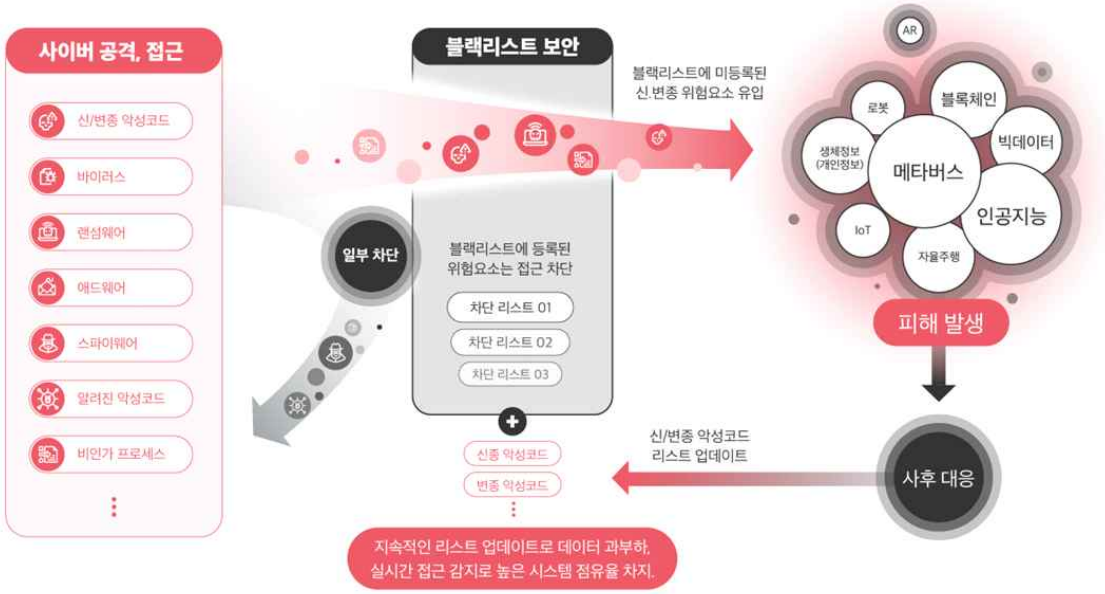
대응 준비 미흡은 공적 제재 대상

- 「국가정보원」은 2021년부터 '정보보안 관리 실태 평가지표'에 보안 위규로 인한 랜섬웨어 피해 발생 시 감점 항목을 신설하여 보안 대책 강구
- 「개인정보보호위원회」는 개인정보 침해행위가 발생할 경우 기업 등 개인정보 처리자에게 '년간 매출액의 최대 3%까지 과징금 부과'할 수 있도록 개인정보보호법 개정안 추진

보안방식의 차이

블랙리스트 보안

- 백신에 주로 사용되는 방식으로 악성코드로 판별된 파일들의 데이터를 악성 DB에 넣어놓고차단하는 방식으로 신종 및 변종 악성코드에 취약함.



행위기반 보안

- 미리 악성행위로 판별된 행위를 악성 DB에 넣어놓고, 행위를 감시하여
  악성 DB에 있는 행위와 비교하여 악성 유무를 판별하는 방식
  대부분의 랜섬웨어 솔루션에서 사용하는 방식으로 암호화하는 행위에 집중되어 있으므로
  암호화 이외의 유출이나 삭제등의 고도화된 랜섬웨어에 취약함.

유출에 대한 대응

- 최근의 랜섬웨어 공격은 초기 암호화방식이 아닌 유출이나 새로운 훼손으로 고도화됨.
  알려진 악성코드라도 악성행위 이전에 데이터 탈취가 선행되기 때문에 암호화 행위를
  탐지하여 차단한다 하더라도 이미 탈취된 주요 데이터에 대한 피해를 막을 수 없음

최선의 방법 '사전차단'

완벽한 사전차단

악성코드의 접근을 사전에 차단하는 방식이 필요함.
특히 알려진 악성코드나 악성행위만 막는것은 하루 수십만개의 신.변종 악성코드를 차단하는 데는 한계가 있음.
독스토리는 화이트리스트 방식의 완전한 사전차단 방식의 보안 솔루션입니다.
화이트리스트 방식은 알려지지 않은 악성코드나 악성행위에 효과적으로 대응할 중요한 수단입니다.

화이트리스트의 최대 취약점 관리 편의성 극복

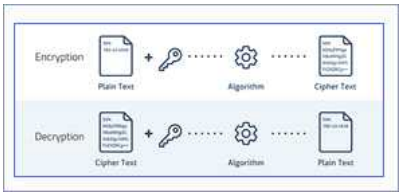
- 불편하고 짜증스러울 수 있는 화이트리스트 보안의 관리 구간을 획기적으로 단축
- 월등한 보안 수준 유지 위한 난제, 관리 포인트 문제를 95%이상 절감

DocStory 주요 기능

- **무결성 확보**
  에이전트와 관리서버의 주요 실행 파일과 운용되고 있는 프로세스 주기적 무결성 검증
  무결성 검증 시 훼손된 파일 자동 복구 및 관리자에게 즉각 통보
  무결성 검증 진행 절차는 국정원 보안 인증 규격 준수

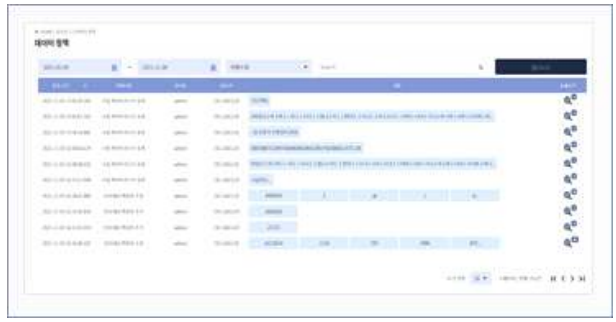
- **가용성 확보**
  파일 변경 권한을 얻기 위한 권한 변경 시도 원천 차단
  주요 실행 파일 삭제 시도 원천 차단
  주요 실행 프로세스 중지 시도 원천 차단
  세션 탈취 시도 차단되고, 일정 시간 정지된 경우 세션 자동 종료

- **기밀성 확보**
  로그인 시 패스워드 생성 규칙을 준수하고, 사용자 계정 정보 암호화 저장
  관리서버와 에이전트 운용 중 발생 및 전달되는 주요 데이터 암호화 저장 및 암호 통신
  주요 파일 숨겨진 상태로 보관되고 사용되는 암호키는 국정원 보안 인증 규격 준수



관리 모듈 주요 기능

- 대시보드를 통한 직관적인 정보 제공으로 상황 발생 시 즉각적인 대응 가능
- 다양한 설정을 통한 정책 설정과 정책 변경 시 즉각 에이전트 반영
- 다양한 상황에 따른 감사 로그 및 갈사로그 다운로드 API제공



구축 실적

엔터프라이즈

- 대기업군

- 중견기업군

- 방송 및 금융

- 기타

공공

- 자자체

구미시청	상주시청	양양군청	속초시청	양구군청	대구시청
영천시청	영암군청	군위군청	고성군청	경북도청	의왕시청
인제군청	목포시청	원주시청	평창군청	춘천시청	김제시청
안동시청	강릉시청	영월군청	강원도청		

- 기관 및 중앙부처

- 기타