화이트 리스트 기반의 전용 보안 솔루션

iMON LOPE 제품 소개

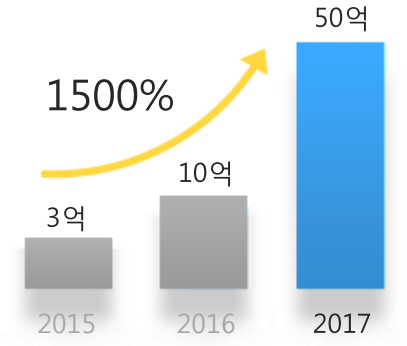
문의처: software@gytni.com

01_제안 배경

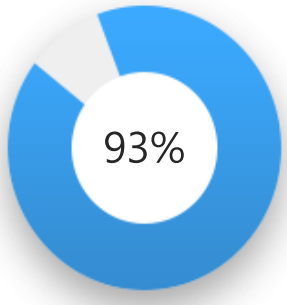
랜섬웨어(Ransomware)

사내 PC에 침투하여 기업의 중요 파일을 암호화시키고 막대한 복구비용으로 금전 탈취
서비스형 랜섬웨어 모델 출현과 윈도우 취약점, 피싱 이메일 등의 **지능화된 수법으로 랜섬웨어 공격 증가**

랜섬웨어 피해현황



[2015~2017 랜섬웨어 피해 현황]



백신 사용 중 감염

[2016년 랜섬웨어 감염 기업 중 백신 설치 비율]

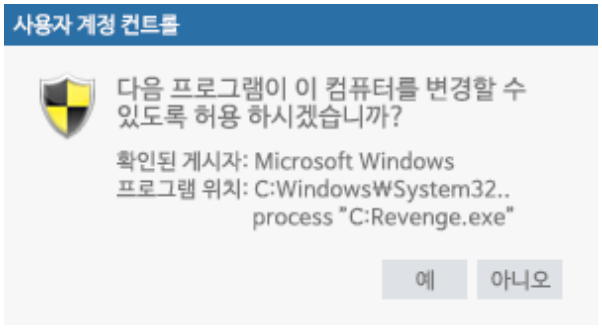
01_제안 배경

랜섬웨어 공격을 대응하기 위한 솔루션 (권한통제, 백업) 이 널리 사용되고 있는 시점

하지만, 기존 솔루션의 사각지대는?

권한 통제 솔루션

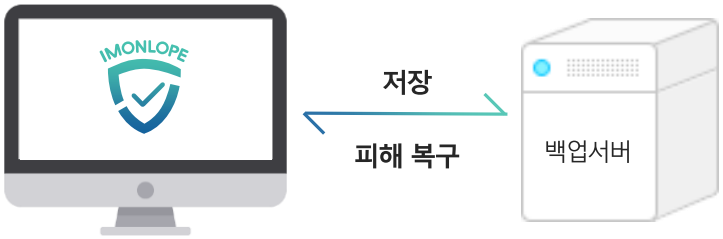
최근 랜섬웨어는 일반 사용자 권한으로도
실행하여 권한 통제만으로는 취약점 존재



※ 관리자 권한이 필요한 드라이브의 파일을
암호화하기 위해 사용자 계정을 우회하여
윈도우 기본 백신인 윈도우 디펜더의 악성코드
패턴을 업데이트 할 수 없으니 이를 복원해야
된다는 가짜 메시지 창을 띄워 사용자의 클릭을
유도하여 권한을 상승함

백업 솔루션

DRM (문서암호화)을 응용한 변조
악성코드 발생 시 백업 파일이 손상 가능성



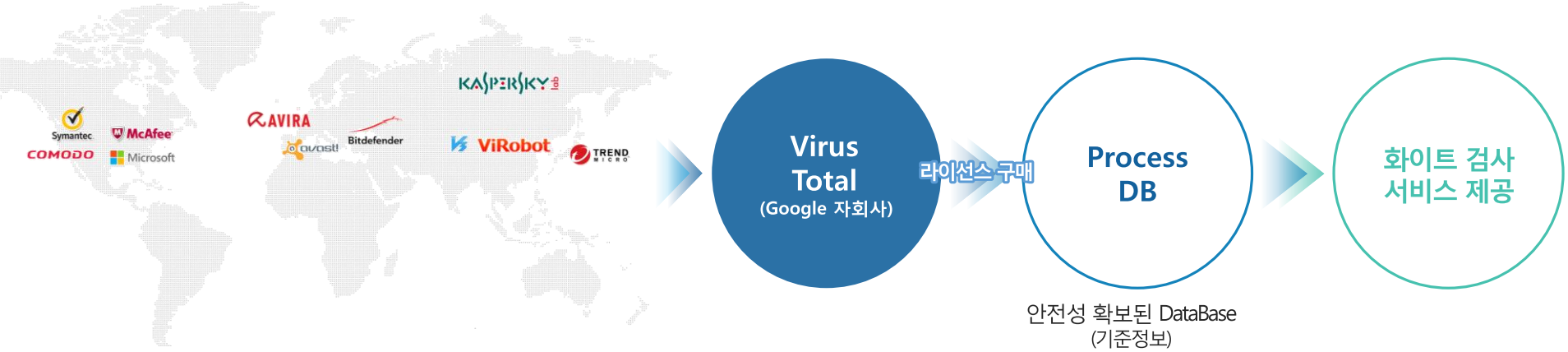
※ DRM 응용 악성코드 출현 시
'저장' 단계에 암호화 시킨 후 저장하여,
피해 복구 암호화된 파일을 읽을 수 없음

02_화이트 통제 솔루션 도입 필요성

기존 백신의 한계성

기존 백신은 블랙리스트 방식으로 등록된 악성코드 패턴을 통해 안전 유무를 판단한 후 통제하기 때문에
새로운 신/변종 악성코드는 사전 대응이 취약함

하지만, iMON LOPE (화이트 통제 솔루션)은 **전 세계 56개 백신 검사 후 "안전" 프로그램만 실행 (exe, dll 외 Script 파일)**



03_특장점 '화이트 통제 자동화 운영'

화이트 통제는 업무 로드 증가 ?

수동으로 개별 등록해야 하는 화이트리스트 방식을 사용할 경우 관리자 업무 증가

화이트 통제의 자동화 운영 방법

VirusTotal 기준으로 **검사한 '안전' 파일은 별도 관리자의 등록 없이 자동으로 실행 가능**

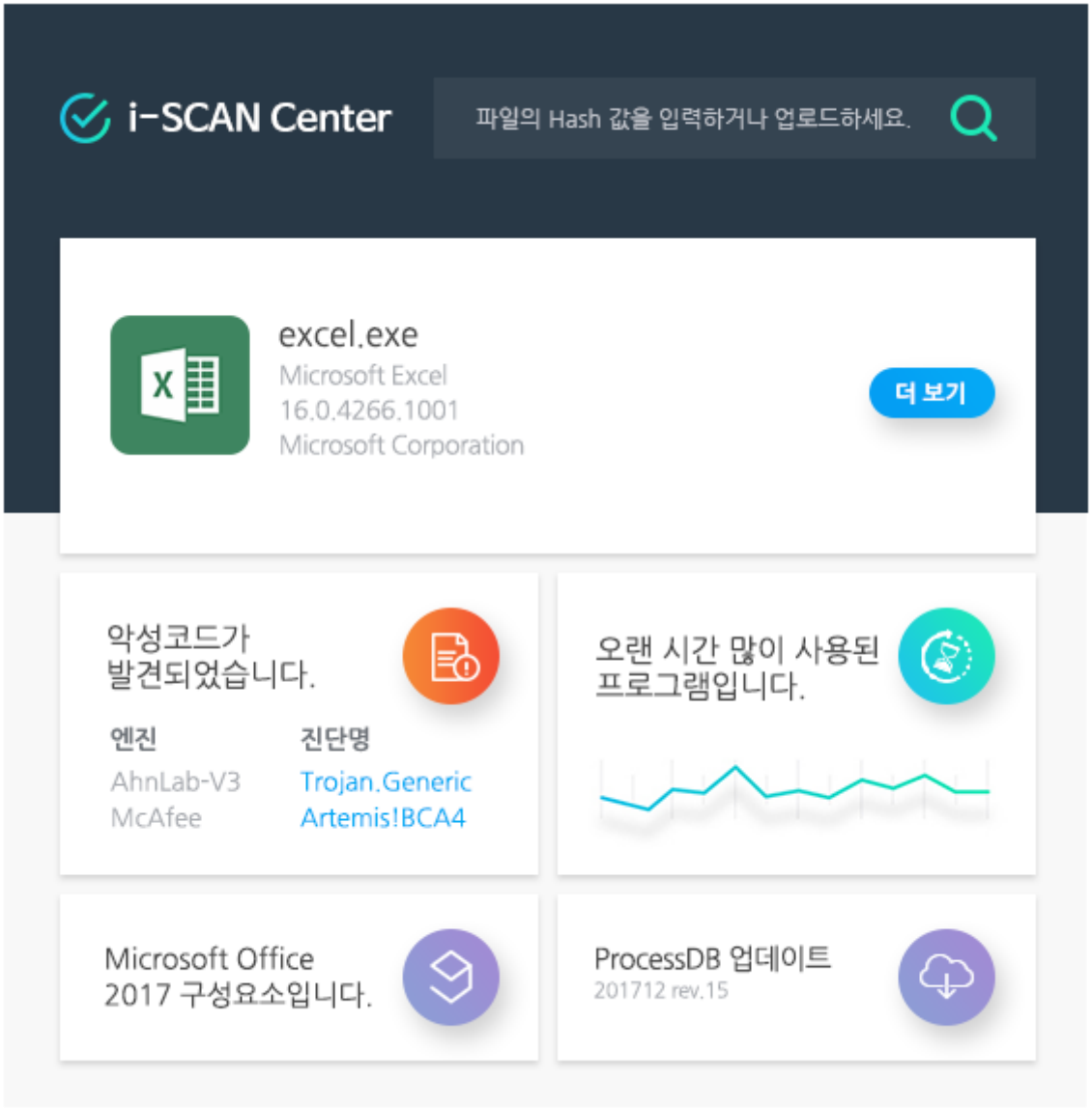
안전한 파일로 검증된 MS · Adobe · Autocad 등 전 세계에서 널리 사용되는 저작권사의 모든 프로그램은 자동으로 실행되며 또한 국내의 모든 상용 프로그램 (한글, 백신, 보안 프로그램 등)도 **자동 실행 가능**

해당 저작권사의 업데이트 · 패치 파일도 통제 없이 실행

수동 등록이 필요한 경우는 언제?

고객사에서 SI로 **개발한 프로그램 등은** '수동 등록' 이 필요하지만 **1회 간단한 Rule 등록**으로 운영이 가능하여 **관리자의 업무 증가 방지**

03_특장점 'i-SCAN Center 운영'



[주요 기능]

▶ 고객사 별 기준 P.DB 업데이트 관리

▶ 프로세스 조회 기능
1) 저작권 조회
2) 바이러스/악성코드 감염 여부
3) 프로세스 별 사용 통계 정보
4) 제품구성 정보

▶ 업데이트 방법
1) 자동 업데이트: 변경 시 실시간
2) 수동 업데이트: 파일 업로드

03_특장점 “56개 백신 검사로 진단 수준 향상”

랜섬웨어 피해 글로벌화

방콕 은행 피해와 같이 해킹 피해는 Global 지역으로 확대되고, 가상화폐 요구 및 가치가 계속 증가하는 추세에 따라 더욱 신종/변종 악성코드 출현 가능성 증가

한 개의 백신 검사보다 56개 백신 검사 결과가 더욱 정밀해짐

피해지역이 전 세계에서 발생됨에 따라서 각 국가의 백신 엔진이 갖고 있는 “악성코드 패턴 DB”가 정밀해짐
따라서, **한 개의 백신 엔진으로 검사할 때 보다, 더욱 정밀하게 백신 검사 수행**

03_특장점 “에이전트 설치 후 PC 영향도 분석”

PC 성능

- PC 리소스: 기존 백신 대비 경량화 ▶ CPU 점유는 1%, 메모리 점유는 3MB
- PC 성능: 영향 없음 ▶ 정밀검사 수행 (Disk Full 스캔) 시 CPU 5~10 % 증가, 필요시 에이전트 설치 후 1회만 수행

트래픽 증가

- i-MON LOPE 서버와 PC 에이전트 통신 관련 트래픽 변화 없음
- LOPE 서버의 화이트 Rule DB를 생성 후 PC 에이전트로 전달 시 트래픽 영향 없음
  ▷ 이유: 화이트 Rule 정보만 전달되어 2KB 이하의 트래픽 발생

에이전트 혹은 서버 장애 영향도

- 에이전트 장애 발생 시 사용자 PC 사용에는 영향을 주지 않아 에이전트 설치 이전 상태와 동일
- LOPE 서버 장애 시 PC 간섭은 없으며, 이전 수신 받은 정책 값으로 화이트 통제 정책 운영