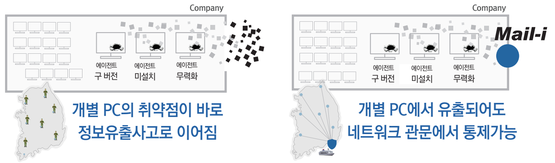
정규군대로 지켜야 할 전쟁에 민방위를 출전시킬 수는 없습니다

〈에이전트방식으로 네트워크를 보안〉할 경우 VS 〈네트워크DLP〉로 네트워크를 보안할 경우



개별 PC의 취약점이 바로 정보유출사고로 이어짐

개별 PC에서 유출되어도 네트워크 관문에서 통제가능

네트워크는 〈네트워크DLP〉로 지켜야 하는 3대 이유

이유1 〈에이전트방식으로 네트워크를 보안〉하는 것은 구조적으로 불가능하기에

설치 불가	MAC, 리눅스, 안드로이드 , IOS기반 PC에는 설치불가능 에이전트 미설치 PC에서 네트워크로 유출하면 보안불가	변화 불가	네트워크 변화속도를 에이전트로 따라잡는 것은 불가능 메신저 유출패턴이 변했다 해서 PC마다 에이전트 업데이트하고 나니 개인정보는 이미 유출된 후	통합 불가	로그통합 불가로 종합적 이상징후분석불가 로그가 개별PC에 쌓이므로 통합 불가

이유2 Gartner로 대변되는 글로벌스탠더드는 〈에이전트방식으로 네트워크를 보안〉하는 것을 DLP로 인정조차 않습니다

Gartner의 DLP 자격 기준

Ability to detect sensitive content in network traffic without the need for an endpoint agent

Inclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

The following vendor attributes are required to qualify for inclusion:

- $5 million in annual revenue specifically for their enterprise DLP product(s).
- Ability to detect sensitive content in network traffic without the need for an endpoint agent.
- Ability to detect sensitive content in either discovery scans (data at rest) or endpoint (data in use).

발췌: Gartner 'Magic Quadrant for Enterprise Data Loss Prevention' 2016.1.28

이유3 〈에이전트방식으로 네트워크를 보안〉하다가 〈에이전트 무력화〉로 유출사고 발생시 귀사는 유죄입니다

서울중앙지법 판결문 2016.01.22	
에이전트 무력화 방법 ①②③	① 〈에이전트방식 보안프로그램〉설치 PC에서...리눅스OS가 설치된 PC로 고객정보를 전송하여...유출
	② 외장하드 허용...〈에이전트방식 보안프로그램〉의 기능유지되지 못한 PC에 고객정보 전송하여...유출
	③ 하드디스크 포맷, 〈에이전트방식 보안프로그램〉을 삭제
이후 정보유출방법	FTP or Telnet을 이용....고객정보를 K의 PC로 전송...원격조정하는 방법으로...
기업측 과실인정 손해배상 판결함	PC에서...〈에이전트방식 보안프로그램〉이 정상유지되도록 관리하지 못하여
	외장HDD 허용과정에서...〈에이전트방식 보안프로그램〉의 기능이 정상유지되도록 관리하지 못하여
	PC 중 1대가 계속하여 〈에이전트방식 보안프로그램〉이 설치되지 않은 상태에서...방치하는 결과를 초래
	〈에이전트방식 보안프로그램〉설치를 지시하였을 뿐 ... 반입PC에... 설치,유지 여부를 확인한 적 없어...

판결문 원문상에는 〈보안프로그램〉으로 되어있으며 이해를 돕기 위하여 〈에이전트방식 보안프로그램〉으로 표기하였습니다

유죄? 무죄? 선택에 달려있습니다

위 사건은 USB로 유출된 사건으로 〈엔드포인트에이전트방식 보안〉이 적합한 보안방식인 경우입니다.
그럼에도 불구하고 에이전트 무력화를 막지못했다는 이유로 유죄판결이 나왔습니다.
만일 귀사가 네트워크를 〈엔드포인트에이전트방식〉으로 보안했다가 유출사고가 난다면
처벌이 훨씬 더 강력할 것입니다. 네트워크에 적합한 보안방식은 네트워크DLP이기때문입니다.

Mail-i 가 있어야만 준수할 수 있는 법규정

금융기관에 적용 금감원 〈기술적 물리적 관리적 보안대책〉 & 〈금융기관검사 및 제재에 대한 규정 시행세칙〉

조항	법규정
1조 (정근동지)	〈개인신용정보〉가 홈페이지, P2P, 공유설정 등 (네트워크로) 공개되지 않도록 설정
5조 (출력복사시 보호조치)	② 〈개인신용정보〉를 이메일 등 외부전송시 사전승인
	③ ②항 준수에 필요한 내부시스템구축

설정하지 않았을 경우

미준수 정도	미준수시 처벌	
	금융기관	임직원
중대	업무정지	정직 이상
보통	기관경고	감봉
경미	기관주의	견책

설정하지 않아 개인정보가 유출되었을 경우

유출건수	직원처벌
50건 이상	정직 이상
5건 이상	감봉
1건 이상	견책

Mail-i 법규준수기능

- 개인정보가 네트워크로 공개되지 않도록 차단, 경보, 기록
- 개인정보 외부전송시 사전승인

금융기관에 적용 〈금융회사의 정보통신수단 등 전산장비 이용관련 내부통제 모범규준〉 준수

금융기관에서 이메일/웹메일로 고객정보유출, 악성루머 유포

→ 금감원이 금융회사 스스로 **내부정보통신수단** 을 통제하도록 모범규준 제시

→ 전자우편, 메신저 등 정보통신망을 통한 정보 송수신장치를 의미(총칙 2조 정의)

조항	세부내용	귀사의 체크리스트	***Mail-i*** 법규준수기능
5조 (업무용 정보통신수단 지정)	① 이메일, 메신저등 〈업무용 정보통신수단〉지정 (로그기록) ② 〈비업무 정보통신수단〉은 차단	• 사내에서 사용중인 정보통신수단은 무엇인가? • 업무용을 지정한 후 로그기록하는가? • 비업무용 수단을 정확히 차단하고 있는가?	• [업무용정보통신수단 로그기록 • [비업무정보통신수단 차단
7조 (업무용 정보통신수단 이용시 금지행위)	영업비밀, 고객신용정보, 시장루머, 타인권리침해, 범죄성네트워, 스팸메일, 공고문구 발송금지	• 〈업무용 정보통신수단〉으로 전송되는 정보를 컨텐트분석하고있는가?	• 컨텐트분석을 통한 개인정보, 기밀정보, 위법내용통제 • 제목, 본문, 첨부파일 내 내용까지 모두 분석 • 압축파일 분석 및 DRM연동 분석
8조 (로그기록 보관)	① 〈업무용 정보통신수단〉 로그기록 3년 이상 보관 의무화 ② 다음 정보 로그기록에 포함: 송수신일자, 시각, IP, ID, 내용/첨부파일, 송수신 상대방정보	• 〈업무용 정보통신수단〉으로 전송되는 정보를 규정대로 로그기록보관하고 있는가?	• 로그기록 자동보관 • 송수신일자, IP, 발신자ID/수신자ID, 제목, 본문,첨부파일/첨부보관 • 빅데이터검색으로 3년치 메일기록을 3초내 검색

모든 공공기관, 기업, 단체에 적용 〈개인정보보호법〉

조항	법규정	귀사의 체크리스트	***Mail-i*** 법규준수기능
34조 1항 (유출통지)	유출시 유출내역(개인정보항목, 시점, 유출경위)을 정보주체에게 통지	• 개인정보 외부전송내역을 기록하고 있는가? • 주기적검색을 통하여 유출발생여부를 파악할수있는가?	• 개인정보 외부전송내역 기록 (개인정보항목, 시점, 송수신자, 유출채널 등)
고시 「개인정보의 안전성 확보조치 기준」 5조	개인정보가 홈페이지, P2P, 공유설정 등 네트워크를 통하여 유출되지 않도록 조치	• 네트워크로 개인정보 외부전송시 기록/경보/차단하는가? • 주기적검색을 통하여 유출발생여부를 파악할수있는가?	• 웹메일, 메신저, P2P, 웹하드를 통한 유출내역 기록 (국내 상위 웹하드, P2P 모두 커버)

정보통신서비스 사업자에 적용 〈정보통신망법〉

구분	개정 내용	귀사의 체크리스트	***Mail-i*** 법규준수기능
27조의3 (누출 통지신고)	누출시 유출내역을 정보주체에게 통지 및 방통위에 신고 (개인정보항목, 시점, 유출경위 등)	• 개인정보 외부전송내역을 기록하고 있는가? • 주기적검색을 통하여 유출발생여부를 파악할수있는가?	• 개인정보 외부전송내역 기록 (개인정보항목, 시점, 송수신자, 유출채널 등)
고시 「개인정보의 기술적 관리적 보호조치」 4조	개인정보가 홈페이지, P2P, 공유설정 등 네트워크를 통하여 유출되지 않도록 조치	• 네트워크로 개인정보 외부전송시 기록/경보/차단하는가? • 주기적검색을 통하여 유출발생여부를 파악할수있는가?	• 웹메일, 메신저, P2P, 웹하드를 통한 유출내역 기록 (국내 상위 웹하드, P2P 모두 커버)

미국영토에서 사업하는 사업자 대상 이디스커버리(디지털 증거개시제도) 준수

이디스커버리란? 소송관련자의 메일/메신저 등 정보통신수단의 송수신로그(첨부파일 포함) 3년치를 소송개시 180일 이내에 법원에 제출하라는 규정
미제출시 고의적 증거인멸로 간주, 소송에서 패소

▶ 미래창조과학부지정 정보보안 컨설팅전문업체 ▶ 행정자치부지정 개인정보 영향평가기관 ▶ 조달청 조달등록기업
▶ 신용평가등급 A, 재무안정성 상위 1% ▶ 창업 이래 무차입경영, 13년 연속 흑자기업
▶ **고객정보보호, DLP분야 40건이상 기술특허보유 및 출원**

SOMANSA

서울특별시 영등포구 영신로 220 KnK디지털타워 9층
TEL 02)2636-8300 FAX 02)2636-8181 www.somansa.com

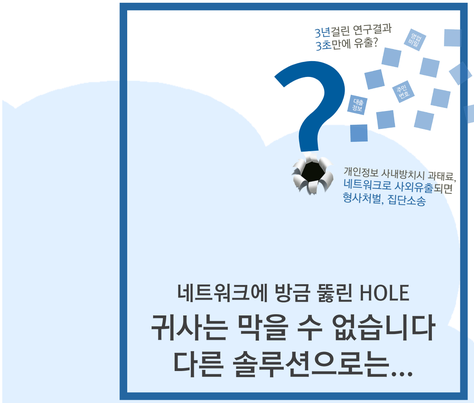
개정 및 2쇄부 인쇄: 2016.5

시장1위, Network DLP 솔루션

Mail-i

V 8.0 HyBoost

아시아 최초. DLP 분야 Gartner Magic Quadrant 등재



Network DLP(Data Loss Prevention) 솔루션이란?
세계적 IT리서치 전문기관인 Gartner사가 명명한 사내정보 유출방지솔루션을 의미합니다.
Gartner사는 DLP를 Discovery, Endpoint, Network 세 영역으로 구분하였으며
그 중 Network DLP는 **이메일, 메신저, P2P, FTP, HTTP, SNS** 등 다양한 네트워크상의 유출채널을 통한 내부정보유출방지솔루션을 지칭합니다.

SOMANSA

DLP의 Global First Mover 소만사 19년간 세계 최초의 기록

2016 Gartner Magic Quadrant 등재
2015 리눅스 플랫폼 개발
2014 암호화웹(HTTPS) DLP 개발 (Mail-i For WebDLP)
2013 빅데이터검색엔진 개발
2010 DLP 패킷처리전문엔진 개발
2008 웹포트(80포트) 우회접속 차단
2005 P2P, 웹하드, 우회접속 분석
2002 메신저 분석
1998 SMTP 웹메일 분석
1997 명함에 이메일주소조차 없던 시대, 네트워크DLP로 창립

세상에 없던 유출채널이 최초로 출몰하는 곳, 한국의 네트워크입니다
그래서 소만사의 역사는 세계 최초의 기록일 수 밖에 없습니다

네트워크DLP는 한국최강이 세계 최강입니다

2,000여 고객사에서 선택한 1위 제품 (시장점유율 65%)

기업 LG전자(글로벌 4대 데이터센터), 삼성, 현대기아차, LG이노텍, LG디스플레이, GS칼텍스, GS건설, LS전선, POSCO, SK텔레콤, SK M&C, SK네트웍스, CJ제일제당, 롯데홈쇼핑, 롯데알심유료, 두산중공업 등

금융 국민은행, 신한은행, 우리은행, 하나은행, NH농협, IBK기업은행, KDB산업은행, 부산은행, 광주은행, 대구은행, 경남은행, 대한생명, 교보생명, 현대증권, 대신증권, 한화증권, 동부화재, BC카드, 롯데카드 등

공공 우정사업본부, 해군본부, 법무부, 경기도청, 국방과학연구소, 방위사업청, 해양경찰청, 한국수자원공사, 한국전력기술, 한국수력원자력, 근로복지공단, 국민연금관리공단, 한국고용정보원, 서울의료원 등

복미 수출 [미 국] JOHNS HOPKINS HOSPITAL, CENTER BANK, TELOS [멕시코] 중앙정부 & 주정부, OXXO 등

미국 연방정부인증 GSA 인증 획득제품

아시아 최초. DLP 분야 Gartner Magic Quadrant 등재

Gartner 'Magic Quadrant for Enterprise Data Loss Prevention' 보고서 중 소만사 평가부분, 2016.1.28

Gartner가 말하는 소만사의 강점

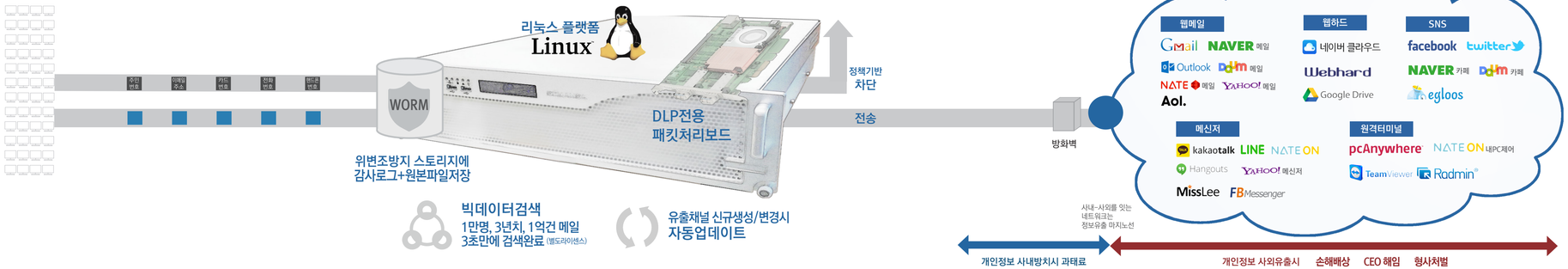
1. 신규등장 유출채널에 강함
Amazon S3, Box, Dropbox, MS OneDrive, MS Office 365, Salesforce and Google Drive 내 민감정보검출

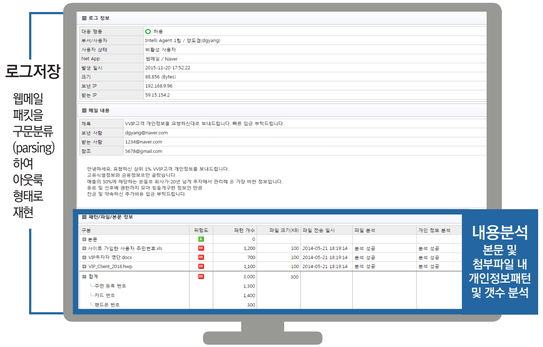
2. 유출채널 신규변경시 업데이트 프로세스 강함
패치, 업데이트 강은 서비스계계의 경우 고객으로부터 아주 긍정적인 피드백

3. 컴플라이언스 충족기능 강함
정책 템플릿 및 결재 기능 등을 통해 이태 지역 주요 법적 컴플라이언스 충족

4. 폭넓은 커버리지
CRM 및 ERP Application에 대한 Discover DLP 지원, 다양한 데이터 타입에 대한 폭넓은 지원 커버리지 보유

네트워크DLP는 큰 회사가 아니라 빠른 회사가 세계 최강입니다





최강의 어플라이언스

성능 최강 세계최초 DLP전용 패킷처리보드 탑재

소만사 자체개발 DLP전용 패킷처리보드 탑재	SW버전 대비 3~5배 패킷처리성능 향상	Full 1G 대용량 트래픽에도 패킷손실 없음

위변조방지 스토리지 별도의 디바이스 구매없이 로그위변조방지저장

리눅스 버전으로 CC인증 획득 MS CAL(Client Access License) 비용부담으로부터 해방

기존문제점

- WORM 스토리지 추가구입 가격 1 TeraByte 당 = 수천만원
- CD 및 DVD구매비용 및 교체시간, 느린 검색으로 인한 업무효율 저하

Benefit 추가비용없이 로그위변조방지구현 업무효율 상승으로 인건비절감

외산솔루션 대비 유출채널 커버리지 3배

웹메일 최강 네이버/다음메일 분석

보낸사람, 받는사람, 참조인, 본문, 첨부파일 등의 메타정보를 정확하게 분류(Parsing)해서 저장	아웃룩메일과 동일한 형태로 제목, 본문, 첨부파일을 재현	ActiveX로 첨부한 대용량첨부파일 (10MB 이상) 전송차단

Mail-i의 네이버메일 로깅

VS

외산제품의 네이버메일 로깅

메신저 최강 메신저 20여종 보안

모바일 메신저 (PC버전 포함) 차단 — kakaotalk LINE

네이트온 메신저 6대 전송방식 모두 보안 — Mail-i 6대 유출방식 모두 보안 VS 외산제품 일반포트 전송만 보안

일반포트 평문	SOCK프록시 평문
일반포트 암호화	SOCK프록시 암호화
	웹프록시 평문만

주요 금융메신저 모두 보안 — Mail-i 주요 금융메신저 모두 보안 VS 외산제품 모두 불가능 MissLee FBMessenger X

웹하드 최강 4대 전송방식 모두 보안

Mail-i 4대 전송방식 모두 보안 VS 외산제품 HTTP방식만 보안가능

외주개발자 & 해커의 주요 유출통로인 **Telnet, FTP 분석능력 최강**

Telnet — 사용자의 Telnet 화면을 CCTV처럼 저장 동영상 Playback

FTP — (2011년 정보통신사) 법원 판결문에서 FTP 허용을 과실로 명시

이외 유출채널 차단

(HTTP, SOCKS4/5 등) 프록시
(E-donkey, Filegurl계열 등) P2P, 공유폴더
(SSH, Xwindows 등) 원격터미널
(Real/HTTP Tunnel, Sconnect 등) 터널링 차단

최강의 검색

빅데이터검색

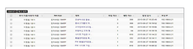
1만명, 3년치, 1억건 데이터를 3초만에 검색완료

기능		소만사	외산제품
검색 속도	3년치 이메일 검색시간	3초 ~10초면 완료	X
	기존대비 개선정도	100배 ~ 1,000배 속도개선	
동시 검색 수준	키워드 수	다수 (1개 검색시간과 여러개 검색시간이 동일)	
	보안담당자 수	수십명 이상이 동시검색가능	

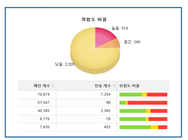
이상징후탐지

주민번호 100건 이상 외부전송자를 신속하게 검색

1. 주민번호 과다전송자 리스트 확인



2. 특정 전송자/를 선택, A의 외부전송리스트 확인 (첨부파일, 개인정보패턴/갯수, 발송시간/대상 확인)

3. 실제 유출정보 확인

부서별, 개인별 위험도 리포팅