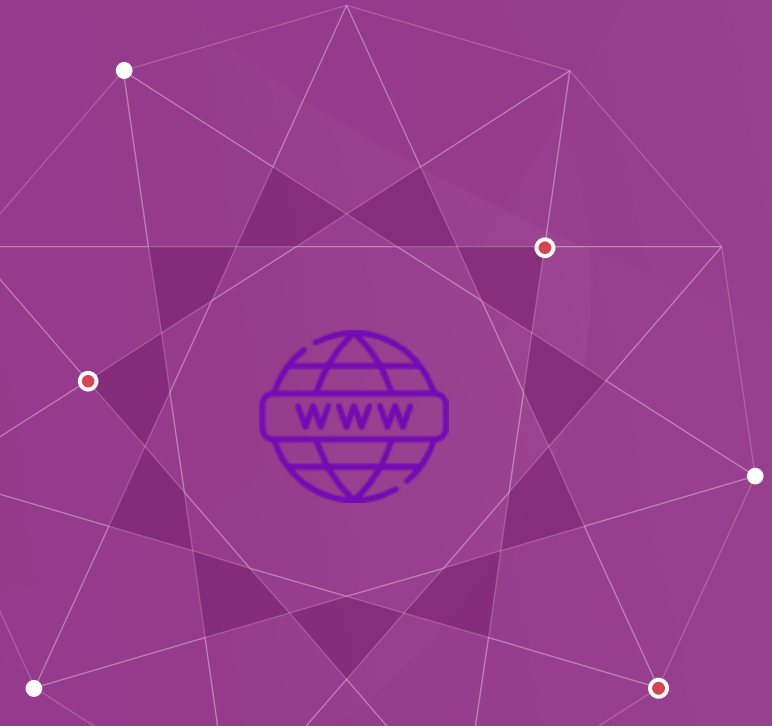
MailGuard v2

비인가웹메일관리시스템

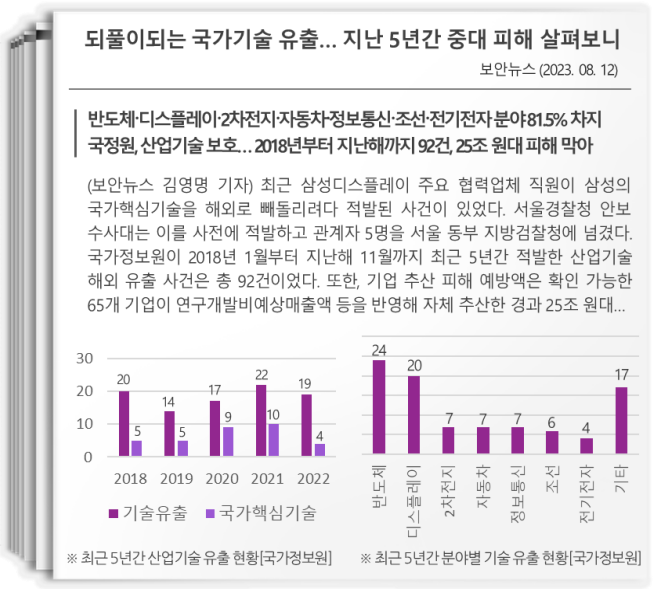


RealSecu
Security System

내부 정보 유출사고의 주 원인

전·현직 임직원의 불법 행위와 부주의

※ 출처 : 국가정보원 산업기밀보호센터



되풀이되는 국가기술 유출… 지난 5년간 중대 피해 살펴보니

보안뉴스 (2023. 08. 12)

반도체·디스플레이·2차전지·자동차·정보통신·조선·전기전자 분야 81.5% 차지
국정원, 산업기술 보호… 2018년부터 지난해까지 92건, 25조 원대 피해 막아

(보안뉴스 김영명 기자) 최근 삼성디스플레이 주요 협력업체 직원이 삼성의 국가핵심기술을 해외로 빼돌리려다 적발된 사건이 있었다. 서울경찰청 안보수사대는 이를 사전에 적발하고 관계자 5명을 서울 동부 지방검찰청에 넘겼다. 국가정보원이 2018년 1월부터 지난해 11월까지 최근 5년간 적발한 산업기술 해외 유출 사건은 총 92건이었다. 또한, 기업 추산 피해 예방액은 확인 가능한 65개 기업이 연구개발비예상매출액 등을 반영해 자체 추산한 경과 25조 원대…

※ 최근 5년간 산업기술 유출 현황[국가정보원]

※ 최근 5년간 분야별 기술 유출 현황[국가정보원]

웹메일 차단의 한계

2017	2018	2019	2020	2021	2022
특수비행선박 설계도 유출	OLED관련 장비 기술 유출 대기오염 방지기술 유출	OLED두께측정 기술 유출	OLED잉크젯 프린팅 기술 유출	2차 전지 핵심기술 유출	첨단 자율주행 기술 유출

기술적 문제

- 알 수 없는 웹메일에 대한 접속 탐지 불가
- 필터링 기술의 근본적인 탐지의 한계

휴머니즘 문제

- 임직원의 오타 등 실수로 인한 정보 유출
- 임직원의 이직 및 퇴사에 의한 불법 행위

정보보안 기본지침(국가정보원)

제 66조(비공개 업무자료 처리)

④ 공무원 등은 제3항제5호 및 제6호에 해당하는 경우를 제외하고는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제2조제1항제2호에 따른 **정보통신서비스(전자우편·메신저 등을 포함한다) 또는 국외에서 제공하는 이와 유사한 서비스(이하 "상용 정보통신서비스"라 한다)를 이용하여 비공개 업무 자료를 작성, 저장, 수·발신하여서는 아니 된다.** <개정 2020.7.1>

제 66조의 2(특정 상황별 비공개 업무자료 처리)

③ 공무원등이 자문 등의 목적으로 비공개 업무자료를 업무자료 공식 소통수단을 활용할 수 없는 **민간인에게 발신하거나 민간인으로부터 수신 받고자 할 경우에는 공무원등의 소속 기관 전자우편 또는 공직자 통합메일을 활용해 발신하거나 수신 받아야 한다.** [본조신설 <2020.7.1>]

머신러닝과 크롤링으로 메일시스템을 탐지하는 차세대 웹메일관리시스템

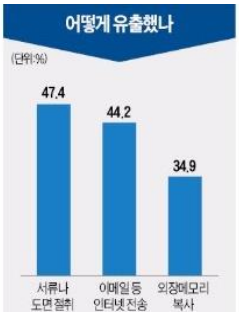
MailGuard v2

승인되지 않은 메일서비스와 알 수 없는 메일서버에 대한 사용자의 접속을 실시간으로 탐지·차단하여 메일을 통한 기밀정보의 유출을 차단하는 화이트보안기술의 비인가웹메일관리시스템입니다.

	대기업	중소기업
수일 이내	30.8%	23.5%
3개월 이내	46.2%	23.5%
6개월 이내	7.7%	5.9%
1년 이내	7.7%	7.7%
1년 이상	7.7%	29.4%

[기술유출 사고 감지 시간별 비율]

* 자료 : 특허청

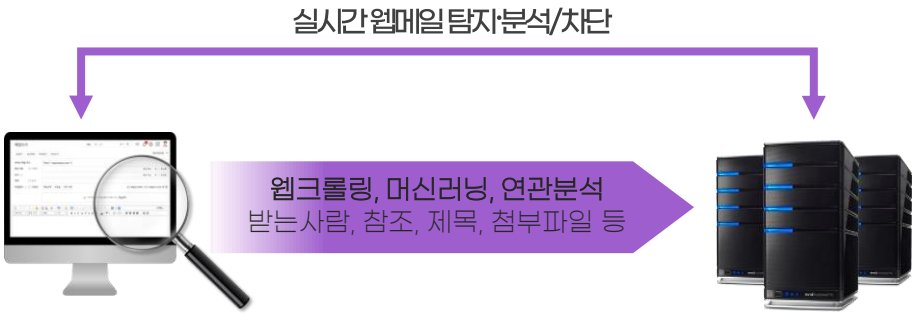


* 자료 : 경찰청

메일가드 필요성

솔루션	역할	탐지 대상	대응 기술
MailGuard v2	. 크롤링으로 알 수 없는 메일 접속을 정확히 탐지 . 알 수 없는 메일 접속에 대한 통제 . 국가별 RBL 적용으로 유해한 웹메일 접속 차단 . 피싱 사이트, 악성도메인 접속 차단(C-TAS) . 발신메일에 대한 로그 저장, 관리	. TCP Port 80,443 . 알 수 없는 메일서버 . Chrome, Edge	. 크롤링 . 머신러닝 . 필터링
인터넷모니터링	. 비업무용 사이트와 유해사이트 접속을 차단하며 관리 . 사용자 정의 카테고리를 통해 차단 이력을 체계적으로 관리 . 분야별 DB를 통해 URL, IP 정보 제공	. 알려진 통신 포트 . HTTP, FTP, SMTP	. 시그니처 기반 탐지 . 프로토콜 감시 및 차단
DLP 솔루션	. 파일과 문서의 외부 반출에 대한 보안 . 출력물에 대한 워터마크 및 프린터 제한 . 중앙통제 감시체계 구축	. 온/오프라인 유출 통제 . 저장매체, 네트워크 등	. 외부매체 제어 . 데이터 감시 및 차단

메일가드 특징



MailGuard v2 Agent

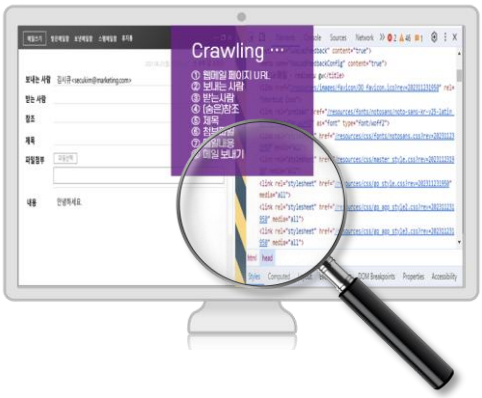
- 메일을 발송하는 웹페이지 탐지
- 한글, 영어 외 다른 언어의 웹페이지 탐지
- 비인가 웹메일 페이지에 접속 시 리다이렉션 또는 차단
- 관리자가 등록한 특정 키워드 입력 시 웹페이지 차단
- 지원 브라우저(Chrome, Edge)

MailGuard v2 Manager

- 다양한 정보를 표현하는 대시보드
- 화이트리스트 관리, 블랙리스트 관리
- 웹페이지 언어기반 필터링 관리
- GlobalRBL, KISA-RBL, C-TAS 등 악성도메인 차단
- 일일, 주간, 월간 등 특정 기간의 다양한 보고서 생성

※ 임직원이 웹브라우저를 실행하여 웹사이트에 접속하면 메일가드가 자동으로 해당 웹사이트를 모니터링합니다.

메일가드 핵심기능



Crawling

1. 웹메일 페이지 URL
2. 보내는 사람
3. 받는사람
4. (숨은)참조
5. 제목
6. 첨부파일
7. 메일내용
8. 메일 보내기

허용된 웹메일을 기간별, 영구, 사용자별 정책 적용

▼

특정한 웹메일 서비스는 관리자에게 승인 요청

▼

허용된 메일에 대하여 로그 저장

▼

차단된 메일에 대하여 경고, 관리자 지정페이지 연결

▼

웹은 자유롭게 사용하고, 메일만 허용 또는 차단

▼

웹메일 서비스를 효율적으로 제어

※ 크롤링기술과 머신러닝으로 수집한 데이터를 연관 분석하여 웹메일페이지를 실시간 탐지·차단합니다.

메일가드 주요기능

웹메일 발신 탐지·차단
. 인가되지않은메일서비스접속차단
. 웹메일에접속하여메일발송차단

악성 도메인 탐지·차단
. C-TAS,GlobalRBL 적용
. 피싱,다크웹등사용자접속차단

사용자 식별 및 인증
. 관리자계정추가/수정/삭제
. 사용자식별및AD인증

다국어 지원
. 관리자영역영어와한글지원
. 관리자로그인시언어선택

데이터 관리
. 웹메일서비스에대한접속관리
. 시스템로그,접속로그,메일로그

통계 및 보고서
. 실시간대시보드
. 일일,주간,월간등자동보고서

※ 메일에 대하여 수신과 발신을 관리자에 의해 사용자별로 다르게 정책을 제공할 예정입니다.
※ PC보안 기능이 추가적으로 적용될 예정입니다.

메일가드 기대효과

기밀 정보 유출 방지
인가되지 않은 웹메일을 통해 기밀정보 유출을 차단하고, 인가된 웹메일만 사용합니다.

메일보안 의식 개선
머신러닝과 크롤링으로 메일을 사전에 차단하여 사용자들의 메일보안 의식을 강화합니다.

기관의 신뢰도 향상
메일에 의한 기밀정보 유출을 방지하며, 인가된 메일을 통한 발송으로 기관의 신뢰도를 향상합니다.

내부 업무 관리
외부로 발송하려는 모든 메일에 대하여 저장, 통계와 검색 및 모니터링으로 효율적인 업무 관리

본사 : 부산시 해운대구 센텀북대로 60, 804호 (재송동, 센텀SE타워)
서울 : 서울시 금천구 가산디지털1로 205-27, 811호 (가산동, 가산A1타워)
Tel : 051-552-9118 | Fax : 051-552-9121 | sale@realsecu.net