SecuLetter Solution Brief

THE VALUE, BEYOND SECURITY

Trust, Fast, Innovate, Connect

SECULETTER

목차

© 2024 SecuLetter Co., Ltd. All rights reserved.

비전 소개

Our Technology

THE VALUE, BEYOND SECURITY

세계 유일의 보안 기술로 새로운 미래를 향해 나아갑니다.

디지털 콘텐츠는 비즈니스 커뮤니케이션의 필수 요소입니다. 시큐레터는 누구나 자유롭게 파일을 사용하며, 의심없이 이메일을 열어볼 수 있는 세상을 만들겠습니다.

콘텐츠를 주고받는 모든 글로벌 디지털 환경에서
발생하는 모든 위협에 대한 보안 솔루션 제공

최근 악성코드 침해 현황

최근 사이버 위협이 고도화되면서 '문서'를 통해 공격을 가하는 해킹 사례가 늘고 있습니다. 악성코드 공격의 상당수는 이메일을 통해 발생합니다. 특히 이메일 내 악성코드의 대부분은 첨부문서 파일로 위장하여 진단이 매우 어렵습니다.

비즈니스 이메일 해킹 시도 건수

3500만 annual

156,000 daily

※ 출처 : MS 사이버 위협 보고서 2023

악성 URL 피싱 공격 건수

417,678

※ 출처 : MS 사이버 위협 보고서 2023

악성 첨부문서 기반 공격 비중

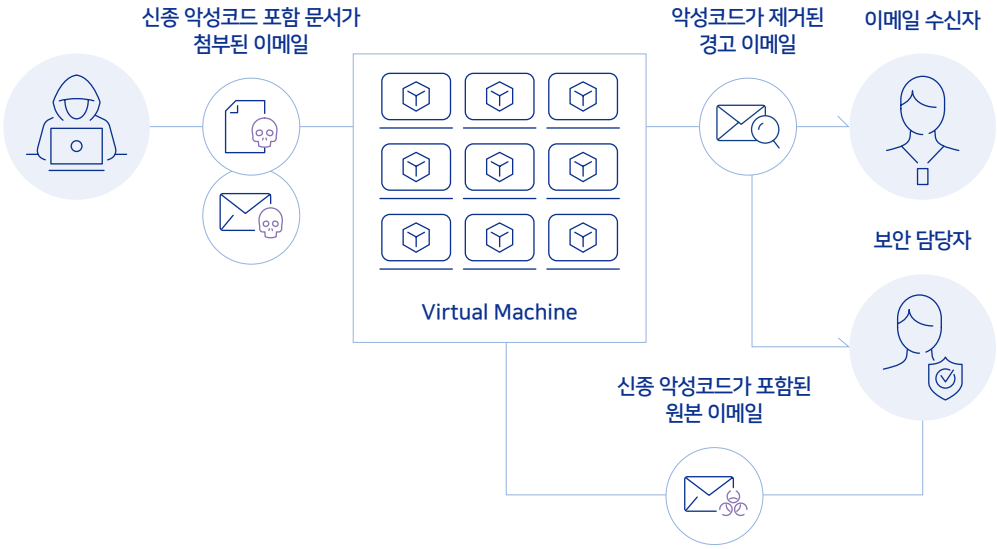
97.1%

※ 출처 : 2022~2023 시큐레터 데모 신청 고객 기준

행위 기반(샌드박스) 지능형 보안 솔루션의 문제점

기존 보안 솔루션의 구조

기존 행위 기반(샌드박스) 지능형 보안 솔루션은 샌드박스 환경에서 이메일을 미리 수신하여 행위 기반 공격을 분석하기 때문에 고도화된 보안 위협을 막을 수 없습니다.



행위 기반 탐지

행위가 일어나지 않을 시 탐지 불가, 여러 형태의 환경에서 행위를 분석하기 때문에 많은 진단 시간 소요	여러 형태의 가상 환경에서 이메일 중복 수신	첨부파일 열람 후 행위 분석

기존 보안 솔루션의 한계

행위 기반(샌드박스) 지능형 보안 솔루션은 느린 진단 속도로 인해 업무 연속성의 지장을 초래하고 다양한 우회 공격 대응이 어렵습니다.

가상 환경 회피

열람 시 가상 환경인 경우 행위 미동작

시간차 공격

열람 시 바로 행위 하지 않고 일정 시간 대기

사용자 행위 조건

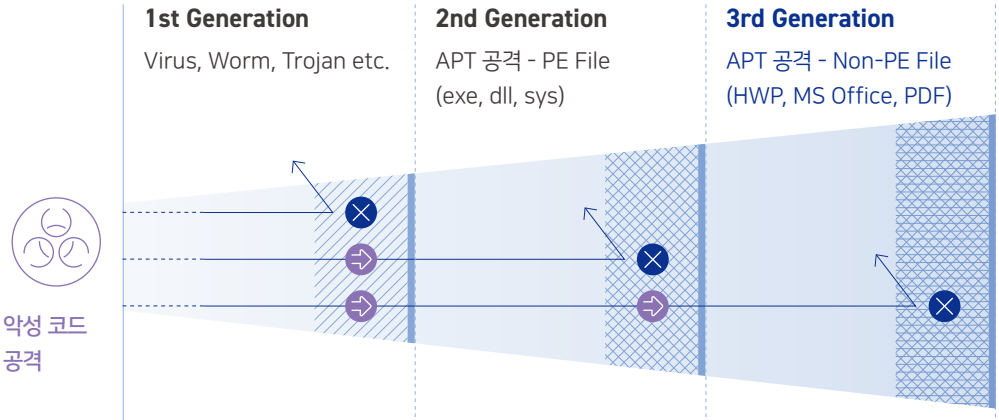
특정 페이지 열람 등 사용자 행위가 있을 경우 악성행위 시작

차세대 위협 탐지 대응 기술

자동화된 리버스 엔지니어링 & 제로 트러스트 기반 콘텐츠 무해화 (CDR)

갈수록 진화하는 악성 사이버 공격 패턴, 기존 보안 시스템을 피해갈 수 있는 기법들은 나날이 증가하고 있습니다. 시큐레터는 독자적으로 개발한 혁신 기술을 통해 알려지지 않은 공격까지 선제 대응합니다.

콘텐츠 무해화(CDR) 기술로 문서 내 악성 액티브 콘텐츠를 제거하고 자동화된 리버스 엔지니어링 기술로 프로그램 취약점을 이용한 신·변종 공격까지 차단해 사용자에게 제로 트러스트 업무 환경을 제공합니다.



	1st Generation Virus, Worm, Trojan etc.	2nd Generation APT 공격 - PE File (exe, dll, sys)	3rd Generation APT 공격 - Non-PE File (HWP, MS Office, PDF)
보안 기술	▶ 시그니처 기반 방어	▶ 행위 기반 APT 공격 방어	▶ 리버스 엔지니어링 & 제로 트러스트 기반 콘텐츠 무해화 통해 APT 공격 방어
보안 취약점 및 대응	▶ 알려진 시그니처 공격에 대해서만 방어 가능	▶ 가상 환경 회피, 시간차 공격, 사용자 행위 조건 공격에 대해 탐지 불가	▶ 행위 기반 탐지 우회 공격, 알려지지 않은 Zero-day 공격, 악성행위가 없는 악성코드까지 정확하게 진단 및 선제 차단

특장점

제로 트러스트 기반 강력한 위협 대응

01

첨부문서 내 악성 URL, 자바스크립트, 쉘코드 등 액티브 콘텐츠를 제거해 잠재적 위협 요소까지도 강력하게 대응

알려지지 않은 공격까지 선제 차단

02

독보적인 콘텐츠 샌드박스(위협 인텔리전스 + 리버스 엔지니어링 기반 디버거 분석 + 콘텐츠 무해화)로 유입되는 알려지지 않은 보안 위협까지 정확하고 빠르게 탐지해 선제 차단

AI 기반 위협 콘텐츠 인텔리전스(TI) 결합

03

최신 AI 기반 콘텐츠 위협 인텔리전스 정보 활용해 지속적인 보안 위협 대응, 전문 위협 분석가의 분석 노하우 분석 가이드 제시

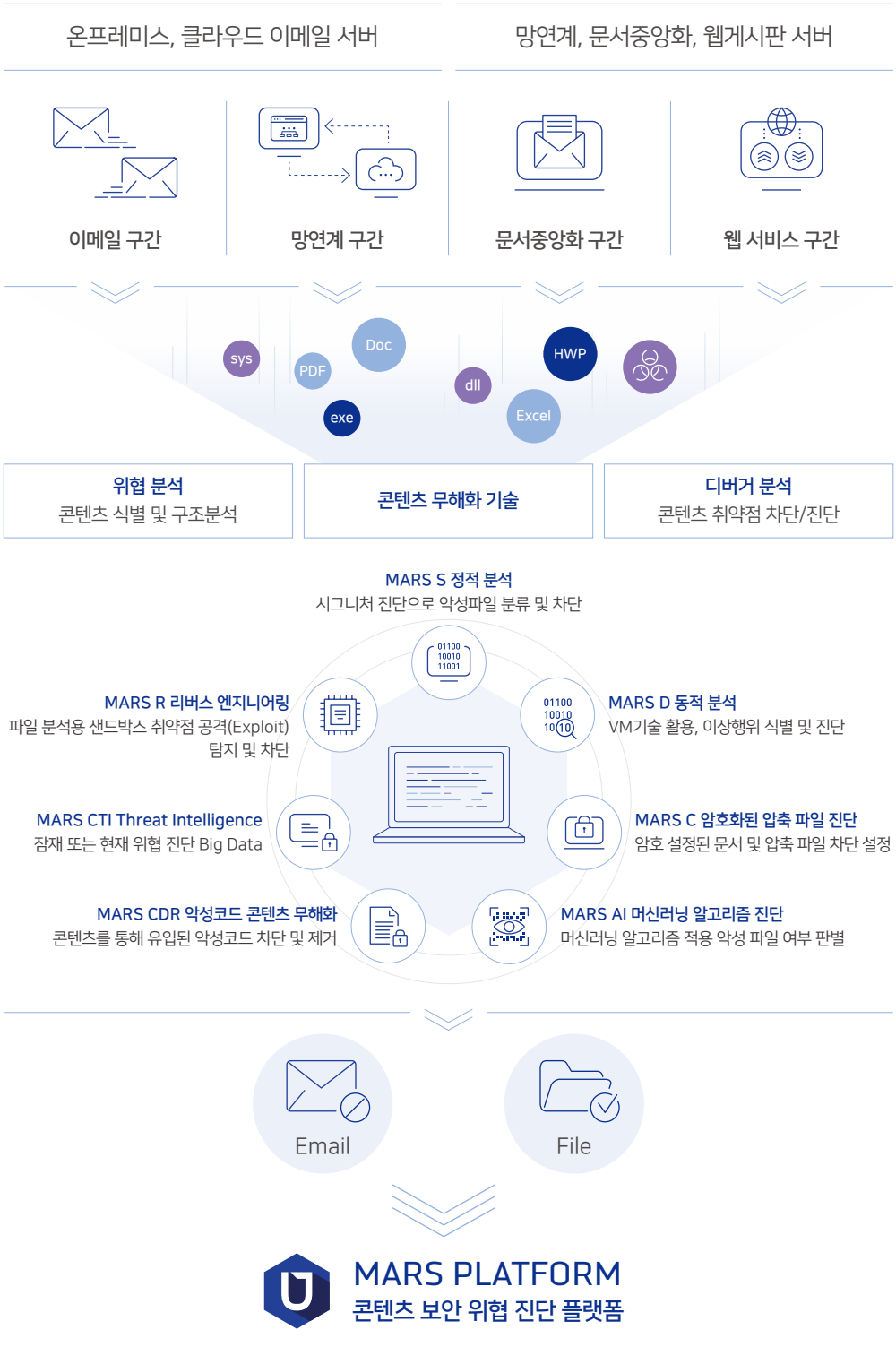
다양한 솔루션 제공

04

이메일, 망연계, 웹 서비스, 클라우드 환경 등 다양한 디지털 환경에 맞춤화된 보안 솔루션 제공

MARS 플랫폼

MARS 플랫폼은 기존 시그니처 및 행위 기반 솔루션의 단점을 극복하는 디버거 분석, 즉 자동화된 리버스 엔지니어링 기반 콘텐츠 보안 위협 진단 플랫폼입니다. MARS 플랫폼에 탑재된 시큐레터 제품은 콘텐츠 또는 비실행형 파일이 수집, 저장, 활용되는 모든 구간에서 보안 위협에 정확하고 빠르게 대응합니다.



제품 & 솔루션 소개

MARS SLE (SLES)

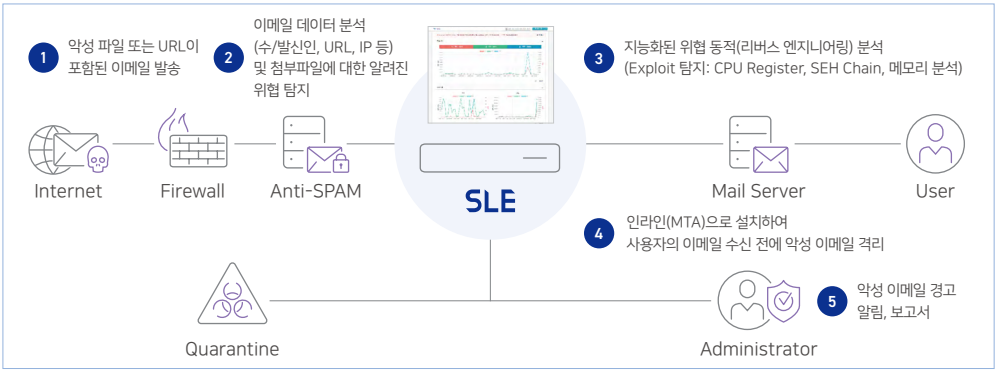
SecuLetter Email Security (Service) : 이메일 보안 솔루션

이메일 첨부파일 및 이메일 본문의 URL 등을 통해 유입되는 비실행형(Non-PE) 파일의 악성코드 탐지·차단에 특화된 위협 대응 전문 솔루션입니다. 구축형과 구독형(IDC, Cloud)로 제공해 다양한 방식으로 도입이 가능합니다. 구독형으로 도입할 경우 상용 이메일 솔루션 및 클라우드 이메일 서비스와 연동할 수 있어 중소기업 및 협회 등에서도 합리적인 가격으로 이메일 보안 전문 솔루션을 도입할 수 있습니다.

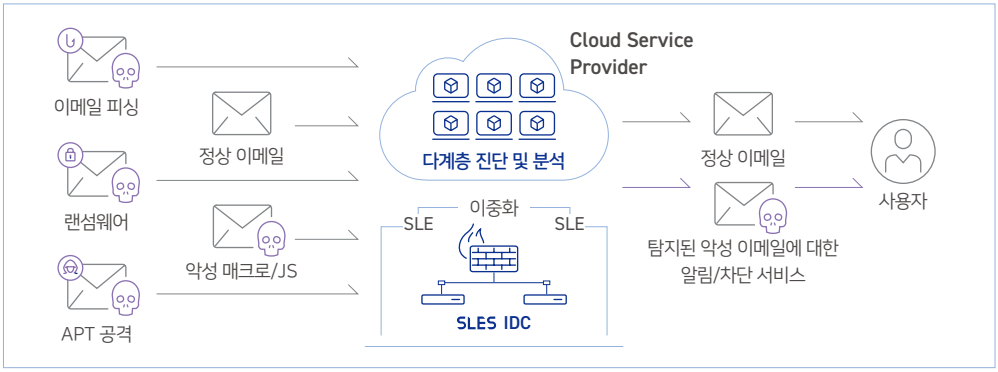
- 이메일 첨부파일의 악성코드 분석
- 이메일 본문에 삽입된 다운로드 링크를 통한 파일의 악성코드 검사
- 암호 설정된 파일의 악성코드 분석
- AI 활용 피싱 메일 탐지
- 수신된 메일의 수·발신자 정보 기반 위협 예측 통해 위험성 알림(이메일 프로파일링)
- 이메일 본문 및 첨부파일의 악성 QR 코드 무해화(큐싱 대응)
- 기존 시스템 변경 없는 유연한 설치 & 편리한 장비 운용(구축형)
- 간단한 MX 레코드 값 변경으로 간편 설치 (구독형)
- 악성 메일에 대한 관리자 알람 기능
- 고가의 보안 서비스를 경제적인 비용으로 이용(구독형)

[Add-on] MARS SLM (통합관리 서버 솔루션) : MARS SLE를 안정적으로 운용하기 위한 통합관리 서버로 통합 로그 관리 및 서버 리소스 관리, 정책 일괄 배포를 지원합니다.

구축형 이메일 보안 구성



구독형 이메일 보안 구성



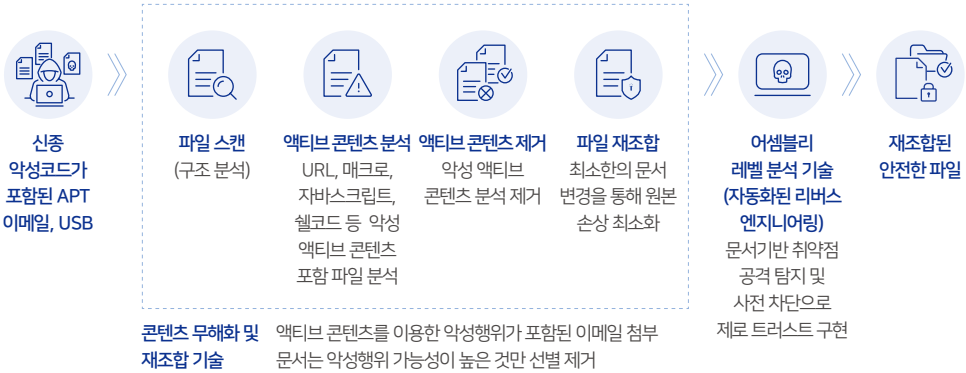
MARS SLF

SecuLetter File Security : 파일 보안 솔루션

파일을 주고받는 모든 환경에서 의심하기 힘든 비실행형(문서) 파일로 침입하는 콘텐츠 매개형 보안 위협과 악성코드를 사전에 탐지·차단합니다. 망연계(망분리), 웹 게시판(파일 업로드 구간), 문서중앙화 솔루션 연계 환경 등의 보안에 최적화된 제품입니다.

- 내부 네트워크로 유입되는 파일에 대한 악성코드 진단 및 차단
- 스토리지 및 저장 파일에 대한 악성코드 감염 내역 진단
- 용량 제한 없는 파일 검사 진행
- 악성코드 탐지 후 관리자 알람, 직관적 관리 보고서 제공

MARS SLCDR 솔루션을 적용한 악성코드 제거 과정

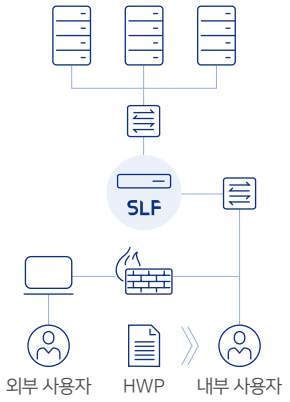


[Add-on] MARS SLCDR (콘텐츠 무해화 솔루션): 기존 CDR 기술과 자동화된 리버스 엔지니어링 기반 악성코드 분석 기술을 결합해 독자적으로 개발한 기술입니다. 문서에서 포함된 URL이나 매크로, 자바스크립트, 쉘코드 등 악성 액티브 콘텐츠를 식별하여 실행 가능한 요소를 제거한 후 깨끗한 새 문서로 재조립함으로써 공격 가능성을 차단합니다.

[Add-on] MARS SLM (통합관리 서버 솔루션): MARS SLF를 안정적으로 운용하기 위한 통합관리 서버로 통합 로그 관리 및 서버 리소스 관리, 정책 일괄 배포를 지원합니다.

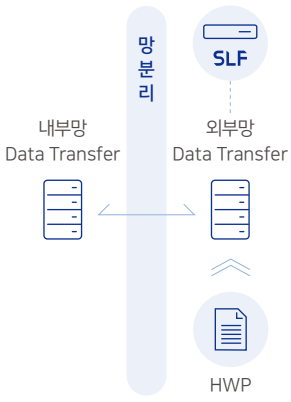
웹 서비스 솔루션 연계

파일이 웹 서비스 서버에 저장되기 전 업로드 된 파일의 악성코드 분석



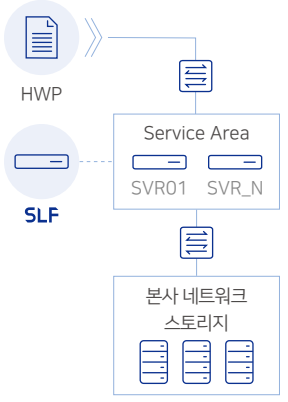
망간 자료전송 솔루션 연계

망연계 구간 파일이 내부망으로 전송되기 전 악성코드 분석



문서중앙화 솔루션 연계

문서집중화(또는 중앙화) 구간 파일이 스토리지에 저장되기 전 악성코드 분석



MARS TI

Threat Intelligence (위협 인텔리전스 서비스)

콘텐츠 기반의 다양한 정보를 관리해 비실행 파일 보안 위협에 빠르게 대응하는 위협 인텔리전스입니다. 문서, IOC 정보 등을 지속적으로 수집하고 데이터화함으로써 최신 트렌드 및 분석 상세 정보, 취약점 정보, 악성 문서 간 상호 연관 정보를 제공합니다.

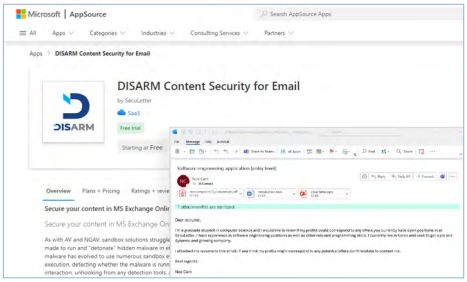
MARS TI 대시보드 화면

- 최신 보안 위협 뉴스 크롤링 수집 정보, IOC 정보 제공
- 비실행 파일 콘텐츠 취약점 탐지 및 진단 기반 위협 정보 제공
- 악성코드 전문가의 전문 위협 기준(M-DICE) 정보 제공
- 악성 콘텐츠 Hash/Domain 정보 제공
- 악성 샘플 분석 리포트 및 월간 분석 리포트 통해 위협 트렌드 제공
- 콘텐츠 위협 정보 통합(수집>추출>가공) 제공

DISARM for MS 365

DISARM Content Security for Email

글로벌 기준에 특화된 클라우드 이메일 보안 서비스로, 유입되는 보안 위협을 AI를 통해 지속적으로 탐지·분석함으로써 피싱 이메일, 랜섬웨어, 이메일 사기 공격(BEC) 등으로부터 사용자를 보호합니다. 시큐레터가 자체적으로 개발한 콘텐츠 무해화(CDR) 엔진과 디버거 분석 엔진을 통합하여 제공하기 때문에 MS 365 이메일 서비스로 유입되는 알려진 보안 위협뿐만 아니라 알려지지 않은 보안 위협까지 모두 선제 방어합니다.



MS 마켓플레이스 화면

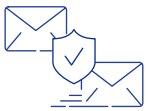
- MS 365 플랫폼과 5분 안에 빠르게 연동
- MS API를 활용으로 MX 레코드 값 변경 불필요 & 이메일 유실 위험 방지
- 이메일 첨부파일에 대한 콘텐츠 무해화
- 이메일 본문 및 첨부파일에 대한 시그니처 분석
- 콘텐츠 보안 전문 TI 지원
- 암호 설정된 파일의 악성코드 차단
- 압축 파일의 악성코드 차단
- 첨부파일 및 메일 본문에 대한 디버거 분석
- 콘텐츠 기반 보안 위협 상세분석 정보 제공
- 수신된 메일의 수·발신자 정보 기반 위협 예측 통해 위험성 알림(이메일 프로파일링)

솔루션 적용 사례

정부 및 금융기관 정보보호 지침을 준수하여 이메일, 망연계(망분리), 웹 게시판, 문서중앙화 구간에 적용 가능합니다.

이메일 보안	파일 보안	웹 서비스 보안	문서중앙화 보안
지능형 위협 보안 솔루션	**망간 자료전송 보안 솔루션**	**웹 서비스 보안 솔루션**	**ECM 보안 솔루션**

MARS PLATFORM



이메일 구간(구축형/구독형)

이메일 구간으로 유입되는 지능형 보안 위협 탐지 및 차단

악성 이메일 차단 및 첨부 파일의 액티브 콘텐츠 무해화

망간 자료전송 구간(구축형)

망/네트워크의 데이터 전송 구간으로 유입되는 보안 위협 탐지 및 차단

외부망 망연계 솔루션과 연동 구성해 유입된 악성 파일 차단 및 콘텐츠 무해화

파일 업로드 구간(구축형)

공공기관 및 기업의 웹 서비스 내 파일 업로드 구간으로 유입 되는 보안 위협 탐지 및 차단

악성 파일 차단 후 격리하고 파일 내 액티브 콘텐츠 무해화

문서중앙화 구간(구축형)

조직 내 정보 문서 및 지식 정보 공유 관리 구간으로 유입 되는 보안 위협 탐지 및 차단

악성 파일의 차단/격리 및 콘텐츠 무해화 후 정상 파일만 문서 중앙서버에 안전하게 저장

주요 고객사

공공/교육기관

경제·인문사회연구회, 광주환경공단, 광진구시설관리공단, 국민건강보험공단, 국민연금공단, 국회사무처, 근로복지공단, 기상청, 농업기술진흥원, 대외경제정책연구원, 대한무역투자진흥공사, 대한체육회, 두원공과대학교, 문화체육관광부, 산업통상자원부, 영화진흥위원회, 예술의전당, 우정사업정보센터, 우주항공청, 울산항만공사, 의료기관평가인증원, 정보통신기획평가원, 제주특별자치도청, 조달청, 중부대학교, 중소벤처기업부, 한국고용노동교육원, 한국과학기술기획평가원, 한국과학기술정보연구원, 한국광해광업공단, 한국교직원공제회, 한국국제협력단, 한국대학교육협의회, 한국도로공사, 한국도박문제예방치유원, 한국문화정보원, 한국서부발전, 한국수자원공사, 한국언론진흥재단, 한국에너지기술평가원, 한국예술종합학교, 한국예탁결제원, 한국인터넷진흥원, 한국자산관리공사, 한국저작권보호원, 한국전력기술, 한국청소년정책연구원, 한국체육산업개발, 한국콘텐츠진흥원, 한국해양진흥공사, 한국환경산업기술원, 한국환경연구원, 한밭대학교, 한전산업개발, 환경부, 횃불트리니티신학대학원대학교 외

금융기관

BNK부산은행, BNK캐피탈, DB손해보험, IBK투자증권, KB증권, NH선물, 다올저축은행, 대신증권, 리치앤코, 메리츠캐피탈, 에스와이오토캐피탈, 오릭스캐피탈코리아, 유안타저축은행, 이베스트증권, 코리안리재보험, 키움예스저축은행, 키움저축은행, 푸본현대생명, 한국투자증권, 한국투자파트너스 외

기업

LIG넥스원, 고려호이스트, 그란코, 넷크루즈, 동훈그룹, 디지털존, 미원홀딩스, 삼성전자판매, 삼화페인트, 서울반도체, 어빌리티시스템즈, 영림원소프트랩, 오스템, 위드펀드 외

SECULETTER

SECULETTER
THE VALUE,
BEYOND SECURITY

대표 문의
Tel: 031-608-8866, Fax: 031-608-8810
E-mail: contact@seculetter.com

솔루션 문의
Tel: 1670-8780
E-mail: sales@seculetter.com

기술 지원
Tel: 031-608-8880
E-mail: se@seculetter.com