SecuLetter Solution Brief

# THE VALUE, BEYOND SECURITY

## Trust, Fast, Innovate, Connect

N2SF 지원 APT+CDR 솔루션
이메일구간·망연계구간·웹게시판구간·문서중앙화구간
OnPrem(구축형 솔루션)·SaaS(구독형 솔루션)


SECULETTER

# 목차

# 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

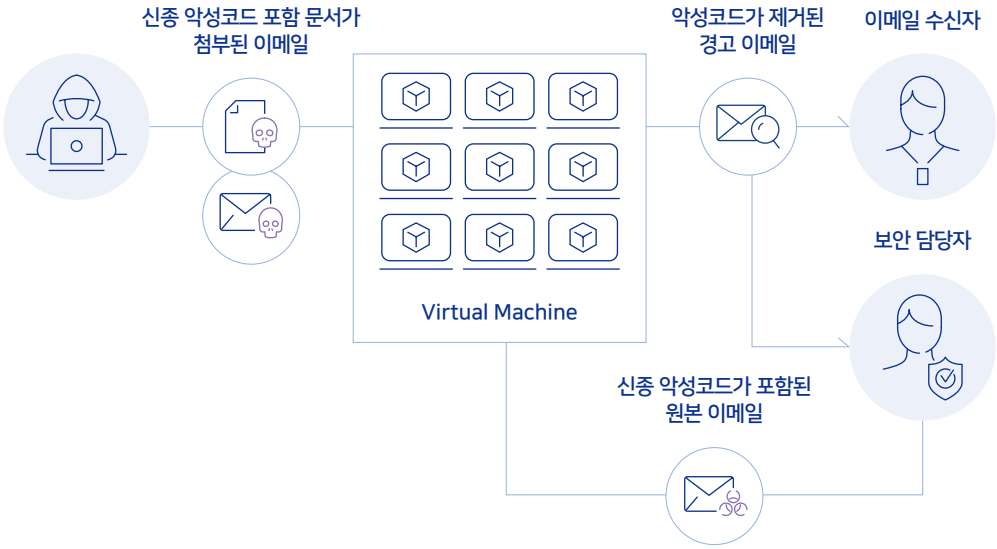
**97.1%**

※ 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

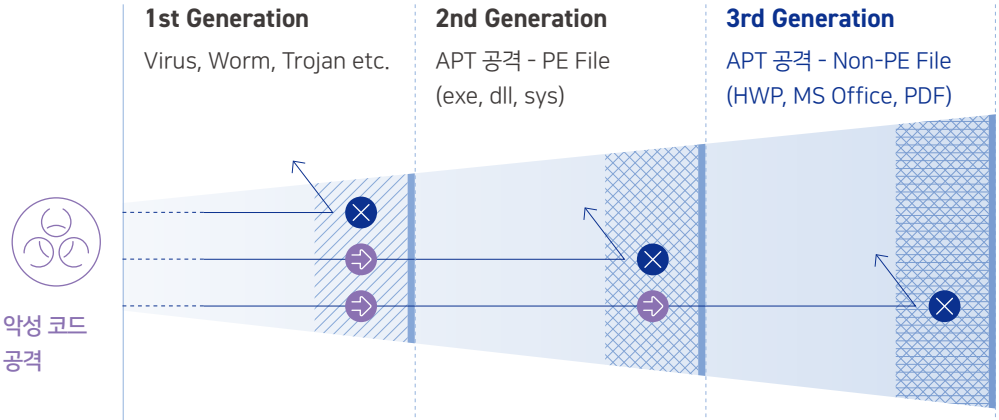
특정 페이지 열람 등 사용자 행위가 있을 경우 악성행위 시작

# 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<br>Virus, Worm, Trojan etc. | 2nd Generation<br>APT 공격 - PE File<br>(exe, dll, sys) | 3rd Generation<br>APT 공격 - Non-PE File<br>(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

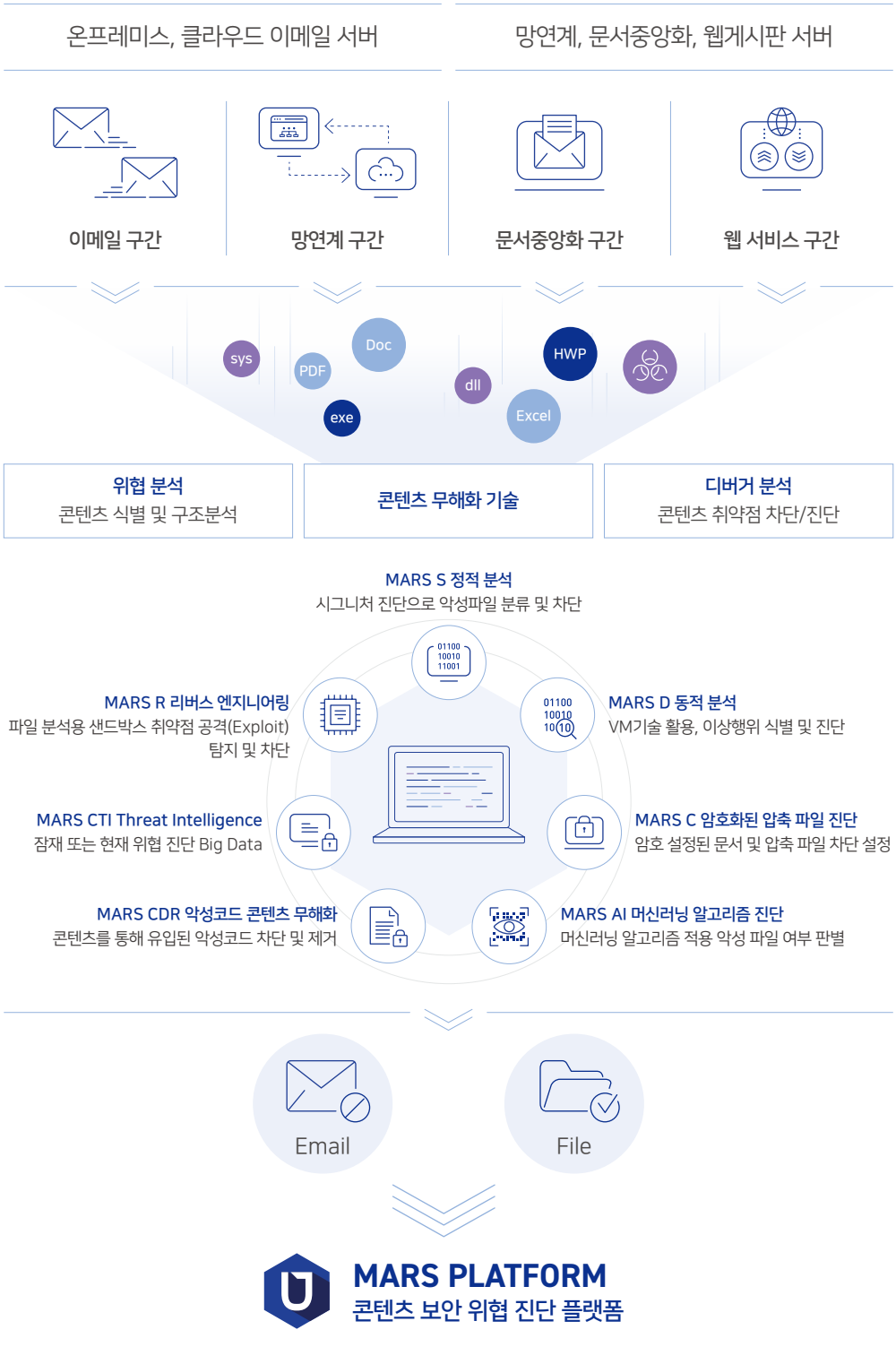
### 지연 없는 실시간 위협 탐지·무해화

04

빠른 속도 위협 탐지 평균 12초 이내, 무해화 파일당 34ms 처리. 기존 샌드박스 대비 10배 이상 빠른 속도로 업무 흐름을 방해하지 않는 실시간 보안 제공

# MARS 플랫폼

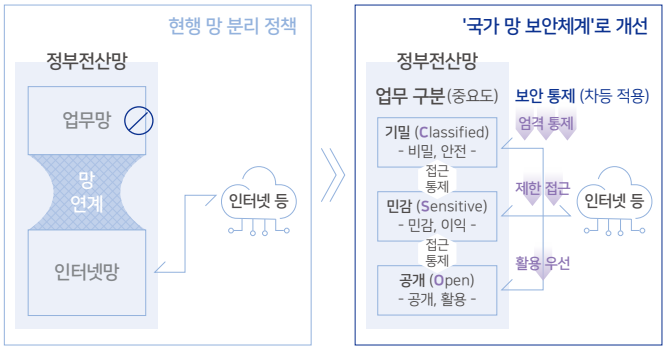
MARS 플랫폼은 기존 시그니처 및 행위 기반 솔루션의 단점을 극복하는 디버거 분석, 즉 자동화된 리버스 엔지니어링 기반 콘텐츠 보안 위협 진단 플랫폼입니다. MARS 플랫폼에 탑재된 시큐레터 제품은 콘텐츠 또는 비실행형 파일이 수집, 저장, 활용되는 모든 구간에서 보안 위협에 정확하고 빠르게 대응합니다.



# 국가 망 보안체계(N2SF) 개요

N2SF(National Network Security Framework)는 국가 정보원이 18년간 유지해 온 획일적 망분리 정책을 대체하기 위해 수립한 새로운 국가 망 보안체계입니다. 2025년 1월 드래프트 버전이 최초 공개되었고, 같은 해 9월 '사이버 서밋 코리아(CSK 2025)'에서 보안 가이드라인 정식 버전 1.0이 발표되었습니다. 업무 정보를 중요도에 따라 기밀(C)·민감(S)·공개(O) 3개 등급으로 분류하고, 등급별 차등 보안통제를 적용합니다. 기존의 물리적 망분리에서 정보 등급 기반 보안통제로 전환되며, 콘텐츠 무해화(CDR) 등 기술적 보안 조치가 핵심 역할을 수행합니다.
따라서 3개 등급으로 분류하고, 등급별 차등 보안통제를 적용하는 프레임워크입니다.


### 기존 망 분리 정책과 국가 망 보안체계 비교




### C/S/O 등급분류 체계

**C 기밀 Classified**
국가 안보·기밀 정보
최고 수준 보안통제

**S 민감 Sensitive**
행정 내부 전용 정보
기술 보안통제 적용

**O 공개 Open**
공개 가능 정보
기본 보안수준 적용

분류된 데이터는 서로 다른 보안등급의 도메인에 존재하며, 등급 간 안전한 정보 이동을 위해 CDS(Cross Domain Solution)가 필수적입니다.

### CDS의 핵심 기술: CDR(콘텐츠 무해화)

CDS는 기능과 목적에 따라 접근 CDS, 다중등급보안 CDS로 구분됩니다. 모든 CDS 유형에서 공통적으로 요구되는 핵심 보안기술이 CDR입니다.

| N2SF ID | 소항목 | 보안통제 설명 | 우선 검토 |
|---|---|---|---|
| N2SF-CD-3 | 일방향 전송 기술 적용 (Data Diode) | 정보 유출 방지를 위해 단방향 전송 장치를 활용하여 일방향 정보 흐름을 강제 | ●● |
| N2SF-CD-4 | 검증 기반 릴레이 시스템 적용 | 수신된 정보는 릴레이 서버를 통해 악성코드 스캔, 포맷 검증, 콘텐츠 정제 후 안정성 판단을 거쳐 송신 | ●● |
| N2SF-CD-5 | 파일 유형 기반 전송 정책 | MIME 타입, Magic Number 등을 기준으로 허용된 파일 유형만 송수신 허용 | ●● |
| N2SF-CD-6 | 콘텐츠 무해화(CDR) 적용 | 전송 전 파일 내 삽입된 숨겨진 객체, 매크로, 스크립트 등을 제거하고 안전한 형식으로 콘텐츠를 정제 | ● |
| N2SF-CD-7 | 메타데이터 통제 | 메타데이터 정책 적용, 필요 시 제거 후 전송 | ● |

※ 출처: 국가정보원「국가 망 보안체계(N2F) 보안 가이드라인 1.0」(2025.9)

# CDR: N2SF의 정보 이동 통제를 구현하는 기술

N2SF는 탐지가 아니라 정보의 '형태'를 통제하는 보안체계입니다. 기존 보안은 '위험한 파일'을 찾지만, N2SF는 '위험하지 않은 형태'만 허용합니다. CDR은 이 원칙을 기술적으로 실현하는 핵심 수단입니다.

## 기존 보안 방식의 구조적 한계

### 기존 보안의 판단기준

× 악성코드 검사

**구조적 한계:**

× 정상문서 + 악성 스크립트 → 통과
× 정상포맷 + 취약점 트리거 → 통과
× 정상매크로 + 정보유출 기능 → 통과
→**"악성이 아니면 통과" 구조**

### N2SF 기반 악성코드 대응 방식

✓악성코드 스캔
✓액티브 콘텐츠 식별
✓액티브 콘텐츠 제거
✓파일 재조합
악성 문서 유입 시도 → CDR 엔진 처리 → 안전한 파일 반입
→**"안전한 형태만 허용" 구조**

## CDR(Contents Disarm and Reconstruction)의 N2SF 정합성

CDR은 파일을 신뢰하지 않고, 구조를 분해하고, 위험 요소를 제거한 뒤, 안전한 형태로 재생성합니다.

| N2SF 요구 개념 | CDS 통제항목 | CDR 역할 |
|---|---|---|
| 외부 유입 통제 | N2SF-CD-4 | 무해화 후 반입 |
| 비정형 데이터 관리 | N2SF-CD-5 | 문서·이미지 직접 처리 |
| 정보 이동 통제 | N2SF-CD-6 | 이동 전 구조 재작성 |
| 메타데이터 통제 | N2SF-CD-7 | 메타데이터 정책 적용·제거 후 전송 |

→CDR의 본질은 탐지가 아닌 "무해화"임
→CDR은 N2SF의 정보이동통제를 기술적으로 구현하는 수단임

## CDR 적용에 따른 보안환경 변화 – N2SF 준수 전환

### 현재 (탐지 중심, N2SF 미충족)

외부 기업 / 민원인
↓
이메일 / 포털 업로드
↓
악성코드 검사
↓
내부망 반입
↓
담당자 열람

판단기준: 악성코드 여부
탐지되지 않으면 내부 유입

### CDR 적용 후 (N2SF 준수)

외부 기업 / 민원인
↓
이메일 / 포털 업로드
↓
악성코드 검사
↓
CDR 무해화 처리 (구조 분해·위험요소 제거·재생성)
↓
안전 문서 생성
↓
내부망 반입
↓
담당자 열람

판단기준: 안전한 구조(파일) 여부
무해화된 파일만 내부 반입
→ N2SF-CD-4, CD-5, CD-6, CD-7 충족

※ 출처: 국가정보원「국가 망 보안체계(N2F) 보안 가이드라인 1.0」(2025.9)

**CDR의 본질은 탐지가 아닌 "무해화"**
CDR은 N2SF의 정보이동통제를 기술적으로 구현하는 수단입니다. 전송 전 파일 내 삽입된 숨겨진 객체, 매크로, 스크립트 등을 제거하고 안전한 형식으로 변환하여 콘텐츠를 정제합니다. (N2SF-CD-6)

# 제품 & 솔루션 소개

## MARS SLF

### SecuLetter File Security : 파일 보안 솔루션

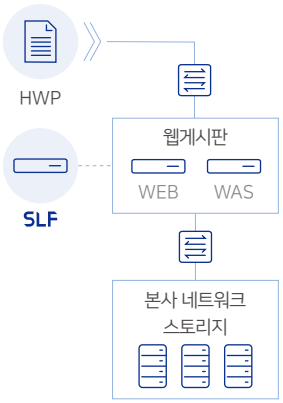
파일을 주고받는 모든 환경에서 의심하기 힘든 비실행형(문서) 파일로 침입하는 콘텐츠 매개형 보안 위협과 악성코드를 사전에 탐지·차단합니다. 망연계(망분리), 웹 게시판(파일 업로드 구간), 문서중앙화 솔루션 연계 환경 등의 보안에 최적화된 제품입니다.

- 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

### 적용 환경별 구성

#### 웹 서비스 솔루션 연계

외부 사용자가 업로드하는 파일이 서버에 저장되기 전 검사

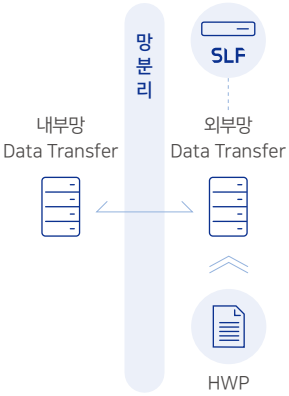



**적용 가능 구간**

홈페이지 게시판, 민원 접수 시스템, 채용 포탈, 고객 문서 수신

#### 망간 자료전송 솔루션 연계

망분리 구간에서 내부망 유입 전 알려지지 않은 위협까지 탐지·차단

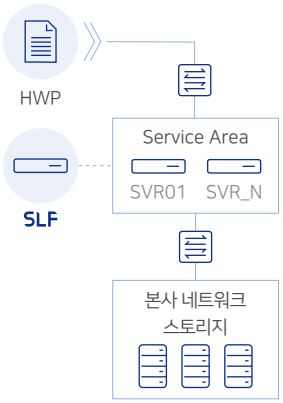



**적용 가능 구간**

금융 내부망, 정부·국방 보안망, 보안USB 검사, 보안 개발망

#### 문서중앙화 솔루션 연계

스토리지에 저장되기 전 검사, 내부 확산 전 위협 원천 차단




**적용 가능 구간**

사내 파일 서버, 클라우드 스토리지, 기밀문서 센터, 메신저 파일 전송

**[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.

# MARS SLCDR

## SecuLetter Content Disarm & Reconstruction : 콘텐츠 무해화 솔루션

문서 내 숨겨진 위협을 제거하고, 원본 사용성을 유지한 상태로 안전한 파일을 제공하는 고성능 CDR 솔루션입니다. 기존 CDR 기술에 자체 개발한 리버스엔지니어링 기반 악성코드 분석 기술을 결합하여, 문서에 포함된 URL이나 메크로, 자바스크립트, 셀코드 등 악성 엑티브 콘텐츠를 식별하고 실행 가능한 요소를 제거한 후 깨끗한 새 문서로 재조합하여 공격 가능성을 원천 차단합니다.

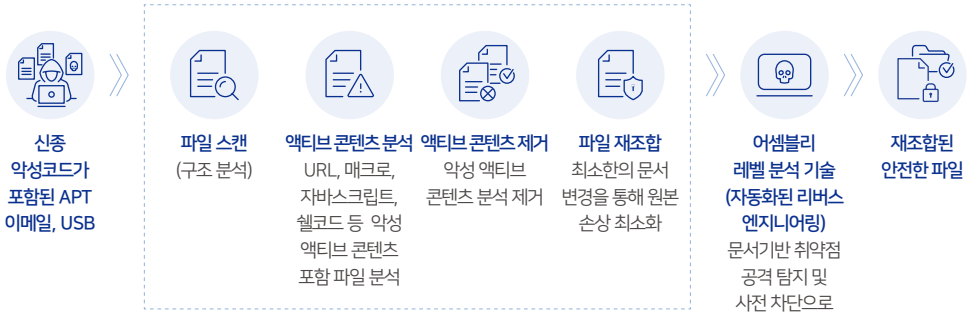
**309종+ 파일 타입 지원**
MS Office, PDF, HWP, 이미지, 영상, CAD 등
세계 최다 파일 포맷 무해화

**파일당 평균 34ms 초고속**
원본 레이아웃·코멘트·스타일·원전 보존
업무 생산성 저하 없는 초저지연 처리

**모든 액티브 콘텐츠 선제 제거**
매크로, JS, OLE, ActiveX, DDE 등
시크니처 없이도 알려지지 않은 APT 차단

**무해화 정책 커스터마이징**
파일 유형·콘텐츠·사이즈별 정책 지원
부서/사용자/위협 수준별 세분화

### MARS SLCDR 솔루션을 적용한 악성코드 제거 과정




## 주요 기능

- 매크로/JavaScript 탐지 및 자동 제거 (AI 해석 기능 포함)
- 비실행 파일 내 악성코드 제거
- CFB + OOXML 모두 지원 (타사는 OOXML만)
- Hash/URL 기반 예외처리 등록
- 원본 레이아웃 유지 재구성 (코멘트·스타일 보존)
- 제로데이 공격 사전 차단
- 무해화 알림 배너 삽입 (조직별 문구 정의)
- QR코드 무해화 지원

## 적용 분야

**망분리/망연계 (CDS)**
N2SF CDS 구간 파일 무해화, 외부→내부 전송 시 위협 원천 제거

**파일 업로드 포탈**
홈페이지 게시판, 민원 접수, 채용 포탈 등 업로드 파일 실시간 무해화

**문서중앙화 연계**
스토리지 저장 전 무해화 처리, 내부 파일 서버·클라우드 보안 강화

**이메일 첨부파일**
수신 이메일 첨부 문서의 악성 엑티브 콘텐츠 제거 후 안전한 파일 전달

**웹 브라우저 격리 (ICAP)**
ICAP 프로토콜 연동, 브라우저 다운로드 파일 실시간 무해화

**외부 파트너 문서 교환**
협력사·고객과의 문서 송수신 시 무해화로 안전한 파일 교환 보장

**공공기관 민원·제안 접수**
시민 제출 문서의 위협 요소 사전 제거, 내부 시스템 보호

※ SLF with CDR add-on 대비 APT 탐지 기능이 빠지는 대신 더 빠른 처리 성능과 더 저렴한 구축 비용이 장점

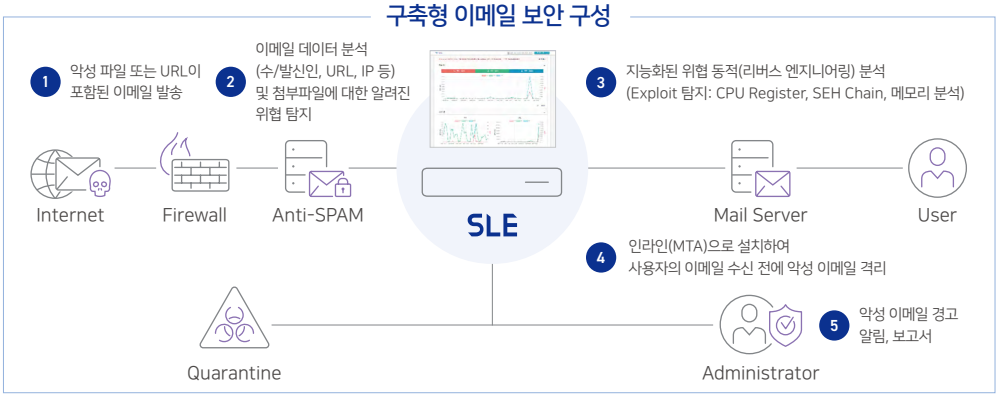
# MARS SLE (SLES)

## SecuLetter Email Security (Service) : 이메일 보안 솔루션

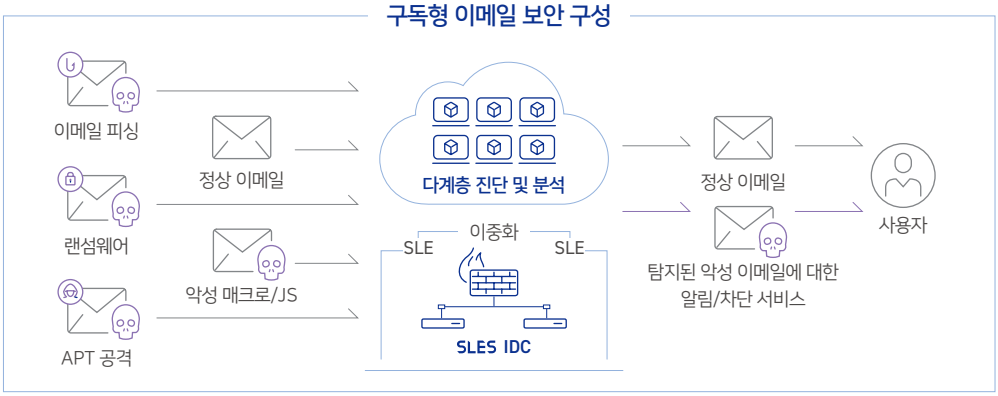
이메일 첨부파일 및 이메일 본문의 URL 등을 통해 유입되는 비실행형(Non-PE) 파일의 악성코드 탐지·차단에 특화된 위협 대응 전문 솔루션입니다. 구축형과 구독형(IDC, Cloud)로 제공해 다양한 방식으로 도입이 가능합니다. 구독형으로 도입할 경우 상용 이메일 솔루션 및 클라우드 이메일 서비스와 연동할 수 있어 중소기업 및 협회 등에서도 합리적인 가격으로 이메일 보안 전문 솔루션을 도입할 수 있습니다.

- 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)

### 구축형 이메일 보안 구성




### 구독형 이메일 보안 구성




**[Add-on] MARS SLCDR (콘텐츠 무해화 솔루션)** : SLE에 CDR 기능을 추가하여 이메일 첨부파일의 잠재적 위험요소 (URL, 매크로, 자바스크립트, 쉘코드 등) 를 제거하고 안전한 파일로 변환

**[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.

# DISARM for Microsoft 365 & Google Workspace

## Integrated Cloud Email Security

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 Microsoft 365 이메일 서비스로 유입되는 알려진 보안 위협뿐만 아니라 알려지지 않은 보안 위협까지 모두 선제 방어합니다.

### Why DISARM — 이런 위협, 기존 보안으로 막을 수 있습니까?

**사칭 이메일 공격**

경영진·거래처를 사칭한 BEC/VEC 공격은 시그니처가 없어 기존 보안을 우회합니다. DISARM은 AI 커뮤니케이션 프로파일링으로 소통 패턴의 이상 징후를 감지해 사칭 메일을 정밀 차단합니다.

**첨부파일 공격·랜섬웨어**

문서에 숨겨진 매크로·스크립트가 랜섬웨어 감염의 시작점입니다. DISARM은 CDR 엔진으로 악성 액티브 콘텐츠를 원천 제거하고 안전한 파일로 재조합하여 제로데이 위협까지 무력화합니다.

**내부 이메일 위협**

외부 수신 메일만 검사하는 기존 보안은 내부 계정 탈취 후 확산되는 위협을 놓칩니다. DISARM은 내부·발신 이메일까지 모니터링하여 조직 전체를 보호합니다.

### 핵심 기능

**콘텐츠 무해화(CDR)**
이메일 첨부 문서 내 매크로, JavaScript, OLE 등 악성 액티브 콘텐츠를 자동 제거하고 안전한 파일로 재조합

**BEC 악성 메일 탐지**
경영진 사칭, 거래처 위장 등 사회공학 기반 이메일 사기(BEC) 공격을 AI가 패턴 분석으로 정밀 탐지

**암호화 파일 처리**
비밀번호 보호 ZIP, 암호 설정 문서 등 기존 보안이 놓치는 사각지대까지 분석·차단

**URL 평판 분석**
이메일 본문·첨부 내 악성 URL을 Cloud TI 기반으로 실시간 탐지하고 차단

**콘텐츠 보안 전문 TI**
Cloud Threat Intelligence 연동으로 최신 위협 정보를 실시간으로 반영, 지속적으로 진화하는 탐지 역량 제공

**이메일 프로파일링**
수·발신자 커뮤니케이션 패턴을 AI가 분석하여 BEC·VEC 사칭 공격을 예측하고 위험성 알림

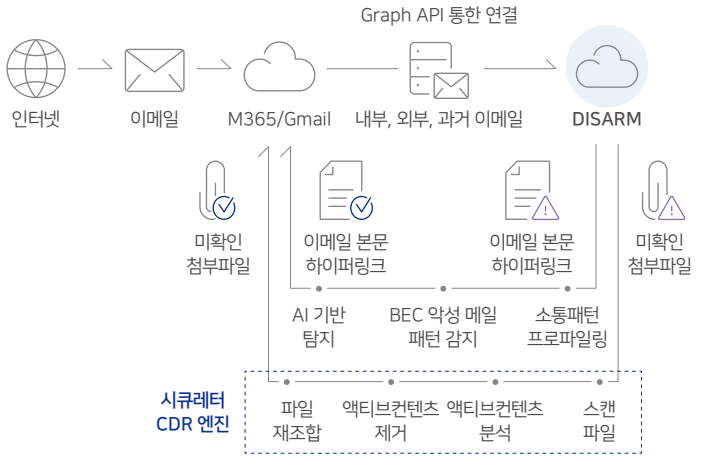
**압축 파일 악성코드 차단**
다중 압축·중첩 아카이브까지 자동 해제하여 은닉된 악성 파일 탐지 및 차단

**위협 상세분석 리포트**
콘텐츠 기반 보안 위협의 상세 분석 결과와 탐지 근거를 시각적 리포트로 제공

### Deployment Model

M365/Gmail Cloud 연동 방식

- API 기반 연동 방식
- MX 레코드 변경 없이 설치



## 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, AI 기반 탐지 정보, 악성 문서 간 상호 연관 정보를 제공합니다.

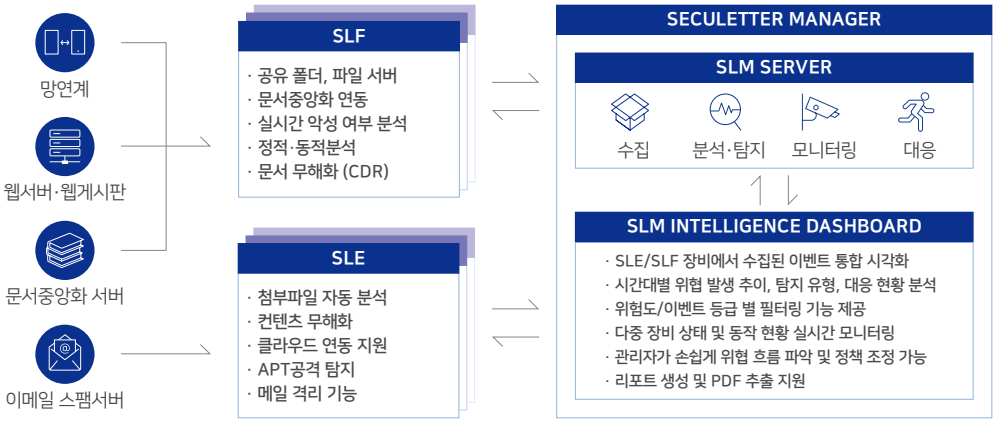
MARS TI 대시보드 화면

- 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
- 최신 보안 위협 뉴스 크롤링 수집 정보, IOC 정보 제공
- 콘텐츠 위협 정보 통합(수집>추출>가공) 제공

## MARS SLM

### SecuLetter Manager : 통합 관리 플랫폼

MARS 솔루션의 중앙 관리 시스템으로, 이메일 및 파일 구간 등 다양한 경로에서 수집·분석된 위협 정보를 한곳에서 통합 관리하는 플랫폼입니다. MARS 어플라이언스 제품과 연동하여 보안 담당자는 다수의 MARS 장비의 자원 현황과 샌드박스 분석 진행 상황까지 한눈에 파악할 수 있습니다. 개별 장비 관리로 대응하기 어려운 지능형 지속 위협(APT)에 대해 '탐지-분석-모니터링-대응'의 전 과정을 아우르는 관제 기능을 제공하여 고도화된 위협을 종합적으로 해결합니다.




**통합 위협 탐지 및 모니터링**
전체 SLE/SLF 장비의 탐지 이벤트와 시스템 현황을 통합 대시보드에서 실시간으로 모니터링할 수 있어, 위협 상황에 대한 직관적인 파악과 빠른 대응이 가능합니다.

**중앙 로그 통합 관리**
사전 구성된 일체형 어플라이언스 형태로 제공되어 별도 설치 없이 빠른 도입이 가능하며, 안정적인 운영 환경을 보장합니다.

**로그 통합 검색**
여러 대의 SLE/SLF장비에서 발생하는 탐지 이벤트 및 로그를 중앙에서 수집하고 검색할 수 있어, 보안 이벤트 분석의 일관성과 운영 효율성이 크게 향상됩니다.

**정책 통합 배포 기능**
다수의 서버에 대해 보안 정책을 중앙에서 일괄 설정 및 배포할 수 있어, 정책 적용의 일관성과 신속한 운영이 가능하며 관리 부담을 줄입니다.

# 대한민국의 국가 자산을 보호하는 시큐레터

시큐레터는 대한민국의 핵심 디지털 자산 — 금융 시스템, 국가 기반 시설, 공공 데이터를 — 피싱, 랜섬웨어, 지능형 사이버 위협으로부터 보호합니다. 문서 무해화, 이메일 보안, 위협 격리 기술을 기반으로, 연금 및 금융 자산 800조 원, 국가 에너지망, 정부 주요 정보 자산을 안전하게 지키고 있습니다. 아래는 시큐레너터의 기술을 신뢰하고 있는 금융, 공공, 기업 분야의 대표 고객사들입니다.

## 금융

한국투자증권 · BEST · KB증권 · 대신증권 · IBK투자증권 · BNK캐피탈 · BNK
에스와이오토캐피탈(주) · NH농협무역 · DB손해보험 · NH선물 · Rich&Co. · 푸본현대생명
DAOL 다올투자증권 · KOREAN Re · MG새마을금고 · meritz

## 공공기관

보험개발원 · 국민건강보험 · 기상청 · 경제·인문사회연구회 · NPS 국민연금공단 · 근로복지공단 · 광한국시설관리공단
KETEP 한국에너지기술평가원 · 산업통상자원부 · 조달청 · 우정사업정보센터 · ex 한국도로공사 · 울산항만공사 · 제주특별자치도
KOICA 한국국제협력단 · KISTEP 한국과학기술기획평가원 · kbc 한국해양진흥공사 · K water 한국수자원공사 · 한전산업개발(주) · 한국전력기술 · KISA 한국인터넷진흥원
KSD 한국예탁결제원 · 한국도박문제예방치유원 · 대한체육회 · 한국언론진흥재단 · 문화체육관광부 · 예술의전당 · 한국저작권보호원
KSPO&CO 한국체육산업개발주식회사 · K-ARTS Korea National University of Arts · 한국콘텐츠진흥원 · kofic 영화진흥위원회 · KCISA 한국문화정보원 · The K 한국교직원공제회 · 한국청소년정책연구원
한국대학교육협의회 · TORCH TRINITY · KEITI 한국환경산업기술원 · CAU 중앙대학교 · 두원공과대학교 · IITP 정보통신기획평가원 · KOMIR
의료기관평가인증원 · 국회사무처 · 대한석탄공사 · 과학기술정보통신부 · KELI 한국고용노동교육원 · LIG 넥스원 · KASA 우주항공청
KIEP 대외경제정책연구원 · kotra Korea Trade-Investment Promotion Agency

## 민간기업

Fodist · 영림원소프트랩 · MIWON · U BASE · 서울반도체㈜ · WITH FUND · HYVISION SYSTEM
Hyundai Oilbank · INNSBRUCK · DONGHOON · ENLIPLE · DIGITAL ZONE · Zenpix International · ENC 이엔씨 엔지니어링
ABILITY SYSTEMS · Granco · netcruz · (주) 크린피아 · KHC 고려호이스트 KOREA HOIST · PLASTAL
genesis lab · COOCON · ITP 인천테크노파크 · PENTACHORD · SAMSUNG 삼성전자판매 · KOREAN AIR · OSSTEM IMPLANT

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