SECULETTER

SecuLetter Email Security

Proactive Protection Against Advanced Cyber Threat

Over 91% of cyber attack initiates from email.
Protect your business from zero-day and everyday threats.

SLE SecuLetter Email Security

SecuLetter provides the next generation email security for advanced threat protection. SecuLetter Email Security uses multi-layered protection with automatized reverse-engineering analysis pattern and deliver the most advanced threat detection capabilities defend against the advanced persistent threats originating from emails.

Automatized Reverse Engineering Assembly Level Analysis

SecuLetter automatized reverse-engineering covers the blind spot of existing APT protection solution. It monitors the entire process by analyzing file input, processing and output. SecuLetter detects and blocks the exploit which occurs the malicious behavior.

Competitive Advantage

- Neutralize Evasive Threats - Accurate detection on document-based malware with no behaviors.
- Assembly Level Diagnosis - Provide accurate diagnosis and reduce false positive/negative.
- 5 Times Faster - Reduce 80% diagnosis time than traditional APT solution.

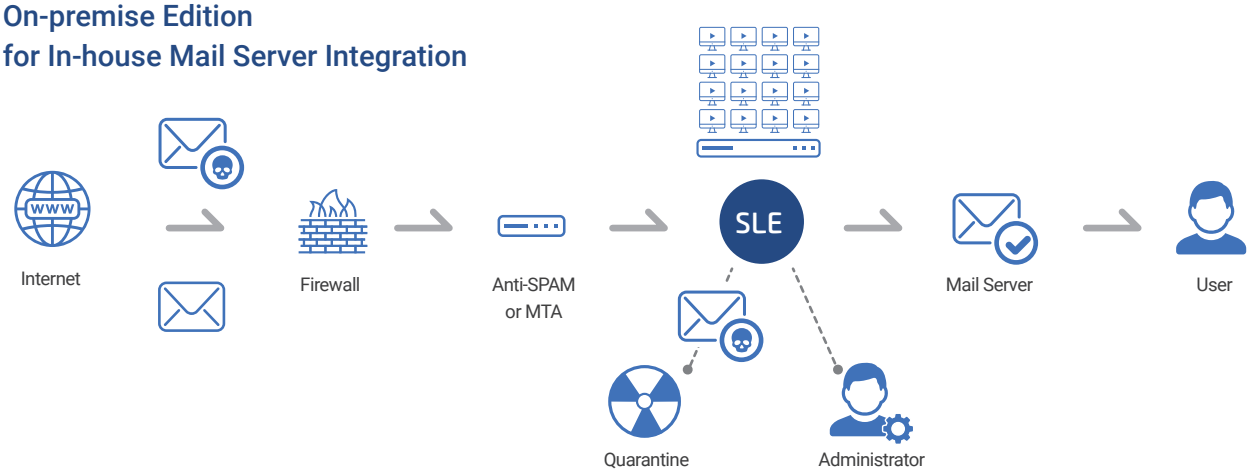
SECULETTER

Key Features

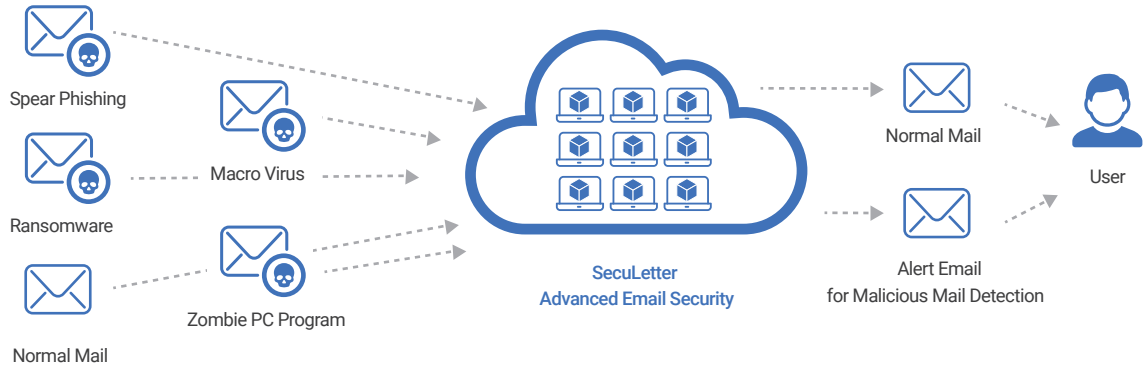
1. Detect and block email containing malicious content.
2. Analyze malicious code hidden in the file attached to the email.
3. Scan file can be downloaded from the URL link included in email.
4. Analyze malicious file included in password protected file.
5. Quarantine and archive detected malicious email.
6. Alert detected malicious email to administrator and recipient.
7. Provide detailed report of detected malicious content in real-time.
8. Support policy management for exceptions.

How It Works

On-premise Edition for In-house Mail Server Integration



Cloud Edition for Public Email Users



SecuLetter Co., Ltd.
3rd Floor, MELFAS Building, 225-14, Pangyoyeok-ro, Bundang-gu,
Seongnam-si, Gyeonggi-do, South Korea 13494

H www.seculetter.com
E global@seculetter.com

SECULETTER

global.seculetter.com

Unknown Threat Detection within 20 Seconds

SecuLetter Solution Guide

SECULETTER

Automated Reverse-engineering

CVE Analysis

Vulnerability Analysis

Process Stack Analysis

Memory Analysis

Debugging Analysis

Decoding Analysis

MARS PLATFORM

Enhanced Standard Layers & Cutting-edge APT Protection Solution

MARS S Static Analysis

Filter inflowed malicious file by signature- based diagnosis.

MARS R Reverse-engineering

Monitoring file input/output process by reverse-engineering to detect & block the exploit.

MARS D Dynamic Analysis

Identify & diagnose unusual behavior when accessing CPU, Memory, File and Network.

MARS CTI Threat Intelligence

Diagnose potential or current threats by threat intelligence source.

MARS CDR
Content Disarm & Reconstruction

Disarm file containing malicious contents and reconstruct.

MARS AI
Machine Learning Algorithm

Diagnose malicious status of the file by applying machine learning algorithm.

Reverse- engineering

VS

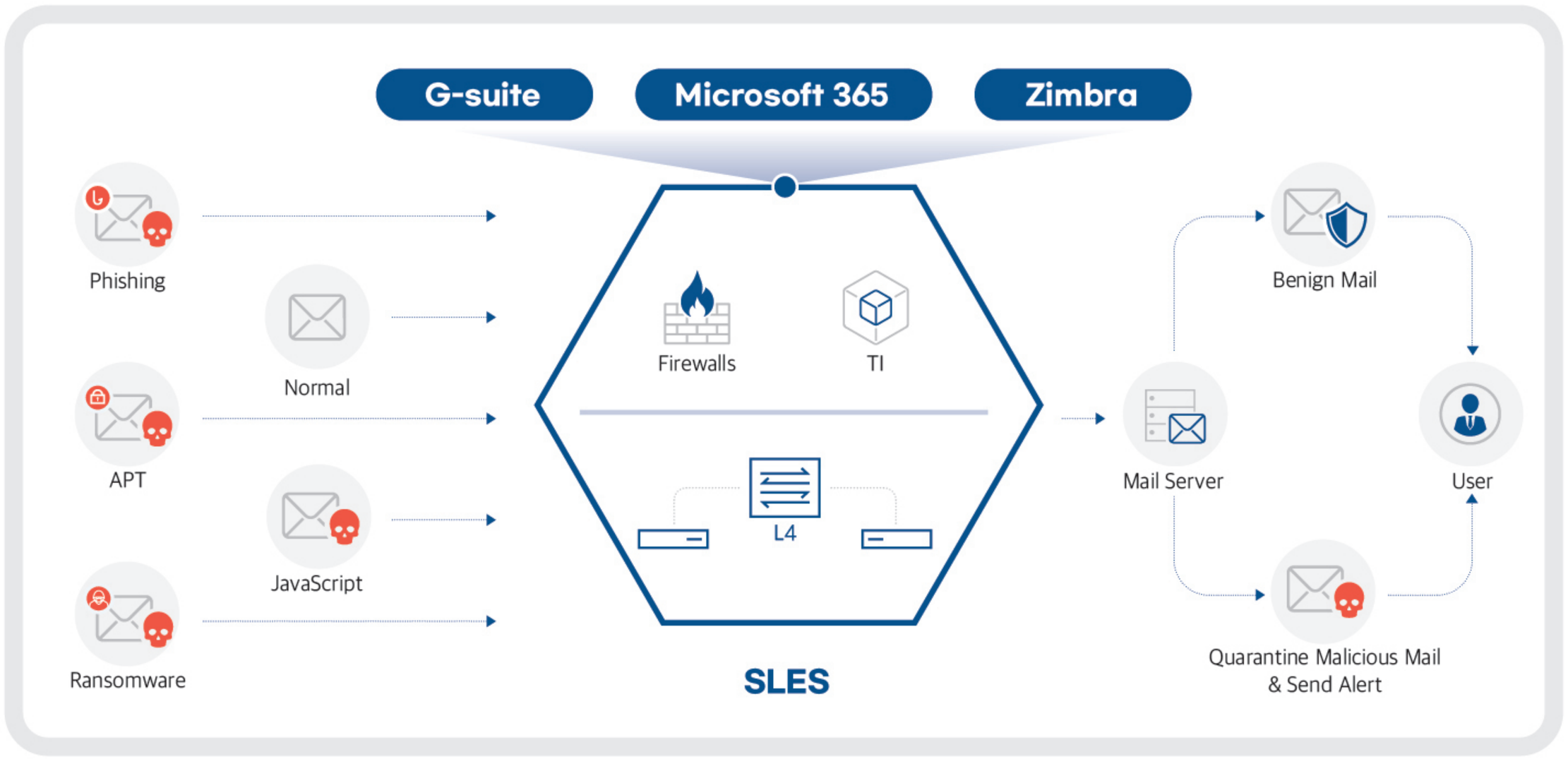
Traditional Threat Protection

Faster detection	Avg. 20 Seconds	Scan Speed	3-5 min
More accurate	Assembly Level	Visibility	Application
Stronger performance	Support	Anti-Evasion Techniques	Partly support

Cloud

MARS SLES Email Security for Microsoft 365

Email Security as a Service for Public Cloud Email.



*Support integration with other public cloud email services.

Cloud

MARS SLCDR Content Disarm & Reconstruction

Removes threats (ex. JS, URL, Shellcode) of files & Reconstruct to deliver safe documents.

Scan File

Analyze Active Content

Extract Active Content

Reconstruct File

Minimize Impact to Productivity

Zero interruption to corporate business process and removes possible malicious content included in files.

Eliminate Potential Threats Proactively

Safely extracts active content which can be used as attack method and repackage the content into safe document files.

Safe & Fast Delivery

SecuLetter CDR delivers safe files by removing executable content and reducing the delay of traditional sandboxing solutions.

Cloud

MARS DEFENDER File Analysis Service

Having suspicious files? Try MARS Platform feature as an online free service.

Figure out if suspicious files are malicious

- Analysis technique based on Software Reverse-engineering.
- Detect malicious document files for hacking attack.

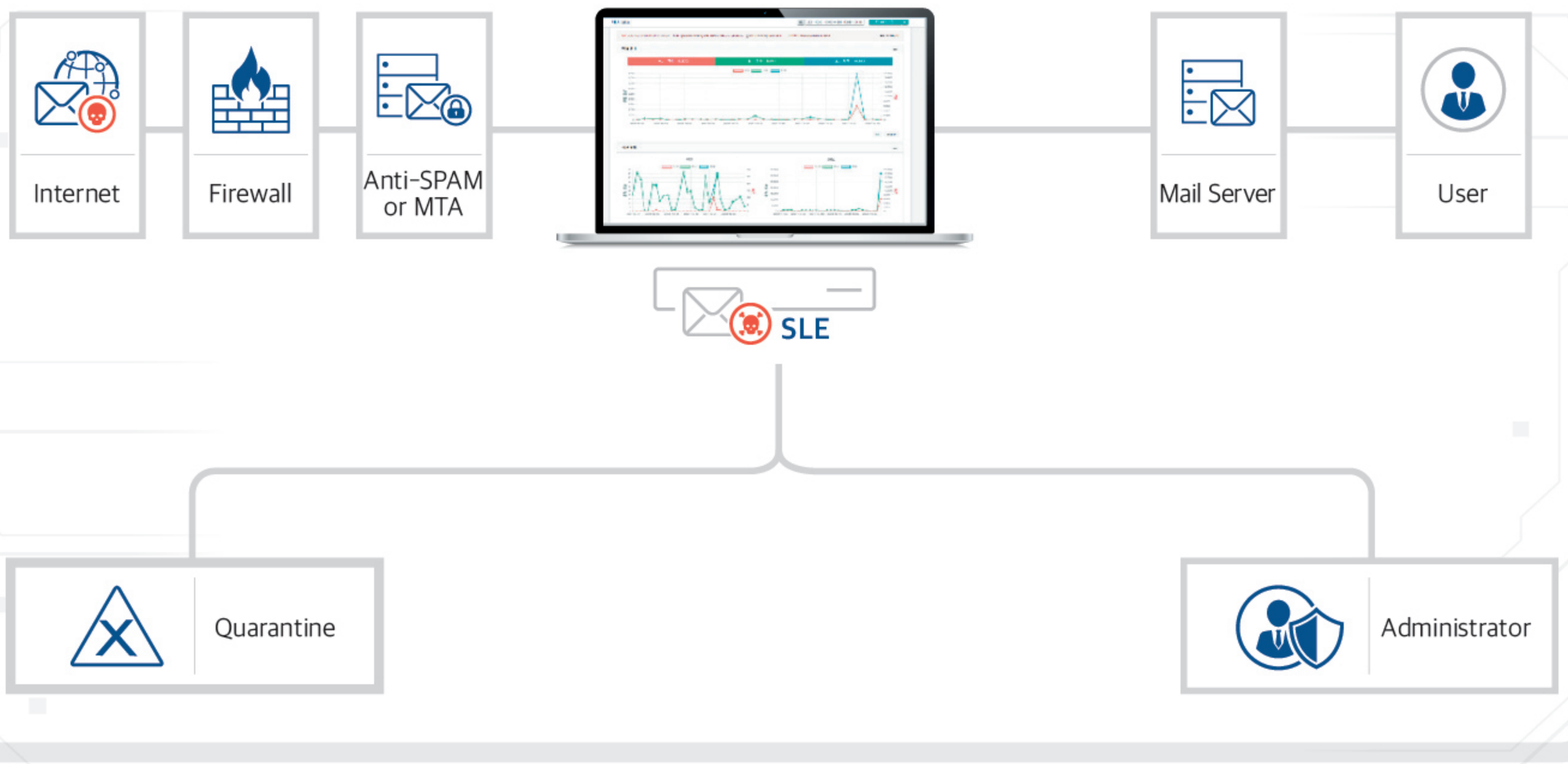
Eliminate potential threat in suspicious files

- Based on ZeroTrust CDR.
- Eliminate potential threats in documents without changing layout and reconstruct the files.

On-Premise

MARS SLE On-Premise Email Security

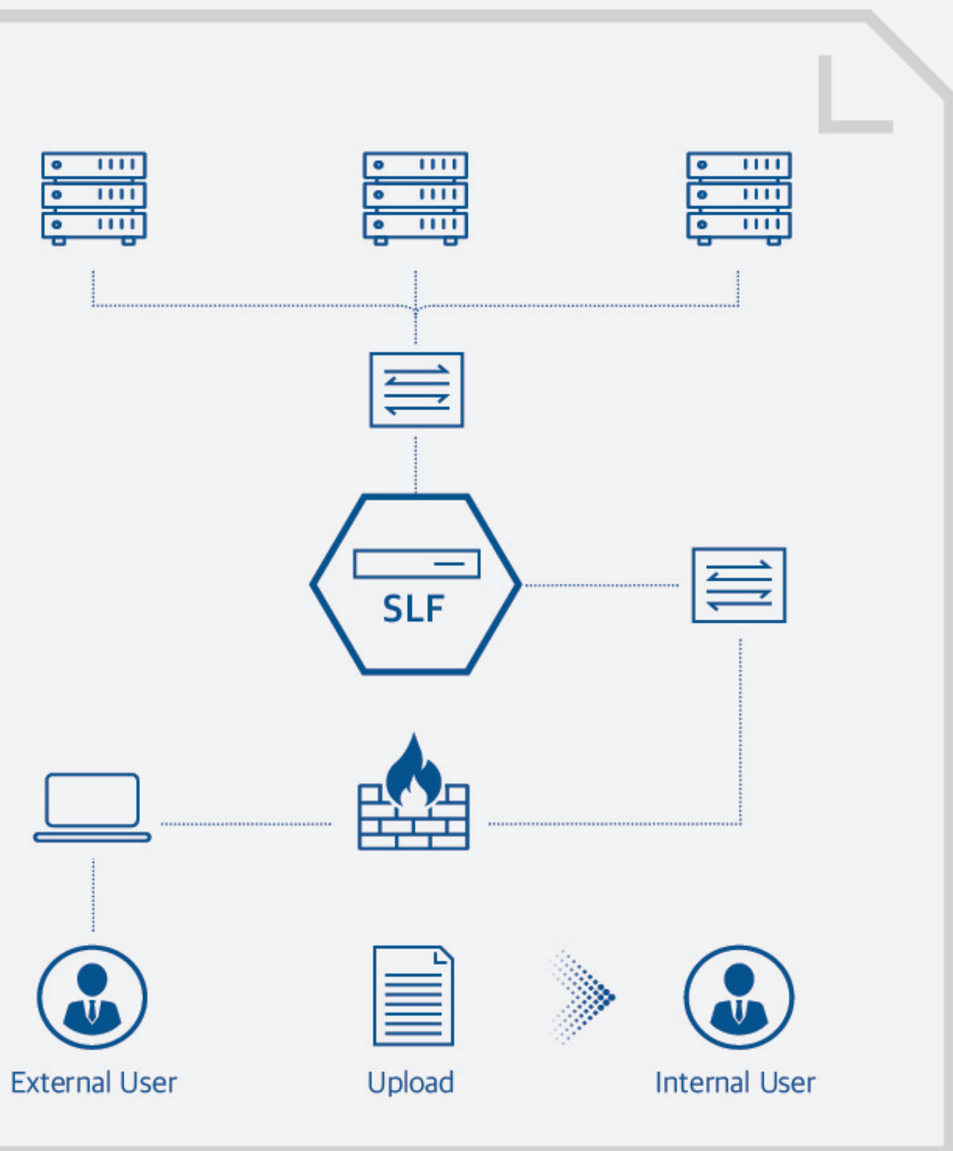
Pre-detects Sophisticated Malicious Code Hidden in the Email.



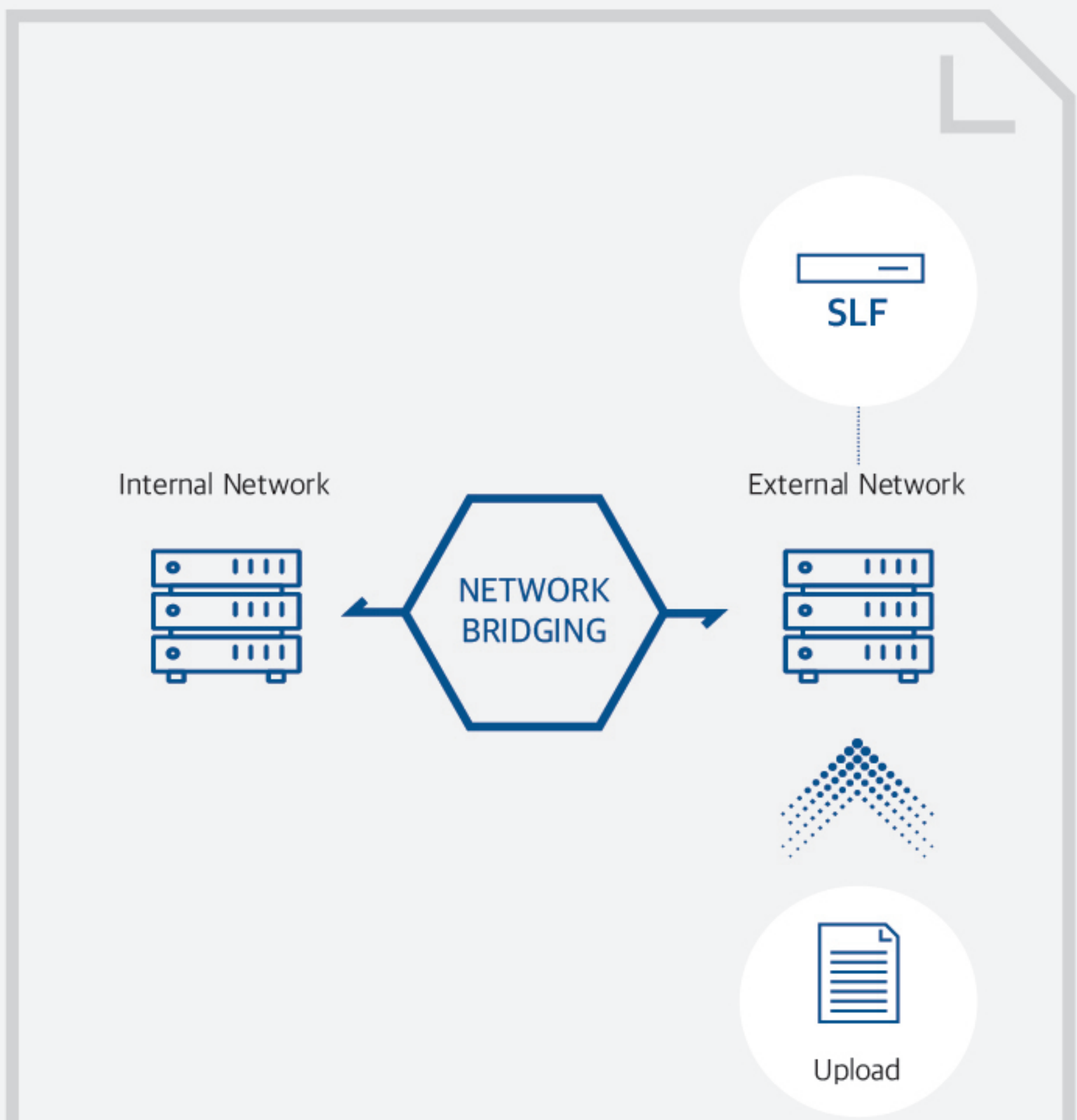
On-Premise

MARS SLF On-Premise File Security

Blocks Malicious File Inflow to Internal Information System.



Web Application Server



Network Airgap Environment

SECULETTER

SecuLetter Co., Ltd.

11 Geumto-ro 80beon-gil, Sujeong-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

T.+82.31.608.8860 I **F.**+82.31.608.8810 I **E.**global@seculetter.com I **global.seculetter.com**