SecuLetter File Security

Proactive Protection Against Advanced Cyber Threat

No files are trustable.
Protect your business from zero-day and everyday threats.
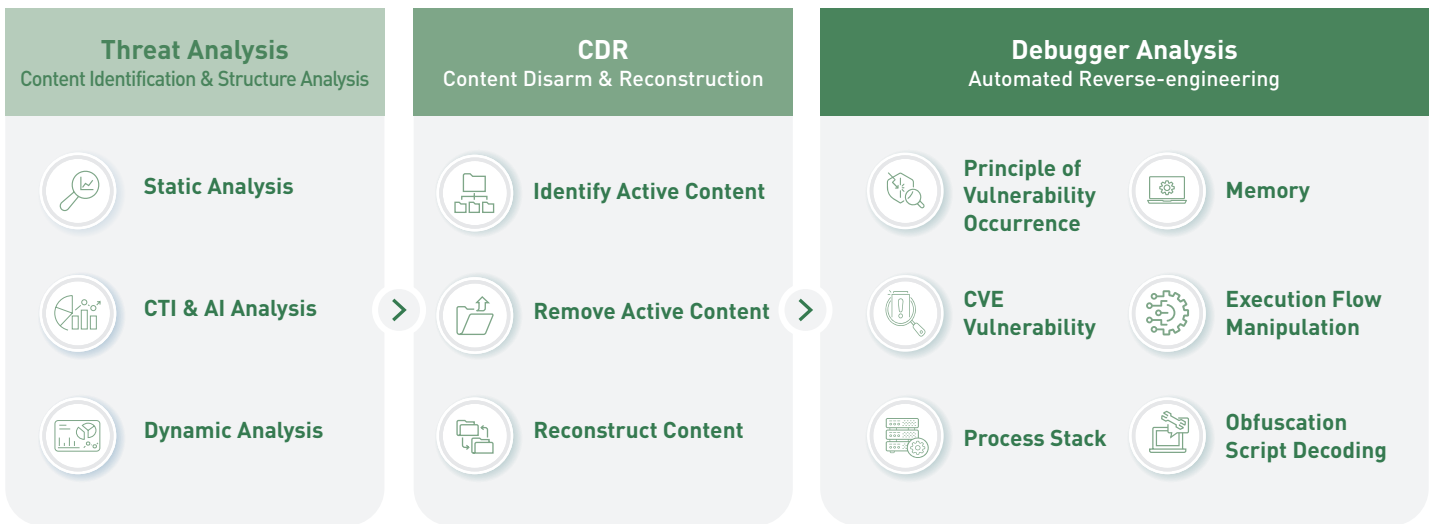
SLF
SecuLetter
File Security

SecuLetter File Security is a file-based malware security solution for advanced threat protection. It monitors the file from external to internal network and detects the malicious file including hidden threats. It proactively scans the file transferred to internal server and analyze the malicious content embedded in the file.

Automated Reverse-engineering
Assembly
Level Analysis

SecuLetter automated reverse-engineering covers the blind spot of existing APT protection solution. It conducts the entire process of reverse-engineering by analyzing file input, processing and output. Using automated reverse-engineering brings you the effect to have malware analyst to stop inflowing malicious code into your system before accident happens.

SecuLetter MARS Platform
Enhanced Standard Layers & Cutting-edge APT Protection Solution

Threat Analysis	CDR	Debugger Analysis
Content Identification & Structure Analysis	Content Disarm & Reconstruction	Automated Reverse-engineering
Static Analysis	Identify Active Content	Principle of Vulnerability Occurrence · Memory
CTI & AI Analysis	Remove Active Content	CVE Vulnerability · Execution Flow Manipulation
Dynamic Analysis	Reconstruct Content	Process Stack · Obfuscation Script Decoding

Competitive Advantage

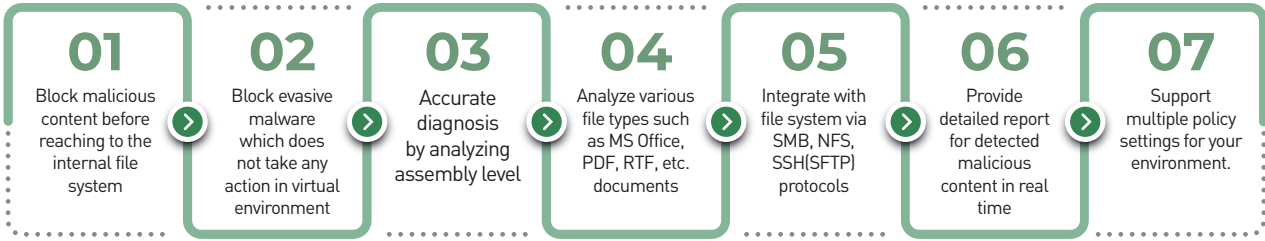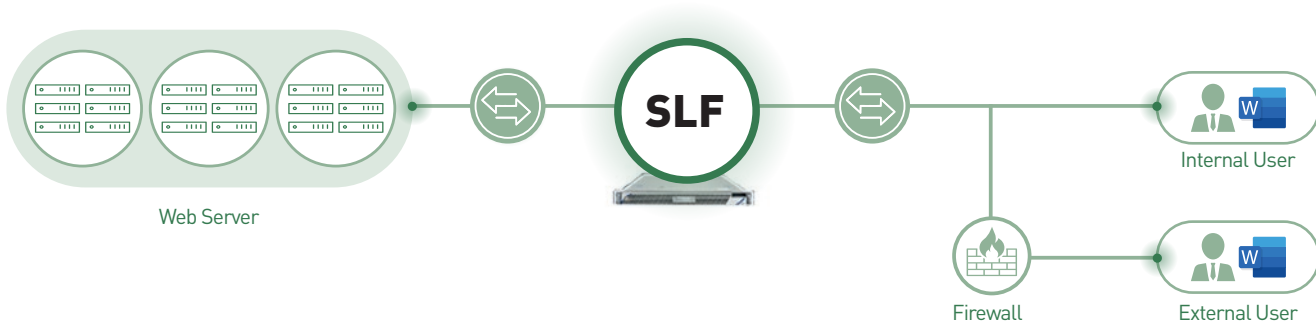| Neutralize Evasive Threats	Assembly Level Diagnosis	5 Times Faster
Accurate detection on file-borne malware with no behaviors.	Provide accurate diagnosis and reduce false positive/negative.	Reduce 80% diagnosis time than traditional APT solution.

Key Features

| 01	02	03	04	05	06	07
Block malicious content before reaching to the internal file system	Block evasive malware which does not take any action in virtual environment	Accurate diagnosis by analyzing assembly level	Analyze various file types such as MS Office, PDF, RTF, etc. documents	Integrate with file system via SMB, NFS, SSH(SFTP) protocols	Provide detailed report for detected malicious content in real time	Support multiple policy settings for your environment.

How It Works

● **Web Application Server**

Web Server · SLF · Internal User · Firewall · External User

> Prevent uploading malicious files to your company's bulletin board.
>
> Protect your company reputation by maintaining secured bulletin board.

● **Airgap Environment**

Data Transfer · External Network · NETWORK BRIDGING · Internal Network · Data Transfer · SLF
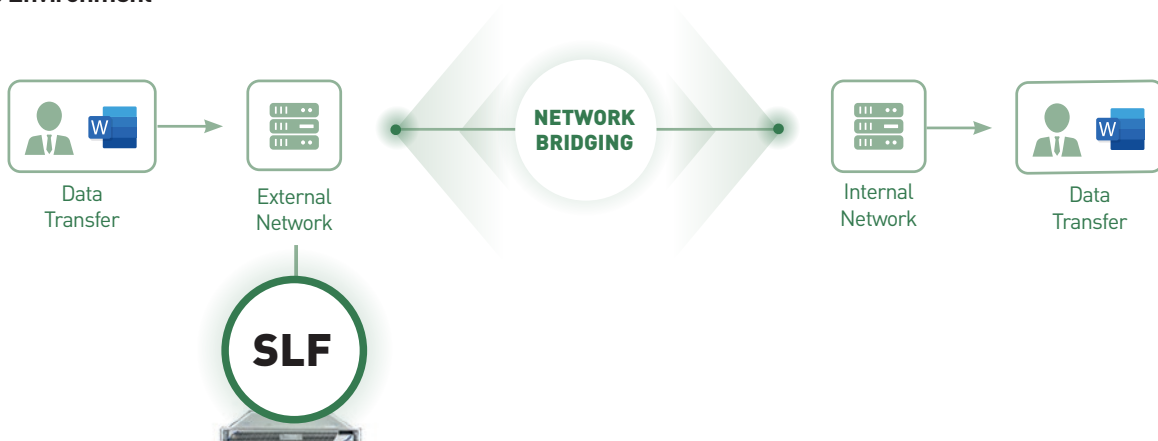
> Prevent spreading malicious files into internal file storage.
>
> Share documents without worrying about malicious code hidden in document.

SECULETTER