Where Files Become Safe.

WHY EXISTING SOLUTIONS ARE INSUFFICIENT

Most security tools only see the tip of the iceberg.

Traditional antivirus and EDR solutions stop only known threats using signatures. Sandboxes go a bit deeper, but still miss evasive and zero-day attacks that hide beneath the surface.

The real danger lies below.

Unknown and sophisticated threats remain undetected until they execute - unless you inspect them at the assembly code level.

Known Threats
(AV, EDR)

Unknown Threats
(Sandbox, Behavior-based Detection)

Unknow Threats
(Assembly-level Reverse Engineering)

This is where SecuLetter goes deeper.

With reverse engineering–based detection,
we uncover what AV, EDR, and sandboxing cannot,
delivering true protection against zero-day and file-borne attacks.

SecuLetter Technology

Used by hundreds of thousands of users worldwide, SecuLetter 's core engine is specially-built for securing content. It provides a multi-layered security pipeline, combining traditional threat analysis with the market's most advanced sandbox and Content Disarm and Reconstruction (CDR) technologies.

Content Analysis
(Known Threats)

Documents going into the SecuLetter's engine go through advanced static and dynamic analysis and are tested against a threat intelligence feed. Any known threats are likely to be caught and neutralized at this point.

	Static Analysis
	CTI & AI Analysis
	Dynamic Analysis

Deep Scan
(Unknown Threats)

SecuLetter detonates suspicious documents inside its advanced Content Sandbox. The sandbox runs applications while monitoring machine instructions in real time, detecting and blocking memory corruption, persistency, or VM evasion attempts before execution. Thanks to this architecture, scans are 5 times faster than legacy sandboxes.

Principle of Vulnerability Occurrence	Memory
CVE Vulnerability	Execution Flow Manipulation
Process Stack	Obfuscation Script Decoding

Content Disarm
and Reconstruct

SecuLetter applies its advanced CDR technology to remove active content hidden in documents like PDFs or Microsoft Office files. This may include macros, DDE/OLE objects, or scripts, with files rebuilt to ensure no exploits remain. Without a "blacklist" approach, CDR eliminates even zero-day exploits - all in milliseconds.

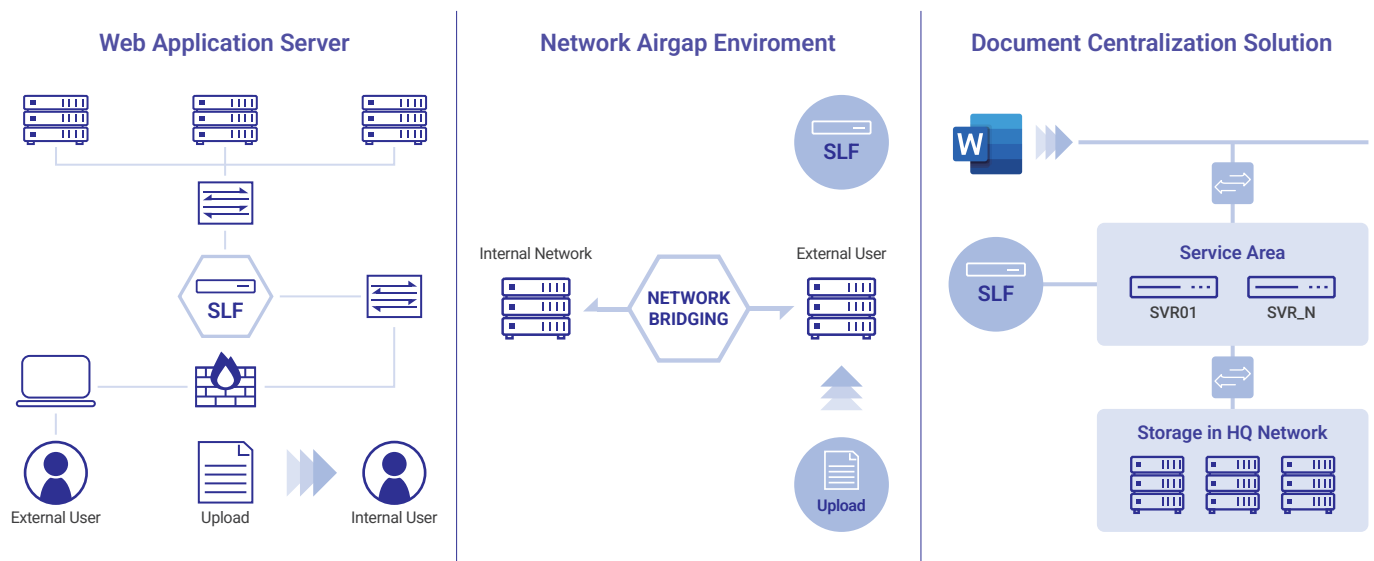|	
	Identify Active Content
	Remove Active Content
	Reconstruct Content

File Security

Needs

Securing Every File - Wherever It Comes From, However It's Used.

Channel	Web Upload	File Share	Internal Transfer
Enviroment	Air-gapped internal network	Web portal	Cross-network file transfer
	USB or removable media	File storage zones	Cloud File strorage
Industry	Government & Public Sector	Defense & Aerospace	R&D / Advanced Manufacturing
	Financial Services	Energy & Utilities	Pharma & Bio Research
Size	Mid to Large Enterprises	Global Corporations	Regulated Environments

Web Application Server

External User   Upload   Internal User

Network Airgap Enviroment

SLF

Internal Network   NETWORK BRIDGING   External User

Upload

Document Centralization Solution

SLF

Service Area
SVR01   SVR_N

Storage in HQ Network

Benefits

Secured uploads and file transfer
without breaking workflows - no sandbox, no delay

• Safe file transfers everywhere.
Protects web portals, file shares, storage zones, and cross-network gateways.

• Critical infrastructure ready.
Deployed in government, defense, energy, and R&D environments where internet isolation is mandatory.

• Disarms 300+ formats.
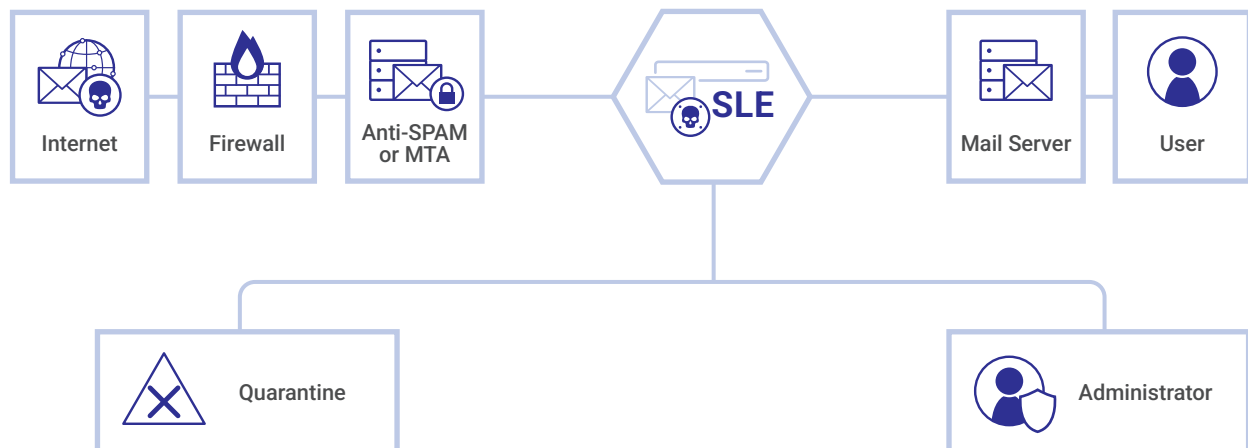Neutralizes exploits hidden in Office, PDF, CAD, archives, even encrypted or nested files.

Email Security

Needs

Defending Every Organization From Every Kind of Email Attack

Infrastructure	On-prem	M365	Google WS

	APT	Weaponized Attachment	BEC
Attack Vectors	Zero-day Exploits	Internal Phishing	Marco Malwave

	Commerce & Retail	Public Sector & Defense	Healthcare & Pharma
Industry	Financial Services	Academic	Manufacturing

Size	Enterprise	SMBs	Multinational

Inline Deplayemnt

Internet — Firewall — Anti-SPAM or MTA — **SLE** — Mail Server — User

Quarantine

Administrator

Benefits

Blocked what SEG missed.
Delivered only clean, safe emails - before users even click.

- **Real-time email defense :**
  Catch what SEGs miss: zero-day exploits, macro malware, and lateral phishing.
- **Seamless user experience.**
  Clean emails delivered instantly with no sandbox delays, no end-user disruption.
- **Flexible deployment.**
 On-prem SEG (SLE), lightweight inline (SLES), or Microsoft 365-native ICES (DISARM).

■ Product Lineup

Email Security	Appliance	**SLE (Secure Email Gateway)** Entry : SLE1000 Middle : SLE3000 High-end : SLE5000
	SaaS (per User)	**SLES (Data-center Hosting)**
		DISARM (M365, Gmail)
File Security	Appliance	**SLF (Secure File Gateway)** Entry : SLF450 Middle : SLF900 High-end : SLF1800
		SLCDR (Content Disarm and Reconstruction) Entry : SLCDR450 Middle : SLCDR900 High-end : SLCDR1800

■ Technology Partner

SecuLetter works with global security vendors, OEMs, and technology leaders to enhance and differentiate their offerings across Secure Email Gateways, Firewalls, Web Gateways, and DLP platforms.
By integrating SecuLetter's reverse engineering–based detection and content disarm technologies through APIs or appliances, partners can deliver faster, more accurate, and cost-efficient protection against advanced file-borne and email-borne threats.

Partner Solution
(SEG / Firewall / Gateway) → **API Integration** → **SecuLetter Engine / Cloud**
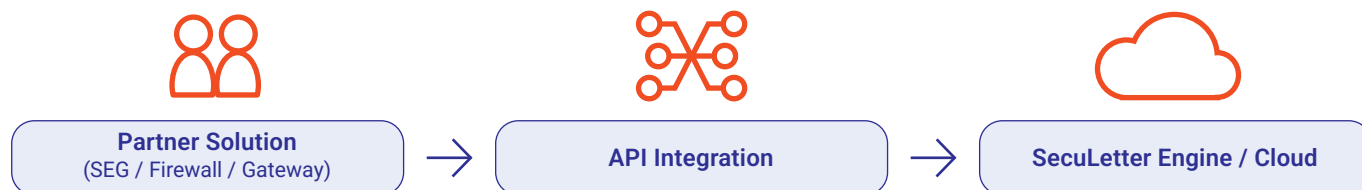
■ DISTRIBUTOR / RESELLER

SecuLetter is available worldwide through a trusted network of distributors and resellers. Our partners provide regional expertise, integration services, and ongoing support, ensuring enterprises and government agencies benefit from enterprise-grade protection tailored to their local compliance requirements.

Local Presence :
Regional distributors across APAC, EMEA, and North America

Value-Added Services :
Deployment, integration, and managed security offerings

Industry Focus :
Government, defense, finance, manufacturing, and critical infrastructure

SECULETTER