SecuLetter Email Security

การป้องกันเชิงรุกต่อภัยคุกคามทางไซเบอร์ขั้นสูง

การโจมตีทางไซเบอร์มากกว่า 91% เริ่มต้นจากอีเมล
ปกป้องธุรกิจของคุณจากภัยคุกคามแบบซีโร่เดย์ และภัยคุกคามอื่นๆในทุกๆวัน

SLE
SecuLetter
Email Security

SecuLetter ให้การรักษาความปลอดภัยอีเมลรุ่นใหม่สำหรับการป้องกัน (APT) Advanced Persistent Threat)
SecuLetter Email Security ใช้การป้องกันหลายชั้นพร้อมรูปแบบการวิเคราะห์วิศวกรรมย้อนกลับแบบอัตโนมัติ (automated reverse-engineering) และมอบความสามารถในการตรวจจับ APT แบบถาวร เพื่อป้องกันภัยคุกคามขั้นสูงที่เกิดจากอีเมล

Automated Reverse-engineering
Assembly
Level Analysis

Automated reverse-engineering ของ SecuLetter ครอบคลุมจุดบอดของโซลูชันการป้องกัน APT ที่มีอยู่ในปัจจุบัน โดยจะดำเนินการกระบวนการ reverse-engineering ทั้งหมดโดยการวิเคราะห์ input, processing และ output ของไฟล์ การใช้ automated reverse-engineering ทำให้เสมือนมีนักวิเคราะห์มัลแวร์ช่วยหยุดการแทรกซึมของโค้ดที่เป็นอันตรายเข้าสู่ระบบของคุณก่อนที่ภัยคุกคามจะเกิดขึ้น

SecuLetter MARS Platform

Enhanced Standard Layers & Cutting-edge APT Protection Solution

Threat Analysis
Content Identification & Structure Analysis

- Static Analysis
- CTI & AI Analysis
- Dynamic Analysis

CDR
Content Disarm & Reconstruction

- Identify Active Content
- Remove Active Content
- Reconstruct Content

Debugger Analysis
Automated Reverse-engineering

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

Competitive Advantage

ปราบปรามภัยคุกคามที่หลบหลีกการตรวจจับ	การวิเคราะห์ ในระดับ Assembly	เร็วกว่า 5 เท่า
ตรวจจับมัลแวร์หลบซ่อนที่เกิดจากไฟล์อย่างแม่นยำ	ให้การวินิจฉัยที่แม่นยำ และลด false positive/negative	ลดเวลาการวินิจฉัยลง 80% เมื่อเทียบกับโซลูชัน APT แบบเดิม

Key Features

01 ตรวจจับและบล็อกอีเมลที่เป็นอันตราย

02 วิเคราะห์โค้ดที่เป็นอันตรายที่ซ่อนอยู่ในไฟล์ที่แนบมากับอีเมล

03 สามารถดาวน์โหลดไฟล์สแกนได้จากลิงก์ URL ที่อยู่ในอีเมล

04 วิเคราะห์ไฟล์ที่เป็นอันตรายซึ่งรวมอยู่ในไฟล์ที่ป้องกันด้วยรหัสผ่าน

05 กักกันและกักเก็บอีเมลอันตรายที่ตรวจพบอย่างถาวร

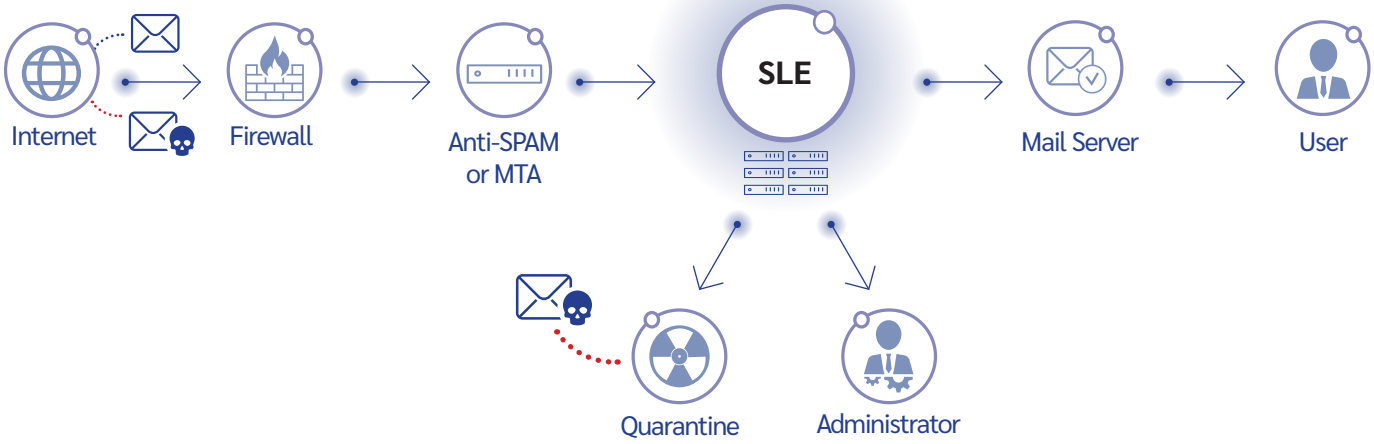
06 แจ้งเตือนถึงผู้ดูแลระบบและผู้รับเมื่อตรวจพบอีเมลที่เป็นอันตราย

07 จัดทำรายงานสำหรับเนื้อหาที่เป็นอันตรายที่ตรวจพบแบบเรียลไทม์โดยละเอียด

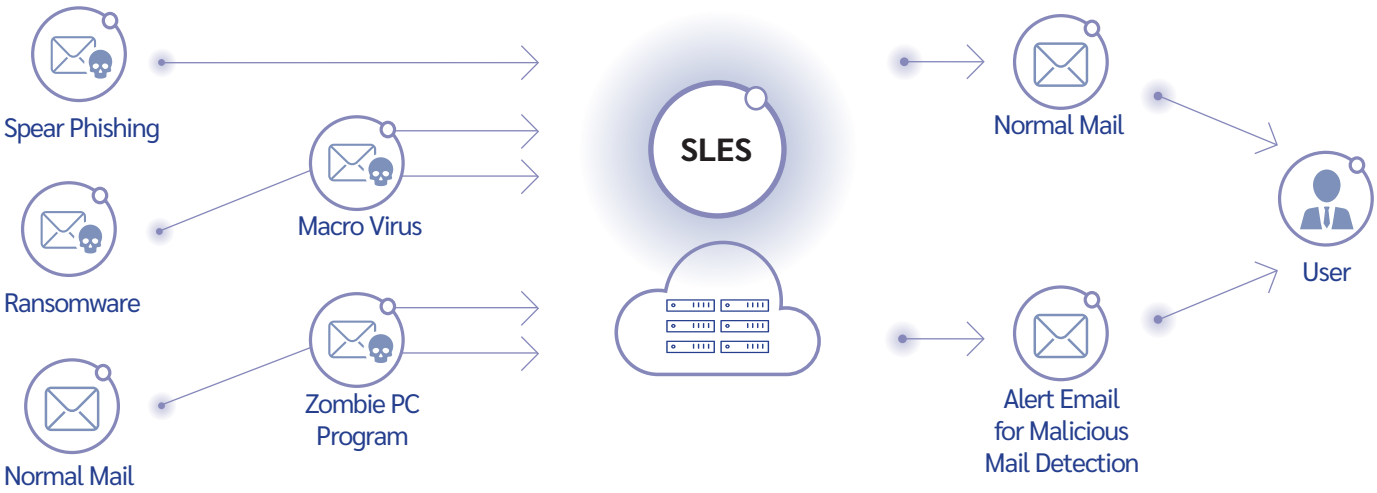
08 รองรับการตั้งค่านโยบายหลายรายการให้เข้ากับสภาพแวดล้อมของคุณ

How It Works

- **On-premise Edition สำหรับองค์กรที่ใช้งานอีเมลแบบ In-house Mail Server**



- **Cloud Edition สำหรับผู้ใช้อีเมลทั่วไป**



SecuLetter Co., Ltd.
14F, PangyoInnovationLab, 422-1, Gumto-dong, Sujeong-gu, Seongnam-si, Gyeonggi-do, South Korea 461380

SECULETTER

global.seculetter.com global@seculetter.com

SecuLetter File Security

การป้องกันเชิงรุกต่อภัยคุกคามทางไซเบอร์ขั้นสูง

ไม่มีไฟล์ใดที่เชื่อถือได้
ปกป้องธุรกิจของคุณจากภัยคุกคามแบบซีโร่เดย์และและภัยคุกคามอื่นๆ ในทุกๆวัน

SLE
SecuLetter
File Security

SecuLetter File Security เป็นโซลูชันรักษาความปลอดภัยมัลแวร์แบบ file-based สำหรับการป้องกันภัยคุกคามขั้นสูง โดยจะตรวจสอบไฟล์จากเครือข่ายภายนอกสู่ภายใน และตรวจจับไฟล์ที่เป็นอันตราย รวมถึงภัยคุกคามที่ซ่อนอยู่ โดยจะสแกนไฟล์ที่ถ่ายโอนไปยังเซิร์ฟเวอร์ภายในแบบเชิงรุก และวิเคราะห์เนื้อหาที่เป็นอันตรายที่ฝังอยู่ในไฟล์

Automated Reverse-engineering
Assembly
Level Analysis

Automated reverse-engineering ของ SecuLetter ครอบคลุมจุดบอดของโซลูชันการป้องกัน APT ที่มีอยู่ในปัจจุบัน โดยจะดำเนินการกระบวนการ reverse-engineering ทั้งหมดโดยการวิเคราะห์ input, processing และ output ของไฟล์ การใช้ automated reverse-engineering ทำให้ เสมือนได้รับการมีนักวิเคราะห์มัลแวร์ช่วยหยุดการแทรกซึมของโค้ดที่เป็นอันตรายเข้าสู่ระบบของคุณก่อนที่ภัยคุกคามจะเกิดขึ้น

SecuLetter MARS Platform

Enhanced Standard Layers & Cutting-edge APT Protection Solution

Threat Analysis
Content Identification & Structure Analysis

- Static Analysis
- CTI & AI Analysis
- Dynamic Analysis

CDR
Content Disarm & Reconstruction

- Identify Active Content
- Remove Active Content
- Reconstruct Content

Debugger Analysis
Automated Reverse-engineering

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

Competitive Advantage

ปราบปรามภัยคุกคามที่หลบหลีกการตรวจจับ	การวิเคราะห์ ในระดับ Assembly	เร็วกว่า 5 เท่า
ตรวจจับมัลแวร์หลบซ่อนที่เกิดจากไฟล์อย่างแม่นยำ	ให้การวินิจฉัยที่แม่นยำ และลด false positive/negative	ลดเวลาการวินิจฉัยลง 80% เมื่อเทียบกับโซลูชัน APT แบบเดิม

Key Features

01 บล็อกเนื้อหาที่เป็นอันตรายก่อนที่จะเข้าถึงระบบไฟล์ภายใน

02 บล็อกมัลแวร์ที่หลบเลี่ยงซึ่งไม่ได้มีการ active ใดๆ ใน virtual environment

03 การวินิจฉัยที่แม่นยำโดยการวิเคราะห์ที่ระดับ Assembly

04 วิเคราะห์ไฟล์ประเภทต่างๆ เช่น เอกสาร MS Office, PDF, RTF ฯลฯ

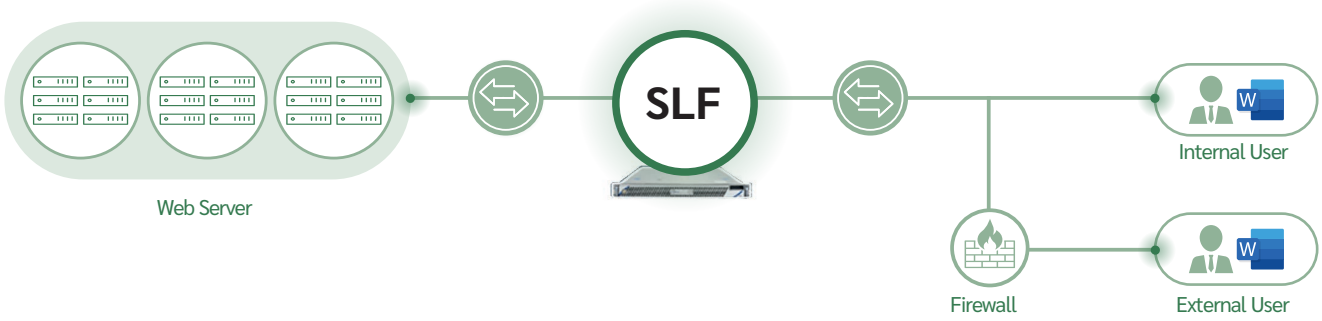
05 Integrate กับระบบไฟล์ผ่านโปรโตคอล SMB, NFS, SSH (SFTP)

06 จัดทำรายงานโดยละเอียดสำหรับเนื้อหาที่เป็นอันตรายที่ตรวจพบแบบเรียลไทม์

07 รองรับการตั้งค่านโยบายหลายรายการให้ตรงกับสภาพแวดล้อมของคุณ

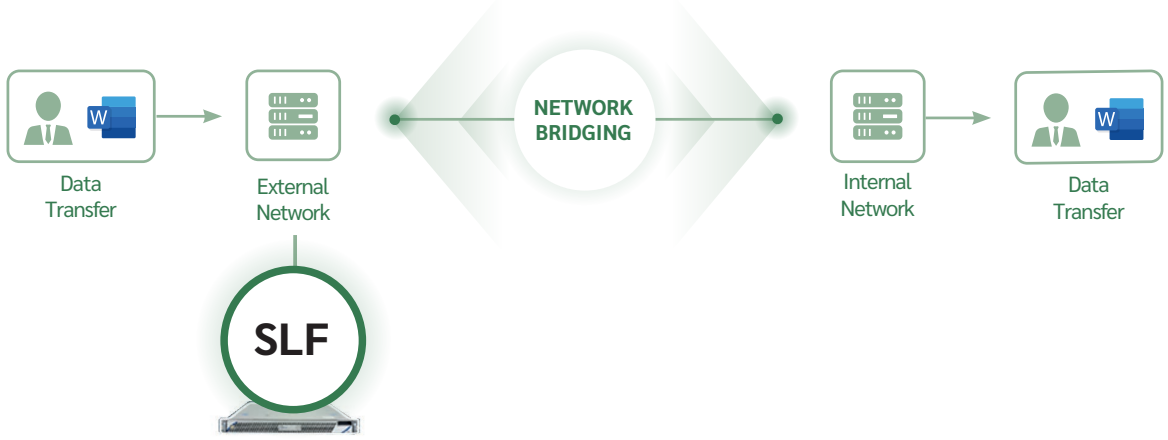
How It Works

- **Web Application Server**



- ป้องกันการอัปโหลดไฟล์ที่เป็นอันตรายไปยังระบบกระดานข่าวของบริษัทของคุณ
- ปกป้องชื่อเสียงของบริษัทของคุณด้วยการรักษาระบบกระดานข่าวที่ปลอดภัย

- **Airgap Environment**



- ป้องกันการแพร่กระจายไฟล์ที่เป็นอันตรายไปยังที่จัดเก็บไฟล์ภายใน
- แบ่งปันเอกสารโดยไม่ต้องกังวลว่าจะมีโค้ดที่เป็นอันตรายซ่อนอยู่ในเอกสาร

SecuLetter Co., Ltd.
14F, PangyoInnovationLab, 422-1, Gumto-dong, Sujeong-gu, Seongnam-si,
Gyeonggi-do, South Korea 461380

global.seculetter.com global@seculetter.com

SECULETTER

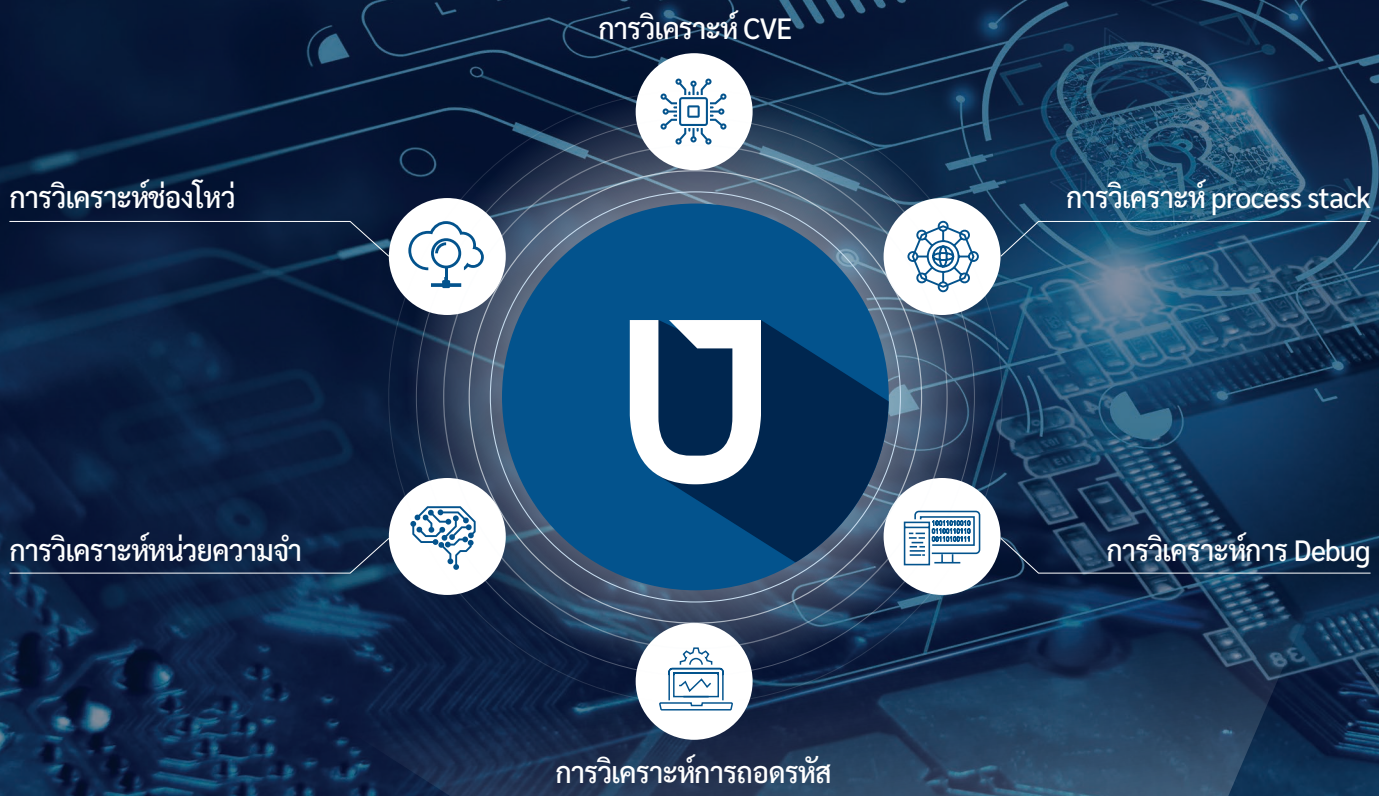
global.seculetter.com

การตรวจจับภัยคุกคามที่ไม่รู้จักภายใน 20 วินาที

SecuLetter Solution Guide

SECULETTER

Automated Reverse-engineering



MARS PLATFORM

โซลูชันการป้องกัน APT ที่มีการเสริมความแข็งแกร่ง และล้ำสมัย

MARS S Static Analysis
กรองไฟล์ที่เป็นอันตรายที่ไหลเข้ามาด้วยการวินิจฉัยตาม signature

MARS R Reverse-engineering
ตรวจสอบกระบวนการอินพุต/เอาท์พุตของไฟล์ด้วย reverse-engineering เพื่อตรวจจับและบล็อกภัยคุกคาม

MARS D Dynamic Analysis
ระบุและวินิจฉัยพฤติกรรมที่ผิดปกติเมื่อเข้าถึง CPU หน่วยความจำ ไฟล์และเครือข่าย

MARS CTI Threat Intelligence
วินิจฉัยภัยคุกคามที่อาจเกิดขึ้นหรือเกิดขึ้นแล้วโดยแหล่งข่าวกรองภัยคุกคาม

MARS CDR
Content Disarm & Reconstruction
แก้ไขไฟล์ที่มีเนื้อหาที่เป็นอันตราย และสร้างใหม่

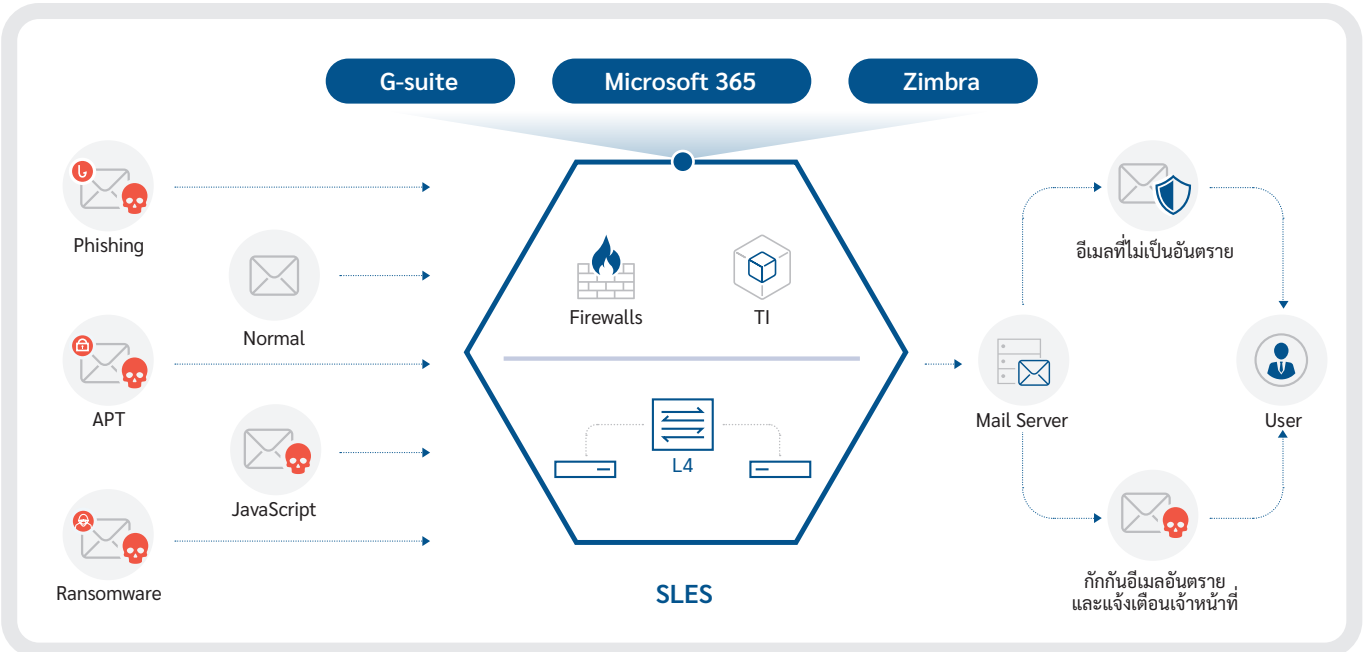
MARS AI
Machine Learning Algorithm
วินิจฉัยสถานะที่เป็นอันตรายของไฟล์โดยใช้ machine learning algorithm

	Reverse- engineering		Threath Protection แบบเดิม
ตรวจจับได้เร็วกว่า	ประมาน 20 วินาที	ความเร็วในการสแกน	3-5 นาที
แม่นยำกว่า	ระดับ Assembly	การมองเห็น	ระดับ Application
มีประสิทธิภาพมากกว่า	รองรับ	เทคนิคการปองกันการหลบหลีก	รองรับบางส่วน

Cloud

MARS SLES Email Security for Microsoft 365

Email Security as a Service สำหรับ Public Cloud Email.



*รองรับการทำางานร่วมกับบริการอีเมลบนคลาวด์สาธารณะอื่นๆ

Cloud

MARS SLCDR Content Disarm & Reconstruction

กำาจัดภัยคุกคามในไฟล์ เช่น JS, URL, Shellcode และสร้างไฟล์ใหม่ที่ปลอดภัยกว่า

สแกนไฟล์ → วิเคราะห์เนื้อหา → แยกเนื้อหาที่ไม่ดีออก → ส้รางไฟล์ใหม่ที่ปลอดภัย

ลดผลกระทบที่อาจเกิดขึ้นกับงาน

ไม่ก่อให้เกิดการหยุดชะงักของกระบวนการทางธุรกิจขององค์กร และลบเนื้อหาที่เป็นอันตรายที่อาจเกิดขึ้นซึ่งรวมอยู่ในไฟล์

กำจัดภัยคุกคามที่อาจเกิดขึ้นแบบเชิงรุก

แยกเนื้อหาที่เป็น active content ซึ่งสามารถใช้เป็นวิธีการโจมตีและบรรจุเนื้อหาใหม่ลงในไฟล์เอกสารที่ปลอดภัย

การส งทีปลอดภัยและรวดเร็ว

Seculetter CDRมอบไฟล์ที่ปลอดภัยโดยการลบเนื้อหาที่อันตราย และลดความล่าช้าของโซลูชันแซนด์บ็อกซ์แบบเดิม

Cloud

MARS DEFENDER File Analysis Service

มีไฟล์ต้องสงสัยอยู่หรือไม่ ทดลอง MARS Platform แบบ online service ฟรี.

พิจารณาว่าไฟล์ที่น่าสงสัยเป็นอันตรายหรือไม่

- เทคนิคการวิเคราะห์โดยใช้ซอฟต์แวร์ Reverse engineering .
- ตรวจจับไฟล์เอกสารที่เป็นอันตรายและอาจถูกใช้ในการแฮ๊ค.

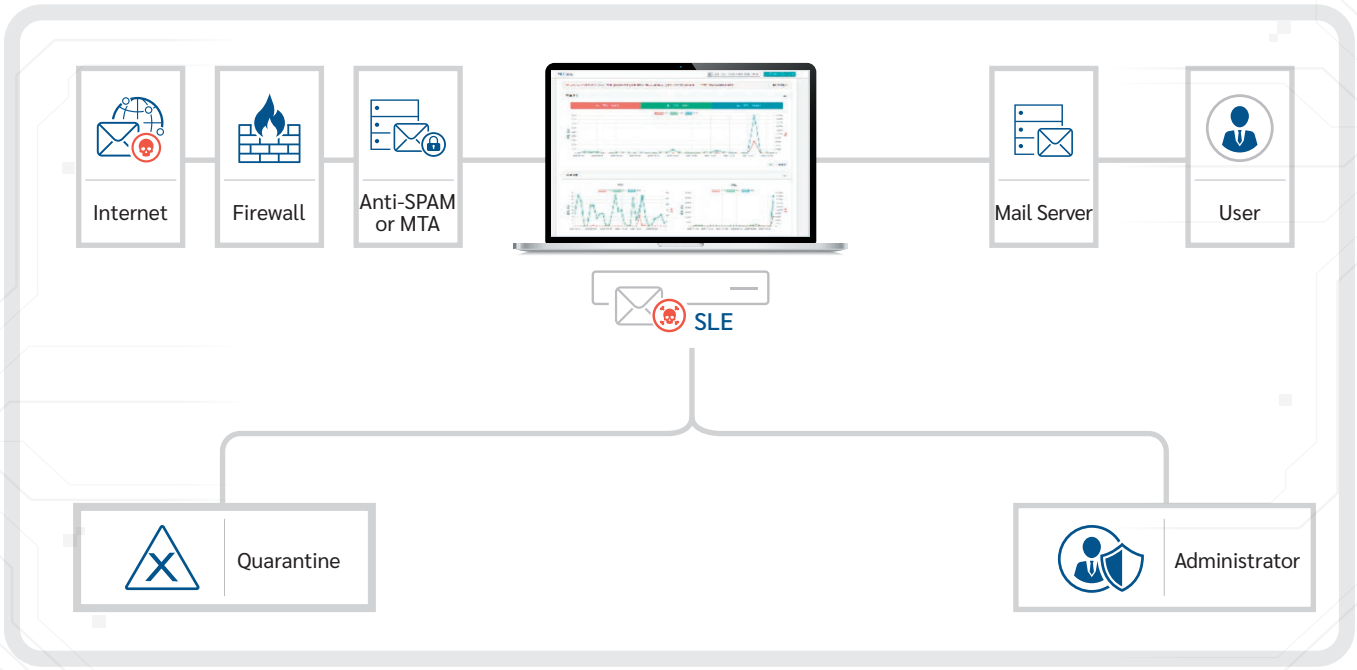
ลบภัยคุกคามในไฟล์ที่น่าสงสัย

- วิเคราะห์จาก ZeroTrust CDR.
- ลบภัยคุกคามในเอกสารโดยไม่ต้องเปลี่ยน layout และสร้างไฟล์ขึ้นมาใหม่

On-Premise

MARS SLE On-Premise Email Security

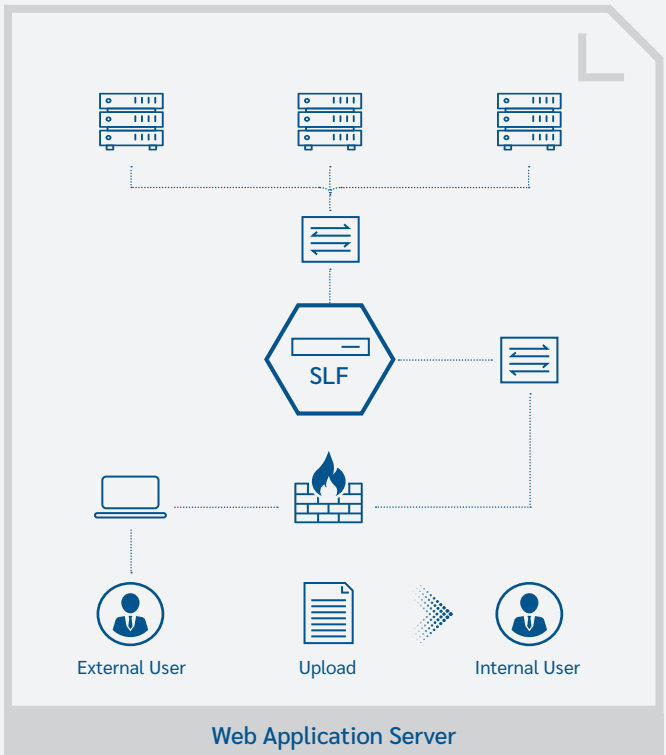
ตรวจจับโค้ดซับซ้อนที่เป็นอันตรายที่ซ่อนอยู่ในอีเมลล่วงหน้า.



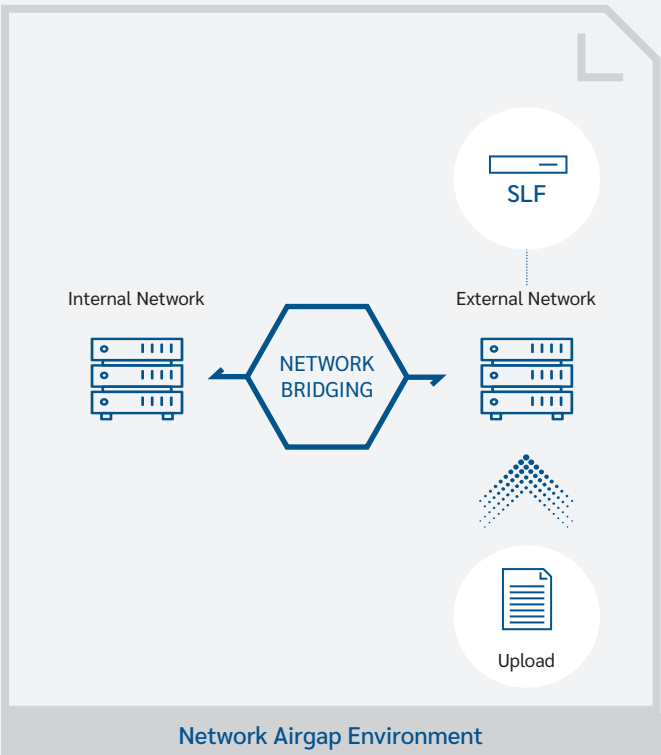
On-Premise

MARS SLF On-Premise File Security

บล๊อคไฟล์อันตรายไม่ให้เข้าสู่ระบบข้อมูลภายใน.



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