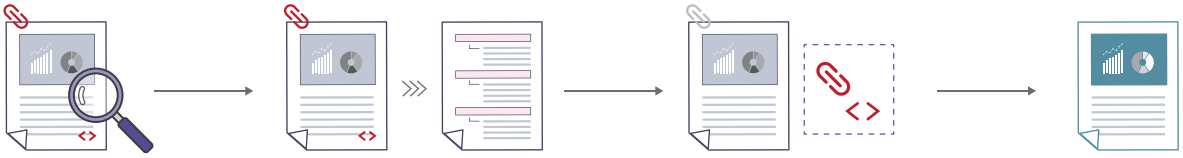
SHIELDEX

Preemptive response to document-type malicious code
File sanitization solution by removing potential threats

- CDR (Content Disarm & Reconstruction) technology that completes removal of suspicious elements in document content
- Sanitizes all malicious document files coming from outside, e-mail, USB, and network separation servers
- Allows only safe files that are made up of clean content in the original format

- Increasing cyber threats by disguising and concealing malicious code via document files
- Inflowing of malicious code through various channels such as e-mail attachments and Internet download files
- More attacks by evading existing technology (vaccines, sandbox detection, etc.) in a highly intelligent way
- Potential threats to files coming from outside for business collaboration, even in a network separation environment



Format Verification

Inspect the structure of document header

Structure Analysis

Verify the structure of all document components such as text, shapes,pictures, tables, etc.

Component Extraction

Extract only the safe components and remove all potentially malicious content

Reconstruction Verification

Reconstruct the documents only with safe components extracted

High-quality CDR technology

Self-development of CDR technology with technology specialized in document security for more than 21 years

Implementing high-quality of document CDR technology with years of deployment experience

Responds to document malware threats

Increasing document-based threats like ransomware, APT attacks

Optimized for unknown malware, zero-day attack

SHIELDEX

Establish Clean Zone of document file

CDR all incoming files even in a network separation environment

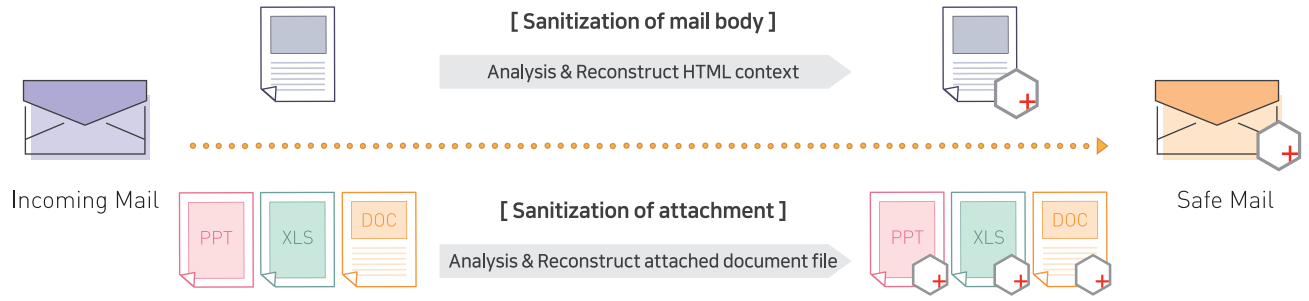
Ensure safety and security by allowing only clean document files into the internal network

Supports diverse cloud environments

Flexible deployment to suit each cloud environment

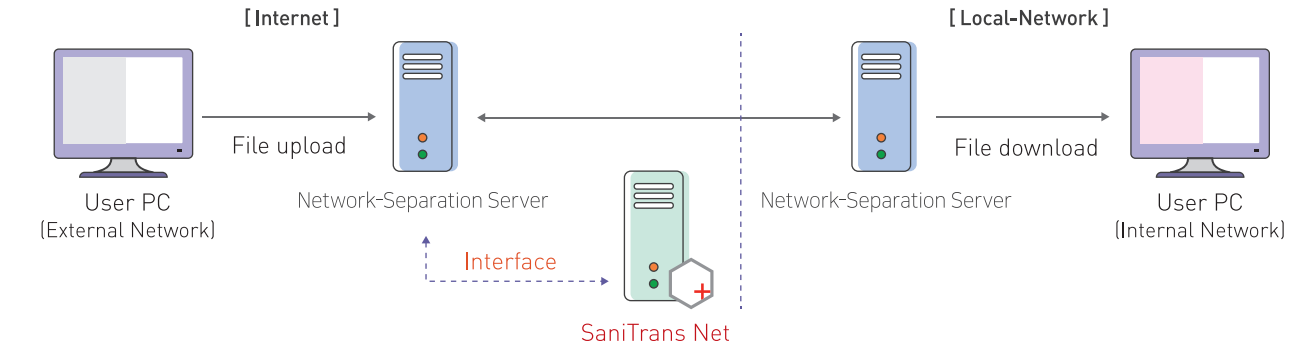
Ability to adapts to local cloud environments

SHIELDEX SaniTrans Mail



Sanitize Mail body	Verify Script, Hyper Link, Linked Image in HTML body
Sanitize Attachment	Analysis and reconstruct the attached file in the original format
Provide result reports	Provide CDR process results that verify details such as malicious files and macro removal

SHIELDEX SaniTrans Net



Optimized for network separation environment	Sanitize files flowing through the network Enhance security of network separation environment
Introduce Self Module	All-in-one product mount self-developed network link module Maintain internet isolation status
Strengthen network separation security system	Interlink with document transfer authorization system Only permit files that are approved by the administrator

Gartner's Suggestion for Next Generation Technology

According to Gartner's report, current APT response technology is in a dilemma, and instead of relying on analysis using sandboxes, companies should be trying new ideas, like content disarm and reconstruction (CDR). (2017.02)

Unlike malware analysis, CDR technology does not determine or detect malware's functionality but removes all file components that are not approved within the system's definitions and policies.