Introduction of CDR

(Content Disarm & Reconstruction)

2018

JIRANSECURITY

1. CDR Engine, SaniTOX

Contents Malware Disarm Engine

SaniTOX

www.jiransecurity.com/products/docuz

- CDR source technology, which was self-developed by JiranSecurity
- Perfectly blocks ransomware/malware/APT and Zero-Day attacks in document files
- Able to respond to security threats in all directions that come through various channels(e-mail, web mail, file server, endpoint, etc.)
- Supports various document file formats such as MS Office, PDF and HWP, providing a security environment optimized for domestic enterprises

*SaniTOX is a **content malware disarm SDK** that fundamentally removes executable active contents(Macro, JavaScript, etc.) in document files through its **own developed CDR* source technology**. Eliminates all active contents coming through the document to fundamentally prevent all the threats that are vulnerable to unknown security as well as ransomware, malware and APT.*

Product Features

Macro/script disarm

Fundamental removal of security threats through documents by eliminating active contents such as Macro, JavaScript, etc., included in the document

Supports various user environments

Response in all directions available by supporting various environments which may expose the user to security threats such as e-mail, web mail, file server, end point, etc.

Detection of abnormal formats

Protection of the user from security threats by detecting document formats and conducting file recombination on any abnormal formats

Supports various document file formats

Blocks security threats coming through documents by supporting not only PDF, MS Office 2003, MS Office 2007+ but also HWP format

2. System Environments

Supported environments and file formats

Supported OS

- CentOS 6, 7 / 64bit
- Python 2.6 / 2.7
- CLI Support (exe file)

Supported files

- MS Office 2003 / 2007+
- HWP
- PDF
- ZIP
- RTF
- Image(JPG, JPEG, PNG, TIFF, BMP, PPM, GIF)

Contents \ File format	MS Office 2003	MS Office 2007+	PDF	Image
Macro	○	○	-	-
JavaScript	-	-	○	○
Flash	○	○	○	○
Attachments	○	○	○	-
OLE Object	○	○	-	-
Active X	○	○	-	-
Embedded Doc	○	○	○	-
Hyperlink	○	○	○	○

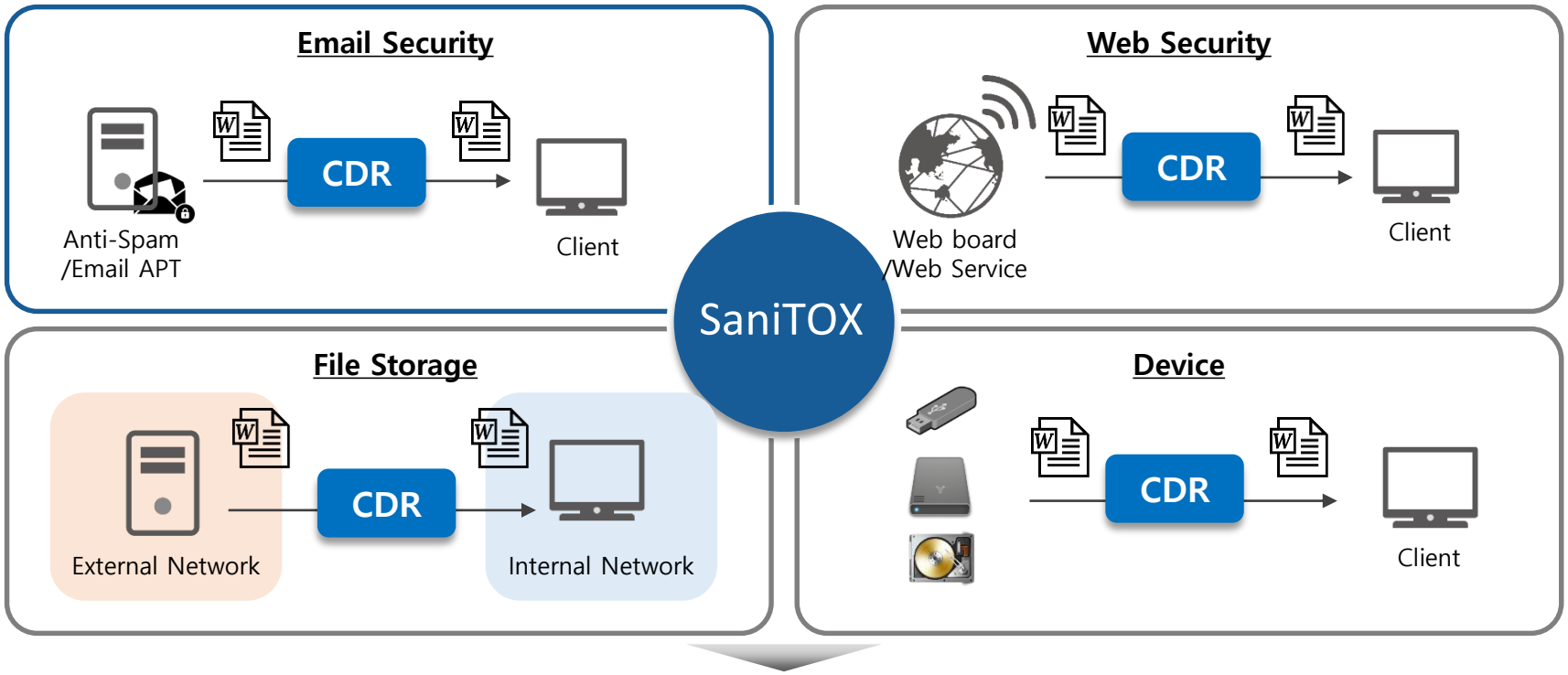
Deployment Options

SDK
We support CDR Software Development Kit.

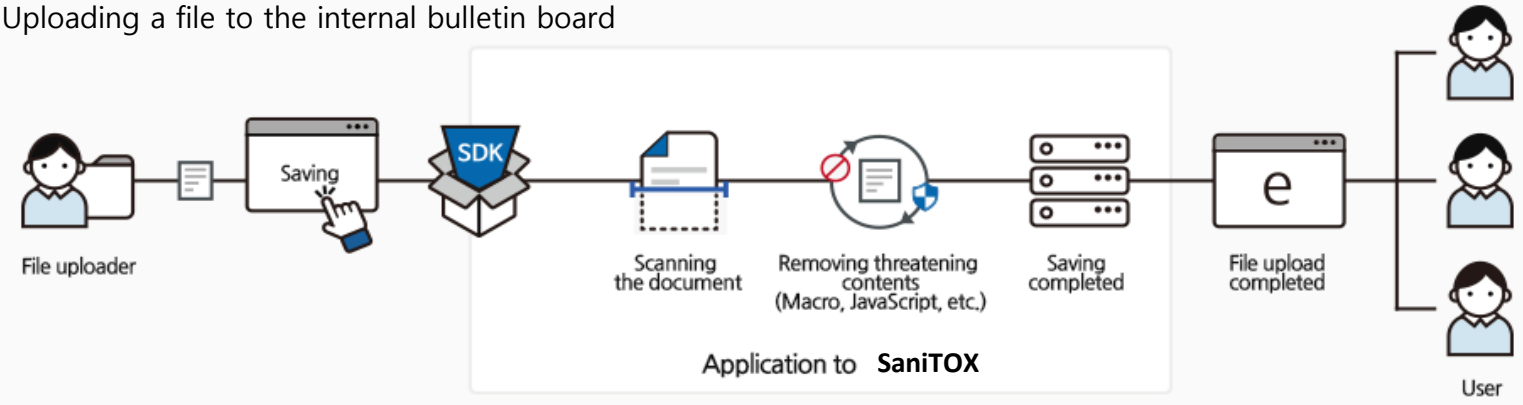
Appliance
Scheduled for release in Q1 2017.
(for Korea, Japan)

Cloud
We plan to support our services through the cloud.

3. Use Case

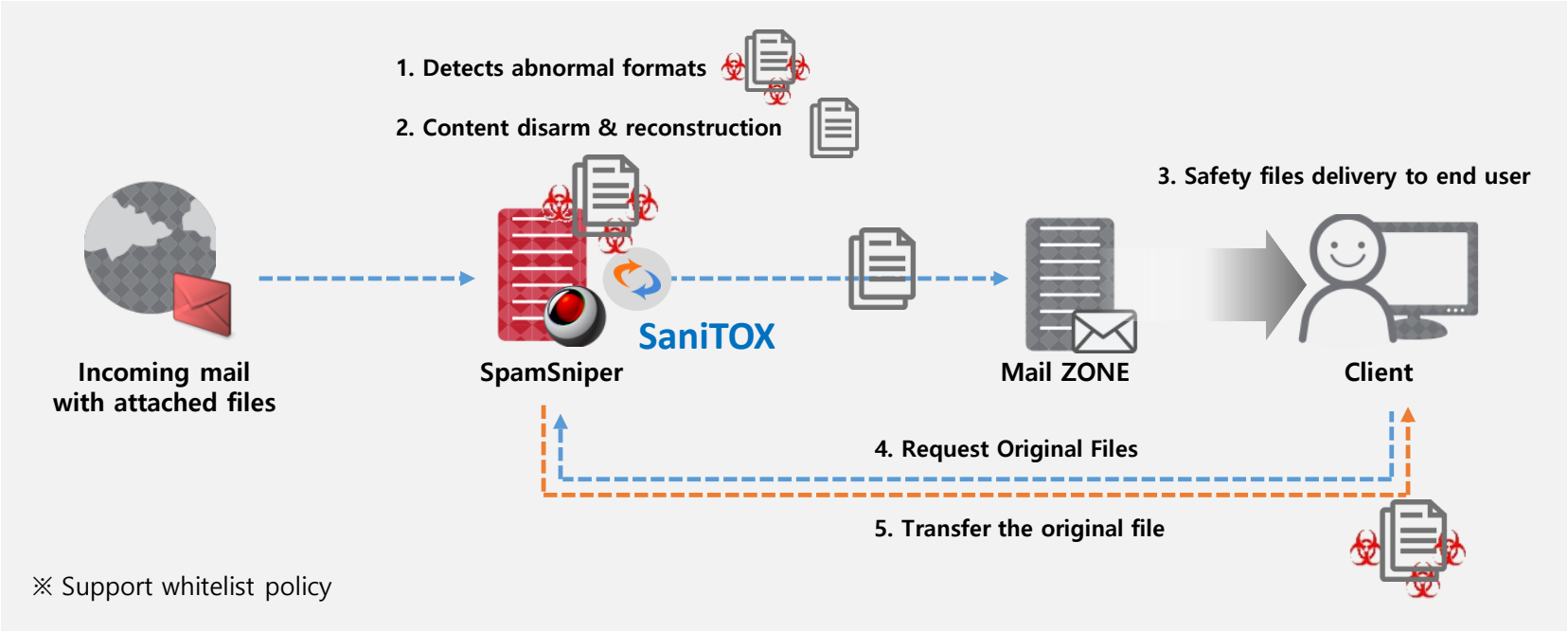


Ex) Uploading a file to the internal bulletin board



4. Examples of spam-mail defense

Configuration Map

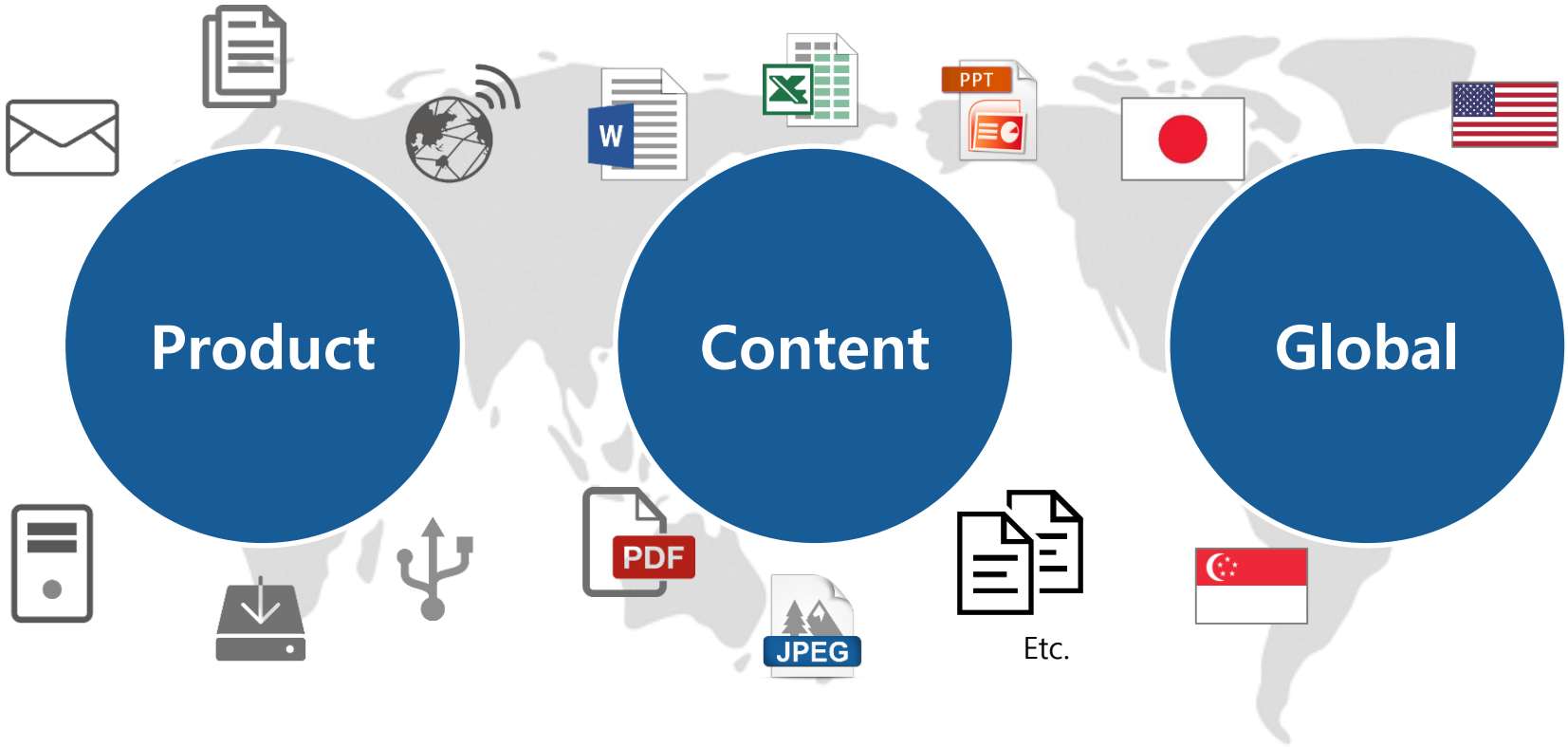


CDR vs. Sandbox vs AV

	SaniTOX(CDR)	Sandbox	Anti-Virus
Concepts	Active contents Sanitization (Signature-less)	Behavior based malware detection	Signature/Heuristic based malware detection
Main Target	Suspicious files (Normal/Abnormal)	Unknown Threats	Known Threats
Zero-day Attack	O	△	X

5. Next SaniTOX

We provide content prevention across all channels in the enterprise.



Our vision is
To be a 100-year-lasting IT Security Company
based on customers' satisfaction and trust.