

製品・テクノロジー最新情報とロードマップ-1

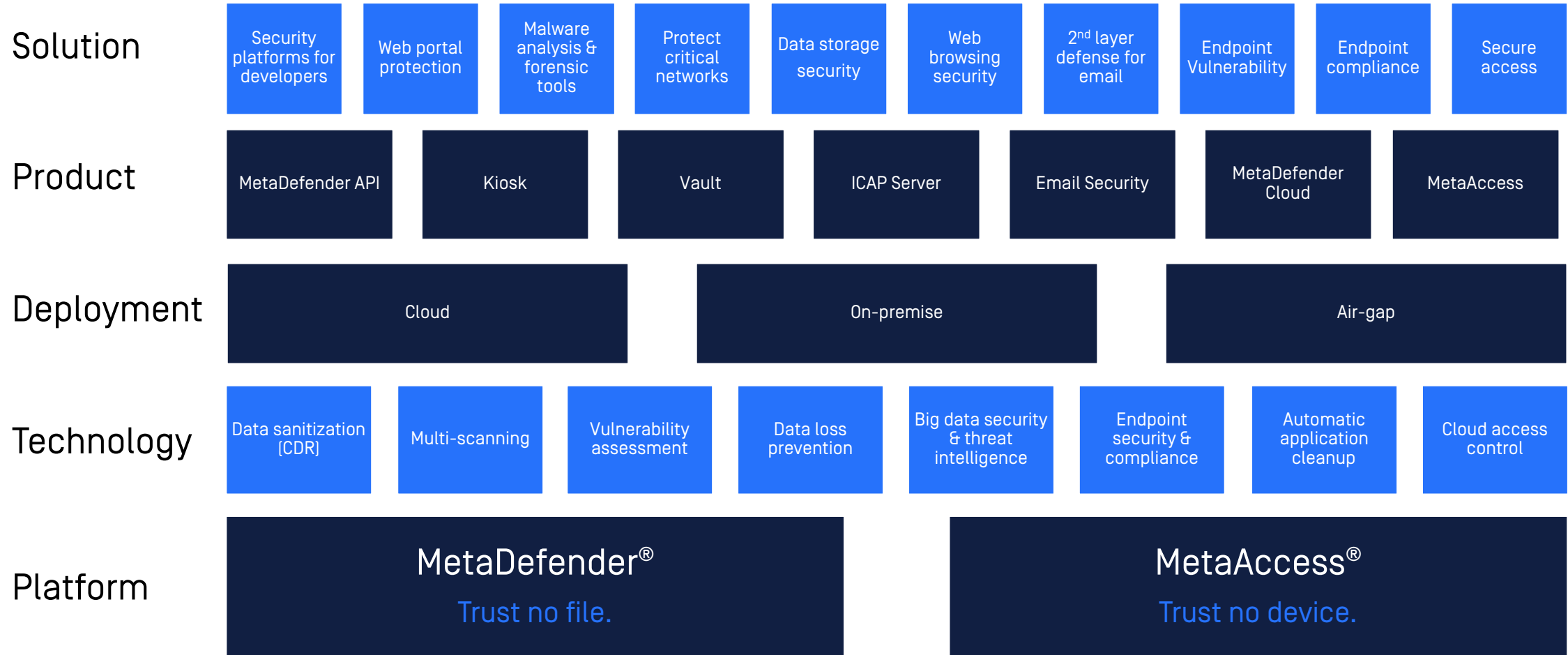
Taeil Goh, CTO

October 2018

Agenda

- OPSWAT Technologies
- Cross Domain & Critical Infrastructure
- File Upload & Web Application Protection
- Email Security
- Secure Access & End Point Compliance

OPSWAT Security Portfolio



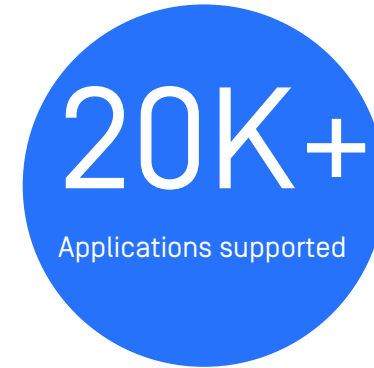
OPSWAT Advanced Technologies



Data Sanitization



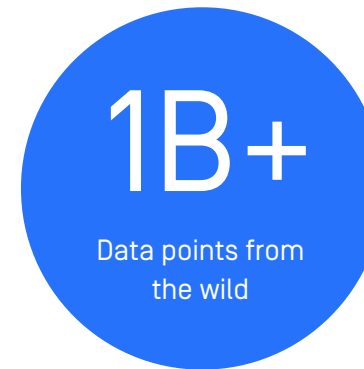
Multi-scanning



Vulnerability Assessment



Data Loss Prevention



Big Data Security &
Threat Intelligence

OPSWAT Technologies: Multi-scanning

Higher detection and faster response

What is Multi-scanning

Multi-scanning

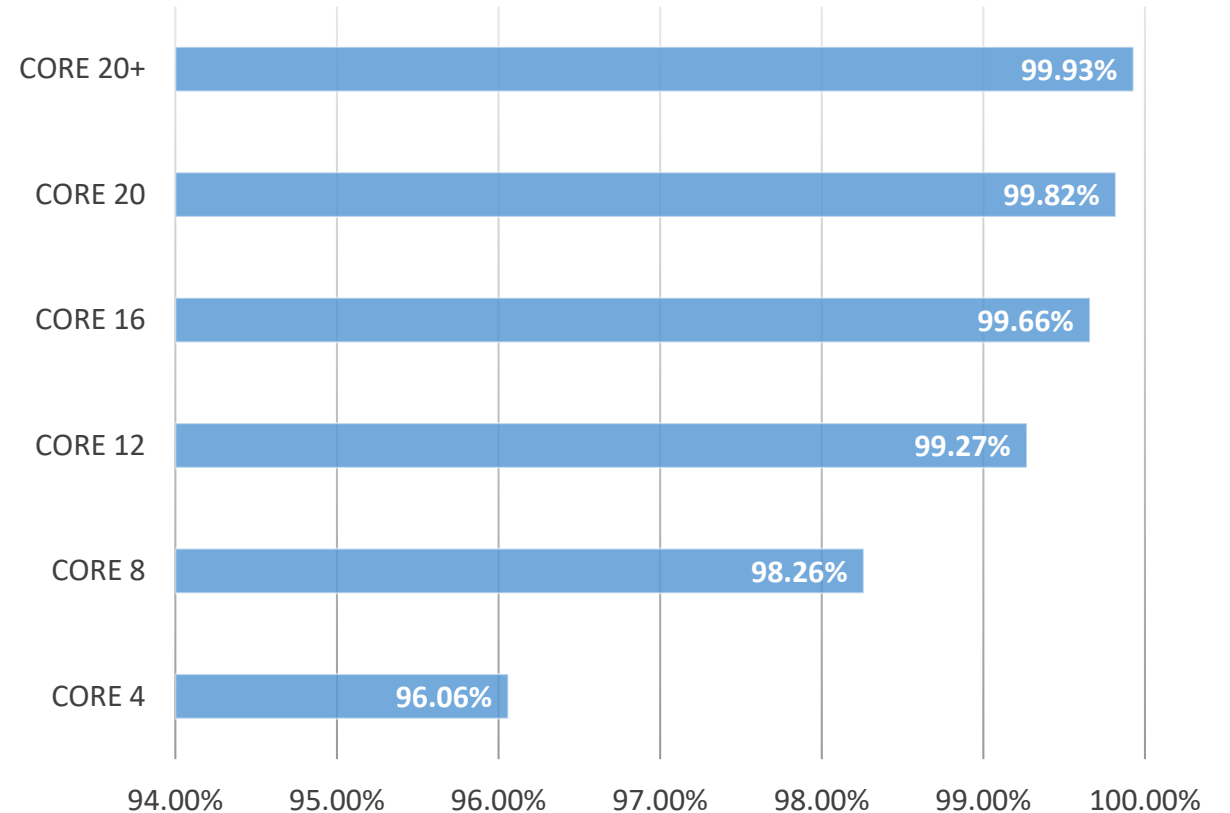
- Combine multiple anti-malware engines into one platform
- Optimization
- Normalization
- Does not replace AV on endpoint



Why Multi-scanning

Multi-scanning

- Higher Detection
- Wide malware detection coverage
- Faster outbreak detection
- Outbreak or False Positive?
- Resiliency



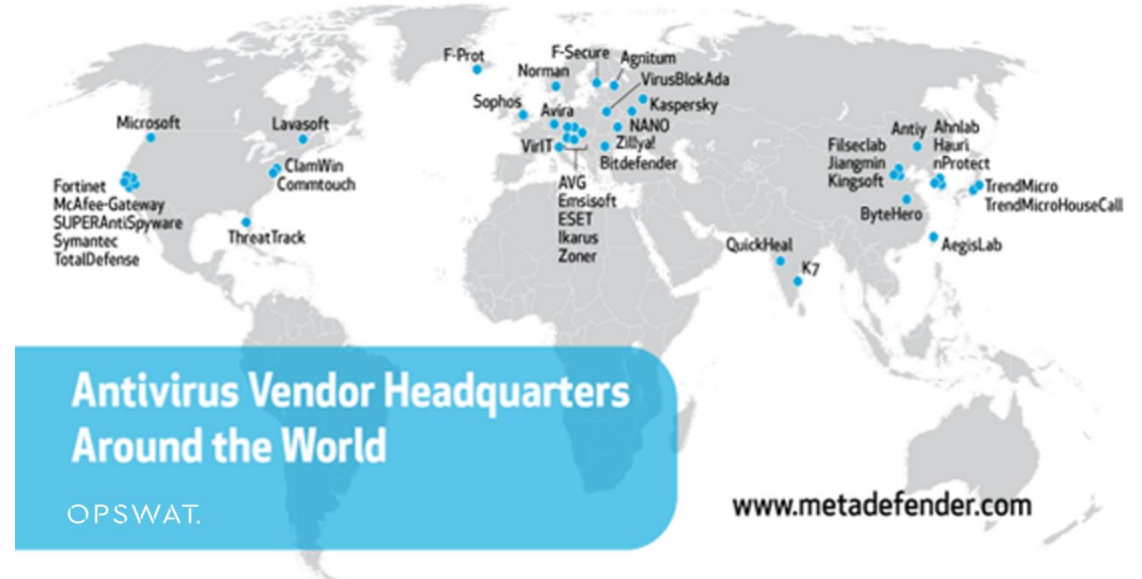
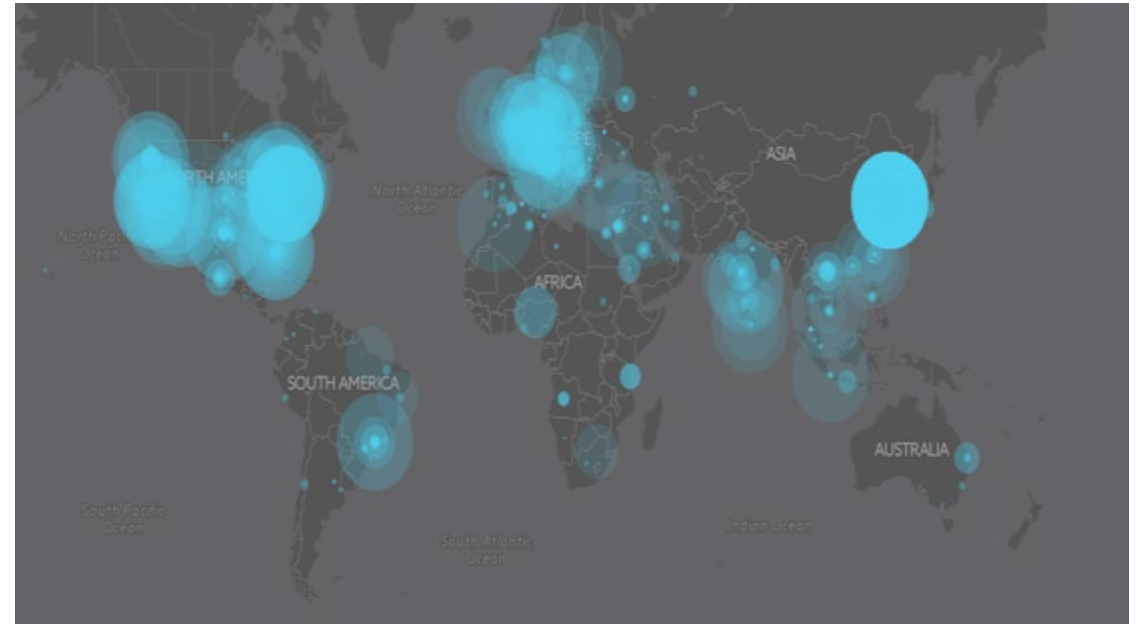
Source: <https://metadefender.opswat.com> [n=10000] Aug 2018

Why Multi-scanning

Multi-scanning

- Higher Detection
- Wide malware detection coverage
- Faster outbreak detection
- Outbreak or False Positive?
- Resiliency

Malware distribution



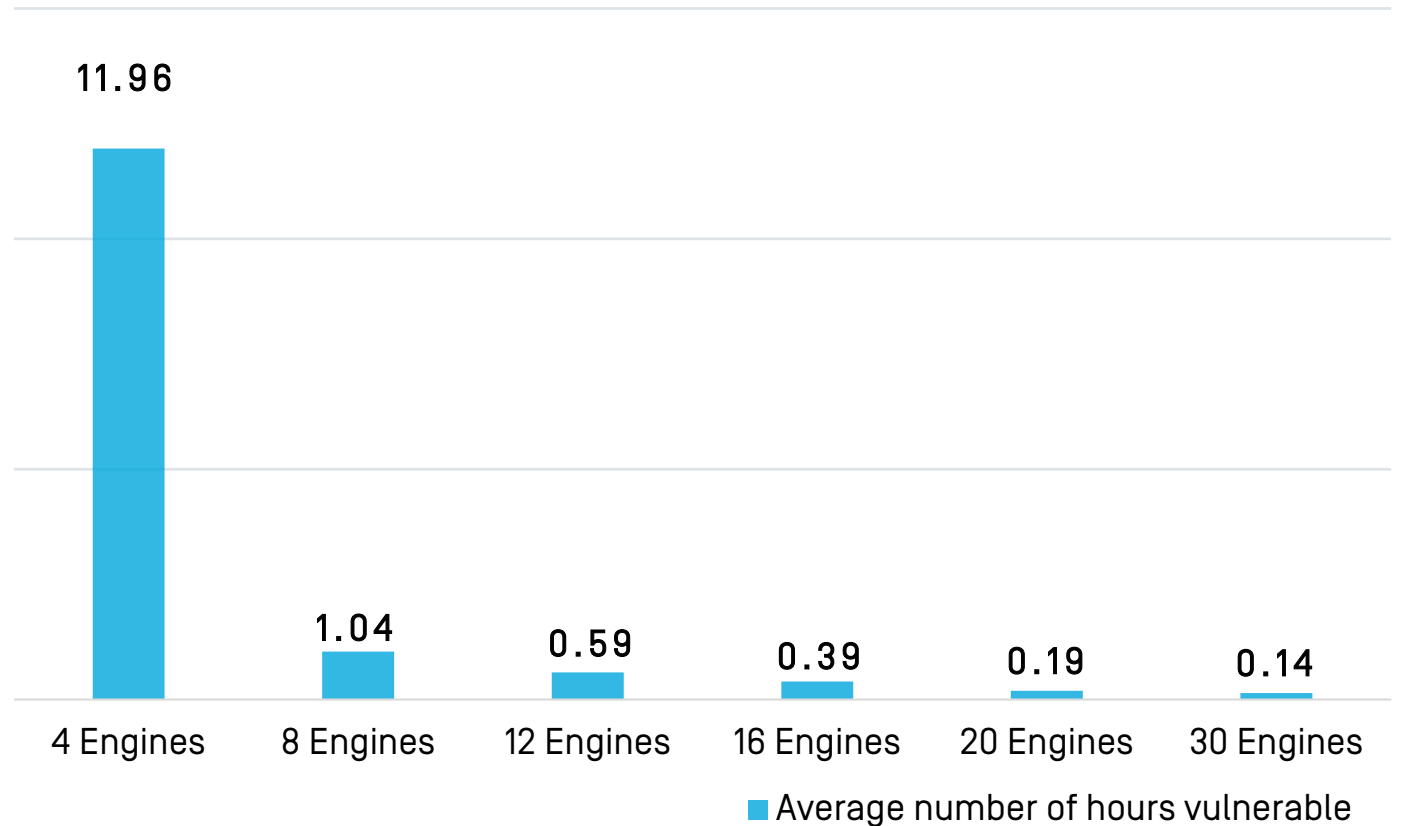
OPSWAT AV vendors distribution

OPSWAT.

Why Multi-scanning

Multi-scanning

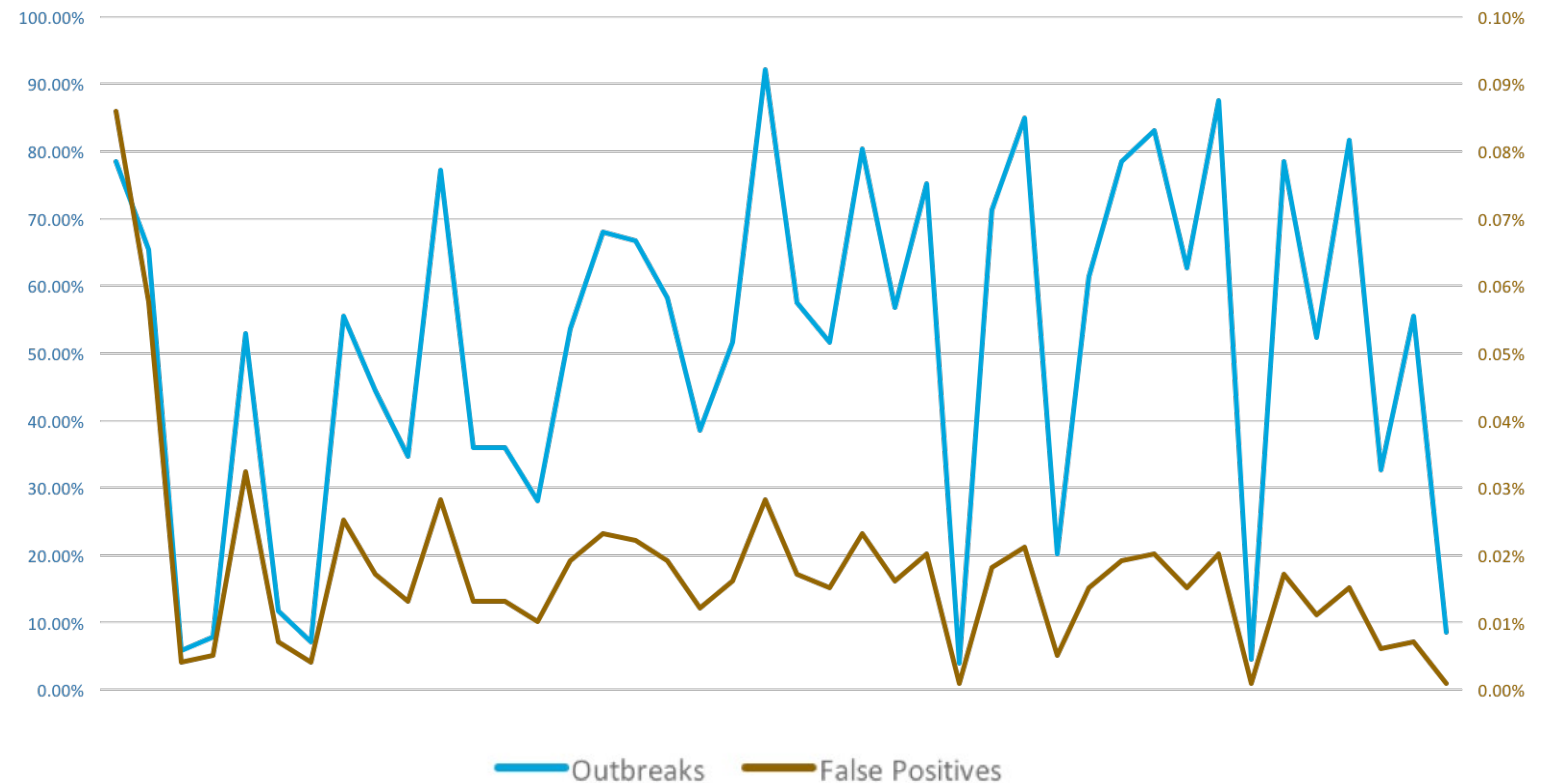
- Higher Detection
- Wide malware detection coverage
- **Faster outbreak detection**
- Outbreak or False Positive?
- Resiliency



Why Multi-scanning

Multi-scanning

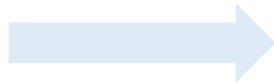
- Higher Detection
- Wide malware detection coverage
- Faster outbreak detection
- **Outbreak or False Positive?**
- Resiliency



Why Multi-scanning

Multi-scanning

- Higher Detection
- Wide malware detection coverage
- Faster outbreak detection
- Outbreak or False Positive?
- Resiliency



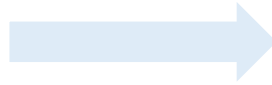
- AV failure
- AV vulnerability
- AV compliance [e.g., The U.S. Government bans Kaspersky]

OPSWAT Technologies: Data Sanitization [CDR]

Content Disarm and Reconstruction

Data Sanitization [CDR]

- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- Deep Dive
- An Analogy to Boiling Water
- Focus [big rocks]



- Removes **potentially malicious code** from files
- Removes all **disapproved file components**
- Validates **file type standard**
- **Not** malware analysis

Data Sanitization [CDR]

- Technical Definition
- **Remove Programmable / Scripting contents**
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- Deep Dive
- An Analogy to Boiling Water
- Focus [big rocks]

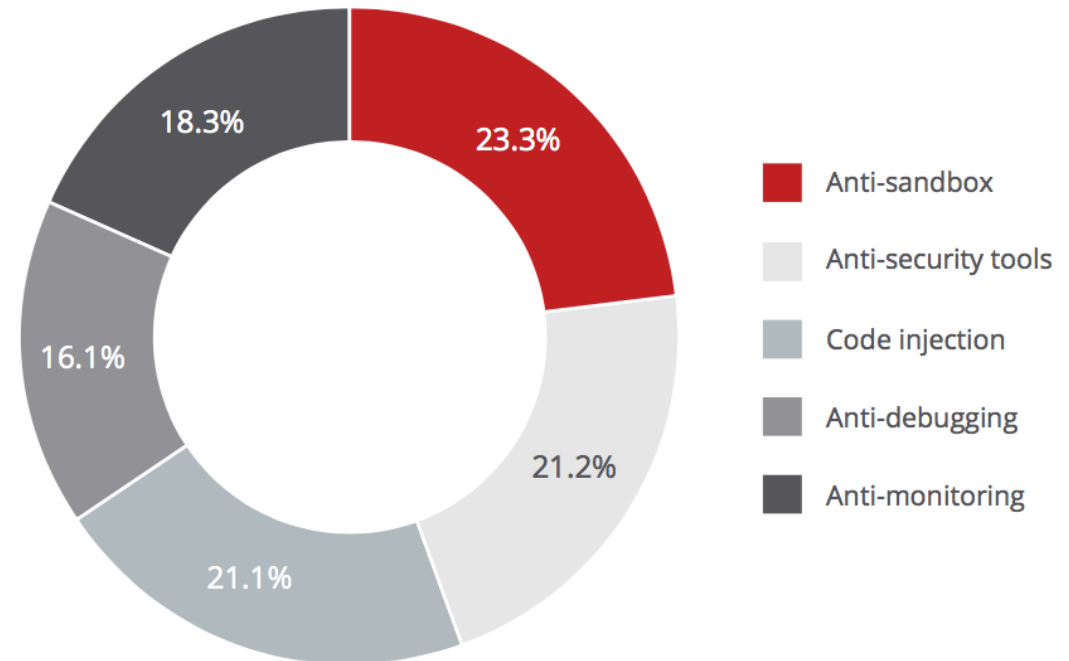


A word cloud of various malicious code types. The words are arranged in a cluster, with 'Macro' being the largest and most central. Other prominent words include 'VBScript', 'ActiveX Control', 'Attachment', 'Javascript', 'OLE object', 'PHP', and 'Malicious code'. The colors of the words vary, including shades of green, blue, orange, and purple.

Formula injection
VBScript
ActiveX Control
Macro
Attachment
Javascript OLE object
PHP
Malicious code

Data Sanitization [CDR]

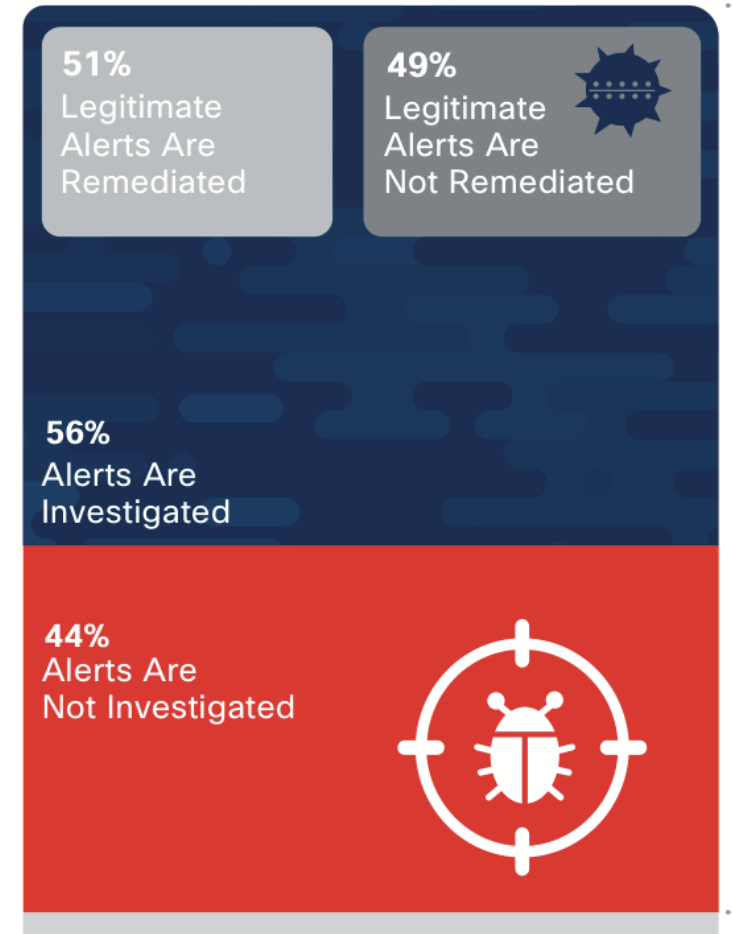
- Technical Definition
- Remove Programmable / Scripting contents
- **Anti-Malware Evasion**
- Efficiently Address Risks With Vulnerability
- Deep Dive
- An Analogy to Boiling Water
- Focus [big rocks]



Source: Virus Total and McAfee, 2017.

Data Sanitization [CDR]

- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- Deep Dive
- An Analogy to Boiling Water
- Focus [big rocks]

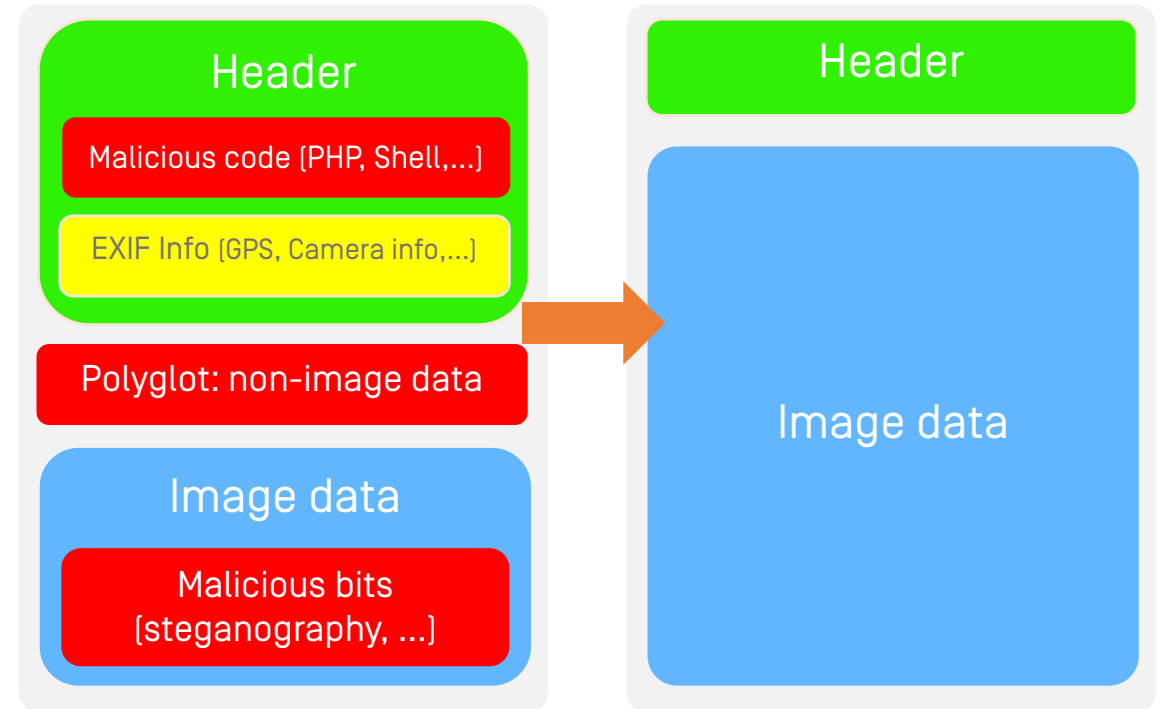


Source: Cisco Report, 2018

Data Sanitization [CDR]

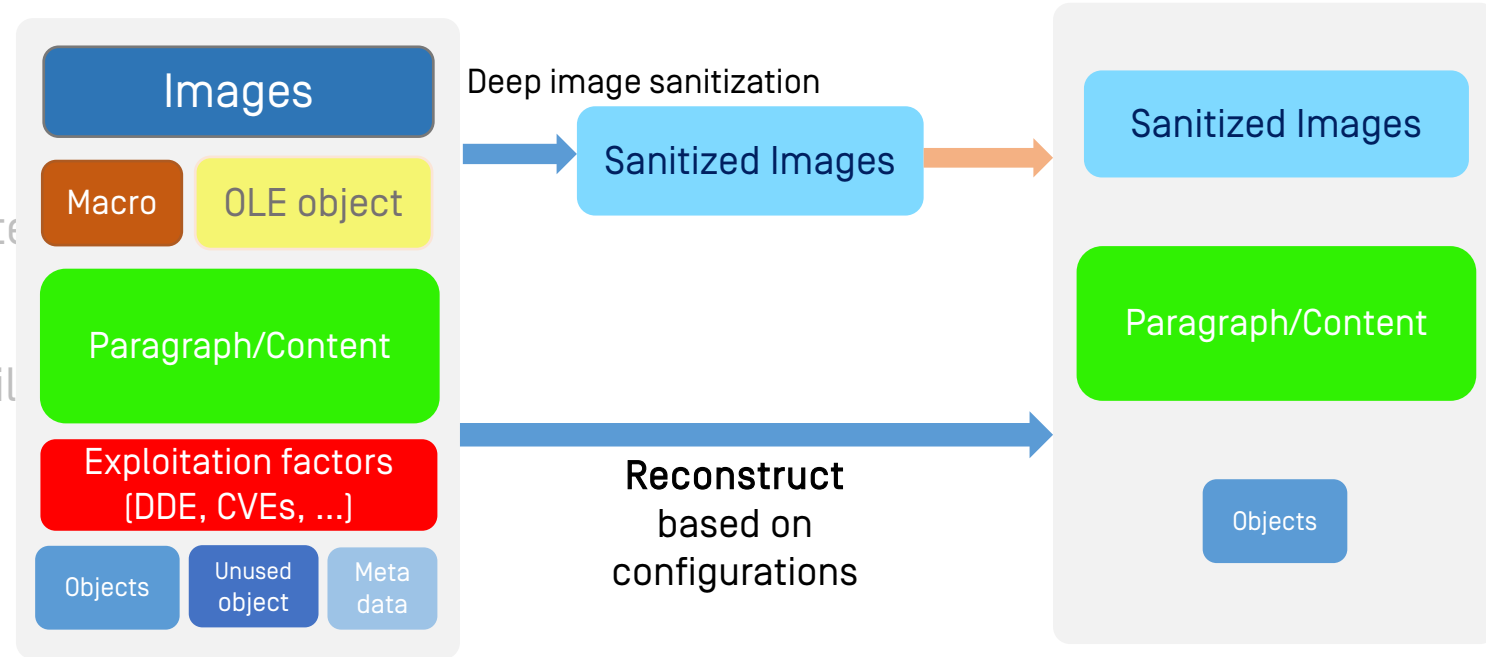
- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- **Deep Dive**
- An Analogy to Boiling Water
- Focus [big rocks]

Image sanitization



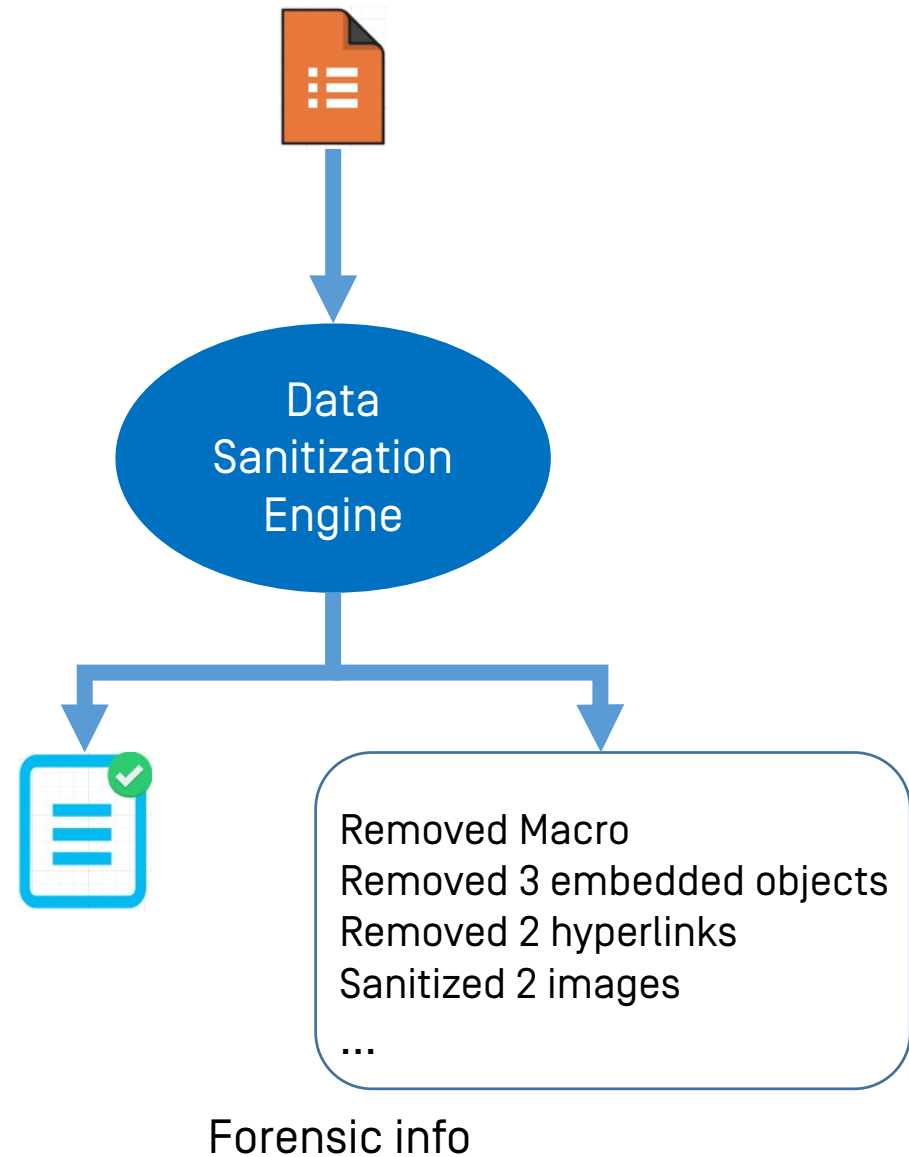
Data Sanitization Engine

- Technical Definition
- Remove Programmable / Scripting content
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerabilities
- **Deep Dive**
- An Analogy to Boiling Water
- Focus [big rocks]



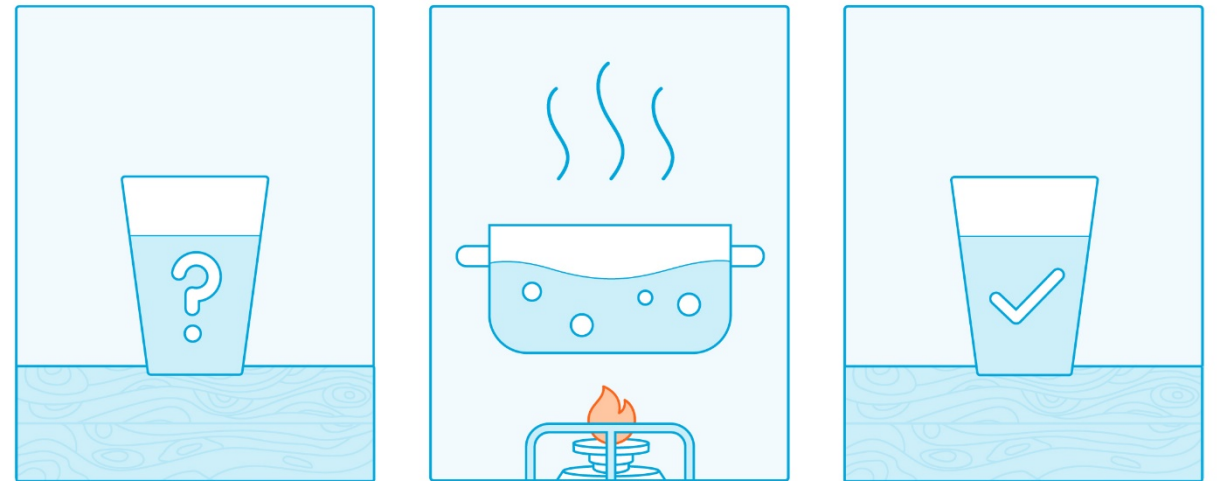
Data Sanitization [CDR]

- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- **Deep Dive**
- An Analogy to Boiling Water
- Focus [big rocks]



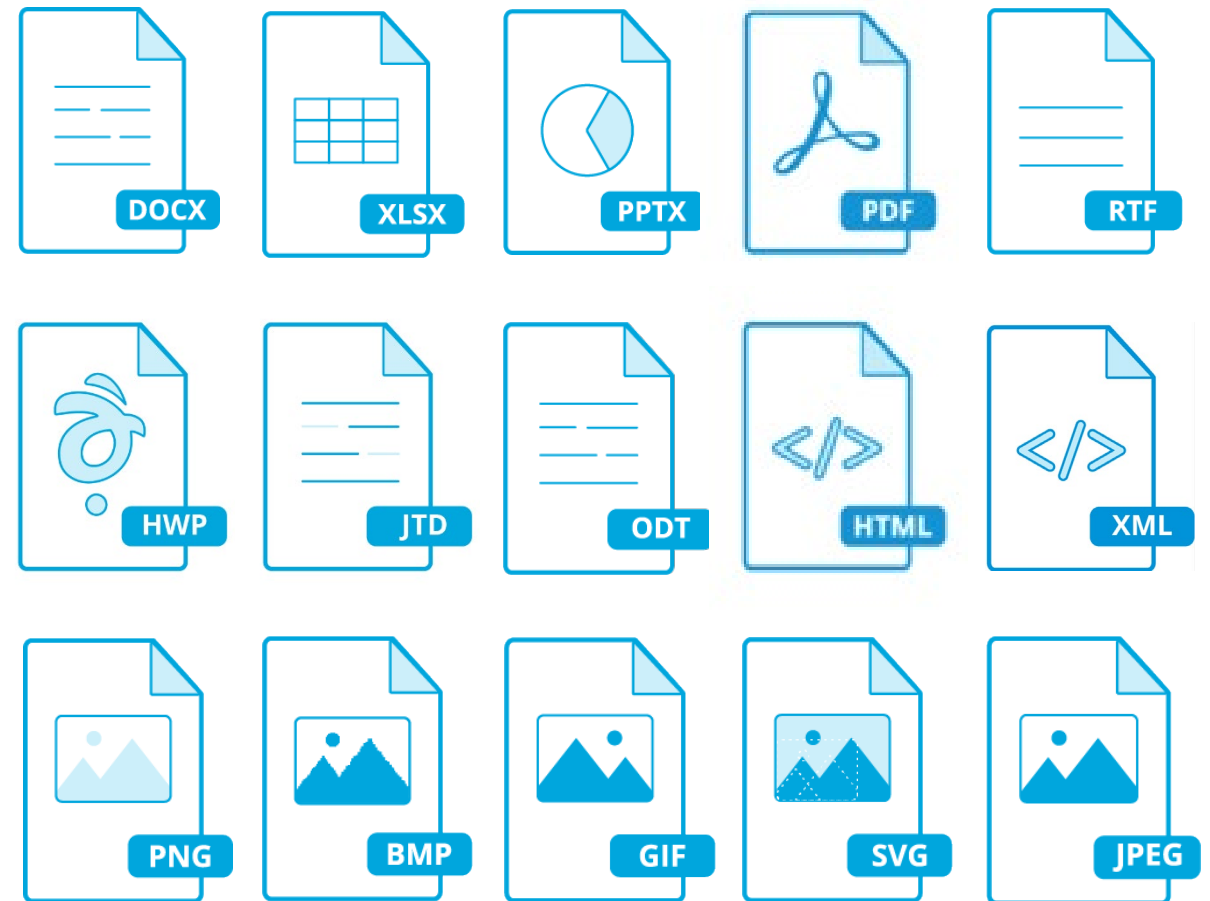
Data Sanitization [CDR]

- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- Deep Dive
- **An Analogy to Boiling Water**
- Focus [big rocks]



Data Sanitization [CDR]

- Technical Definition
- Remove Programmable / Scripting contents
- Anti-Malware Evasion
- Efficiently Address Risks With Vulnerability
- Deep Dive
- An Analogy to Boiling Water
- Focus [big rocks]



More OPSWAT Technologies:

Vulnerability Assessment

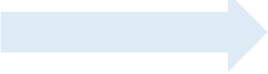
Data Loss Prevention

Endpoint Security & Compliance

Threat Intelligence Platform

Identifying application vulnerabilities

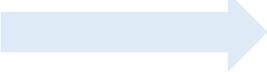
Vulnerability Assessment

- Vulnerability Assessment 
 - Data Loss Prevention
 - MetaDefender Cloud
- Prevent threats
 - Work in both online and offline
 - Unique – Detect vulnerabilities in installers

() patent pending*

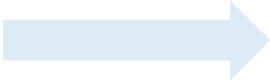
Identifying application vulnerabilities

Vulnerability Assessment

- **Vulnerability Assessment** 
 - Data Loss Prevention
 - MetaDefender Cloud
- 250+ top vulnerable applications
 - 14,000+ associated CVE with severity information
 - 300,000+ identified active vulnerable hashes
 - 30+ times faster than existing solutions on the market

Detect potential data breaches

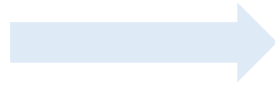
Data Loss Prevention

- Vulnerability Assessment
 - Data Loss Prevention
 - MetaDefender Cloud
- 
- 30+ supported file types
 - Metadata and file content check
 - Detect Social Security Numbers
 - Detect Credit Card Numbers
 - Support Custom Regular Expressions

Threat Intelligence Platform

Seamless integration

- Vulnerability Assessment
- Data Loss Prevention
- MetaDefender Cloud



- metadefender.opswat.com
- Upload any file to the cloud for analysis
- Search or scan a CVE, file HASH or IP address
- Scan history
- Available as a simple URL for all API calls
- Coming soon
 - URL filtering
 - Cloud sandbox integration

Use Case 1: Cross Domain & Critical Infrastructure

OPSWAT Flagship Products



MetaDefender Kiosk



MetaDefender Vault

MetaDefender Kiosk

Checkpoint for Portable Media

- Support portable media and devices
- Multi-scanning and data sanitization
- Audit
- Supports encrypted devices
- Localization and customization

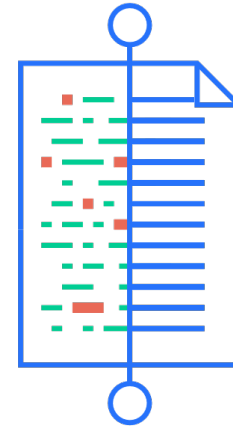
Android
USB CD
iPhone DVD
Floppy disk
SD Cards

MetaDefender Kiosk

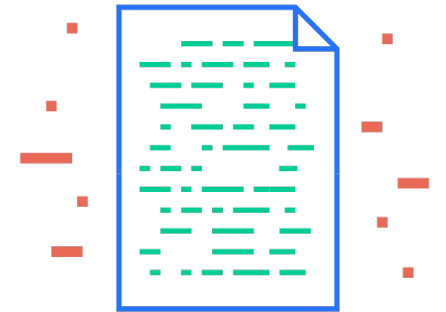
Checkpoint for Portable Media

- Support portable media and devices
- Multi-scanning and data sanitization
- Audit
- Supports encrypted devices
- Localization and customization

IDENTIFY & SCAN



SANITIZE (CDR)



MetaDefender Kiosk

Checkpoint for Portable Media

- Support portable media and devices
- Multi-scanning and data sanitization
- Audit
- Supports encrypted devices
- Localization and customization

OPSWAT.

EXIT & EJECT

1 LOG IN 2 INSERT MEDIA 3 SCANNING 4 RETRIEVE FILES

Login

Domain KIOSK Name \

A name is required

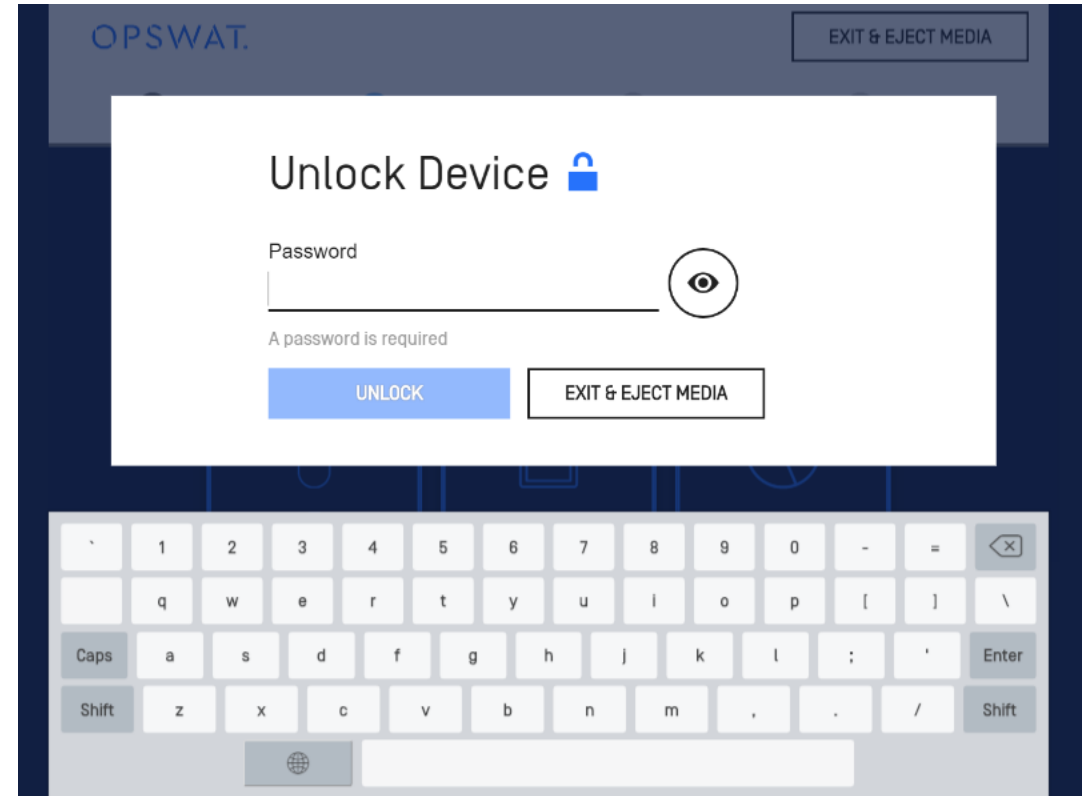
NEXT CANCEL

Virtual keyboard interface showing keys: Caps, Shift, and alphanumeric keys.

MetaDefender Kiosk

Checkpoint for Portable Media

- Support portable media and devices
- Multi-scanning and data sanitization
- Audit
- Supports encrypted devices
- Localization and customization



MetaDefender Kiosk

Checkpoint for Portable Media

- Support portable media and devices
- Multi-scanning and data sanitization
- Audit
- Supports encrypted devices
- Localization and customization

User Questions Policy

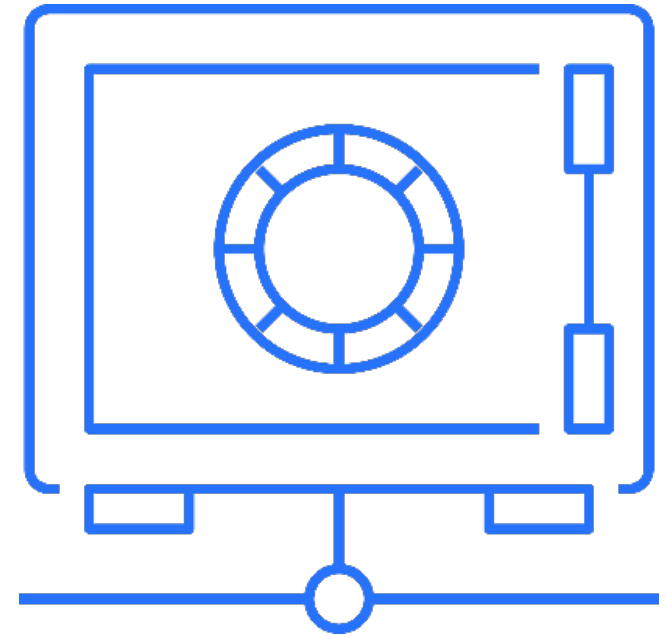
Questions for user prior to scanning.

Display	Question	Response Required
<input checked="" type="checkbox"/>	What is your badge number?	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	What is the ID of the media you will be scanning?	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	What is the source of the files on this media?	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Which systems will access the files on this media?	<input checked="" type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>

MetaDefender Vault

Secure File Transfer and Storage

- Multi-scanning and data sanitization
- Outbreak prevention
- No special client software needed
- Seamless integration with MetaDefender Kiosk



MetaDefender Vault

Secure File Transfer and Storage

- Multi-scanning and data sanitization
- **Outbreak prevention**
- No special client software needed
- Seamless integration with MetaDefender Kiosk

Outbreak Prevention

TOTAL FILES PROCESSED

22

Locked files

0

Currently processing

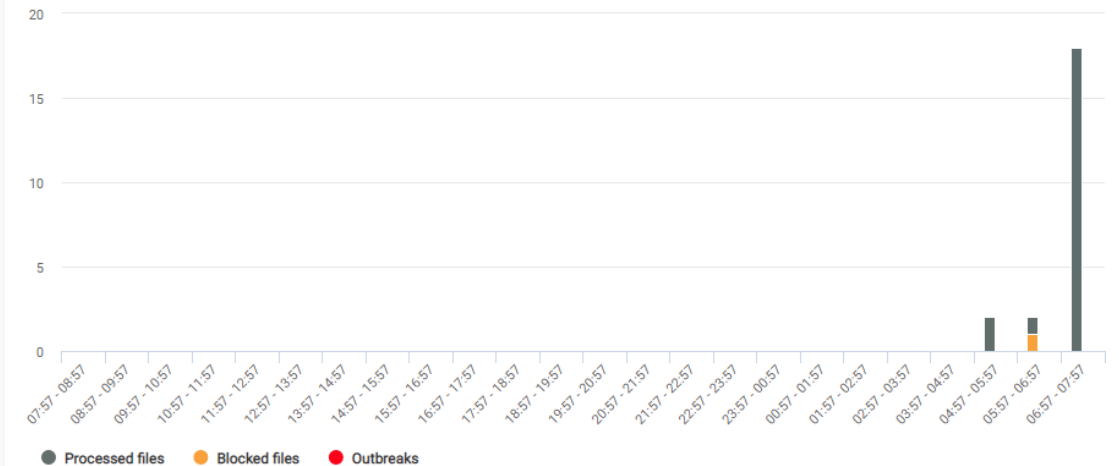
0

Outbreaks

0

OUTBREAK DETECTION ACTIVITY

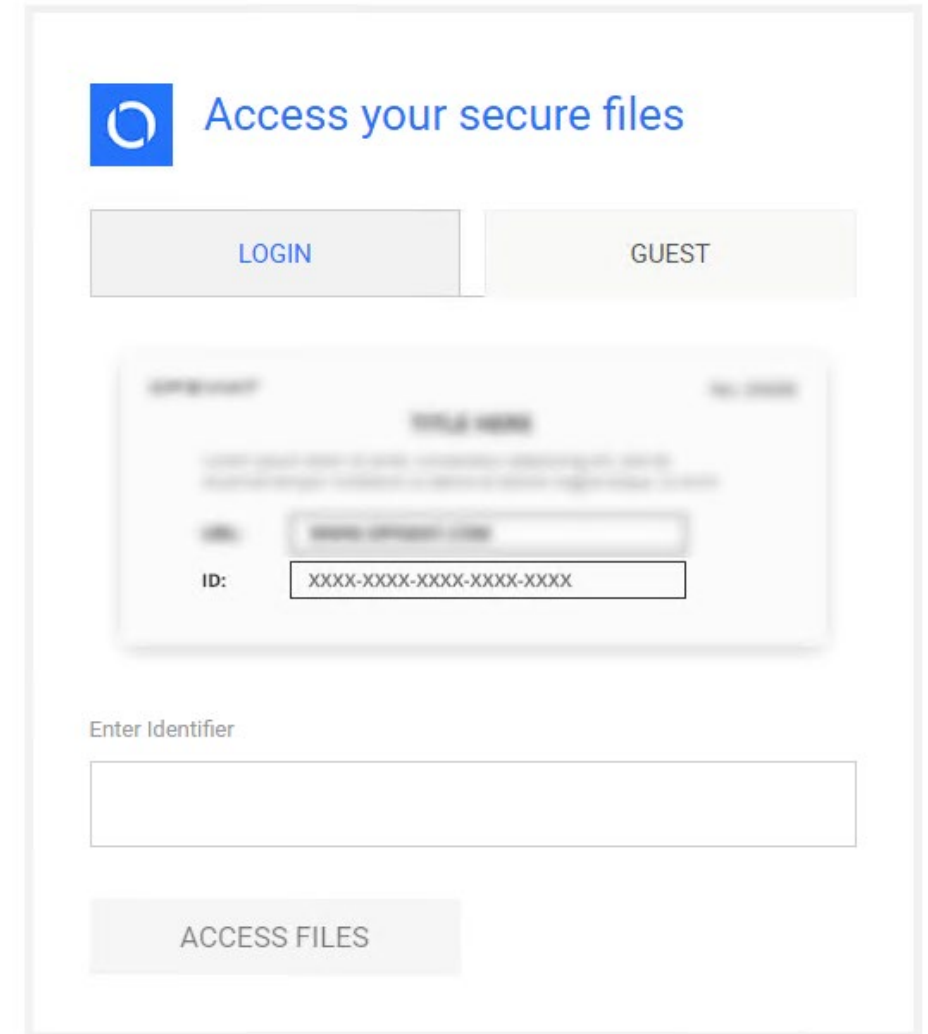
Last 24 hours ▼



MetaDefender Vault

Secure File Transfer and Storage

- Multi-scanning and data sanitization
- Outbreak prevention
- **No special client software needed**
- Seamless integration with MetaDefender Kiosk

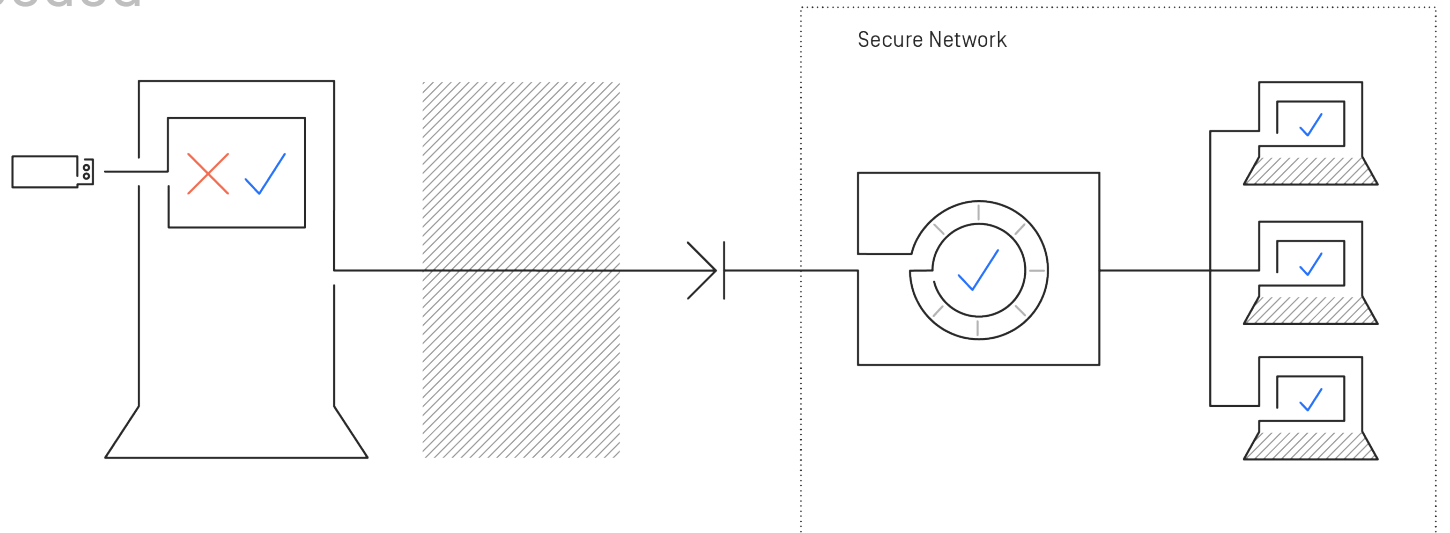


The image shows a web-based login interface for MetaDefender Vault. At the top left is a blue circular logo with a white 'Q' inside. To its right is the text 'Access your secure files'. Below this are two buttons: 'LOGIN' (light grey) and 'GUEST' (light yellow). In the center is a blurred screenshot of a document or interface. Below the screenshot is a label 'Enter Identifier' followed by a large, empty rectangular input field. At the bottom is a light grey button labeled 'ACCESS FILES'.

MetaDefender Vault

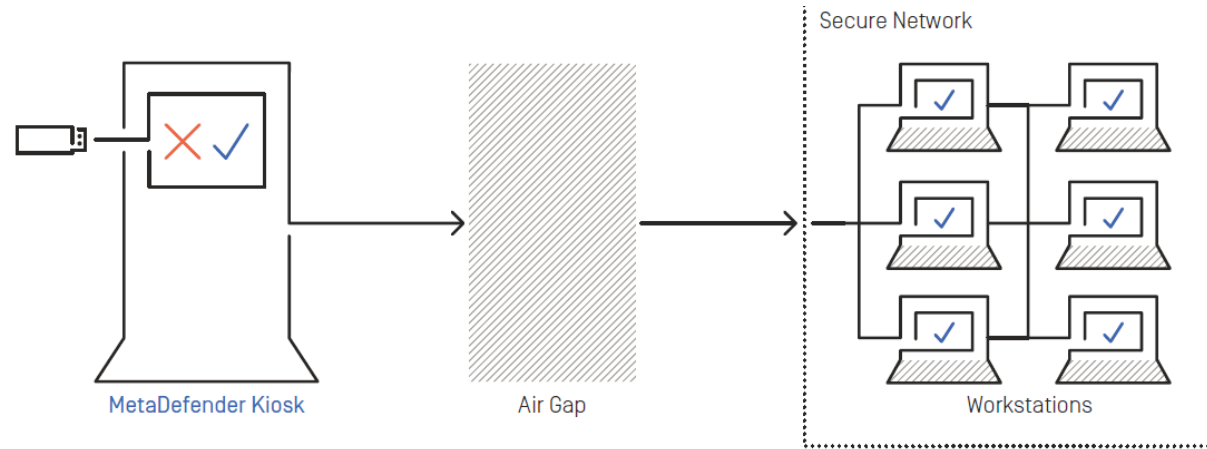
Secure File Transfer and Storage

- Multi-scanning and data sanitization
- Outbreak prevention
- No special client software needed
- Seamless integration with MetaDefender Kiosk

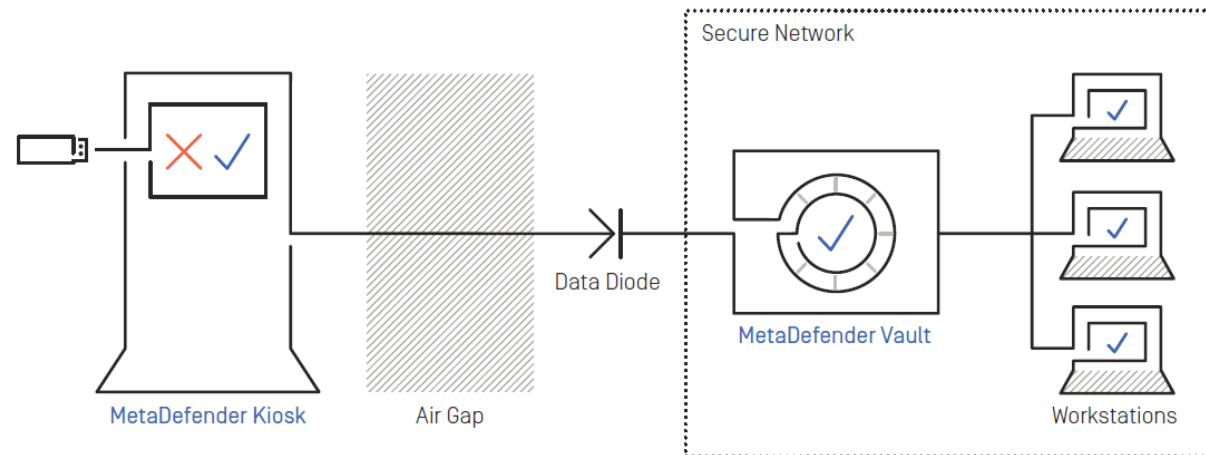


Air Gap Use Case

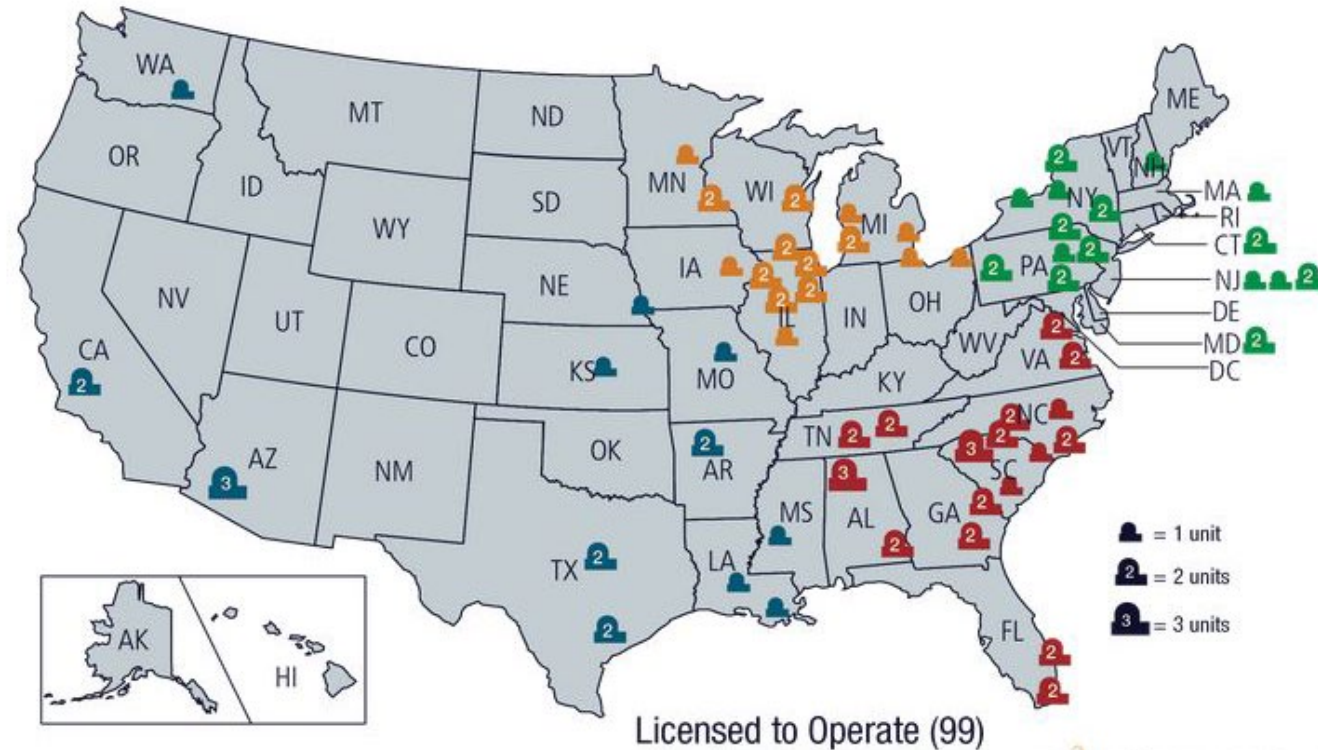
Kiosk Air Gap Use Case



Kiosk Air Gap with Data Diode and Vault Use Case



Protecting over 95% of nuclear power facilities in the US



As of May 2017



Case Study

Oil & Gas

Challenges

Managing files and data being brought to offshore oil rigs

Risk of malware compromising critical systems

Bandwidth limitations requires transfer by physical media

Solution

MetaDefender Kiosks to scan all files on portable media

Scan files with multiple anti-malware engines

Ruggedized kiosk hardware for offshore conditions

Omaha Public Power District

OPSWAT for Critical Infrastructure



Challenge

- The constant threat of malware infiltration
- Strict industry regulations

Solution

- MetaDefender Kiosk across multiple locations

Results

- Easily able to monitor and manage data entering their facilities
- Greater auditing capabilities
- File scan logs easily attributed to users and projects



“We needed to track and manage the constant flow of data in and out of our facilities. MetaDefender has enabled us to set up detailed security policies for specific users and keep pace with the ever-changing industry requirements. It adds another layer of protection for us.”

*Malie Combs
Cyber Security Analyst
Information Technology
OPPD*



Road Map [Kiosk, Vault]

- Kiosk multiple hardware form factors (regional)

