



# Web Application Security in Vietnam

Prepared for: VNISA

Prepared by: Cuong La, Nhut Ngo

Saturday, March 25, 2023

# Agenda

---

About OPSWAT

Report on Web Application Security in Vietnam

OPSWAT's File Upload Security

OPSWAT Technologies

- Multi-scanning
- Proactive DLP
- Deep CDR

Q&A



OUR MISSION

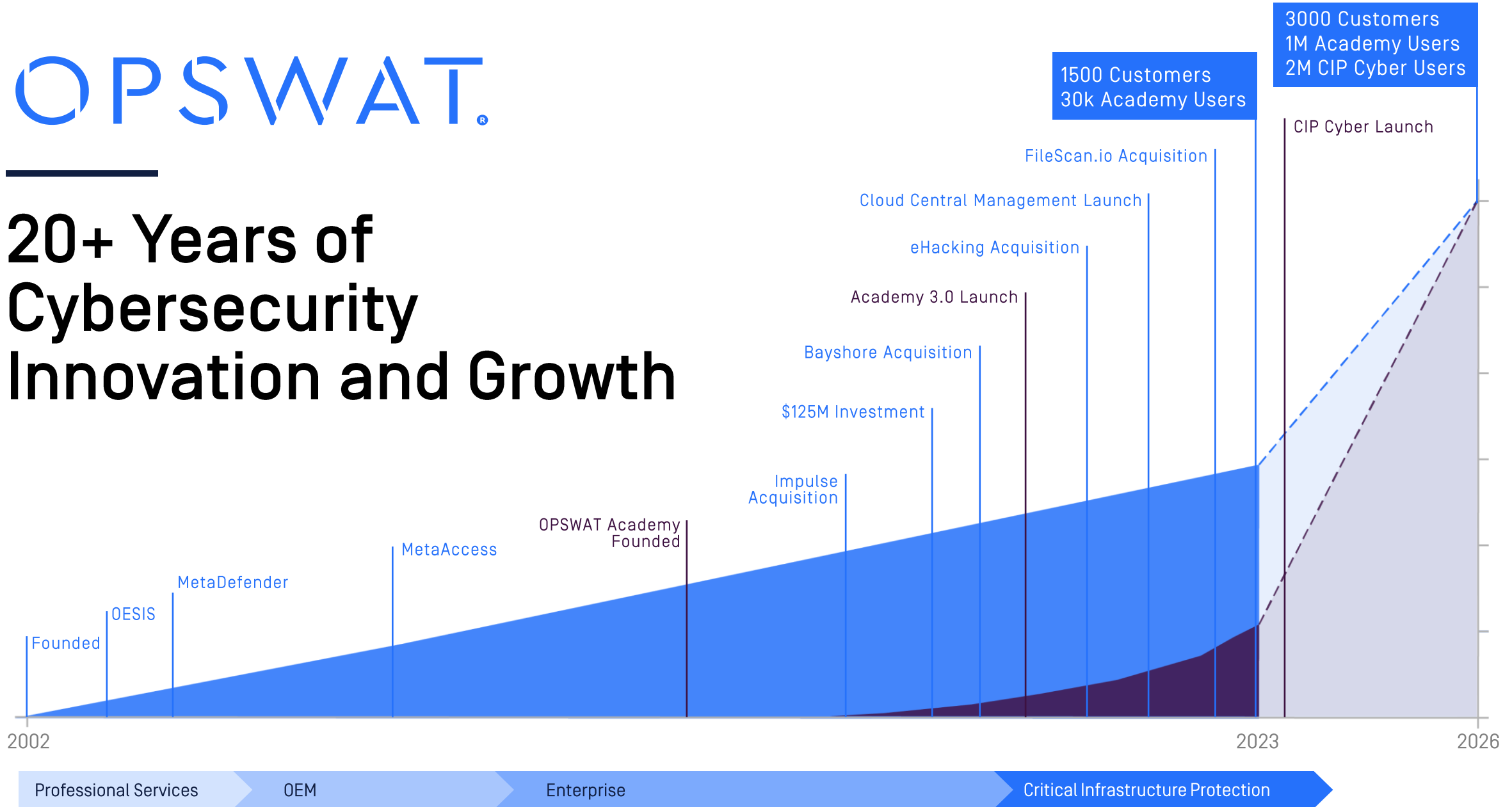
**We Protect the World's  
Critical Infrastructure**

---

**OPSWAT.**



# 20+ Years of Cybersecurity Innovation and Growth



# 1400+ Active OPSWAT Customers by Sector



Chemical



Commercial Facilities



Communications



Critical Manufacturing



Dams



Defense Industrial Base



Emergency Services



Energy



Financial Services



Food and Agriculture



Government Facilities



Healthcare and Public Health



Information Technology



Nuclear Reactors, Materials and Waste



Transportation Systems

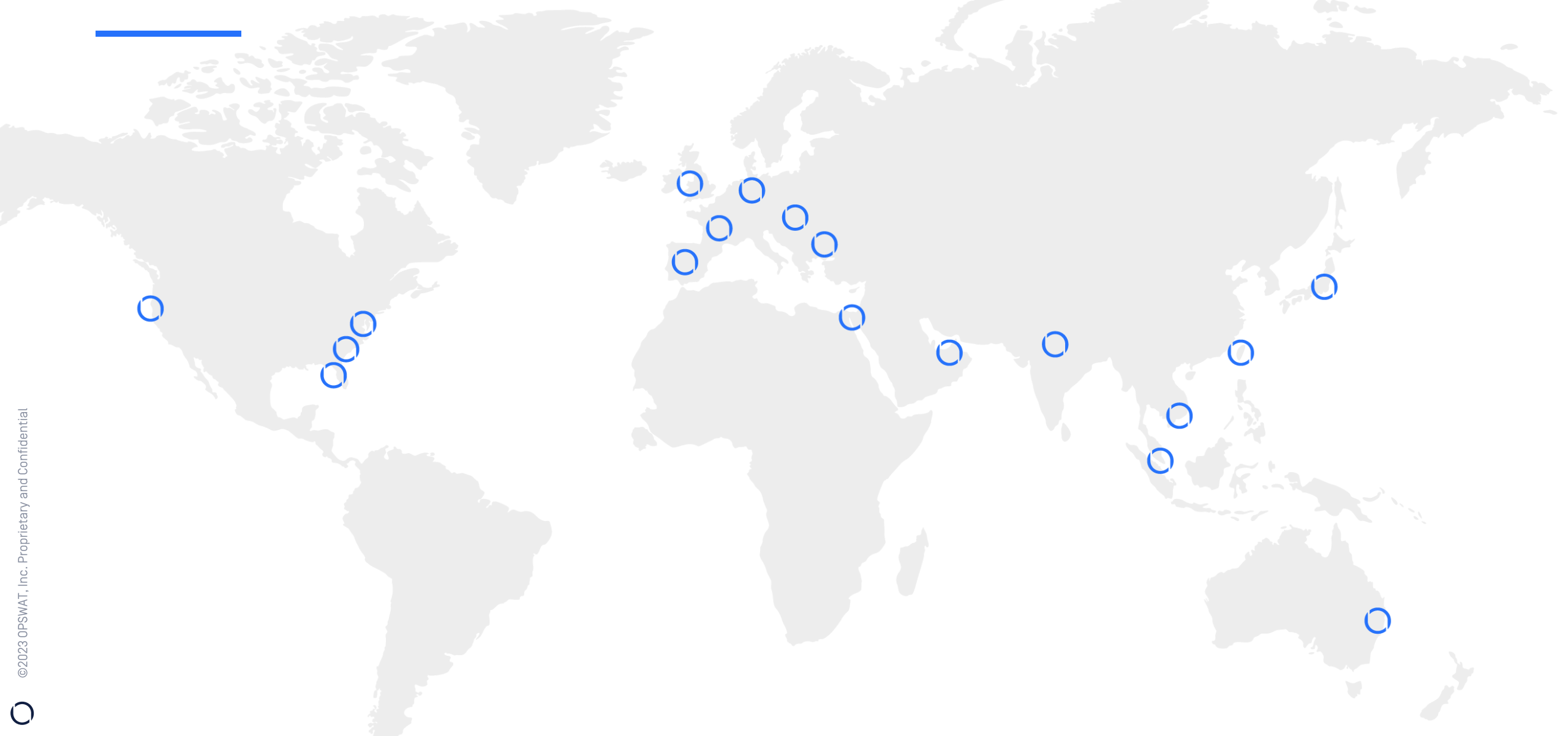


Water and Wastewater Systems



# Global Presence, Trust and Support

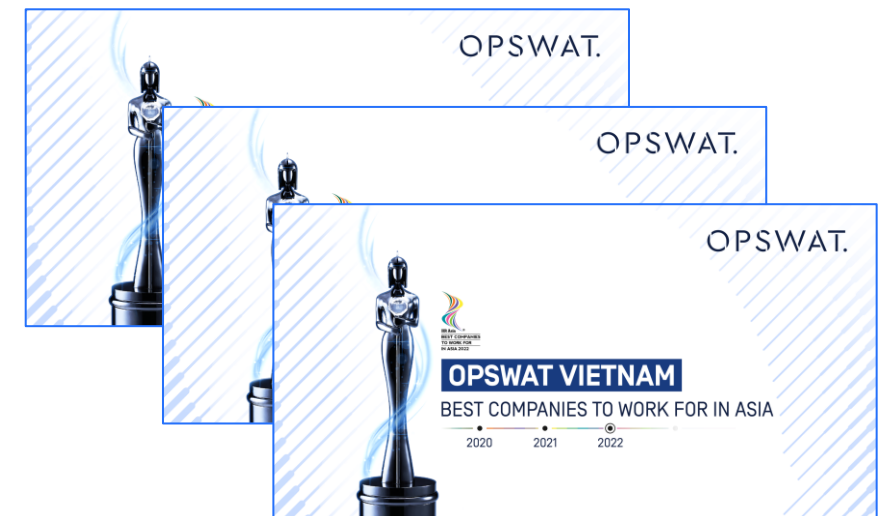
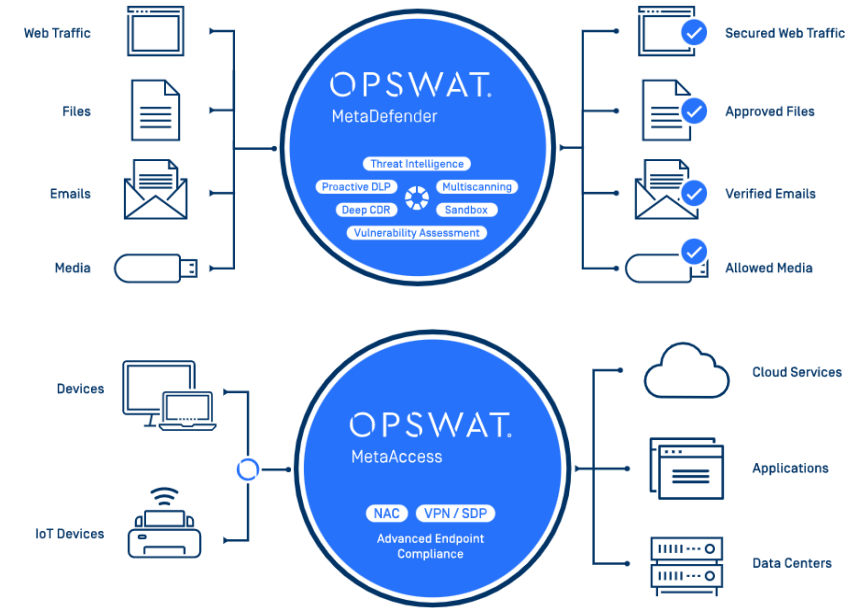
---



# OPSWAT In Vietnam

## OPSWAT Vietnam's key facts:

- 10+ years of operations in Vietnam
- Nearly 300 top-notch talents and is still growing fast
- R&D ownership of several key products and technologies of OPSWAT
- Biggest, most diversified Customer Experience Team
- Strong marketing & back-office teams support APAC and global
- Sales staff & channel partners support Vietnam market
- “Best Company to Work for in Asia” by HR Asia Magazine in 3 consecutive years 2020-2022





# Report on Web Application Security in Vietnam



# Websites with File-Upload

We search for websites in Vietnam that have file upload feature exposed.

The found websites are then populated with interested attributes: industry, OS, Web server

OPSWAT. MetaCrawler SDR. Location: United States Select Location. SEARCH

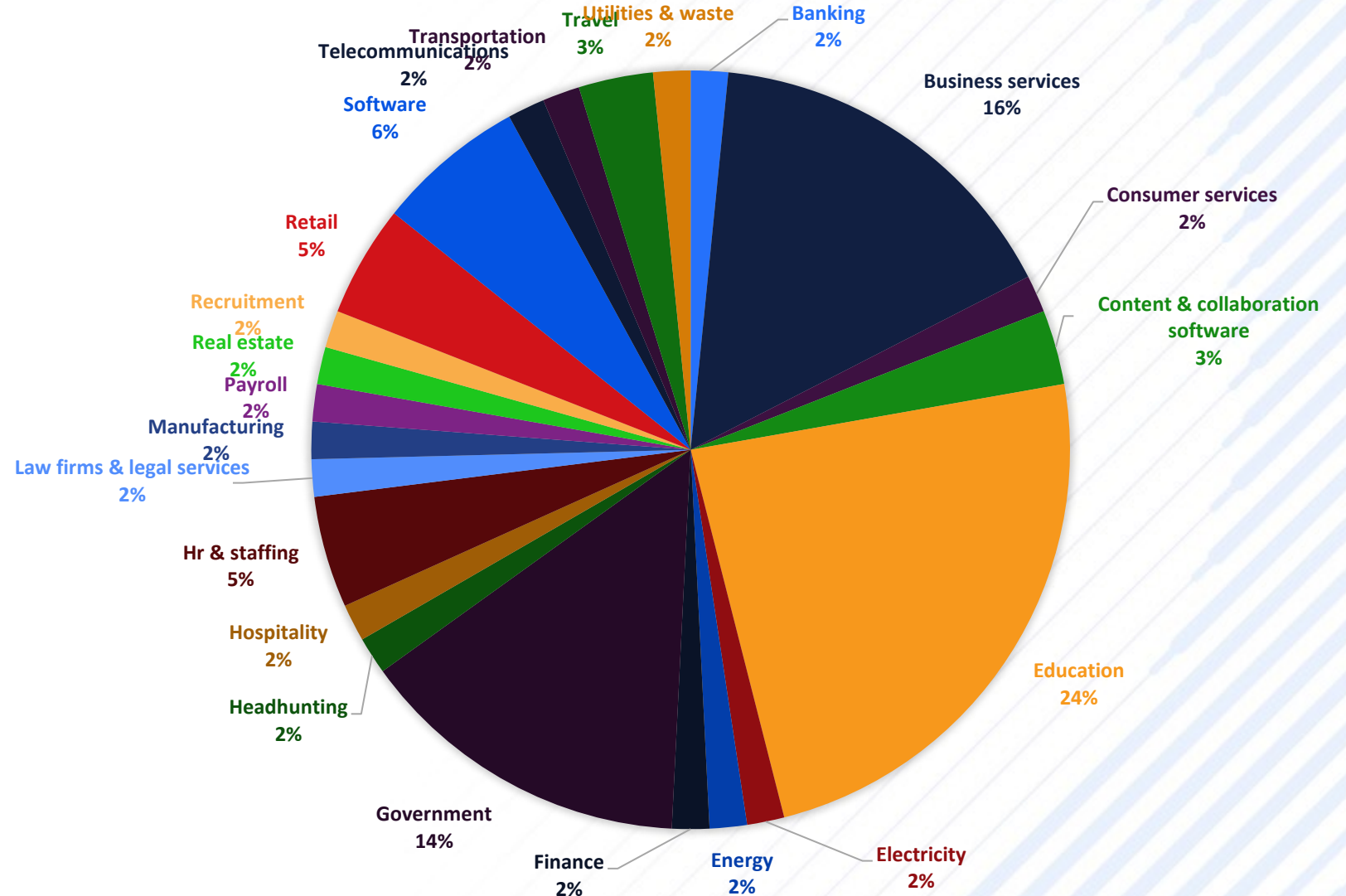
FOUND 1030 SITES

NO.	ID	ORGANIZATION NAME	WEBSITE	UPLOAD URI	LOCATION	SUGGESTED EMAIL ADDRESSES	CRAWLED AT (MM-DD-YYYY HH:MM:SS)	STATUS	REAL FILE UPLOAD PAGE	ACTION
1	2	Arcade Database <span>UNVERIFIED</span>	adb.arcadetaila.net	http://adb.arcadetaila.net/?mame=chase...	Alaska	jscott@archive.org fujix@e2j.net arcadedatabase@gmail.com FILTER EMAILS	09-26-2022 19:31:11	Viewed	Unmarked	⋮
2	3	Arcade Database <span>UNVERIFIED</span>	adb.arcadetaila.net	http://adb.arcadetaila.net/?mame=spnch...	Alaska	jscott@archive.org fujix@e2j.net arcadedatabase@gmail.com FILTER EMAILS	09-26-2022 19:41:17	Lead Created	Unmarked	⋮
3	4	Southeast Agricultural Research & Extensio... <span>ZOOMINFO</span>	agsci.psu.edu	http://ailab-projects2.ist.psu.edu/RNABin...	Pennsylvania	git@github.com admissions@psu.edu FILTER EMAILS	09-26-2022 19:48:08	Viewed	Unmarked	⋮
4	5	Arcade Database <span>UNVERIFIED</span>	adb.arcadetaila.net	http://adb.arcadetaila.net/?mame=suprm...	Alaska	jscott@archive.org fujix@e2j.net arcadedatabase@gmail.com FILTER EMAILS	09-26-2022 19:51:17	Lead Created	Unmarked	⋮
5	6	State Board of Cosmetology <span>ZOOMINFO</span>	www.legis.state.la.us	http://laserfiche.adminlaw.state.la.us/For...	Nevada	No Email Address Found	09-26-2022 21:38:26	Viewed	Unmarked	⋮
6	7	Emory University Department of Environmen... <span>ZOOMINFO</span>	www.envs.emory.edu	http://bbisr.shinyapps.winship.emory.edu/...	Georgia	No Email Address Found	09-26-2022 21:48:18	New	Unmarked	⋮
7	8	Adobe	acrobat.adobe.com	https://community.adobe.com/t5/coldfusi...	Mississippi	aecpanel@adobe.com chitamba@adobe.com	09-26-2022 21:58:07	Lead Created	Unmarked	⋮



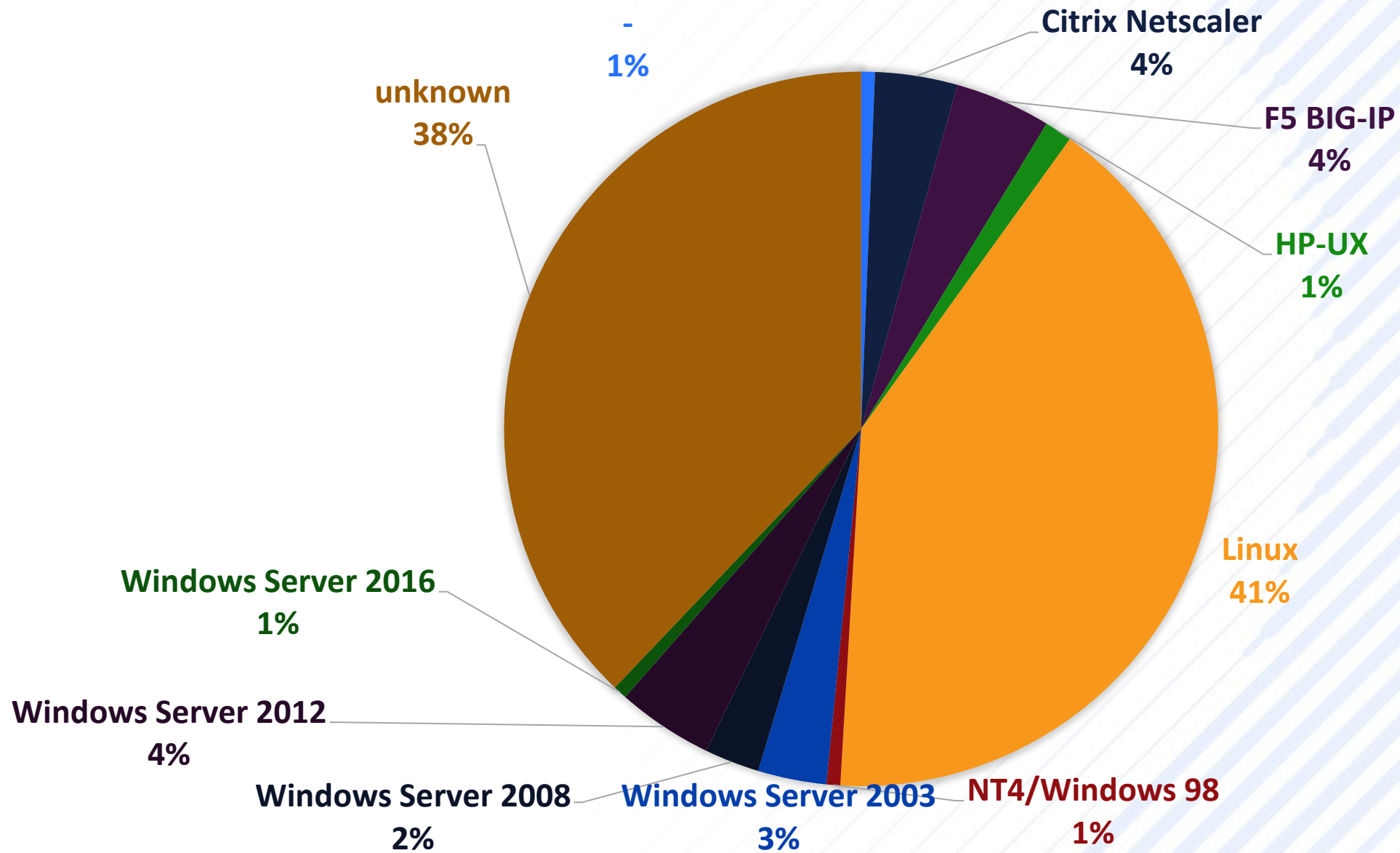
# By Industry

WEBSITE WITH UNSECURE FILE UPLOAD



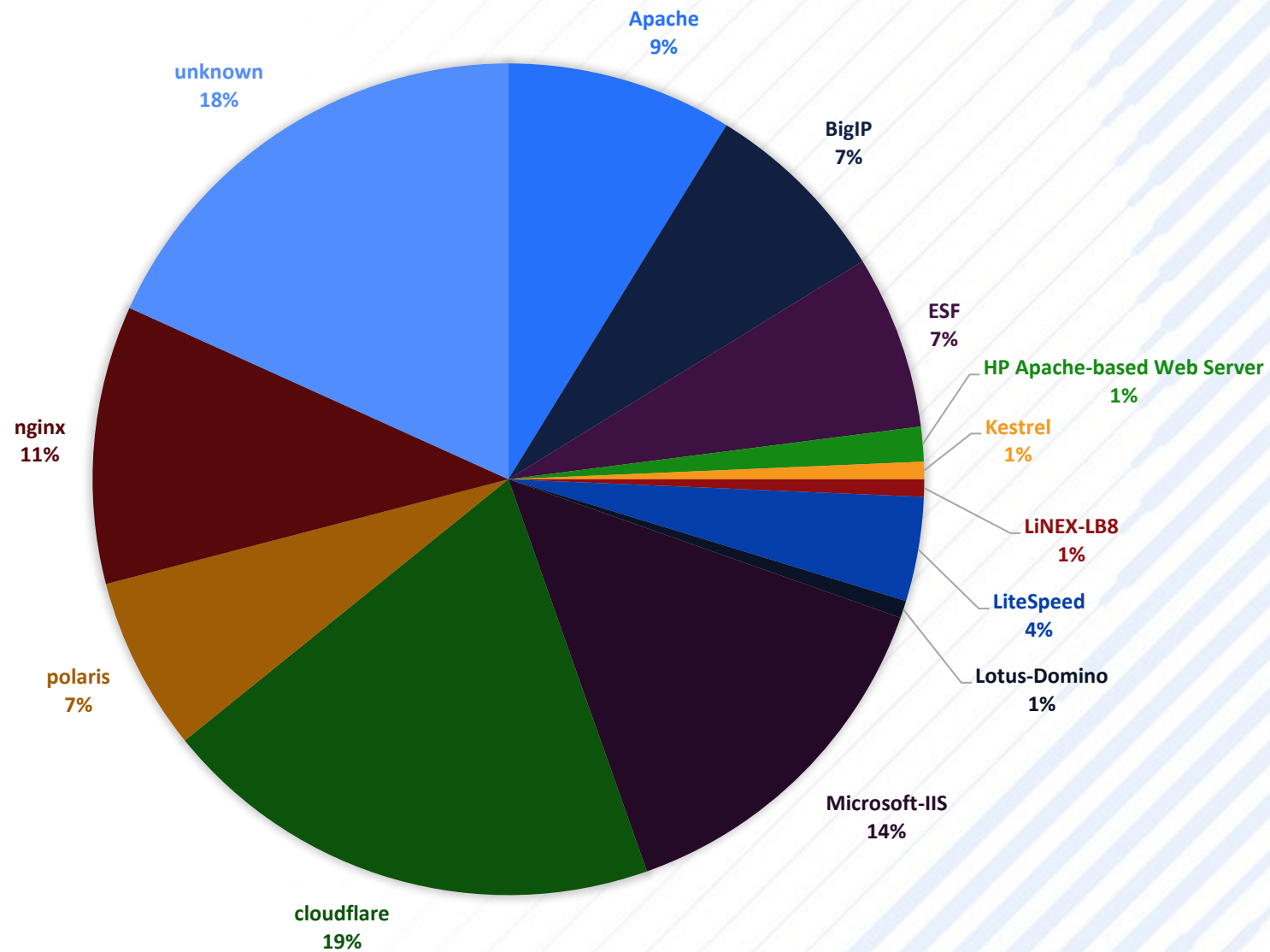
# By OS

WEBSITE WITH UNSECURE FILE UPLOAD



# By Webserver

## WEBSITE WITH UNSECURE FILE UPLOAD



OPSWAT.

---

# OPSWAT File Upload Security

# Unsecured File Uploads in Web Applications

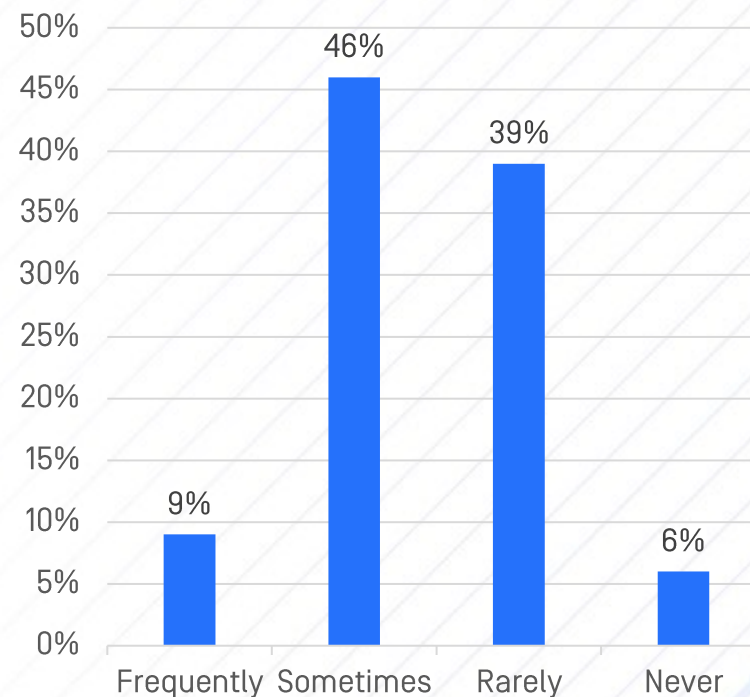
43% of breaches were attacks on web applications

- 10% attacks used file upload
- 13% attacks used local file injection, which usually involves an uploaded file

Existing perimeter network gateways are not equipped for deep inspection of files

Common risks:

- Attack organization's infrastructure
- Attack application users
- Upload enormously large files
- Hosting malicious payload on reputed sources



Has web-borne malware bypassed your WAF within last 12 months?

Source: Ponemon Institute: Trends in Cost of Web App DDoS Attacks

# Best Practices for File Uploads in Web Application Security

---



Authenticate Users



Scan All Files for Malware



Store Uploaded Files Outside the Web Root Folder



Limit the Specific File Types



Check Files for Vulnerabilities



Set Maximum File Name Length and Size



Use Simple Error Messages



Verify Actual File Types



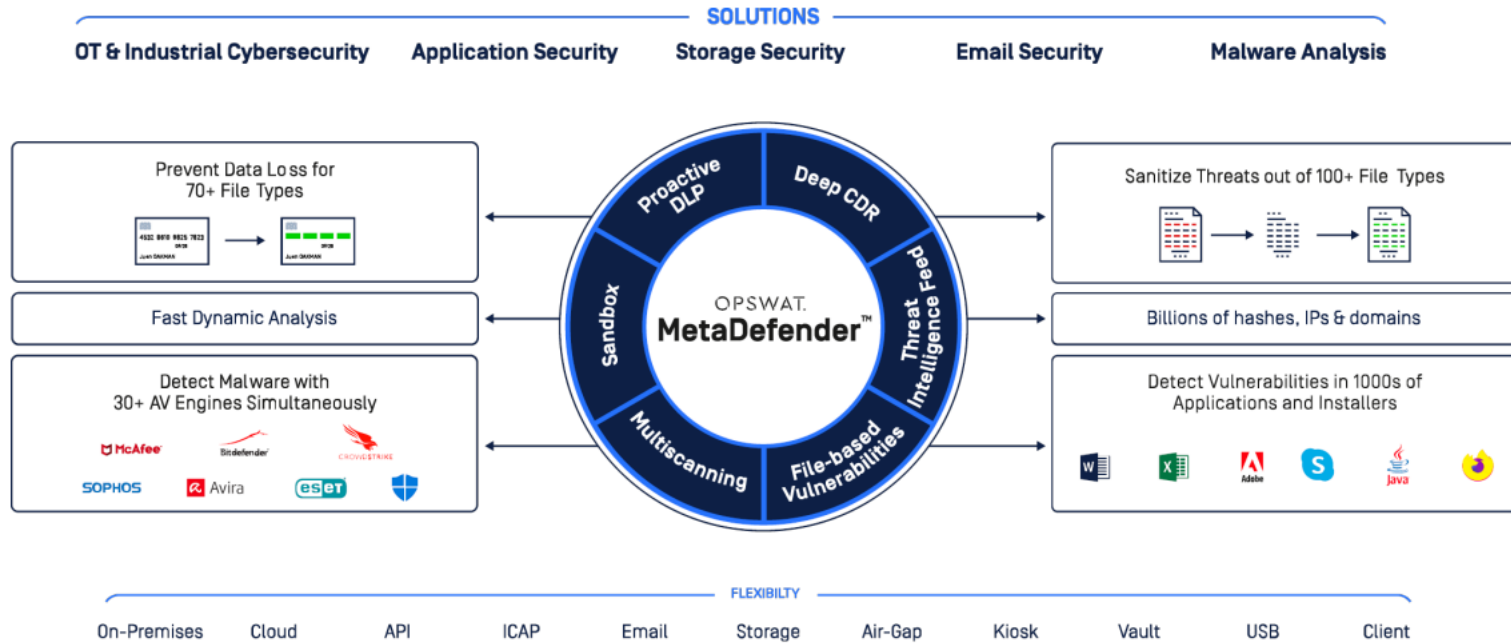
Randomize File Names



Remove Embedded Threats with CDR

# Powerful Advanced Technologies

Detection and Prevention of Known and Unknown Malware



**Multiscanning with Metascan** – Leverage 30+ anti-malware engines to detect nearly 100% of known threats

**Deep CDR** – Disarm active embedded threats and reconstruct every file to prevent zero-day and advanced evasive malware

**Proactive DLP** – Check for sensitive and confidential file content to prevent data leakage

**File-based Vulnerability Assessment** – Scan and analyze binaries and installers to detect vulnerabilities before exposure

**Sandbox [cloud]** – Analyze malware with fast dynamic analysis

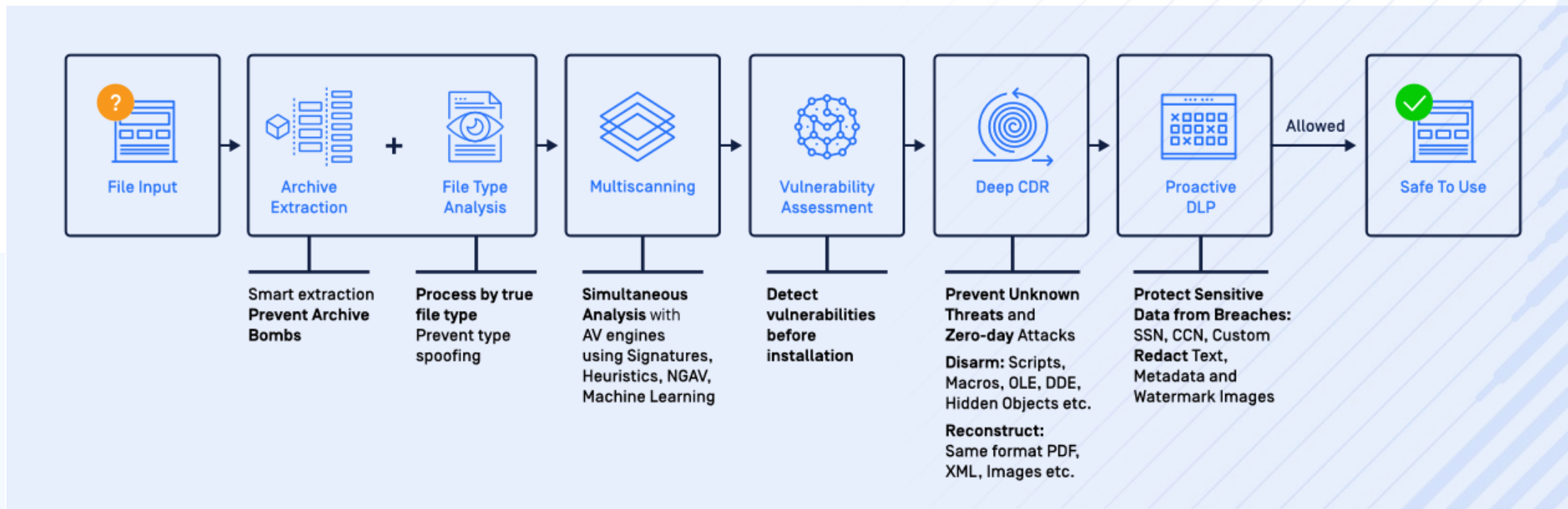
**Threat Intelligence [cloud]** – Provide enriched intelligence on threats on billions of hashes, IPs and domains





# File Processing Workflow

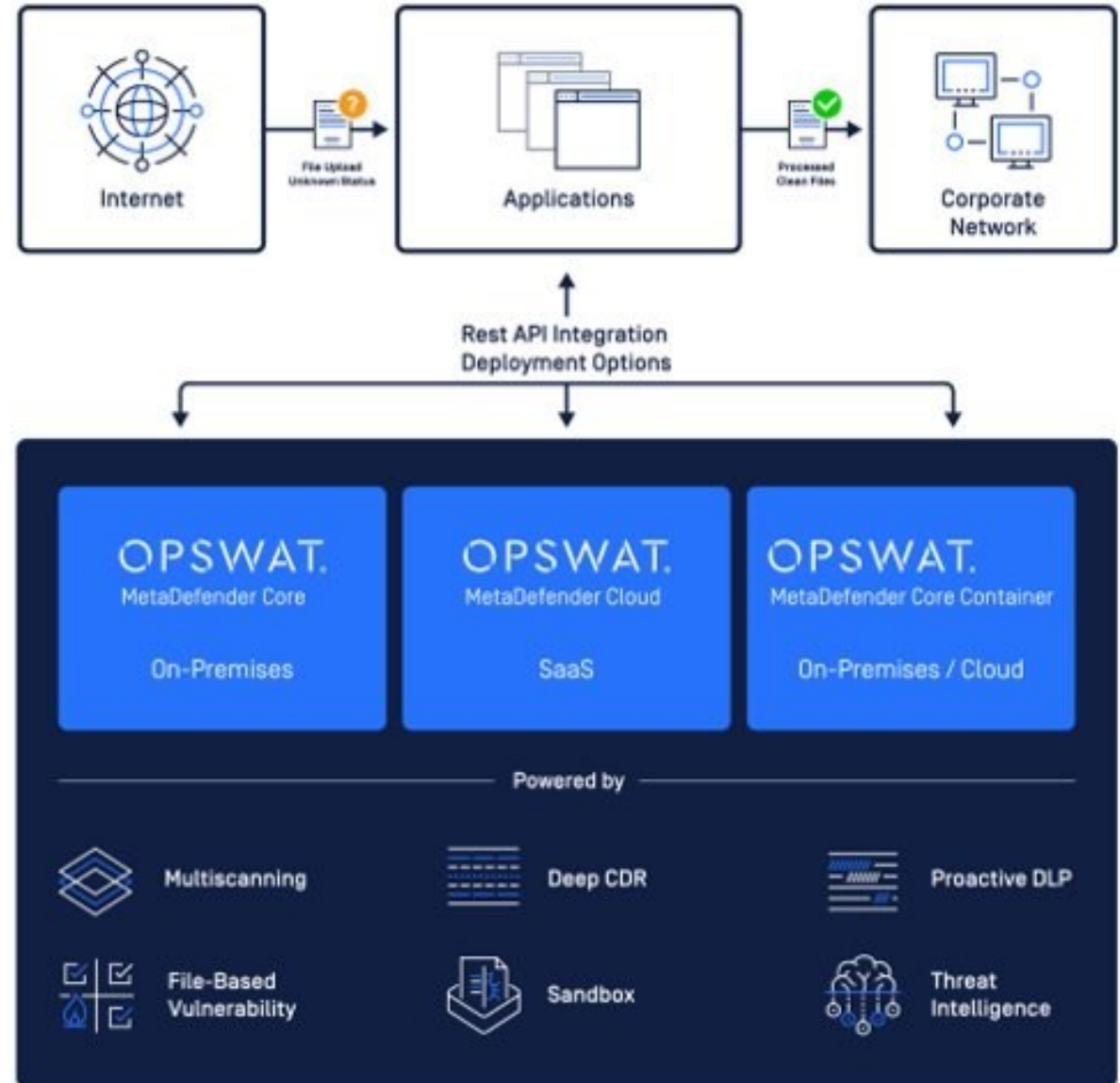
Enterprise performance with ability to analyze 10 files per second, per deployment



# MetaDefender Core

## Features and Benefits

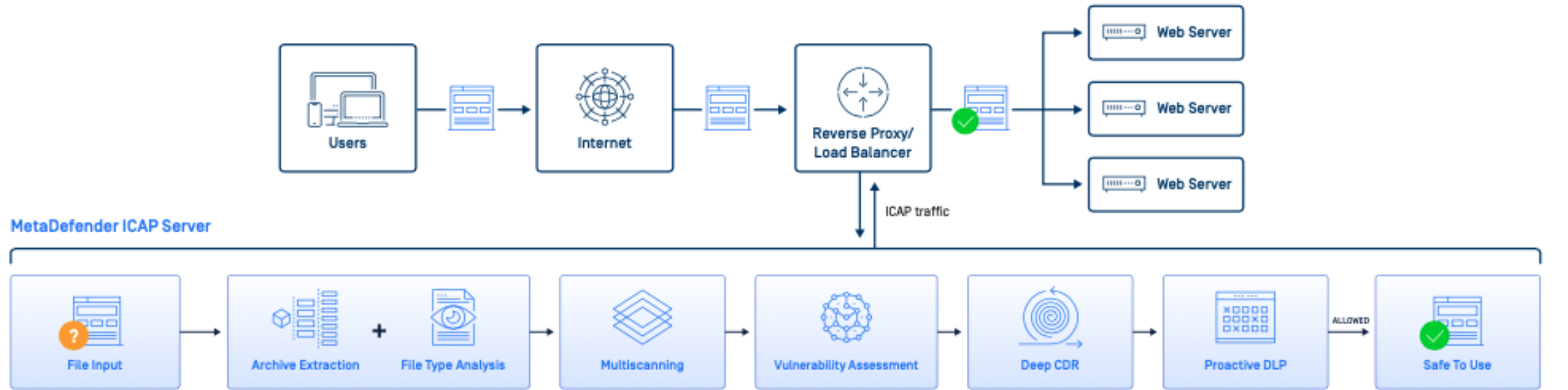
- Comprehensive protection with proprietary advanced technologies
  - Detection rates greater than 99%
  - Zero-day attack prevention
  - Sensitive data protection
- Meet regulatory compliance requirements
  - Prevent sensitive data entering or leaving your organization
  - Cloud Storage vulnerability detection and malware prevention
- Simple and flexible deployment options
  - On-premises, air-gapped, private cloud, SaaS
  - AWS, Azure
  - Windows or Linux
  - ICAP enabled devices: Reverse and Forward Proxy / Web Application Firewall / Load Balancer / Firewall / Web Gateway / MFT
- High performance and scalability
  - Faster outbreak detection
  - Low false positives
- Low total cost of ownership (TCO)
- Continuous visibility and control
- Custom security policies and workflow



# MetaDefender ICAP Server

Plug-and-play malware prevention solution for network devices

- Quickly extend MetaDefender's advanced malware prevention technologies to your perimeter
- Simple integration with any ICAP enabled device: Reverse and Forward Proxy / Web Application Firewall / Load Balancer / Firewall / Web Gateway / MFT
- Prevent sensitive data entering or leaving your organization



# MetaDefender Cloud

Cloud-based threat prevention and malware analysis

Consume MetaDefender Cloud through our UI or REST APIs

- Prevent file-based attacks by leveraging multi-scanning with top-tier AV engines that provides a detection rate of **99.4%**
- Defend against zero-day attacks utilizing Deep CDR to sanitize and reconstruct files while preserving their integrity and quality
- Detonate malicious [or potentially malicious] content in OPSWAT Sandbox to understand it's behavior
- Verify the safety of IPs, domains, and URLs by scanning them against our aggregation of multiple real time, reputation sources

## Primary use cases



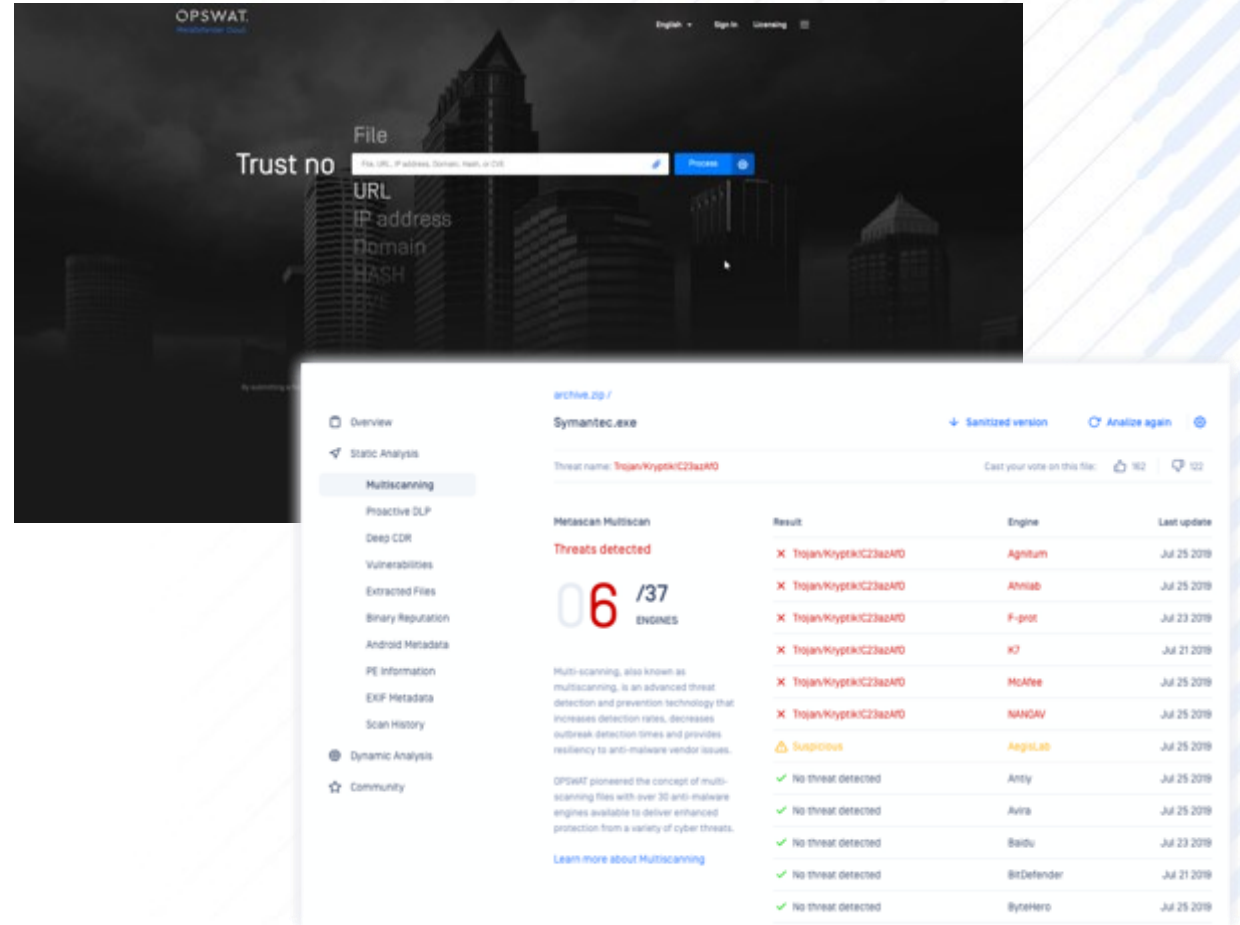
Prevent malicious file uploads



Perform malware analysis



Prevent unknown threats



OPSWAT.®

---

**Technologies**

# Multiscanning

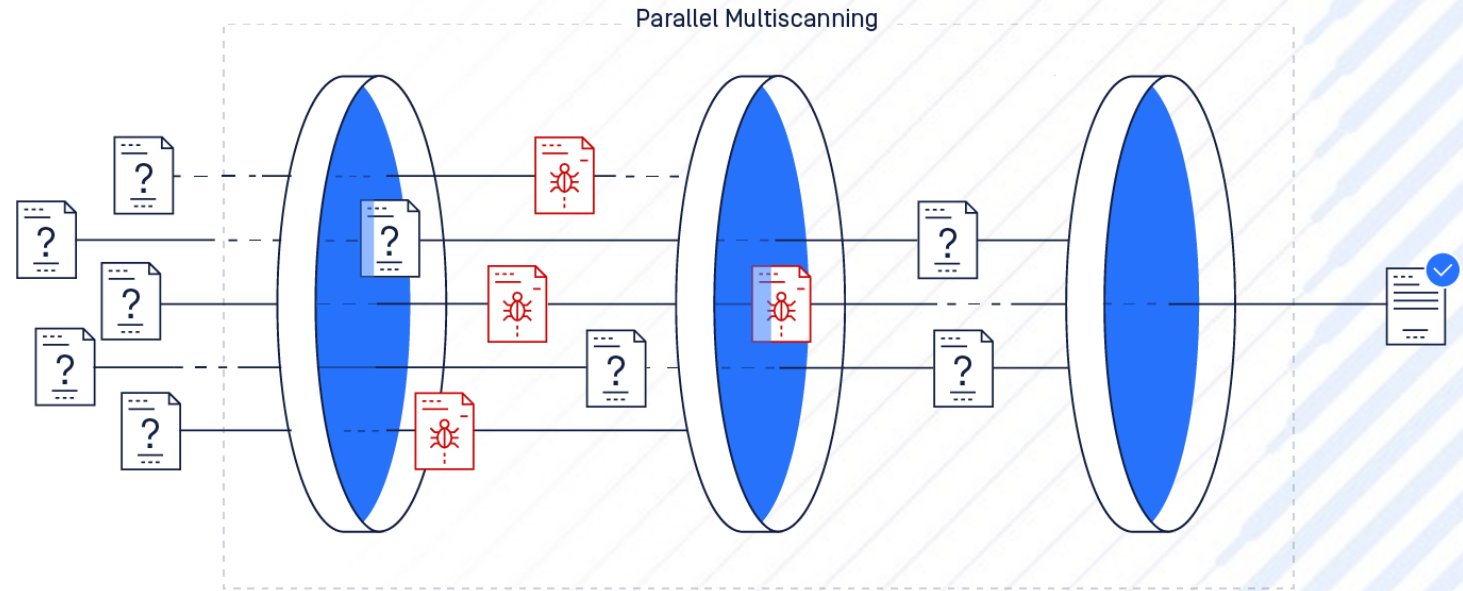
---

OPSWAT.

# OPSWAT Metascan

## Multiple layers of defense

- Combine 30+ commercial anti-malware engines into one platform
- Combine analysis mechanisms/techniques [Signatures, Heuristics, AI/ML, Emulation, etc.] to increase detection ratio
- Detection optimization
- Not replacing AV on endpoint



# Why Multiscanning

- Different vendors will be the first to discover new malware (polymorphic & non-polymorphic)
- Some vendors may take days, weeks, months, or even years to add detection
- Vendors use proprietary heuristic algorithms
- Different algorithms have their own strengths and weaknesses
- Proactive defense
- Defense in depth

0b56a52ba6dc4ad79f6895e5fcd06672.html  
Hypertext Markup Language - 108.9 KB  
Infected

File process | LOCAL/admin | Nov 8, 2021 at 6:41:17 PM | Nov 8, 2021 at 6:41:17 PM | 805 ms

METASCAN™ | DEEP CDR | PROACTIVE DLP | VULNERABILITY ASSESSMENT | FILE TYPE VERIFICATION | YARA

Engine	Result	Definition Date	Scan Time
...	✓ No Threat Detected	2021-11-09 (9 hours ago)	108 ms
...	✗ JS/Agent.G1	2021-11-08 (a day ago)	10 ms
...	✓ No Threat Detected	2021-11-08 (22 hours ago)	29 ms
...	✓ No Threat Detected	2021-11-08 (17 hours ago)	67 ms
...	✓ No Threat Detected	2021-11-08 (a day ago)	18 ms
...	✓ No Threat Detected	2021-11-08 (a day ago)	324 ms
...	✗ Exploit [04c55c361]	2021-11-08 (19 hours ago)	6 ms
...	✗ JS.Trojan.37225	2021-11-08 (a day ago)	42 ms



# Improved Malware Detection

The more anti-malware engines added, the better the malware detection rates

MetaDefender Core Package	4 Engines	8 Engines	10 Engines	12 Engines	15 Engines	16 Engines	20 Engines	Max Engines	Cloud *
Detection of top 10000 threats	86.20%	88.80%	90.00%	91.00%	94.60%	93.80%	95.20%	98.50%	97.80%

The most searched for threats on MetaDefender Cloud based on user requests

\* Commercial Cloud with 20+ engines. For a complete list see our [licensing](#) page



# Example

**Threats Found**

UST.exe

SHA256 13C46E83D2DFF56078BE8D3E1F91A10C8E52A6B23E24C78

THREAT NAME Trojan/Variant!FeBA9zn2 [Learn more](#)

---

MULTISCAN SCORE

**1/42**

VULNERABILITY SCORE

[REPORT VULNERABILITY](#)

No vulnerabilities reported!

November 2015

Only 1 AV scanner found the threat (Filseclab)

**Threats Found**

UST.exe

SHA256 13C46E83D2DFF56078BE8D3E1F91A10C8E52A6B23E24C78

THREAT NAME Trojan/Variant!FeBA9zn2 [Learn more](#)

---

MULTISCAN SCORE

**4/42**

VULNERABILITY SCORE

[REPORT VULNERABILITY](#)

No vulnerabilities reported!

February 2016

Only 4 AV scanners found the threat (Antiy, AegisLab, Filseclab, and Zillya)

**Threats Found**

UST.exe

SHA256 13C46E83D2DFF56078BE8D3E1F91A10C8E52A6B23E24C78E6566C6334829DF5A

THREAT NAME Trojan/Variant!FeBA9zn2 [Learn more](#)

---

MULTISCAN SCORE

**16/39**

VULNERABILITY SCORE

[REPORT VULNERABILITY](#)

Until May 2020

Only 16 scanners found the threat, many of the best-known AV still do not detect this malware

# Faster Outbreak Detection

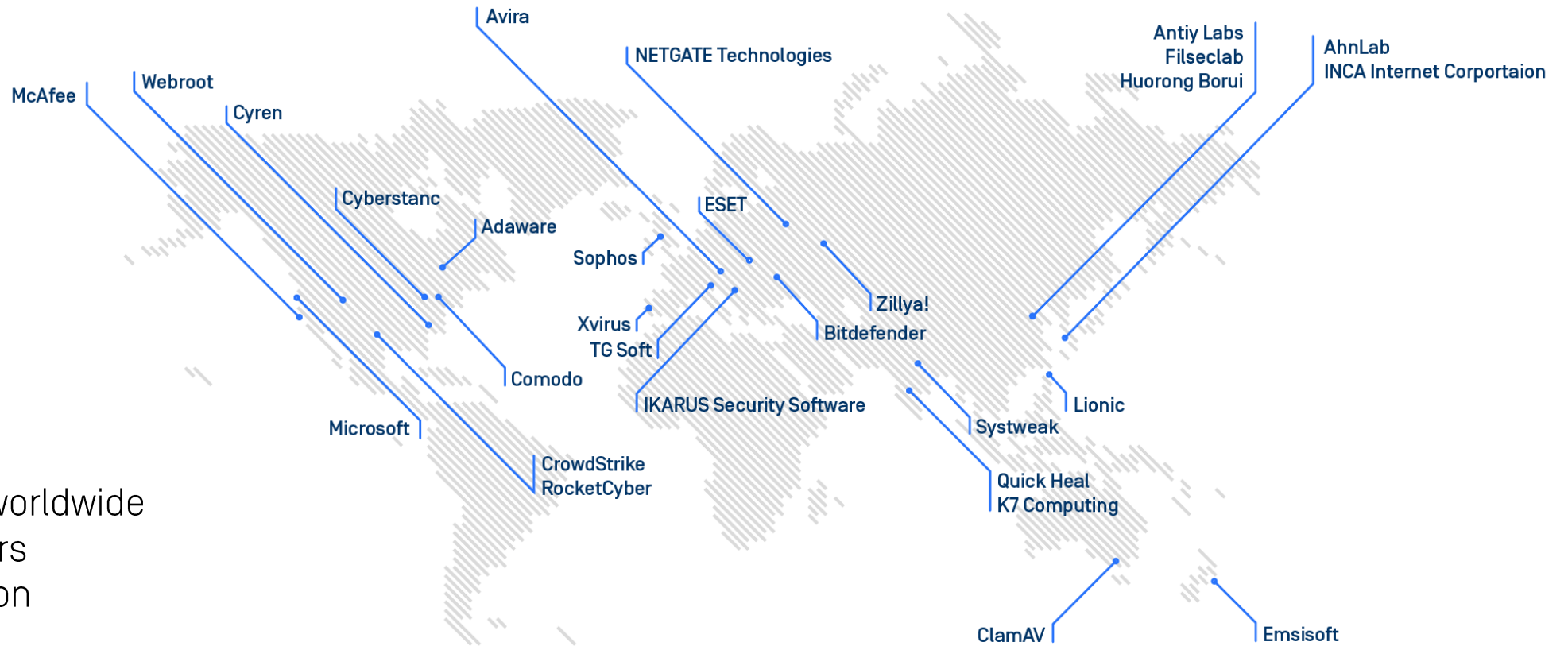
More anti-malware engines are added, malware detection rates improves

MetaDefender Core	Vulnerable Time*	Outbreaks detected
◇ 8 Engines	132.32	188
◇ 12 Engines	115.20	246
◇ 16 Engines	107.76	253
◇ 20 Engines	102.48	256
◇ Max Engines	100.54	256
☁ Cloud Engines	97.55	256



# Wide Malware Detection Coverage

Quickly respond to regional malware outbreaks



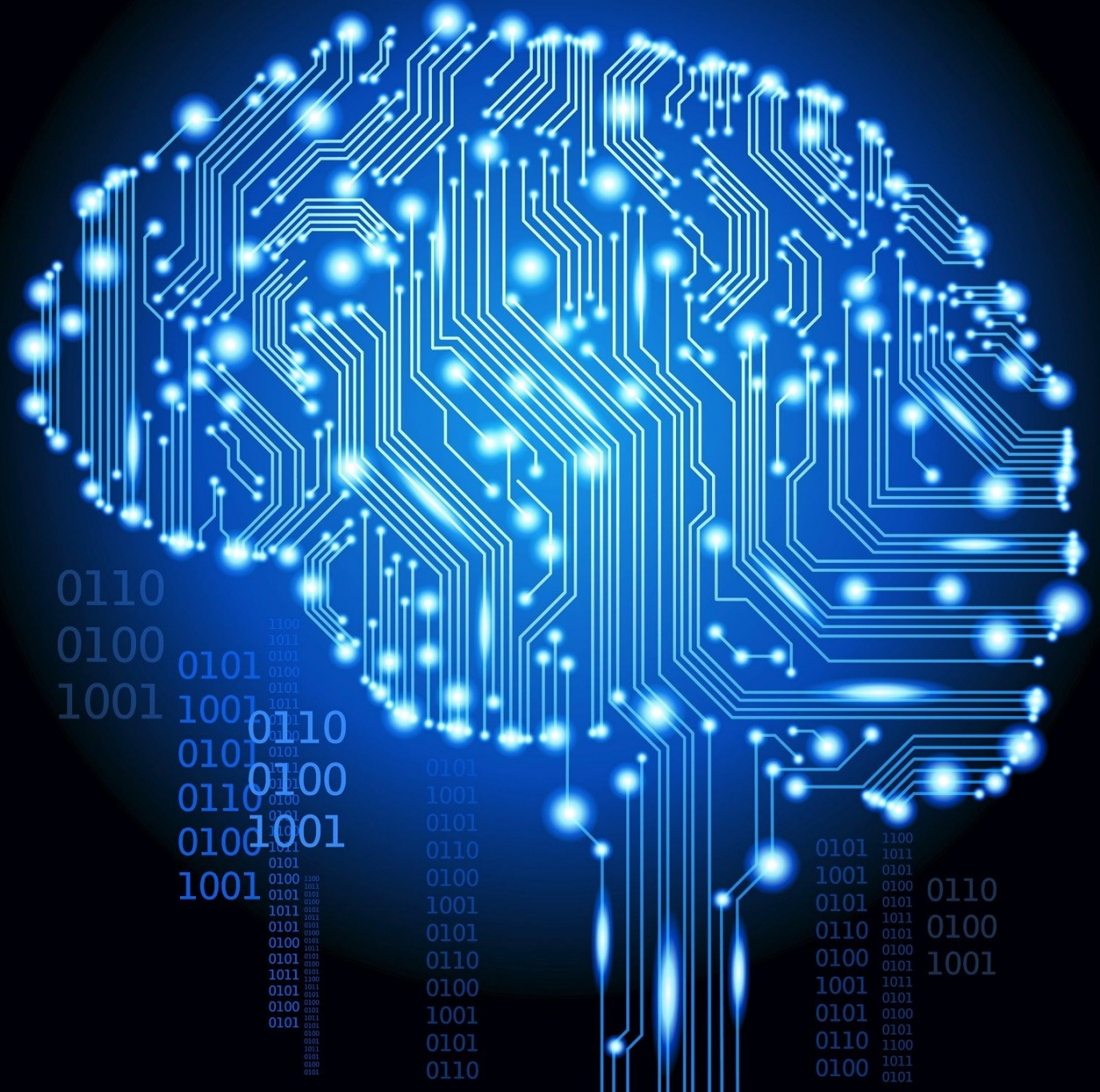
OPSWAT worldwide  
AV vendors  
distribution



# Machine Learning Engines

- ✓ Do not require signatures and heavy updates frequently
- ✓ Particularly effective at stopping new, polymorphic or obfuscated malware

OPSWAT's AV vendors:



Proactive DLP

---

OPSWAT.

# Proactive Data Loss Prevention

Detect and Block Sensitive Data in Files and Emails



# Features

Prevent Potential Data Breaches and Regulatory Compliance Violations



Detect and Redact



Watermark



Remove Metadata





# Detection

70+ file types supported

Credit Card Number

- **NOT** just 16 digits check
- **Luhn10** algorithm check
- BinBase (bank identification number) database check

Social Security Number

- Challenge: Possible False Positive
- Solution: Context checking

IPv4/CIDR [Classless Inter-Domain Routing]

Regular expression to define your own sensitive info detection

Secrets in text files (AWS, Microsoft Azure, and Google Cloud Platform)

Column/header-based detection

The screenshot displays a security tool interface. At the top, there is a search bar with the text "Process a file or search for history by HASH" and a "Process" button. Below this, a file named "embedded\_text.docx" is shown, identified as a "Microsoft Word Document - 12.7 KB". A red "BLOCKED" status is visible, along with a "Sensitive Data Found" warning. The interface includes a breadcrumb trail: "File process | LOCAL/admin | Nov 8, 2021 at 6:05:17 PM | Nov 8, 2021 at 6:05:17 PM | 44,498 ms". A list of files extracted from the archive is shown, including "word\embeddings\oleObject1.docx" (marked "Sen"), "word\fontTable.xml", "word\document.xml", "word\styles.xml", "word\\_rels\document.xml.rels", "\_rels\.rels", "word\media\image1.emf", "docProps\app.xml", "docProps\core.xml", "[Content\_Types].xml", and "word\settings.xml". On the right, an "Actions" section shows "File redacted" and "Metadata removed". Below this is a table of detected data types:

Data Type	Certainty ↓	Hit
Credit Card Number	Medium	adipiscing elit. Quisque malesuada eget
Social Security Number	Low	semper non purus id, posuere <b>XXXXX44</b>
Social Security Number	Low	justo dapibus imperdiet. Suspendisse ac

At the bottom, there is a pagination control showing "1-11 of 11" and a dropdown menu set to "100 items per page".



# Redaction

✓ Separated certainty level for each sensitive info type.

E.g.: Only redact high certainty SSN but all detected Credit Card info

✓ Supported file types:

Portable Document Format [PDF]

Microsoft Office Word [DOC/DOCX]

Microsoft Office Excel [XLS/XLSX]



Credit Card Authorization Form  
One-Time & Repeat Gifts

### CARDHOLDER INFORMATION

Name: Brandon Patterson  
Billing Street Address: 7134 Glenridge Road  
Street Address (cont.): \_\_\_\_\_  
City: Mahwah State: NJ Postal Code: 07430  
Country: U.S. Email: [REDACTED]  
Address: \_\_\_\_\_  
Direct Telephone: (\_\_\_\_) \_\_\_\_\_ - \_\_\_\_\_

### GIFT INFORMATION

Fund Name or Gift Purpose: Give a gift to my son  
 I authorize a one-time charge against my credit card for the follow amount \$ 500.0  
 I authorize a recurring charge against my credit card for the following amount

### CREDIT CARD INFORMATION

Credit Card Type:  MasterCard  Visa  American Express  Discover Card  
Number: [REDACTED]  
Expiration Month: 5 Expiration Year: 2020  
Cardholder Signature X \_\_\_\_\_ Date 5 / 21 / 2019  
Security Code: 783

Text-searchable

Hey I want to send you my credit card information to enable you to use it for payments. Here goes the front side.



The actual numbers are: 4532 8613 9890 7018

Original document

Hey I want to send you my credit card information to enable you to use it for payments. Here goes the front side.



The actual numbers are: [REDACTED]

Redacted document

Non-text-searchable



# Watermark

✓ Supported file types:

JPEG

TIFF

PNG

GIF

PDF

✓ Flexible input string from client



Downloaded from 56.34.123.24



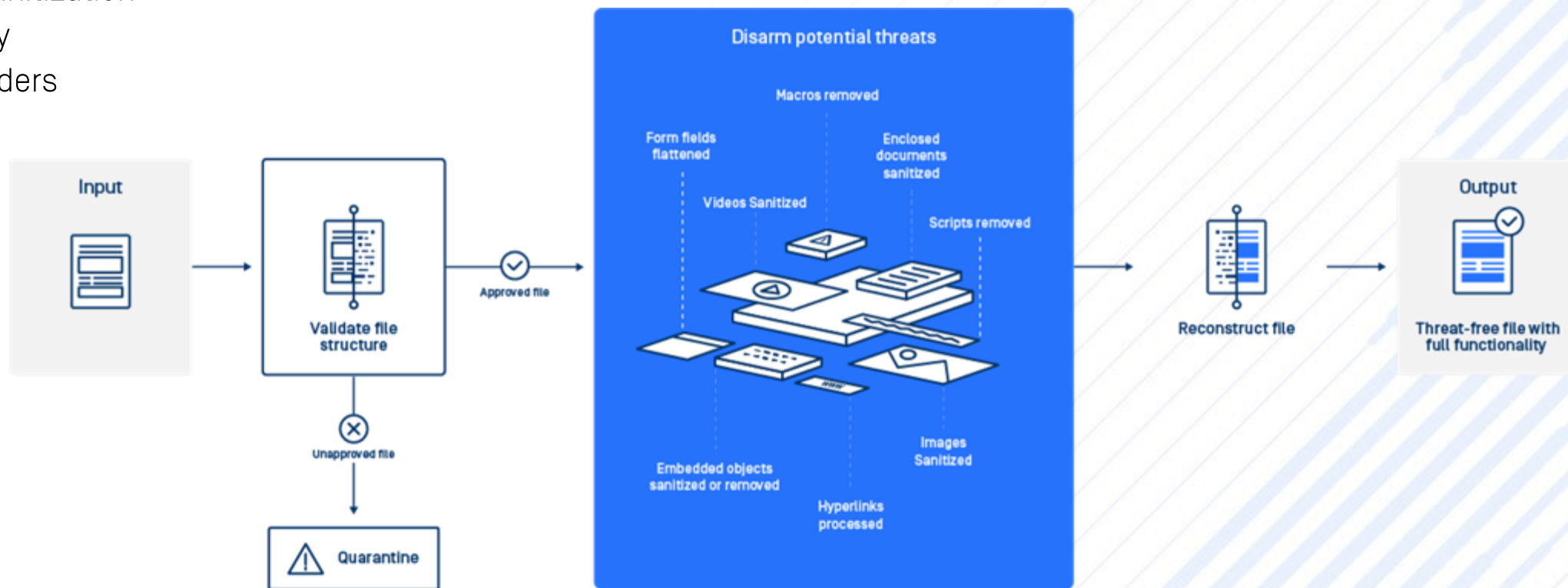
Deep CDR



OPSWAT.

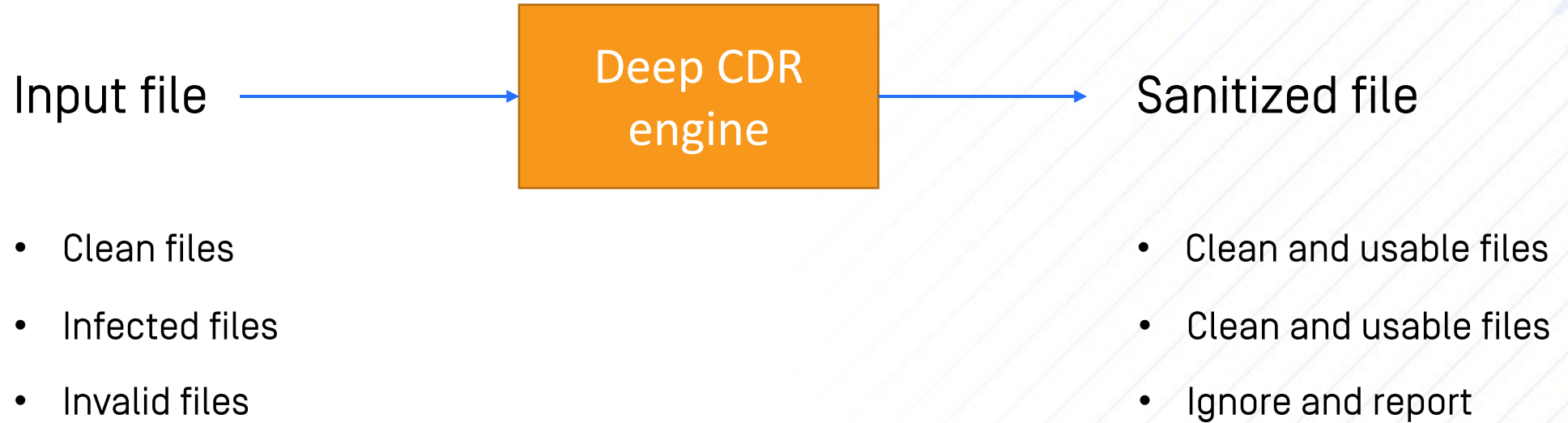
# Deep Content Disarm and Reconstruction

- Extensive coverage: 100+ file types, 200+ sanitization/conversion options, 4500+ file type verification
- Recursive sanitization within milliseconds even for nested archives
- Remove all embedded active content
- Deep Image Sanitization
- Steganography
- Metadata/Headers
- Hyperlinks



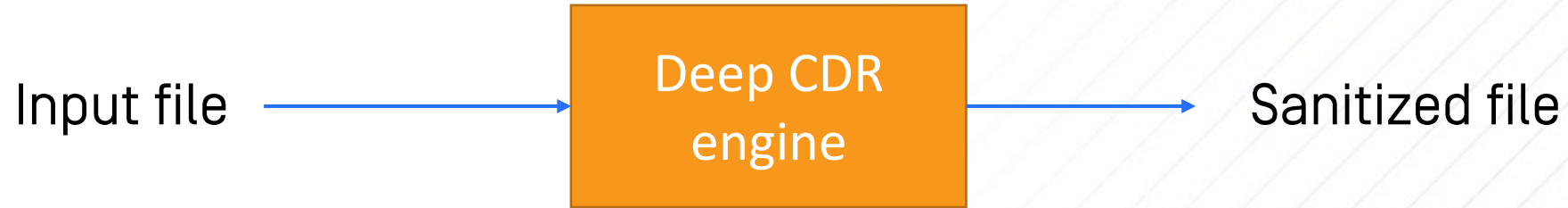
# Deep CDR workflow

---



# Deep CDR workflow

---

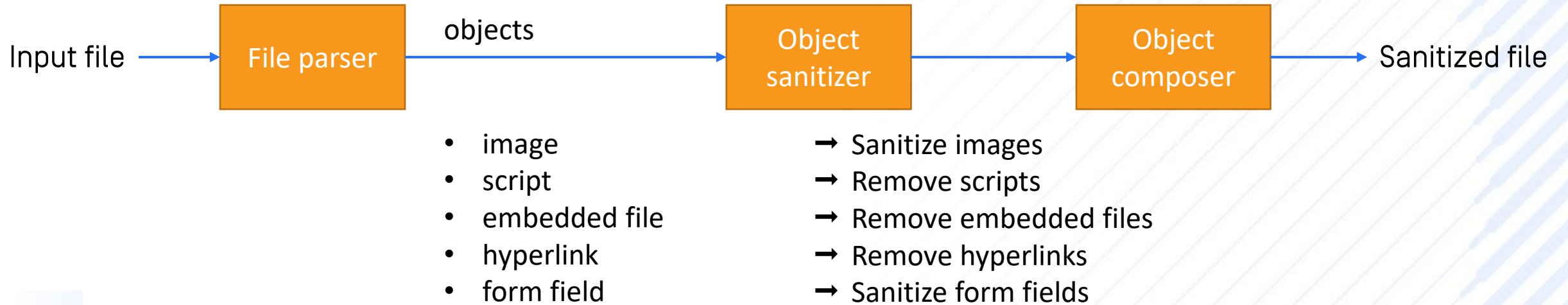


## Challenge: security vs. usability

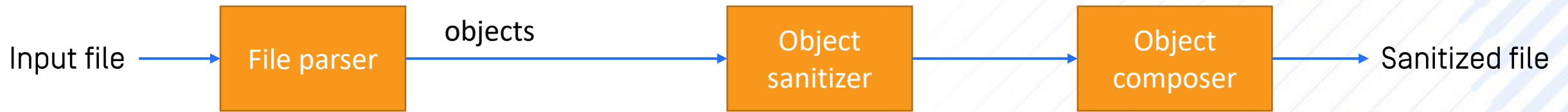
- Security
  - Remove all potential-to-have-threat objects
- Usability
  - Keep usable content: interactive, active



# Deep CDR workflow



# Deep CDR workflow



## File parser: key and challenging parts

- Help sanitize every object and detail in the file
- Ensure integrity of file content after reconstruction
- Comprehensive understanding of file structures
- Strong skills on designing and creating architecture
- Cover all possible cases: wide variant, special, exceptional, invalid

## Our own parsers

- PDF, CSV
- DOCX, XLSX, PPTX
- MP3, WAV, MP4, AVI
- ICS, VCS
- TIFF, WMF, EMF
- OLE, EML, MSG



# Our work

PDF content (partially redacted):

```
1 %PDF-1.7
2 %uuum
3 1 0 obj
4 <</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot
  135 0 R/MarkInfo<</Marked true>>/Metadata 1066 0
  R/ViewerPreferences 1067 0 R>>
5 endobj
6 2 0 obj
7 <</Type/Pages/Count 39/Kids[ 3 0 R 19 0 R 24 0 R 31 0 R
  33 0 R 37 0 R 40 0 R 43 0 R 46 0 R 49 0 R 52 0 R 55 0 R
  58 0 R 61 0 R 64 0 R 66 0 R 69 0 R 72 0 R 75 0 R 78 0 R
  83 0 R 86 0 R 89 0 R 91 0 R 94 0 R 97 0 R 100 0 R 103 0 R
  104 0 R 106 0 R 109 0 R 112 0 R 115 0 R 118 0 R 121 0 R
  125 0 R 127 0 R 129 0 R 132 0 R]>>
8 endobj
9 4 0 obj
10 <</Filter/FlateDecode/Len
  stream
11 xœ-UÛNÛ@DDE}·"Œ]D6;EÖ^$,,E
12 ASO,,
13 dÉ-Niî9ÇgfBBI GUJL°>SUBŽG'
14 îE äw"'=1-'!) "îçâ;ÊUS-KfR
  ÔSOËSTXe...Ö`*VT*DC4ÛzUSA
  BBI BBI jÑÈÙ DLEá! ESSTÛj
15 DÔJ&`c·ÛçJ»} @ôÄESCHST¿) `<
```

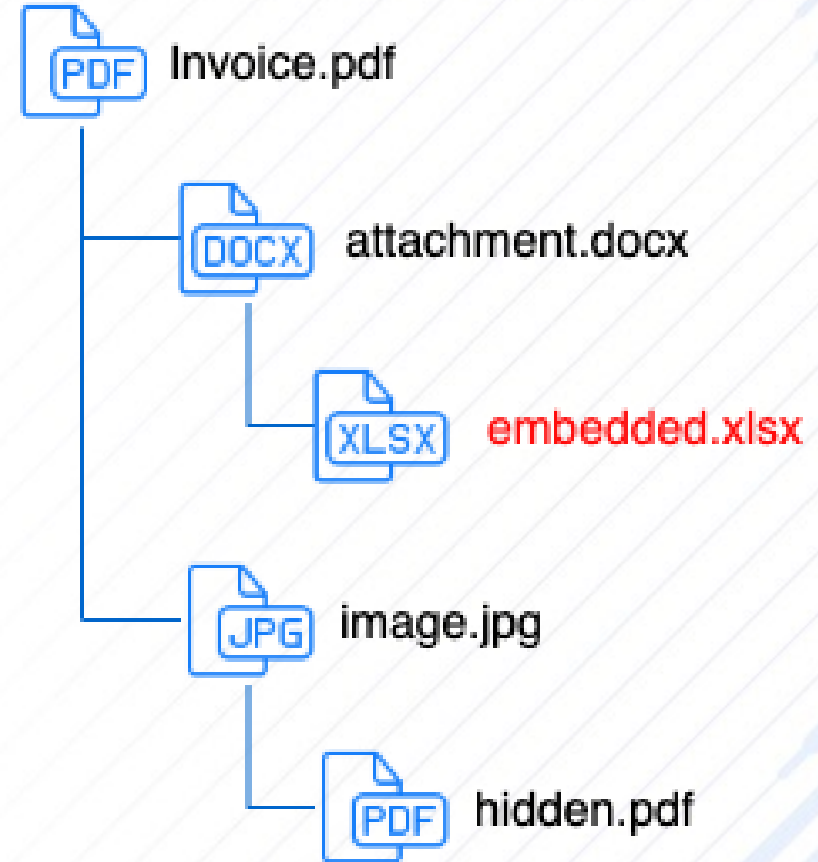
Name	Size	Packed Size	Modified	CRC	Method	H...	Offset
charts	86 664	13 662		4584A184			
drawings	3 886	758		17006515			
embeddings	36 457	36 457		9597DDD0			
media	7 343 309	7 343 309		575029B3			
notesMasters	7 827	1 645		458CBC98			
notesSlides	102 084	35 338		AEC29EE3			
slideLayouts	29 085	8 260		AAAC749B			
slideMasters	10 802	1 637		ACF4DB22			
slides	402 169	76 681		3D9782F1			
theme	13 494	3 080		239C75C6			
_rels	6 391	540		AB0C920E			
commentAuthors.xml	401	232	1980-01-01...	FC945B0E	Deflate:Fastest	FAT	1 968 954
presentation.xml	7 942	1 647	1980-01-01...	E2852D00	Deflate:Fastest	FAT	15 424
presProps.xml	1 554	611	1980-01-01...	041FE61D	Deflate:Fastest	FAT	7 546 351
tableStyles.xml	1 853	527	1980-01-01...	41B94800	Deflate:Fastest	FAT	7 547 009
viewProps.xml	1 467	503	1980-01-01...	B69E9232	Deflate:Fastest	FAT	7 545 801

Hex editor content (Offset 00000000):

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	Decoded text	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	PNG.....I	
0000000D	48	44	52	00	00	04	03	00	00	02	A8	08	06	HDR....."	
0000001A	00	00	00	02	B5	36	39	00	00	00	01	73	52	....p69....sR	
00000027	4E	48	00	00	25	0E	10	E9	00	00	00	04	67	41	GB.ÿ.é....gA
00000034	0B	FC	61	05	00	00	00	00	00	00	00	00	00	00	MA...±...üa....
00000041	00	12	74	00	00	12	74	.pHYs...t							
00000048	00	6A	6B	49	44	41	54	.Pp.f.x..jkIDAT							
00000055	F4	D7	59	1F	78	F2	17	x^iyÿÓð×Y.xò.							
00000062	EC	CC	66	26	3F	AC	6A	iîLmîiîîf&?-j							
00000069	AD	DD	D4	A4	CA	3F	8C	Sµ5;S@.ÝÓ=Ê?E							
00000076	B0	45	42	76	37	2C	E0	&5.É..°EBv7,à							
00000083	D9	1D	70	2C	DB	4C	50	\$ãL@dØÛ.p,ÛLP							
00000090	C0	32	26	36	B1	21	42	.È.À.c^À2&±!B							
00000097	92	EC	02	4B	8A	6D	59	."Ù2Ä6'ì.KŠmY							
00000104	58	B2	2C	59	96	6D	6C	`,...ÛX²,Y-m1							

# Recursive Sanitization

- Embedded documents in a document
- Archives inside an archive
- Attachments in an email
- Real Archives
  - TAR / ZIP / RAR / CAB
- Common files
  - Office Suite [docx, xlsx, pptx, etc.]
  - PDF
  - Images [jpg, png, bmp, etc.]



# How Can You Know If The File Is Fully Sanitized?

## Processed objects

- What objects are processed?
- What were the scripts?

## Why can't Deep CDR process the file?

- Invalid file structure
- Password protected
- Unsupported version

**Recursive2.docx**  
Microsoft Word Document - 2.1 MB  
**BLOCKED** **Infected**

File process | LOCAL/admin | Nov 8, 2021 at 6:05:47 PM | Nov 8, 2021 at 6:05:47 PM | 15,863 ms

Archive extraction

- word\embeddings\Microsoft\_W... **Inf**
- \_rels\.rels
- word\\_rels\document.xml.rels
- word\document.xml
- word\media\image1.emf
- word\embeddings\Microsoft\_PowerP...
- word\media\image7.emf
- word\theme\theme1.xml
- word\media\image5.emf
- word\media\image6.emf
- word\media\image4.emf
- word\embeddings\oleObject1.bin
- word\media\image2.emf
- word\embeddings\oleObject2.bin
- word\embeddings\oleObject3.bin


Object	File Name	Action
DOC file	\word\embeddings\oleobje...	✓ Sanitized
DOCX file	\word\embeddings\ooxmlp...	✓ Sanitized
(1) OLE	-	✓ Removed
PDF file	\word\embeddings\oleobje...	✓ Sanitized
PDF file	\word\embeddings\oleobje...	✓ Sanitized
PPTX file	\word\embeddings\ooxmlp...	✓ Sanitized
XLSX file	\word\embeddings\ooxmlp...	✓ Sanitized
XML content	-	✓ Sanitized
(7) image	-	✓ Sanitized

1-20 of 25

# Hyperlink Processing

- Remove hyperlinks
- Report only and clients consume it
- Redirection: integrate with a safe redirect solution

An example with MetaDefender Cloud redirect



**Threat detected**

<http://example.infectedsite.com>

Risk Score: **1** / 8

The webpage you are trying to access has been detected as dangerous by 1 engine(s). It may perform malicious actions like installing malware or trying to capture personal information (passwords, credit cards or phone numbers).

Result	Source	Assessment	Last Detected
<b>Malicious</b>	malwaredomainlist.com	malware	June 11, 2019

Reputation intelligence data collected from multiple vendors. Please read our [documentation](#) for details.

[CONTINUE, I UNDERSTAND THE RISK](#) [VIEW DETAILS](#)



# Deep image sanitization

Effectively defend against Stegosplit

Thoroughly eliminate malware in Metadata/Header

Verified by many steganography tools

<http://stegosplit.info/>

<http://desudesutalk.github.io/f5stegojs/>

<https://www.openstego.com/>

<https://futureboy.us/stegano/encinput.html>

<https://futureboy.us/stegano/decinput.html>

<https://sourceforge.net/projects/crypture/>

<https://www.softpedia.com/get/Security/Security-Related/rSteg.shtml>

[https://download.cnet.com/Hide-N-Send/3000-2092\\_4-75728348.html](https://download.cnet.com/Hide-N-Send/3000-2092_4-75728348.html)

<https://github.com/peewpw/Invoke-PSImage>

<https://github.com/DimitarPetrov/stegify>

...more

Original image



Sanitized image

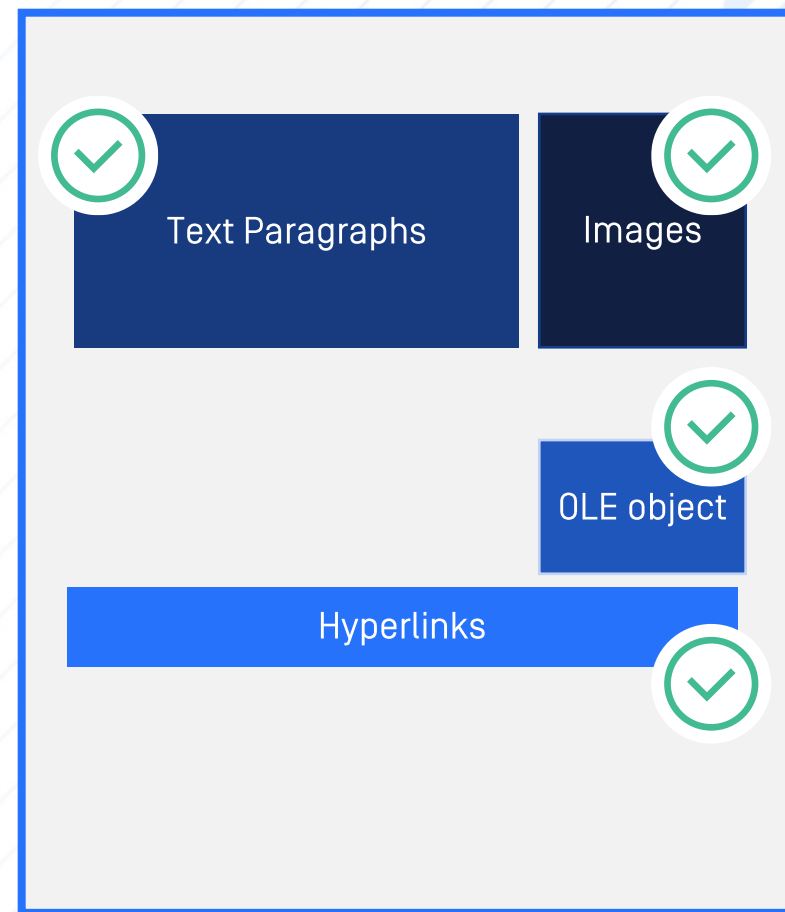


# An example with MS Office document



- Deep image sanitization
- Recursively sanitize OLE objects

AND  
reconstruct based on  
configurations





# Examples

Malware	Features	Solution	Result
<b>BLINDINGCAN North Korea</b>	<ul style="list-style-type: none"><li>Reported by FBI/CISA in Aug 2020,</li><li>use Attached Template to link to a malicious file</li></ul>	Deep CDR removes all linked files	No malware downloaded
<b>Locky ransomware attack</b>	<ul style="list-style-type: none"><li>Delivered by email with an attached MS Word file containing malicious macro</li><li>Enabled macro drops the malware</li><li>The malware detects whether it is running within a <u>virtual machine</u> or a physical machine and relocate of instruction code.</li></ul>	Deep CDR removes Macros	No malware downloaded
<b>Cobalt Strike Backdoor</b>	<ul style="list-style-type: none"><li>Exploited MS vulnerabilities CVE-2021-40444</li><li>Docx file contains an ActiveX object to download an HTML file</li><li>HTML file downloads several files and Cobalt Strike malware payload</li></ul>	Deep CDR removes OLE objects	No shellcode dropped

OPSWAT.®

---

Thank you

OPSWAT.®

---

Q&A