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

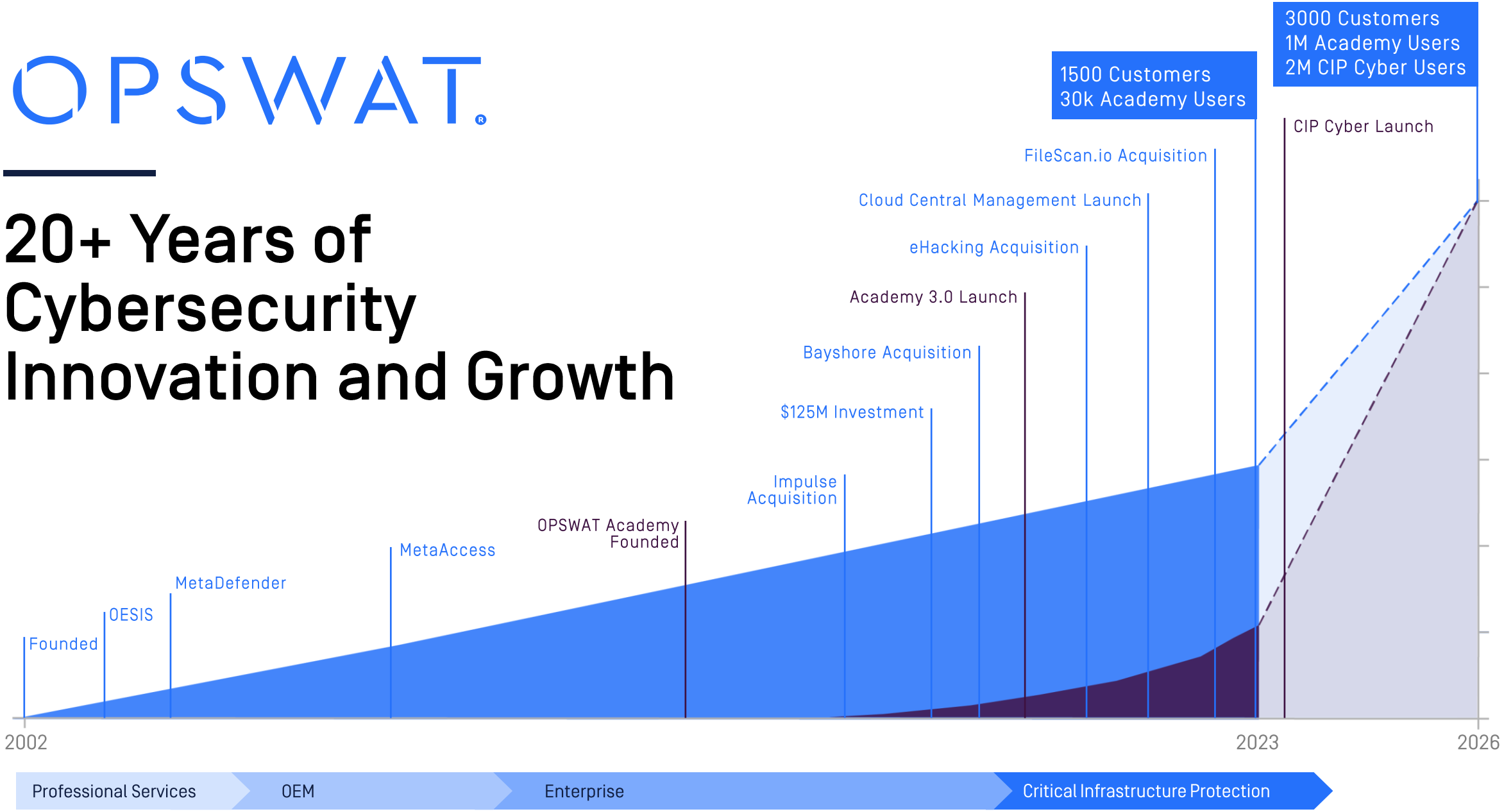
OUR MISSION

We Protect the World's Critical Infrastructure

OPSWAT.

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

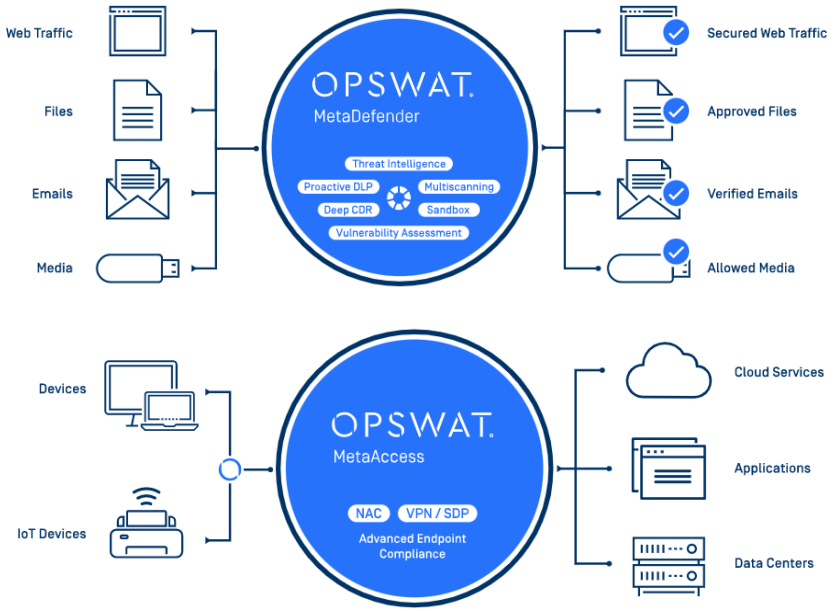
Water and Wastewater Systems

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

OPSWAT Report

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.

Input Keywords

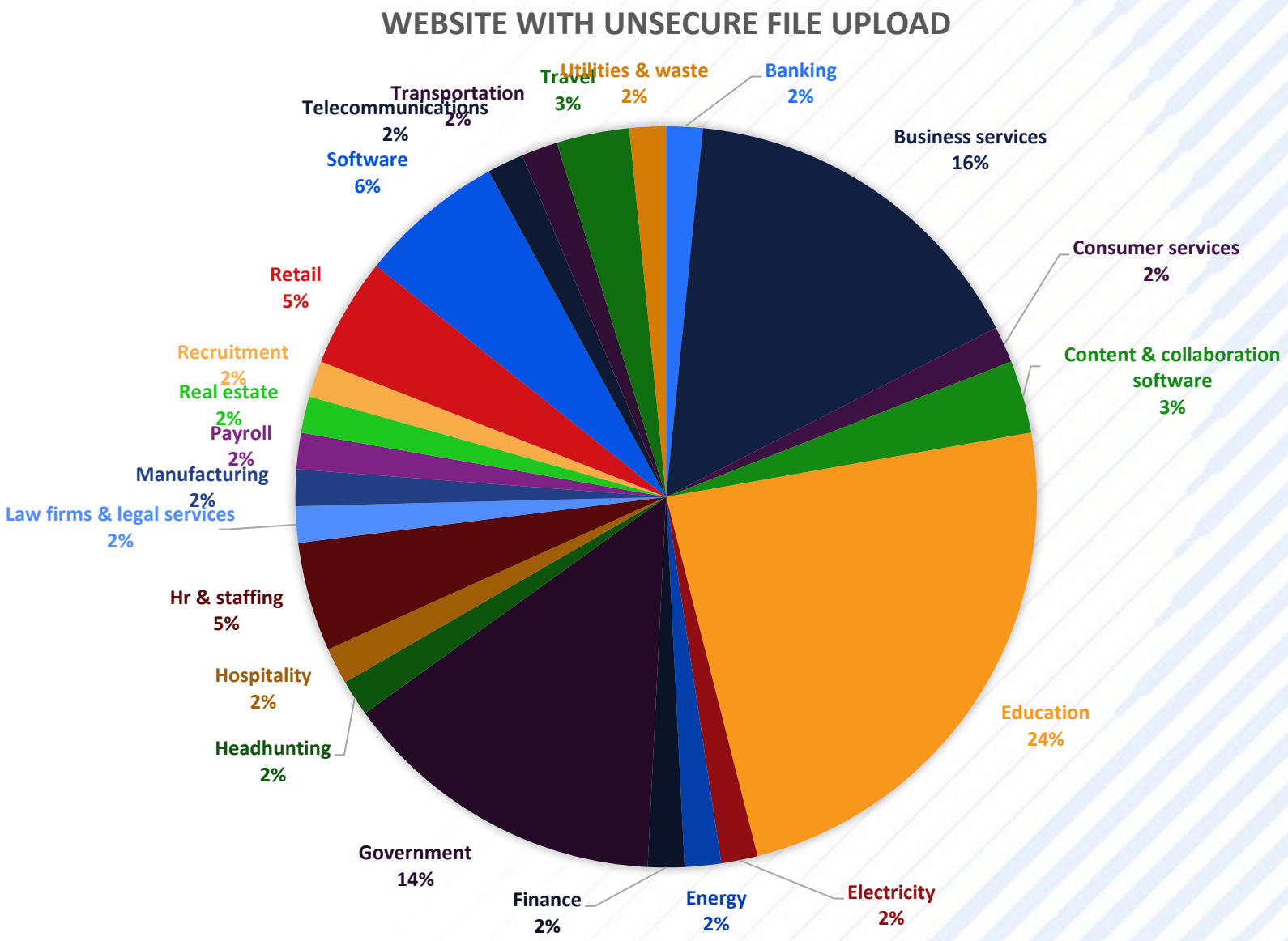
Location: United States | Select Location

SEARCH

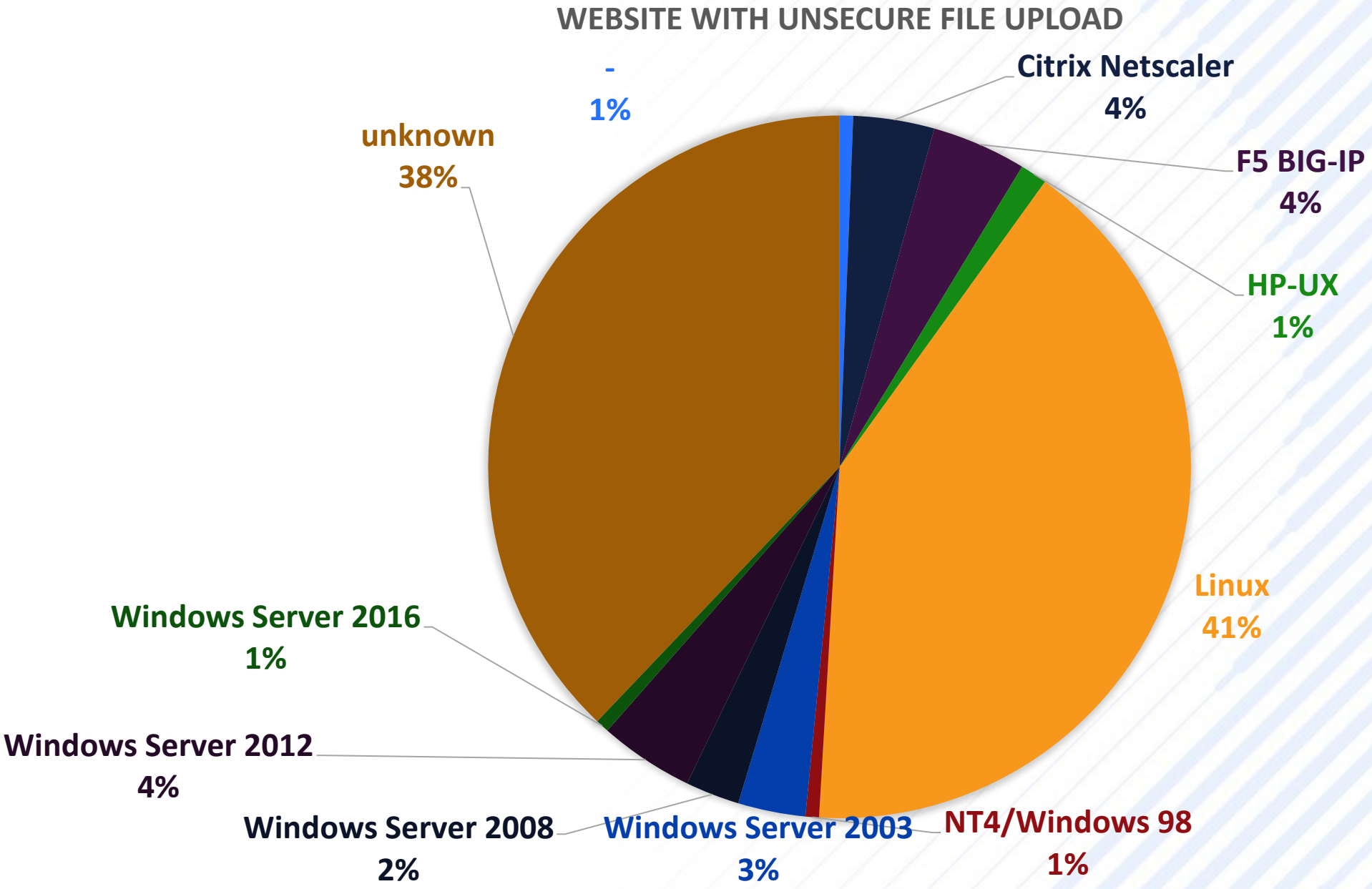
FOUND 1030 SITES

NO.	ID	ORGANIZATION NAME	WEBSITE	UPLOAD URI	LOCATION	SUGGESTED EMAIL ADDRESSES	CRAWLED AT (MM-DD-YYY HH:MM:SS)	STATUS	REAL FILE UPLOAD PAGE	ACTION
1	2	Arcade Database UNVERIFIED	adb.arcadeitalia.net	http://adb.arcadeitalia.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 UNVERIFIED	adb.arcadeitalia.net	http://adb.arcadeitalia.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... ZOOMINFO	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 UNVERIFIED	adb.arcadeitalia.net	http://adb.arcadeitalia.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 ZOOMINFO	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... ZOOMINFO	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

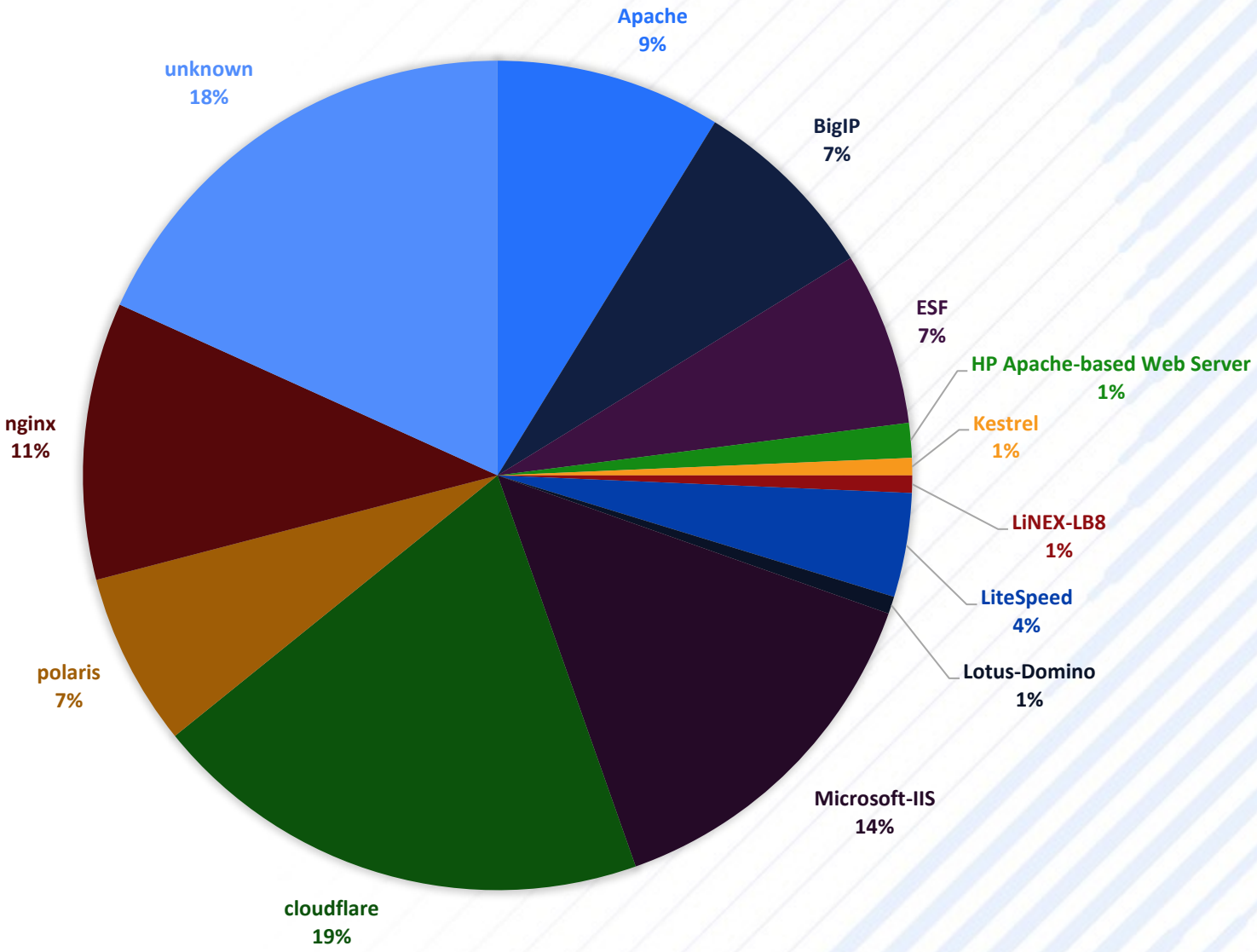


By OS



By Webserver

WEBSITE WITH UNSECURE FILE UPLOAD



OPSWAT File Upload Security

Unsecured File Uploads in Web Applications

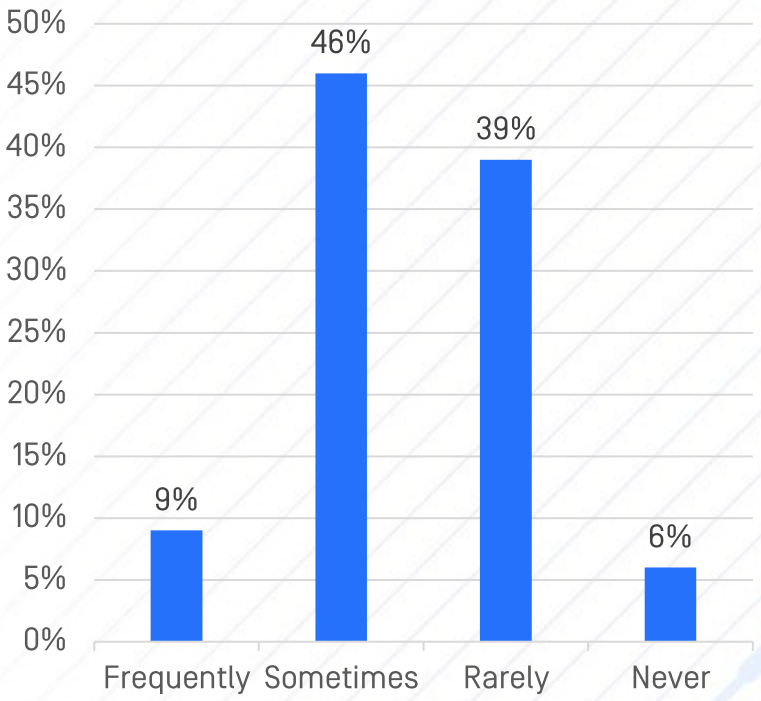
43% of breaches were attacks on web applications

- 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

Source: Statista

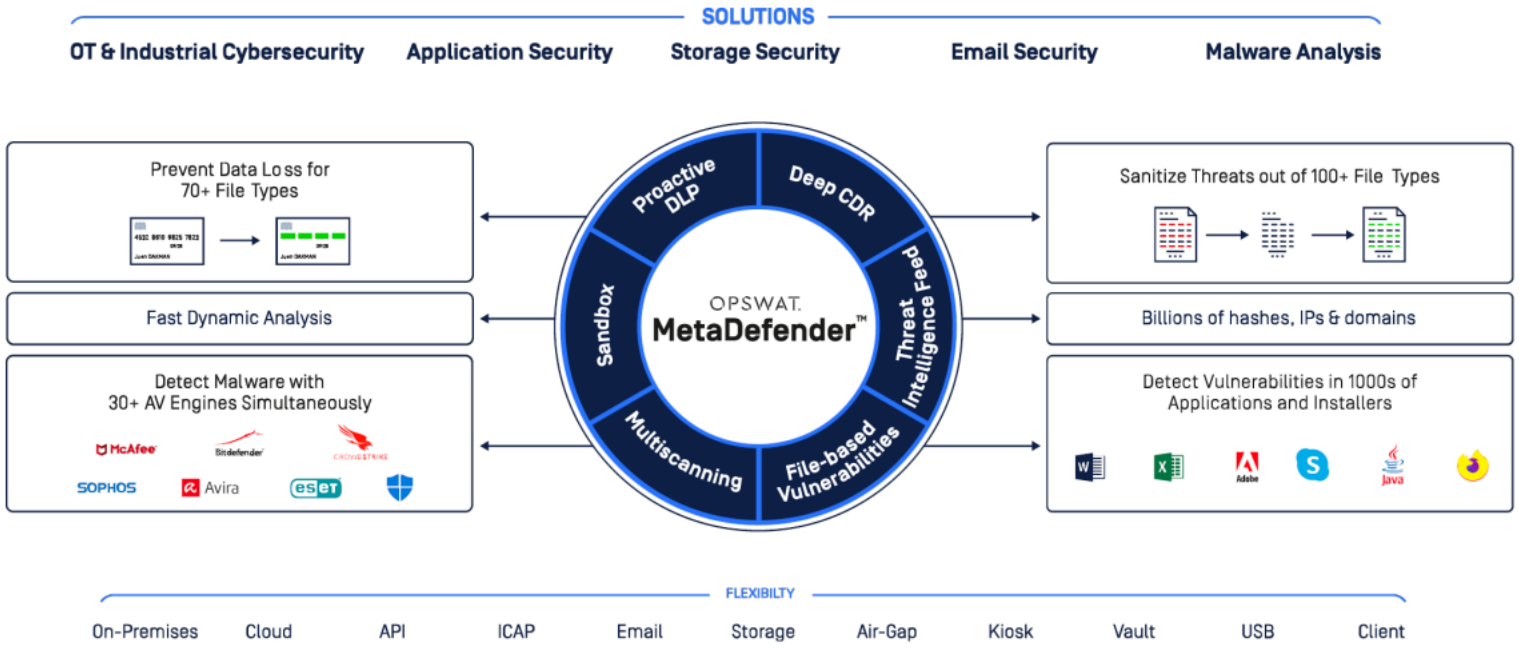
Best Practices for File Uploads in Web Application Security

- 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

Source: OPSWAT Web Application Security Report 2021

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 prevents 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

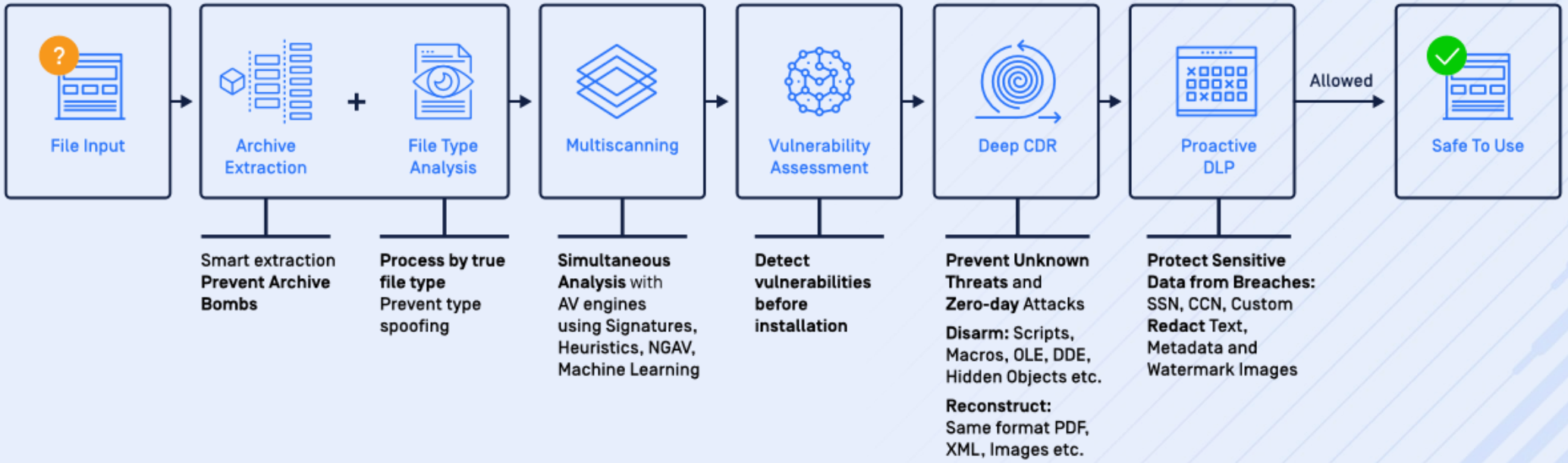
Sandbox (cloud) – Analyze malware with fast dynamic analysis

Threat Intelligence (cloud) – Provide enriched intelligence on threats on billions of hashes, IPs and domains

OPSWAT Solution

File Processing Workflow

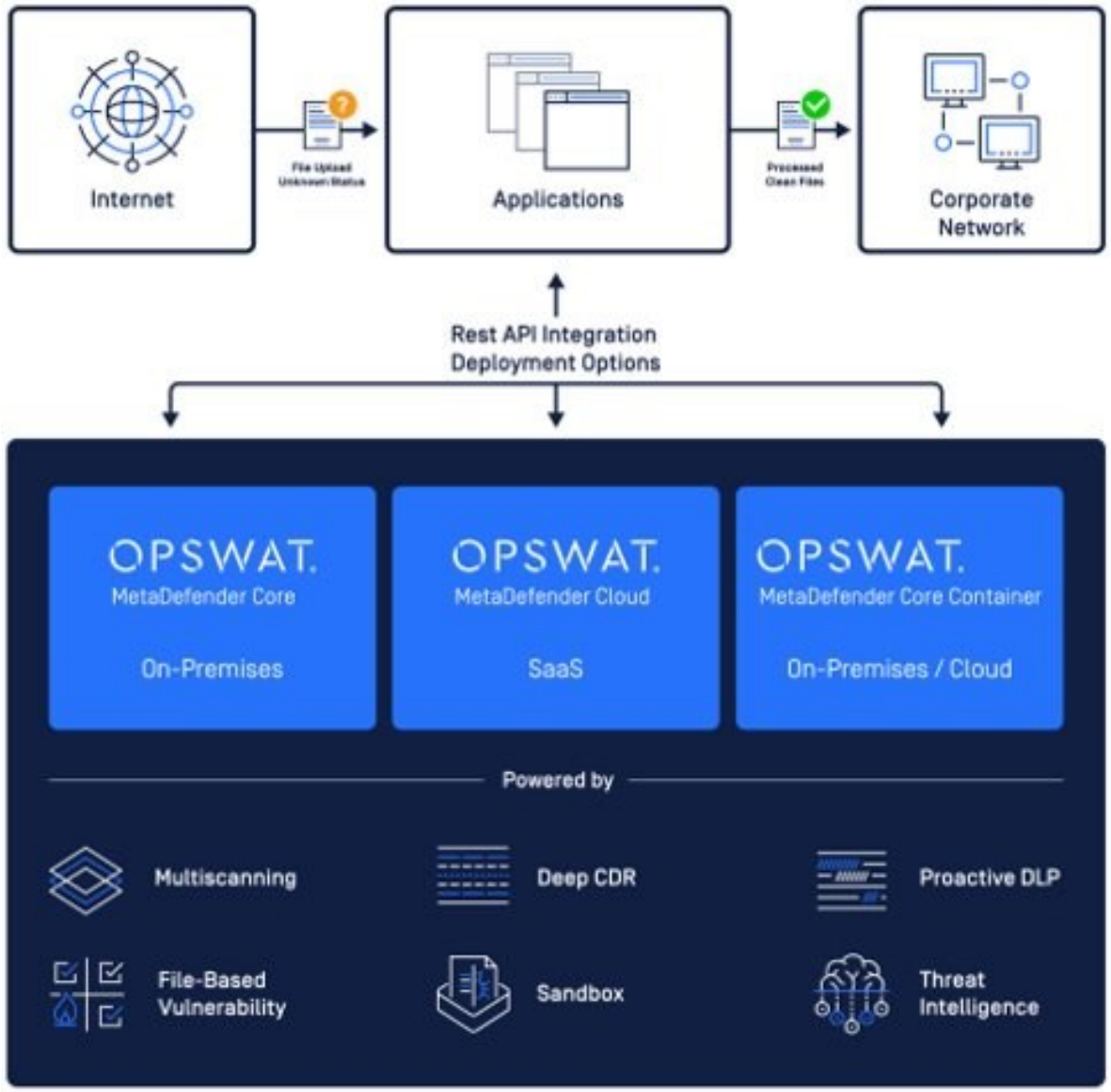
Enterprise performance with ability to analyze 10 files per second, per deployment



MetaDefender Core

Features and Benefits

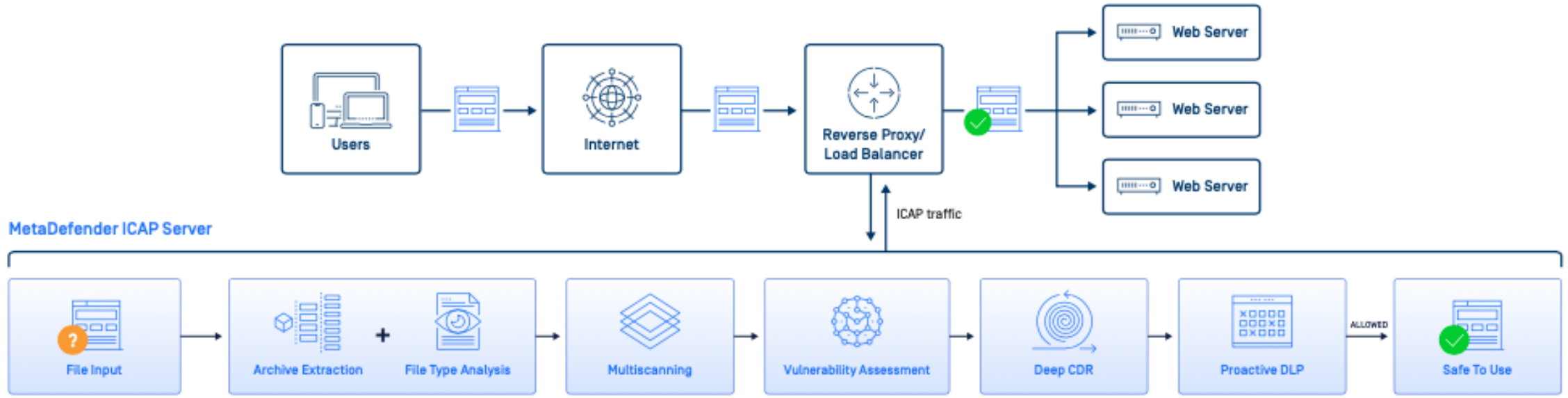
- Comprehensive protection with proprietary advanced technologies
  - Detection rates greater than 99%
  - Zero-day attack prevention
  - Sensitive data protection
- Meet regulatory compliance requirements
  - Prevent sensitive data entering or leaving your organization
  - Cloud Storage vulnerability 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

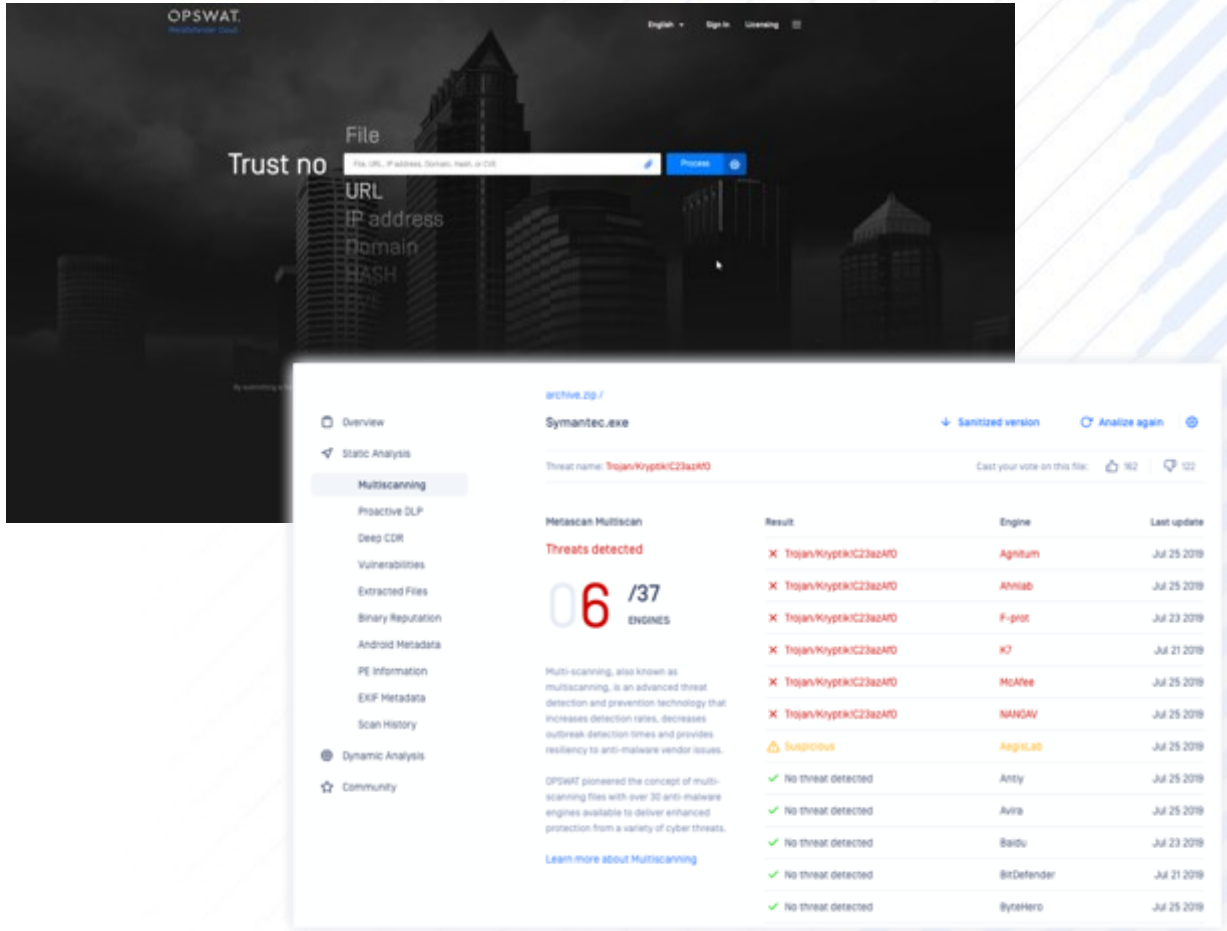


MetaDefender Cloud

Cloud-based threat prevention and malware analysis

- 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

Consume MetaDefender Cloud through our UI or REST APIs



Primary use cases

Prevent malicious file uploads

Perform malware analysis

Prevent unknown threats

Technologies

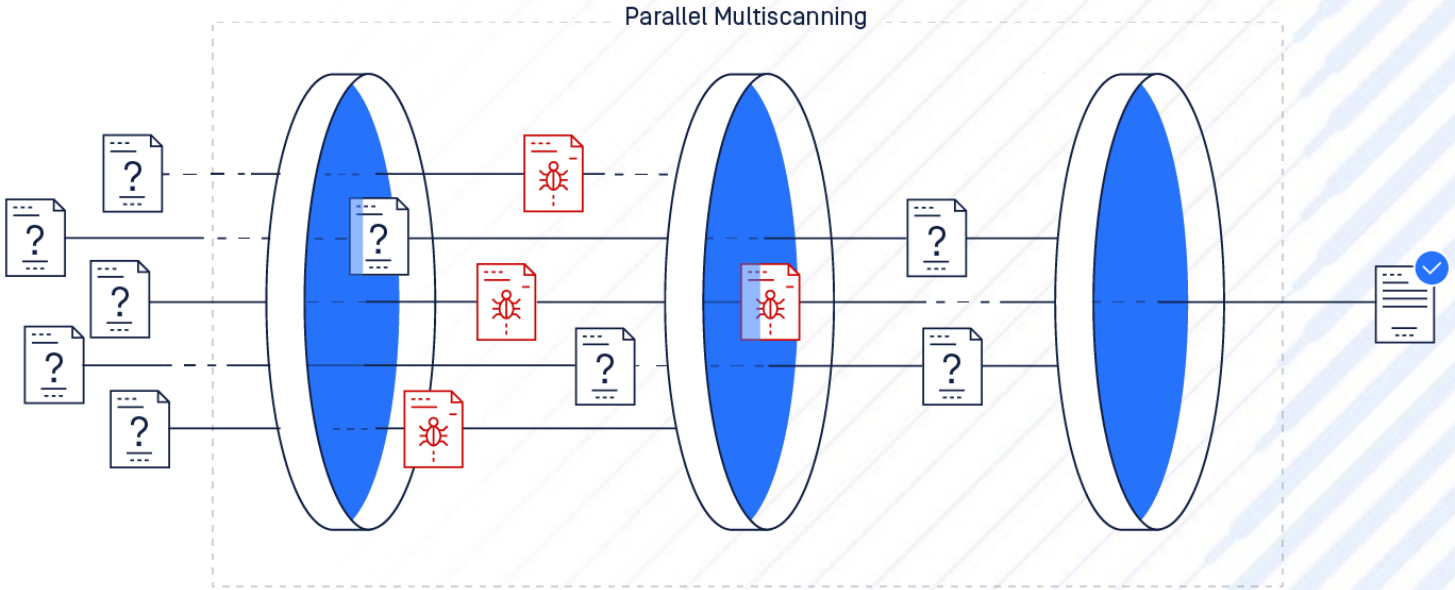
Multiscanning

OPSWAT.

OPSWAT Metascan

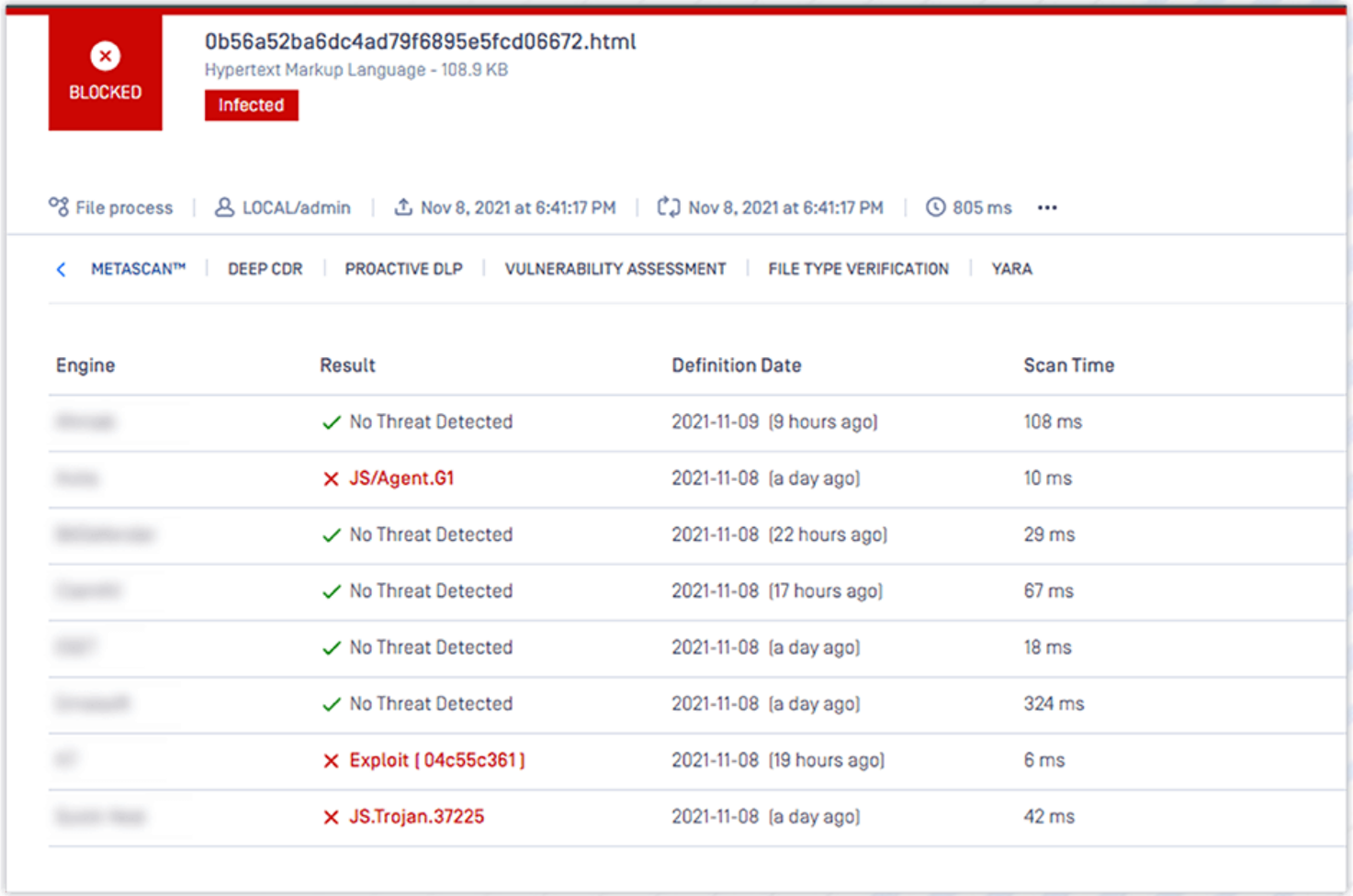
Multiple layers of defense

- 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



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

Metascan

Improved Malware Detection

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

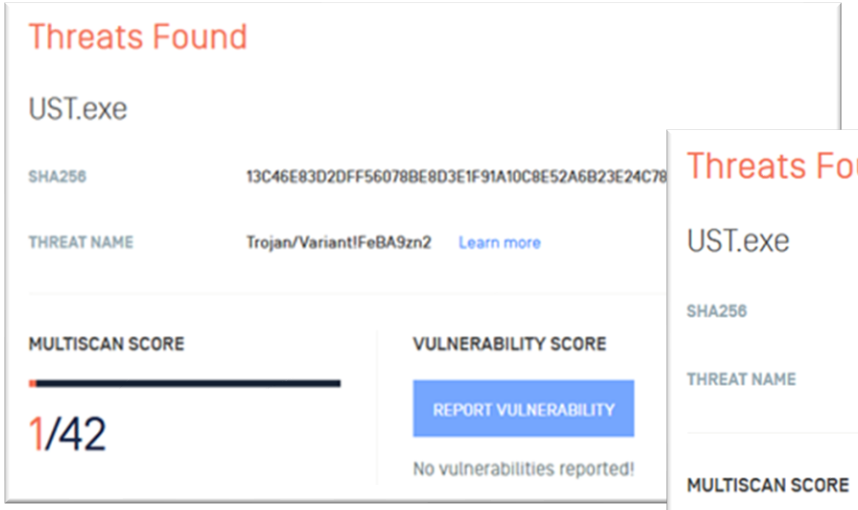
MetaDefender Core Package	4 Engines	8 Engines	10 Engines	12 Engines	15 Engines	16 Engines	20 Engines	Max Engines	Cloud *
Detection of top 10000 threats	86.20%	88.80%	90.00%	91.00%	94.60%	93.80%	95.20%	98.50%	97.80%

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

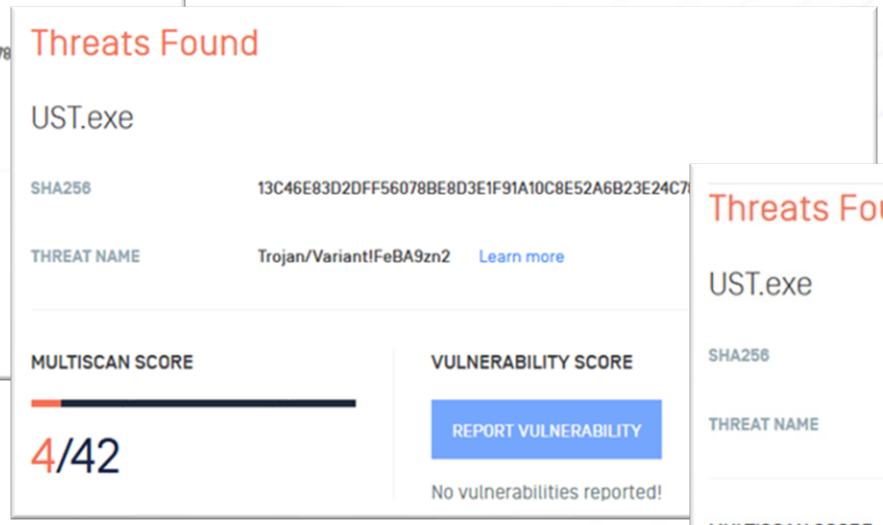
* Commercial Cloud with 20+ engines. For a complete list see our licensing page

Source: https://metadefender.opswat.com, March 2023

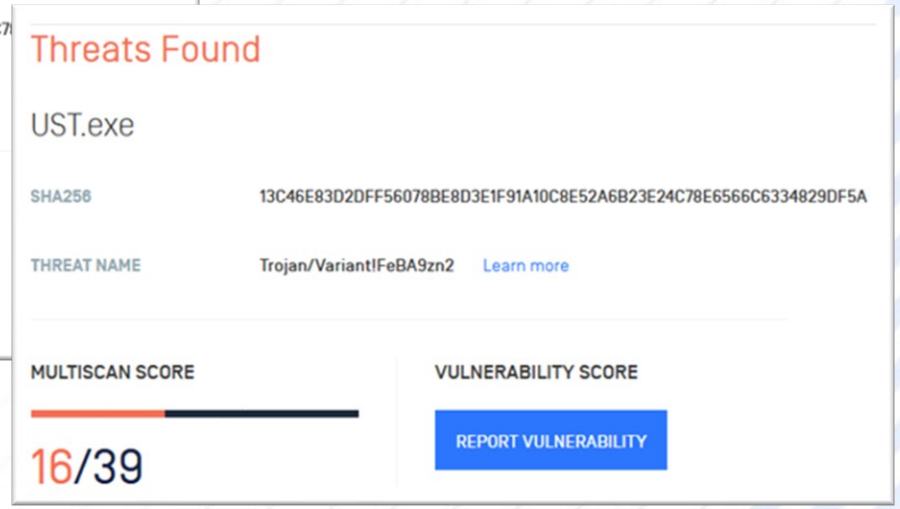
Example



November 2015
Only 1 AV scanner found the threat
(Filseclab)



February 2016
Only 4 AV scanners found the threat
(Antiy, AegisLab, Filseclab, and Zillya)



Until May 2020
Only 16 scanners found the threat,
many of the best-known AV still do not detect this malware

How It Works

Faster Outbreak Detection

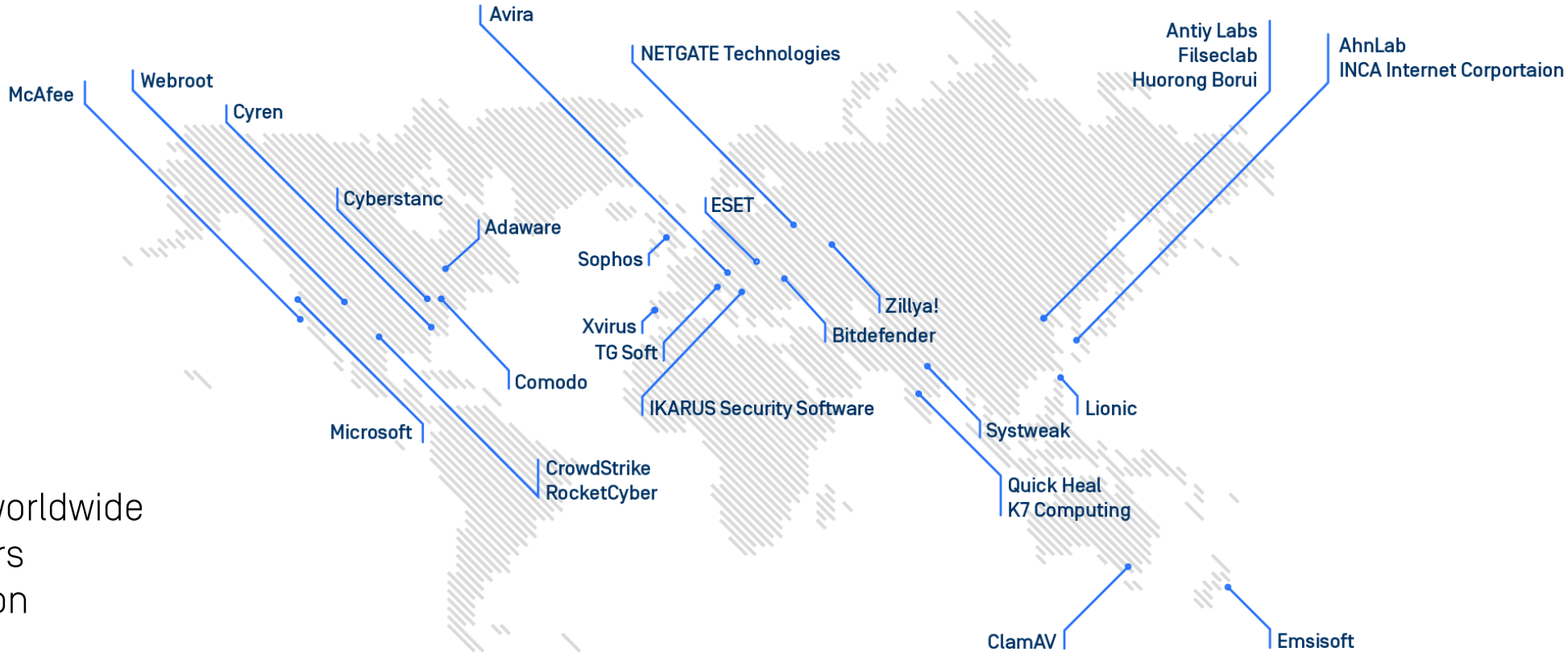
More anti-malware engines are added, malware detection rates improves

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

Source: Executable Outbreak Report, OPSWAT. March 2023

Wide Malware Detection Coverage

Quickly respond to regional malware outbreaks



OPSWAT worldwide
AV vendors
distribution

Metascan

Machine Learning Engines

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

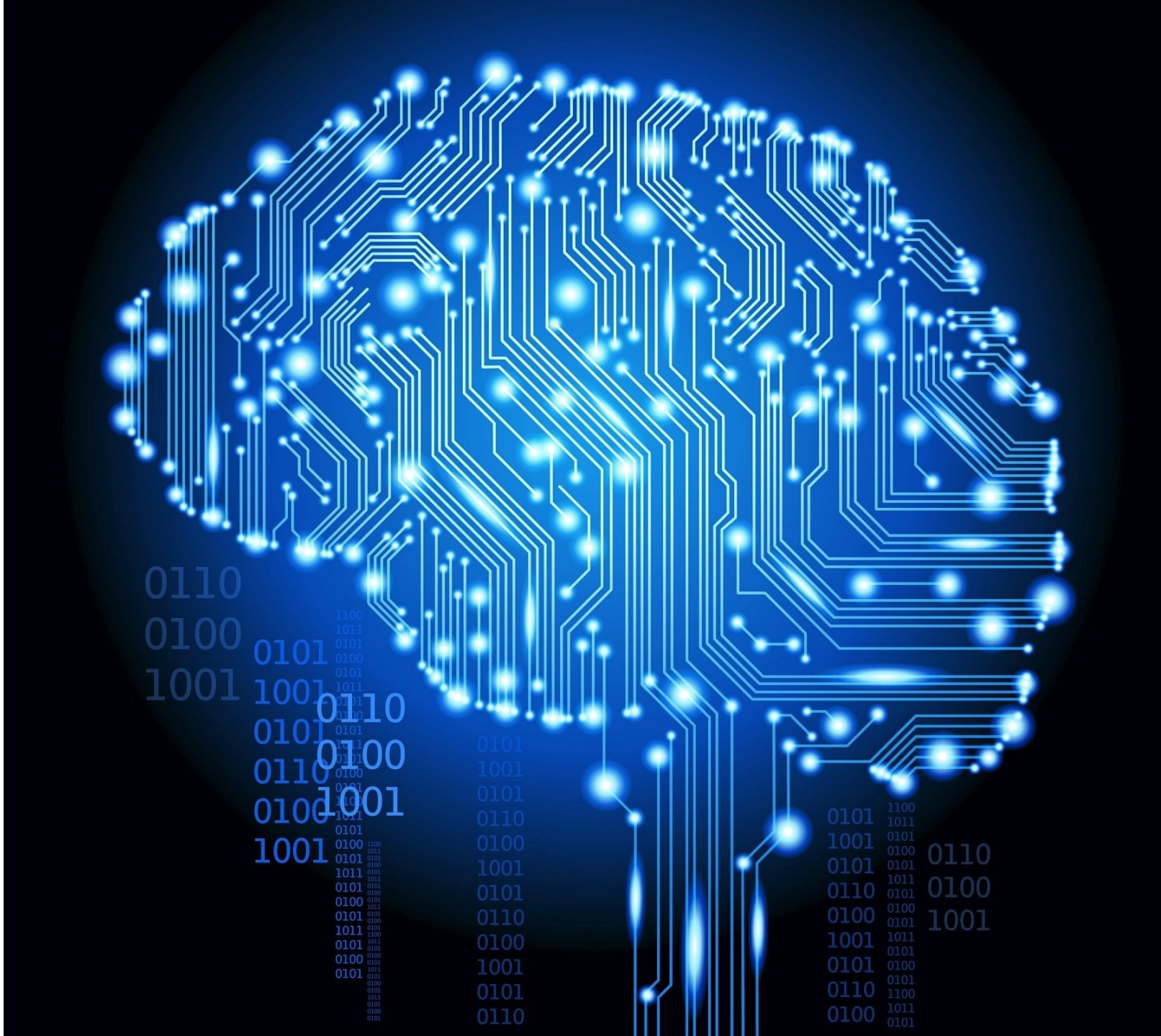
OPSWAT's AV vendors:

Avira

CROWDSTRIKE

WEBROOT
an opentext company

RocketCyber



Proactive DLP

OPSWAT.

Proactive Data Loss Prevention

Detect and Block Sensitive Data in Files and Emails

Proactive DLP

Features

Prevent Potential Data Breaches and Regulatory Compliance Violations

Detect and Redact

Watermark

Remove Metadata

Proactive DLP

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

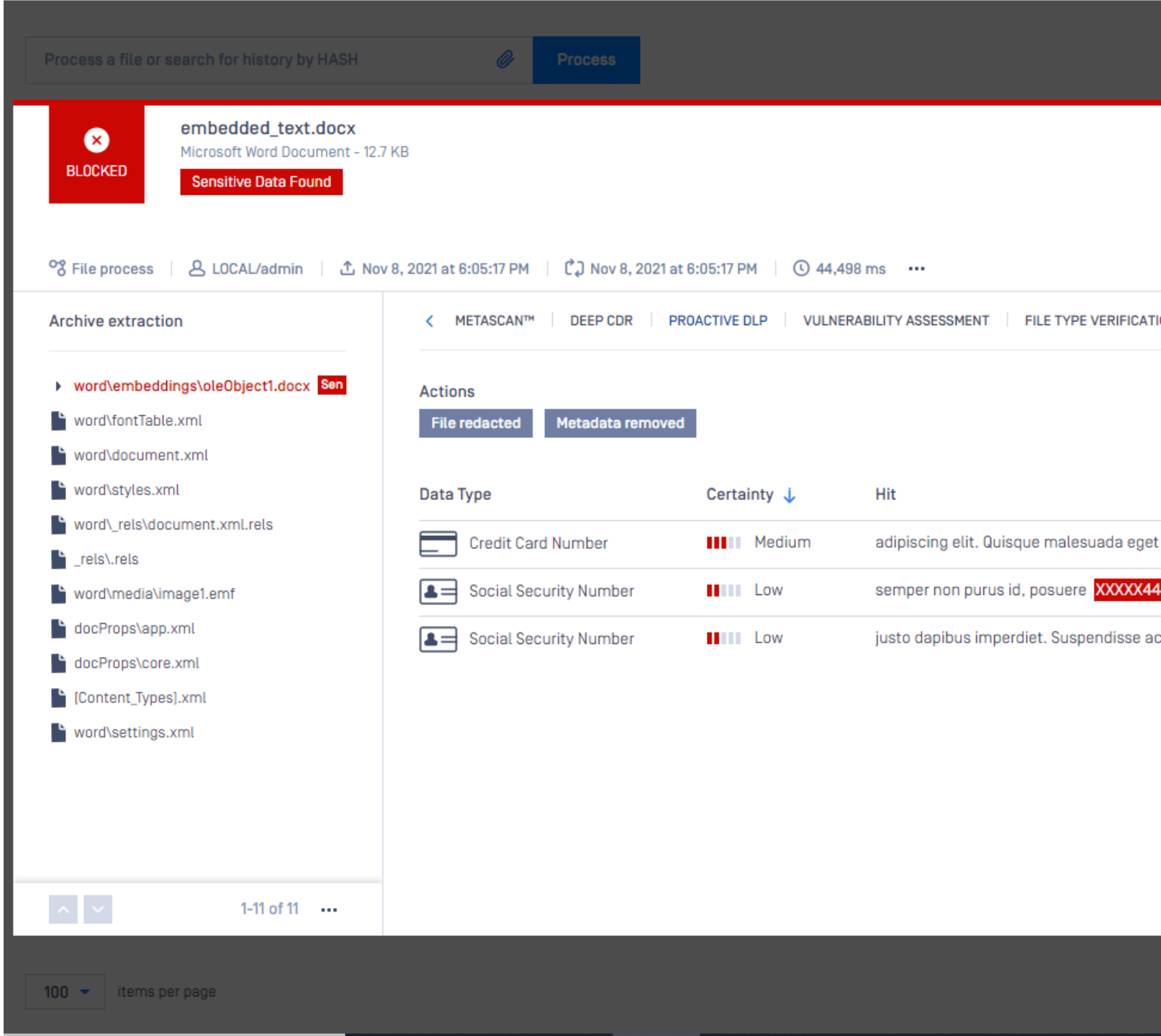
- Challenge: Possible False Positive
- Solution: Context checking

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



Redaction

✓Separated certainty level for each sensitive info type.

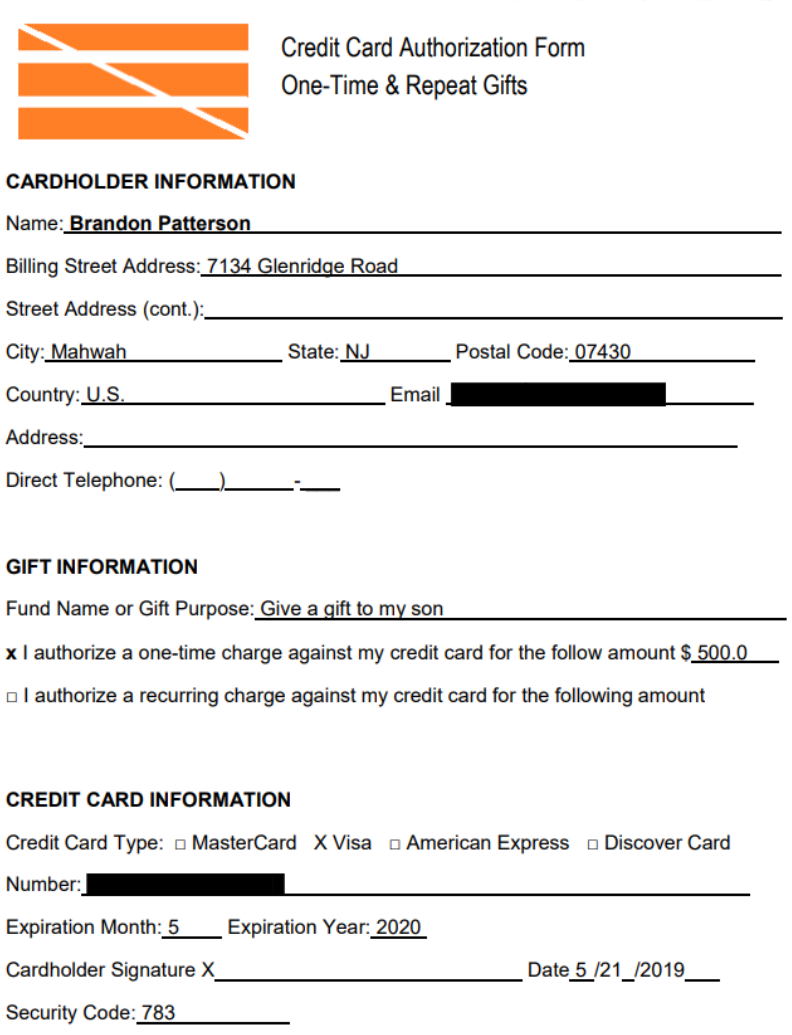
E.g.: Only redact high certainty SSN but all detected Credit Card info

✓ 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

x 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 X Visa □ American Express □ Discover Card

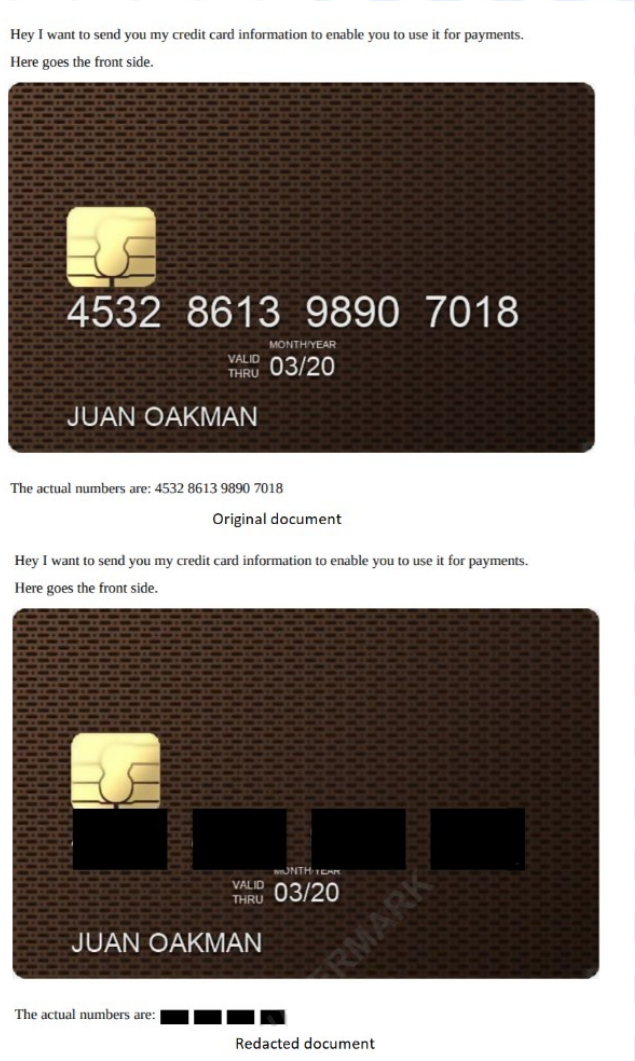
Number: [redacted]

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.

4532 8613 9890 7018
VALID THRU 03/20
JUAN OAKMAN

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.

[redacted]
VALID THRU 03/20
JUAN OAKMAN

The actual numbers are: [redacted]

Redacted document

Non-text-searchable

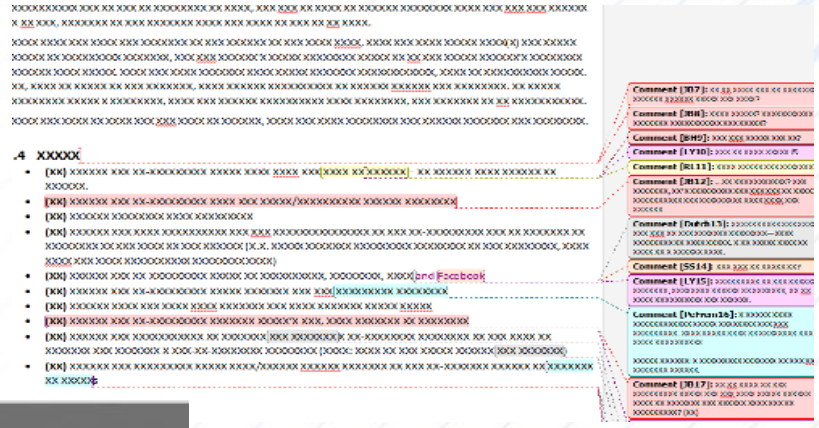
Remove Metadata

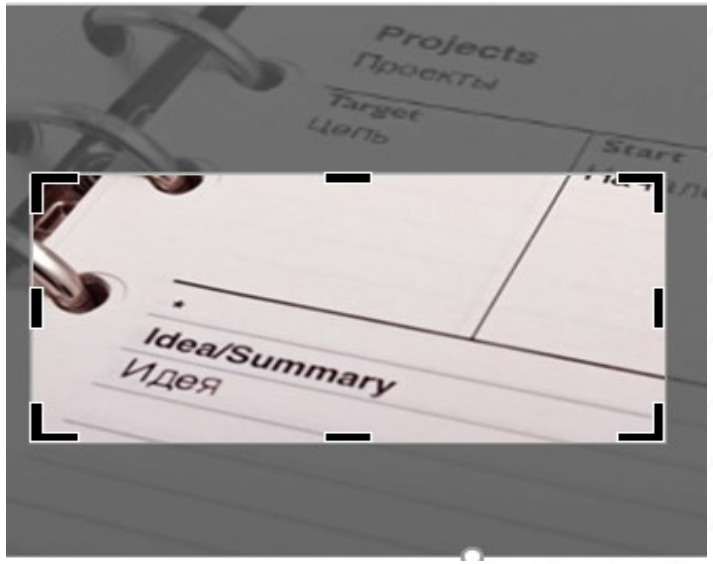
✓Supported image file types:

- JPEG
- TIFF
- PNG
- GIF

✓Sensitive info: name, company, subject, GPS locations, authors, etc.

Comment, revision





Cropped image

GPS Location

Proactive DLP

Watermark

✓Supported file types:

- JPEG
- TIFF
- PNG
- GIF
- PDF

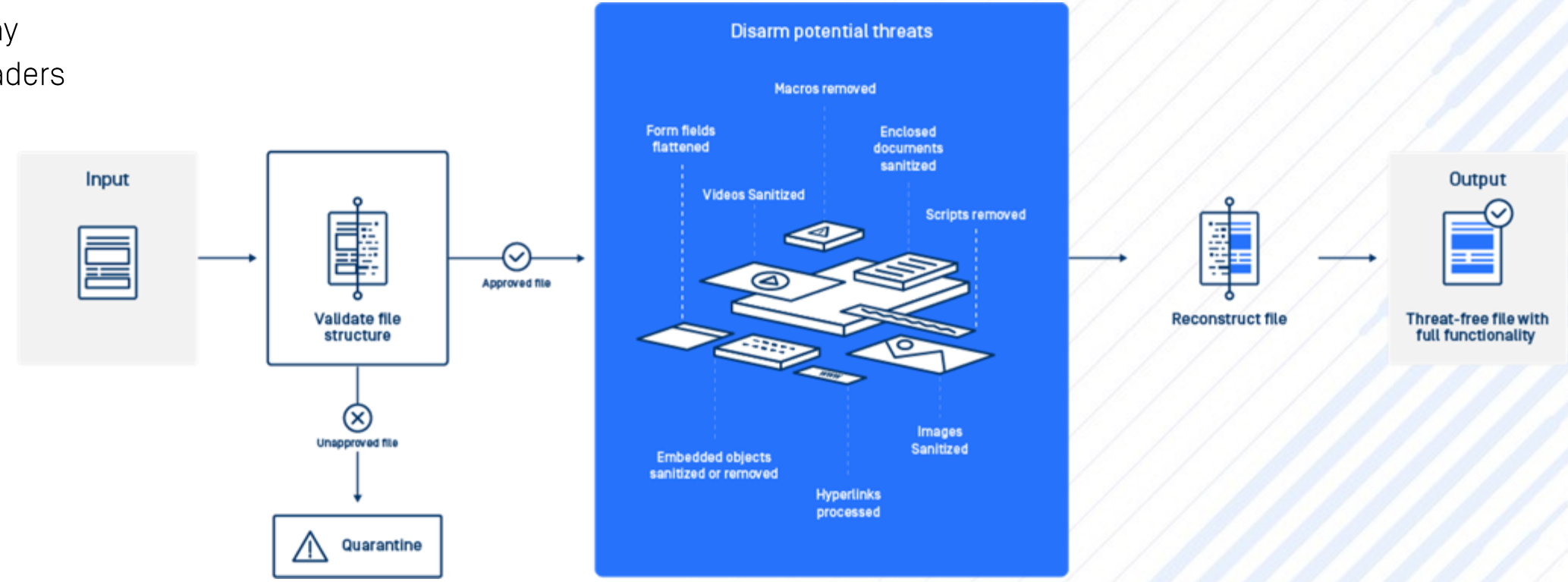
✓Flexible input string from client

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

Input file → Deep CDR engine → Sanitized file

- Clean files
- Infected files
- Invalid files

- Clean and usable files
- Clean and usable files
- Ignore and report

Deep CDR workflow

Challenge: security vs. usability

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

Deep CDR workflow

- image
- script
- embedded file
- hyperlink
- form field

➞ Sanitize images
➞ Remove scripts
➞ Remove embedded files
➞ Remove hyperlinks
➞ Sanitize form fields

Deep CDR workflow

File parser: key and challenging parts

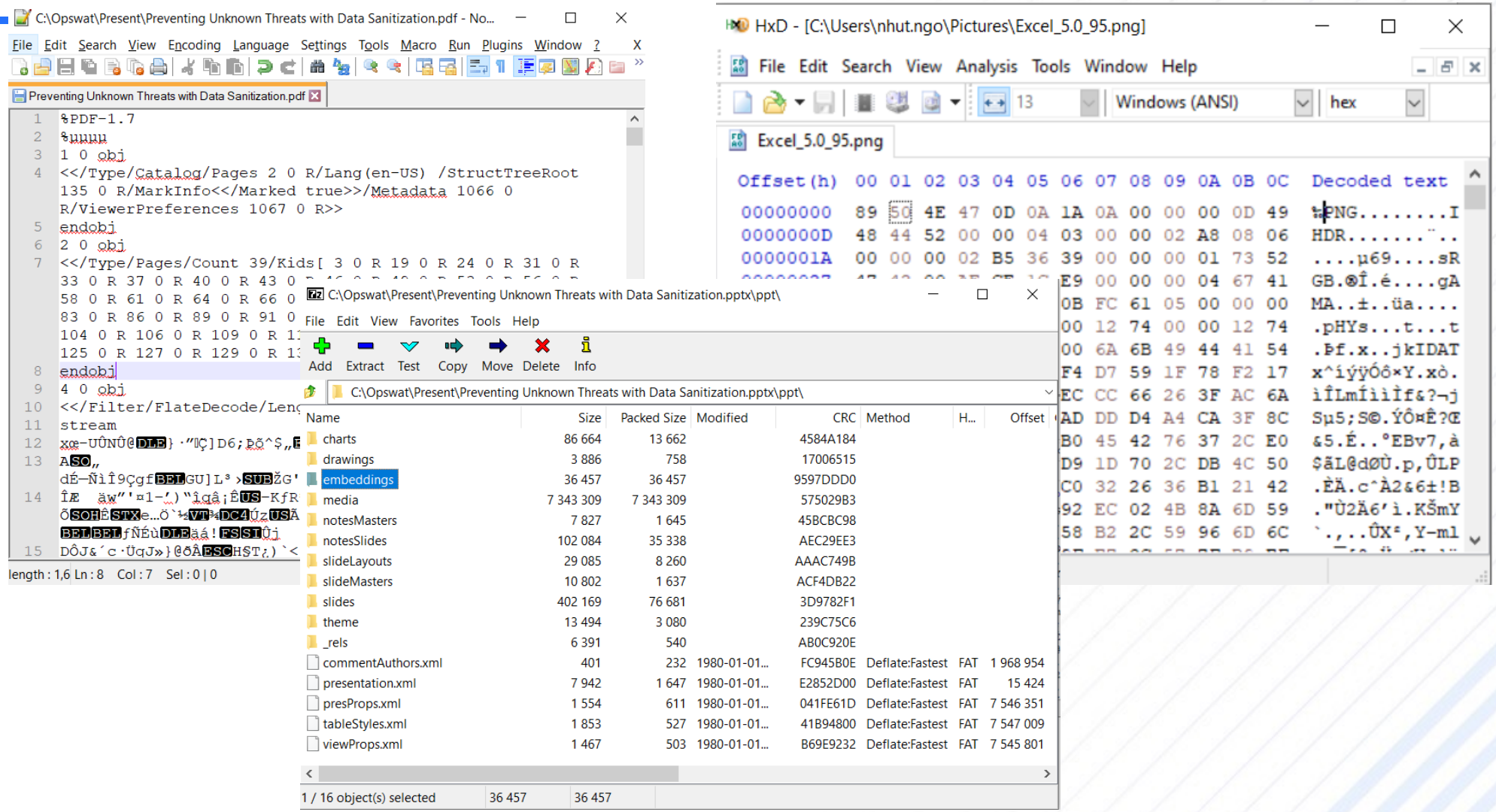
- Help sanitize every object and detail in the file
- Ensure integrity of file content after reconstruction
- Comprehensive understanding of file structures
- Strong skills on designing and creating architecture
- Cover all possible cases: wide variant, special, exceptional, invalid

Our own parsers

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

Deep CDR

Our work

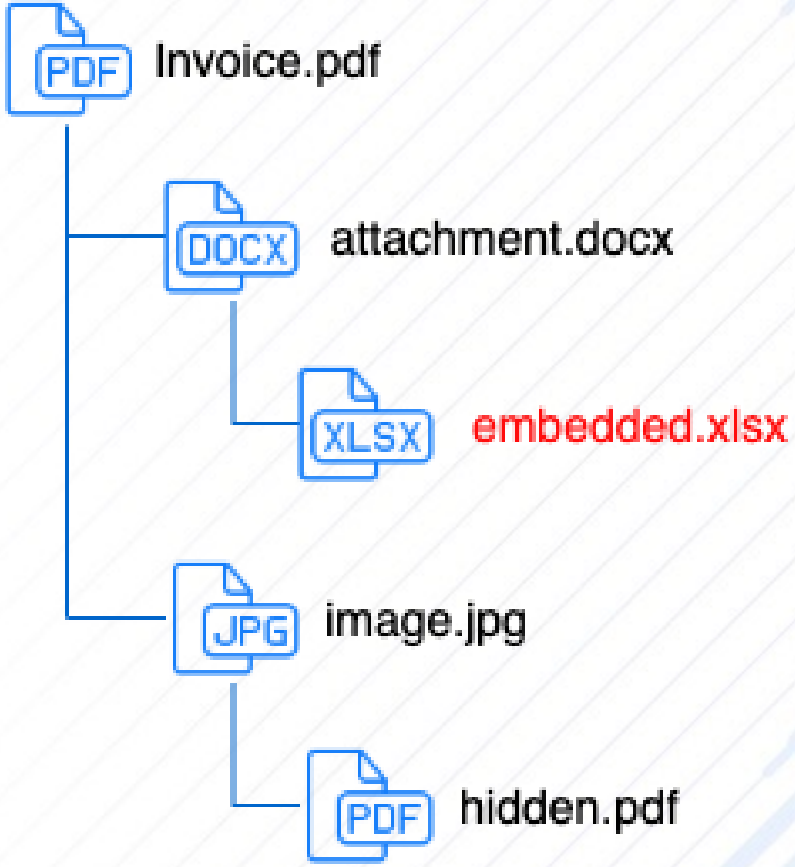


Deep CDR

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.)



Deep CDR

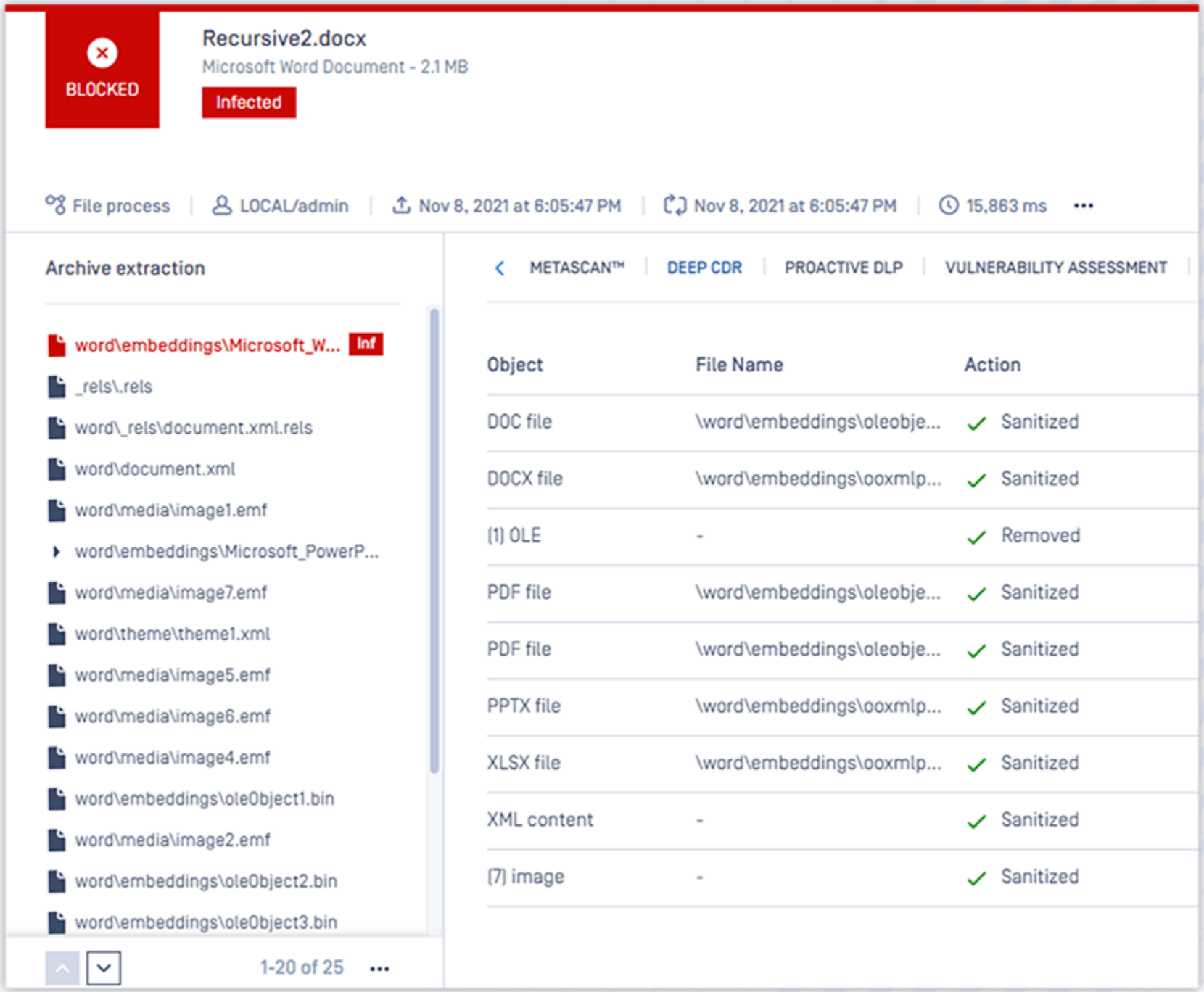
How Can You Know If The File Is Fully Sanitized?

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

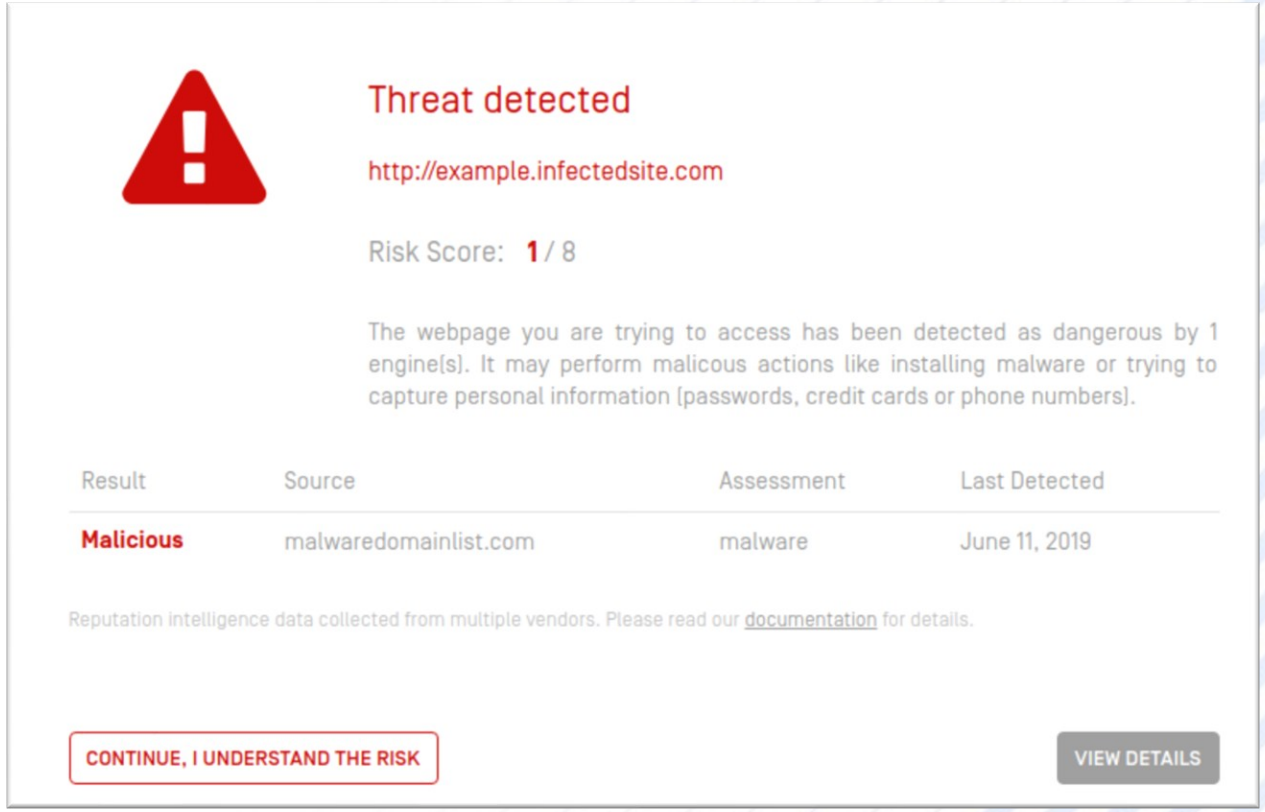


Deep CDR

Hyperlink Processing

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

An example with MetaDefender Cloud redirect



Deep image sanitization

Effectively defend against Stegosploit

Thoroughly eliminate malware in Metadata/Header

Verified by many steganography tools

http://stegosploit.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://github.com/peewpw/Invoke-PSImage
https://github.com/DimitarPetrov/stegify
...more

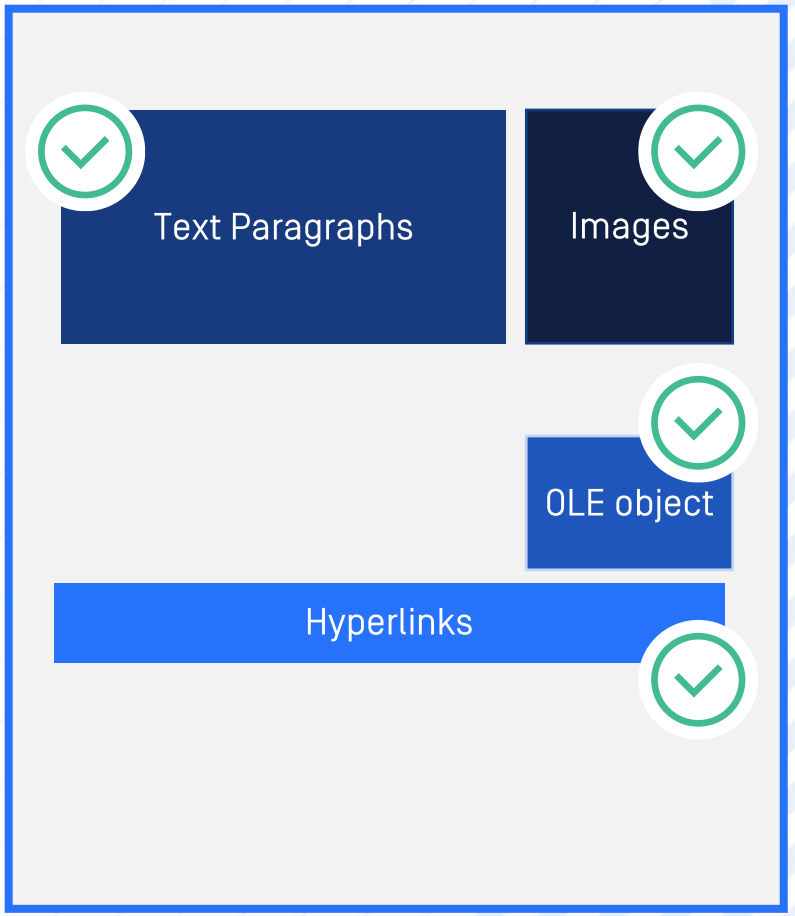
Original image

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
BLINDINGCAN North Korea	• Reported by FBI/CISA in Aug 2020, • use Attached Template to link to a malicious file	Deep CDR removes all linked files	No malware downloaded
Locky ransomware attack	• Delivered by email with an attached MS Word file containing malicious macro • Enabled macro drops the malware • The malware detects whether it is running within a virtual machine or a physical machine and relocate of instruction code.	Deep CDR removes Macros	No malware downloaded
Cobalt Strike Backdoor	• Exploited MS vulnerabilities CVE-2021-40444 • Docx file contains an ActiveX object to download an HTML file • HTML file downloads several files and Cobalt Strike malware payload	Deep CDR removes OLE objects	No shellcode dropped

OPSWAT®

Thank you

OPSWAT®

Q&A