OPSWAT®

Trust no file. Trust no device.

Protecting Critical Networks: Design Considerations for Secure Data Workflows

Benny Czarny, Founder and CEO, OPSWAT
ITHome CYBERSEC Conference 2019

OPSWAT.

About Me

OPSWAT

OPSWAT

OPSWAT.
398 kansas

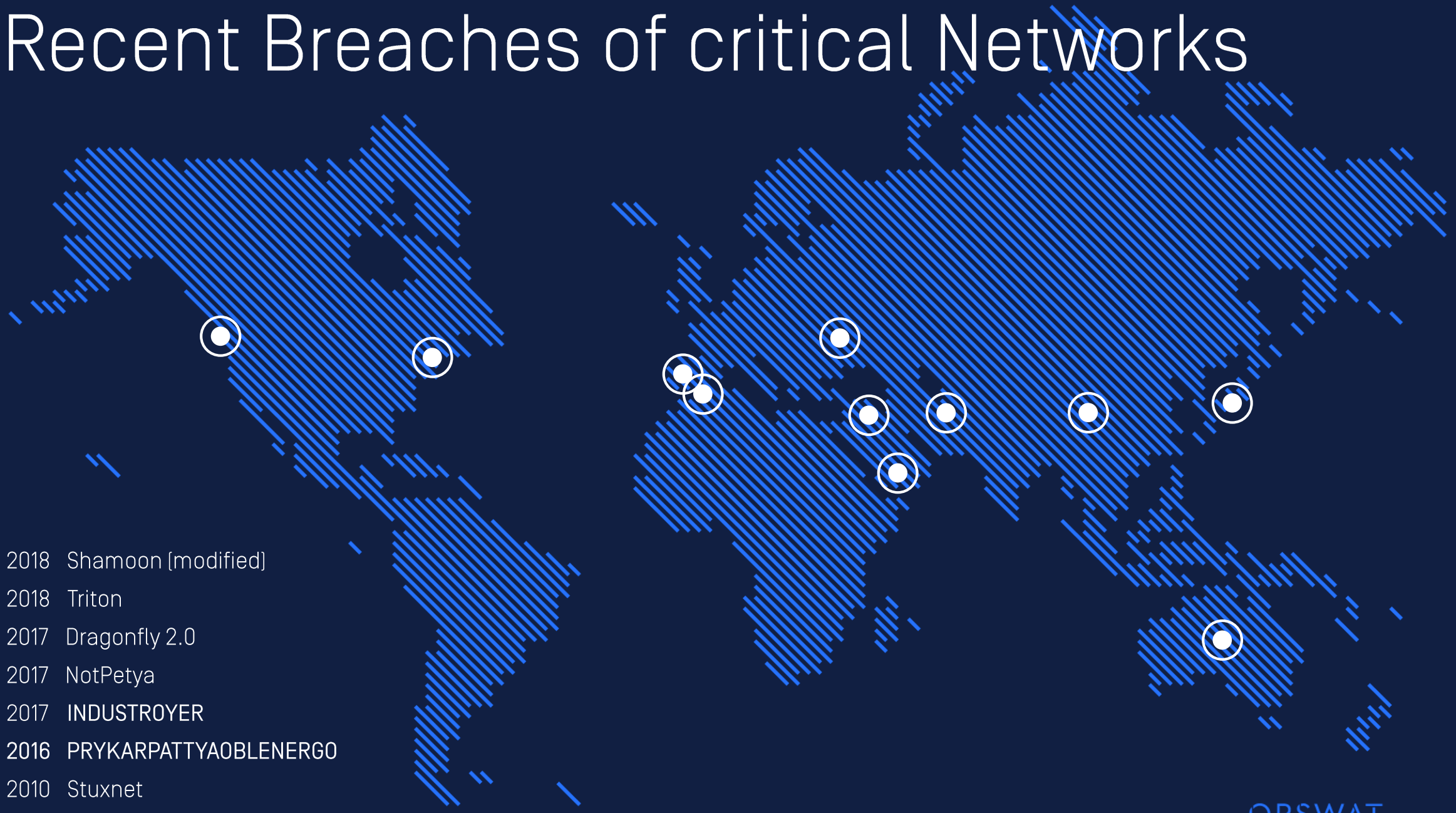
About Me

Isolated network protection

Email
Web and Email security

Secure Device Access

Recent Breaches of critical Networks



2018 Shamoon (modified)

2018 Triton

2017 Dragonfly 2.0

2017 NotPetya

2017 INDUSTROYER

2016 PRYKARPATTYAOBLENERGO

2010 Stuxnet

OPSWAT.

Protecting critical networks

Protecting critical networks

Existing IT security tools

How prevention works

prevention is based on detection

Machine learning

Heuristics and signatures

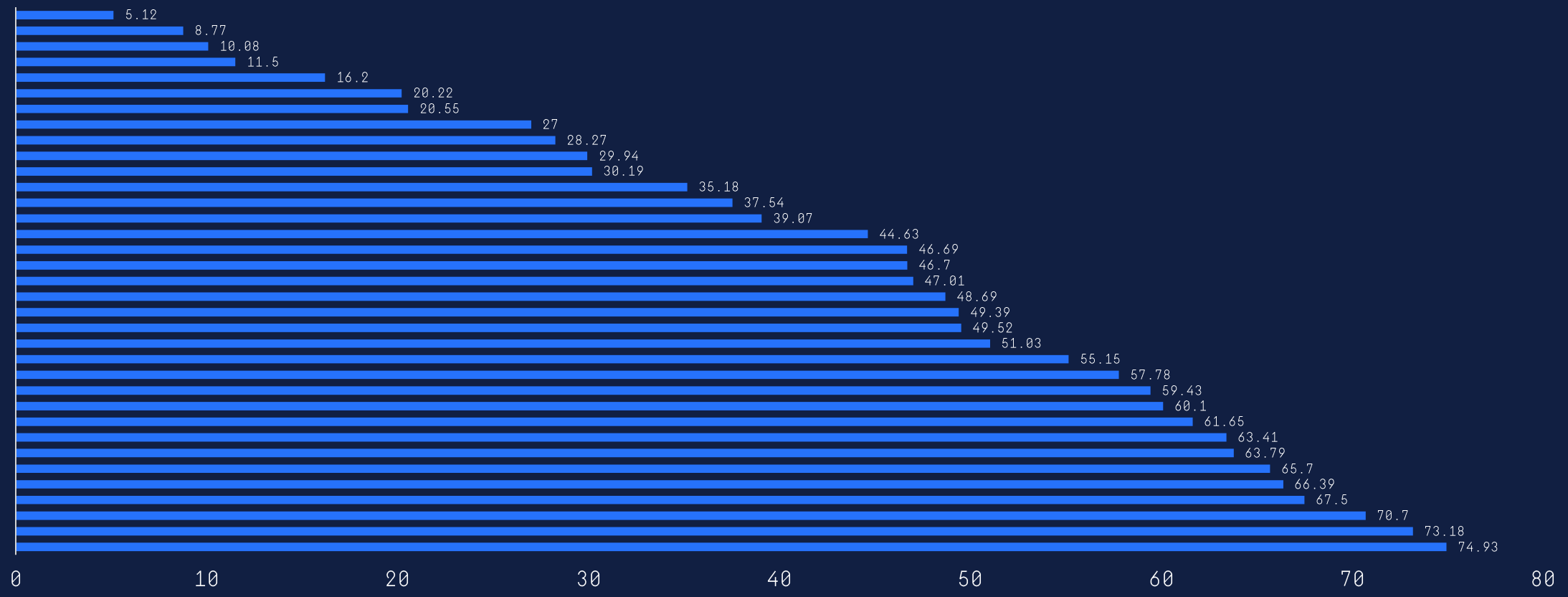
Sandbox

WHY BREACHES HAPPEN

Detection is not perfect

Single anti-malware detection rate percentage

Source: MetaDefender Cloud top 10,000 threats

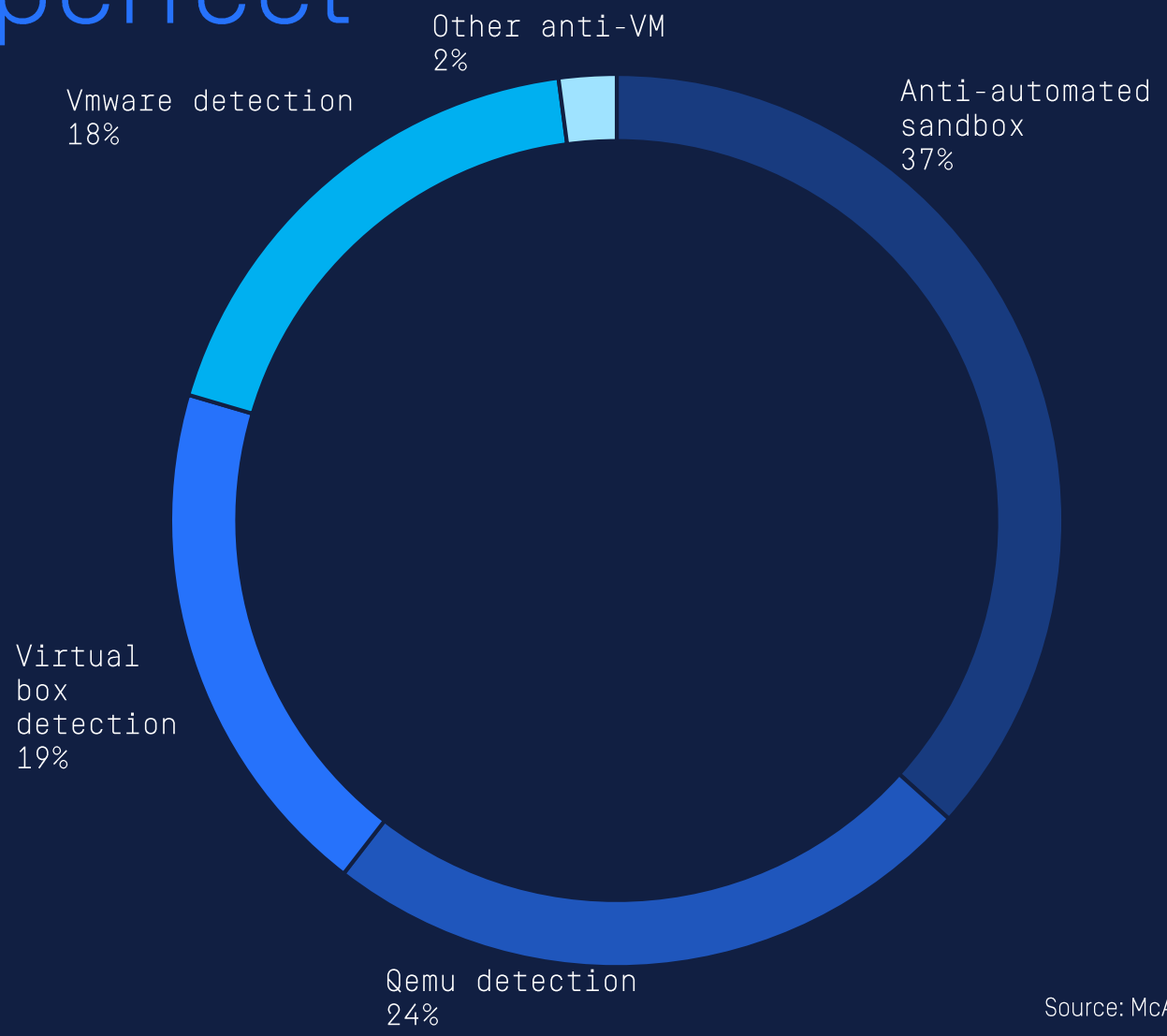


OPSWAT.

WHY BREACHES HAPPEN

Detection is not perfect

Malware evade sandbox



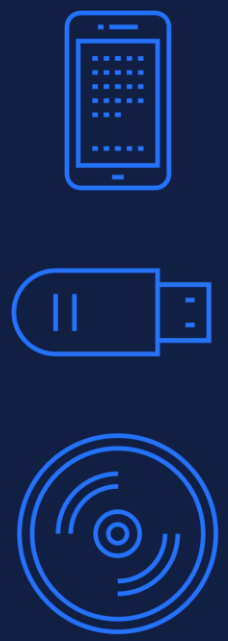
Source: McAfee

OPSWAT.

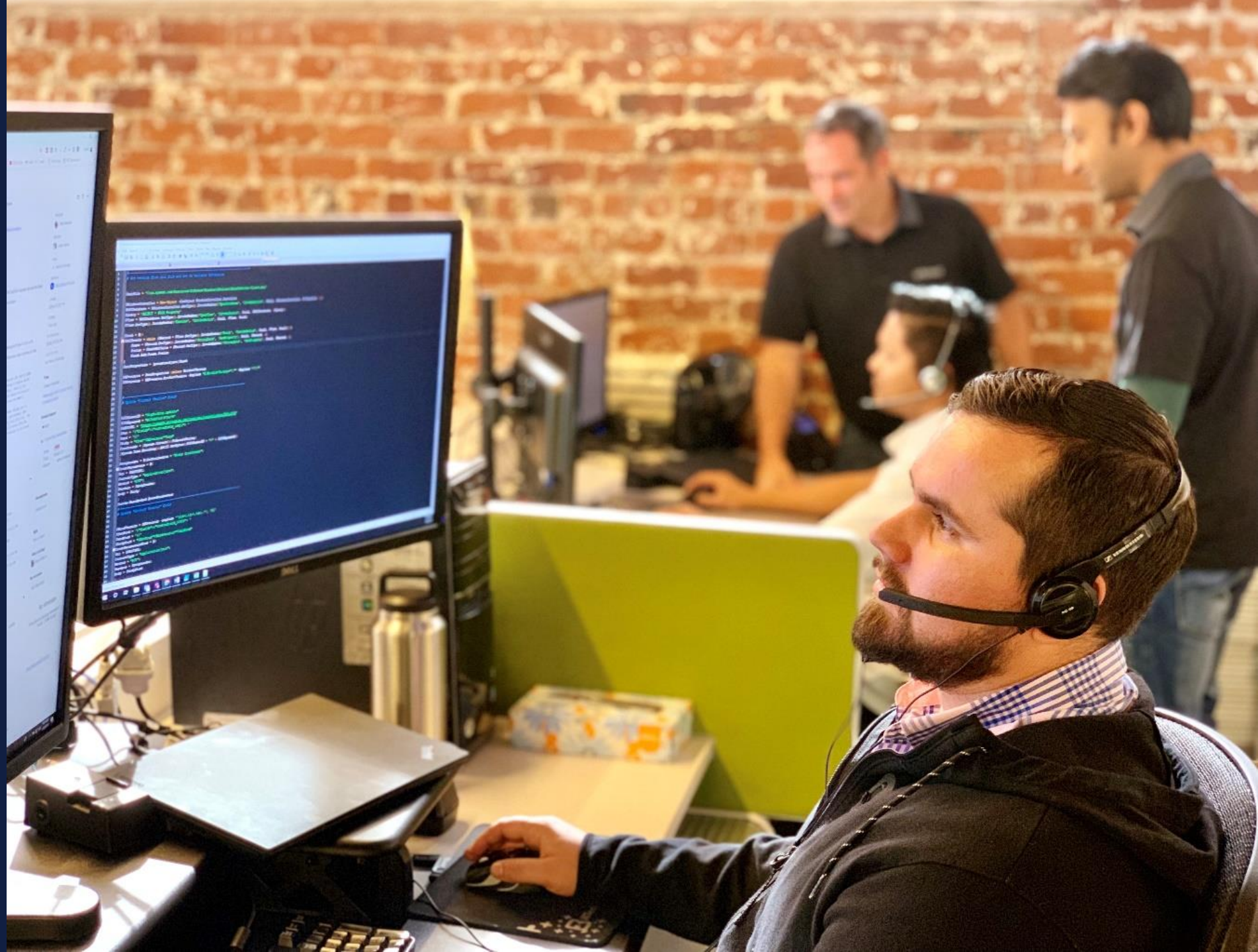
WHY BREACHES HAPPEN

Lack of process

Security transfer files to and from critical networks



Critical Network

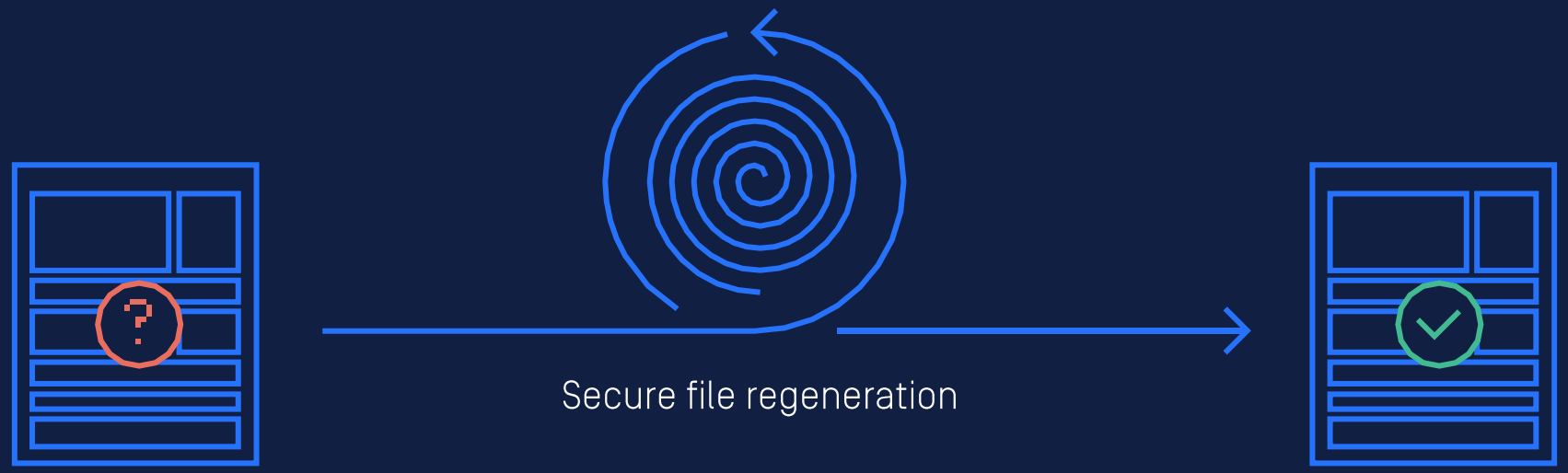


Design Considerations for Secure Data Workflows

OPSWAT.

Prevention not based on detection

Data sanitization (CDR)



Assume All files are malicious
Trust No File™

Use regenerated file

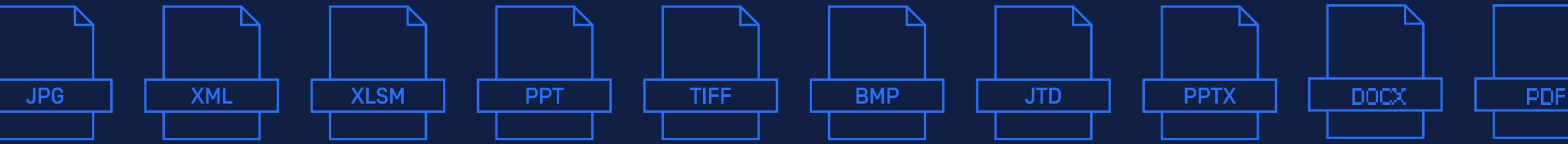
An Analogy to Boiling Water

01

02

03

Apply this to any filetype



Secure the Data

Additional conisderaion securing data flow to and from critical networks

- Scan data for recent vulnerabilities
- Search the data for sensitive information (DLP)
- Scan Data with Many Antimalware engines
- Integrate threat intelligence
- Keep rescanning your data

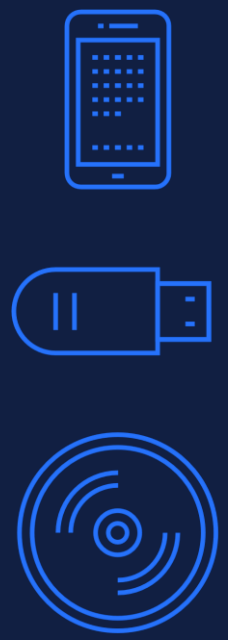
Secure the Data

Quantity Of Antimalware Engines [AI and Next Gen]	Malware Detection Rate
4	76
8	87.5
12	96.2
16	97.92
20	99.04

Source : https://metadefender.opswat.com/reports/statistics#!/

Isolate your network

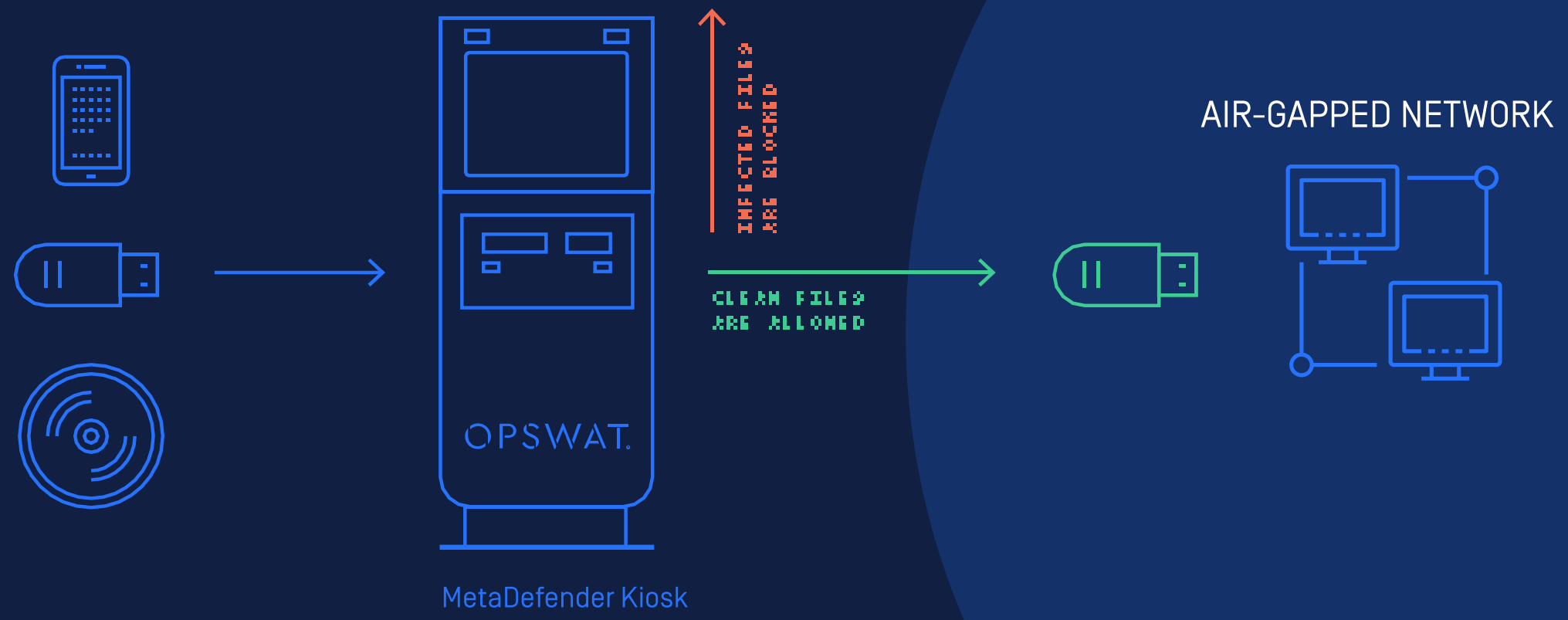
Create a secure process to transfer files tom and from your critical networks



Isolate your Critical Network

Create A Secure Data Transfer Process

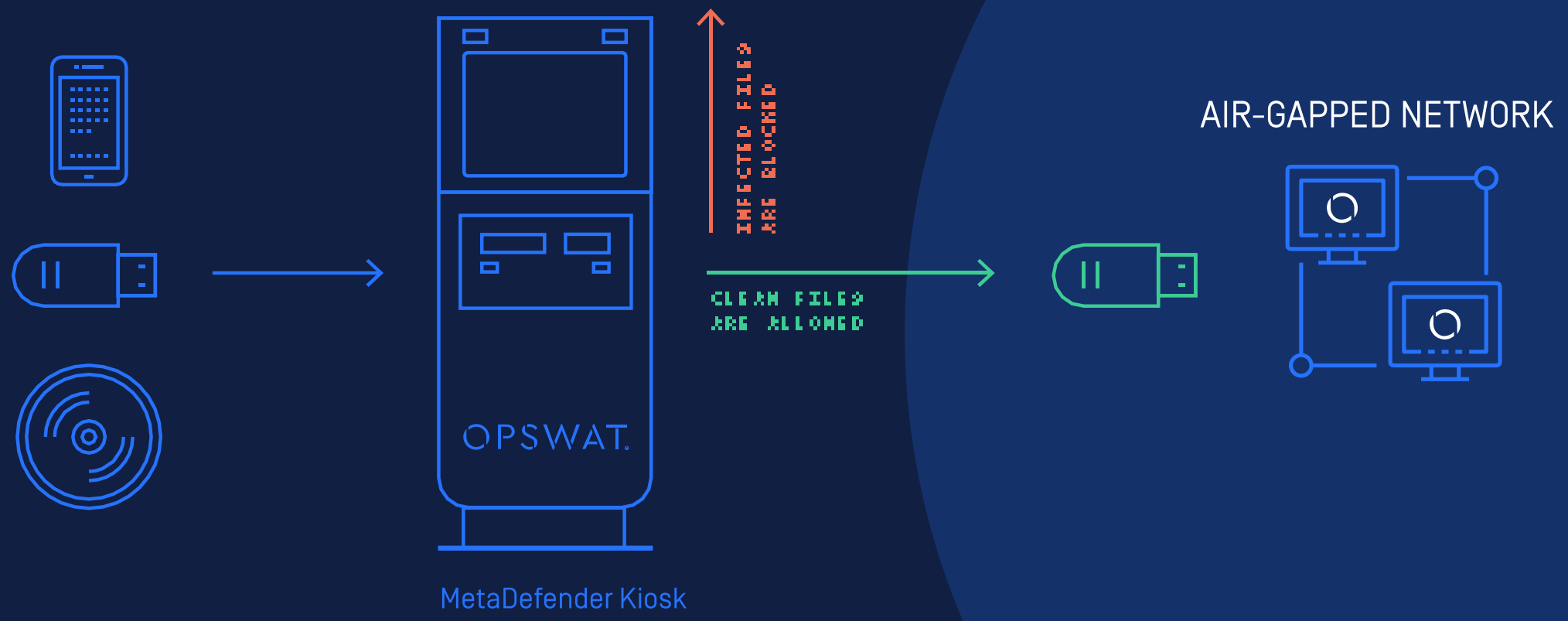
Safely moving data into secure networks



MetaDefender Kiosk

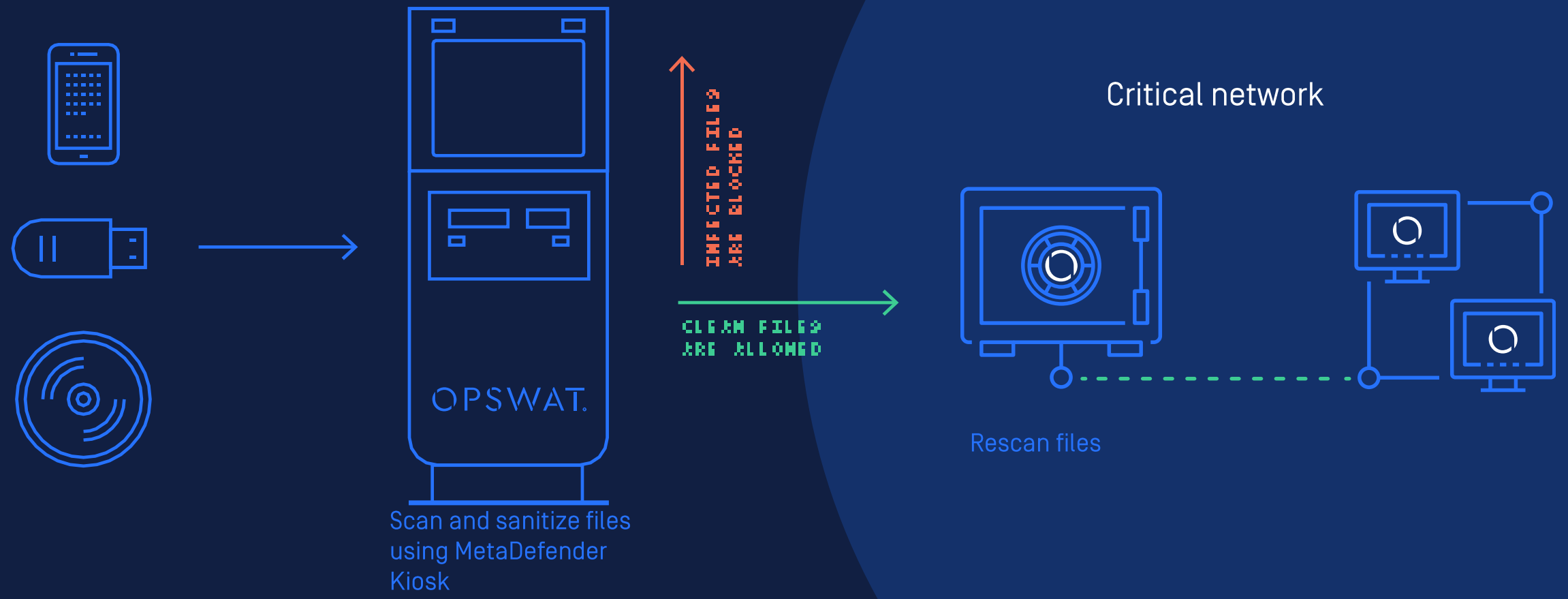
Create A Secure Data Transfer Process

Bring In the Verified Media Using endpoint Validation



Create A Secure Data Transfer Process

Create local secure storage



Thank You

OPSWAT.