VIRGINIA
IT AGENCY

Welcome to the Feb. 7, 2024 ISOAG Meeting

Information Security Officer's Advisory Group

February 7, 2024

VIRGINIA
IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Erica Bland/ VITA
Protect Critical Infrastructure	Dylan Higgs, Rusty Byers /OPSWAT
Virginian Identity Program (VIP) Update	Ron Sticinski/ VITA
Splunk add on	Richard White/ VITA
New OKR Introduction	Matthew Umphlet/VITA
Upcoming Events	Erica Bland/ VITA
Adjourn	

OPSWAT.

INTRODUCTIONS

Corporate Overview

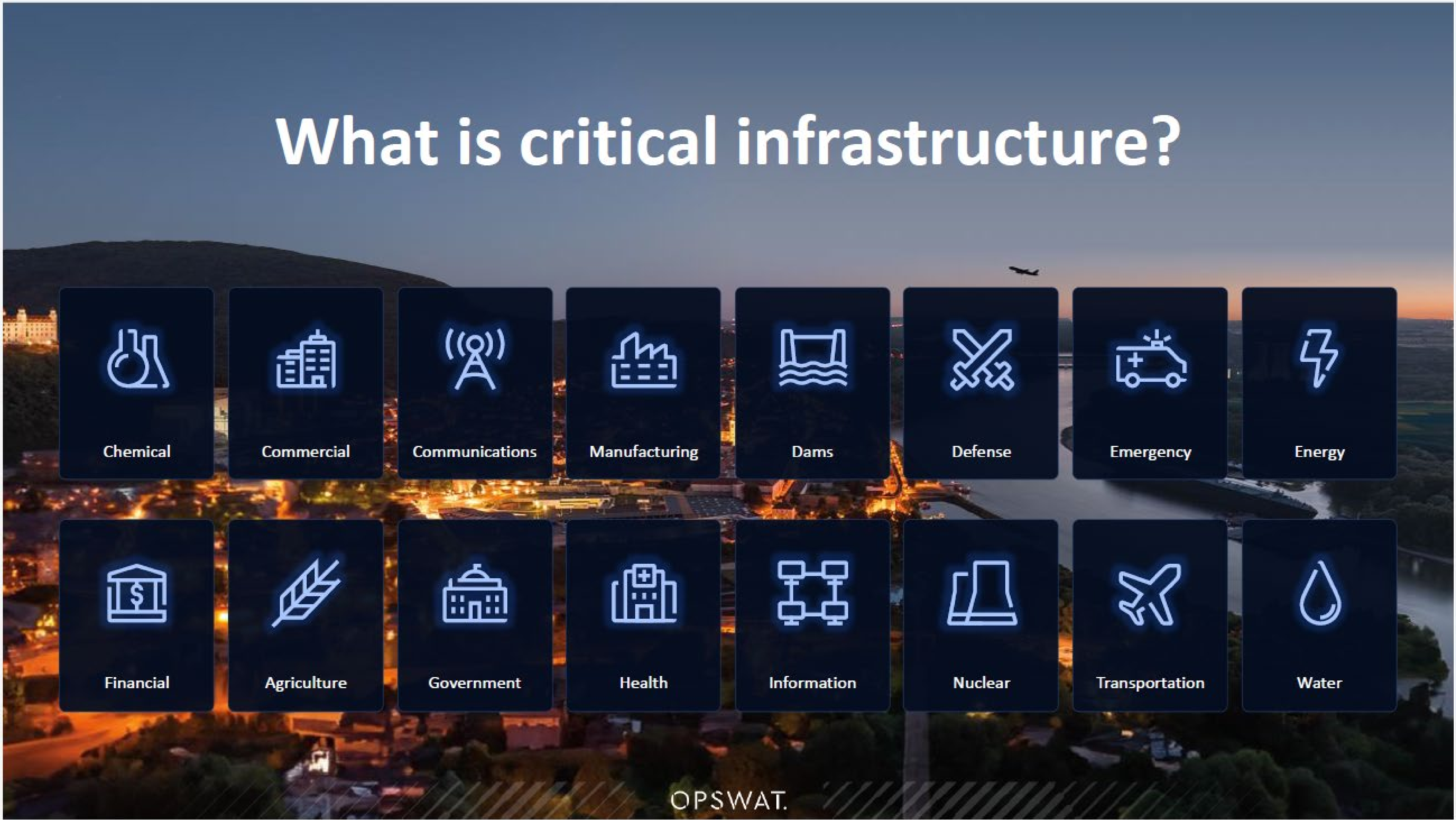
State of Virginia - VITA

Prepared for: State of Virginia - VITA
Prepared by: Rusty Byers & Dylan Higgs
Release Date: v20-5 2024-01
For more information email rusty.byers@opswat.com & Dylan.higgs@opswat.com

OPSWAT.

We Protect the World's Critical Infrastructure

What is critical infrastructure?



- Chemical
- Commercial
- Communications
- Manufacturing
- Dams
- Defense
- Emergency
- Energy
- Financial
- Agriculture
- Government
- Health
- Information
- Nuclear
- Transportation
- Water

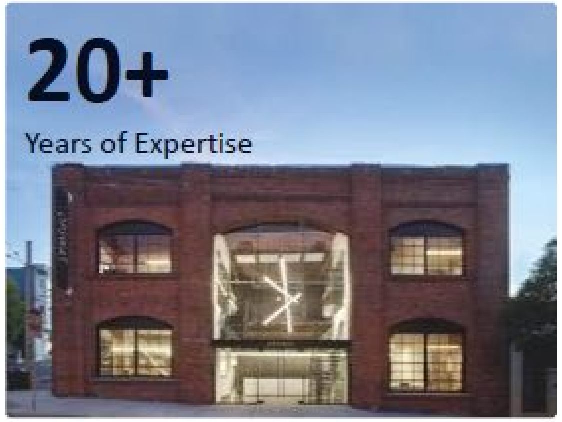
We Are Innovators

80+

Countries Served

1700+

Customers



20+

Years of Expertise

600+

Employees

98%

of US Nuclear Facilities

100K+

Professionals Certified

2023 Cybersecurity Excellence Awards
Gold – ICS/SCADA Security
Gold – Web Application Security
Gold – CS Solution

2023 Globee Awards
Bronze – Cybersecurity

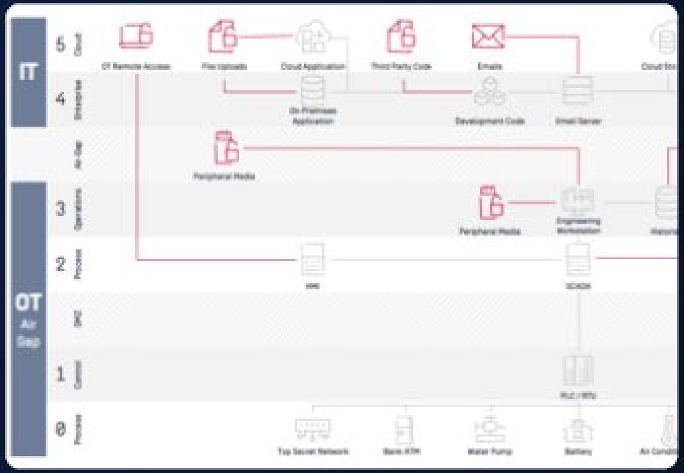
CyberSecurity Breakthrough Awards 3 Years Running
2023 Overall Enterprise Email Security Solution
2022 Professional Certification Program
2021 Overall Infrastructure Security Solution Provider

2023 The Channel Co.
CRN Partner Program Guide

ISO/IEC 27001:2013 Certification.

OPSWAT MetaDefender Core achieved EAL2+
(ALC_FLR. 1) Met all Common Criteria Evaluation Assurance Level

Why It Happens



Network Complexity

- IT-OT Convergence
- Cloud Transformation
- IoT Adoption
- Wide Attack Surface
- Compliance Mandates

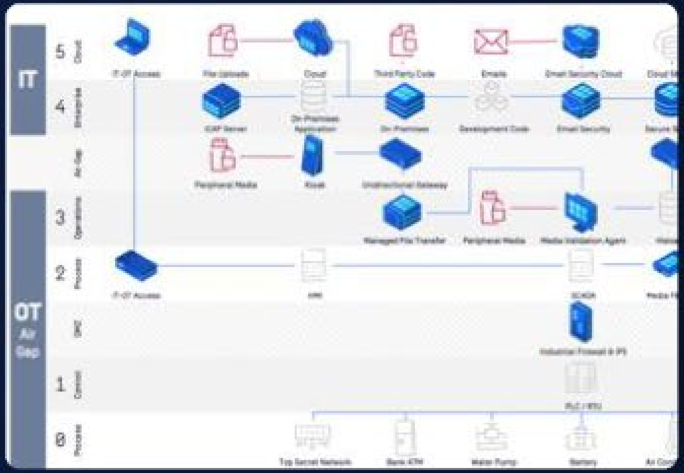
Technology Gaps

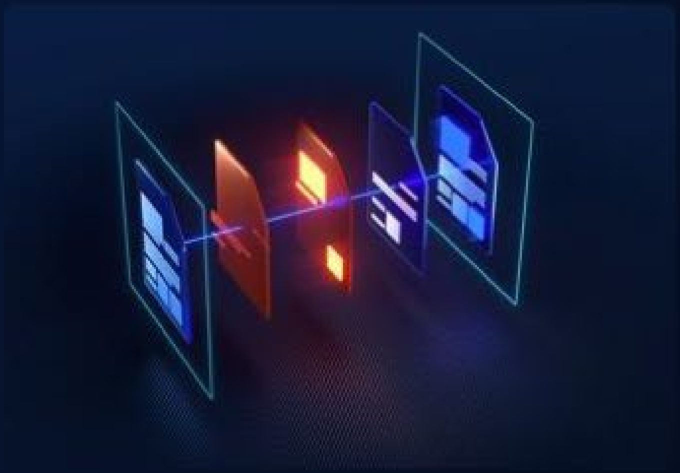
- Malware Bypasses Detection
- Supply Chain Vulnerabilities
- Data Leak Exposure
- Device Exploits
- Network Intrusions

Training Gaps

- Lack of Practical Training
- Means of Certification
- Expert Workforce Shortage
- Lack of Expert Support

Our Approach





Comprehensive Platform

- Covers IT, OT & ICS Use Cases
- Supports Air-gapped Networks
- Cloud, Software and Hardware
- 21 Products and Growing

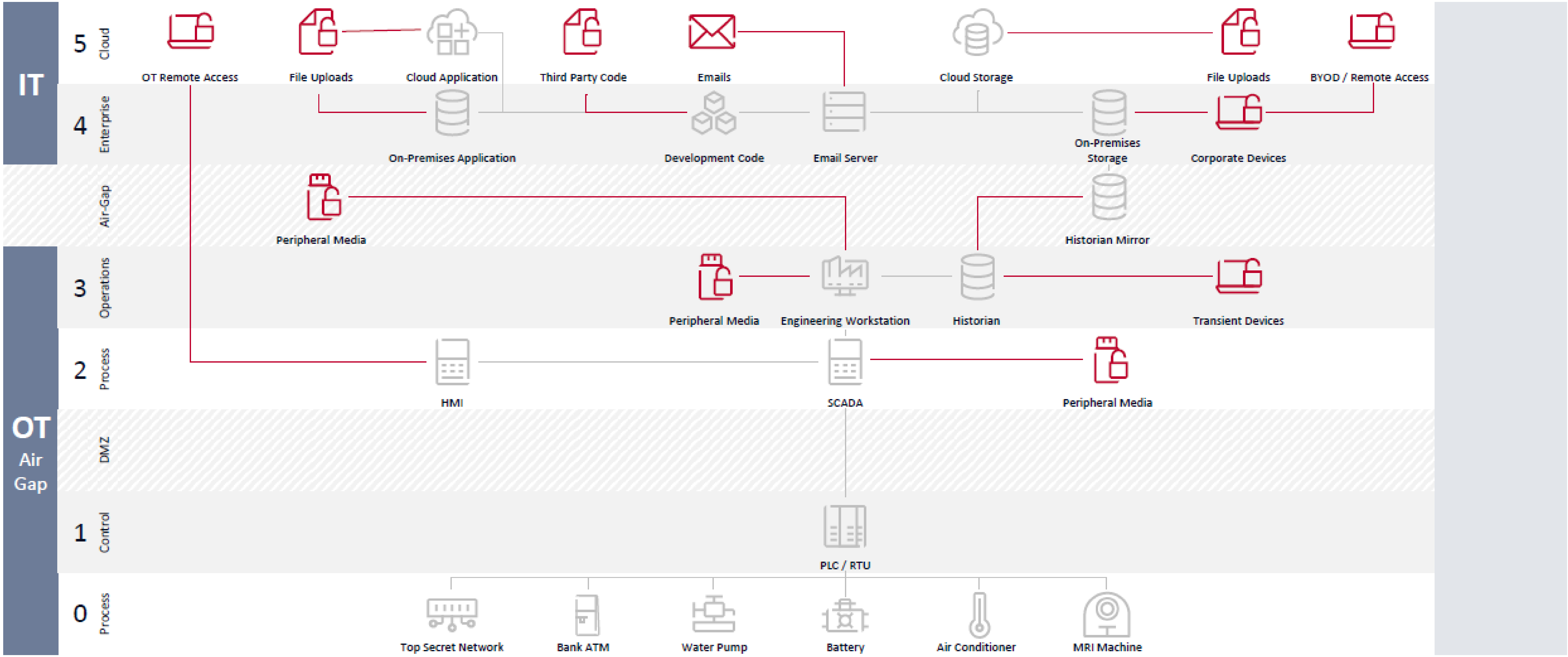
Purpose-Built Technologies

- Prevention Not Based on Detection (CDR)
- Multi-Antivirus Engine Scanning
- File Based Vulnerabilities
- Country of Origin Detection
- Malware Analysis for IT/OT
- CIP Protocol Support

Training Gaps

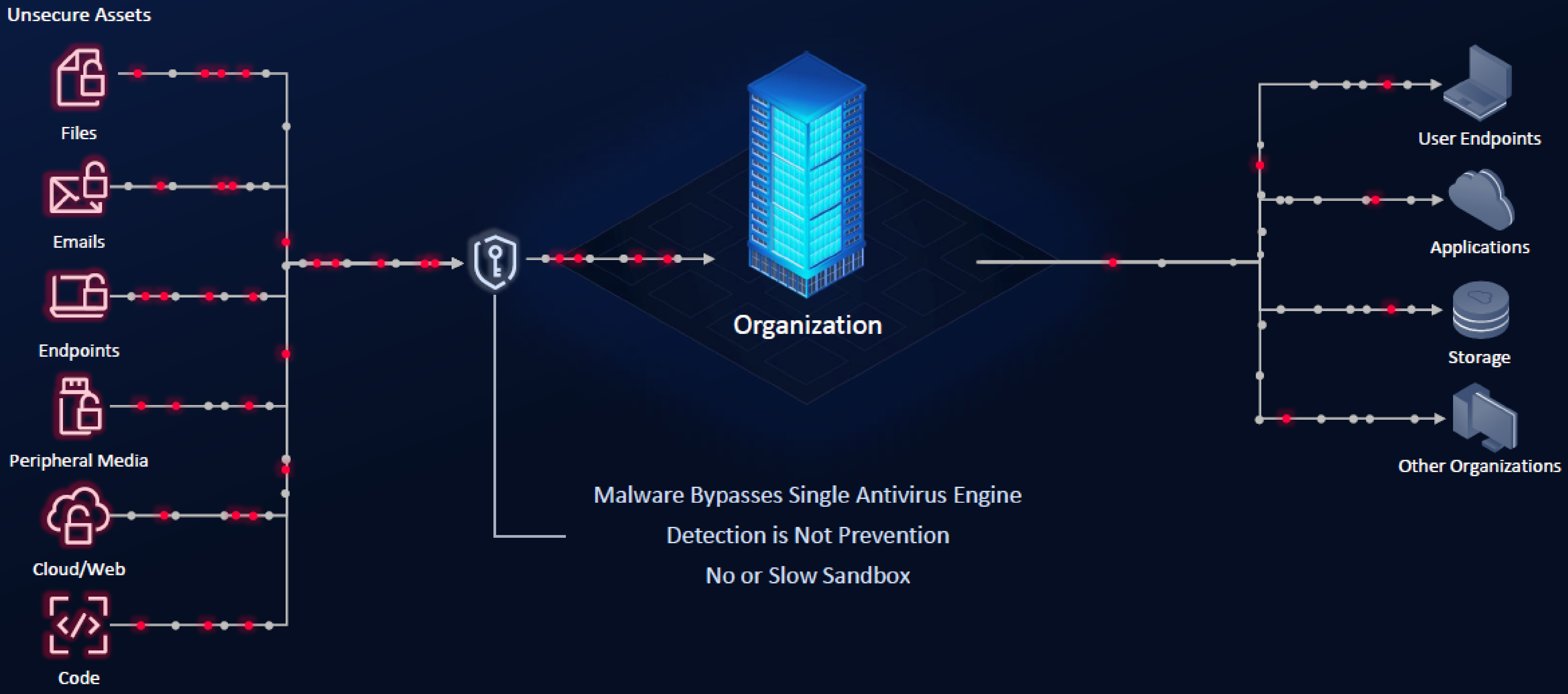
- Practical Online Training and Certification
- Regional CIP Labs

Networks Are Complex, Under Attack, and Require Compliance



OPSWAT.

Traditional Defenses Are Insufficient

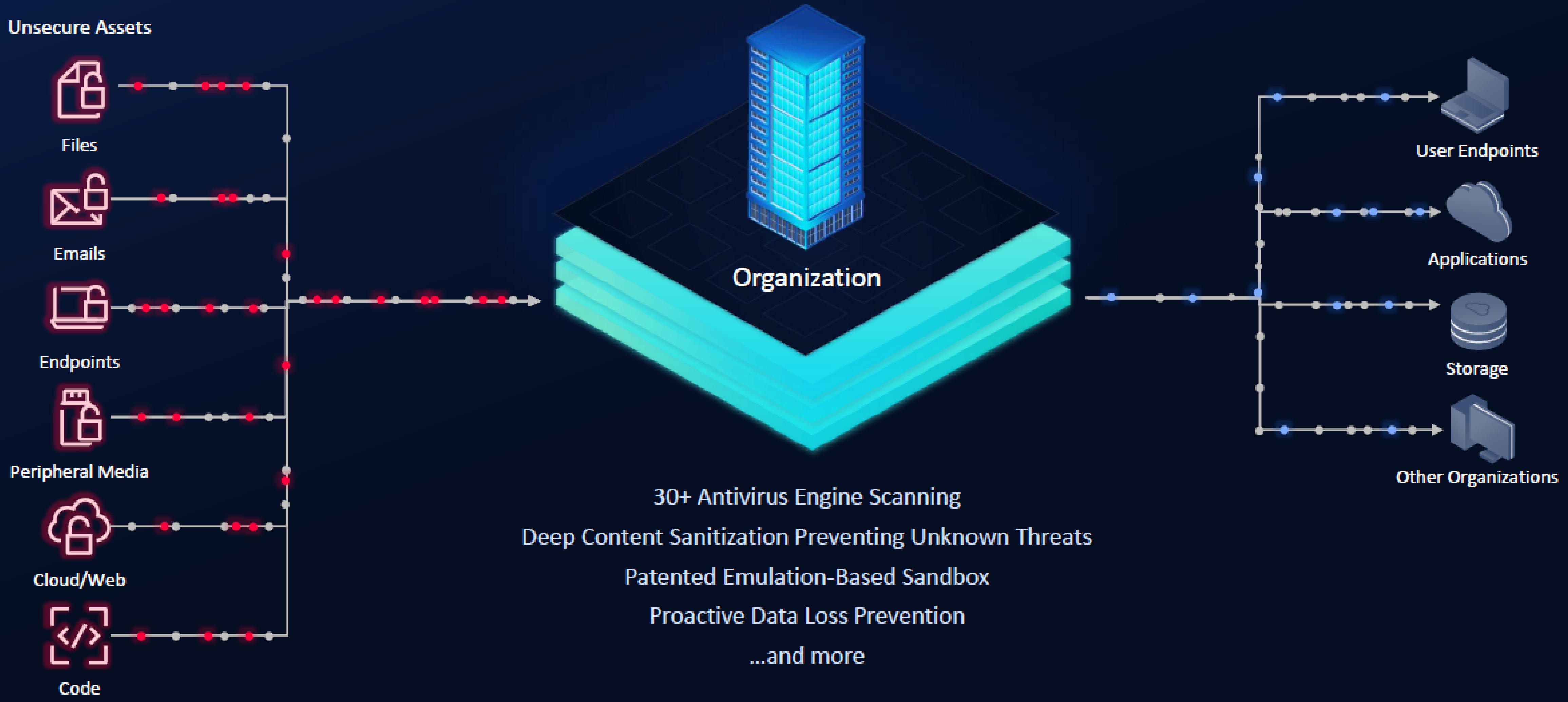


Malware Bypasses Single Antivirus Engine

Detection is Not Prevention

No or Slow Sandbox

We Secure the Flow of Data



30+ Antivirus Engine Scanning

Deep Content Sanitization Preventing Unknown Threats

Patented Emulation-Based Sandbox

Proactive Data Loss Prevention

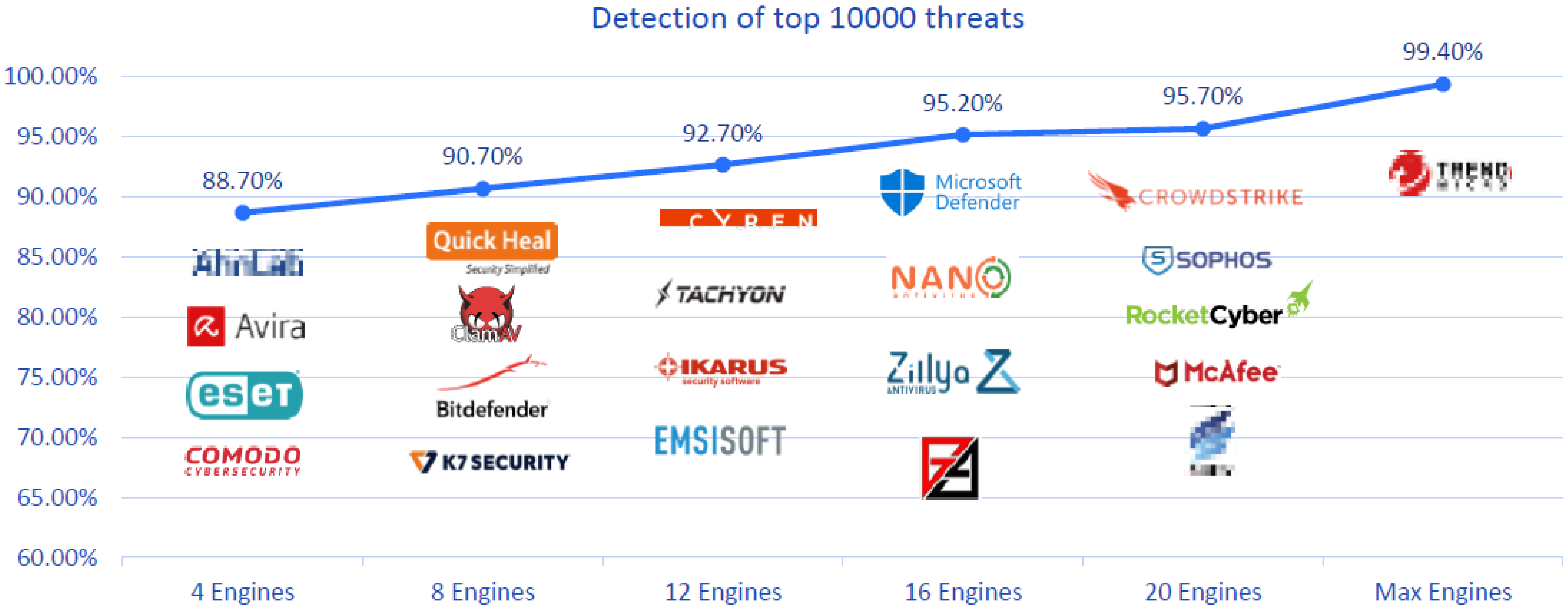
...and more

OPSWAT.

Multi-scanning

The Power of Multiscanning

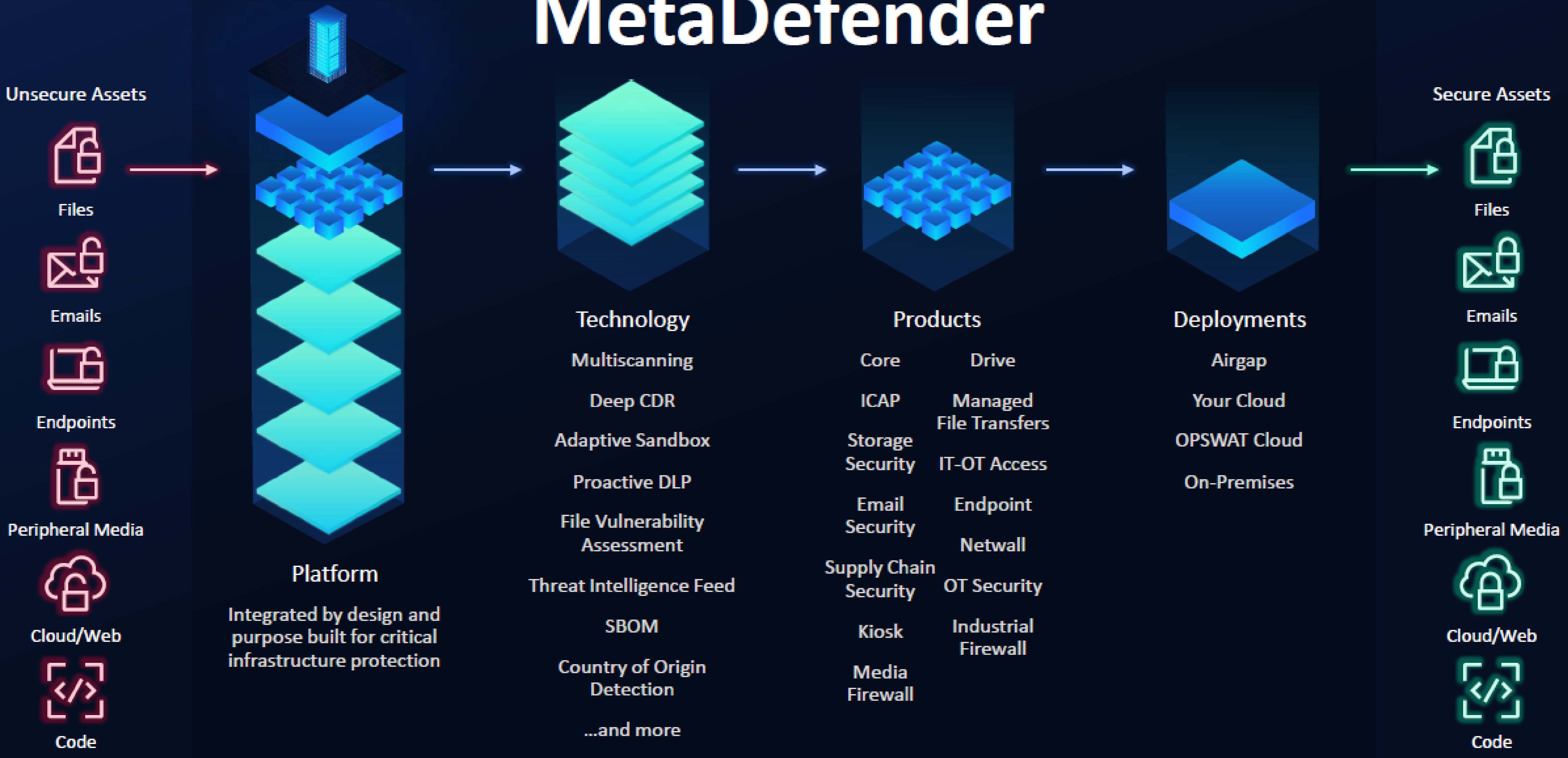
The more anti-malware engines added, the better the malware detection rates



Source: https://metadefender.opswat.com, March 2022

Trust No File. Trust No Device.

MetaDefender



Unsecure Assets

- Files
- Emails
- Endpoints
- Peripheral Media
- Cloud/Web
- Code

Platform

Integrated by design and purpose built for critical infrastructure protection

Technology

- Multiscanning
- Deep CDR
- Adaptive Sandbox
- Proactive DLP
- File Vulnerability Assessment
- Threat Intelligence Feed
- SBOM
- Country of Origin Detection
- ...and more

Products

- Core
- ICAP
- Storage Security
- Email Security
- Supply Chain Security
- Kiosk
- Media Firewall
- Drive
- Managed File Transfers
- IT-OT Access
- Endpoint
- Netwall
- OT Security
- Industrial Firewall

Deployments

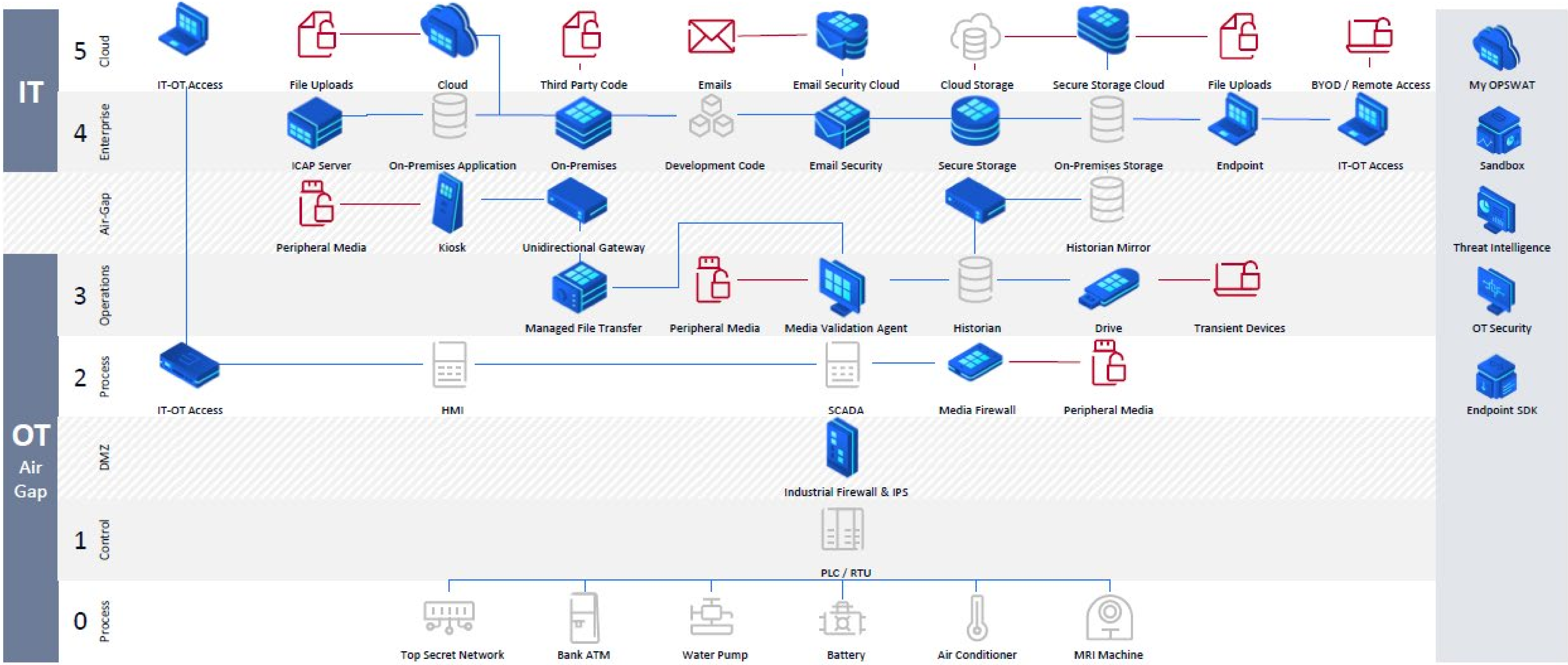
- Airgap
- Your Cloud
- OPSWAT Cloud
- On-Premises

Secure Assets

- Files
- Emails
- Endpoints
- Peripheral Media
- Cloud/Web
- Code

OPSWAT.

OPSWAT Delivers Multiple Lines of Defense

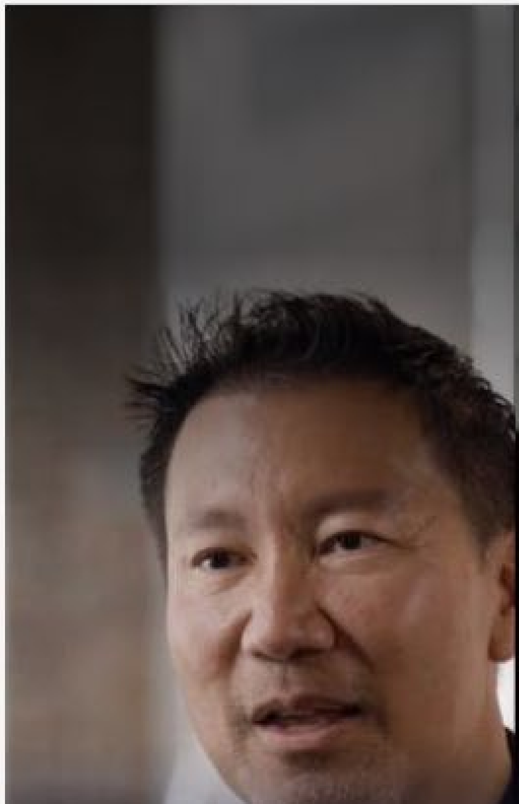


OPSWAT.

#1 Market Leader

Multiscanning & Deep CDR Technology

Customer Success Stories



zoom

Nick Chong
Chief Services Officer

Zoom leverages Advanced cybersecurity threat protection keeping their communication platform malware free.

Read or Watch the Story

Hitachi Energy

Jeremy Morgan
Global Cybersecurity Manager

Hitachi Energy enhances software supply chain resilience with OPSWAT Solutions in the energy sector.

Read or Watch the Story

ivanti

Srinivas Mukkamala
Chief Product Officer

Ivanti implements stringent measures to ensure that devices with secure access are free from malicious code.

Read or Watch the Story

vmware

Kristina de Nike
Director of Product Management

VMware strengthens the security of their VDI environments with a secure access flow.

Read or Watch the Story

BER FLUGHAFEN BERLIN BRANDENBURG

Ronnie Querfurth
IT Solutions and Platforms

Berlin Airport efficiently manage their large file flow while guarding against potential threats hidden in files.

Read the Story

OPSWAT Academy

Award-Winning Associate & Professional Certifications for Practical Cybersecurity Expertise

2022 Cybersecurity Breakthrough Award

Professional Certification Program of the Year

Get Started

opswatacademy.com/get-started

VIRGINIA IT AGENCY

Virginian Identity Program (VIP)

ISOAG Meeting

Ron Sticinski
VIP Program Manager

February 7, 2024

Virginian Identity Program (VIP) update

Program goal and objectives

The goal of single sign-on for Commonwealth of Virginia (COV) applications:

- Create ease of doing business with state and local government agencies by providing a single username and password for constituents
- Provide a central Virginian identity management solution at VITA
- Provide protection of identities and systems with items such as multifactor authentication (MFA) and additional identity proofing tools
- Allow agencies to reprioritize personnel resources and reduce infrastructure
- Ensure compliance with COV standards

Virginian Identity Program (VIP) update

Recent accomplishments

- Released a request for information (RFI) for identity verification services
  - Received responses from 21 vendors including industry leaders such as Experian, TransUnion, ID.me, LexisNexis and IDEMIA
  - All responses used facial recognition for identity verification; several responders indicated participation in NIST Face Recognition Verification Testing (FRVT)
  - Many responses cited certification by Kantara Initiative for their identity assurance level (IAL)2/authenticator assurance level (AAL)2 processes
- Leveraging the service portfolio life cycle management (SPLM) process to develop security, training and support documentation

Virginian Identity Program (VIP) update

Next Steps – Conduct a pilot with the Governor's Office

- Set up the FedRAMP-certified high production and preview Okta CIAM tenants
- Integrate and test Okta CIAM with Governor's Office applications; Working with Governor's News Release and Flag Information applications
- Conduct pilot with Governor's Office applications no later than March 2024
- Stabilize and provide operations and maintenance support for the Governor's Office

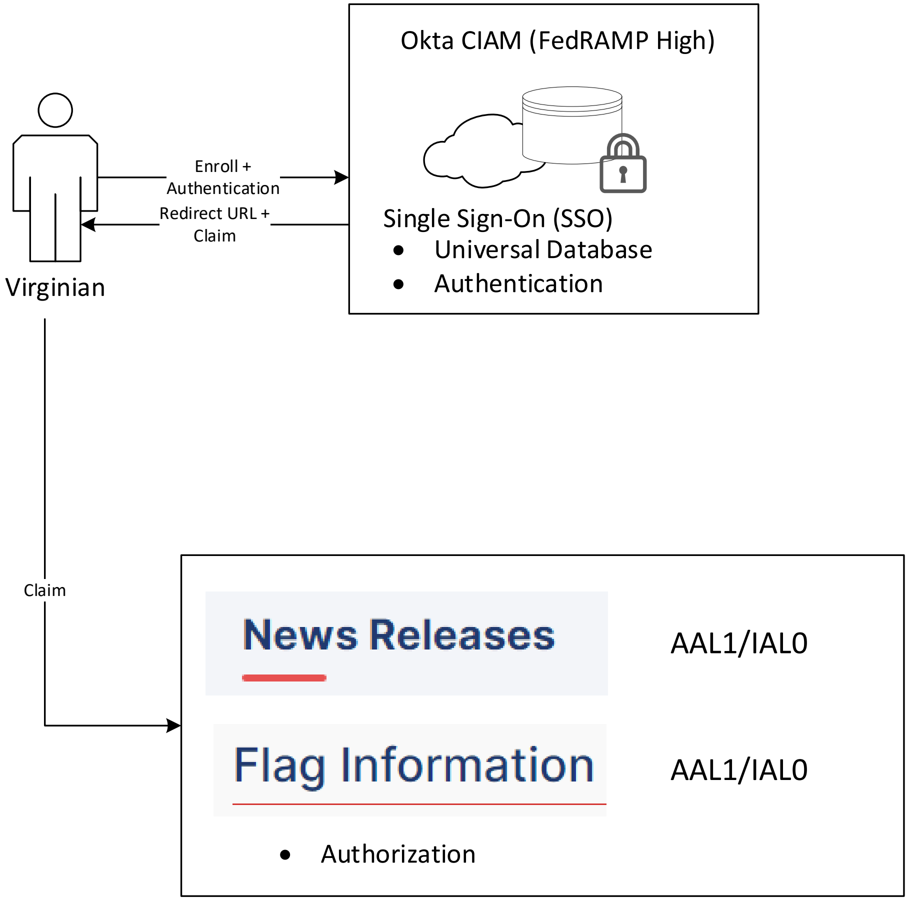
Virginian Identity Program (VIP) update

Additional activities – Prepare and release a request for proposal (RFP) for identity proofing services

- Acquiring licenses, implementation services, technical support (L2/L3) and Client-Facing Help Desk (L1)
- Identity and select source Evaluation Team board members
- Continue to collect and analyze agency technical requirements
- Define the requirements for the RFP
- Prepare a draft RFP for review by VITA and Office of the Attorney General
- Release the RFP for bid by April 2024

Virginian Identity Program (VIP) – Pilot Planning

VIP - Governor's Office Pilot



Pilot Activities

- End Users will attempt to login to the Pilot Applications (only AAL1/IAL0).
- End Users will be required to enroll in VIP.
- Enrollment will allow End Users to self-verify their passwords, email addresses, and phone numbers (authenticators). Use of additional authenticators such as Google Authenticator will be expanded after the pilot.
- Once authenticated, Okta provides a redirect URL for the application along with a claim (Okta ID, user name, etc.)
- The application receives the claim and authorizes the end user.
- Once enrolled End Users will benefit from the VIP SSO service by using the same authenticators to access the Pilot Applications.

LEGEND

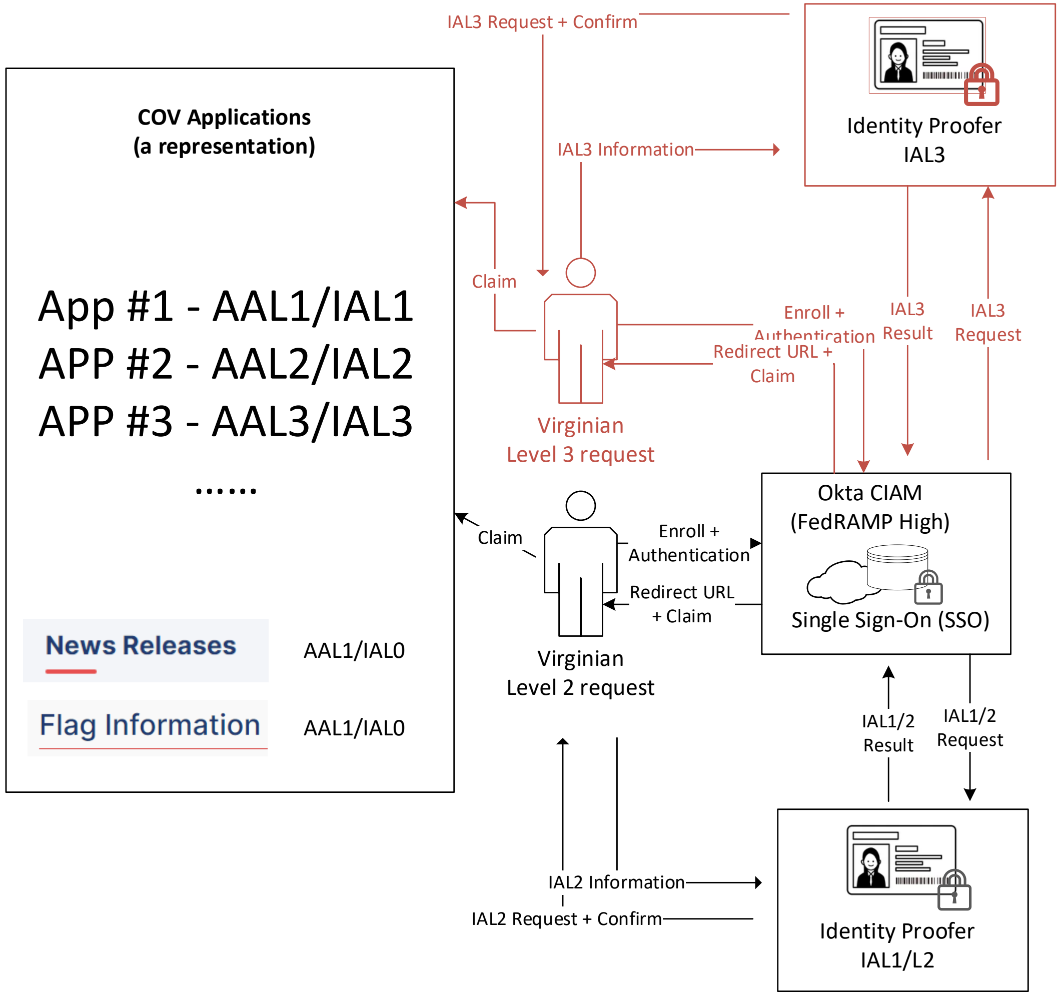
- AAL1 – Authentication Assurance Level 1
- IAL0 – Identity Assurance Level 0

GLOSSARY

- Authentication – Confirms the End User is in control of their authenticators
- Authorization – Once authenticated, the Pilot Applications will grant the privileges for the End User
- Universal Database – End User accounts will be created and stored here by the Okta CIAM
- Virginian – an individual who needs access to COV applications or services for their personal use. Individuals will be expanded at a later time.

Virginian Identity Program (VIP) – Identity Proofing (Part of RFP)

VIP – with Identity Proofing (Projections)



COV Applications
(a representation)

App #1 - AAL1/IAL1
APP #2 - AAL2/IAL2
APP #3 - AAL3/IAL3
……

News Releases AAL1/IAL0

Flag Information AAL1/IAL0

IAL3 Request + Confirm

IAL3 Information

Identity Proofer
IAL3

Claim

Enroll + Authentication

Redirect URL + Claim

IAL3 Result

IAL3 Request

Virginian
Level 3 request

Okta CIAM
(FedRAMP High)

Single Sign-On (SSO)

Claim

Enroll + Authentication

Redirect URL + Claim

Virginian
Level 2 request

IAL1/2 Result

IAL1/2 Request

IAL2 Information

IAL2 Request + Confirm

Identity Proofer
IAL1/L2

Identity Proofing Activities

- End Users will attempt to login to a COV application
- End Users will be required to enroll in VIP
- Enrollment will allow End Users to create authenticators consistent with the AAL of the application
- Okta will request identity proofing consistent with the IAL of the application
- The End User will provide information that will be processed by the Identity Proofer.
- The Identity Proofer will provide the results of the proofing attempt.
- Okta will record the results of the identity proofing attempt.

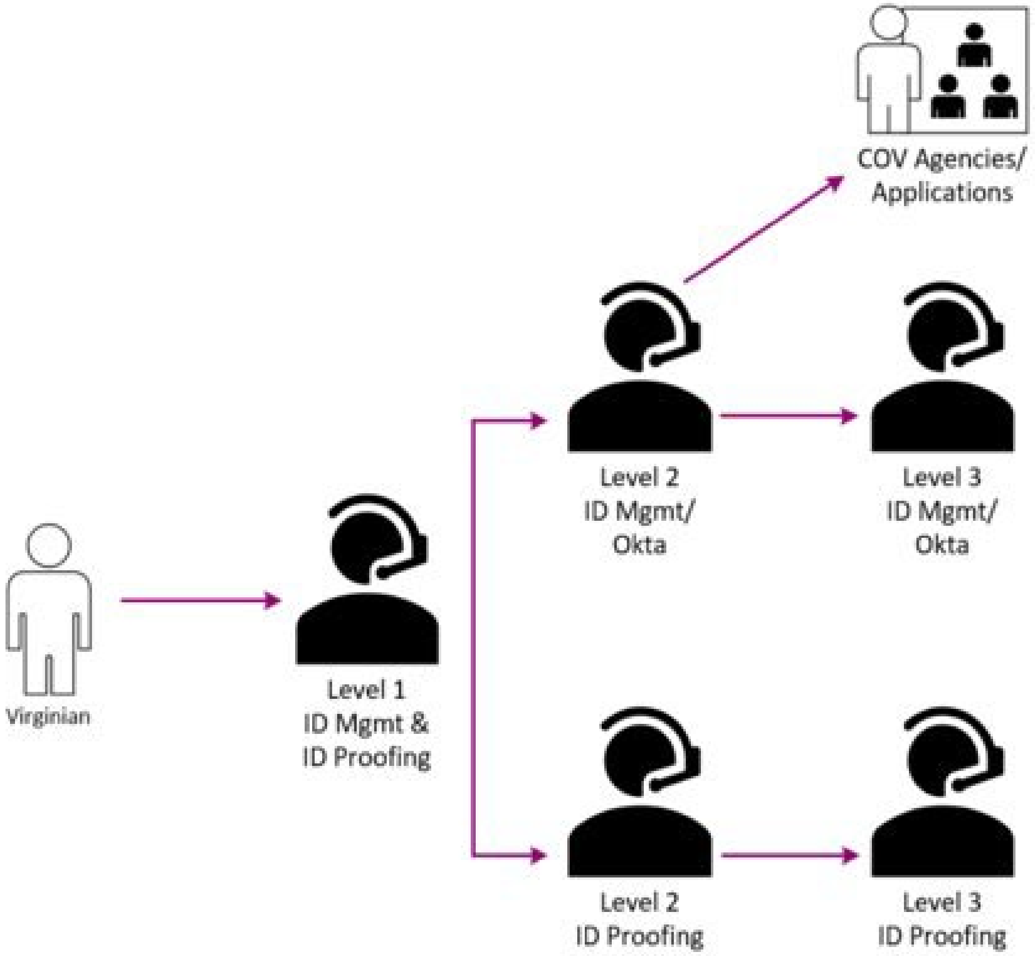
LEGEND

- AAL2/3 – Authentication Assurance Levels 2 or 3
- IAL1/2/3 – Identity Assurance Levels 1, 2, or 3

GLOSSARY

- Identity Proofing – the process of collecting, validating, and verifying the information about a person
- Virginian – in addition to individuals using COV applications for personal use, scope will be expanded to include individuals representing an organization

Virginian Identity Program (VIP) – Help Desk and Technical Support (Part of the RFP)



Questions?

splunk>

VIRGINIA
IT AGENCY

Richard White

Director of Security Services and Product Management

Feb. 7, 2024

VIRGINIA IT AGENCY

New Vulnerability OKR

Jonathan Smith, Director of Risk Management

Matthew Umphlet, Threat Intelligence Analyst

ISOAG

January 7th,2024

How we Choose our Top 5

- VITA’s new initiative to eliminate critical vulnerabilities in COV environments
- Vulnerabilities Criteria
  - Critical and High Vulnerabilities
  - Vulnerabilities that will have a large impact on the security posture of the COV
  - Vulnerabilities are spread across servers and workstations
  - Across a majority of agencies
- Every agency may not be affected by every vulnerability in the monthly top 5
- More Information can be found in Nucleus for each vulnerability, including affected systems, by clicking on vulnerabilities tab and searching by name.
- Vulnerabilities are also grouped by Responsibility (Agency vs Tower)

Escalation Path

- Additional vulnerabilities will be added each month, with previous months being marked as overdue for remediation. If these vulnerabilities are not remediated in the following timeframes, notifications will be completed as follows.
- 30 Days: VITA CSRM will Issue a Risk Alert Message
- 45 Days: Message will go to Agency head
- 60 Days: Message will go to Secretariat

Critical Vulnerabilities for January

- Apache Log4j < v2.16 RCE (this will include the two for Apache Log4j < 2.15 for NIX and for Windows)
- Oracle WebLogic Multiple Vulnerabilities (April 2017 & July 2017 Quarterly patches missing)
- KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update (Win 2K8 and 2K8R2 went EOL on 1/14/20)
- KB5032249: Windows Server 2012 R2 Security Update (November 2023) (Win 2K12 and 2K12 R2 went EOL on10/10/23)
- Microsoft Edge (Chromium) < 117.0.2045.31 Multiple Vulnerabilities (affects both servers and workstations)

Upcoming Events

VIRGINIA IT AGENCY

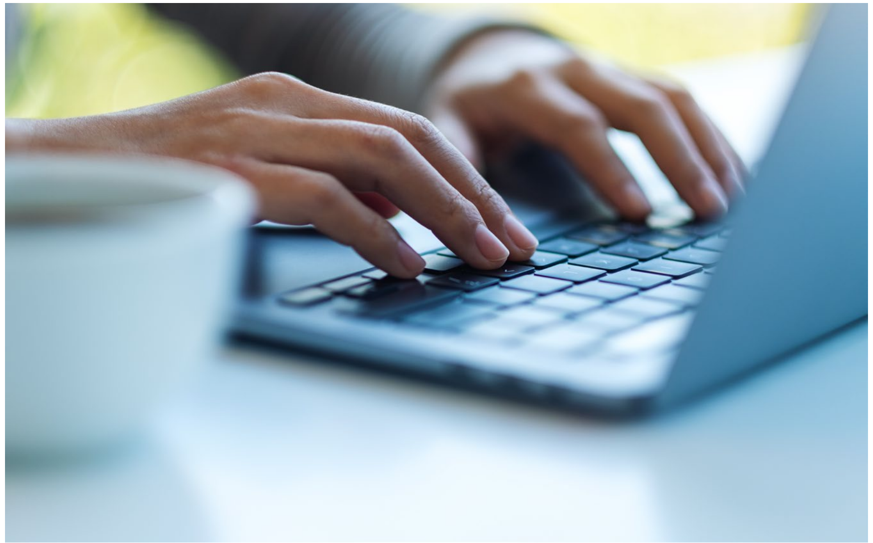
vita.virginia.gov

IS Orientation

The next IS Orientation is being held on March 27, 2024

- It will be held virtually via WebEx from 1pm-3pm
- Please register at the link below:

https://covaconf.webex.com/weblink/register/rd212e769bb8f06f1b608aebd01be1cd7



Hybrid ISOAG Meeting

The April 3, 2024 Information Security Officer's Advisory Group will be held both in-person, and remotely via WebEx.

- In-person will be held at VITA, located at the Boulders, seating will be limited to 50 persons and attendees must pre-register. Registration for in-person is on a first come, first served basis. The virtual meeting is open to all.
- For **in-person**, please register at:

  https://covaconf.webex.com/weblink/register/r87b82b890ceb4dc5cb1e345c753e720e
- For **remote**, please register at the link below:

  https://covaconf.webex.com/weblink/register/redb8bc29e26e987624b761cd4b7cbd2f

CIS Center for Internet Security®
Creating Confidence in the Connected World.™

NATIONWIDE CYBERSECURITY REVIEW

NCSR Assessments are Due Feb. 29, 2024

- Please submit your completed Assessment prior to end of month!

Government Innovation Virginia

Transforming Virginia: Bridging Innovation and Progress

PUBLIC SECTOR NETWORK

Public Sector Network is presenting: Government Innovation Virginia

- Held on Wednesday, April 17, 2024, at the Downtown Richmond Marriott
- The registration link is below, and attendance is free of charge.
- Government Innovation Virginia 2024 - Public Sector Network

MEETING ADJOURNED

VIRGINIA
IT AGENCY