Securing File Transfer & Threat Prevention in Air-Gapped OT Environments

Practical controls for removable media, secure transfer workflows, and offline-capable inspection

OTCEP Forum 2026 | Speaker: Sal Morlando CTO, Diodes & Security Gateways, OPSWAT

What This Session Will Cover

In scope

Practical file transfer controls for OT zones, air-gapped sites, removable media, contractor workflows, supply chain updates, offline inspection, and governance.

Not in scope

Product architecture, product demos, proprietary screenshots, or claims that one vendor category solves the whole OT problem.

- **Balanced threat framing:** files, credentials, exposed remote access, and network exploitation all matter.
- **Practical emphasis:** how to run controls without blocking legitimate engineering work.
- **Outcome:** a reference model operators can adapt to their own risk tolerance and regulatory environment.

OT Risk: It’s Not Just the Transfer. It’s What Crosses the Boundary.

Air-gapped OT environments still depend on:

- **Software updates**
- **Engineering projects**
- **Vendor packages**
- **Reports and logs**
- **Backups and configurations**
- **Removable media**

Control Objective
Only authorized, inspected, policy-compliant content crosses into OT.

4 Common Ways Risk Reaches OT

1. Removable media

USB drives, maintenance kits, test results, field laptops

2. Insecure transfers (data, files)

Ad hoc file shares, historian exports, reports, patch packages, telemetry data

3. Supply chain and software updates

Firmware, installers, licenses, project files, engineering tools

4. Third party and vendor remote access

VPNs, jump hosts, contractor laptops, living-off-the-land activity

The file layer is a control point, not the whole threat model.

Incidents Point to Practical Controls, Not One Silver Bullet

Ukraine power disruption

CISA documented the 2015 Ukraine power outage and BlackEnergy malware reports.

Lesson: harden remote access, logging, recovery, and file-handling paths.

Internet-Facing PLCs Attack

ISA and the FBI reported state-affiliated compromises of exposed PLCs across critical infrastructure sectors.

Lesson: minimize OT exposure, enforce segmentation, and restrict remote access.

Volt Typhoon activity

CISA and partners warned about PRC actors using living-off-the-land techniques and valid accounts against critical infrastructure.

Lesson: file inspection must sit beside identity, monitoring, and segmentation.

Takeaway: build controls that catch malicious content before use and also contain paths where no malicious file is needed.

Air-Gapped OT Changes the Operating Model

Offline by design

Updates and security content must be transferred manually.

Constrained by reality

Legacy systems and limited downtime restrict security operations.

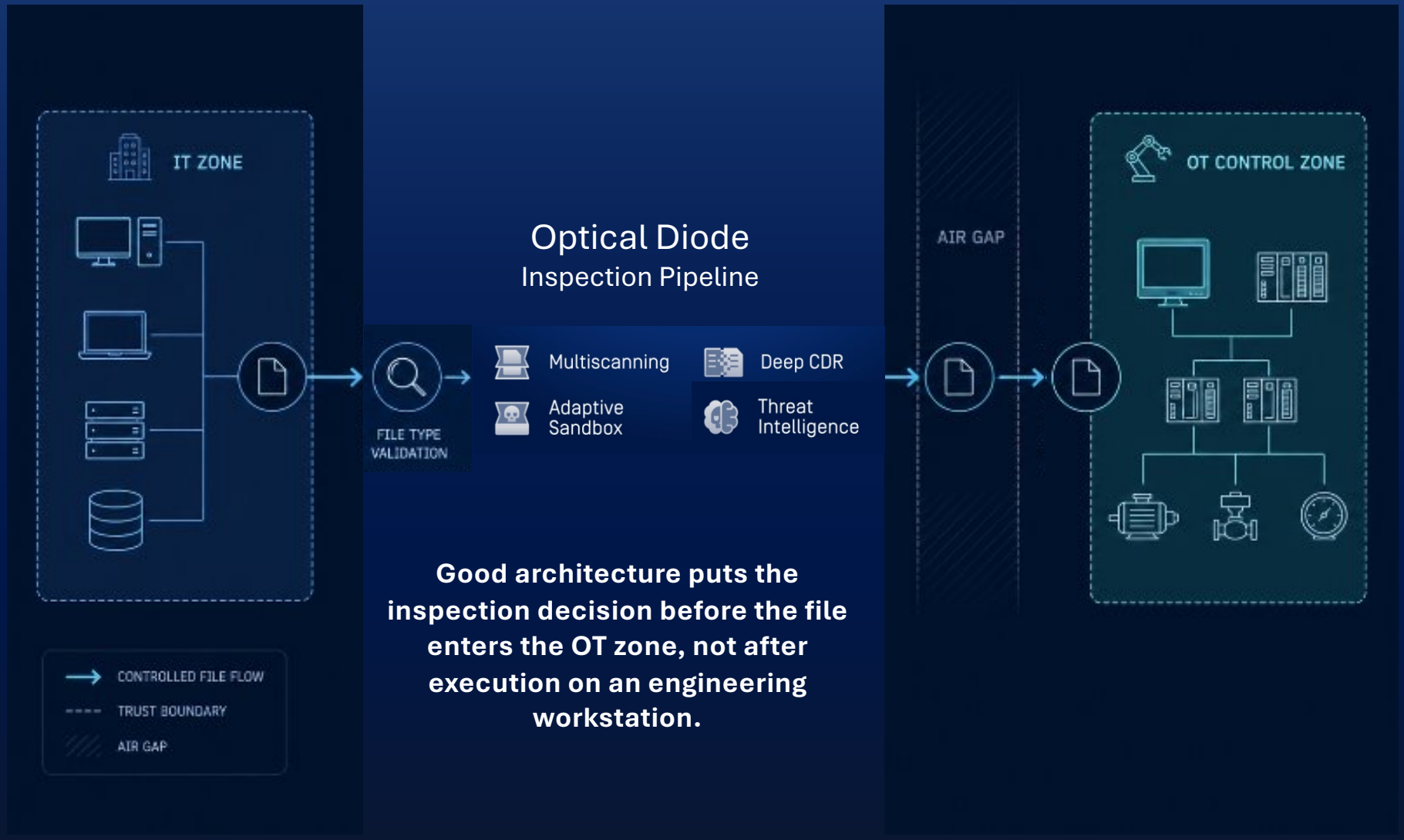
Operational tolerance

Security controls cannot disrupt maintenance or production.

Audit & Accountability

Every file movement and approval must be auditable.

Reference Model: Inspect at the Trust Boundary



Good architecture puts the inspection decision before the file enters the OT zone, not after execution on an engineering workstation.

Step 1: Define File Transfer Policies

Classify

File type, source, destination, business purpose, sensitivity

Authorize

Named requestor, approver, transfer window, expiry, policy owner

Inspect

Required controls by file class and destination zone

Record

Hash, verdict, user, approval, release decision, retained evidence

Control design question:
What would make this transfer unacceptable even if the file scans clean?

Removable Media Inspection: Design It So People Actually Use It

1. Register

Link media to a person, site, purpose, and time window.

2. Inspect

Verify file type, scan for known threats, sanitize supported content, analyze unknown high-risk files.

3. Release

Write only approved content to clean media or a controlled transfer point.

4. Audit

Keep evidence of what was blocked, what was released, who approved exceptions, and why.

Operational rule:
Never make the secure path slower than the workaround.

Secure File Transfer Workflow: Separate Delivery From Trust

Business purpose & destination defined

File lands outside OT zone first

Controls run by policy class

- Scan
- Deep CDR
- Analysis

Human or automated decision with evidence

Only approved content crosses boundary

A secure transfer service should enforce policy, not just encrypt movement.

Capability Map: 5 security technologies, different jobs

1. File type verification

Stops spoofed extensions, malformed files, and policy violations before deeper analysis.

2. Multiscanning

Catches known malware quickly using diverse detection engines and offline signature updates.

3. CDR

Removes active content from supported documents without needing to know whether it is malicious.

4. Sandboxing

Executes or emulates suspicious high-risk content to observe behavior and extract indicators.

5. Reputation & Threat Intelligence

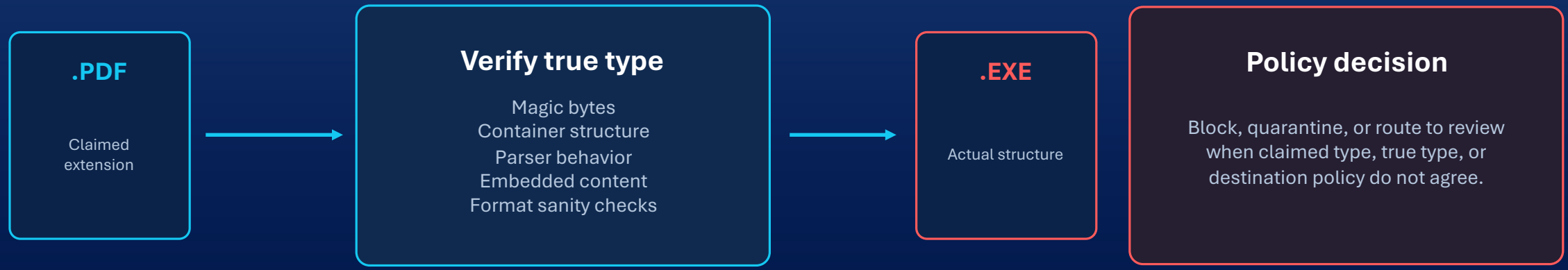
Adds context from known hashes, URLs, domains, certificates, patterns, and related campaigns.

1. File Type Verification

Stop spoofed, malformed, or unauthorized files before deeper inspection or OT release.

What it answers

Does the file match its claimed identity and the policy for this OT destination?



OT examples

A firmware .bin, PLC project, STEP file, or license package should be verified before it reaches an engineering workstation.

Why it matters

Spoofed extensions, polyglots, malformed files, and embedded executables often bypass simple policy checks.

Where it sits

Run this first at the staging area, kiosk, transfer gateway, or cross-domain boundary before scan, CDR, or sandboxing.

Evidence to keep

Claimed type, detected type, hash, source, destination, rule triggered, decision, approver, and timestamp.

Design rule: Do not trust the extension. Trust the parsed structure, policy context, and release decision.

2. Multiscanning: useful fast signal, not final truth

Where it shines

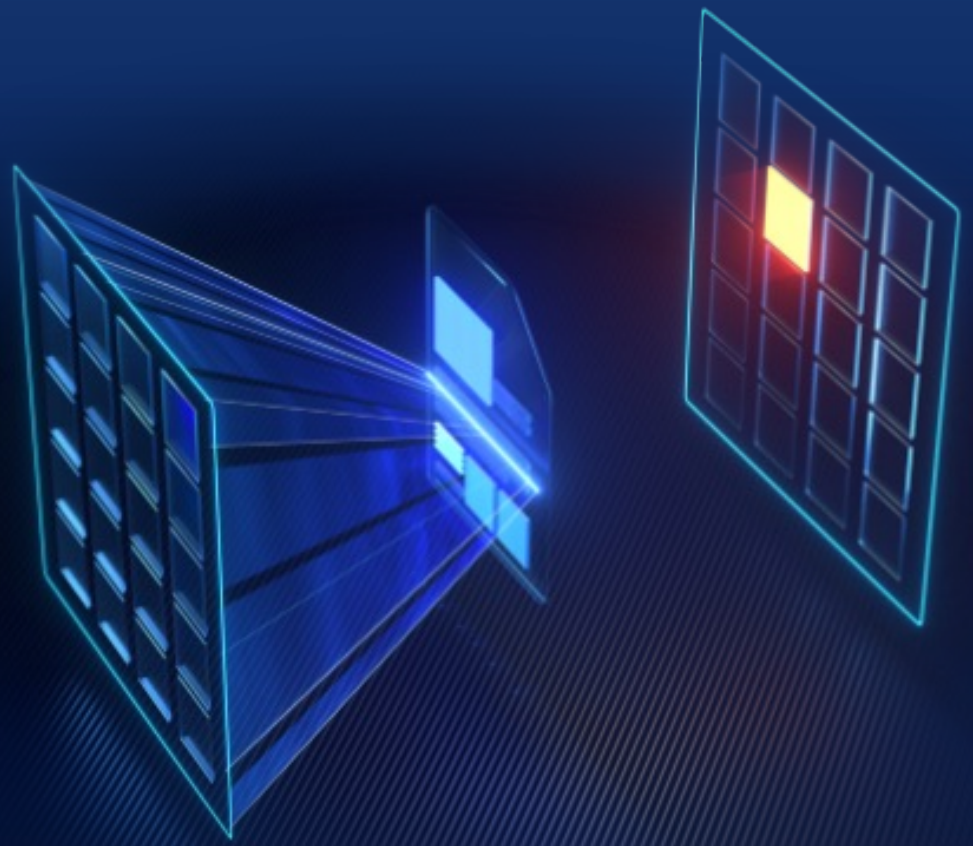
Known malware, known suspicious files, rapid triage, broad signature coverage, and high-volume screening.

Where it struggles

Brand-new payloads, heavily modified samples, fileless behavior, and threats hidden behind execution conditions.

Offline operating point

Use signed update packages, staged import, validation checks, rollback options, and documented update cadence.



Design decision: use multiscanning as the first high-speed filter, then route unknowns by policy.

3. CDR: prevention when detection is uncertain

Best fit

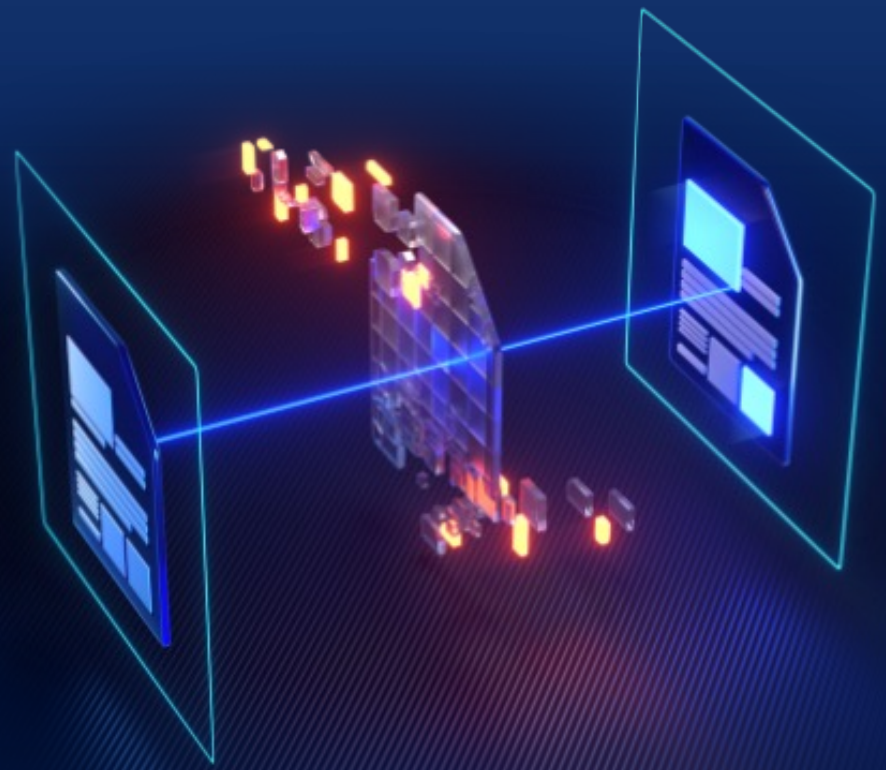
Office documents, PDFs, images, archives, and formats where active content can be removed or rebuilt safely.

Security value

It does not need to identify the malware. It removes risky active content and reconstructs a usable clean file.

Limits to plan for

Executables, firmware, engineering files, signed packages, and files where alteration breaks authenticity or function.



CDR is strongest when paired with policy: sanitize what can change, analyze what must remain intact.

4. Sandboxing & Behavioral Analysis: Reserve Depth for the Right Files

Use it for

Executables, scripts, installers, firmware packages, suspicious archives, unusual behavior, or files that cannot be sanitized.

Avoid the bottleneck

Do not detonate everything by default. Route by file risk, source trust, destination criticality, and previous verdicts.

Offline considerations

Keep analysis local when required, control sample retention, and define how IOCs move back into monitoring tools.

Measure success

Time to verdict, queue depth, analyst touch rate, false block rate, and number of exceptions.

5. Threat Intelligence in Air-Gapped OT is a Logistics Problem

Package

Signed updates: reputation data, YARA, allowlists, detection rules, known-good hashes

Transport

Data diode, controlled connection window, removable media, or couriered media

Apply

Staged deployment, scan regression, operational change record

Validate

Integrity checks, version tracking, rollback, source verification

Export

Indicators, reports, metrics, and blocked-file evidence leaving the zone safely

Quarantine & Exception Handling are Where Trust is Won or Lost

Quarantine

Store blocked or uncertain files outside the OT destination. Preserve the original and any transformed version.

Review

Use a risk-based decision path. High-criticality zones need stronger approval and evidence than low-impact transfers.

Release

Use clean media or controlled handoff. Do not let users self-release from quarantine without policy guardrails.

Bad exception processes create shadow workflows.
Good ones make the secure path usable under pressure.

Fit File Inspection Into the Existing OT Control Stack

Governance

Transfer policy, asset ownership, change management

Identity

MFA, privileged access, contractor accounts

Network

Segmentation, conduits, jump hosts, one-way flows

Endpoints

Engineering workstation hardening, application control

Monitoring

OT network detection, logs, SIEM, incident response

File controls

Media inspection, CDR, sandboxing, reputation, secure transfer

Layered defense works when each layer knows what the others cannot see.

Framework Alignment: Translate Requirements Into Procedures

IEC 62443

Zone and conduit controls, least privilege, malware protection, system integrity. Translate into boundary transfer rules and evidence.

NERC CIP

Malware prevention, removable media, transient cyber assets, change control. Translate into scanning, authorization, and audit records.

Singapore CCoP 2.0

Protection, supply chain, incident readiness, and secure operations. Translate into transfer governance and supplier validation.

Do not present a control map as compliance.
Present evidence that the workflow runs consistently.

90-Day Roadmap

Days 1-30

Map file flows. Identify media entry points, transfer paths, file classes, owners, and bypasses.

Days 31-60

Pilot removable media inspection and secure staging for one OT site or one high-value transfer workflow.

Days 61-90

Add policy-based routing: sanitize supported content, scan known-risk files, analyze high-risk unknowns, and formalize exceptions.

Success metric: fewer unmanaged transfers, faster approved releases, and clearer evidence when something is blocked.

Bottomline: Make File Movement a Controlled Operation

- Treat file transfer as a risk decision, not an IT utility.
- Inspect before OT exposure, especially for removable media and supply chain content.
- Use layered controls: verify type, scan, sanitize, analyze, enrich, approve, and log.
- Design offline operations deliberately: update logistics, quarantine, exceptions, and evidence.
- Keep the secure path usable. If it blocks maintenance work without a clear process, teams will route around it.

THANK YOU