Why You Should Add Air Gaps Before and After a CDR/XDR File Cleansing Server

By Juda Slomovich – Head of U.S. Expansion, Terafence

In today's advanced threat landscape, even powerful tools like Content Disarm and Reconstruction (CDR) and Extended Detection & Response (XDR) need reinforcement. For sectors like critical infrastructure, defense, healthcare, and OT networks, the best practice is clear: implement air-gaps before and after your CDR/XDR server —with a trusted data diode in between.

What Is a CDR/XDR File Cleansing Server?

A CDR/XDR file cleansing server protects internal systems by sanitizing incoming files:
- Disassembles files into individual components
- Removes malicious code (scripts, macros, obfuscation)
- Reconstructs clean, usable versions
- Passes them into a secure environment

Unlike antivirus tools that rely on known signatures, CDR solutions proactively treat all files as potentially malicious. XDR adds monitoring and detection across endpoints and applications, providing visibility post-ingestion.

Why Air-Gapping Is Critical

Even the best CDR/XDR solution can be targeted. That's why physical and logical isolation through air-gapping is essential—it stops threats before they reach critical networks and prevents any chance of reverse communication.

1. Air Gap Before the CDR Server

Goal: Prevent direct exposure to the internal network.
- Files from external sources (USB, email, FTP) first pass through a DMZ or an offline device.
- Reduces chances of a compromised file infecting the CDR system itself.

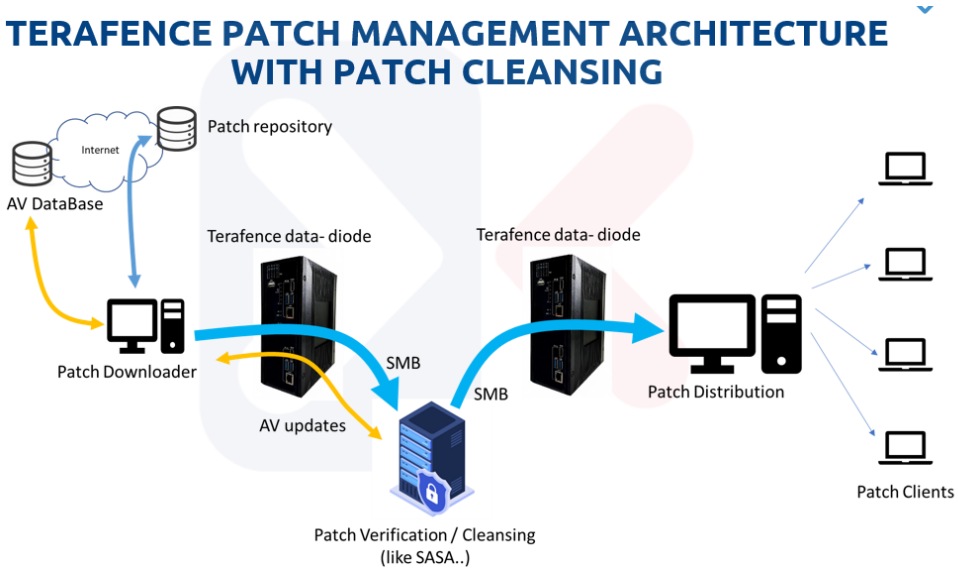
2. Air Gap After the CDR Server — with Terafence Data Diode

Goal: Guarantee one-way data flow into secure networks.

At Terafence, we provide industry-leading hardware-enforced data diode solutions designed specifically for OT and mission-critical environments. Our data diodes:
- Physically enforce unidirectional communication
- Block all reverse flow—no call-backs, no data exfiltration
- Meet the highest security standards (ICS/SCADA, IT, medical)

This ensures that even if a threat attempts to bypass CDR, it can never reach your protected systems.

Recommended Architecture



Case Study: Kaseya VSA Ransomware Attack (July 2021)

In July 2021, the REvil ransomware gang exploited vulnerabilities in the Kaseya VSA patch and remote management platform to distribute malicious updates to over 1,000 customer endpoints—including managed service providers and their clients. The attackers gained access to Kaseya's update infrastructure, signed malicious patches using legitimate credentials, and pushed ransomware payloads to thousands of systems worldwide.

Impact: Massive ransomware deployment across the supply chain, significant operational disruptions, and hundreds of organizations affected.

How a Terafence Data Diode Would Have Helped

By inserting a one-way Terafence data diode between the patch management system and internal networks, you ensure that:

1. Upstream channels are strictly unidirectional files (patches) can flow in, but no connections go out.
2. Even if attackers compromise Kaseya's infrastructure, malicious patches fail to reach internal systems.
3. Prevents command-and-control, rollback, or lateral movement, breaking the attack chain even at the source.

Takeaway for Your Security Architecture

In scenarios like Kaseya—and similar supply-chain attacks—adding a Terafence data diode provides:

- An airtight one-way barrier, ensuring that patch deployment doesn't become a backdoor.
- A clear defense-in-depth strategy:
  Patch management → CDR/XDR sanitization → Data diode → Secure internal network

Benefits of This Architecture

Feature	Benefit
Front-End Air Gap	Isolates entry; prevents initial breach
CDR/XDR Cleansing	Removes malware, zero-days, malicious scripts
Terafence Data Diode	Physically blocks reverse flow, ensures one- way entry
Layered Defense-in-Depth	Redundancy, segmentation, and reduced attack surface

Final Thoughts

Modern attacks are stealthy, persistent, and increasingly file-borne. Sanitization is critical—but isolation is non-negotiable. By combining CDR/XDR technologies with air-gapping and Terafence data diodes, you implement a true zero-trust perimeter around your most sensitive assets.

CDR/XDR + Dual Air Gaps + Terafence Diode = Maximum Security

If you're looking to secure your critical networks and would like help evaluating or implementing this architecture, I'd be glad to assist.

Please contact: Juda@terafence.com

www.Terafence.com