

CDR/XDR Server Vendors & Air-Gap Architecture with Terafence



Terafence TFG1U-RP – Hardware Data Diode Appliance

In critical infrastructure, government, OT/ICS, and high-security networks, combining CDR (Content Disarm and Reconstruction) and XDR (Extended Detection and Response) solutions with Terafence data diodes provides unmatched protection against malware, ransomware, and advanced persistent threats.

What Is CDR/XDR?

- CDR sanitizes files by removing embedded threats like macros, scripts, and executables.
- XDR provides behavioral monitoring and response across endpoints, networks, and cloud environments.

Leading CDR Vendors

Vendor		Product Suite	Notes
Sasa Software		GateScanner	Strong in ICS/OT, healthcare, supports API
Glasswall		Glasswall CDR	API-first, on-prem/cloud
Deep Secure		Content Threat Removal	UK government/military focus
ReSec		ReSecure Platform	Advanced zero-day protection
ODIX		FileWall, CDR Vault	Microsoft 365 integration
Fortinet		FortiMail CDR	CDR built into secure email gateway

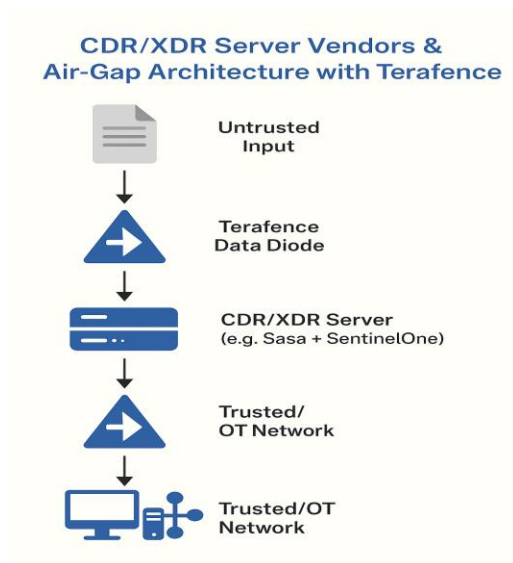
Leading XDR Vendors

Vendor	Product	Notes
CrowdStrike	Falcon XDR	AI-powered, endpoint-centric
SentinelOne	Singularity XDR	Offline-capable, autonomous AI
Microsoft	Defender XDR	Native to Microsoft ecosystem
Palo Alto Networks	Cortex XDR	Tight integration with firewall & cloud
Trend Micro	Vision One	Multi-layered telemetry correlation
Sophos	Sophos XDR	Unified endpoint + firewall

Recommended Architecture with Terafence

The most secure model involves two Terafence data diodes:

- One before the CDR/XDR server to ingest untrusted data safely
- One after the CDR/XDR to deliver sanitized files into the trusted network



This ensures:

- Unidirectional data flow
- Zero backchannel or callback risk
- Total separation of external and internal trust zones

An example of a recommended stack:

Terafence (Front) → Sasa GateScanner → SentinelOne → Terafence (Back) → OT Network

Summary

By combining CDR and XDR technologies with Terafence's hardware data diode, organizations can protect even the most sensitive networks from zero-days, ransomware, and lateral threats. The physical enforcement of one-way communication ensures air-gap-level security in real-time data environments.

For additional information contact: Juda Slomovich, Head of US expansion USA

Juda@terafence.com www.Terafence.com