ITF ROUNDTABLE · CLYDE & CO · 3 JUNE 2026

Future-Proofing Enterprise Trust Against Smart Threats

The data layer is the new battleground.
CTERA is how you defend it.

Jon Arnold

Senior Sales Director, Northern Europe | CTERA Networks

Alongside:

Richard Meeus
Akamai

Nick Gibbons
Clyde & Co

THE REALITY — 2026

AI hasn't invented new attacks. It has made yours much less defendable with existing tools.

$6.08M

Average FS breach cost
(IBM Cost of a Data Breach 2024)

29 min

Average attacker breakout time —
down 65% YoY (CrowdStrike GTR 2026)

24 days

Average ransomware recovery
time across industries (Sophos 2025)

One intrusion in 2025: exfiltration began within 4 minutes of access. Your perimeter didn't fail. Your data governance did.

WHY TRADITIONAL SECURITY MISSES THIS

Traditional tools protect systems. AI attacks target data.

No File-Layer Visibility

Firewalls and EDR tools see network traffic and process behaviour. They cannot see what files exist, who owns them, or whether permissions make sense. An AI enumeration attack is invisible to them.

Permissions Are Unchecked

Inherited ACLs, over-permissioned service accounts and broken permission chains are the attacker's first target. No traditional tool audits these continuously.

Unclassified Data = Blind Spot

If you don't know what sensitive data you hold or where it lives, you can't protect it. AI-driven classification of your file estate is not optional — it's foundational.

Backup ≠ Resilience

Ransomware now targets backup infrastructure first. Traditional backup solutions restored from yesterday's copy take days. That's 24 days average downtime industry-wide (Sophos 2025) — and weeks more to full containment.

We bring intelligence to your data. Not your data to someone else's cloud.

CTERA is a Global File System — unifying on-premises, remote and cloud file storage into a single governed, zero-trust platform with AI-powered intelligence across the entire estate. 50,000+ locations worldwide. 4× GigaOm Radar Leader.

CTERA Search

Find anything across your entire file estate in seconds — with permissions enforced on every result.

CTERA Classify

AI-driven classification at scale. DORA, FCA, GDPR — compliance becomes infrastructure, not a project.

CTERA Experts

Governed AI assistant. Answers from authorised data only. Source-cited. Fully audit-logged.

If you can't find it, you can't protect it.
If you can't classify it, you can't govern it.

CTERA Search

Scenario: Regulator calls at 9am requesting all documentation on a specific class of business across your syndicate.

Legacy approach: three-day fire drill, four teams.

CTERA Search: one query, two minutes, fully audited — with ACLs enforced on every result.

CTERA Classify

DORA Art. 9	ICT data mapping — auto-generated audit trail
FCA / PRA	Operational resilience — data location & sensitivity mapped
GDPR Art. 30	Records of processing — generated automatically
Lloyd's MS11	Data quality standards — addressed at classification

Not ChatGPT on your file server. Something your CISO and regulator can stand behind.

NOT THIS

- An open LLM with access to all your data
- A tool that ignores your permissions model
- Answers without sources or audit trail

THIS

- Permission-enforced — authorised data only
- Source-cited — every answer links to the file
- Fully audit-logged — CISO and regulator ready

Lloyd's use cases: Underwriting — query a decade of loss experience, source-cited, in 30 seconds · Claims — surface precedent matching current fact pattern · Compliance — which contracts reference a sanctioned entity?

RANSOMWARE RESILIENCE — THE RECOVERY GAP

The attacker's business model depends on recovery being painful.

Without CTERA

24 days

average ransomware downtime, all sectors (Sophos 2025)

With CTERA

< 15 min

point-in-time recovery, immutable snapshots

Immutable snapshots

Every file version stored in a format ransomware cannot encrypt or delete — even with admin credentials.

Anomaly detection

Monitors for mass encryption patterns in real time. Alert before the damage is complete.

Air-gapped cloud copy

Cloud replica isolated from on-prem estate. Ransomware cannot reach it.

Three things to take away from this table.

1. Your file estate is the target. Govern it before an AI maps it for the attacker.

2. DORA, FCA and GDPR already require what CTERA provides — classification, audit trails, data mapping. This is not a new cost; it's the infrastructure your obligations demand.

3. Safe AI adoption starts with a governed data estate. You cannot deploy AI responsibly on top of an unclassified file share.

Interested in a governed file estate assessment? jona@ctera.com mobile 07795976735| ctera.com