TRACE3

RESILIENCE

Clients stopped asking if it will happen.

Now it's how fast to recovery.

Attackers now target the backups and identity recovery depends upon - and autonomous AI agents widen the blast radius. Resilience, mapped to NIST CSF, lets you anticipate, absorb, adapt, and recover.

NIST CSF 2.0

Recover clean

Isolated Recovery Environments validate restore before you trust it.

Identity first

Restore trust, clean permissions, and rotate credentials after an incident.

Battle tested

Peacetime preparation: simulation exercises and recovery testing prove readiness.

From Prevention to Recovery

Then: Fight the fire	Prevent	→	Detect	→	Contain	
Now: Recover the business	Isolate	→	Validate	→	Recover	→ Re-secure

THE GAP

- Cloud, hybrid, and M365 tie on-prem, SaaS, and shared identity that fail together.
- Attackers hit the same environment repeatedly, targeting backups and identity.
- Few teams can prove a clean restore, or safely halt a rogue AI agent.

WHAT IT TAKES

- Isolated Recovery Environments and Resilient Recovery Assessments at the core.
- Agentic AI resiliency: scoped agent identity, approval gates, and tested rollback.
- Simulation exercises and validated recovery testing that prove readiness.

The Trace3 Path

1	2	3	4	5
Assess	**Design**	**Isolate**	**Validate**	**Manage**
Rapid resilience gap review	Target model and roadmap	Recovery environments	Simulation and testing	24/7 managed resilience

© Trace3 2026