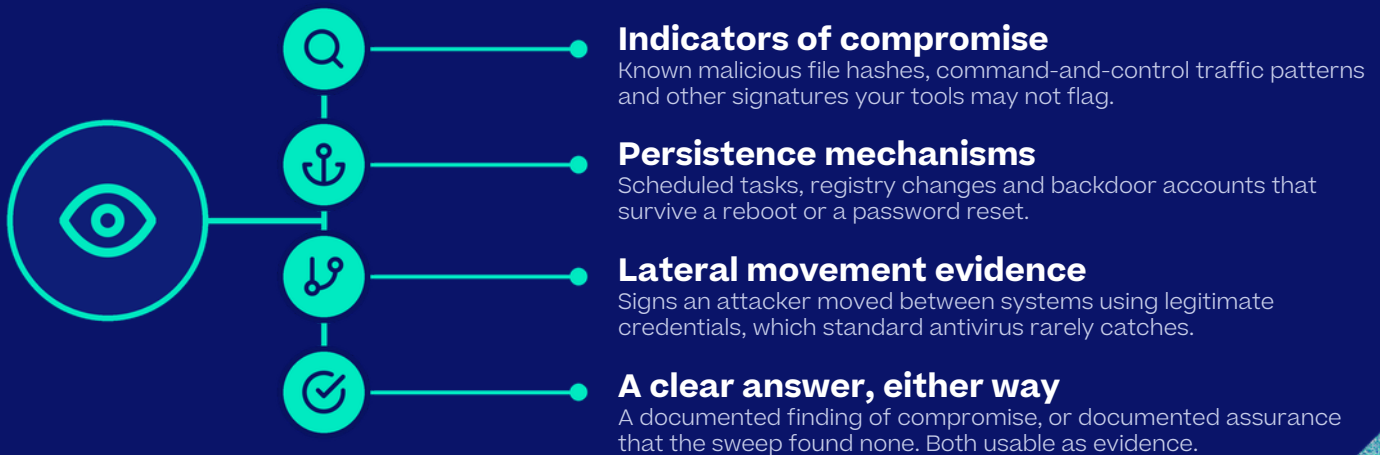


COMPROMISE ASSESSMENT

A point-in-time forensic sweep for undetected compromise.

Most breaches sit undetected for months. This forensic sweep covers endpoints, servers, network traffic and identity logs, for indicators of compromise, persistence and lateral movement your tools missed. It answers one question: is someone already inside?

FIND OUT IF YOU'RE ALREADY COMPROMISED.



WHY DIGITALERA

Certified forensics

Chain-of-custody handling throughout the sweep.

3 tiers by urgency

Rapid, Standard and Extended depth, sized to scope.

Before an incident

Runs when no incident is confirmed yet, just reason to check.

Fixed quote

A fixed quote based on tier and environment size.

WHAT YOU CAN EXPECT

- Evidence of compromise, or documented assurance of none
- Hidden persistence and lateral movement surfaced
- Assurance before an acquisition or system migration
- Documentation for cyber insurers and client contracts
- Written findings usable as evidence

WHAT YOU RECEIVE

- ✓ Written forensic findings
- ✓ Indicator-of-compromise review
- ✓ Documented assurance or finding
- ✓ Containment guidance

How it's scoped

3 tiers: Rapid (core endpoints), Standard (full environment) and Extended (deep forensic review). Fixed quote.

Right fit if you suspect compromise but have no confirmed incident, are acquiring a company, or need a documented assessment.

Something else first if you have a confirmed incident (call the emergency line), or want to test defenses (Penetration Testing) or ongoing detection (MDR).



Talk to an expert

digitaleragroup.com/contact/compromise-assessment

Active incident? Certified responders answer 24/7, no retainer required.

CALL US: 1-786-621-8600