gruve

SOLUTION BRIEF

Compromise assessment

Enteprise-wide threat assurance with AI-driven validation.

01

Business problem

Most boards eventually ask the same question: have we been breached, and how do we know?

Despite years of investment in SIEMs, EDRs, and firewalls, hidden compromises remain common. CrowdStrike and Kroll both report that compromise assessments frequently uncover active or historic intrusions inside “secure” environments. Undetected dwell time directly drives breach cost: IBM’s 2025 study puts the global average breach cost at $4.44 million (and $10.22 million in the U.S.), with containment time the strongest cost factor.

Unlike vulnerability scans, compromise assessments search for evidence of intrusion—correlating signals across endpoints, identity systems, and cloud telemetry to reveal latent malware, insider activity, persistence mechanisms, or credential abuse. Without them, organizations face:

- Unverified exposure and long dwell time
- Regulatory risk under SEC, NYDFS, or GLBA
- Erosion of customer and investor confidence
- Inability to prove “clean status” for M&A or audit events

02

Why now

Hidden dwell time is the cost multiplier.
Average attacker dwell time is still about 204 days (IBM 2025). Proactive assessments shorten that window and materially reduce breach cost.

Regulatory deadlines have tightened.
The SEC's disclosure rule now requires a Form 8-K filing within four business days of determining material impact, forcing companies to produce verified facts, not suspicions.

M&A and executive assurance expectations are rising.
Boards and investors now expect documented proof of clean systems before closing transactions or certifying financials. (Kroll 2024)

Insider and credential misuse continue to climb.
The 2025 Ponemon/DTEX study shows insider risk programs averaging $17.4 M annually, emphasizing the need for assurance.

AI and automation finally enable scale.
What once took weeks of manual log review can now be done in days when AI correlation is paired with human DFIR validation.

03

Solution overview

Gruve's Compromise Assessment delivers verified, defensible answers to the questions leadership, legal, and audit teams need most: *Are we compromised? If not, how can we prove it? If yes, what must we fix first?*

Our service fuses AI-accelerated analytics with expert forensic review to identify hidden threats, insider misuse, or compromise evidence across enterprise telemetry.
It is not a vulnerability scan or MSSP hygiene check—it is a assurance service aligned to NIST SP 800-61 Rev. 3, MITRE ATT&CK, and U.S. disclosure standards.

Core elements:

- Automated ingestion of SIEM, firewall, cloud, and identity logs
- AI summarization to cluster anomalies and surface patterns
- Human validation by senior DFIR analysts for defensible results
- Framework mapping to MITRE ATT&CK and NIST for context and reproducibility
- Executive-ready reporting for boards, counsel, and regulators

Gruve's solution items

Component	Description
Automated data ingestion	Secure connectors pull relevant logs from SIEMs, firewalls, cloud, and identity providers into Gruve's analysis pipeline.
AI-assisted correlation & summarization	Machine learning models cluster anomalies, summarize patterns, and flag deviations for analyst review.
Human forensic validation	Senior DFIR analysts validate AI findings, discard false positives, and craft defensible narratives.
Risk scoring & framework mapping	Findings mapped to MITRE ATT&CK and NIST 800-61 for clear operational context.
Executive reporting	Board- and counsel-ready summary detailing confirmed anomalies, business impact, and remediation roadmap.

04

Benefits of Gruve's solution

- **Enterprise visibility:** Unified analysis across SIEM, firewall, and SaaS telemetry closes detection gaps.
- **Speed & efficiency:** AI summarization reduces manual review time by up to 60 %, cutting breach lifecycle and cost.
- **Regulatory confidence:** Delivers factual basis for SEC and privacy disclosures.
- **Audit & insurance readiness:** Generates repeatable, evidence-based assurance reports for auditors and underwriters.
- **Predictable cost model:** Offered as a fixed-fee or subscription service to avoid unpredictable hourly investigations.

05

Compromise assessment service offerings

Service	Focus/scope	Core activities	Key deliverables	Ideal for
Enterprise compromise assessment (one-time)	Point-in-time review of enterprise telemetry (SIEM, firewall, identity, SaaS).	Data ingestion · AI correlation · Analyst validation · Remediation guidance · Yara/Sigma scans	Assurance report · Risk matrix · Executive summary	Security leadership · Internal audit · Board assurance
Enterprise compromise assessment + depth	Multi-domain, cross-network investigation including on-prem + cloud correlation and limited endpoint sampling.	Multi-source analysis · Behavioral clustering · Root-cause hypothesis · Counsel collaboration	Counsel-ready documentation · Prioritized remediation plan	Enterprises · Legal/ Compliance leaders
Continuous compromise monitoring (subscription)	Quarterly or monthly reassessments leveraging automated collectors.	Scheduled log pulls · Trend baselining · Delta analysis · Quarterly reporting	Ongoing "clean-bill-of-health" dashboard · Trend metrics	Regulated industries · Boards · Insurance-linked programs

06

Tabletop exercise offerings

Offering	Focus/scope	Core activities	Key deliverables	Ideal for
Core TTX (Annual)	Single realistic scenario (ransomware, data exfiltration, insider threat).	Scenario customization · 2–3 hr simulation · Facilitated discussion · AI summaries	After-action report · Gap analysis · Readiness certificate	Organizations meeting insurance or audit testing requirements.
Advanced Multi-Scenario TTX	Multi-team simulation integrating Legal, HR, and Comms.	Complex injects · Parallel decision tracks · Real-time capture	Executive debrief · Comprehensive readiness report · Improvement roadmap	Mid- to large-enterprises; regulated sectors.
Executive TTX (Board Simulation)	Strategic, board-level exercise focused on disclosure, investor communication, and continuity.	Role-playing for C-suite · AI-driven injects	Board-ready summary · Crisis communication playbook	Boards, GCs, and executive leadership teams.
Continuous Readiness Program (TTXaaS)	Quarterly rotating scenarios with improvement tracking.	Scheduled sessions · Trend analysis · Coaching	Year-over-year maturity metrics · Continuous improvement plan	Enterprises and insurers requiring recurring validation.

07

Competitors

Competitor	Market focus/strengths	Limitations/Gruve advantage
Mandiant (Google Cloud)	Market leader for compromise assessments, global threat intel integration.	High-cost, multi-week engagements; limited AI automation. Gruve offers faster, fixed-fee assessments with AI summarization + human validation.
CrowdStrike	"Compromise Assessment Services" using Falcon telemetry; fast triage for Falcon customers.	Requires Falcon deployment; less cross-platform log correlation. Gruve ingests any SIEM/firewall/identity telemetry.
Kroll / Stroz Friedberg	Well-known forensic assessments with legal defensibility.	Heavy enterprise pricing, slower cycle time. Gruve delivers mid-market speed with governance parity.
Blackpanda (APAC)	Productized, automation-driven assessments (IR-1, fixed-price).	Focused on Asia-Pacific market; limited U.S. legal alignment. Gruve brings U.S. governance + AI/human hybrid model.
Cynet / Arctic Wolf / ReliaQuest	MSSP compromise assessments tied to monitoring services.	Lacks independent forensic validation; focuses on alert detection. Gruve adds human forensic review + legal defensibility.

Gruve differentiators

- Hybrid automation + human validation (AI-accelerated forensics)
- Vendor-agnostic ingestion from any SIEM/firewall/log source
- NIST SP 800-61 / MITRE ATT&CK aligned methodology
- Fixed-fee, repeatable assurance model for U.S. enterprises

08

Use case / case study

At a glance

A U.S. financial-services firm preparing for a merger required validated assurance that no undetected compromise existed within its hybrid cloud and on-prem environment.

Key Results

- 72-hour turnaround from log ingestion to executive report.
- Two dormant misconfigurations and one misused service account identified and remediated.
- Cleared for disclosure under SEC guidance, avoiding merger delay.

About the client

Mid-sized financial institution operating multi-cloud infrastructure, regulated under GLBA and NYDFS cybersecurity rules.

Challenges

Fragmented telemetry across SIEM, firewall, and identity systems; internal teams lacked bandwidth for comprehensive correlation.

Solutions

- **Automated log ingestion** from SIEM, firewall, and identity providers.
- **AI summarization** to highlight anomalies; **human validation** to confirm findings.
- **Executive assurance reporting** aligned to regulatory frameworks.

Results & benefits

Delivered verified assurance within three days, enabling on-schedule disclosure and successful merger completion. Demonstrated Gruve's ability to merge automation and human expertise for defensible enterprise assurance.

Stop guessing—know whether you’re compromised today.

Gruve’s Compromise Assessment unifies your telemetry, applies AI correlation, and delivers human-validated, defensible results that satisfy leadership, auditors, and regulators.

Email: sales@gruve.ai
Web: www.gruve.ai