gruve

SOLUTION BRIEF

Proactive assurance sweep

Executive confidence before hidden risk becomes a reportable event

01

Business problem

Many organizations believe they are “fine” because controls are deployed, tickets are closed, and no one has declared an incident. In practice, that is often the most dangerous operating assumption. Hidden compromise activity, risky identity behavior, stale privileged access, SaaS misconfigurations, and policy violations can persist quietly between annual assessments, major technology changes, and day-to-day security operations. By the time leadership asks for assurance, the organization is often trying to prove a negative under time pressure.

The cost of getting that assumption wrong remains material. IBM reports the 2025 global average cost of a data breach at USD 4.44 million, while breaches involving data spread across multiple environments average USD 5.05 million. Google Cloud M-Trends 2025 reports that exploits were the most common initial infection vector in the investigations Mandiant handled in 2024, and that global median dwell time rose to 11 days. That means organizations can carry hidden exposure longer than leadership expects, especially across hybrid estates that combine endpoint, identity, SaaS, and cloud workflows (IBM; Google Cloud / Mandiant).

The challenge is not simply “finding malware.” CISOs, risk leaders, and boards increasingly need a fast, defensible answer to a broader question: is there evidence of hidden compromise, risky behavior, or meaningful control drift in the parts of the environment that matter most right now? That is especially important after cloud migrations, identity-platform changes, workforce reductions, acquisitions, leadership transitions, or investor and audit scrutiny. A point-in-time sweep that is risk-scoped, executive-readable, and evidence-backed closes that gap.

$4.44M

global average breach cost

$5.05M

average cost of breaches involving data spread across multiple environments

11 days

global median dwell time

02

Why now

Attackers are moving faster, and the margin for uncertainty is shrinking. IBM X-Force reported a 44% increase in attacks beginning with exploitation of public-facing applications in 2025, driven in part by weak authentication and AI-enabled vulnerability discovery. Palo Alto Networks Unit 42 reported that in the fastest cases it investigated, adversaries moved from initial access to data exfiltration in just 72 minutes - four times faster than the prior year. In other words, organizations no longer have the luxury of assuming they will “see it later” (IBM; Palo Alto Networks Unit 42).

The external pressure is also higher. Public companies still face the SEC requirement to disclose material cybersecurity incidents generally within four business days of determining materiality. Even when an organization is not yet at the point of disclosure, leaders increasingly need a fact-based narrative quickly enough to decide whether a suspected issue is routine noise, a contained exposure, or the start of a material event (SEC).

At the same time, the attack surface is widening. IBMs 2025 Cost of a Data Breach reporting highlights an AI oversight gap, noting that ungoverned AI systems are more likely to be breached and more costly when they are. NIST similarly warns that generative AI lowers barriers for offensive cyber activity while also expanding the attack surface through risks such as prompt injection and data poisoning. A modern assurance sweep therefore has to evaluate not just classic compromise indicators, but also whether rapid change, AI adoption, and cross-platform complexity have created quiet exposure paths leadership should understand now (IBM; NIST).

44%

increase in attacks beginning with exploitation of public-facing applications

72 minutes

attack timeline from initial access to data exfiltration

03

Solution overview

Gruve's Proactive Assurance Sweep is a fixed-scope compromise assessment built for moments when leadership needs evidence-backed confidence, not vague reassurance. The engagement reviews priority segments of the environment—typically a targeted mix of endpoint, identity, SaaS, cloud, administrative workflows, and critical user populations—to determine whether there are signs of hidden compromise, suspicious behavior, control drift, or policy violations that merit remediation or escalation.

This is not a generic vulnerability scan and not a full incident response activation. It is a defensible "current-state" review tailored to the organizations highest-concern assets, business changes, and decision timeline. Gruve combines threat-informed review methods, cross-source evidence correlation, and AI-teammate acceleration for orientation, clustering, and narrative drafting; however, every substantive finding is validated by investigators, and all conclusions remain expert-led and evidence-backed.

The result is a concise, leadership-ready view of whether the organization appears clean, where material risk may be hiding, what needs to be remediated first, and whether any issue should be escalated into a broader response, forensic, or legal track.

04

Gruve’s solution items

Gruve's solution items	Description
Risk-scoped environment review	Focuses the sweep on the users, systems, identities, SaaS platforms, cloud control planes, and administrative workflows that matter most to the business decision at hand.
Evidence-driven compromise and drift analysis	Looks for signs of hidden compromise, risky access patterns, suspicious changes, and material security drift across priority data sources rather than relying on a single telemetry view.
AI-teammate correlation and prioritization	Uses AI to accelerate summarization, clustering, and cross-source pivoting so investigators can surface the highest-value anomalies faster, while validating every substantive finding before it informs the report.
Executive assurance reporting	Translates technical observations into a plain-language current-state narrative leadership can use for board updates, audit conversations, risk decisions, or post-change validation.
Remediation and escalation guidance	Provides a prioritized action path that distinguishes between routine hygiene gaps, meaningful exposure, and issues that warrant a broader compromise assessment or incident response escalation.

05

Benefits

Benefits of Gruve's solution	Description
Faster confidence in current state	Gives leaders a grounded answer to whether priority parts of the environment appear sound, materially exposed, or in need of deeper investigation.
Lower surprise risk after change	Surfaces compromise indicators, control drift, and risky behaviors that often emerge after mergers, migrations, layoffs, major deployments, or identity changes.
Clearer prioritization for remediation	Converts a broad universe of possible issues into a smaller, executive-meaningful set of actions tied to real business risk.
Reduced overreaction and underreaction	Helps organizations avoid both false comfort and unnecessary incident activation by grounding decisions in evidence rather than intuition.
A credible assurance narrative	Creates a board-, audit-, or leadership-ready summary that explains what was reviewed, what was found, and what the organization should do next.

06

Distinct service offerings

Tiers	Focus / scope	Core activities	Key deliverables	Target audience
Event-triggered assurance sweep	A rapid review after a specific risk event such as a migration, workforce action, tooling change, or suspicious activity wave.	Targeted scoping · priority-source review · anomaly validation · leadership briefing	Current-state assurance report · priority findings · remediation actions · escalation recommendation	CISOs · security leaders · risk owners
Leadership / board assurance sweep	An executive-oriented compromise sweep used before a board update, audit checkpoint, financing event, or external diligence milestone.	Risk-focused review · executive narrative development · evidence correlation · reporting support	Board-ready summary · detailed appendix · risk matrix · next-step guidance	Executives · boards · audit and risk functions
Sensitive-environment assurance sweep	A focused validation of high-value users, crown-jewel systems, or regulated workflows where hidden exposure carries outsized business impact.	High-value asset review · privileged access analysis · SaaS and identity checks · defensible documentation	Sensitive-environment findings brief · prioritized corrective actions · optional follow-on plan	Security leadership · legal and compliance · business-unit leaders

07

Competitors

Competitor	Market focus / strengths	Limitations / Differentiation opportunity for Gruve
Mandiant / Google Cloud	Well-known compromise assessment and incident response capabilities backed by frontline threat intelligence and broad enterprise credibility.	Strong broad-market option, but typically oriented to larger response programs. Gruve is differentiated when the client wants a fast, risk-scoped assurance sweep with tighter executive narrative, change-event sensitivity, and AI-assisted but human-validated review.
CrowdStrike Services	Established compromise assessment services with strong Falcon-based telemetry and rapid endpoint visibility.	Highly effective where Falcon coverage is already mature, but more dependent on platform telemetry and less tailored to a business-driven assurance question spanning endpoint, identity, SaaS, and high-sensitivity stakeholder reporting.
Kroll / advisory-led cyber diligence firms	Strong legal, diligence, and cyber-risk posture support for transactions and high-scrutiny environments.	Often oriented toward broader diligence or post-breach workflows. Gruve provides a more operationally nimble current-state sweep with a tighter bridge between compromise validation, executive reporting, and practical remediation.
Internal SOC / MDR teams	Close to the environment and able to pull existing telemetry quickly.	Internal teams often optimize for alerts and ongoing operations, not for a discrete, evidence-backed assurance engagement framed around leadership questions and current-state confidence.
Tool-only exposure management vendors	Useful for surfacing misconfigurations, attack-path issues, and hygiene findings at scale.	They identify findings, but they do not deliver human judgment on whether anomalies represent hidden compromise, meaningful business risk, or the need for escalation into DFIR or legal processes.

08

Gruve differentiators

- **Purpose-built to answer a business assurance question**, not just to produce another list of technical findings.
- **Human-validated, AI-teammate accelerated workflow** that compresses time to facts without letting AI make conclusions.
- **Designed for hybrid environments** where the answer lives across endpoint, identity, SaaS, and administrative activity.
- **Delivers an executive-readable narrative** and a technical appendix in the same engagement.
- **Fits naturally** before incident response, board reporting, M&A diligence, or broader resilience planning.

09

Case study

A private-equity backed software company had just completed an identity-platform consolidation, a workforce reduction, and a series of privileged-access changes ahead of a board meeting. Security leadership did not have evidence of an active incident, but the CISO was not comfortable telling the board the environment was “clean” without a defensible current-state review. Gruve was engaged to perform a Proactive Assurance Sweep across priority identities, high-value SaaS administrators, cloud control-plane activity, and a targeted set of executive and engineering endpoints.

Key results

- Confirmed no evidence of active hands-on-keyboard compromise across the scoped environment at the time of the assessment.
- Identified dormant privileged access and risky OAuth grant conditions that materially increased exposure but had not yet triggered an incident.
- Surfaced logging and change-control gaps that would have slowed future investigations and remediation if left unaddressed.
- Delivered a board-ready assurance narrative and prioritized remediation plan within the clients reporting window.

About the client

Mid-market software platform with a lean internal security team, multiple SaaS administrative surfaces, and a mix of cloud-native and endpoint-heavy workflows.

Challenges

The clients concern was not a declared incident; it was uncertainty. Major changes had occurred quickly, and leadership wanted confidence that the combination of identity changes, administrator churn, and compressed operational timelines had not created hidden compromise or control drift. Existing tooling could show alerts and configuration snapshots, but not a single, evidence-backed answer to the broader question of current-state risk.

The board timeline added pressure. Security leadership needed to move quickly enough to support a near-term executive update, but not so quickly that the work degraded into an indiscriminate hunt for noise. The engagement had to be scoped intelligently, framed around real business risk, and delivered in a way that could support both technical follow-up and executive communication.

Solutions

- **Risk-scoped review design:** Gruve worked with the client to define a review boundary centered on privileged identities, administrative SaaS activity, recent access changes, and high-value users most relevant to the boards risk question.
- **Cross-source evidence correlation:** Investigators examined identity, SaaS, cloud, and endpoint signals together to differentiate harmless operational churn from suspicious or materially risky behavior patterns.
- **AI-assisted orientation and prioritization:** Gruve used AI teammates to accelerate the clustering of access changes, admin actions, and anomaly candidates, while investigators validated all substantive findings and decided what belonged in the assurance narrative.
- **Executive and technical reporting:** The final deliverable provided a plain-language conclusion on the current-state risk picture, supported by detailed technical observations and prioritized remediation actions.

Results and benefits

- Enabled the CISO to brief the board with confidence and without overclaiming certainty.
- Reduced real exposure by prioritizing cleanup of dormant privilege and weak governance conditions before they could be exploited.
- Improved future readiness by identifying logging and workflow gaps that would have made a later incident more expensive and harder to explain.
- Demonstrated the value of a compromise-assessment style review for change-driven assurance, not just post-incident validation.

Get an evidence-backed answer before quiet exposure becomes a crisis.

See how Gruve's Proactive Assurance Sweep helps leadership validate current-state risk, prioritize action, and brief stakeholders with confidence

Website: https://www.gruve.ai/

Email: contact@gruve.ai