gruve

SOLUTION BRIEF

Digital forensics for macOS

Defensible investigations powered by Gruve's AI-accelerated expertise.

01

Business problem

Organizations struggle to collect and interpret the right evidence from Apple devices fast enough for HR, legal, or incident response needs. Most internal playbooks and tools are still Windows-centric, which slows fact-finding on macOS and increases downstream costs and disclosure risk. Breach cost remains tightly linked to investigation/containment time (global average $4.44M in 2025; U.S. substantially higher) (Baker Donelson).

macOS requires different investigative workflows and specialized experience, and the lack of macOS-native expertise creates delays and uncertainty (Google Cloud).

02

Why now

- **Regulatory clock:** Public companies must disclose material cyber incidents on Form 8-K within four business days of determining materiality, forcing faster, fact-based narratives (SEC).
- **Insider & hybrid risk:** Insider-related program costs now average $17.4M annually, reinforcing the need for consistent, defensible DFIR on endpoints and SaaS (DTEX Systems)
- **macOS adoption outpacing DFIR maturity:** Mac usage continues to rise across engineering/executive roles while many orgs lack Apple-native investigation depth, creating blind spots that lengthen breach lifecycle and cost (Google Cloud).
- **AI readiness:** Automation and summarization now materially shorten analysis cycles when paired with expert validation; helping reduce overall breach lifecycle (Baker Donelson).

03

Solution overview

Gruve's Digital Forensics for macOS delivers defensible, AI-teammate accelerated investigations that stand up to legal, regulatory, and executive scrutiny, while also powering faster incident response (root-cause analysis, impact verification). We combine Apple-native acquisition/preservation, AI-assisted correlation and summarization, and human-led validation aligned with NIST SP 800-61 Rev.3 and ISO/IEC 27037 principles. NIST Publications,ISO

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
Apple-native acquisition & preservation	Secure collections (including imaging when appropriate) built for macOS; chain-of-custody to support HR, legal, and eDiscovery (left-of-EDRM-aligned).
AI-teammate evidence triage	Summarization and correlation across endpoint/SaaS/identity data to surface anomalies faster; experts review and validate all findings.
Executive & legal reporting	Plain-language briefs with forensic appendix that support disclosure decisions and regulatory reviews.
Continuous feedback loop	Forensic findings feed directly into incident response workflows (containment, eradication, lessons learned) per NIST SP 800-61 Rev.3.

04

Benefits of Gruve's solution

Defensible outcomes: Our investigation lifecycle is grounded in industry-recognized standards (e.g., NIST SP 800-61 Rev. 3, EDRM Model) and built for audit, legal and regulatory scrutiny. Every case includes a documented chain of custody when applicable, reproducible workflows, and executive-ready reporting.

Faster time to facts: We incorporate automation and AI-teammates (e.g., log-summarization, IOC enrichment, and narrative drafting) into our forensic/IR workflows. These tools don't replace expert judgement; they amplify it, enabling our team to deliver high-quality investigations with consistency and defensibility.

Lower reactive spend: We speak the language of CISOs, GCs and HR: faster fact-finding, clearer impact, fewer surprises during disclosure or litigation, and ultimately, lower total incident cost. Our aim is not only to resolve an event but to give leadership confidence in what happened and what to do next.

macOS confidence: Our team brings over a decade of investigations on Apple-endpoints across enterprise, legal and HR environments. This experience removes the typical learning curve many IR teams face on macOS platforms resulting in faster evidence collection, clearer timelines, and fewer blind spots for leadership.

05

Distinct service offering

Tiers	Focus/scope	Core activities	Key deliverables	Target audience
macOS Incident Response (Reactive)	Rapid investigation and containment of confirmed or suspected security incidents involving Apple devices.	Incident triage · Evidence preservation (including full-device imaging) · Root-cause and impact analysis · Containment guidance · Executive briefings	Verified incident scope · Root-cause documentation · Containment actions · SEC/board-ready summary	CISOs · Security leadership · Enterprises handling live incidents
macOS Digital Forensics (HR / Legal / Left-of-EDRM)	Court-defensible investigations supporting insider risk, offboarding, HR complaints, IP theft, or legal disputes.	Forensic imaging and preservation · Artifact and behavior correlation · AI-assisted triage with analyst validation · Legal collaboration	Counsel-ready report · Defensible evidence package · Chain-of-custody and audit trail · HR/legal decision support	HR · Legal counsel · Compliance and investigation teams
macOS Compromise Assessment (Proactive)	Fixed-scope forensic review of priority macOS and SaaS endpoints to identify dormant threats, risky behaviors, or policy violations.	Endpoint and SaaS telemetry review · IOC correlation · Risk scoring · AI summarization · Remediation recommendations	"Current-state" assurance report · Risk matrix and remediation plan · Executive summary · Optional validation follow-up	Security leadership · Risk and audit functions · M&A or due-diligence assessment

06

Competitors

Competitor	Market focus/strengths	Limitations/Gruve advantage
Mandiant / Google Cloud	Global IR reputation, heavy Windows/Linux focus, strong threat intel.	Minimal macOS artifact expertise; slower turnaround on Apple endpoints. Gruve is Apple-native with forensic automation and AI summarization.
CrowdStrike Falcon Forensics	Integrated endpoint visibility via Falcon; can perform forensic triage.	Dependent on deployed Falcon agent; not full-disk forensic imaging. Gruve provides court-defensible imaging and offline analysis.
Stroz Friedberg (Aon)	Longstanding eDiscovery & legal-support forensics leader.	eDiscovery focus, slower investigative response, limited AI acceleration. Gruve offers rapid macOS DFIR with integrated IR and legal deliverables.
FTI Consulting / Lighthouse / Epiq	Enterprise eDiscovery and legal forensics services.	Primarily litigation-focused; less active-incident expertise. Gruve unifies live IR + legal defensibility.
Cellebrite / Magnet Forensics	Forensic tools providers with macOS capabilities.	Product vendors rather than managed DFIR services. Gruve delivers expert-as-a-service outcomes, not just tooling.
Mendicant (Specialized IR)	Boutique IR firm with strong malware analysis.	Windows/Linux specialization; limited Apple expertise. Gruve fills the macOS niche with enterprise-grade scalability.

Gruve Differentiators

- 10+ years Apple forensic expertise
- Court-defensible imaging & chain-of-custody workflows
- AI-assisted correlation and reporting
- Dual focus: incident response + legal/HR investigations

07

Use case / case study

At a glance

A senior executive at a multinational enterprise triggered an insider-risk alert after downloading a large volume of internal files shortly after announcing their resignation. Human Resources' initial interview yielded inconclusive answers, prompting leadership to engage Gruve's Digital Forensics & Incident Response (DFIR) team. Leveraging Apple-native acquisition methods, AI-assisted correlation, and expert validation, Gruve conducted a discreet, defensible investigation that protected sensitive intellectual property and informed legal action, without operational disruption.

Key Results

- Behavioral correlation suggested screen recording of confidential designs using an external device.
- Legal validation confirmed Gruve's hypothesis, preventing multimillion-dollar IP loss.
- No litigation or disclosure required; matter resolved internally with HR and Legal. Reinforced leadership confidence in macOS-native, repeatable DFIR processes for insider-risk containment.

Challenges

The client's existing tools were designed for Windows and cloud investigations, offering little visibility into macOS activity. Leadership faced an urgent insider-risk scenario with limited direct evidence of data exfiltration.

What made the case particularly difficult was that the suspected behavior—screen recording of confidential designs—would leave no traditional forensic trace on the device. The investigation required expert correlation of indirect artifacts and behavioral patterns to form a defensible hypothesis that could guide legal action.

Solutions

- **macOS forensic imaging & preservation:** Full Apple-native acquisition conducted under ISO/IEC 27037 evidence handling standards to preserve integrity and admissibility.
- **Correlated artifact analysis:** AI-teammate assisted timeline correlation across endpoint and identity data revealed activity patterns consistent with screen recording from an external device.
- **Expert-driven hypothesis validation:** Gruve's investigators documented a high-confidence behavioral hypothesis, allowing counsel to compel independent third-party verification (through subpoena) that ultimately confirmed the misconduct.
- **Executive & legal reporting:** Delivered a concise, defensible narrative aligned with HR decision-making requirements, supported by a full evidentiary appendix.

Results & benefits

- Legal and HR obtained actionable, defensible evidence enabling internal containment and resolution.
- Prevented loss of trade secrets valued in the millions.
- Avoided disclosure, litigation, and operational impact.
- Demonstrated Gruve's ability to derive defensible conclusions from incomplete evidence under time pressure.

Accelerate truth-finding on Apple devices.

See how Gruve's Digital Forensics for macOS delivers defensible evidence and faster outcomes for legal, HR, and incident response teams.

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