druva

The DruAI Handbook:
Your Guide to Investigations, Operations & Agentic Actions

Explore how DruAI works, its data foundations, and how teams simplify daily security workflows with just a prompt.

Whitepaper
02/02/2026

v.1.1

Executive Summary

IT and security teams are under pressure from every direction. Attacks are faster and more identity-driven. Compliance requirements are expanding. Environments are more distributed across SaaS, cloud, endpoints, and data centers. At the same time, teams are expected to respond faster, prove what happened, and recover cleanly, often with fewer people and less time.

The challenge is not a lack of data. It is the effort required to connect it, interpret it, and turn it into answers that can be acted on with confidence.

DruAI is Druva's AI-powered intelligence layer, built directly into the Druva Data Security Cloud. Beyond simple assistance, it is Agentic Intelligence. Leveraging agentic memory, collaborating AI agents, and deep analysis agents, DruAI is a system engineered to *complete* complex, multi-day work. DruAI allows customers to ask plain-language questions, run deep investigations, surface hidden risks, and resolve issues across cyber incidents, compliance, identity, and operations. All without exporting data, stitching tools together, or manually correlating logs.

With the introduction of agentic memory, collaborating AI agents, and deep analysis agents, DruAI moves beyond simple assistance. It becomes a system that completes work on behalf of IT and security teams. Investigations that once took days can now be completed in minutes, with results delivered as clear, ready-to-share reports. Speed only matters if outcomes are reliable. DruAI improves accuracy by grounding answers in your tenant-specific environment, using Dru MetaGraph to understand "what's connected to what," and applying continuity and context across investigations. Instead of generating generic responses, DruAI correlates backup telemetry, identity activity, configurations, and historical signals so teams can act on conclusions with confidence.

This whitepaper explains how DruAI works, why it is secure by design, and the real-world use cases it enables for customers today.

Why AI Must Change How Cyber & IT Work Gets Done

Modern IT teams do not just fix problems. They are expected to explain them.

After a ransomware incident, teams must answer questions like:

- What happened?
- When did it start?
- Who was impacted?
- What data was affected?
- Are we restoring clean data?

During audits and compliance reviews, teams are asked:

- Are retention policies being followed?
- Who accessed sensitive data?
- Were backups protected and immutable?
- Can you prove it?

Operationally, teams spend hours chasing down issues:

- Why did this backup fail?
- Why is storage growing unexpectedly?
- Which policies are misconfigured?
- What should be fixed first?

In most organizations, answering these questions still requires manual effort. Analysts dig through logs. Administrators export reports. Teams correlate timestamps across tools. The work is slow, error-prone, and stressful. Compliance-related tasks alone average 9.5 hours per week, nearly 12 work weeks per year, largely due to manual evidence collection and reporting.

Conversational GenAI isn't Enough for Cyber and IT Work

Generic AI chat experiences can be helpful for explaining concepts, but cyber and IT work requires more than a well-written answer. Real investigations are multi-step, evidence-driven workflows that require continuity, correlation, and outputs that can be validated and shared.

Most AI experiences are also stateless—forgetting context when a session ends. That's a non-starter for enterprise operations, where consistency and environmental context are everything.

Agentic AI changes the model from "ask a question, get a response" to "delegate a workflow, receive an outcome." In cyber and IT operations, this matters because agentic AI can:

- Correlate evidence across systems and timelines (not just summarize a single input)
- Maintain continuity across investigations so teams don't restart from zero
- Translate complex findings into structured, ready-to-share reports that reduce rework
- Provide guided next steps that move teams toward resolution instead of leaving them to piece together the process
- Improve triage accuracy by incorporating broader context, reducing false leads and phantom misconfiguration hunts

What Is DruAI?

DruAI is an AI-driven intelligence layer embedded into the Druva platform. It allows customers to interact with their data using natural language and receive accurate, contextual answers grounded in their own environment.

Unlike generic AI tools, DruAI is purpose-built for cyber resilience and data protection. It understands backups, identities, policies, configurations, activity, and recovery workflows.

At its core, DruAI is powered by **Dru MetaGraph**, Druva's tenant-specific, graph-based foundation that maps relationships across:

- Users and identities
- Devices and workloads
- Backups and snapshots
- Policies and configurations
- Activity, changes, and anomalies
- Historical context over time

This graph provides the "map" of your environment. DruAI's agents use that map to reason, investigate, and act with context and continuity.

Productivity & Accuracy: From Answers to Outcomes

DruAI is built to compress multi-step cyber and IT work into outcomes—without sacrificing confidence. It improves productivity by completing the tasks that typically consume the most time: evidence collection, correlation across systems, and turning findings into a report that can be shared. It improves accuracy by grounding conclusions in your tenant's environment and continuously learning what "normal" looks like over time.

How DruAI improves productivity:

- Delegates multi-step investigative work (and the reporting that comes with it) so teams spend less time stitching evidence together.
- Reduces time-to-answer for complex investigations from days to minutes by breaking work into steps, coordinating analysis, and synthesizing results into a finished output.
- Minimizes rework and follow-up questions by producing clear, ready-to-share summaries instead of partial answers.

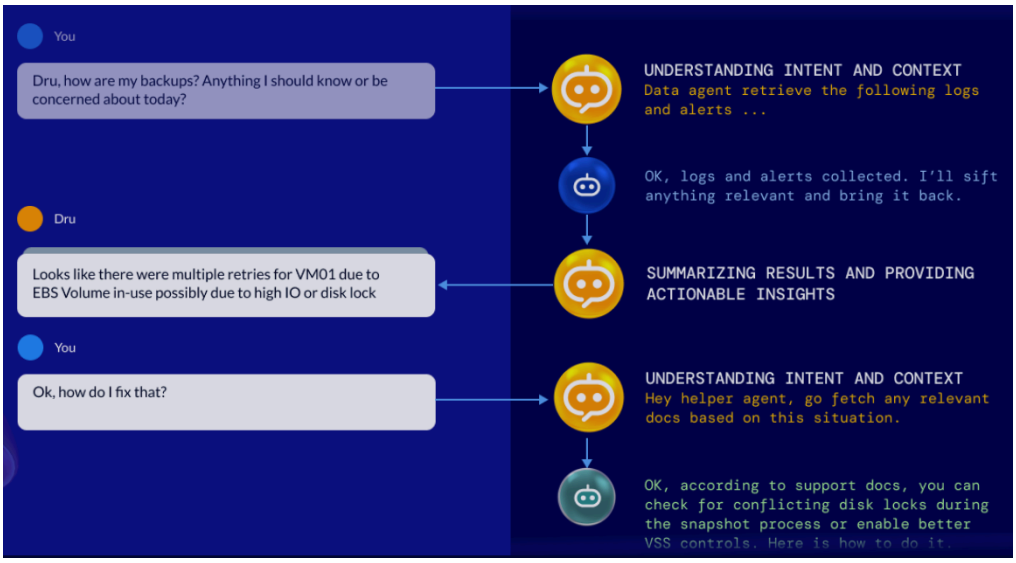
How DruAI improves accuracy:

- Correlates evidence across telemetry, identity signals, logs, configurations, and historical trends—reducing guesswork and missed relationships.
- Maintains continuity across interactions so investigations don't restart from zero every time a question is asked.

- Learns your organization's unique context and terminology over time (grounded in metadata), improving relevance and reducing ambiguity.

How DruAI Works. From Assistance to Agentic Intelligence

DruAI has evolved from answering questions to completing complex work. It does this through three core capabilities.



Agentic Memory

Agentic memory allows DruAI to maintain context across interactions. It understands what has already been investigated, what matters to your role, and how your environment behaves over time.

This means DruAI does not start from zero every time you ask a question. It builds on prior knowledge to deliver more relevant, personalized insights.

Collaborating AI Agents

Different tasks require different kinds of intelligence. DruAI uses multiple specialized agents that collaborate behind the scenes. One agent may analyze identity activity. Another may review backup metadata. A third may assess policy compliance.

These agents coordinate automatically, sharing findings and narrowing the investigation without human direction.

Agentic Workflows

Cyber resilience work is rarely a single question—it is a workflow. DruAI uses multiple collaborating agents to move from prompt → evidence → decision → next action, without forcing teams to manually gather, filter, and interpret signals across tools.

A typical agentic workflow looks like this:

- **Interpret intent**: Understand what the user is trying to accomplish (investigate, validate, explain, or resolve).
- **Gather evidence**: Pull relevant signals across backup metadata, identity activity, configurations, anomalies, and historical context.
- **Correlate and reason**: Connect findings across systems and timelines to isolate root cause and blast radius.
- **Deliver outcomes**: Produce a structured summary with conclusions, supporting evidence, and recommended next steps.
- **Carry context forward**: Retain continuity so follow-up questions build on what's already known about the environment and investigation.

Deep Analysis Agents

Deep Analysis Agents are designed for extended, multi-step investigations. They:

- Break complex questions into logical steps
- Query telemetry, logs, identity data, configurations, and historical signals
- Correlate findings across systems and timelines
- Analyze results over time, not just at a point in time
- Produce clear, structured outputs and summaries

Deep investigations don't always fit into an interactive back-and-forth. Teams can trigger deep analysis, step away, and receive an emailed synthesized report when it's complete. For teams juggling active incidents, this changes the work pattern from "I'll get to that later" to "the

work is already done." Investigations that previously took 2 to 3 days can now be completed in as little as minutes, with results formatted for direct use by security, compliance, or operations teams.

Personalized Intelligence

As DruAI learns what matters to your organization and your role, it can tailor the experience without compromising permissions or privacy. Personalized Intelligence adapts dashboards, responses, and reports based on whether you're an IT admin, SOC analyst, or compliance officer—and can learn preferences over time, such as:

- How you like reports formatted (high-level summaries vs. detailed evidence, historical comparisons, trends)
- What areas you commonly investigate
- Which follow-up actions you typically take

This reduces "blank page syndrome." Instead of starting from scratch, teams get context-aware starter prompts and directed flows that reflect what's most relevant now—accelerating the path from alert → understanding → decision.

Security & Trust. Why DruAI Is Safe to Use

AI is only valuable if it is trusted. DruAI is designed to be secure by default.

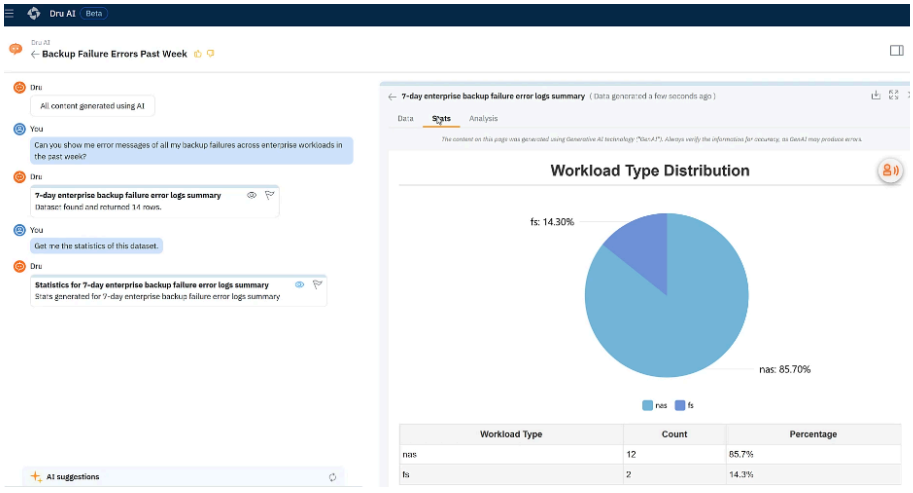
Key principles include:

- **Tenant isolation.** Each customer's data and intelligence are isolated. DruAI operates within the customer's tenant context only.
- **No data training leakage.** Customer data is not used to train public or shared models.
- **Role-aware responses.** DruAI respects access controls and permissions. Users only see what they are authorized to see.
- **Auditability.** Actions, findings, and outputs are traceable and auditable.
- **Built on Druva's platform.** DruAI leverages the same secure, immutable, and compliant architecture that protects customer data.

Customers can use DruAI confidently in regulated, security-sensitive environments.

Key Use Cases Enabled by DruAI

Cyber Investigations



The challenge

Threat investigations often start with a simple question and spiral into days of work. Teams must collect evidence, correlate events, and build a narrative that explains what happened and why.

How DruAI helps

With DruAI, teams can start investigations using plain-language questions:

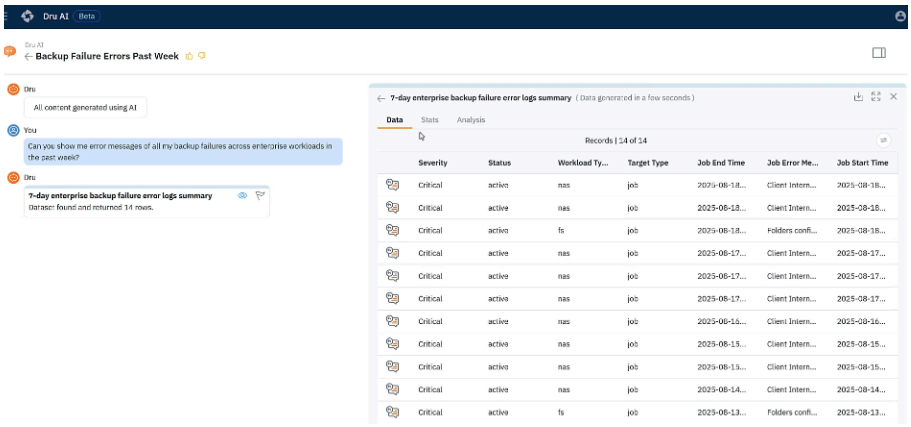
- "When did this ransomware activity begin?"
- "Which users and devices were involved?"
- "What data was accessed or modified?"
- "Which backups are clean?"

DruAI connects identity activity, backup telemetry, anomalies, and configuration changes into a single investigation. Deep Analysis Agents trace timelines, identify blast radius, and surface relationships that would otherwise be missed.

Outcome

Teams receive a clear, end-to-end investigation summary. No log digging. No manual correlation. No guesswork.

Lifecycle & Compliance Management



The challenge

Compliance risks often hide in plain sight. Retention gaps, orphaned data, over-privileged users, and misaligned policies are difficult to detect manually and even harder to fix consistently.

How DruAI helps

DruAI allows teams to ask questions like:

- "Where are we out of compliance with retention policies?"
- "Do any unauthorized users have access to sensitive data?"
- "Are there backups that violate regulatory requirements?"

DruAI surfaces hidden risks in real time and guides users through corrective actions. Instead of static reports, teams get living insights tied directly to their environment.

Outcome

Reduced audit preparation time, fewer compliance surprises, and continuous confidence in data governance.

Insights & Diagnostics

The challenge

Operational issues are often discovered after something fails. Teams spend time hunting for root causes instead of resolving them.

How DruAI helps

DruAI shifts operations from reactive searching to a conversational health check:

- "Why did backups fail last night?"
- "What is driving storage growth?"
- "Which policies are misconfigured?"
- "What should I fix first?"

DruAI provides personalized summaries, trends, and console-ready views. It also delivers a clear plan of action, prioritized by impact.

Outcome

Faster resolution, less manual effort, and improved operational efficiency.

Troubleshooting & Customer Support

The challenge

Even simple issues can take time to resolve when teams must search documentation or open support cases.

How DruAI helps

DruAI provides intelligent, in-product assistance that anticipates user needs and guides them step by step. It understands the customer's configuration and environment, not just generic best practices. When escalation is required, DruAI ensures context is preserved so customers do not need to repeat themselves.

Outcome

Faster resolution, better user experience, and less friction with support.

Why This Matters Now

The nature of cyber and IT work has changed.

- Attacks are more identity-centric and harder to trace.
- Compliance demands proof, not promises.
- Environments are more complex and distributed.
- Teams are under pressure to do more with less.

Manual processes cannot keep up. Point tools cannot connect the dots. AI that only chats without context cannot complete the work.

DruAI addresses this moment by turning AI into a partner that investigates, analyzes, and delivers outcomes.

As Stephen Manley, CTO at Druva, explains:

"IT teams are drowning in evidence collection and manual reporting. This turns AI from a conversational assistant into a partner that completes work. We are enabling teams to delegate multi-day investigations to agents that finish in minutes and deliver a final report that can be immediately shared with security, compliance, or operations teams."

The Druva Advantage

DruAI is not an add-on. It is a natural extension of Druva's Data Security Cloud.

Because Druva already protects data across SaaS, cloud, endpoints, and data centers, DruAI has direct access to the signals that matter most. Combined with Dru MetaGraph, this creates a foundation that other AI tools cannot replicate. Customers turn investigation and operations work into outcomes, not just answers. When teams can delegate multi-step workflows to agents, they reduce manual correlation, improve accuracy through evidence-driven reasoning, and produce outputs that are ready to share and act on.

Customers benefit from:

- **Faster time-to-answer**: Investigations that used to take days can be completed in minutes, with a finished report for stakeholders.
- **Fewer handoffs and less rework**: Outputs are structured for direct use by security, compliance, and operations teams.
- **Higher-confidence decisions**: Conclusions are grounded in tenant-specific context and correlated evidence, not generic assumptions.

Conclusion

DruAI represents a shift in how cyber resilience and IT operations are executed.

- Instead of hunting for answers, teams ask questions.
- Instead of stitching tools together, intelligence is unified.
- Instead of spending days proving what happened, reports arrive in minutes.

By combining agentic memory, collaborating agents, deep analysis, and a graph-powered foundation, DruAI delivers a personalized experience that adapts to how you work.

For customers facing growing risk, rising complexity, and relentless pressure, DruAI is not just helpful. It is transformative.

Visit the DruAI page of the Druva site to learn more about our AI capabilities: https://www.druva.com/use-cases/ai

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com