



# AI Changed the Rules. Resilience Must Evolve.

Understanding the new risks of AI-Powered business and how to build AI Resilience.

## In This White Paper

- Executive Summary
- Why AI Resilience, Why Now?
- What Changes in the AI Era
- The AI Resilience Risk Landscape
- What Organizations Need for AI Resilience
- The Resilience Cloud: A Platform Built for the AI Era
- The Four Outcomes of AI Resilience
- Pillar One: Recover
- Pillar Two: Govern
- Pillar Three: Defend
- Pillar Four: Accelerate
- Dru Metagraph: The Intelligence Layer
- What Makes Druva Different
- A Practical Blueprint for Building AI Resilience
- Conclusion: AI Resilience Starts with Trust

# Executive Summary

AI fundamentally changes enterprise operations. AI agents, copilots, orchestration systems, and autonomous workflows access data, invoke APIs, modify configurations, update workflows, and execute actions across systems. This changes both the operating model and the threat model. Trusted systems can now initiate unintended actions at machine speed, while external threat actors use AI to automate credential abuse, API misuse, policy manipulation, and coordinated disruption.

At the same time, AI creates and depends on a new class of business-critical assets. Prompts, workflow logic, contextual memory, vector databases, reasoning history, agent definitions, generated artifacts, and governance relationships are becoming operational records. If these assets are deleted, corrupted, or disconnected from their trusted context, the impact extends beyond data loss. Organizations risk losing institutional knowledge, governance continuity, reliable decision support, and confidence in AI-enabled operations.

This creates a new enterprise requirement: **AI resilience**.

AI resilience is the ability to preserve the availability, trustworthiness, governance context, and recoverability of the systems, data, and operational knowledge that AI depends on. It requires organizations to protect AI-critical data and context, detect AI-driven or identity misuse threats, reconstruct what changed, reverse autonomous actions, and safely extend trusted intelligence into the AI ecosystems the business chooses.

Druva is uniquely positioned to help organizations meet this requirement. Through its fully managed, cloud-native SaaS platform, secure-by-design architecture, air-gapped and immutable protection, backup-derived metadata, governance relationships, identity-aware context, and recovery intelligence, **Druva provides a foundation for enhanced AI resilience at cloud scale**.

This white paper discusses:

- Why AI changes both enterprise operations and enterprise risk.
- The new AI-driven threats organizations must prepare for.
- The pillars of Druva's AI resilience strategy: Govern, Defend, Recover, and Accelerate.
- How Dru MetaGraph provides a unified operational foundation for trusted context, visibility, and recovery intelligence.
- Why Druva's cloud-native SaaS architecture is well suited for the speed, scale, and complexity of AI-enabled operations.

## Why AI Resilience, Why Now?

As one of the most significant technology shifts since the transition to cloud computing, AI is arriving at an even faster pace than cloud computing did. Microsoft Copilot is becoming the default interface for everyday work. Claude is embedded in software development, research, and knowledge work. Autonomous agents are beginning to execute multi-step business processes with limited human oversight. For most enterprises, AI is no longer experimental. It is operational.

AI is also creating a new generation of business-critical assets, including conversations, prompts, AI-generated content, enterprise knowledge, operational knowledge, and enterprise intellectual property.

AI changes both the operating model and the threat model. Organizations now depend on autonomous systems that act at machine speed, while attackers use AI to automate credential abuse, API misuse, and policy manipulation. A misconfigured agent can alter thousands of records in minutes. A compromised identity can trigger destructive actions across multiple SaaS platforms before a human notices. A poisoned retrieval pipeline can quietly shape every answer an enterprise AI assistant gives. None of this looks like a traditional security incident, but all of it can undermine the business.

What once unfolded over hours or days can now occur in seconds as AI agents make decisions and execute actions at machine speed. This is not simply a new cybersecurity problem. It is a structural change in how disruption originates and spreads. Traditional resilience assumed disruption came from external attackers, accidental deletion, or infrastructure failure. AI adds a

new source of disruption: trusted identities, autonomous agents, and approved automation acting in unexpected or unintended ways. Recovering from that requires more than restoring data. Organizations must understand what changed, determine what can be trusted, and restore trusted operations with confidence.

*Understanding AI Resilience starts with understanding how AI changes business itself.*

## What Changes in the AI Era

Traditional resilience programs were built to recover systems, applications, and files. AI-powered organizations must protect a broader operational foundation: the context, knowledge, and relationships that let intelligent systems operate reliably. The table below summarizes how each dimension of resilience shifts as AI becomes embedded in daily operations.

| Dimension           | Traditional Resilience                                | AI Resilience                                                                                                                                          |
|---------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating model     | Humans and applications follow predictable workflows. | AI assistants, copilots, and agents act across interconnected systems at machine speed.                                                                |
| Business assets     | Files, databases, applications, and infrastructure.   | Traditional data, AI-generated work, conversations, enterprise knowledge, project context, prompts, workflows, operational context, and vector stores. |
| Threat model        | External attackers, ransomware, accidental deletion.  | Agent overreach, compromised identities, context poisoning, machine-speed disruption.                                                                  |
| Foundation of trust | Trusted data                                          | Trusted data, trusted context, and restore trusted operational state with confidence.                                                                  |
| Recovery objective  | Restore systems to a known point in time.             | Determine what changed, what can be trusted, and restore trusted operational state with confidence.                                                    |
| Business outcome    | Resume operations after disruption.                   | Maintain trusted operations while confidently adopting AI at enterprise scale.                                                                         |

Trusted context is becoming as important as trusted data. Conversations, prompts, enterprise knowledge, workflows, and AI-generated content now form the operational context intelligent systems depend on. Protecting and recovering that operational context is becoming just as important as protecting the underlying data itself.

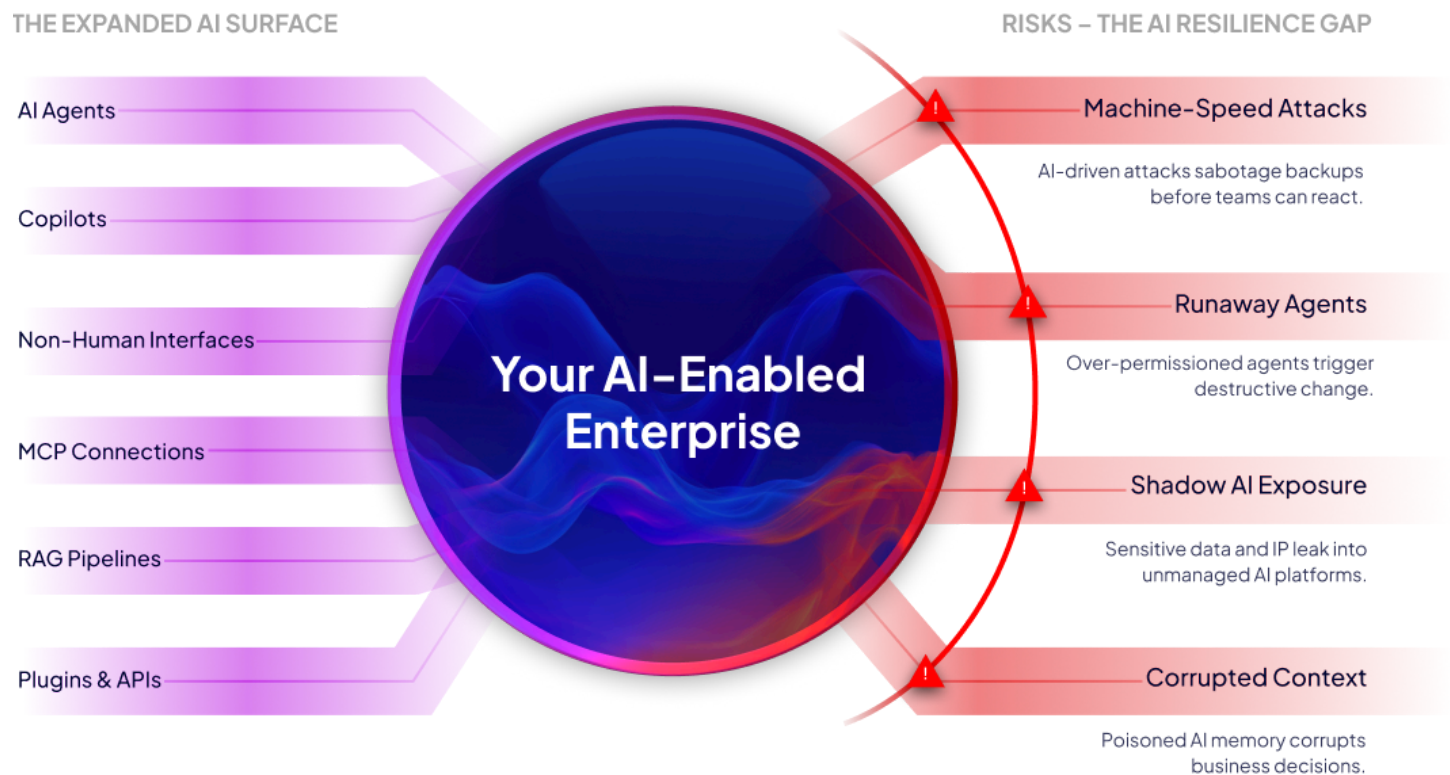
Understanding these changes is the first step toward building AI Resilience. The next step is understanding the risks they introduce.

# The AI Resilience Risk Landscape

AI fundamentally changes how operational risk develops, propagates, and impacts the business. Trusted assistants, copilots, and autonomous agents operate at machine speed, inherit enterprise identities, invoke APIs, and create new categories of business-critical knowledge. As a result, disruption spreads faster across systems, and with greater operational impact than traditional resilience models were designed to address.

## KEY INSIGHT

*AI changes both what organizations depend on and how disruption spreads.  
Resilience must evolve from protecting data to preserving trusted operational state.*



| Risk Area                                                                              | What Can Go Wrong                                                                                                                                                                               | What AI Resilience Requires                                                                       |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>AI-powered attacks</b>                                                              | Attackers use AI to automate reconnaissance, phishing, and credential abuse at machine speed.                                                                                                   | Earlier detection, clean recovery points, and faster response through recovery intelligence.      |
| <b>Compromised identities &amp; autonomous agents</b>                                  | Trusted accounts or agents inherit broad permissions that can unintentionally or maliciously alter data.                                                                                        | Understand identity relationships, monitor privileged activity, preserve trusted recovery points. |
| <b>AI-generated business records, enterprise knowledge &amp; intellectual property</b> | AI-generated business records, conversations, project context, enterprise knowledge, workflows, and intellectual property become business-critical but are lost, corrupted, or left ungoverned. | Protect, govern, and recover AI-generated work as first-class business records.                   |
| <b>Autonomous AI actions</b>                                                           | Trusted AI agents unintentionally modify systems, workflows, permissions, or business processes at machine speed.                                                                               | Understand what changed, validate recovery integrity, and recover with confidence.                |
| <b>RAG pipelines, vector stores &amp; contextual grounding</b>                         | Enterprise knowledge sources, RAG pipelines, vector stores, embeddings, or contextual grounding become corrupted, poisoned, or outdated, reducing AI reliability and trusted decision-making.   | Protect knowledge repositories and recover AI context alongside supporting data.                  |
| <b>Policy drift &amp; recovery sabotage</b>                                            | Retention, permissions, and backup configurations quietly drift without visibility.                                                                                                             | Continuously monitor configuration health and preserve governance continuity.                     |
| <b>Third-party AI ecosystem risk</b>                                                   | Multiple AI platforms create inconsistent governance and disconnected visibility.                                                                                                               | Extend consistent protection and recovery across every AI ecosystem in use.                       |

## What Organizations Need for AI Resilience

AI-powered businesses cannot rely on disconnected backup products or isolated security tools. The organizations that scale AI successfully will not necessarily have the most advanced models; they will be the ones that can confidently answer three questions:

- Can we trust our AI?
- Can we trust our data?
- Can we recover our business?

Answering yes to all three requires six foundational capabilities:

- **Trusted Data and Operational Context** — Protect and recover conversations, AI-generated work, enterprise knowledge, operational context, prompts, workflows, and vector stores alongside traditional data.
- **Recovery Intelligence** — Understand what changed, what can be trusted, and identify the right recovery point before restoring trusted operational state.

- **Continuous Recovery Readiness** — Visibility into backup health and configuration drift before disruption, not just during it.
- **Identity-Aware Operations** — Understand how identities, agents, permissions, and workloads interact to investigate and recover faster.
- **Trusted Governance** — Extend protection, governance, retention, legal hold, eDiscovery, federated search, compliance, and preservation to AI-generated work, ensuring business-critical knowledge remains trusted, discoverable, and recoverable.
- **Open AI Ecosystem Integration** — Extend trusted backup intelligence into the AI assistants, copilots, and agents employees already use, enabling trusted AI interactions grounded in recovery intelligence and operational context. The Resilience Cloud: A Platform Built for the AI Era

## CUSTOMER OUTCOME

*Rather than taking a reactive approach to disruptions, organizations that combine trusted data, operational context, and recovery intelligence into a single operating model are prepared to confidently adopt AI while remaining resilient to whatever comes next.*

## The Resilience Cloud: A Platform Built for the AI Era

Organizations don't need another point solution for AI. They need a resilient operational foundation that enables them to adopt AI confidently while protecting the business against disruption. **The Druva Resilience Cloud** is the cloud-native platform that delivers AI Resilience. By bringing protection, governance, recovery intelligence, and AI-powered operations together in a single cloud-native platform, it provides the trusted foundation organizations need to operate AI-powered businesses with confidence.



Most organizations have assembled resilience from multiple products, each solving a different problem. One protects workloads, while others govern data, detect threats, and power AI. As AI connects these domains, fragmented architectures create operational blind spots just when organizations need confidence the most.

Druva is a unified, cloud-native platform that integrates data protection, governance, and recovery intelligence. Instead of just securing data, it preserves the critical context needed to identify changes, verify trust, and reliably restore operations. By consolidating identities, permissions, and operational data, the Resilience Cloud builds a stable foundation for AI-driven business.

These capabilities work together to deliver the four outcomes of AI Resilience.

At the heart of the platform is **Dru MetaGraph**, the intelligence layer that transforms backup-derived metadata into trusted operational context by connecting identities, permissions, governance relationships, operational telemetry, and recovery history. This shared intelligence powers every outcome.

As AI assistants, agents, cloud workloads, and governance policies all contribute to an organization's operational state. Understanding those relationships transforms backup from stored data into trusted operational context and recovery intelligence. This enables organizations to restore trusted operations quickly and with confidence.

## The Four Outcomes of AI Resilience

AI Resilience is delivered through four business outcomes. Together, they help organizations protect AI-generated work, protect backups and recovery readiness, restore trusted operational state, and confidently adopt AI across the business.

| Outcome    | Business Challenge                                                                                                                                                                      | Business Outcome                                                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Recover    | AI-driven disruption can spread across systems before anyone understands what changed.                                                                                                  | Restore trusted operational state with confidence using recovery intelligence and identity awareness.                     |
| Govern     | AI is creating a new generation of business-critical knowledge organizations must protect.                                                                                              | Protect and govern AI-generated work, enterprise knowledge, and business records alongside traditional data.              |
| Defend     | AI-powered threats target backups, recovery infrastructure, identities, and resilience operations, while configuration drift and operational change silently reduce recovery readiness. | Protect backups and recovery infrastructure while continuously strengthening recovery readiness before disruption occurs. |
| Accelerate | Organizations want to adopt AI without compromising governance or recoverability.                                                                                                       | Extend trusted backup intelligence into the AI assistants, copilots, and agents the business already uses.                |

## Recover

### *Restore trusted operations with confidence.*

Recovery in the AI era is no longer about restoring the latest backup. AI assistants, agents, and automated workflows can modify data, permissions, configurations, and business processes across multiple systems simultaneously. Organizations must understand what changed, determine what can be trusted, and restore trusted operations with confidence.

Recover is the foundation of AI Resilience. Every other outcome depends on an organization's ability to confidently restore trusted operations after disruption.

- **Recovery intelligence** — Correlates identities, permissions, operational context, and recovery history to identify trusted recovery points.
- **Identity-aware recovery** — Accounts for how users, agents, and permissions interacted before disruption.
- **Trusted recovery validation** — Validate clean recovery points through isolated recovery operations before workloads return to production.
- **Cross-workload orchestration** — Restore interconnected SaaS, cloud, identity, AI, and data protection assets together to rebuild trusted operational state rather than isolated systems.

## CUSTOMER OUTCOME

*Organizations understand what changed, determine what can be trusted, and restore trusted operational state with confidence, recovering business operations, not simply data.*

## Govern

### **Protect and govern AI-generated work, enterprise knowledge, and business context.**

Organizations cannot govern, recover, or trust AI-created work unless it is first protected. Every conversation, prompt, project, and AI-generated report contributes to a company's institutional knowledge. Organizations must protect and govern this new generation of AI-created work with the same confidence they apply to traditional business records.

AI-created work now includes conversations, prompts, business records, project context, enterprise knowledge, generated content, workflows, and intellectual property.

- **Protection for AI-generated work** — Conversations, collaborative projects, AI-generated business records, and enterprise knowledge are protected alongside traditional workloads.
- **Governance and compliance** — Extend retention, legal hold, eDiscovery, federated search, compliance, and preservation to AI-generated work.
- **Apply consistent governance across AI ecosystems** — Protect and govern AI-created work consistently across Claude, Microsoft Copilot, and future AI platforms without creating isolated management silos.

### **Protect and Govern the New Record of Business**

Protect AI-generated business records, conversations, and enterprise knowledge while extending governance, discovery, and recovery to Microsoft Copilot.

### **Protect the AI Workspace**

Protect conversations, projects, generated content, and enterprise knowledge while extending governance, discovery, and recovery to Claude.

## CUSTOMER OUTCOME

*Organizations protect and govern AI-generated work, preserve enterprise knowledge and intellectual property, strengthen compliance, and ensure the AI-created information that powers the business remains trusted, recoverable, and discoverable.*

## Defend

### ***Protect backups from AI-powered threats and continuously improve backup reliability.***

As AI-powered attacks become more sophisticated, they target backups, recovery infrastructure, identities, and the resilience layer itself. Compromised identities, policy manipulation, configuration drift, and AI-assisted attacks quietly undermine an organization's ability to recover long before an incident occurs.

Reliable recovery depends on a protected resilience layer. Air-gapped and immutable backups, isolated recovery environments, hardened control planes, and AI-powered threat detection help ensure trusted recovery points remain secure, available, and ready when they're needed most.

But protection alone isn't enough. Recovery confidence must be continuously maintained. As environments evolve, backup jobs can succeed while protecting the wrong data. Policies can drift, and protection coverage can quietly degrade. Traditional monitoring provides visibility, but doesn't continuously improve backup reliability.

This is where AI-powered Site Reliability Engineering becomes essential. **The Dru SRE Agent** applies modern Site Reliability Engineering principles to backup resilience by continuously identifying issues, determining root causes, recommending corrective actions, and improving the operational reliability of the backup environment so organizations are always ready to recover.

- **Protect the Resilience Layer** — Air-gapped, immutable backups, isolated recovery environments, and hardened control plane protections help ensure recovery remains possible even during sophisticated AI-powered attacks.
- **Detect and Contain Threats** — AI-powered threat detection, anomaly detection, threat hunting, and managed detection and response identify risks before recoverability is compromised.
- **Continuously Improve Recovery Readiness** — Dru SRE Agent continuously identifies operational issues, explains root causes, recommends corrective actions, and improves backup reliability.
- **Actionable Recommendations** — Help administrators resolve issues faster through prioritized recommendations and continuous reliability improvements.

## KEY INSIGHT

*Protecting backups makes recovery possible. Continuously improving their reliability makes recovery trustworthy.*

## CUSTOMER OUTCOME

*Organizations protect backups from AI-powered threats, continuously improve backup reliability, and strengthen confidence that trusted recovery will succeed when disruption occurs.*

## Accelerate

### **Enable trusted AI adoption across the enterprise.**

Organizations now interact with enterprise software through AI assistants like Claude or Microsoft Copilot rather than traditional administrative interfaces. To provide meaningful recommendations, investigations, and operational guidance, these assistants need access to trusted backup intelligence, recovery context, and governance insights. Without that context, AI cannot answer critical resilience questions or support informed operational decisions.

Organizations shouldn't have to choose between adopting AI and maintaining resilience. As AI tools become the primary interface for enterprise software, resilience intelligence must be available wherever AI-powered work happens.

**Druva MCP** extends trusted backup intelligence from the Resilience Cloud into enterprise AI ecosystems, letting AI assistants securely access backup metadata, operational context, and recovery intelligence through governed interactions. It brings trusted resilience knowledge into the AI experiences employees already use.

### **Druva MCP**

Bring trusted backup intelligence into enterprise AI, with secure, governed access to backup metadata, operational context, and recovery insights.

### **Open AI Ecosystem Support**

Extend consistent resilience across Microsoft Copilot, Claude, and future enterprise AI platforms — with no added infrastructure.

- **Governed AI interactions** — Securely expose backup intelligence through existing identity and authorization controls.
- **Natural language resilience operations** — Enable investigations, reporting, recovery planning, and operational insights directly from AI assistants.
- **Cloud-native innovation** — Continuously extend capabilities without plugins, client upgrades, or additional infrastructure.

## CUSTOMER OUTCOME

*Organizations extend trusted backup intelligence into the AI assistants, copilots, and agents their employees already use, enabling AI-powered operations grounded in trusted data, operational context, and recovery intelligence.*

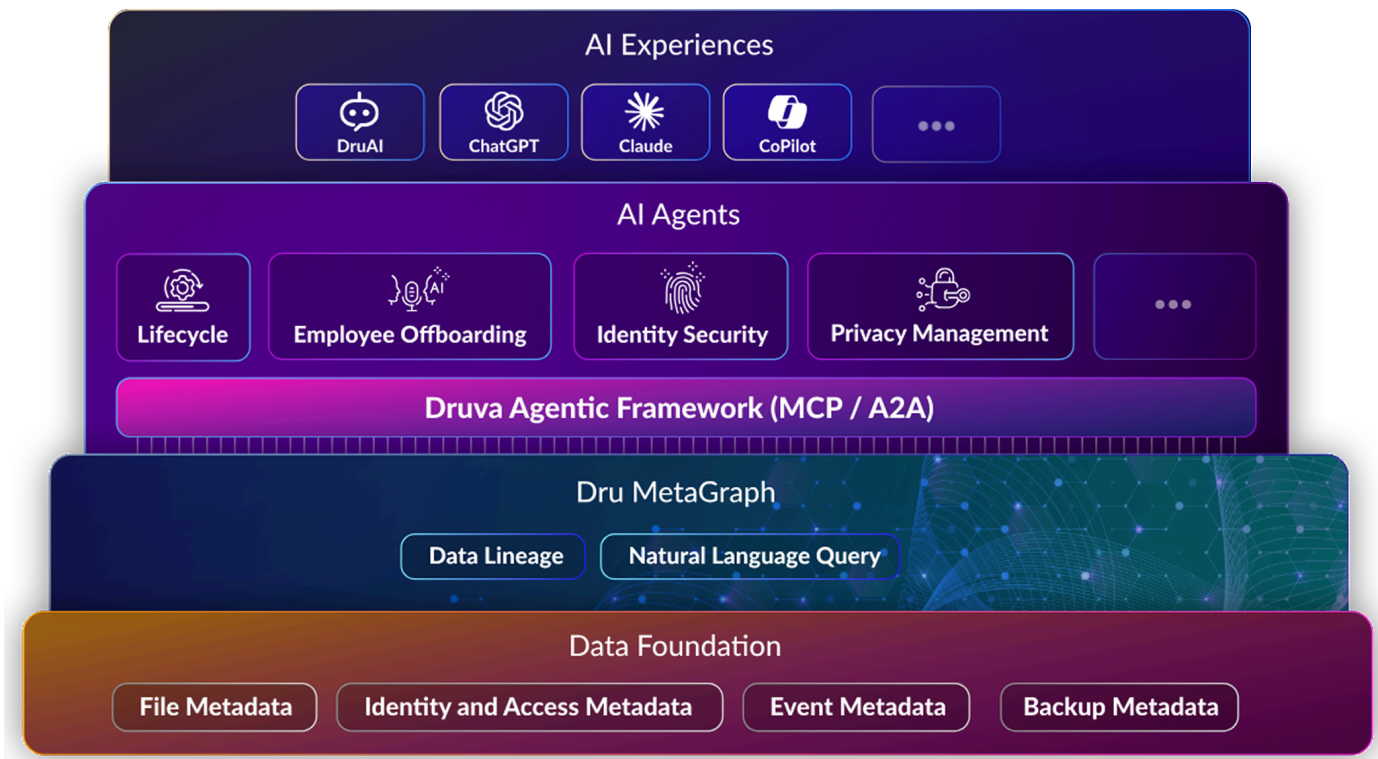
## Dru MetaGraph: The Intelligence Layer

### ***The intelligence behind every AI Resilience outcome.***

More than on protected data, AI Resilience depends on the intelligence to understand how identities, permissions, workloads, governance relationships, and recovery history connect to one another. During an incident, organizations rarely start with complete information: a compromised identity here, an unexpected configuration change there. Recovering confidently means understanding how these signals connect.

Dru MetaGraph is the intelligence layer that connects these relationships, turning isolated backup metadata into trusted operational context that supports every outcome the Resilience Cloud delivers.

Rather than building separate intelligence for recovery, governance, defense, and AI-powered operations, Dru MetaGraph provides a shared foundation that powers every AI Resilience outcome.



| Outcome    | How Dru MetaGraph Contributes                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------|
| Recover    | Correlates identities, permissions, operational context, and recovery history to identify trusted recovery points. |
| Govern     | Connects AI-created work, governance relationships, and enterprise knowledge to preserve trusted business records. |
| Defend     | Correlates operational telemetry and historical trends to strengthen backup reliability and recovery readiness.    |
| Accelerate | Extends trusted backup intelligence into AI assistants, copilots, and agents.                                      |

KEY INSIGHT

*AI Resilience isn't powered by data alone. It's powered by trusted operational context.*

## What Makes Druva Different

Most organizations have built resilience one product at a time. AI exposes the gaps between them. Recovering trusted operations now requires protection, governance, recovery intelligence, and operational context to work together as a single system. Druva takes a different approach. The Resilience Cloud unifies protection, governance, recovery intelligence, and AI-powered operations into a single cloud-native operating model for AI Resilience.

The result is a single platform for AI Resilience, rather than a collection of disconnected tools. Druva doesn't deliver separate products for recovery, governance, defense, and AI-powered operations. It delivers a unified AI Resilience operating model through its Resilience Cloud.

| Differentiator         | Why It Matters for AI Resilience                                                                               |
|------------------------|----------------------------------------------------------------------------------------------------------------|
| 100% Cloud-Native SaaS | Eliminates infrastructure management, so teams focus on resilience outcomes, not backup systems.               |
| Single Control Plane   | Consistent visibility and recovery across cloud, SaaS, endpoints, and AI-enabled workloads.                    |
| Recovery Intelligence  | Understand what changed, determine what can be trusted, and restore trusted operational state with confidence. |

|                                                |                                                                                                              |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Dru Metagraph</b>                           | Transforms backup-derived metadata into trusted operational context that powers every AI Resilience outcome. |
| <b>Continuous Recovery Readiness</b>           | Continuously improves backup reliability and recovery confidence before disruption occurs.                   |
| <b>Support the AI Ecosystem of Your Choice</b> | Extends trusted backup intelligence into the AI assistants, copilots, and agents organizations already use.  |

## A Practical Blueprint for Building AI Resilience

AI Resilience isn't achieved through a single deployment. It develops over time as organizations identify AI-created work, strengthen recovery readiness, build trusted operational context, and extend trusted backup intelligence into the AI ecosystem.

| Step                                               | Recommended Action                                                                                     | Business Outcome                                         |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>1. Identify AI-Critical Assets</b>              | Inventory AI-generated work, knowledge, prompts, and pipelines alongside traditional data.             | Visibility into the information AI depends on.           |
| <b>2. Protect and Govern AI Work</b>               | Apply consistent protection and governance across enterprise and AI-generated assets.                  | A trusted foundation for AI-powered operations.          |
| <b>3. Connect Operational Context</b>              | Connect identities, permissions, and recovery history to improve investigation.                        | Faster, better-informed incident response.               |
| <b>4. Strengthen Recovery Readiness</b>            | Continuously evaluate posture and reduce policy drift before disruption occurs.                        | Confidence that recovery will succeed.                   |
| <b>5. Recover with Confidence</b>                  | Validate trusted recovery points and restore trusted operations.                                       | Reduced uncertainty, faster continuity.                  |
| <b>6. Extend Trusted Backup Intelligence to AI</b> | Connect trusted backup intelligence to the AI assistants, copilots, and agents your teams already use. | Accelerate AI adoption with trusted operational context. |

# Conclusion: AI Resilience Is the New Foundation for Business

Every organization is becoming an AI-powered organization. The question is no longer whether AI will transform the business, but whether the business will be ready to recover, govern, defend, and confidently operate in that new reality.

AI is changing how work gets done. It also changes how disruption spreads.

Business continuity is no longer just about recovering systems. It's about recovering the context those systems depend on. Organizations must also preserve the conversations that capture institutional knowledge, the context that lets intelligent systems make reliable decisions, and the recovery intelligence that lets teams confidently restore operations after disruption. Together, these capabilities define **AI Resilience**.

AI Resilience is becoming foundational for every organization that intends to operate AI at scale.

*Recover, Govern, Defend, and Accelerate* work together to create AI Resilience. Organizations that combine them, delivered through a single cloud-native platform, gain the operational confidence to embrace AI at enterprise scale, rather than reacting to disruption after the fact.

The organizations that succeed in this era will do so much more than deploy AI tools quickly. They'll build the operational confidence to trust AI, knowing their business-critical information is protected, understanding what changed when disruption occurs, and continuously improving recovery readiness. **Druva's Resilience Cloud provides the operational foundation that enables AI Resilience.**

## EXECUTIVE TAKEAWAY

*AI changes how businesses operate. AI Resilience changes how businesses stay operational. By combining trusted data, operational context, recovery intelligence, and AI-powered innovation through the Resilience Cloud, organizations can confidently recover, govern, defend, and accelerate AI — while remaining resilient against whatever comes next.*

## Learn More

- Explore [the Resilience Cloud](#)
- Learn about [AI Resilience](#)
- [Microsoft Copilot Protection & Governance](#)
- [Claude Protection & Governance](#)
- [Dru SRE Agent](#)
- [Druva MCP](#)
- Visit [druva.com](#)

**druva** Sales: +1-800-375-0160 | [sales@druva.com](mailto: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](mailto:japan-sales@druva.com)  
Singapore: [asean-sales@druva.com](mailto:asean-sales@druva.com)  
Australia: [anz-sales@druva.com](mailto:anz-sales@druva.com)

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit [druva.com](#) and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).