

Druva Premium Security

Turn backups into proactive defense with automated monitoring, hunting, and recovery workflows.

Enhanced Detection, Forensics & Response

Recovery is hollow if it reintroduces the infection. Druva eliminates the operational panic of speculative recovery through a precise, forensic understanding of data risk. By unifying these critical insights with automated orchestration, our evidence-driven verification enables a clean, predictable return to operations. This strategic certainty removes the gamble of re-infection, allowing businesses to restore continuity and organizational trust with unrivaled confidence.

Modern ransomware attacks no longer stop at encrypting production files—they actively target the infrastructure, applications, and operational dependencies required for recovery itself. While security teams primarily rely on SIEM/EDR tools focused on the active perimeter, backup data frequently remains an unmonitored blind spot. With 94% of ransomware attacks targeting backup infrastructure and organizations facing a 258-day mean time to contain a breach, treating backups as a passive insurance policy is no longer sufficient. Recovery without validation isn't resilience—it's risk. True assurance during an active incident relies on built-in forensics, verification, and orchestration. Together, they replace chaos with confidence, transforming recovery from a theoretical plan into a battle-tested reality.

The Challenge: The Backup Security Blind Spot

Recovering clean data after a cyberattack is far more complex than a standard disaster recovery event where data integrity can be trusted; ransomware forces teams to assume compromise at every stage. Without a unified, security-led layer built directly into backup data, organizations face several critical challenges:

- **Hidden Persistence & Sleeper Threats:** "Low and slow" threats routinely evade perimeter tools and remain dormant across backup timelines, leading to unexpected surprises when it's time to restore.
- **The Reinfection Loop:** Restoring directly back into production without verification can reintroduce the same malware that caused the outage, turning recovery into a cycle of speculative guesswork and reinfection.
- **Manual Investigation & Recovery:** Under intense pressure, security and IT operations teams must coordinate across multiple siloed systems and fragmented, manual workflows, driving up downtime and data loss.
- **Complex Native Overheads:** Relying on native infrastructure snapshots or M365 native tools adds operational complexity, lacks centrally enforced immutability, and increases the administrative burden.

The Solution

Druva Premium Security closes critical backup security blind spots, transforming your data protection layer from a passive insurance policy into an active security control. By combining Druva's core immutability with purpose-built Ransomware Detection, advanced Threat Insights, and Cyber Recovery Runbooks, Premium Security delivers true recovery assurance across the detection, investigation, and recovery lifecycle:

- **Continuous Preparedness:** Built-in behavioral ransomware detection, continuous threat monitoring, forensic validation, and scheduled testing help teams identify threats with greater confidence and maintain recovery readiness.
- **Clean Recovery:** Advanced forensics, proactive threat hunting, and automated orchestration eliminate malware re-infection loops and accelerate containment.

Key Features

Ransomware Detection: Behavioral Detection & Forensic Validation

Confidently identify and confirm known and unknown ransomware with AI-powered, multi-stage detection. Druva analyzes ransomware behaviors across backup snapshots — including ransom note proliferation, suspicious file-extension changes, and mass file renaming — then automatically escalates high-risk activity for deeper in-platform forensic validation.

Structural analysis, entropy checks, and file-type verification confirm ransomware presence and encryption while reducing alert noise. Confirmed findings are surfaced with explainable evidence and recovery context, helping administrators understand impact and identify clean pre-infection restore points and move quickly into validated recovery workflows.

Threat Insights: Continuous & User-Driven Monitoring

Druva Threat Watch and Druva Threat Hunting deliver continuous threat detection alongside targeted incident investigation across backup snapshots. Together, they enable IT and security teams to inspect backup data for indicators of compromise (IoCs) and execute on-demand searches, ensuring risky restore points are isolated early, reinfection risks are eliminated, and clean recovery is accelerated — all without adding infrastructure overhead.

Threat Watch: Always-On Monitoring & Auto-Quarantine

Scans backups automatically every 8 hours on incoming and changed data to identify threats early. When new IoCs are identified, Druva automatically triggers retrospective rescans across the last 30 days of backup data. Upon detection, Druva instantly quarantines contaminated data from backups to prevent the utilization of infected datasets.

Threat Hunting: Cross-Workload Hunting

Allows teams to reactively investigate historical backups to pinpoint the root cause and scope of an attack. Hunt for static IOCs in metadata — such as file hashes, attributes, and extensions — map the attack timeline and blast radius, and defensibly delete infectious data from backups to ensure recovery proceeds with only kept data.

Threat Insights: Key Capabilities

- **Global Intelligence & Retrospective Analysis:** Aggregates threat intelligence feeds from CISA, Mandiant, Google, and Druva's ReconX Labs.
- **Broad Coverage & Defensible Cleanup:** Supports search, quarantine, and cleanup workflows across cloud-native (EC2, Azure, M365) and data center workloads (VMware), ensuring verified malicious files are permanently purged from recovery paths.
- **Zero-Infrastructure Footprint:** Get powerful threat monitoring without requiring agents or dedicated scanning nodes, simplifying deployment and reducing operational overhead.

Cyber Recovery Runbooks: Orchestrated Response & Verification

Replace tribal knowledge with automated, repeatable, and controlled workflows. Acting as your critical orchestration layer, it sequentially automates the entire recovery lifecycle — from threat hunting and data curation to antivirus scanning and post-recovery validation. This eliminates human error during a crisis and guarantees a clean, verified restoration every time.

- **Automated Sequencing:** Coordinates predefined recovery paths for interdependent systems, ensuring workloads are restored in the exact correct order during high-pressure events.
- **Recovery Testing & Orchestration:** Test for operational readiness and compliance. In a live incident scenario, orchestrate rapid, secure recovery of workloads into segmented environments for investigation and remediation.
- **Isolated Recovery Environments (IRE):** Orchestrates rapid, guided recovery into a secure, segmented "clean room" sandbox to investigate, validate, and remediate systems before production cutover.
- **Post-Restore Validation Tasks:** Automates crucial last-mile validation steps, including automatic Network Interface Card (NIC) detachment and OS boot checks, while supporting custom post-boot scripts.



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

Druva is the resilience foundation for the AI enterprise, helping organizations secure and recover from connected risk across data, cyber, identity, and AI. The Resilience Cloud is a fully managed, cloud-native SaaS platform that delivers air-gapped and immutable protection across cloud, SaaS, on-premises, endpoint, and edge environments. Powered by Dru MetaGraph, Druva's graph-powered intelligence layer, the platform connects critical business context so customers can understand risk, respond faster, recover cleanly, and govern data with greater confidence.

Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva helps safeguard the critical information and systems businesses depend on in an increasingly connected world. Visit druva.com and follow us on [LinkedIn](#) and [Facebook](#).