Security Posture and Observability

Druva's posture and observability capabilities provide a real-time overview of your data security posture and deep observability into how your data has changed. Fortify the security of data in your backup environment and accelerate incident response with enhanced security insights into your data.

The Challenge

Ransomware has evolved into one of the most disruptive threats facing enterprises today. Attackers are no longer satisfied with encrypting production systems — they are deliberately targeting backup environments, understanding that recovery is the last line of defense. By corrupting backups, delaying detection, and hiding in the environment for weeks or even months, adversaries ensure maximum damage when they strike.

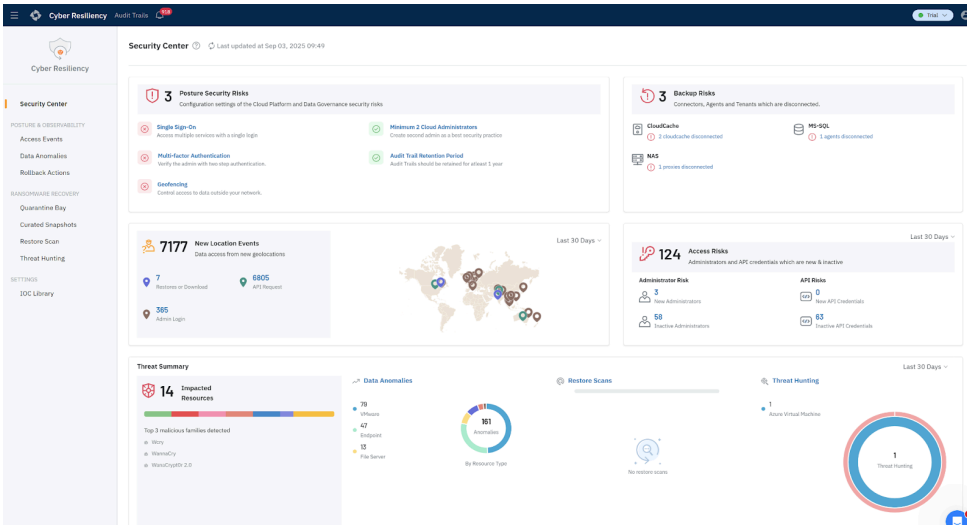
Unfortunately, most organizations are relying on traditional security tools that were designed to secure the perimeter, not enable fast recovery. These tools, often siloed from backup operations, can detect anomalies but rarely help IT teams identify which data is clean and recoverable. This disconnect means early warning signs are missed, and recovery is slowed when time is most critical.

IT and security teams now operate under an assume-breach mindset. They are investing heavily in detection and response, but without a direct connection to the backup environment, their response capabilities remain limited. When the attack's primary target is data itself, the ability to simply restore backups is no longer sufficient. Clean data must be rapidly identified, validated, and restored — all while coordinating with security workflows.

The consequence of this gap is severe. Without deep integration between backup and security operations, recovery takes longer, downtime stretches into days or weeks, and the business faces escalating costs in lost productivity, revenue, and reputation. What should be an opportunity for resilience too often becomes an extended crisis.

Ensure Attack Readiness with Druva

Your backup data mirrors your primary data and is a rich source for improving your security posture and preparing for a potential attack. With Druva, continuously monitor your backup data and environment, respond to potential threats, and extend data to SIEM platforms for further insights with pre-packaged integrations.



Druva's Security Command Center dashboard ▶

The Benefits of Integrated Posture and Observability

- Easily monitor the security posture of your backup environment and detect problems before they cause damage.
- Automate detection of access events and data anomalies within your backup environment such as restore requests from an unusual location, data encryption, unusual data deletion patterns, and more.
- Prevent accidental or malicious deletion of business-critical backup data despite compromised credentials.
- Enhance SecOps time-to-value with out-of-the-box, prepackaged SIEM integrations.

Key Features

- **Access Events Dashboard and Alerting** — Get relevant situational awareness about backup activity. A security event dashboard makes it easy to see unusual activity or drill into details about who has accessed your backup environment and data — administrators, users, and APIs, whether access occurred from a usual location, what occurred (e.g., backups or restores), and investigate alerts for data anomalies.
- **Rollback Actions** — With traditional disk and cloud storage systems, once an administrator deletes your backup data, it is gone. Only Druva allows you to roll back the deletion of backup data, using self-serve capabilities. Druva Rollback Actions can restore deleted backup data from a secure cache for up to 7 days — accessible only to you.
- **Data Anomaly Detection** — Druva uses AI/ML to detect malicious backup activity—such as deletions, modifications, or encryption—by analyzing data behavior to uncover ransomware. This capability spans endpoints (workstations, servers, NAS), virtual machines (VMware ESXi/vSphere), and cloud workloads (M365, SharePoint). Deployment is flexible: agentless for zero-touch, cloud-based protection without credentials or complex setup, or agent-based for deep integration with storage and file server infrastructure.
- **Recovery Intelligence** — Allows users to visually identify ideal restore points based on anomalous data activity, presence of IOCs, and observance of encryption activity.
- **Pre-Packaged Security Integrations and APIs** — Extend security event alerts and data into SIEM tools with one of several pre-packaged integrations or with Druva APIs. Some examples include:
    - Monitor compliance to geo-based data access and restore policies and API requests from new locations
    - Track user access patterns to recover data and unauthorized login attempts
    - Create alerts from pre-built rules to trigger pre-configured playbooks
- **Security Command Center** — Gain real-time visibility into your security posture with comprehensive risk assessments, including a Cyber Resilience Scorecard that validates proper configuration of critical resilience features. Unlock deep insights into risks across cloud platform security (e.g., administrators without MFA), data compliance, backup reliability (e.g., disconnected agents), and data access (e.g., users, APIs). Take swift, corrective action directly from a centralized command center.

You can not prepare for today's advanced threats and tomorrow's risks without including security posture and observability into your daily operations and security toolset. Trying to build and maintain this capability on your own becomes one more integration effort to maintain. The Druva Data Security Cloud delivers automation, unique data insights, and pre-built interactions to ensure your organization is attack-ready.

CROWDSTRIKE | Microsoft Sentinel
paloalto NETWORKS | splunk>
Trellix | Microsoft Entra ID
sumo logic | BetterCloud
okta | servicenow
exterro | BOCADA

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

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, X (formerly Twitter), and Facebook.