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

IT and security teams today operate with an assume-breach mentality and are increasing investments in detection and response capabilities as traditional prevention methods alone are inadequate. Your data is the primary target for both bad actors and ransomware attacks making backup data ever more critical to your organization. Unfortunately, the ability to simply recover backup data is not enough when an attack occurs. Today, IT and security teams lack deep integration between the backup environment and their security operations that can enable response workflow and tooling. This slows both response and data recovery times resulting in greater downtime and lost revenue.

Our perspective

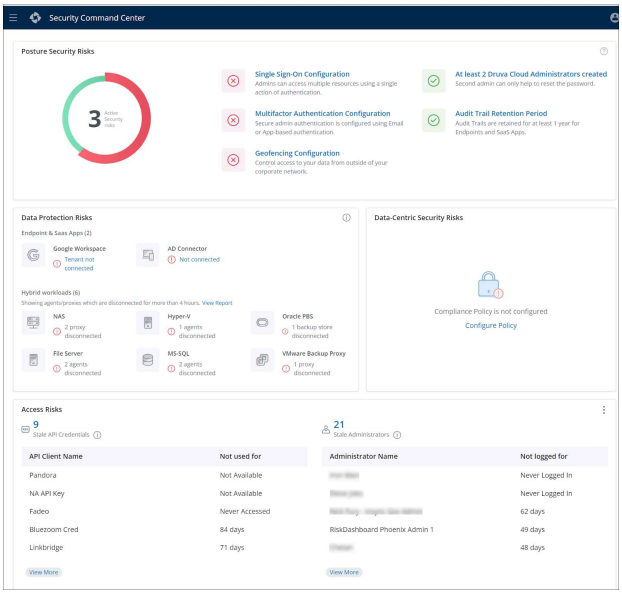
Historically, integration between backup platforms and SIEM tools has been difficult due to costs, timelines, and ownership. While APIs have existed for years, integrations require constant care and feeding. Yet, despite efforts to share data, many organizations still lack a single comprehensive view of the security of their backup environment, one that provides insights into security controls, configurations, and abnormal changes. There is a need for integrated, out-of-the-box capabilities that allow IT and security teams to easily understand their data security posture, observe backup data changes without analyst time or new integrations, and drill into dashboards or alerts that are unique to their deployments. By simplifying both access and the use of posture and observability data IT and SecOps teams can enable better preparedness, faster incident investigation and response, and better root cause analysis.

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. Continuously monitor your backup data and environment, respond to potential threats, and extend data to SIEM platforms for further insights with pre-packaged integrations.

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 security 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.



Druva's Security Command Center dashboard

Key features

- **Security 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 unusual data activity (UDA).
- **Unusual data activity (UDA)** — Identify and respond to threats with AI/ML-based anomaly detection that understands your data and sends automated alerts for unusual data activity (UDA). Currently, it is available for endpoint, file, and NAS workloads. See Druva documentation for the latest workload updates.
- **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.
- **Threat hunting** — Search for threats across an extended timeline of backups and the entire end-user data — endpoint devices and apps like Microsoft 365 and Google Workspace. Locate and quarantine threats to prevent reinfection risks from backups. Eliminate threats from backups and primary environments with defensible deletion.
- **Backup MDR (Managed Detection & Response)** — Included standard with Druva's foundational security, backup telemetry generates real-time alerts for potential threats. Our analysts serve as an extra set of eyes on your data, thoroughly examining alerts, and conducting a detailed analysis to verify their validity. Druva Cloud Ops communicates with customers, and if risks are verified, takes proactive measures to secure and remediate threats.
- **Pre-packaged security integrations and APIs** — Extend security event alerts and data into SIEM tools with one of several pre-packed integrations (Trellix Helix(FireEye) and Splunk) 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 dashboard** — Receive a real-time security posture risk assessment and in-depth insights into risks for cloud platform security (e.g., administrators not using MFA), data compliance, data protection reliability (e.g., disconnected agents), and data access (e.g., users, APIs). Quickly take corrective actions from the 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 Resiliency Cloud delivers automation, unique data insights, and pre-built interactions to ensure your organization is attack-ready.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
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 industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.