Data Anomaly Detection

Druva's data anomaly detection leverages agentless deployment, cloud-based indexing, and comprehensive threat detection to ensure real-time protection, SLA adherence, and robust security while maintaining high operational efficiency.

The Challenge

Ransomware has matured far beyond smash-and-grab tactics. Today's attacks are stealthy, multi-stage operations designed to quietly infiltrate, escalate privileges, and then target the organization's most valuable asset—its data. Attackers methodically encrypt, delete, or corrupt information long before traditional defenses detect suspicious activity.

Security tools such as EDR, SIEM, XDR, and intrusion prevention remain critical to any defense strategy. They are highly effective at detecting *who* is attacking and *how*—monitoring endpoints, identities, and network traffic. But they were never designed to see *what is happening to the data itself*. This creates a blind spot — by the time these tools issue an alert, the ransomware may already have compromised, encrypted, or destroyed large volumes of business-critical data, forcing organizations into costly, reactive recovery efforts.

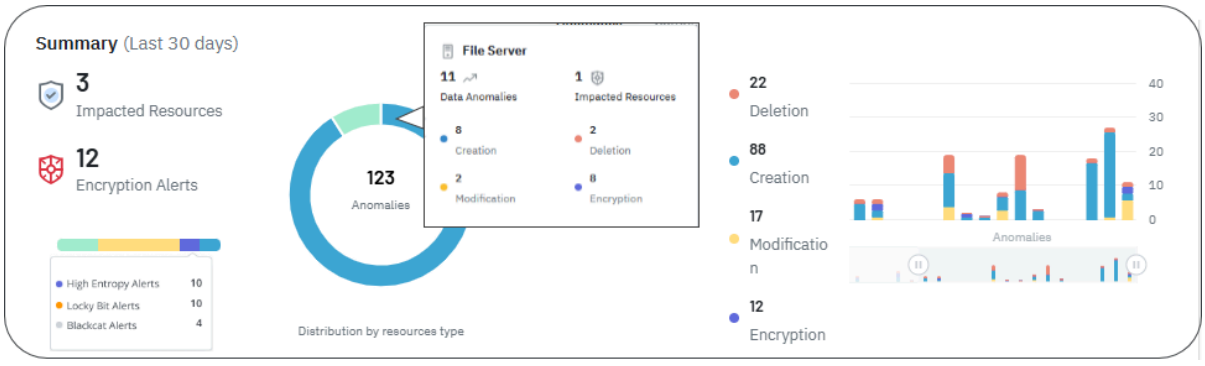
The Solution

Data Anomaly Detection closes the visibility gap by serving as an early warning system at the data layer. By continuously analyzing backup data, it detects suspicious patterns—such as unusual deletions, abnormal modification spikes, or unexpected encryption activity—that signal ransomware or insider threats in their earliest stages.

Crucially, this capability doesn't replace existing defenses; it complements and enhances tools like EDR, SIEM, and XDR by adding the missing context of *what is happening to the data*. This enables security teams to detect threats sooner, investigate with richer insights, and respond before widespread damage occurs.

Druva's approach to data anomaly detection transforms cyber resilience. Delivered as a fully managed, cloud-native service, it provides scalable and seamless protection without operational overhead or credential risk. Druva extends this protection across the enterprise—from endpoints (workstations, servers, NAS) to virtual machines (VMware ESXi/vSphere) to SaaS workloads (Microsoft 365, SharePoint). Deployment is flexible — agentless for zero-touch, credential-free protection, or with agents where deeper integration into storage and file server infrastructure is required.

In short, Druva's data anomaly detection ensures that when ransomware or insider threats target data, organizations are not caught off guard. Instead, they gain the early warning, scale, and resilience needed to stay ahead of evolving threats.



Get an overview of the number of impacted resources, alerts generated, and more. Use this information for your analysis and take appropriate action.

Key Features

- **Flexible Deployment —** Agent and agentless deployment options reduce operational complexity, enabling instant, hassle-free setup and maintenance-free operation across your on-prem and cloud environments.
- **Comprehensive Anomaly Detection —** Detects data creation, modification, deletion, and encryption anomalies, including potential ransomware threats across endpoints (workstations, servers, NAS), virtual machines (VMware ESXi/vSphere), and cloud workloads (M365, SharePoint).
- **Consistent SLA Adherence** — Guarantees alert generation within one hour post-backup, ensuring timely response and mitigation of potential threats.
- **Robust Security Controls** — Provides highly secure indexing and anomaly detection processes, adhering to stringent access and privacy controls to protect sensitive data.

The Benefits

Druva's cloud-based data anomaly detection delivers unmatched protection and simplicity. Its agentless design, robust scalability, superior security, and optimized cost-efficiency make it the ideal solution for organizations seeking comprehensive, proactive, and sustainable ransomware defense strategies.

- **Ease of Adoption** — A zero-touch, cloud-based deployment removes operational overhead and eliminates prerequisites, significantly boosting adoption rates.
- **Enhanced Security** — By removing the need for guest OS credentials and intrusive agents, organizations substantially reduce their attack surface and mitigate risks associated with credential exposure.
- **Scalability and Efficiency** — Cloud-based anomaly detection efficiently scales across large environments, seamlessly handling extensive workloads with minimal impact on resources and infrastructure.
- **Rapid Threat Identification** — Swift detection capabilities ensure alerts are generated within one hour of backup completion, drastically reducing incident response times and minimizing potential damage.

Druva's data anomaly detection delivers a new layer of defense that complements and strengthens existing security investments. Its flexible architecture removes barriers to adoption, enabling near 100% coverage across VMware environments and beyond. By analyzing backup data in real time, Druva provides early warning of ransomware through detection of unusual deletions, modifications, or encryption activity—signals that traditional tools often miss until it's too late. Scalable, secure, and effortless to manage, Druva empowers organizations to detect threats earlier, respond faster, and minimize disruption, dramatically improving their overall cyber resilience.

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