THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

The MSP Security Imperative

Enterprises expect their MSPs to deliver not just infrastructure management but also robust cyber-resilience. Without a unified data protection and threat-detection platform, MSPs risk losing contracts to vendors that can prove rapid recovery and compliance.

→ Clients demand ransomware-ready backups

→ Regulatory audits increasingly focus on data integrity

→ MSPs need a single pane of glass for security and operations

CONTROL FRAMEWORK

Druva's New Security & Resilience Features

Druva adds immutable backup storage, AI-driven ransomware anomaly detection, and integrated SOC alerts to its data-protection suite, giving MSPs a turnkey security layer that aligns with industry best practices.

→ Immutable backups prevent alteration after write

→ Behavioral analytics flag anomalous file activity

→ SOC integration surfaces incidents in real time

CONTROL FRAMEWORK

How MSPs Integrate Druva into Their Service Stack

MSPs layer Druva's APIs over existing ticketing, monitoring, and billing platforms, creating a unified workflow that automates backup provisioning, security alerts, and client reporting.

→ API-driven onboarding reduces provisioning time

→ Alert forwarding to existing NOC tools

→ Automated compliance dashboards for each client

CONTROL FRAMEWORK

Value Delivered to MSPs

The added security capabilities unlock new revenue streams and improve client retention by positioning the MSP as a trusted cyber-resilience partner.

- → Ability to sell security-focused SLA tiers
- → Reduced churn as clients see measurable risk mitigation
- → Cross-sell opportunities with compliance consulting

CONTROL FRAMEWORK

Client Outcomes with Druva-Powered Resilience

Clients experience faster recovery from ransomware incidents, clearer audit trails, and confidence that their data cannot be tampered with after backup.

- → Recovery point objectives (RPO) shrink to minutes
- → Audit logs are immutable and searchable
- → Incident response time improves with real-time alerts

CONTROL FRAMEWORK

Implementation Blueprint for MSPs

A three-phase rollout ensures minimal disruption and rapid value capture:

- → Phase 1 – Assess existing backup and security gaps
- → Phase 2 – Deploy Druva immutable storage and enable ransomware analytics
- → Phase 3 – Integrate SOC alerts and launch client-facing dashboards

EXECUTIVE TAKEAWAY

Executive Takeaway

Druva's expanded security and cyber-resilience suite gives MSPs a ready-made, compliance-ready foundation that transforms data protection into a strategic growth lever. By embedding immutable backups, AI-driven ransomware detection, and SOC integration, MSPs can differentiate their portfolio, deepen client trust, and capture new revenue without building security capabilities from scratch.