Dropsuite
A NinjaOne Company

Datasheet

LEGAL FOCUS:

# Build an MSP Archiving and Compliance Offering

## Introduction

Courts want indisputable facts, not lengthy fishing expeditions. As a managed service provider (MSP), how can you help your customers produce a defensible record on demand? Treat that outcome as a repeatable service you configure, monitor, and prove. When a discovery request hits, companies need more than just stored emails. They need preserved communications to provide during audits, along with lightning-fast search across mail and Microsoft Teams. MSPs that standardize search, export, and evidence collection make this predictable instead of ad hoc. The goal is simple: produce a clean, solid record whenever it's requested.

A compliance strategy is what makes that possible. Maintaining retention schedules, legal holds, chain of custody, and immutable logs is essential for firms and businesses that handle sensitive legal information. For MSPs, this means aligning technical controls with the firm's matter workflows and keeping proof ready on demand. Doing this well reduces risk, cuts review costs, and builds client confidence. Gaps in compliance don't just trigger fines; they erode trust, delay timelines, and raise sanction risks.

## Setting the Scene

Picture this, your customer gets a discovery request tied to a departing employee. Legal asks for six months of Microsoft Outlook and Teams history, but journaling was never enabled for shared mailboxes. You also discover that messages aged out, with a short retention rule leading to partial backups. Microsoft Entra logs are incomplete, so you can't even show who had access or when policies changed. The gaps in your evidence cause extended timelines as your team must try to manually recover what they can, all while your client's trust dips. This is the exact failure pattern MSPs are hired to prevent through correct defaults, coverage checks, and extended audit visibility.

The MSPs who sail through this do a few simple things early. They have a solution in place to issue the hold, journal every required mailbox, align retention to the case, and keep Entra logs so access is traceable. To meet a discovery request, they can scope the people, search mail and Teams without guesswork, and deliver exports with headers and a protected audit trail. Prebuilt export templates and chain of custody notes keep the evidence package consistent across matters. The result is a record set that is complete, timely, and easy to defend.

## What Could Go Wrong

**Legal Hold Missed:**
An employee quits and triggers a discovery request, but no hold was issued. Messages age out under a short retention policy, creating gaps the other side can challenge and forcing costly reconstruction work.

**Unjournaled Mailboxes:**
Six months of Outlook and Teams are requested, yet shared mailboxes were never journaled. Content that fell between backup intervals is missing, so you cannot show message completeness or produce clean exports with full headers.

**Incomplete Entra Trail:**
Access and policy changes need to be proven, but Entra logging is spotty. You cannot clearly show who had access, when policies shifted, or whether a control was disabled, which weakens defensibility and invites timeline slippage.

## Building in Compliance

Regulated clients are asking MSPs to do more than keep systems running. They want a partner who can help them stay out of trouble and defend them when questions come up. With privacy rules tightening and discovery requests on the rise, a solid compliance program fosters trust and opens up steady, high-margin work. Package this as a managed service with clear SLAs, named owners, and scheduled reviews tied to the firm's matter lifecycle.

This only works when your offer runs on real controls and habits you can repeat. Legal holds go out when they should, mailboxes are captured continuously, retention follows the case timeline, and the record stays intact. Automated checks and simple dashboards help you and the firm see coverage and exceptions at a glance. You can retrace access and admin changes, find what you need across mail and Teams without guesswork, and hand over exports that preserve headers and metadata. Keep a small evidence kit that includes export templates, chain of custody notes, and an access report so the response package is consistent every time. Put that together and you have a compliance platform clients trust.

Legal buyers want you to show your work. Be ready to demonstrate a hold process you can evidence from notice through release and retention that matches the client's policy and the matter at hand. Search should span mail and Teams while preserving headers and other metadata, and controls limit who can touch the data with audit logs for views, exports, and policy changes. A short walkthrough of this process builds credibility and shortens approvals for future matters.

| What Clients Expect | Evidence to Show on Request |
|---|---|
| Timely legal hold when litigation is reasonably anticipated | Hold log with timestamps and custodians; confirmation the hold stayed in place |
| Defensible preservation with integrity and a clear chain of custody | Journaling/config report, active retention policy for the period, immutability/WORM status if required |
| Proportionate search and targeted retrieval with intact metadata | Search summary (custodians, dates, keywords) and export manifest preserving headers and metadata |
| Auditability of who accessed data and when policies changed | Access and admin activity logs; policy-change history, with Entra sign-in and role events for context |

## Drosuite to the Rescue

You need a simple way to position your team as the compliance expert your clients rely on. **Dropsuite Archiver** gives you the building blocks of defensible discovery: immutable storage, policy-based retention, legal hold, fast search, and exports that preserve headers and metadata. Search is targeted across mail and collaboration data, and exports keep headers intact for defensibility.

Pair that with **Entra Backup** and you cover the identity side of the story. You can show how access was configured at a point in time, who signed in, and when roles or policies changed. Many mature MSPs standardize on Microsoft 365 Business Premium for the security baseline, and then add backup for Entra to protect identity configuration alongside the data.

Together, **Archiver and Entra Backup** help you prove what was kept, who had access, and when controls were in place. Package this as a compliance offering to start leading the conversation, strengthening trust, and creating room for higher-margin services.

| Features | Entra Backup with Dropsuite Backup | Entra Backup with Dropsuite Archiver |
|---|---|---|
| Entra ID Protection | ✓ | ✓ |
| Incremental Backup for Continuous Protection | ✓ | ✓ |
| Email Journaling | ✗ | ✓ |
| Unlimited Storage | ✓ | ✓ |
| Advanced Search | ✓ | ✓ |
| Search within Documents | ✗ | ✓ |
| Granular, Point-in-Time Restore | ✓ | ✓ |

| | | |
|---|---|---|
| Reporting Dashboard | ✓ | ✓ |
| Retention Policies | Flexible Options | Fully Customizable Policies |
| Audit Log | ✓ | ✓ |
| eDiscovery & Saved Searches | ✗ | ✓ |
| Tagging & Alerting | ✗ | ✓ |
| Legal Hold & Data Review Process | ✗ | ✓ |

Want a faster path to defensible discovery? Learn more about **archiving and compliance** or **try a demo** to see how simple implementing an archiving solution can be.