

 CrashPlan™

**How to Make Legal
Hold Frictionless for IT,
Legal, and the End User
with Endpoint Backup.**

Introduction

As legal hold challenges rise, endpoint backup emerges as a must-have solution

With some form of corporate litigation now ever-present within nearly every organization, legal hold has become an ongoing challenge. Yet while the volume, complexity and velocity of legal hold demands keeps growing, most organizations still rely on highly manual approaches to enacting and managing legal holds—especially when it comes to collecting and preserving endpoint device data. This conventional approach is time-consuming and labor-intensive for IT teams, risky and unreliable for legal teams, and disruptive for end users whose devices are quarantined, resulting in substantial tangible and intangible costs.

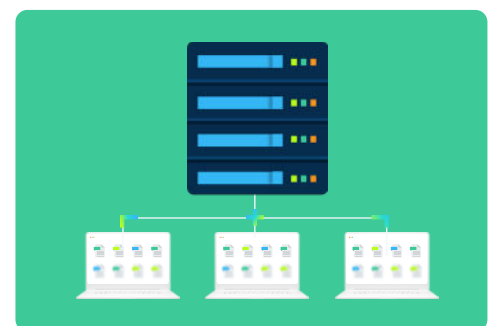
Forward-thinking IT and legal leaders are turning to endpoint backup solutions to drive a modernized approach to reliable, repeatable, and efficient legal hold. By automatically and continuously collecting and preserving endpoint data, endpoint backup solutions streamline the legal hold process and ensure continuous access to business-critical files and data — without burdening IT teams or disrupting end-user productivity.

A legal hold is placed on data to prevent it from being deleted pursuant to the company's involvement in current or imminent litigation or criminal cases. When a company has a reasonable expectation that it will become involved in litigation or criminal proceedings, part of its responsibilities include saving documents that may be involved in that legal proceeding.



70%

of data is unstructured. This is information that is not arranged according to a preset data model or schema, and therefore cannot be stored in a traditional relational database (e.g. business documents such as email, videos, photos, webpages, and audio files.)



almost

50%

of all data is distributed across company laptops

The flaws of conventional legal hold solutions

In a legal hold scenario, organizations need to collect and preserve all relevant data — from enterprise systems, cloud-based SaaS applications, and users' endpoint devices.

The reality is that **a tremendous amount of data still lives (exclusively) on endpoint devices.**

And for most organizations, the process of collecting and preserving endpoint data is anything but reliable and elegant.

Reliance on cumbersome manual device collection

The conventional approach to legal hold centers on manual collection of the physical endpoint device: physically obtaining laptops, smartphones and other endpoint devices and quarantining them for the duration of the legal hold/litigation process. This manual process has several painful outcomes:



Huge burden for IT teams

Manual device collection is extremely time-consuming and labor-intensive for the IT teams tasked with executing legal holds, especially with remote and hybrid workers — not to mention the potentially contentious situations.



Significant wasted IT spend

Most IT teams are familiar with the “closet full of laptops” — the result of ongoing device quarantines as part of the conventional legal hold approach. Device quarantines easily add up to tens (or hundreds) of thousands in annual IT spend that's wasted on devices sitting idle.



Major disruption to end users

Employees impacted by a legal hold typically have their devices taken for weeks or even months. They generally get a replacement, but this device migration process is inconvenient and may miss some files. Productivity disruptions are magnified because legal hold frequently impacts top-level business unit leaders and executives.



Unreliable for legal teams

The time and costs around manual device collection make legal teams slower to enact legal holds. Then there's the inherent time lag between the decision to enact and when IT actually collects the device. This latency amplifies spoliation risks for legal teams.



Increases (already high) corporate litigation costs

The conventional approach of manually collecting devices leads to slow, less effective eDiscovery. This is one primary reason that eDiscovery now accounts for 80% of corporate litigation costs.

Why targeted hold solutions fall short

Lack of IT alignment

The market for dedicated eDiscovery solutions is now quite mature, and some of these vendors are now offering targeted legal hold solutions. Yet organizations that have attempted to implement these targeted solutions struggle with shortcomings that center on a fundamental flaw:

Legal hold solutions must be built with IT in mind!

Since IT is almost always tasked with executing and managing legal holds, IT teams will be the primary users of any dedicated legal hold solution. However, almost all of the targeted legal hold products on the market grew out of eDiscovery products and were built with legal teams' needs in mind. As a result, they're not well integrated with the rest of the tech stack, not designed to fit within common IT workflows, and not aimed at the specific pain points that IT experiences when enacting legal holds.

Are you creating Shadow Data? Shadow Data is when structured (spreadsheets, databases, etc.) and unstructured data (Word documents, emails, photos, etc.) is saved on endpoints, mobile devices, in personal SaaS solutions, or even cloud storage.





A recent study by SANS determined 80% of organizations have shadow data despite strict policies against it.

To learn more, visit <https://bit.ly/shadowdatawhitepaper>




The high (and hidden) costs of inaction

Legal hold is now an unavoidable ongoing responsibility. Sticking with conventional approaches brings high and often hidden costs, including the possibility of things being omitted or overlooked:

Measurable Costs

-  Excessive IT time
-  Lower productivity
-  Unnecessary technology spend
-  Legal risk/spoilation sanctions

Hidden Costs

-  Employee frustration
-  Damage to company culture and loss of business opportunities
-  Reputation damage and adverse references

Endpoint backup redefines modern legal holds

As IT and legal leaders look for a better approach to legal hold, they're homing in on the problems around manual device collection and quarantine. The root challenge: collecting and preserving endpoint device data

The solution already exists: Endpoint backup

Reframing a complex challenge in terms of its most essential root cause often reveals a simpler solution. In this case, forward-thinking organizations are recognizing that endpoint backup is designed specifically to:



Automatically collect and preserve endpoint data

Data collection happens continuously, without the physical device present.



Provide granular control over the scope of data preservation

Preservation can be as comprehensive as every version of every file, including all relevant metadata.



Not burden IT or disrupt end users

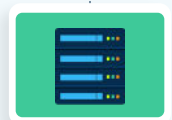
Data collection happens automatically and silently — without IT intervention and with zero impact on end users' machines.



Endpoint backup is the secure storage of a copy of data from a device such as a tablet, phone, laptop, or desktop computer, commonly called an "endpoint. An endpoint is considered "backed up" when there is a copy of important files available to restore from should something happen to the device (Eg. accidental deletion, site disaster, or hardware failure).

Focused legal hold capabilities that align IT and legal needs

Endpoint backup solutions are already built for IT workflows and are designed to be easy to implement and manage for IT teams. Best-in-class endpoint backup solutions like CrashPlan have layered on purpose-built legal hold functionality that take that the core backup product and provide focused capabilities that meet legal specifications while aligning with IT needs.



The value of using endpoint backup for legal holds



Cost savings

Reducing the cost of IT devices and IT team's time.



Increased productivity

Minimizing disruption to end users and define clear workflows and division of duties for Legal, IT and HR.



Reduced legal & eDiscovery costs

Lowering legal and Spoilation risks and improving eDiscovery efficiency.

Foundational business continuity and resiliency

Building the foundation for future-ready cyber resiliency and business continuity by ensuring continuous access to business critical information and also providing protection against tech failures, human error, ransomware, and cyberattacks.

A versatile solution

Using endpoint backup to streamline employee offboarding

While legal hold is an increasingly common scenario, employee offboarding is an everyday responsibility for IT teams. The same functionalities and capabilities that make endpoint backup powerful as a legal hold solution also make it an ideal tool for accelerating offboarding processes while eliminating the risk of data loss and the high costs of device quarantines:

- 1 IT teams proactively capture all endpoint device data.
- 2 Devices can be wiped and put back into circulation immediately.
- 3 Every version of every file is securely preserved for easy, instant access in the future, guarding against accidental or intentional IP theft and data loss during employee departure.

Identifying the right legal hold solution

The ability to leverage an existing endpoint backup solution to modernize a legal hold program offers a powerful path to ROI. But wading into the market of endpoint backup products reveals that not all endpoint backup offers the same level of protection—or the capabilities required to enable a modern approach to legal hold. Below are the essential capabilities to look for in an endpoint backup solution:

Continuous preservation of all endpoint data

The ability to continuously and automatically capture and preserve all endpoint data—including remote devices—as frequently as every 15 minutes, with no manual action or IT intervention required.

Frictionless agent

The endpoint backup should be executed by a frictionless agent that is installed on every endpoint that can carry out regular backups without slowing down the machine, disrupting end-user productivity, or requiring end-user action.

Comprehensive coverage & granular control

To meet legal hold needs, an endpoint backup solution must be able to capture every aspect of every file, automatically—including all file metadata like timestamps, file permissions, and directory paths. The solution should also make it easy to define data preservation policies by user, device, data source, and more.

Secure, unlimited storage & chain-of-custody controls

To make proactive legal hold and data preservation practical, an endpoint backup should offer unlimited cloud storage that makes it cost-effective to preserve data early and in perpetuity. This makes it easy to comply with potential litigation requirements, data retention requirements, or data preservation policies. The solution should also provide strong security controls to maintain the integrity of preserved files as well as complete audit trails enabling chain-of-custody validation.

Centralized access & access control

All preserved data should be immediately discoverable—anytime, anywhere, regardless of whether or not the device is currently online. Additionally, the platform should make it simple to set preservation policies, create legal matters, manage custodians, and data access.

Searchable storage architecture

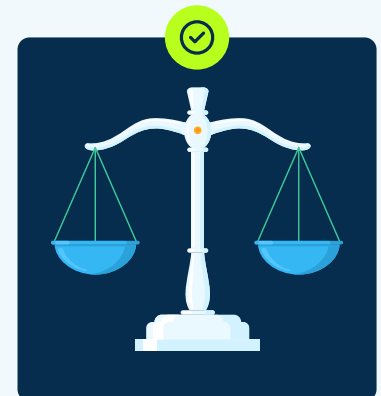
To streamline data review and eDiscovery, the endpoint backup solution should automatically organize all collected data, including unstructured data, in a searchable storage architecture.



Legal Hold Shortlist

Does the endpoint backup/legal hold solution enable me to...

- ✓ Instantly enact legal holds and proactively preserve data — without the physical device?
- ✓ Capture critical endpoint data that's often missed?
- ✓ Avoid user disruption?
- ✓ Keep devices in use to eliminate excess IT spend?
- ✓ Streamline eDiscovery and incident investigation?



Building the case for change

Overcoming the inertia of the status quo is the toughest part in driving any change. While various stakeholders (Legal, IT, HR, etc.) likely recognize the pain points and frustrations of conventional approaches to legal hold, champions for modernizing legal hold will need to build a clear business case that speaks to those unique concerns and priorities and describes the value of the new solution in role-specific terms:

Legal Teams

Avoid spoliation risk with continuous data preservation.

Proactively enact legal holds and automatically and continuously preserve users' endpoint data to avoid spoliation sanctions, fines, and adverse inferences.

Close endpoint data gaps in eDiscovery process.

Make every version of every file, including metadata, from any laptop or remote device immediately discoverable.

Eliminate custodian cooperation issues with automatic data capture.

Instantly implement legal holds and capture in-scope data without requiring end-user/custodian action and cooperation.

Automatically provide chain-of-custody validation.

Maintain the integrity of preserved files and provide chain-of-custody validation with automatic audit trails of all file access.

IT Teams

Set granular permissions for easy, secure collaboration with Legal and HR.

Easily define granular roles and permissions (by individual, role or group) to allow Legal and HR teams to collaborate faster and more effectively, from a single source of truth.

Enact legal holds without obtaining the physical device.

Instantly implement legal holds and capture in-scope data without manually obtaining the physical endpoint device.

Capture in-scope data without requiring end-user action/cooperation.

Execute silent data capture without requiring any action, cooperation or even awareness of end users.

Cut out wasted IT spend by eliminating device quarantines.

Eliminate thousands of dollars in annual wasted spending on idle, quarantined endpoint devices. Devices do not need to be quarantined during legal holds and can be wiped during employee offboarding and immediately returned to circulation.

HR Teams

Follow data preservation/retention requirements without requiring end-user action/cooperation.

Follow legal hold and data retention policies without requiring end-user/custodian action and cooperation.

Improve collaboration with IT and Legal teams.

Collaborate with internal stakeholders from a single, purpose-built legal hold dashboard to set data preservation policies, create legal matters, manage custodians and data access. .

Avoid the individual & collective anxiety around legal hold and internal investigations.

Conduct data capture, legal holds, and internal investigations silently, without alerting end users.

Simplify employee offboarding.

Accelerate the offboarding process while eliminating the risk of data loss and the high costs of device quarantines.

Estimate the ROI of modernized legal hold

No business case is complete without a confident estimate of ROI and time to value.

Calculate the expected ROI of a modernized legal hold program leveraging purpose-built endpoint backup:

Evaluate current costs around legal hold

- ✓ Tech costs for current legal hold, backup, data storage, etc.
- ✓ IT costs of time spent on manual device collection
- ✓ Device spend to accommodate device quarantines
- ✓ Lost productivity from device quarantines
- ✓ Spoilation sanctions
- ✓ eDiscovery costs

Estimate savings through streamlined legal hold program

- ✓ Reduced IT costs
- ✓ Reduced device costs
- ✓ Improved end user productivity
- ✓ Reduced/eliminated spoilation sanctions
- ✓ Reduced eDiscovery costs

Calculate ROI

$$\left(\frac{\text{(Total Estimated Annual Savings – Annual Cost of Investment)}}{\text{Annual Cost of Investment}} \right) \times 100$$

= Expected ROI



Transform your **legal hold program**

Visit <https://www.crashplan.com/legal-hold/> to see how CrashPlan drives an automatic, frictionless approach to legal hold, eDiscovery, and data preservation.

