DATA SAFE
SOLUTIONS

COMPARISON OVERVIEW · SEPTEMBER 2026

Process, or outcome?

Two models sit in this market. One certifies that a method ran. The other verifies, on each device, that the data is gone. Everything else follows from that.

	CONVENTIONAL ERASURE PLATFORM	DSS SMART WIPE
Method selection	Chosen in advance by an operator or a configuration, applied across the batch	**Determined by the engine from the individual device, bound per unit**
Operator role	Chooses the method, runs the job, confirms completion	**Starts the job. Nothing else, and no override**
Failure handling	**Substitutes a weaker method and certifies it** 57 of 193 drives in four live erasure reports were certified erased by overwrite Clear after the selected Purge was refused	**Fails closed. Quarantine, remediation or destruction** Certificates carry the field "Fallback allowed: No"
Verification	Confirms the selected method completed, and at best that the addressable area reads clean	**Confirms known data written before the erase cannot be read after it, at the device**
Certificate basis	That a process was executed	**That the data on this device has been rendered irretrievable**
Responsibility	**Sits with the ITAD and the controller. The vendor licence disclaims the outcome**	**Retained by DSS where destruction is successful**

In a conventional platform, correctness depends on human judgement. **In DSS it is enforced by design.**

ONE · THE TECHNICAL MODEL

The decision moves from the human to the device.

Purge is a category, not a command. Cryptographic erase, block erase, SCSI Sanitize, ATA Sanitize and NVMe Sanitize are all Purge-class, and two identical-looking drives in one chassis can take different ones.

CONVENTIONAL

Select, then check

1. A method is selected in advance, by the operator or the configuration.
2. The tool checks the drive supports it.
3. If supported, it runs. If refused, a weaker method is substituted.
4. A pass is recorded either way.

DSS

Interrogate, determine, test, fail closed

1. The engine interrogates the drive: interface, controller, firmware, self-encrypting status.
2. It determines the one correct method for that unit and applies only that.
3. It tests the result at the device, not the return code.
4. If it cannot prove the outcome, no certificate is issued.

	SELECT, THEN CHECK	INTERROGATE, DETERMINE, TEST
What the check can reject	**Only a method the drive cannot run** Plain overwrite is supported on effectively every drive in service, so the safeguard passes precisely when it matters least	**Any method that is not the correct one for that unit**
Same model, different drives	One setting for all On 61 drives of one identical model, all reporting Purge support, the selected Purge did not complete on 57 and completed on 4	**Read individually. The variation is resolved at the drive**
Where the residue goes	Remapped and spare area is outside the method and outside the check Three drives carried remapped sectors under a status of Erased, one of them 2,045	**Reported where readable, made unreadable by key destruction where it is not** The control drive, where the Purge ran, went from 1 remapped sector to 0

A support check confirms the method already chosen is permitted. **It cannot tell you it is the wrong one.**

TWO · OPERATIONAL AND COMMERCIAL

Same rigs. Same drives. Same firmware.

95 drives from four live erasure reports, re-run against the correct method for each device. Nothing else changed.

399h 02m	7h 16m	88 of 95	331
AS RUN	CORRECT METHOD PER DEVICE	WOULD HAVE COMPLETED IN SECONDS	SLOT-HOURS HANDED BACK

	AS RUN	CORRECT METHOD PER DEVICE
Drives finishing in seconds	**0 of 95**	**88 of 95**
Array time per batch	26h 12m, gated by the slowest drive One drive ran 12h 23m and held 28 other slots, most long finished	**c. 3h 36m, hot swap on completion**
Slots locked and idle	**331 slot-hours**	**Zero**
Wipe operations per device	Two on 29.5% of drives, the first producing nothing	**One**
Commercial model	**Volume licences bought up front. On the illustrative basis below, £500,000 committed before a single drive is processed**	**No upfront commitment. Charged in arrears, and only for a successful wipe**
Licence cost of the duplicates	**c. £147,500 a year** Illustrative basis: 250,000 devices a year at £2 a wipe, applying the observed 29.5% duplicate rate. Substitute your own volume and rate, the arithmetic is the same	**£0**
Drives a failed Purge condemns	Written off to destruction, resale value lost	**Recovered to resale by correct selection**

This is not a faster command. Two tools issuing the same firmware command take the same time. **The entire difference is correct per-device method selection.**

THREE · ASSURANCE AND COMMERCIAL POSITION

What the certificate is worth when it is tested.

	CONVENTIONAL ERASURE PLATFORM	DSS SMART WIPE
Certificate states	That a process was executed	**That the data on the identified device is irretrievable**
Warranty	**None. Software supplied as is, certificates descriptive only**	**Outcome warranted at clause 5.1, with nothing contradicting it**
Liability for data loss	**Excluded or capped at fees paid**	**Uncapped for the outcome, clause 17.1**
Insurance response	None behind the certificate	**£10m Technology Professional Indemnity, each and every claim, and £10m Public and Products Liability** The standard inefficacy exclusion is deleted by endorsement, so the cover responds to the destruction having failed
Failure record	Reported as completed unless an error is detected	**Recorded as an attempt, with no warranty and no charge**
Resale impact	Drives the tool cannot handle are condemned	**Correct selection recovers them, released in seconds**
Independent assessment	Assurance level assessed once, as a process	**ADISA Product Assurance Level 5. Fallback is not permitted under the certification**
Protection	A settings change any competitor can copy	**The integrated per device chain is patented and published, GB2638704**

Proven

The outcome is tested at the device, not inferred from a return code

Warranted

The licence accepts uncapped liability for that outcome

Insured

£10m and £10m of cover, the professional indemnity each and every claim, with the standard inefficacy exclusion deleted by endorsement

A conventional certificate does not protect the ITAD if data is later recovered. **A DSS certificate is built to.**

TEST IT

Do not take our word for it. Take your own drives.

Every figure in this document came out of ordinary erasure reports. You can produce the same comparison on your own floor, and you do not need us to interpret it.

1

Run 100 drives through your current system.

Your rigs, your firmware, your operators, your normal configuration. Change nothing.

2

Run the same 100 drives through ours.

The same devices, not a second sample, so it is a true device by device match.

3

Compare them yourself.

Purge match rate, verified outcomes, drives recovered rather than condemned, and throughput.

You keep the results, whichever way they fall. There is no upfront commitment, no rip and replace, and nothing to unpick if you walk away. The OpenAPI and XML interfaces are already built.

Proof, not promises.

Data Safe Solutions Ltd
2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY
0151 440 3200 · hello@datasafe360.com · datasafe360.com
VAT 425206721 · Company 12245066