PastWipe

BRIEF FOR PROCUREMENT AND LEGAL TEAMS

Post-breach data control for enterprise and government

PastWipe™ reduces the usable value of stolen or exfiltrated data outside approved conditions, using policy, cryptographic validation, identity and device context, and evidence records. It complements existing security tools rather than replacing them.

What PastWipe is

When data is duplicated, leaked or exfiltrated, organisations need more than perimeter security and incident response. PastWipe is built on one principle: **protected data should not be treated as permanently trusted merely because access was valid when it was first obtained.**

- **Applies policy** to selected protected data: purpose, identity, device, environment and time conditions.
- **Validates at the point of use** before content is released, rendered or accepted.
- **Records the decision** as evidence for technical, legal, compliance and insurance review.

What PastWipe is not

- Not a replacement for prevention, detection or response tools
- Not a guarantee that data will never be stolen or copied
- Not a reputation-management, PR or "content removal" service
- Not a search-engine deletion service

> RepSec™ is an optional protocol framework for expressing policy, validation and evidence across participating systems. PastWipe does not depend on it.

How it works

1 Protect
Start with selected data where post-breach misuse would cause material harm: customer records, regulated files, contracts, intellectual property, sensitive exports.

2 Attach policy
Define when data may be opened, validated, rendered, transferred or relied upon: purpose, identity, device, environment, time.

3 Evaluate
Before protected content is released, rendered or accepted, check whether current conditions still satisfy the policy.

4 Enforce and record
Allow, deny, restrict or degrade, and create an evidence record of what was requested, evaluated and decided.

If an incident is declared, a device or identity is no longer trusted, or a policy changes, subsequent requests are evaluated against the new state. Controls can be scoped to the affected data, workload or environment so that unaffected operations continue.

Deployment

- Deployed **on-premises, in hybrid environments or in the customer's own cloud account**, next to the systems that hold the selected protected data.
- **Not a shared, multi-tenant hosted service.** Evaluation environments are set up per customer.
- Works with the organisation's own key-management systems; keys stay under the client's control (KMS, HSM or equivalent).
- **Identity:** enterprise identity providers supply identity signals.
- **Monitoring:** evidence records and control events can be streamed to SIEM/SOAR.
- **Storage, applications and APIs:** connectors for selected systems; APIs for embedding policy checks. Named products and connectors are confirmed per evaluation.

Enforcement scope

- Enforcement covers protected data used through supported, policy-aware workflows, alongside prevention and detection controls.
- Photographs, screenshots and manual retyping by an authorised viewer, and copies that have already become independent plaintext, are outside technical enforcement.
- Coverage across legacy, offline and third-party workflows is defined for each deployment.

Data handling

Client-controlled data and keys

- Client data remains in the client's own infrastructure, cloud account, virtual private cloud or approved trusted environment.
- Encryption and decryption take place inside that client-controlled environment.
- PastWipe does not require access to client plaintext, client decryption keys or the underlying protected information.
- Residency and processing locations are agreed in writing before processing starts. UK incorporation of PastWipe Ltd is not a promise of UK-only processing.

During an evaluation

- No production data is needed. Synthetic or representative data is preferred; the scope records any real data, its location and who can access it.
- Key arrangements for each evaluation are written into its scope.
- At the end, evaluation environments and any customer data in them are returned or deleted as agreed, with written confirmation on request.
- Security, architecture and data-handling documentation is shared during scoping, under NDA where needed.

Evidence records

Each control decision can be recorded: **what** was requested (protected object and operation), **who or what** requested it (user or workload identity, device or environment context), **what was evaluated** (policy, declared purpose, security state), **what happened** (permitted, denied, restricted or degraded) and **when**. Records use signatures for integrity, timestamps and tamper-evident logs that can be streamed into existing SIEM and audit systems.

> Evidence covers decisions made within supported, policy-aware workflows. No claim is made that a record is automatically admissible in court, sufficient for a regulator or insurer, or proof that every copy of information has become unusable. References to laws and frameworks describe how PastWipe supports and maps to those obligations; compliance decisions remain with your organisation.

Evaluation process

A controlled evaluation tests whether PastWipe reduces the usable value of stolen or exfiltrated data **for a defined data class, within a defined workflow, under measurable operating conditions**.

1. Scope	One or two priority data flows; expected users, systems and consequences of unauthorised reuse; success criteria agreed before anything is deployed.
2. Conditions	Which identity, device, environment and attestation signals are available and trustworthy; online, offline, legacy and third-party dependencies; failure and recovery behaviour.
3. Deploy	Alongside your stack, integrated with existing identity, monitoring and key-management systems. Nothing is ripped out or replaced.
4. Test	Authorised use, attempted misuse and simulated exfiltration; a change in security state and controlled restoration of legitimate access.
5. Evidence and review	Outcomes, false-positive and availability impact, evidence records and a final evidence pack for security, legal, compliance and insurance review, with an agreed recommendation on next steps.

Duration and commercial terms are agreed during scoping. Nothing is deployed and no data is shared until the scope is agreed in writing. **What to bring:** a sponsor from security (ideally also risk, legal or compliance), one or two candidate data flows, and access to test environments and the relevant identity and monitoring systems.

Contact

Enquiries	info@pastwipe.com · pastwipe.com/contact
Procurement pack	pastwipe.com/contact/?topic=procurement
Trust Centre	pastwipe.com/trust
Security reports	info@pastwipe.com, subject "Security report"
Legal entity	PastWipe Ltd, registered in England and Wales. 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom
Official channels	pastwipe.com, portal.pastwipe.com, @pastwipe.com email

PastWipe™ and RepSec™ are trademarks of PastWipe Ltd. This brief summarises pastwipe.com; scope-specific terms are agreed in writing.