Internet-Draft
Intended status: Informational
Expires: October 2026

R. Ehlers
PastWipe Ltd

April 2026

RepSec: Post-Breach Data Neutralisation Protocol
draft-ehlers-repsec-01

Abstract

This document introduces RepSec, a post-breach data neutralisation protocol designed to reduce the utility of exfiltrated or unauthorised data copies. RepSec operates independently of traditional perimeter and access-control security models by enforcing conditional data usability based on attestation and environmental integrity. The goal is to limit downstream exploitation, resale value, and operational impact of compromised data without disrupting legitimate use.

1. Introduction

Traditional cybersecurity architectures focus on preventing unauthorised access to data. However, once data has been exfiltrated, copied, or otherwise exposed, existing controls provide limited mechanisms to govern its subsequent use.

This document defines a conceptual framework for post-breach data control, where the objective shifts from access prevention to sustained control over data usability after exposure.

RepSec introduces a protocol model that enables data to become conditionally usable based on verifiable environmental and contextual factors.

2. Problem Statement

Current security models assume that data, once accessed, remains inherently usable. This assumption creates a structural gap:

- Exfiltrated data can be reused indefinitely
- Data resale markets retain economic value
- Insider threats bypass perimeter controls
- Encryption protects transport and storage, not post-theft use

As a result, organisations face persistent risk even after detection, containment, and remediation.

3. Design Goals

RepSec is designed with the following objectives:

- Post-exposure control: Maintain influence over data usability after loss
- Environmental binding: Restrict data function to approved contexts
- Low operational overhead: Avoid significant latency or workflow disruption
- Compatibility: Operate alongside existing security infrastructure
- Auditability: Provide verifiable evidence of data state and access conditions

4. Architectural Overview

RepSec operates as a data-centric control layer that introduces conditional execution semantics to protected data objects.

At a high level, the system includes:

- Data objects with embedded or associated control logic
- An attestation mechanism validating execution environment integrity
- A policy framework governing permitted usage conditions
- A response mechanism that degrades or invalidates data outside approved parameters

The protocol does not require modification of underlying storage systems but instead overlays a control plane governing data usability.

5. Operational Model

Under RepSec, data access is evaluated dynamically at the point of use.

Example flow:

1. A data object is requested for use
2. The execution environment is assessed against defined policies
3. If conditions are satisfied, full functionality is granted
4. If conditions are not satisfied, data is degraded, restricted, or rendered unusable

This model ensures that possession of data does not guarantee its utility.

6. Security Considerations

RepSec addresses several threat vectors:

- Data exfiltration and resale
- Insider misuse
- Unauthorised duplication
- Long-term exploitation of archived stolen data

The protocol assumes that adversaries may obtain full data copies and focuses on reducing their ability to derive value from them.

Detailed implementation strategies, including cryptographic methods and enforcement mechanisms, are outside the scope of this document.

7. Performance Considerations

RepSec is designed to minimise performance impact by:

- Performing lightweight attestation checks
- Avoiding full system re-architecture
- Operating at the data interaction layer rather than network layer

Specific performance characteristics depend on deployment context.

8. Interoperability

RepSec is intended to integrate with:

- Identity and access management systems
- Data loss prevention tools
- Endpoint detection and response platforms
- Existing encryption and key management systems

The protocol complements rather than replaces these controls.

9. IANA Considerations

This document makes no requests of IANA.

10. References

[1] Zero Trust Architecture, NIST SP 800-207
[2] Data-Centric Security Concepts, Various Sources

Author’s Address

Ralph Ehlers
PastWipe Ltd
Email: contact@pastwipe.com