Verifiable Digital Trust

A New Security Framework for the Modern Gaming Ecosystem

Traditional security models fail in dynamic, collaborative environments like RuneFrameOS. A new paradigm is needed—one built on a foundation of verifiable trust, where security is a core feature, not a background function. This requires a shift to a data-centric model grounded in Data Provenance and Data Attestation.

The Two Pillars of Verifiable Trust

Data Provenance and Data Attestation are the foundational concepts that enable a system to prove its own integrity and the history of its data.

Data Provenance: The Pedigree of Data

Provenance provides a complete, historical record of a data asset's lifecycle, answering *who, what, when, where,* and *why*. It's distinct from Data Lineage, which only tracks the data's path. Provenance establishes authenticity and trustworthiness, which is critical for managing user-generated IP.

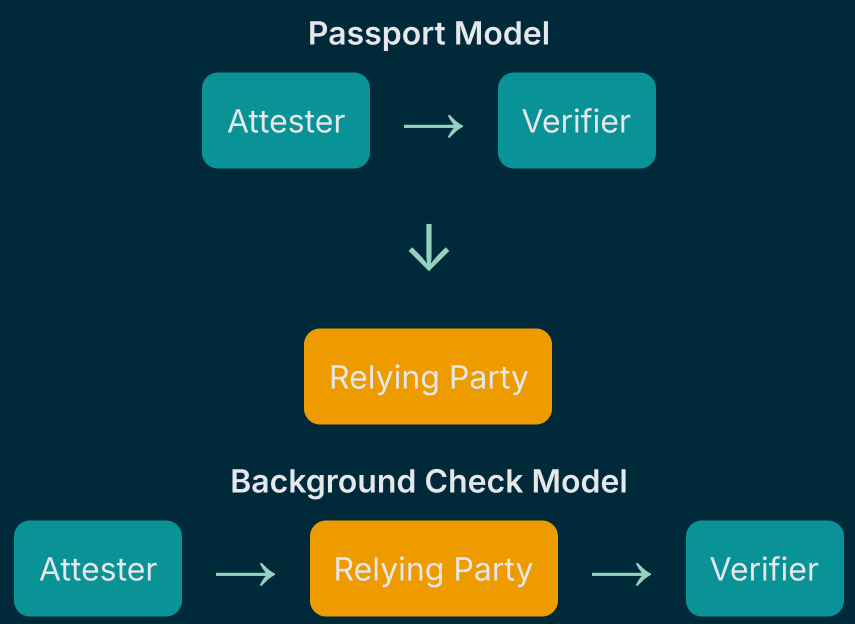
Feature	Data Lineage	Data Provenance
Question	How did it get here?	Where did it come from?
Focus	Path & Transformation	Origin & Authenticity

Feature	Data Lineage	Data Provenance
Analogy	Package Shipping Tracker	Artifact's Chain of Custody

Data Attestation: The Act of Verification

Attestation is the active process of proving integrity and identity in real-time. It functions like a digital notary, using cryptographic evidence to allow a system to verify the trustworthiness of a client or another service before granting access. This is the key to privacy-preserving anti-cheat systems.

Attestation Models


Passport Model

Background Check Model

Securing the Software Supply Chain

A Software Bill of Materials (SBOM) provides provenance for the code itself, creating a transparent inventory of all components and dependencies.

Driven by federal mandates like EO 14028, SBOMs are becoming the industry standard for software transparency. They are not the "recipe" of your IP, but the "ingredient list," essential for vulnerability management and license compliance. For RuneFrameOS, embracing radical transparency by publishing an SBOM is a competitive advantage.

Format	Maintainer	Primary Use Case
SPDX	The Linux Foundation	Broad-spectrum transparency, license compliance, and vulnerability management.
CycloneDX	OWASP	Lightweight and security-focused, designed for identifying risk in the supply chain.
SWID Tags	ISO/IEC	Software asset management and tracking installed software on endpoints.

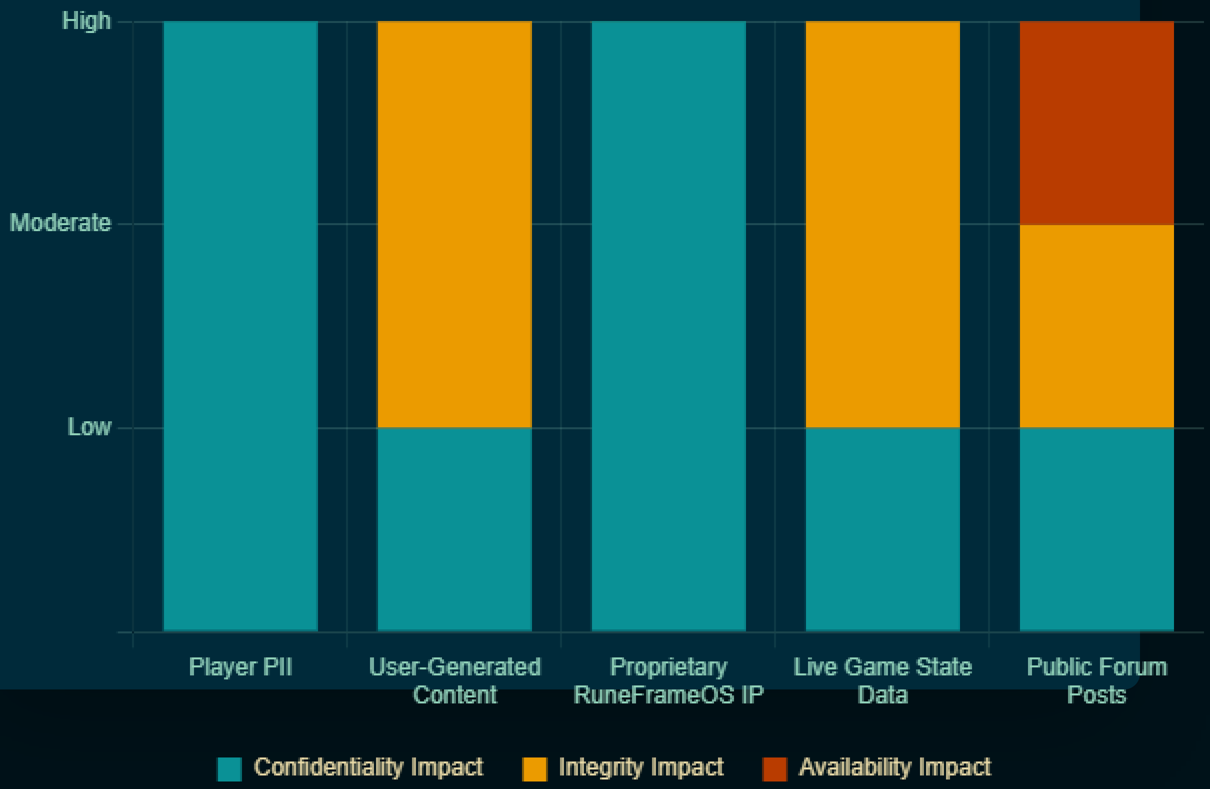
84.7%

of enterprises experienced data loss in 2023.

Traditional Data Loss Prevention (DLP) fails because the perimeter is gone. Security must be attached to the data itself.

Data Classification: The Prerequisite for Protection

Before data can be protected, it must be understood. Using the NIST FIPS 199 framework, we classify data based on the potential impact of a breach on its Confidentiality, Integrity, and Availability. This allows for a nuanced, risk-based approach to security.



The Unifying Framework: Data-Centric Zero Trust

Zero Trust isn't just about networks; it's a philosophy that must be applied directly to data. Every access request is treated as hostile until proven otherwise, using provenance and attestation as evidence.

Verify Explicitly

Never trust, always verify. Authenticate and authorize every single access request based on all available signals—identity, device health, data classification, and more.

🔑

Use Least Privilege

Grant users and systems only the minimum access required to perform their function, using just-in-time and just-enough-access policies to shrink the attack surface.

💥

Assume Breach

Design the system assuming a breach will happen. Minimize the blast radius with micro-segmentation, end-to-end encryption, and continuous monitoring.

A Phased Implementation Roadmap for RuneFrameOS

A full transition to Data-Centric Zero Trust is a journey. This phased approach builds value incrementally.

Phase 1: Foundational (0-6 Months)

Conduct comprehensive Data Classification using NIST framework. Integrate automated SBOM generation into the CI/CD pipeline and mandate it from suppliers.

Phase 2: Provenance & Attestation (6-18 Months)

Build a UGC provenance system to protect creator IP. Implement client attestation for "trusted" lobbies and server attestation for critical backend services in TEEs.

Phase 3: Data-Centric Zero Trust (18+ Months)

Deploy a central Policy-as-Code engine. Refactor critical data access to require real-time policy checks. Log all decisions for continuous monitoring and refinement.

Infographic based on the research paper: "Verifiable Digital Trust: A Strategic Framework for Data Provenance, Attestation, and Security in the Modern Gaming Ecosystem."