RitAPI

Soverign by Design

API Protection with Data Independence

IT Security is
Our Main Concern

Sydeco

Introduction

In a world where competitive advantage depends on trust and control, digital sovereignty has become essential for every organization. The ability to define your own digital destiny—managing your data, infrastructure, and governance on your terms—is no longer optional. This sovereignty is crucial for several reasons:

- **Compliance with Local Data Laws**: Nations worldwide are enacting stringent data protection regulations. Operating locally ensures that sensitive data is managed according to regional laws, avoiding complex cross-border legal challenges.
- **Building Trust**: Customers and citizens are increasingly aware of how their data is used. By processing data locally and ensuring it never leaves a trusted boundary, organizations can build a foundation of transparency and trust.
- **Ensuring Independence**: Relying on external, cloud-based services for critical security functions creates dependencies that can be disrupted by geopolitical shifts, network outages, or unilateral changes in terms of service. A sovereign solution guarantees operational continuity, independent of external factors.

RitAPI is engineered from the ground up to deliver API security with data independence, putting you in complete control of your digital assets.

Deployment Models

RitAPI offers flexible deployment models to fit any infrastructure strategy, ensuring that your API security layer resides exactly where you need it. All models are designed to be fully self-contained.

- **On-Premises Appliance**: A physical or virtual appliance deployed directly within your data center. This model offers the highest level of physical control and isolation, ideal for legacy environments or organizations with strict hardware security mandates.
- **Private Cloud (VMware / OpenStack)**: Deployed as a virtual machine within your private cloud environment. This leverages your existing virtualization infrastructure, combining the scalability of the cloud with the security of a private network. It integrates seamlessly with orchestration tools like VMware vSphere or OpenStack.
- **Edge (Kubernetes)**: Deployed as a containerized application within a Kubernetes cluster. This model is perfect for modern, cloud-native architectures, enabling you to deploy API protection at the network edge, closer to your users and services, for minimal latency and maximum scalability.

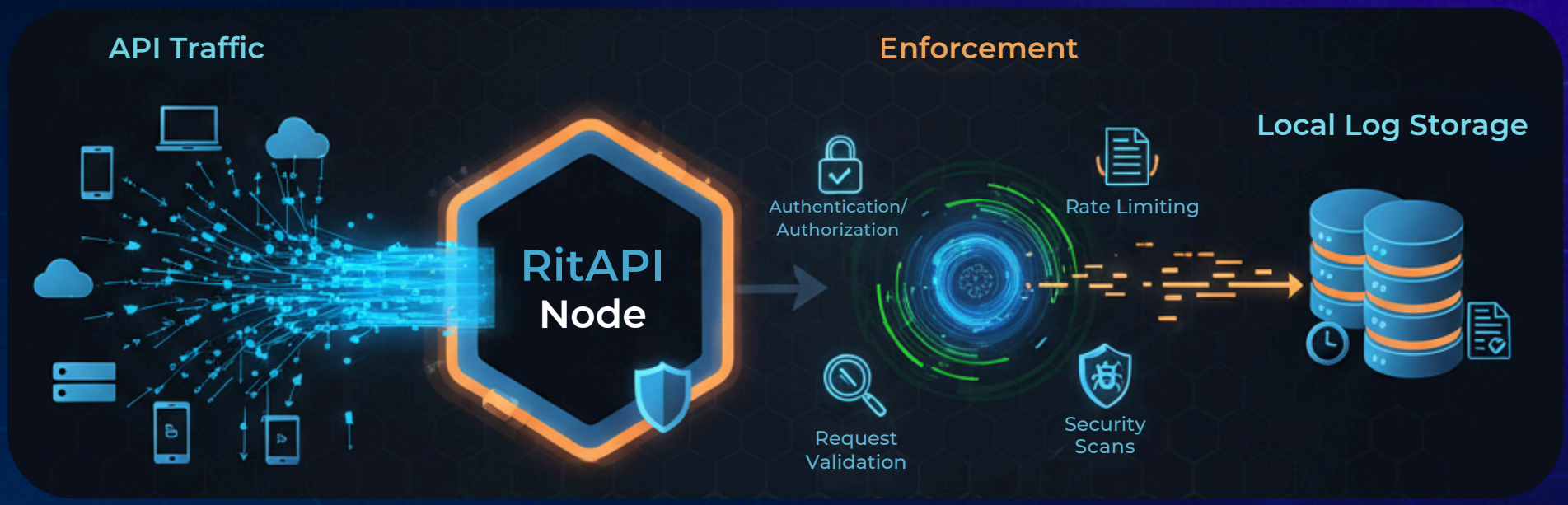
Key Features

RitAPI's feature set is purpose-built to enforce sovereignty and ensure robust, independent operation.

- **Offline Mode**: RitAPI is designed to function indefinitely without an internet connection. All policy enforcement, analytics, and logging occur locally on the node. This "air-gapped" capability is critical for secure, sensitive environments where external connectivity is a risk.
- **Local Data Residency**: All data—including API request logs, analytics, and configuration—is stored and processed exclusively on the deployed instance. No data is ever transmitted to an external cloud service, guaranteeing that you maintain 100% control and meet data residency requirements.
- **Signed Update Bundles**: Software updates are delivered as cryptographically signed packages. The system verifies the signature before applying any update, ensuring the integrity and authenticity of the code and protecting against supply chain attacks.

Architecture Diagram

The RitAPI architecture is designed for simplicity and efficiency, ensuring that all processing remains within your sovereign control.



In this model, the RitAPI node acts as a secure gateway. It inspects every incoming API call, enforces the security policies you define, and logs the transaction locally. At no point in the process does data leave the node or your controlled environment.

Update Mechanism

Maintaining security requires timely updates, but these must not compromise the system's sovereign nature. RitAPI uses a secure, offline-first update process.

1. **Package Delivery**: Updates are provided as standard Debian packages (`.deb`). These bundles contain all necessary binaries, libraries, and configuration files.
2. **Proprietary Verification**: Each update package requires validation through a custom-built verification program. This program checks the integrity and authenticity of the package using a unique combination of device-specific information, such as its serial number and a pre-issued validation token. This verification step is mandatory and ensures that only authorized updates are installed on a specific device. This is a proprietary mechanism and does not use standard cryptographic encryption.
3. **Atomic Installation**: If the verification is successful, the package manager proceeds with the update. This process is atomic, ensuring the system remains in a consistent state.

This mechanism allows for secure updates even in fully air-gapped environments, where the package file can be transferred via a secure physical medium.

Compliance Mapping

RitAPI's sovereign architecture directly supports compliance with major data protection regulations by design.

Regulation	RitAPI Feature Alignment
GDPR (General Data Protection Regulation)	Local Data Residency and Offline Mode ensure that personal data from EU citizens is processed within a defined boundary, satisfying data transfer and processing requirements.
Indonesian PDP Law (UU No. 27 of 2022)	By deploying On-Premises or in a Private Cloud within Indonesia, organizations can meet the law's requirements for local data processing and prevent unauthorized cross-border data transfer.
HIPAA (Health Insurance Portability and Accountability Act)	The Offline Mode and Local Data Residency features provide technical safeguards to ensure that Protected Health Information (PHI) is contained within a secure, controlled environment, preventing unauthorized access or disclosure.