

SmartDefense

Digital finance integration and unified command and control

SmartDefense is AI DIGIMARKET's product family for connecting digital identity, institutional systems and operational information through explicit authorization, intelligent workflows and auditable human decisions.

Two editions address distinct needs: SmartDefense Finance coordinates identity and transaction workflows for tokenized assets; SmartDefense Command brings operational information and response teams into a unified command and control environment.

Two editions with one shared foundation

	SmartDefense Finance	SmartDefense Command
Purpose	Digital monetary and tokenized asset integration	Situational awareness and coordinated response
Customers	Banks, asset issuers, tokenization platforms and payment providers	Government agencies, emergency services and infrastructure operators
Primary workflow	Verify participants, check eligibility and track transaction outcomes	Validate incidents, assign responders and track resolution
Future expansion	Approved CBDC interfaces and additional asset and payment networks	Additional operational systems and authorized interagency coordination

Connect systems while preserving institutional authority

The shared core provides identity and access services, policy evaluation, integrations, workflow management and audit records. Each edition applies these services to its own customer workflows and data environment.

A practical path to deployment

Begin with one defined use case and a focused assessment. Validate the workflow in a controlled prototype, agree measurable pilot outcomes, then expand through reusable integrations and licensed software modules.

Product status: proposed capabilities and development roadmap. Availability and integration scope are agreed per engagement; this brochure does not represent completed deployments or certifications.

SmartDefense - Finance

Identity and transaction assurance for digital assets

SmartDefense Finance is designed to connect identity providers, tokenized asset platforms, blockchain networks and payment systems. It helps institutions coordinate participant checks, approvals and transaction exceptions in one traceable workflow.

Core capabilities

- Digital identity integration: Validate credentials and associate approved identities with institutional accounts or wallets.
- Authorization and eligibility: Apply configured participation rules, asset restrictions, transaction limits and approval requirements.
- RWA connectivity: Connect tokenized asset records with issuer information, eligibility conditions and lifecycle events.
- Blockchain integration: Read ledger events and interact with supported contract interfaces through controlled adapters.
- Transaction workflows: Coordinate requests, approvals, payment status, asset transfer status, reconciliation and exception handling.
- Audit and AI assistance: Record decisions and policy versions; assist document processing and flag inconsistencies for review.

Example customer workflow

An investor requests a tokenized asset. SmartDefense checks the investor's credentials, approved wallet association and eligibility. It routes exceptions to the responsible team, tracks connected payment and asset systems, and records the final outcome with its supporting evidence.

CBDC as a future capability

Future adapters can connect to approved Central Bank Digital Currency infrastructure when access and suitable interfaces are available. The initial edition can work with existing payment integrations or simulators. Central banks and payment operators retain issuance and settlement authority.

Settlement coordination depends on the connected systems and their finality rules. Cross-system atomic settlement is a separately validated capability, rather than an assumed result of connecting two ledgers.

First pilot and intended value

Start with one asset class, jurisdiction, identity provider, blockchain and payment interface. Measure onboarding time, manual interventions, unresolved transaction exceptions and audit preparation effort. The intended value is less manual coordination and clearer operational accountability.

RWA tokens represent rights defined by the underlying legal and operational arrangements. Institutions remain responsible for those arrangements and the rules configured in SmartDefense.

SmartDefense - Command

Unified command and control for authorized operations

SmartDefense Command is designed to connect approved operational feeds, incident systems and response teams in a common workspace. It supports situational awareness, incident assessment, resource coordination and documented human decisions.

Core capabilities

- Unified operational dashboard: View incidents, alerts, resources and system status across approved sources.
- GIS and mapping: Locate incidents, relevant infrastructure and authorized response resources.
- Operational integrations: Connect approved cameras, sensors, access control, incident management and emergency service interfaces.
- AI and computer vision: Assist defined detection and review tasks, such as smoke indicators or restricted area entry alerts.
- Incident and response workflows: Classify and escalate incidents, assign tasks, record acknowledgments and track progress.
- Evidence and accountability: Preserve source references, operator actions, approvals and incident timelines.

Example customer workflow

A sensor reports an incident at a facility. SmartDefense displays the location and relevant feeds. An operator validates the alert, assigns responders and tracks their progress. The team records the resolution and completes an auditable incident history.

Human authority within the workflow

AI alerts support operator assessment. Operational control functions are enabled only through explicitly approved integrations and permissions. Access is bounded by role, institution, purpose and scope; sensitive actions require the configured approval process.

The intended use is a defined and authorized operational environment. Privacy controls, retention rules and access logging form part of each deployment design.

First pilot and intended value

Begin with one facility, campus or infrastructure operator, a limited set of feeds, a map and an incident workflow. Measure alert triage time, task acknowledgment time, incident handoff quality and completeness of the response record.

The intended value is a more coherent operational picture and better coordination across teams and existing systems.

Technology and engagement

Reusable engineering with separately governed operations

Six technology domains

Technology	Role in the SmartDefense family
Digital ID	Credential verification, user authentication and identity context for authorization.
RWA tokenization	Connections to defined asset rights, participant eligibility and asset lifecycle events in Finance.
Blockchain	Optional ledger and smart contract connectivity for supported digital asset workflows.
CBDC	Future Finance adapters for institutionally approved digital currency interfaces.
AI and computer vision	Document processing, anomaly analysis and defined visual detection tasks with human review.
Software engineering	APIs, databases, dashboards, testing, monitoring, backups and recovery that underpin both editions.

Shared core with separate data controls

Both editions reuse identity and access services, authorization policies, connectors, workflow services, AI services and audit components. They can be sold and deployed independently.

Shared technology does not grant shared access to information. Finance and Command maintain separately governed data and permissions. Any exchange between them requires a defined purpose, appropriate authority and explicit access controls.

Start with a focused assessment

Proposed discovery engagement: 100 hours at USD 100 per hour, totaling USD 10,000. Select one edition and one priority workflow. Receive a system and stakeholder map, authorization model, integration architecture, risk register, prototype specification and phased roadmap.

Prototype development, production integrations, external services and licensing are scoped separately. Subsequent commercial engagements can combine implementation, an annual platform license, optional connectors and ongoing support.

Discuss your SmartDefense use case

AI DIGIMARKET LLC, USA | aidigimarket.com/smartdefense

Brochure version 2.0 | October 2026 | Finance and Command editions