



SensAI Gateway

Integrity Intelligence for high-stakes access, screening and decision workflows

WHITE PAPER

Identity tells you who someone is.

Gateway adds real-time Integrity Intelligence before trust, access or authority is granted.

SensAI Gateway is a contact-free, video-based screening and orchestration layer designed to integrate into existing operational processes. It supports rapid, contextual interactions and produces analytical indicators that help organizations decide who can proceed, who requires additional questions, and where human attention should be focused.

The core idea

Do not add another universal checkpoint. Add a new intelligence layer to the decision point that already exists.

October 2026 | SensAI Veritas

Executive Summary

Modern security and access systems are increasingly effective at establishing identity, validating credentials, checking permissions and comparing people or transactions against known-risk information. Those capabilities are essential, but they do not answer a different operational question: does this specific interaction contain signals that justify additional attention?

SensAI Gateway is designed to add that missing layer. Using standard video during a brief, contextual interaction, Gateway analyzes multiple physiological signal patterns and produces real-time analytical indicators for integrity assessment and risk routing. It is contact-free and designed to fit the workflow an organization already operates.

Gateway is not a replacement for identity, biometrics, watchlists, physical security or trained personnel.

It is an additional Integrity Intelligence layer that can help determine what should happen next.

Five operating principles

- Fast enough to fit operational workflows rather than create a new investigative process.
- Contact-free and compatible with standard video acquisition.
- Integrated into existing access, screening, vetting or secondary-review processes.
- Designed for progressive routing: most people continue; a smaller population receives additional scrutiny.
- Human-controlled: the deploying authority defines questions, thresholds, policies, escalation rules and final actions.

What Gateway changes

Gateway shifts the question from “How do we screen everyone more deeply?” to “How do we identify the small fraction of interactions that justify deeper attention, while allowing the majority to move quickly?”

1. The Missing Layer Between Identity and Trust

High-stakes organizations increasingly operate with sophisticated identity and access technology. Digital identity, biometrics, credential validation, authorization engines, watchlists and physical-security systems can answer critical questions.

Existing layer	Primary question	What remains unresolved
Identity / biometrics	Who is this person?	Identity does not establish present intent.
Authorization / credentials	May this person proceed?	Permission does not eliminate situational risk.
Watchlists / intelligence	What is already known?	Unknown or first-time risk may not exist in a database.
Physical security	Is a prohibited object or anomaly present?	It does not assess the person's physiological response to contextual questions.
Human interview	Does this case warrant concern?	High-value, but difficult to apply at population scale.

The operational gap is therefore not identity. It is the lack of a scalable, real-time information layer about the interaction itself. Gateway is designed for that gap.

Identity establishes who someone is. Integrity Intelligence helps assess whether the interaction warrants additional attention.

The two layers are complementary, not competitive.

2. What SensAI Gateway Is

SensAI Gateway is a software-led screening and orchestration product for controlled environments where an organization must decide whether to grant access, continue a process, ask more questions or refer a case for human review.

Core characteristics

- Standard video: operates from conventional camera input or a dedicated kiosk configuration.
- Contact-free: no physical sensor, wearable or wired connection to the subject.
- Real-time: indicators are produced while the interaction is taking place.
- Brief interaction: designed for short operational screening rather than a full investigative interview.
- Contextual questioning: the organization controls the questions and aligns them to the operational objective.
- Flexible deployment: can support on-premise, cloud, online and offline architectures according to the deployment environment.
- Workflow integration: intended to connect to the client's existing process rather than require a separate operational universe.
- Orchestration: can trigger routing, additional questions, human review or downstream system actions according to configured policy.

The kiosk is an interface, not the product definition

Gateway can be delivered through a dedicated kiosk with an avatar or other guided interface, but its strategic value is broader than the kiosk. The product is the Integrity Intelligence and orchestration layer: the ability to conduct a short interaction, analyze physiological response patterns, and feed the result into an existing decision process.

3. How Gateway Works

Gateway combines a brief contextual interaction with contact-free physiological analysis from standard video. The system analyzes multiple signal families and produces analytical indicators that can be associated with elevated response, potential deception, hidden risk or ill intention. The output is used as decision support and routing intelligence, not as a standalone legal or factual determination.

Stage	Function	Operational meaning
1	Context	The organization defines the purpose, population, questions and operational thresholds.
2	Interaction	The subject answers a small set of contextual questions through a kiosk, avatar or integrated interface.
3	Video physiology	The system extracts and analyzes multiple contact-free physiological signals while compensating for operational variability within validated limits.
4	Integrity indicators	Gateway generates real-time analytical indicators linked to the interaction and relevant topics.
5	Routing	Configured business rules determine whether the person continues, receives additional questions or is referred for human review.

Signal quality matters

Gateway is designed to be flexible with real-world testing conditions, including normal movement and lighting variation, but every optical measurement system has operating limits. If signal quality is insufficient, the correct system behavior is to avoid presenting a misleading result and follow the configured fallback path, such as retrying under improved conditions or referring the case to the conventional process.

4. From Universal Screening to Progressive Risk Routing

The most scalable deployment model is a funnel. High-throughput, low-friction processes handle the broadest population. Additional interaction and human attention are reserved for progressively smaller groups when risk indicators justify it.

The objective is not to subject everyone to the deepest assessment.

The objective is to use new information to allocate deeper scrutiny more intelligently.

Broad population	Identity, authorization and existing controls
Selected interaction	Short Gateway screening
Elevated / uncertain cases	Additional questions or configured checks
Narrowest segment	Human-led secondary review or specialist intervention

Why the funnel matters

- It preserves throughput by keeping the initial interaction short.
- It treats trained human attention as a scarce resource.
- It allows the organization to define different escalation thresholds for different populations and scenarios.
- It provides a path for low-risk interactions to clear quickly instead of increasing friction for everyone.
- It makes Gateway compatible with existing screening architecture rather than forcing a wholesale process redesign.

5. Representative Use Cases

Gateway is designed as a configurable platform rather than a single-purpose checkpoint. The same architecture can be adapted to different high-stakes environments by changing the questions, workflow, routing logic and integration points.

Environment	Gateway role
Border and immigration	Add a brief Integrity Intelligence layer before, during or after identity and admissibility processing; route selected cases to existing secondary procedures.
Aviation and safety-critical workforce	Use short, contextual screening at defined risk-sensitive moments for personnel with access to aircraft, secure zones or other safety-critical functions.
Prisons and corrections	Support controlled access, visitor screening, staff screening or contraband-risk workflows where fast triage can focus limited investigative resources.
Critical infrastructure	Add a person-centric risk layer to secure facilities, energy, defense, data centers, ports and other environments where valid credentials alone may be insufficient.
Law enforcement and public safety	Use Gateway for rapid pre-screening or triage before a fuller investigator-led process when operational scale makes a full interview impractical for everyone.
Workforce integrity and sensitive roles	Support defined pre-employment, re-vetting or high-trust access workflows, subject to applicable employment, privacy and AI regulation.
Financial / KYC and high-risk transactions	Introduce a contextual Integrity Intelligence interaction at selected high-risk stages rather than applying deeper review to every customer or transaction.
Other secure-access environments	Deploy wherever an organization must decide whether a person should proceed, receive additional questions or be referred for closer review.

6. Integration and Deployment Architecture

For Gateway, deployment architecture is as important as sensing performance. The strongest model is not a standalone SensAI process. It is a new information layer inserted at the point where the customer already makes a decision.

Integration options

- Dedicated Gateway kiosk with camera, guided interface and local peripherals.
- Existing kiosk or eGate environment where video and interaction can be integrated into the current user journey.
- Desktop or workstation flow used by an operator or investigator.
- API or orchestration connection into an existing case-management, access-control or risk engine.
- Central command-and-control and reporting through the broader SensAI platform architecture.

Deployment considerations

Dimension	Configuration choices
Hosting	On-premise, cloud or hybrid according to security and sovereignty requirements.
Connectivity	Online or offline architecture according to operational constraints.
Interface	Avatar, guided questions, operator-led interaction or embedded client UX.
Policy	Customer-defined questions, thresholds, routing logic and fallback procedures.
Data	Retention, minimization and access controls aligned with applicable law and client policy.
Scale	Single node, multi-site deployment or enterprise orchestration.

7. Scientific and Technical Foundation

SensAI's platform uses remote physiological sensing from video to analyze multiple signal families associated with autonomic and cardiovascular response. The technical approach is designed around multi-signal analysis rather than relying on one isolated measurement.

Signal families may include

- Heart rate and heart-rate variability patterns.
- Blood-flow and capillary color variation derived from remote photoplethysmography (rPPG).
- Cardiovascular mechanical dynamics derived from remote ballistocardiographic methods (rBCG).
- Respiratory and oxygenation-related indicators where signal quality supports measurement.
- Cross-signal temporal features and response changes associated with specific topics or moments in the interaction.

Operational robustness requires more than signal extraction. The system must also address camera geometry, movement, illumination changes, subject variability and signal-quality thresholds. Gateway therefore treats measurement quality as part of the decision logic rather than assuming a valid result is always available.

A scientific instrument should know when not to answer.

When acquisition quality falls outside validated operating conditions, the workflow should use a retry or fallback path rather than force an interpretation.

8. Governance, Validation and Human Control

Integrity-related systems operate in sensitive decision environments. Technical performance alone is not sufficient. A responsible deployment requires explicit governance, validation and clear limits on how the output is used.

Deployment principles

- Purpose limitation: define the precise screening objective and permitted use of the indicators.
- Human control: final decisions and consequential actions remain governed by the deploying authority and its personnel.
- Proportionality: use the least intrusive process consistent with the security or integrity objective.
- Workflow clarity: predetermine what happens when an indicator is elevated, ambiguous or unavailable.
- Environmental validation: test real lighting, camera position, movement, noise and operational conditions.
- Population validation: evaluate performance across the populations relevant to the deployment.
- Data minimization: collect and retain only what is required for the defined purpose and applicable law.
- Auditability: preserve sufficient records to understand system contribution and downstream routing.
- Fallback paths: maintain conventional processing for technical exceptions, accessibility requirements and policy alternatives.
- Cybersecurity and sovereignty: align hosting, access control, logging and data movement with the environment's security requirements.

Gateway should be treated as decision-support instrumentation. Its indicators can strengthen a risk-based process, but should not be represented as infallible proof of truth, deception or intent.

9. Operational Value

Gateway's value is created when a real-time integrity signal changes resource allocation. The relevant business case is therefore not simply "accuracy." It is the combined effect on throughput, escalation quality, human workload and the ability to surface risk that existing identity or database layers may not identify.

Operational KPIs

- Average screening time and total impact on process throughput.
- Percentage of interactions cleared without additional intervention.
- Percentage routed to additional questioning or human review.
- Secondary-review yield and quality of escalations.
- Human time spent per meaningful escalation.
- Technical exception, retry and fallback rates.
- System availability and multi-site operational visibility.
- Auditability and consistency of configured decision workflows.

Scale attention, not friction.

The strategic advantage of Gateway is the ability to reserve deeper scrutiny for fewer, more relevant cases while keeping the broad process fast.

10. Conclusion: From Identity to Integrity Intelligence

The security technology stack has become highly capable at proving identity, validating credentials and finding known risk. The next layer is different: understanding whether the live interaction itself contains signals that warrant more attention.

SensAI Gateway is designed to provide that layer in a form that can operate inside real processes: contact-free, in real time, through standard video, with short contextual interactions and configurable routing.

Its purpose is not to replace the systems already trusted by governments and enterprises. Its purpose is to give those systems and the people operating them new information before a high-stakes decision is made.

Identity tells you who someone is. It does not reveal intent.

SensAI Gateway provides Integrity Intelligence before trust is given.

About SensAI

SensAI Veritas develops Integrity Intelligence technology using contact-free, multi-signal physiological analysis from standard video. Its platform is designed for high-stakes screening, assessment and secure-access environments where organizations need an additional real-time information layer to support human decision-making and risk routing.

www.SensAI-tech.com

Important notice

This white paper describes a technology and deployment framework, not a universal operational or regulatory recommendation. Any deployment should be validated and configured for the applicable legal, privacy, employment, accessibility, security and operational requirements.