STREAMING DEFENSE

Atlas
Features and Capabilities

See what matters.
Understand it. Act.

The Streaming Defense workspace for real-time visibility, investigation and customer-controlled response across IT and OT.

Observe Investigate Analyze Report Validate Manage

Voyager observes. Gluon detects. Atlas explains.

A customer guide to the Atlas interface, operational controls and evidence workflows.

streamingdefense.com 28 November 2026

Contents

1 Atlas: see, investigate and act **3**

1.1 How Atlas fits the platform . . . 3

1.2 One workflow for IT and OT . . . 3

2 Observe: the live operational picture **3**

2.1 Read the label as evidence . . . 4

3 Replay: return to the moment **4**

4 Investigate: explain the finding **5**

5 Analytics and Full Take: search and prioritize **5**

5.1 Preserve the meaning of the selection . . . 6

6 Reports and data: communicate the result **6**

7 Customer-controlled detection and noise management **6**

8 Identity, integrations and Active Defense **7**

9 Private AI, Entities and access **7**

10 Voyager lifecycle and system Health **8**

11 Red Team: prove the operational path **9**

12 A simple analyst workflow **10**

12.1 See it . . . 10

12.2 Understand it . . . 10

12.3 Decide and act . . . 10

12.4 Improve and prove . . . 10

12.5 Get help without leaving Atlas . . . 10

1 Atlas: see, investigate and act

Atlas is the operational workspace for Streaming Defense. It brings live network visibility, explainable evidence, retained search, customer-controlled detections and response workflows into one interface for IT and OT.

Capability	What the analyst can do
Observe	Follow network activity as it arrives. Select a Voyager, inspect an observation and jump from the map to its evidence.
Investigate	Understand what fired, read the supporting observations and provenance, and pass the finding into a configured ticket workflow.
Analytics	Review priorities, changes and relationships. Search retained evidence and produce analyst or executive reports.
Health	Check capture, processing, delivery and storage independently. Separate missing access, stale samples and actual service failures.
Red Team	Run defined validation scenarios and review the recorded results and controls.
Configure	Manage Voyagers, Entities, access, rules, intelligence, identity, private AI and integrations.

How Atlas fits the platform

Voyager captures traffic and extracts supported network facts. Gluon evaluates streaming evidence and publishes detections. Atlas presents the evidence and operational controls. Gluon's sub-millisecond processing measurement is not a browser-rendering or firewall-response timing claim. Customer-authorized downstream automation connects eligible findings to protective action.

One workflow for IT and OT

The same interface connects enterprise activity such as SMB, SSH, RDP and DNS with industrial traffic such as Modbus, DNP3, S7 and OPC UA. Operators can inspect converged networks while keeping Voyager and Entity scope visible.

2 Observe: the live operational picture

Observe combines the Live map, Live Perspective and Observation Inspector. The map provides public geography; the evidence panels also expose eligible private-to-private activity without inventing a geographic location for private addresses.

Capability	What the analyst can do
Live map	Watch delivered observations and connections appear in geographic context. Pan, zoom, center the map and expand the map workspace.
Voyager and direction	Select all permitted Voyagers or one monitoring point. Filter inbound, outbound or unknown direction relative to the observed network.
Live Perspective	Review new flows, wire facts, names, applications and analyst signals. Freeze the view, search recent observations and filter by category or priority.
Focus traffic	Narrow the display with supported traffic conditions. Display filters and routine suppression shape presentation; they do not redefine the underlying captured facts.
Observation Inspector	Select a map indication or record to inspect its endpoints, class, time, protocol/application evidence, scope and related details.
Signal panels	Inspect separate Behavior, Threat intelligence and Sigma groups. Show or hide their lists, reposition panels and follow a selected group into its evidence.
Application and protocol tags	Show available parsed application labels separately from protocol context. A missing application label stays blank rather than being replaced with a generic encrypted-traffic application name.

Continued on next page

Capability	What the analyst can do
Other map tags	Choose domain, fingerprint, fact, outcome, identity, observed frame MAC, public IP, ASN and analytical tag views as appropriate to the available evidence.
Label priority	Give filled, relevant labels display priority so useful application evidence remains visible within the presentation budget.
Map appearance	Adjust circle sizing/color options, direction arrows, callouts and visualization lifetime. Save a browser-local master view or return to factory settings.
Map tiles	Use the local offline map. Select external OpenStreetMap tiles only where enabled and permitted.
Legend and display status	Read the map legend and inspect connection/display status. Presentation suppression and live-stream delivery are distinct from probe capture loss.
Auto and audio	Use Auto to inspect new indications and enable spoken titles where available. Audio is a browser choice; historical and hidden views remain silent.
Compact and expanded views	Use responsive drawers and expanded map/inspector views at smaller widths. Supporting text and controls retain the compact Atlas scale.

Read the label as evidence

A parsed SMB label, a DNS question and a TLS server name are different observations. Port 443 is not an application name. A visible requested hostname is not proof of authenticated user identity. Atlas keeps those distinctions available while the analyst investigates.

3 Replay: return to the moment

Pause the live display and choose a timeline bar to inspect the selected arrival second. Exact replay uses the records actually retained for that second.

Capability	What the analyst can do
Timeline and time selection	Pause, select a bar, choose a date/time and use Go for historical selection. Adjust the visible timeline span and resume live with Play.
Counted versus available	See the original count and the exact records still available. The bounded replay buffer can retain fewer records than the count after expiry, eviction or capacity pressure.
Filters off	Relax display filters for replay so available DNS or private observations can be examined. Entity authorization continues to apply.
Snapshot	Export available records for the selected replay context.
View in Full Take	Open retained connection evidence whose lifetimes intersect the selected second and Voyager. Connection overlap and exact arrival-second replay remain distinct.
Manual tags	Press Tag to save the displayed time without pausing. Keep up to 200 timestamp bookmarks in this browser; select a tag to jump without Go.
Recent detections	Keep the last 20 deduplicated detection descriptions from the live Behavior, Threat intelligence and Sigma panels, separately from manual tags.
Bookmark deletion	Delete a selected manual tag or detection bookmark. A newer occurrence of a deleted detection may appear again.
Browser-local persistence	Tags and detection bookmarks persist in this browser/site only. They save navigation metadata, not the evidence itself; storage restrictions are shown explicitly.

4 Investigate: explain the finding

Investigate preserves a direct path from the selected observation to its explanation, source evidence and next steps.

Capability	What the analyst can do
What was published	Read the deterministic explanation of the selected behavior, intelligence match or Sigma result.
Observation and provenance	Inspect available source fields, identifiers, timestamps, Voyager name, endpoints, capture context and supplying evidence.
Supporting evidence	Review the observations and references attached to a finding, alongside the stated evidence scope and relevant uncertainties.
Identity context	Read device/user associations supplied by approved identity sources, with their scope and validity. Frame MACs retain their capture-point meaning.
Retained evidence handoff	Continue into the supported retained searches for a focused period, endpoint, relationship or Voyager.
Private AI assistant	Ask about selected evidence using the authorized private provider. Suggested prompts cover notable changes, evidence, alternatives and the next check.
Stay in the workspace	Turn AI on or off without leaving Investigate. Enabling the switch alone does not submit a prompt; turning it off stops its active request.
Ticket delivery	Create or locate a ticket through configured destinations. Read its delivery state and, when confirmed, follow the returned ticket link.
External intelligence lookup	Use public-IP/domain lookup links and optional in-page VirusTotal context when enabled. External lookups are a deliberate information-sharing action.

5 Analytics and Full Take: search and prioritize

Analytics presents a selected evidence window. Full Take has its own Voyager, time and condition selection, independent of the analytical priority focus.

Capability	What the analyst can do
Priority review summary	Review grouped subjects and occurrences by assigned priority. Priorities express review order; they do not automatically authorize a block.
Category and priority controls	Select Behavior, Threat intelligence and Sigma categories. Focus P1–P4 review subjects and relationships while retaining the stated ranking scope.
Observed relationships	Connect probe-scoped endpoints to their most frequent published patterns. Select an endpoint to focus the graph and continue the investigation.
Graph density and rankings	Choose a bounded 20- or 50-endpoint window, with up to 12 patterns and scrolling. Endpoint rankings show the selected window; focused views can show fewer nodes.
Full Take search modes	Search Connections, Protocol evidence, Recorded TIP matches or Recorded detections.
Search conditions	Select a Voyager and period, including custom dates. Use supported IP/MAC, domain/DNS, application, named protocol, numeric IP protocol and other evidence fields.
AND and OR	Combine supported conditions with All or Any. Relationship-scope and recorded-detection constraints retain their explicit combination rules.
Result inspection	Inspect row details, choose visible columns, page through the fixed selection and select individual results.
CSV download	Export the current page, selected rows or all returned rows. The current bounded search returns up to 2,000 rows; CSV follows that same selection and its limits.
Cancel and clear	Cancel an active search or clear its selection. Narrow the time and conditions when a read or response limit is reached.
Noise review	Review repeated behavior candidates and their supporting context before proposing a narrow exception.
Endpoint AI	Ask about a selected bounded endpoint summary using the approved provider and the current authorized scope.

Preserve the meaning of the selection

Relationship lines show shared observations, not a newly established network connection or a proven attack path. Connection searches match retained first/last-seen overlap; protocol evidence uses its observed timestamp. A result list or graph is a bounded view of the selected evidence.

6 Reports and data: communicate the result

Atlas produces customer-facing outputs from the selected period, Voyager and enabled analytical categories.

Capability	What the analyst can do
Analyst Reports	Present review items, priorities, supporting observations, explanations, evidence/provenance and next checks.
Executive Reports	Summarize review priorities and the operational picture for the selected scope.
Manual report generation	Create private downloads from the selected Analytics period, Voyager and categories. Manual reports do not inherit Full Take row selections.
Report manifest	Read report type, dates, Voyager name/scope, review-item count, supporting observations, timezone and enabled categories.
Review-subject CSV	Export the ranked review subjects as a distinct reporting unit.
Endpoint CSV	Export the ranked endpoints and their observed analytical context.
Observation sample CSV	Export a bounded sample of the newest supporting observations. It is separate from the complete retained connection search.
Scheduled reporting	Configure the daily Executive report schedule and recipients. The scheduled report uses its stated all-Voyager, 24-hour scope.
Delivery automation	Route configured reports through the delivery workflow to Email, Slack or WhatsApp channels where enabled.
Delivery activity	Check worker/channel readiness, queued jobs and provider acceptance. Provider acceptance is distinct from an end-user read receipt.

7 Customer-controlled detection and noise management

Atlas exposes explicit rules and narrow exceptions so customers can focus review while preserving the evidence behind their decisions.

Capability	What the analyst can do
Sigma starter library	Search 78 templates by name and purpose. Build supported policies for destinations, services, identity/MAC context, DNS, applications, encryption posture and transfer volume.
Validate and activate	Preview the supported Sigma representation, validate/compile the draft and activate it in Gluon. Inspect rule name, conditions, creator, scope, priority and status.
Rule scope and revisions	Choose all Voyagers or an explicit Voyager scope, edit a rule, enable/disable it and retain its revision context.
Observed communication	Require observed payload in both directions on the same flow for applicable Sigma alerts, reports and tickets, while recorded matches remain searchable.
Customer intelligence	Add indicators individually or by supported upload, assign source/score and Voyager scope, then validate and activate the draft.
TIP connection and schedule	Configure TIP URL, organization and key. Update intelligence, schedule synchronization and inspect synchronization status.
Behavior observations	Review behavior types, publication controls and supported threshold tuning. Inspect the current 32 definitions and three additional correlation chains.
SMB tuning	Adjust supported distinct-file, rename/delete and observation-window thresholds for bulk modification and existing-file rewrite cues.

Continued on next page

Capability	What the analyst can do
Detection priorities	Assign review priority per detection. Processing and tuning are instance-wide in the shared-instance design; Entity viewing scope does not create independent tuning.
Behavior noise exceptions	Stage an exception for a specific behavior, endpoint pair, direction and Voyager scope, with a reason, verified creator and expiry. Validate before activation.
Approved scanner context	Register a documented scanner for a specific Voyager and exact private source, with the intended scope and validity.
Whitelisting	Manage supported IP, CIDR and domain entries, including source/destination scope and optional subdomain matching.
Bulk whitelist upload	Use the supplied CSV or JSONL sample, stage the bounded upload, review the draft and validate it before activation.

8 Identity, integrations and Active Defense

Atlas manages the connection between network evidence and operational workflows. Credentials, routing and authorization remain specific to the configured destination.

Capability	What the analyst can do
Identity sources	Configure read-only directory, device, DHCP and network-session sources through supported normalized adapters.
Identity uploads	Use supported scoped upload files to supply device/address associations when a live source is not available.
Minimal, time-valid identity	Retain the device/user association, IP/MAC binding, source, relationship and validity needed for the investigation, with Voyager/capture context.
Identity validation	Validate the draft, save configuration and run the available contract simulation. Inspect source/lookup results instead of treating configuration as proof of a live association.
Automation webhook	Configure the authenticated production HTTPS workflow, enabled Voyager scope and selected priorities.
Hard Block Eligible routing	Include eligible records in the configured downstream route. Response policy and the appliance workflow determine the resulting protective action.
Repeat deduplication	Send the first eligible match promptly and summarize repeated matches over the selected window, with observable capacity/refusal behavior.
Ticket destinations	Configure and test ServiceNow or Jira Cloud workflow destinations where used. Confirmed responses provide the ticket link.
Syslog and SIEM export	Configure UDP Syslog and available export formats, send a synthetic test and verify the receiving system. Gluon export carries supported records into the wider stack.
VirusTotal context	Enable optional server-held API access for an in-page summary, or use public lookup links. Third-party context remains distinguishable from Streaming Defense detections.
Appliance workflow	Connect authorized findings to the customer's firewall or security automation. Verify the command, acknowledgement and traffic outcome; a ticket or eligibility flag alone is not enforcement.

9 Private AI, Entities and access

Atlas separates network connectivity, role permissions, viewing scope and AI access. Private AI supports analyst reasoning; it does not make authoritative risk decisions.

Capability	What the analyst can do
Named secure access	Connect the user's named security tunnel, then unlock the role assigned to that same user.
Investigation access	Enable protected Investigate, Analytics and Health data, plus permitted configuration actions.

Continued on next page

Capability	What the analyst can do
Voyager management and Red Team	Authorize enrollment/management and validation exercises separately from ordinary investigation access.
Administrator access	Manage instance configuration, named users and roles subject to the required all-Entities scope.
Access status	Show Token missing or expired access explicitly and provide an Unlock route, rather than presenting every authorization failure as a storage outage.
Instance owner branding	Set the instance owner and upload a PNG or SVG logo. The logo auto-sizes; the owner name and logo hide together in tight headers.
Entities for viewing access	Assign users and Voyagers to an Entity, or grant an authorized operator all-Entities viewing.
Preserved history	Keep historical Voyager ownership and recorded data meaningful when assignments change. Shared viewing scope does not provision separate processing infrastructure.
Protected Entity deletion	Require the initial owner's Master Admin key for deletion. Deletion removes the Entity's viewing/AI access while retaining recorded evidence and historical ownership.
AI provider and model	Select the approved private-cloud or air-gapped provider and model at instance level.
Entity-specific AI key	Save and validate the Entity's key to enable AI automatically. Remove key disables that AI access without deleting the Entity.
Key protection and persistence	Keep saved keys masked and encrypted rather than returning them for display. Configured access persistence supports browser access across Atlas restarts.
Evidence-bound AI	Use scoped observation/endpoint summaries in Observe, Investigate and Analytics. Customer policy and regulator guidance can inform the private AI environment.

10 Voyager lifecycle and system Health

Operational readiness requires both a connected probe and evidence that its traffic is being processed and retained.

Capability	What the analyst can do
Voyager table	Manage named probes, their platform, location, pairing state and intended Entity.
Add Voyager	Generate the setup URL and choose the matching installer for Mac, Ubuntu 24.04, Ubuntu 26.04 or Windows 11 Alpha host monitoring.
Automatic pairing	Let the matching installer enroll and establish its dedicated probe connection from the setup URL. Setup links and named-user access credentials serve different purposes.
Renew and recover	Renew an expired pending setup link and retry using retained identity/recovery state. Use the guarded platform procedure for removal/reinstallation.
Capture ingress	View aggregate reported capture throughput and its trend with time-range and sample-freshness context.
Voyager probe Health	Inspect received/processed packets, parser/reconstruction warnings, queue drops and exporter counters where available.
Gluon Health	Inspect receive/admission, processing, enrichment, bounded state and output queue status.
Writers	Check observation, Full Take and Health writer progress, failures and refusals independently.
Data Lake	Inspect database responsiveness, current work, storage and sample freshness.
Atlas delivery	Inspect the live UI stream and display-only losses separately from capture and ingestion.
Time ranges and export	Read Live, 5-minute, 30-minute, 1-hour, 24-hour and 7-day views; refresh or download a Health report.
Retention and capacity	Review authorized Data Lake retention and state-capacity settings, validate supported changes and use the required controlled apply/restart workflow.

11 Red Team: prove the operational path

Use a selected Voyager and authorized Red Team access to run or schedule a defined exercise. Review preflight, replay, admission and detection receipts alongside the expected outcomes and controls.

Capability	What the analyst can do
SMB impact scenarios	Validate bulk file modification and existing-file rewrite cues with defined SMB operations and their control cases.
Discovery and relationships	Validate address-sweep and port-probe geometry, new peer/provider relationships and enrolled MAC/IP context.
Internal activity	Validate administrative-service fanout and ordered activity sequences in the declared scope.
External contact and transfer	Validate recurring connection timing, DNS failure patterns, transfer concentration and volume changes.
OT Modbus	Validate the transition from established read history to a new write request using isolated test traffic.
Inbound and baseline changes	Exercise scoped source/service pressure and the supported baseline-deviation dimensions.
TIP and Sigma checks	Use scoped synthetic intelligence/rules with positive and nonmatch controls, retaining matched values and signed run receipts.
Run lifecycle	Inspect readiness, profile, timing, processing/drop counts, admission and recorded outcome. Schedule supported runs and manage eligible completed archives.
Separate exercise evidence	Keep validation traffic out of production map/Analytics totals. Replay validation and physical capture coverage answer different questions.
Response proof	For appliance validation, follow the authorized event through workflow delivery to appliance acknowledgement and the resulting traffic outcome.

12 A simple analyst workflow

See it

Choose the relevant Voyager, watch the map and Live Perspective, then select the indication. Tag the time if it needs to be revisited.

Understand it

Read the explanation and provenance. Check identity, communications and supporting evidence. Use replay and retained search to establish the sequence.

Decide and act

Apply the customer's policy. Create the appropriate ticket or pass an eligible finding into the authorized response workflow. Confirm the destination result.

Improve and prove

Narrow routine-noise exceptions, tune the rule and run the positive and negative controls. Report the evidence and verify that Health still shows capture, delivery and retention.

Get help without leaving Atlas

Open the SD-logo Operations guide and search its workflows and full application/protocol dictionary. Use the companion Application, Protocol and Detection Guide for the complete catalog descriptions.

Edition: 28 November 2026. Features shown depend on the connected user's role, Entity scope and configured integrations.

streamingdefense.com