STREAMING DEFENSE

Eliminate the noise. Interrupt the attack.

Real-time network defense for IT and OT.
Authoritative evidence. Customer-controlled response.

Sub-ms
Observed mean Gluon local input-to-output processing

212
Application and protocol catalog entries

IT + OT
One investigation and response workflow

Attacks cross systems. Follow the sequence.

AI can accelerate the path from exposed service to discovery, lateral movement and destructive activity. Your defense needs to connect the observable steps while there is still time to act.

Streaming Defense brings live network evidence, defined behaviors, Sigma rules and threat intelligence into one continuous workflow. Analysts see what triggered a finding and the observations behind it.

Precision replaces the noise.

Require relevant communication. Set review priorities. Account for approved scanners and routine services with narrow, time-bound exceptions. Keep the evidence and keep your team in control.

Outcomes that matter

Focus the analyst

Explainable findings and precise exceptions concentrate review on meaningful activity.

Connect the response

Carry eligible findings into existing tickets, tools and authorized firewall workflows.

Investigate with context

Inspect identity, supporting evidence and provenance. Replay the moment or search retained activity.

Prove the protection

Run defined Red Team scenarios and controls. Verify detection and the configured response.

STREAMING DEFENSE

From packet to protective action.

Voyager observes. Gluon detects. Atlas explains.
One evidence-led platform, integrated with the tools you already trust.

VOYAGER

Capture the evidence.

Observe supported hosts and SPAN/TAP feeds. Reconstruct visible exchanges and identify network services and protocols.

Preserve capture context, quality and provenance.

GLUON

Detect what matters.

Evaluate activity on arrival. Combine defined behaviors, customer Sigma rules and exact intelligence matches.

Publish explainable findings and policy-related response signals.

ATLAS

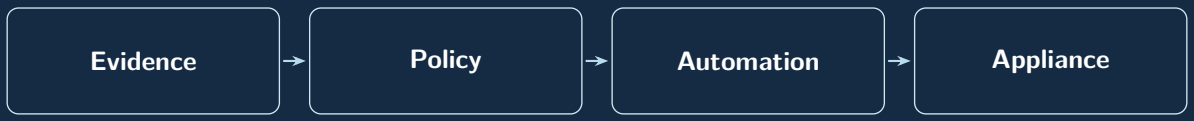
Understand. Act. Prove.

See activity live. Investigate evidence, replay events and search retained traffic. Tune detections and report clearly.

Manage access, inspect Health and run Red Team validation.

Behaviors • **Sigma** • **Threat intelligence** • **Time-valid identity**

Connect detection to protection.



Route Hard Block Eligible findings through customer-authorized workflows.
Confirm the command, appliance acknowledgement and traffic outcome.

Private AI supports the analyst.

Use private-cloud or air-gapped models for guidance and research informed by your policies. Authoritative risk decisions stay grounded in evidence and customer policy.

STREAMING DEFENSE

Protect operations. Prove the outcome.

One operational picture across IT and OT.

Systemic AI attacks

Follow observed discovery, administrative reach and transfer sequences across connected systems.

Ransomware-associated activity

Inspect confirmed SMB writes, renames, deletes and existing-file rewrite patterns.

Lateral movement

Expose probing, new internal relationships and administrative-service fanout.

Industrial communication

Recognize OT protocols and review a new Modbus write after retained read activity.

Callbacks and transfers

Investigate regular contact, DNS failure bursts and concentrated outbound payload.

Distributed operations

Bring supported hosts, cloud workloads and remote sites into scoped Atlas views.

Validate the chain: run the scenario and its control, inspect the evidence, then verify the authorized response at its destination.

Integrate with the tools you trust.

Connect SIEM, ticketing, intelligence and authorized firewall workflows through supported APIs, Syslog and automation. Deploy on-premises, in private cloud or air-gapped environments.

Request a tailored demonstration

streamingdefense.com

An operational path toward ACIS: continuous observation, explainable findings, authorized response and repeatable validation.[1]

1. Gartner, Preemptive Cybersecurity, 2025.