



SAM SUITE

More instruction. Less disruption.

SAM stops most voice and email threats before they reach staff, warns districts when threat patterns spread across districts and states, and helps law enforcement investigate faster while student data stays under district control.

SAM-VOICE

SAM-EMAIL

STUDENT PRIVACY ENGINE

SAM-LE

STOP MOST THREATS. MANAGE BY EXCEPTION.

A TDR TECHNOLOGY SOLUTIONS PRODUCT



PROTECTING THE SCHOOL DAY

More instruction. Less disruption.

SAM reduces staff exposure, provides earlier warning, and gives law enforcement organized context while people remain in control.

1

STOP EARLIER

Most voice and email threats are stopped, redirected, or contained before they reach school staff.

2

WARN SOONER

Districts can be alerted when the same threat appears across other districts and states.

3

INVESTIGATE FASTER

Authorized law enforcement receives organized evidence and recent threat-pattern context.

THE COMFORT IS IN THE OPERATING MODEL

Quiet when healthy. Clear when attention is needed.

Every avoided disruption protects instructional time, school routines, and student well-being. Routine screening and health monitoring continue in the background while staff focus on exceptions and consequential decisions.

FOUR CAPABILITIES. ONE POSTURE.

Meet the SAM Suite.

Each module has a distinct job. Together, they create a continuous path from first signal to privacy-aware, authorized follow-through.



SAM-VOICE

SCREEN THE CALL

Screens inbound calls before connection using district-defined policy. Threatening calls can be blocked or redirected before staff exposure, while source evidence is preserved.



SAM-EMAIL

CONTAIN THE MESSAGE

Screens incoming school email, checks authentication evidence, and contains threatening or suspicious messages for approved review while preserving evidence.



STUDENT PRIVACY ENGINE

APPLY THE PRIVACY RULE

Turns approved privacy policy into local decisions to allow, deny, minimize, or require human review, with a versioned rationale and auditable record.



SAM-LE

SUPPORT THE CASE

Retrieves authorized call and email evidence automatically, adds recent threat-pattern context, and prepares investigative drafts after privacy processing.

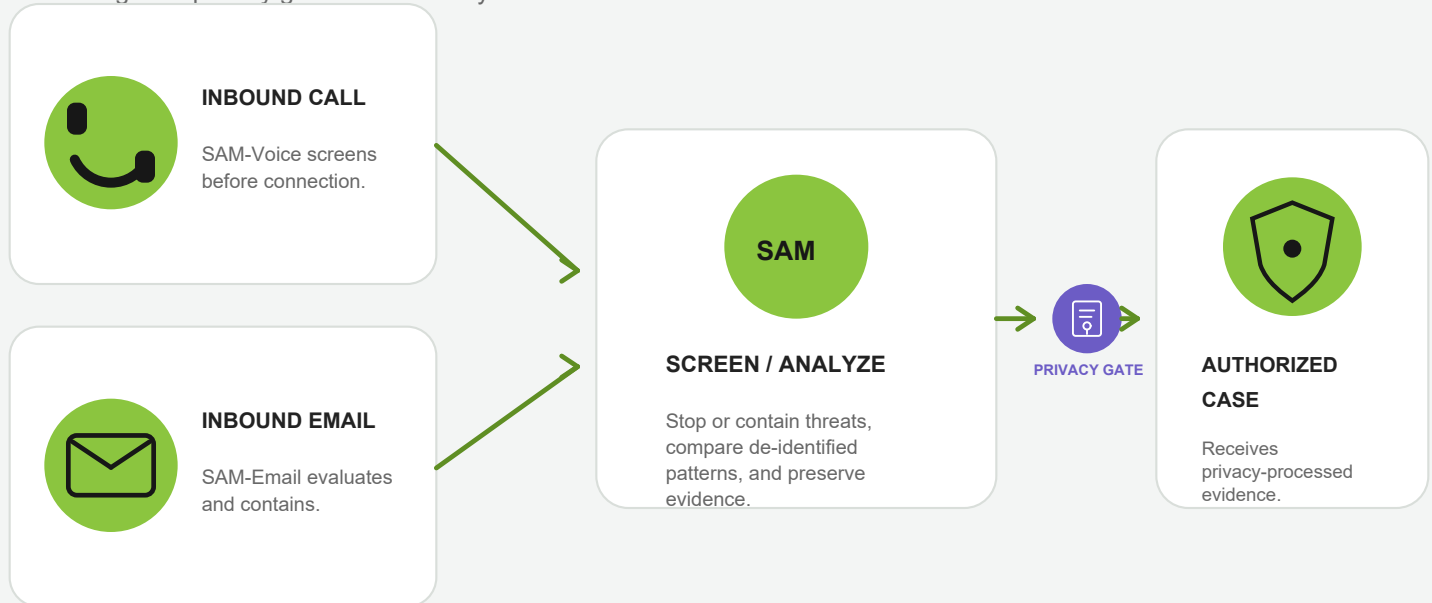
ONE SHARED PRINCIPLE

Stop most threats before staff exposure. Minimize data by default. Keep people responsible for consequential decisions.

HOW IT WORKS

A coordinated path from signal to response.

SAM screens voice and email, compares de-identified patterns across districts and states, and processes evidence through the privacy gate before use by authorized law enforcement.



STUDENT PRIVACY ENGINE - REQUIRED GATE

Student data stays inside the district; only de-identified patterns and authorized evidence move forward.

WHAT MOVES - AND WHAT DOES NOT

DISTRICT-CONTROLLED

Raw student-identifying content and local evidence remain in the authorized school lane.

SHARED WITH PURPOSE

Only privacy-processed, authorized evidence, case references, and operational telemetry move between services.

HUMAN REVIEW GATE

AI-assisted analysis organizes and prioritizes information. Authorized law enforcement determines credibility; district personnel decide the school response. No score or pattern match decides the outcome.

THE SCHOOL-FACING LAYER

Stop most threats before they reach staff.

SAM-Voice and SAM-Email work inside the communication systems schools already use.



SAM-VOICE

The front door for inbound calls.

- ✓ Stops or redirects most threatening calls before staff exposure.
- ✓ Supports allow, block, redirect, and flag outcomes.
- ✓ Provides per-call explanations and operational visibility.
- ✓ Preserves call continuity if screening is unavailable.

LOW-TOUCH VALUE

Policy runs continuously; staff focus on exceptions and changes.



SAM-EMAIL

A quieter inbox and a clearer review queue.

- ✓ Contains most threatening messages before they reach staff inboxes.
- ✓ Uses authentication evidence and threat patterns to support triage.
- ✓ Routes suspicious messages into approved containment and review.
- ✓ Preserves evidence without sending raw student content to external AI.

THE INVESTIGATIVE LAYER

Help law enforcement investigate faster.

SAM-LE automatically retrieves authorized call and email evidence, adds recent pattern context across districts and states, and prepares investigative drafts after privacy processing.



SAM-LE

Collect. Compare. Organize. Support the case.

AUTOMATED EVIDENCE RETRIEVAL

Retrieves approved call and email evidence directly from SAM-Voice and SAM-Email, reducing record searches and manual handoffs.

THREAT-PATTERN CONTEXT

Compares de-identified patterns across districts and states so investigators can identify related recent threats faster.

INVESTIGATIVE DRAFTS

Prepares draft Industry Traceback Group (ITG) requests, emergency carrier requests, preservation notices, subpoenas, and search-warrant materials for authorized review.

CONTROLLED COLLABORATION

Supports role-based coordination among authorized agencies and school safety partners.

CLEAR BOUNDARY

SAM-LE is not a public portal and does not replace an agency's investigative judgment, evidence policy, or legal authority.

DEPLOYMENT NOTE

SAM-LE is in a controlled, transitional implementation. Final availability and integration scope are confirmed during deployment planning.

PRIVACY BY CONSTRUCTION

Student Privacy Engine

Student privacy is a core design principle, not a feature that can be turned on or off.

FOR THE PRIVACY LEADER

Clear controls. Clear evidence.

- ✓ Versions the applicable policy and decision basis
- ✓ Returns an allow, deny, minimize, or human-review outcome
- ✓ Applies data minimization and least privilege
- ✓ Produces decision receipts for audit and review
- ✓ Supports jurisdiction-specific policy overlays



PRIVACY GATE APPLIES.

STUDENT-IDENTIFYING DATA DOES NOT LEAVE THE DISTRICT.

Before evidence is shared with SAM-LE, the engine removes student-identifying data under district-approved policy.

Only privacy-processed, minimum-necessary evidence is eligible for authorized sharing. The engine fails closed when purpose, authority, recipient, jurisdiction, or policy integrity cannot be established.

DESIGNED FOR APPLICABLE REQUIREMENTS

SAM's privacy control objectives are designed to help districts address applicable FERPA, COPPA, PPRA, and state student-privacy obligations.

Applicability is deployment-specific and is validated against current law, district policy, contracts, and qualified review.

CURRENT DELIVERY POSTURE

Existing product-level privacy safeguards remain active while the unified shared engine is consolidated and must pass policy-signature, fail-closed, rollback, offline, jurisdiction, and integration testing.



READY TO STOP MORE THREATS EARLIER?

More instruction. Less disruption.

Start with a readiness conversation. We will map your phone, email, student-privacy, threat-alerting, and law-enforcement workflows, then identify the smallest responsible deployment path.

TDR TECHNOLOGY SOLUTIONS

sales@tdrtechnologiesolutions.com

www.tdrtechnologiesolutions.com

1-845-293-3588



SAM supports prevention and disruption reduction; no technology can guarantee that every threat will be detected or prevented. Capabilities and integrations are confirmed for each deployment.

SAM-Voice | SAM-Email | Student Privacy Engine | SAM-LE

TDR TECHNOLOGY SOLUTIONS