PLATFORM ARCHITECTURE

DEFENSESTORM
THE BEST OFFENSE

GRID Active Platform

The intelligent data platform that powers detection, evidence, and oversight for banks and credit unions.

THE CHALLENGE

Disconnected Tools, Siloed Data, and No Single Source of Truth

Financial institutions rely on dozens of security, risk, and compliance tools that were never designed to work together. Firewalls, endpoints, identity systems, cloud platforms, and core banking applications each generate their own telemetry, but that data lives in silos. When a threat emerges, analysts chase context across multiple consoles. When examiners ask for evidence, teams scramble to stitch together artifacts from disconnected systems.

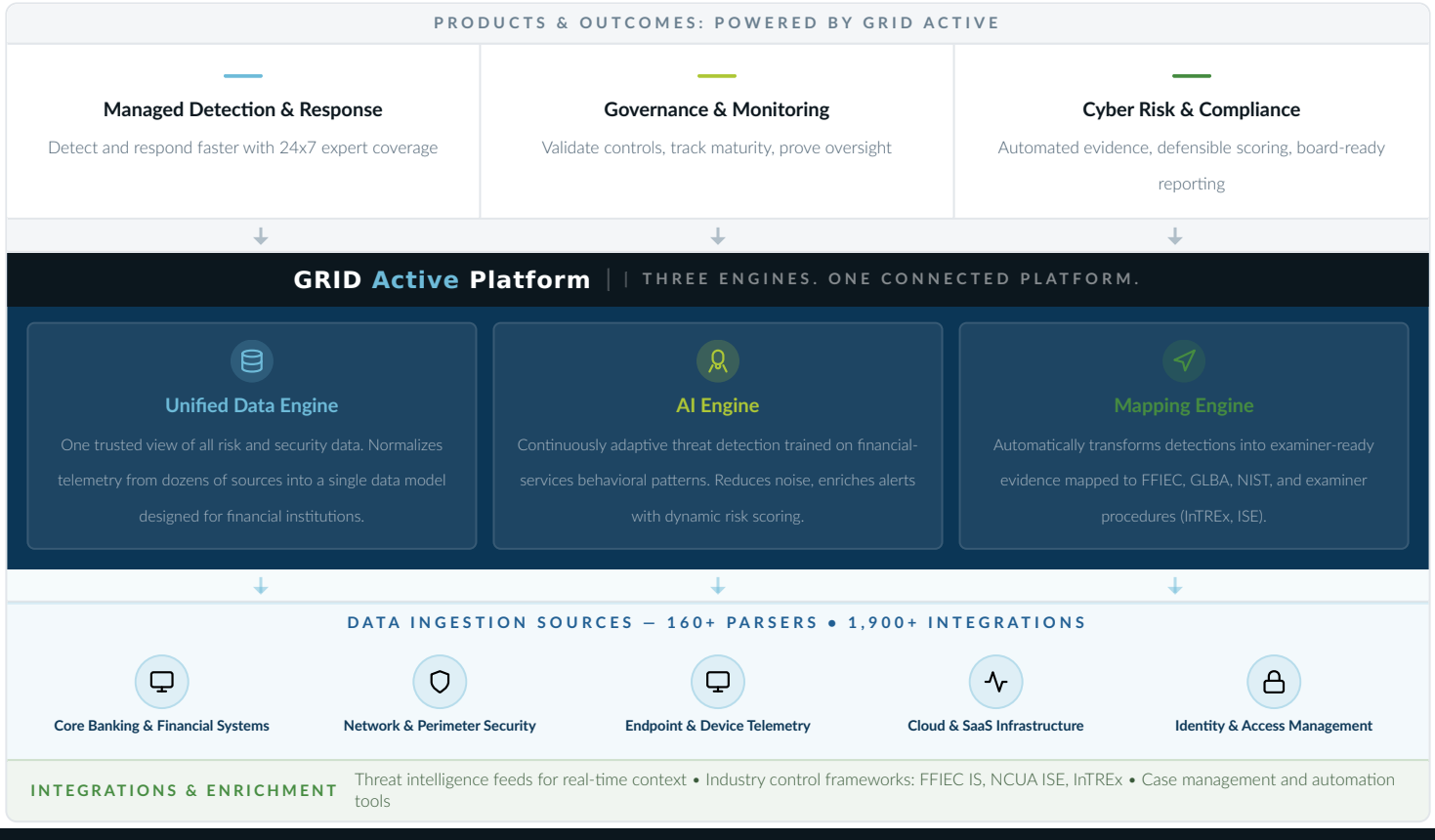
Generic SIEM and GRC platforms ingest data but lack the intelligence to connect detections to regulatory frameworks or translate telemetry into examiner-ready evidence. The result: slower investigations, incomplete oversight, and a risk posture built on manual effort.

One Platform. Unified Intelligence. Built for Banking.

GRID Active is DefenseStorm's unified, cloud-native platform that combines real-time data ingestion, AI-driven analytics, and intelligent control mapping to deliver proactive detection, faster investigations, and examiner-ready evidence in one place. It is the engine behind every DefenseStorm product, normalizing telemetry from across your entire environment, applying behavioral analytics tuned for financial services, and automatically mapping detections and controls to examiner frameworks.

PLATFORM ARCHITECTURE

Data flows bottom to top: ingestion → intelligence → outcomes



THREE ENGINES. ONE CONNECTED PLATFORM.

How GRID Active Works

Unified Data Engine

One trusted view of all your risk and security data. Ingests and correlates activity across IT, security, cloud, identity, and core banking to enable faster, more confident decisions. Normalizes telemetry from dozens of sources into a single data model designed for financial institutions.

AI Engine

Continuously adaptive threat detection trained on financial-services behavioral patterns. Reduces noise, enriches alerts with dynamic risk scoring, and prioritizes what matters. Detection models are tuned specifically for FI environments, not generic enterprise patterns.

Mapping Engine

Automatically transforms detections into examiner-ready evidence mapped to FFIEC, GLBA, NIST, and examiner procedures (InTREx, ISE). Connects controls and evidence to frameworks, closing the loop between security operations and compliance oversight.

THE FOUNDATION BEHIND EVERY DEFENSESTORM PRODUCT

What GRID Active Powers

Managed Detection & Response

GRID Active ingests, correlates, and analyzes telemetry in real time. The AI Engine detects threats using FI-tuned behavioral models. The Mapping Engine produces examiner-ready evidence of detection and response, while our Collaborative SOC investigates with full banking context.

Governance & Monitoring

GRID Active's Mapping Engine connects controls to frameworks and evidence, enabling continuous control validation, maturity tracking, and board-ready reporting powered by a single connected data foundation.

Cyber Risk & Compliance

GRID Active automates evidence collection, maps controls to FFIEC, GLBA, and NIST expectations, and delivers real-time dashboards that translate risk posture into clear business terms for leadership and examiners.

Why GRID Active

Built for Banking

Purpose-built for the data, regulatory, and operational realities of financial institutions. Detection models, framework mappings, and data normalization reflect FI environments, not generic enterprise security.

Unified Data Foundation

One platform replaces the need to stitch together separate SIEM, GRC, and reporting tools. All products draw from the same trusted data, eliminating silos and reducing integration burden.

Detection to Evidence in One Flow

From raw telemetry to enriched alert to mapped evidence, GRID Active closes the loop without manual handoffs. Detections become proof. Proof becomes oversight.

Cloud-Native & Scalable

Built for modern infrastructure with ingestion-based pricing. Scales with your institution without hidden costs or capacity surprises as your data volume grows.

By the Numbers

5M+
Events ingested and analyzed daily

82 sec
Mean time to acknowledge (MTTA)

<15 min
Mean time to detect, critical alerts

91%
Detection triggers mapped to regulatory controls

138+
Examiner-ready artifacts generated per month

200+
Banks and credit unions protected

Based on customer cohort averages.

One platform. **Complete intelligence. Built for banking.**

See how GRID Active connects your data, detections, and evidence into one unified platform built for banking.

470-519-0020
info@defensestorm.com