PRESIDIO®

SOLUTION OVERVIEW

Deliver trusted, secure data for financial services apps and AI

As more financial institutions move AI into production, they need to establish trusted context for data while protecting access to systems. F5 and Presidio together provide that trusted data foundation while securing apps and APIs.



Key benefits

Establish trusted financial context
Implement a reusable, scalable production pattern to ensure consistent, trusted, fit-for-use data for AI apps and agents.

Protect AI interactions
Apply policy enforcement, PII protection, authorization controls, and auditability across every AI interaction.

Improve accountability and compliance
Track every data access, AI request, agent action, and tool invocation with comprehensive audit trails.

Secure AI systems
Protect client-facing and internal services with AI-powered WAF, bot defense, DDoS protection, and API discovery.

Financial institutions struggle to trust the data powering AI

Financial institutions are rapidly accelerating AI adoption. But even as organizations race to move more AI apps and agents into production, many still lack the trusted, governed data foundation they need for accurate, AI-assisted decision-making. Meanwhile, they face critical challenges safeguarding sensitive information and maintaining compliance.

These challenges become more significant as organizations scale up AI. Sensitive information can be exposed through a growing number of AI interactions. And an expanding fleet of agents can invoke tools without authorization controls.

Institutions need to simultaneously establish a trusted financial context for AI and protect their fast-growing collection of AI systems. Because adoption is likely to continue unabated, they need solutions that will enable them to define a repeatable, scalable pattern for governance and security.

Establish trust across data, AI, applications, and APIs

The Presidio Data Trust Accelerator for Financial Services creates a centralized data trust and orchestration layer that governs how client data is interpreted, validated, managed, accessed, and consumed throughout the organization. The solution creates a golden record and trusted output layer that delivers consistent and reliable information across systems, analytics platforms, workflows, and AI applications.

F5 provides the runtime protection for every AI, API, application, and agent interaction. All traffic moving between trusted data sources and consuming applications passes through a unified enforcement layer where identity, policy, authorization, audit logging, and data protection are applied in real time.

The solution operates across five connected stages:

1. **Ingest and normalize**: Connect and standardize enterprise data into trusted canonical models and golden records.
2. **Govern and observe**: Continuously monitor data quality, reliability, governance, and model performance.
3. **Govern the flow**: Apply runtime controls, guardrails, authorization, telemetry, and AI security policies.
4. **Activate intelligence**: Deliver trusted data to AI models, analytics platforms, and business applications.
5. **Enable personalized and compliant engagement**: Support compliant, personalized client interactions powered by trusted intelligence.

Key features

Govern data for AI
Implement an operating layer that governs what data every AI agent, workflow, and system can access and how.

Enforce AI guardrails in real time
Apply pre-built guardrails (including PII protection, prompt injection defense, and restricted-topic controls) and extend with unlimited custom policies to meet any organizational or compliance requirement. Enforce inline, out-of-band, or across distributed environments for consistent protection at every point in the AI traffic flow.

Control agent and tool access
Apply per-tool authorization, identity forwarding, and activity auditing for autonomous agents with the MCP Gateway.

Maintain complete visibility and lineage
Track source quality, data lineage, schema changes, governance status, budgets, and policy decisions across the environment.

Secure every application surface
Protect web applications, APIs, portals, advisor tools, and AI-enabled services from attack and abuse with F5 Distributed Cloud.

Pinpoint vulnerabilities
Automate testing of AI models, apps, and agents to find and address vulnerabilities with F5 AI Red Team.

The combined approach enables organizations to achieve consistent outcomes across systems and AI platforms while maintaining regulatory alignment, operational visibility, and enterprise-wide governance.

Build trust in data and trust in AI

Organizations cannot successfully scale AI without confidence in both data quality and data security. The Presidio Data Trust Accelerator for Financial Services, combined with F5 runtime governance and security capabilities, establishes a unified framework for trusted data, trusted AI, and trusted operations.

By combining data governance, AI governance, application security, API protection, and agent controls into a single operating model, financial institutions can accelerate modernization while reducing risk, improving compliance, and enabling sustainable AI adoption.

Schedule an assessment to establish a data quality baseline, map AI flows, and identify governance gaps.

Speak with an expert to discover how trusted data and governed AI can accelerate business outcomes.

©2026 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC 10.2026 | JOB-CODE-123456789