Forcepoint

Solution Brief

AI Security with Forcepoint and F5: From Data Visibility to Runtime Assurance

Challenge:

- **Data Blindness:** Organizations lack a complete understanding of what data exists, where it resides, or which AI systems can access it.
- **Disconnected Controls:** Data security, application security and AI governance are managed in silos, creating gaps between policy intent and runtime behavior.
- **No Runtime Assurance:** Security teams cannot validate that AI systems behave safely once deployed.

Solutions:

- Partnership between Forcepoint and F5 to align AI data readiness with runtime security.
- A continuous AI security lifecycle that connects data truth with runtime assurance.

Outcome:

- A mature, scalable way to secure AI innovation with confidence and operational proof.

A Joint Approach: Data-Driven AI Security with Runtime Enforcement

AI adoption is accelerating across copilots, agents and autonomous workflows. But most organizations still lack the visibility and runtime controls needed to secure them.

Traditional security models weren't built for AI's data hungry, dynamic behavior and ever-expanding exposure surface. Forcepoint and F5 have partnered to address AI security as a continuous lifecycle, not a point solution.

This joint approach connects:

→ Data understanding and policy context with Forcepoint

→ Real-time runtime enforcement and resilience with F5

Together, organizations can move from data truth to runtime trust, ensuring AI systems are secure by design and resilient in operation.

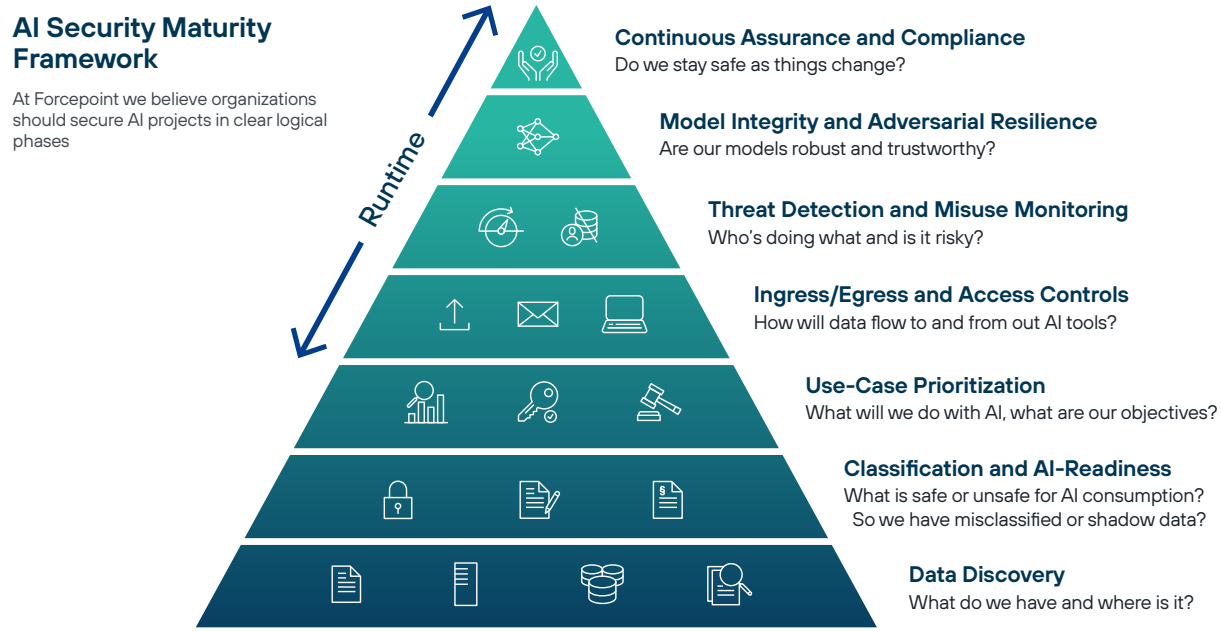
Forcepoint ensures organizations have clear, accurate visibility into their data layer and can safely provide the right data to the right AI systems.

F5 focuses on securing how AI systems behave at runtime, protecting the applications, APIs, and models that operationalize that data.

Rather than treating AI security as a standalone category, this model integrates AI into existing security foundations, extending them with AI-specific visibility, controls, and assurance.

The AI Security Maturity Framework

This framework reflects how organizations mature their AI security posture over time. The lower layers establish trust; the upper layers enforce and sustain it at runtime.



Data Integrity

Before AI can run safely, organizations must know what data they have, what it means and what it's ready for.

1. Data Discovery

Organizations begin by identifying structured and unstructured data across cloud, SaaS, endpoints and data platforms, including shadow data sources used by AI systems, to create a factual baseline of AI-relevant data exposure.

How Forcepoint helps

- → Delivers enterprise-scale discovery of sensitive and business-critical data
- → Provides visibility into data sprawl and AI-accessible repositories
- → Establishes a clear, authoritative view of AI-relevant data exposure

2. Data Classification

Classify data using explainable, auditable methods so that sensitivity, regulatory relevance and business importance are clearly understood and data becomes governable, not just visible.

How Forcepoint helps

- → Applies explainable, AI-aware classification powered by Forcepoint's AI Mesh technology, ensuring consistent understanding of data sensitivity across environments
- → Uses persistent labels that travel with data across environments

3. Use-Case Prioritization

Not all AI use cases carry equal risk. Organizations must determine which AI workflows pose the greatest business risk based on data sensitivity, exposure and usage. This will allow security teams to focus on high-impact AI risks first.

How Forcepoint helps

- → Correlates sensitive data with specific AI workflows to quantify risk
- → Prioritizes AI use cases based on real business impact and exposure
- → Provides data-context signals (via classification & AI Mesh) to guide safe AI adoption

Runtime Security

At this point, security moves from preparation to active runtime protection.

4. Ingress, Egress and Access Control

Apply controls to AI interactions as they occur, governing what data can enter or exit AI systems and who or what can access them, ensuring AI systems operate within clearly defined boundaries.

How F5 helps

- → Validates and protects runtime access paths for APIs, gateways, and workloads

How Forcepoint helps

- → Provides data classification and policy context to guide runtime access decisions (e.g., what data AI is allowed to see or output).

5. Threat Detection and Misuse Monitoring

Continuously monitor AI systems for misuse, abnormal behavior and indicators of compromise, enabling faster detection and a clearer understanding of risk.

How F5 helps

- → Proactively tests AI systems, including models, applications and agents, to find and fix vulnerabilities before systems fail
- → Detects prompt abuse, data exfiltration and anomalous activity

How Forcepoint helps

- → Contextualizes alerts based on data sensitivity and business impact

6. Model Integrity and Adversarial Resilience

Safeguard models against adversarial manipulation, poisoning and integrity drift so AI systems remain reliable, predictable and safe.

How F5 helps

- → Defines and deploys agile data security, threat management and governance for AI models, apps and agents
- → Defends models against runtime attacks and integrity degradation

How Forcepoint helps

- → Ensure models never train on or expose prohibited data

7. Continuous Assurance

Validate AI security continuously through telemetry, policy validation and operational evidence, providing ongoing confidence for security leaders, boards and regulators.

Joint value

- → Forcepoint provides posture, policy validation and auditability
- → F5 delivers runtime telemetry and enforcement evidence

Impact Summary: What This Delivers

Together, Forcepoint and F5 enable organizations to:

- → Reduce AI risk by grounding runtime security in real data context
- → Prevent AI misuse and exposure before incidents occur by understanding and mitigating AI runtime risks
- → Align data governance, application security and AI assurance
- → Demonstrate continuous observability and compliance across data and runtime environments
- → Secure AI innovation without slowing business velocity

Book a meeting today to learn more about how Forcepoint and F5 can enhance your AI security