FLEXENTIAL®

Flexential AI Platform Engineering

AI operations with governance, security, and resilience built in

Overview

As AI workloads move from experimentation into production, they become business-critical systems. Production AI platforms introduce distributed services, data pipelines, model hosting, and network dependencies that increase operational complexity, availability risk, and security exposure. Organizations must keep AI services running and continuously prove security hygiene, resilience, and recovery readiness to executives, auditors, and cyber insurers.

Flexential AI Platform Engineering is an operations service that builds, operationalizes, secures, and continuously manages AI platforms. The service integrates platform engineering, cybersecurity operations, data architecture, DataOps, and network engineering to improve availability, reduce risk, and deliver ongoing validation through monitoring, testing, and reporting, resulting in AI platforms remaining reliable, secure, and resilient at scale.

Problems we solve

Organizations moving AI into production commonly face the following challenges:

- A business requirement to build a new AI platform or challenges running an existing AI deployment
- Unreliable production AI operations caused by immature operational tooling and inconsistent run processes
- Security exposure from AI-specific threats (prompt injection, data/model poisoning, supply-chain risk) that are not addressed by traditional controls
- Inability to sustain rigorous security hygiene, such as patching, scanning, and configuration hardening, due to skills and capacity gaps
- High business impact from outages and complex recovery across distributed and hybrid AI dependencies

High urgency

Production AI failures drive outages, security incidents, and loss of executive trust if operational ownership and validation are unclear.

When full adversarial scans are run on enterprise AI systems, critical vulnerabilities surface within minutes:

16 minutes

Median time to first critical failure

87 minutes

90% of systems fail

—ThreatLabz AI Security Report

Key benefits

Flexential AI Platform Engineering delivers measurable improvements across operations, security, and resilience:

- Improved availability and performance for AI workloads
- Reduced operational and cybersecurity risk through continuous monitoring, patching, and vulnerability management
- Improved compliance and audit readiness through documented processes, testing, and reporting artifacts
- Faster detection, response, and recovery through 24x7 support, monitoring, and incident response workflows

Key features

Flexential AI Platform Engineering delivers integrated capabilities aligned to core cyber resilience functions:

Identify and govern

- Discovery and inventory of AI platform components, dependencies, and data flows
- Clear operational ownership and accountability across platform, data, network, and security teams
- Baseline risk and readiness assessment impacting availability and resilience
- Governance artifacts and reporting to support audit readiness and executive oversight

Protect

- Cybersecurity posture assessment with prioritized remediations and maturity improvements
- Routine patching, configuration hardening, and access control management
- Network security, performance, and scalability management

Detect

- 24x7 monitoring, alerting, and observability across the AI platform
- Monthly vulnerability scanning with consolidated reporting and remediation guidance

Respond

- Defined incident response workflows and priority-based response tiers
- 24x7x365 Flexential expert support
- Annual AI-focused penetration testing with remediation validation (including prompt injection and data poisoning scenarios)

Recover

- Backup and recovery operations with monitored restore readiness
- Network availability validation and scheduled HA/DR failover testing

Improve

- Industry-proven lean-agile delivery model and DevOps practices
- Continuous improvement driven by recurring reviews, re-testing, and prioritized remediation backlogs
- Continuous operational and technical modernization and optimizations

Next step

If your organization is moving AI into production or struggling to keep production AI reliable and secure, **Flexential AI Platform Engineering** provides a clear path to operational confidence and cyber resilience.

Outcomes we deliver

Customers adopt **Flexential AI Platform** Engineering to achieve durable, business-level outcomes:

- Stronger governance for AI initiatives generates increased stakeholder trust and confidence
- Reduced business risk and disruption from AI-enabled services through increased security and resiliency
- Increased ROI from productivity gains and cost-effectively offloading operational and security run tasks
- Improved user experiences and operational availability through proactive maturity improvements

How it works

- Delivery follows a structured lifecycle designed for production readiness and continuous validation
- Onboarding and discovery to define scope, validate access and monitoring, and deploy operational tooling
- Architecture, cybersecurity, network, and data assessment to establish a production-ready baseline
- Transformation and build to implement a targeted platform, DataOps, and network improvements
- Ongoing management and support with monitoring, testing, reporting, and resilience validation