Fabrix.ai

Case Study

Fortune 500 Energy Company Transforms Network Operations with AI Agents

How a top-tier North American energy company replaced fragmented, tool-hopping operations with intelligent multi-agent orchestration — achieving continuous visibility, faster RCA, and proactive service assurance.

Situation

- Large multi-site network and infrastructure estate managed from a central NOC.
- Splunk, Dynatrace, Cisco, ServiceNow and ThousandEyes were data-rich but siloed.
- Network blamed for VPN, VDI and app issues even when root cause lived elsewhere.

Impact

- Swivel-chair correlation across 8+ platforms for every investigation.
- 1.7B+ Splunk events/day across 18+ indices, but no direct path to answers.
- VPN and VDI issues escalated to senior engineers after help desk playbooks.
- Cisco advisories required manual inventory cross-referencing before risk classification.

Resolution

- Fully managed SaaS on AWS with on-prem worker nodes.
- Teams Copilot for natural-language operations and automated notifications.
- Splunk + ITSI: leveraged existing data; automated services, KPIs and episode policies.
- Enterprise Ontology + MCP tooling connected customer systems into the agentic ecosystem.

The customer saw Fabrix.ai as the unified agentic operations layer they had been trying to build for years: a single pane of glass that does not merely display dashboards, but asks tools the right questions, correlates signals across domains, and returns recommended actions in the flow of work.

Customer Snapshot				
Industry	**Scale**	**Data Estate**	**Deployment**	**Go-Live**
Energy & Utilities (Fortune 500, NYSE-listed)	25,000+ devices 27+ sites 10+ VPN gateways 3,300+ VPN users	1.7B+ events/day 18+ Splunk indices 15+ tools integrated	Fully managed SaaS AWS + on-prem worker nodes	Direct to production No prolonged POC

The Solution

Fabrix.ai deployed its Agentic Platform as an always-on layer across the customer's existing tools, making every system agent-accessible for governed AI investigation and action.

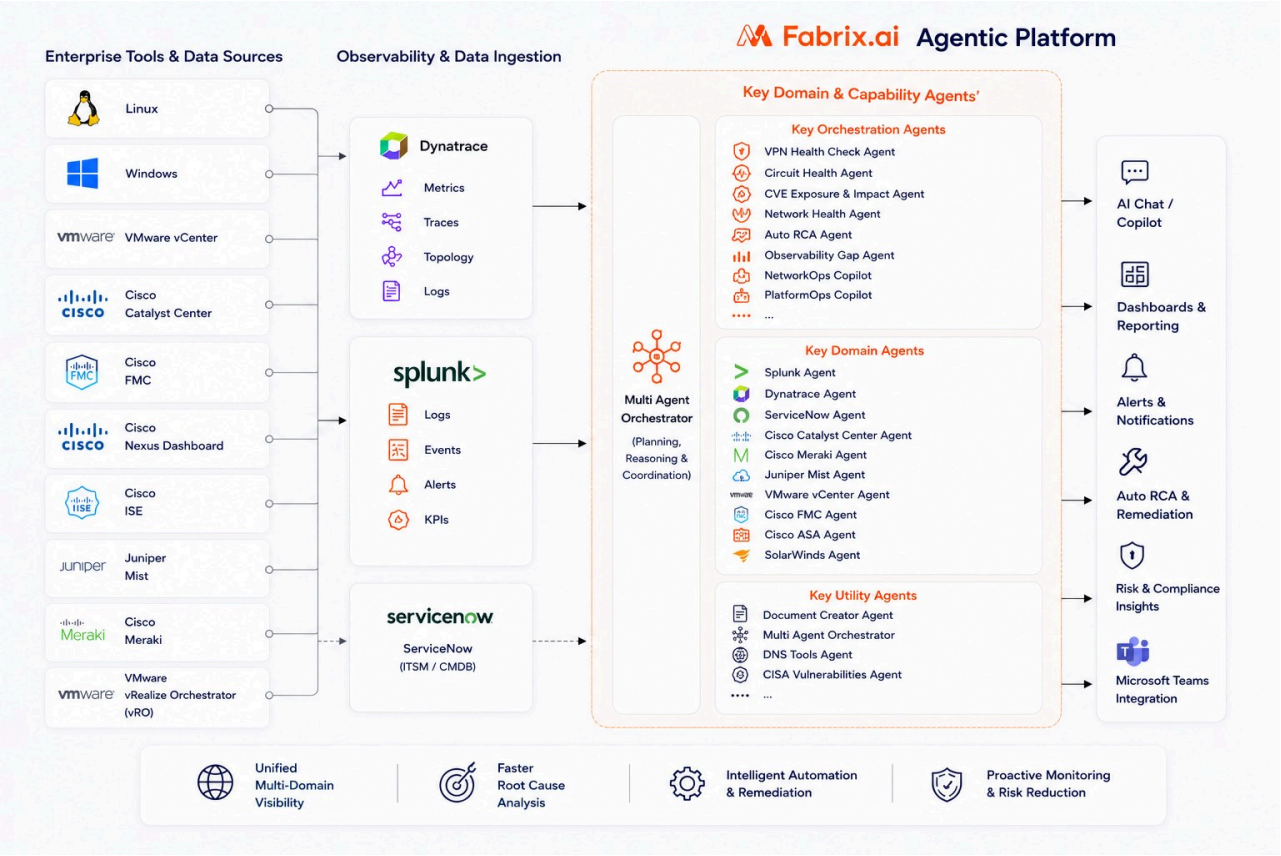
- **Splunk + ITSI** — existing Splunk data, automated services, KPIs and episode policies.
- **Enterprise Ontology** — knowledge graph for multi-domain topology and dependencies.
- **MCP Tooling** — customer systems connected into the agentic ecosystem.

How It Works

- **Automate** — daily and hourly checks across network, infrastructure, security and applications.
- **Correlate** — multi-source data correlation for accurate root cause and risk analysis.
- **Act** — deliver answers, reports, Teams notifications and ServiceNow actions automatically.

Key Agents Delivered	
Network Health Agent	Daily multi-platform health score, issue triage and ticket recommendations.
VPN Health Check Agent	Hourly gateway checks across path, routing, authentication, sessions and IP assignment.
CVE Exposure & Impact Agent	Cisco PSIRT advisories matched to live inventory with device-level verification.
Auto RCA Agent	Incident analysis tied to ServiceNow with correlated evidence across tools.
Observability Gap Agent	Reachability and data coverage checks across tools and Splunk indices.
NetworkOps & PlatformOps Copilots	High-level routing agents that orchestrate use-case agents and task-focused micro-agents.

Fabrix.ai Agentic Platform Architecture



Validated Agent Library Pattern

1

Tool MCPs

Connect Splunk, Dynatrace, Cisco, ServiceNow, VMware and other systems.

2

Micro Agents

Task-focused agents with clear instructions for reliable repeatability.

3

Use-Case Agents

Reusable workflows for VPN, CVE, circuit, observability and access scenarios.

4

Routing Copilots

NetworkOps and PlatformOps copilots route questions to the right use-case agents.

Emerging Agent Categories

- **Proactive / ambient agents** — continuously scan for VPN, Wi-Fi, application access, telemetry and observability issues before users escalate.
- **Help Desk triage agents** — give Tier 1 teams a governed place to check a user, device, location, VPN state and likely root cause.
- **Employee self-service agents** — a future portal experience where users can check device, VPN, app access and remediation guidance themselves.

Field-Validated Use Cases

On-site deployment exposed live operational problems that had historically required several teams, tools and escalations. Fabrix.ai agents analyzed the same incidents in minutes, creating a validated library of repeatable use cases for NetworkOps, Help Desk and future employee self-service.

Use Case	Before Fabrix.ai	Agent-Led Outcome	Why It Matters
VPN User disconnects	Help desk playbooks, reboots and escalations; senior engineers searched ISE, ASA/FTD, FMC and Splunk.	Agent resolved user identity variants, correlated auth/tunnel/session evidence and pinpointed client-side network instability in ~3 minutes.	Moves repetitive VPN RCA from Tier 3 to Help Desk and gives written evidence when the network is not the cause.
VDI Virtual desktop hangs	Weeks or months of blame between VDI and network teams with no clear owning domain.	Agent analyzed logs and surfaced load-balancer TTL / timeout configuration as likely root cause in ~5 minutes.	Shifts the conversation from blame to a precise remediation owner and next action.
Observability Observability gaps	Teams did not always know when Splunk indices or API access stopped receiving data.	Agents continuously check reachability across tools and data freshness across critical indices.	Agentic dashboards monitor the monitoring layer and warn before investigations fail.
Proactive VPN health	Issues were discovered after users complained or tickets escalated.	Ambient agents identify users with VPN stability issues across the last 24–48 hours and pre-run RCA.	NOC and Help Desk can see likely problem users before or as tickets arrive.
CVE Exposure assessment	Cisco advisories required manual inventory checks and cross-referencing.	Cisco PSIRT advisories are matched against live inventory with device-level verification and risk classification.	Turns days of advisory triage into minutes of agent-led assessment.

Shift Left

Help Desk answers common VPN/access tickets first.

Detect Earlier

Proactive agents surface issues before escalation.

Reuse Fast

Micro-agents become repeatable enterprise use cases.

> **For nearly 20 years, I have been waiting for a true single pane of glass. With Fabrix.ai, I am finally seeing it come to life — agents that reason across tools and tell us what is happening, why, and what to do next.**
>
> — VP, IT Infrastructure Operations

Results That Matter

Key ROI Metric	Before Fabrix.ai	After Fabrix.ai	Impact
Multi-platform visibility	8+ disconnected tools; manual correlation per investigation	Single agent entry point; parallel checks across platforms	Proactive operations vs. reactive fire-fighting
VPN incident RCA	Hours of cross-platform log hunting; escalations to senior engineers	Automated RCA in minutes with user identity, ISE and ASA/FTD correlation	Faster MTTR; Tier 3 effort shifted left
VDI / access issues	Weeks or months of ownership debate across teams	Agent analysis identified likely load-balancer timeout/TTL configuration in minutes	Faster problem ownership and remediation
VPN estate health	Reactive checks after complaints	Hourly automated check across VPN gateways and user stability patterns	Issues detected before users escalate
CVE assessment	Days of manual inventory cross-referencing per advisory	Daily automated scan with per-device risk classification	Days of effort to minutes of analysis
NOC efficiency	Analysts spend shifts gathering evidence from tools	Agents handle first-pass analysis, correlation and reporting	Analysts focus on decisions, not data gathering

Quantified Impact (Initial Phase)

~3 min
VPN user RCA turnaround

~5 min
VDI access issue analysis

24–48h
Proactive user stability window

9/9
Tool reachability checks

18+
Splunk indices monitored

What's Next

With Network and Infrastructure Operations running in production, the customer is expanding Fabrix.ai into Application Operations, Help Desk triage and proactive employee experience. New use cases are emerging from live operational demand: VDI, application access, device posture, telemetry gaps, circuit health, and self-service checks for employees and partners. Network Operations leadership is championing the platform at the executive level, positioning Fabrix.ai as the long-term agentic operations layer across the enterprise technology stack.

> **We are solving real Tier-3 problems in minutes, with evidence, using the systems we already run. That changes the conversation from who owns the issue to what action we should take next.**
>
> — Director, Network Operations