2025

FYNITE

Case Study

Enterprise Achieves Autonomous Threat Detection & Response with Fynite

End-to-End Data-to-Decision Framework for Cybersecurity Operations

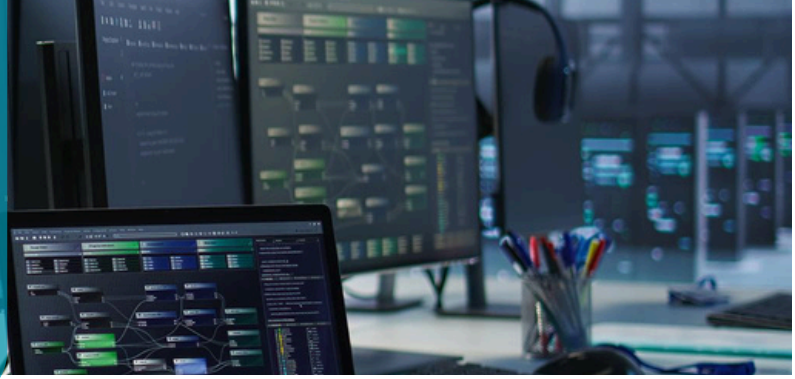
SOC 2 Compliant SECURE

(414) 364-2156

fynite.ai

contact@fynite.ai

Overview



Introduction

Organization: Fortune 500 Financial Services Enterprise
Industry: Cybersecurity / IT Operations
Infrastructure: Hybrid cloud, 90K+ endpoints, 10 data streams
Challenge: Fragmented visibility, delayed threat response, and inconsistent data trust across security sources.

Annual Volume:

240K
Events

20K
Alerts

2K
Incidents

The client operates one of the world's largest enterprise cybersecurity environments, managing multi-cloud and on-prem infrastructures across global clients. With rising data complexity, they aimed to improve data integrity, enhance threat detection accuracy, and reduce MTTR through autonomous, AI-driven incident response.

CHALLENGES BEFORE FYNITE

Before automation, fragmented threat data and inconsistent sources caused poor data integrity, manual triage, and delayed containment—slowing response times and increasing risk due to lack of autonomous, unified cybersecurity execution.

1

Fragmented Data Streams

- **Threat logs, network telemetry,** and **endpoint data** were siloed across systems—making unified analysis difficult.

2

Manual Triage & Decisioning

- **Security analysts** manually reviewed alerts and reports, leading to slower MTTR and increased exposure windows.

3

Data Inconsistency

- Conflicting data between **SIEM, EDR**, and **firewall** systems led to false positives and missed alerts.

4

Lack of Autonomous Execution

- **Threat** mitigation required human validation, resulting in longer containment times.

The result: reactive security posture, delayed response cycles, and unquantified risk exposure.

FYNITE
AI-POWERED BUSINESS AUTONOMY

contact@fynite.ai
www.fynite.ai
2135 City Gate Ln, Suite 300
Naperville, IL, 60563

Fynite's Solution

End-to-End Data-to-Decision Automation

FyniteOS unified the enterprise's security data fabric through AI-driven pipelines, enabling real-time anomaly detection, data rationalization, and autonomous execution across all layers of cybersecurity.

Intelligent Incident Management

1 **Core Capabilities Delivered**

Data Rationalization & Correlation: Fynite's intelligent data pipelines aggregated inputs from 25+ data sources—SIEM, EDR, network logs, identity management, and vulnerability scanners. AI agents automatically validated data integrity, de-duplicated redundant alerts, and ensured each event was contextually tied to known assets, configurations, and user behavior patterns.

2 **Anomaly Detection & Risk Prioritization:** Predictive AI models continuously scanned network and system metrics to detect deviations, classify threats, and assign severity scores based on impact likelihood.

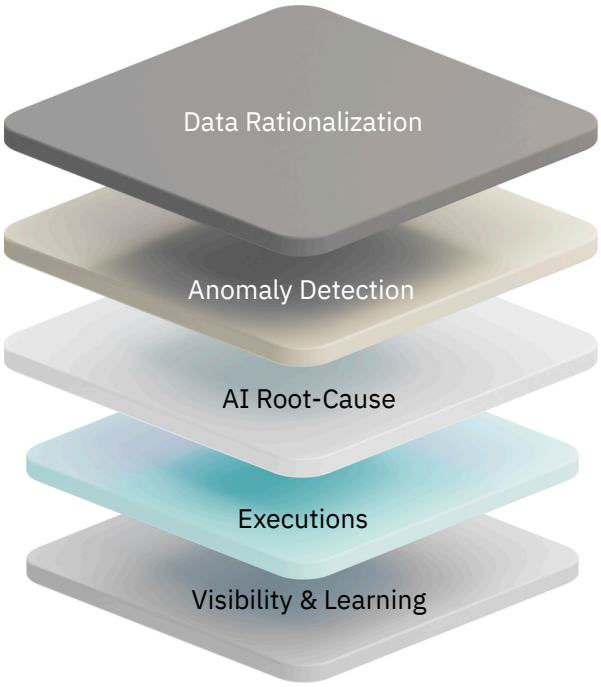
3 **Root-Cause Analysis & Decision Layer:** Using historical event data, FyniteOS' AI Decision Layer identified relationships between recurring anomalies and configuration drift, mapping potential root causes and recommended actions.

4 **Autonomous Execution:** Upon approval or predefined policy triggers, Fynite executed remediation workflows directly from its Execution-as-a-Service™ layer—closing the loop between detection and action.

Examples of Executed Actions:

- Isolated compromised endpoint from network
- Revoked and reissued expired access certificates
- Deployed patch to vulnerable nodes via MDM integration

5 **Closed-Loop Visibility & Learning:** All actions were logged in real time dashboards, providing audit-ready visibility and feeding outcomes back into learning models to reduce false positives over time.

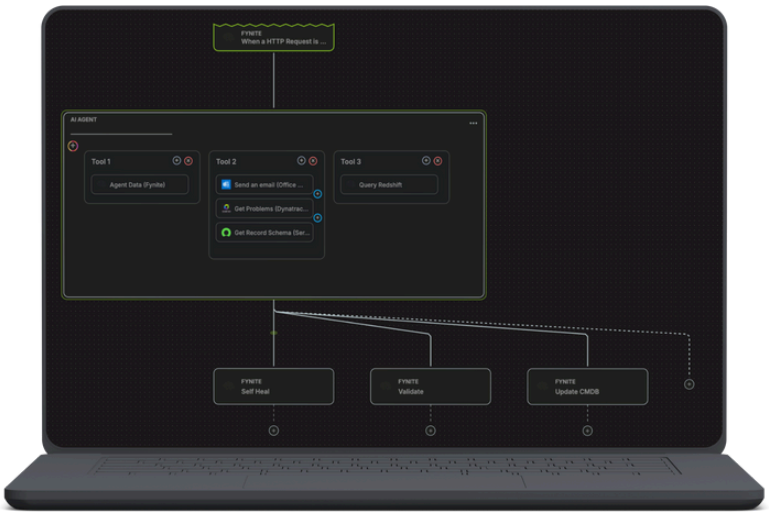


IMPACT & ROI

Metric	Before Fynite	After Fynite
Mean Time to Detect (MTTD)	4 hours	**< 15 minutes**
Mean Time to Respond (MTTR)	12 hours	**< 1 hour**
Manual Workload Reduction	-	**65% fewer manual triage tasks**
Data Consistency Index	72%	**98% accuracy post-rationalization**
ROI	-	**Achieved within 12 weeks via reduced risk exposure and automated workflows**

In: Monitored Events

Out: Action Executions



End to End Workflow Automation

CONCLUSION

By integrating **data-to-decision pipelines** with **autonomous execution**, Fynite transformed cybersecurity operations from reactive defense to predictive resilience.
The enterprise now operates with continuous monitoring, AI-driven response, and auditable trust across its digital ecosystem.

FyniteOS empowers security teams to think less about threats—and focus on strategy.

Fynite.ai | **Execution-as-a-Service™**

(414) 364-2156

CONTACT@FYNITE.AI

TAKE AWAY

Case study shows FyniteOS automates and significantly improve incident management process.

Cross functional
Data visibility and analytics boost logistics efficiency.

Efficiency
Use generative AI for efficiency opportunities and insights.

Automation
End to end workflow Automation.

2135 City Gate Ln, Suite 300 Naperville, IL, 60563, US

www.fynite.ai