CASE STUDY | QUICKSTART

Threadfin's AI-Ready Network Assessment QuickStart

Customer: Frontier Fidelity Banking
Industry: Banking
Locations: Dallas HQ + multiple branch offices across the Midwest
Employees: 3,500
Duration: 20 business days
Delivery Model: Fixed fee

OVERVIEW

Frontier Fidelity Banking is a midwestern regional banking group headquartered in Dallas, with a distributed branch footprint across the Midwest. With over 3,500 employees, their IT environment must support high compliance standards, secure transactional traffic and evolving business needs like remote work, digital banking and intelligent workload adoption. They have been a long-time Threadfin customer, historically engaging for security and network advisory services.

ASSESSMENT SCOPE & OBJECTIVES

Threadfin was engaged to evaluate Frontier's current network architecture and assess readiness for modern, intelligent workloads with an emphasis on:

- Network segmentation and policy enforcement
- Firewall and traffic inspection posture (north/south and east/west)
- Performance baselines and bottlenecks
- Cloud and SaaS connectivity
- AI/ML workload preparedness
- Alignment with zero trust principles

CURRENT COMPUTE ENVIRONMENT

Frontier maintains a multi-site MPLS-based WAN architecture, with firewalled links between HQ, branches and cloud endpoints. Their infrastructure includes:

- Core network: Cisco-based switching & routing backbone
- Firewalling: Fortinet FortiGate appliances deployed across core & branch locations
- Segmentation strategy:
  - VLAN-based segmentation implemented inconsistently
  - Minimal east/west inspection or policy enforcement
  - North/south traffic largely dependent on centralized egress controls
- Cloud connectivity: Azure workloads accessed via site-to-site VPN; some SaaS traffic backhauled through HQ
- Observability tools:
  - FortiAnalyzer deployed, but underutilized
  - No central telemetry for lateral movement or microsegmentation
- Security stack:
  - Fortinet for perimeter
  - Defender for Endpoint in progress
  - Basic DLP policies enforced via M365

threadfin

threadfin.com | info@threadfin.com | 904.473.4840

Threadfin's AI-Ready Network Assessment QuickStart

EXECUTION ACTIVITIES

The assessment was conducted over 4-weeks, combining remote analysis and collaborative workshops. Key execution tasks included:

- **Kickoff & discovery:** Conducted working sessions with network, cloud and security teams to identify architectural goals, pain points and ongoing initiatives.
- **Documentation collection:** Gathered topology diagrams, firewall configs, routing tables and traffic flow documentation. Accessed Fortinet and Cisco devices directly where possible.
- **Firewall rulebase analysis:** Exported and analyzed FortiGate configurations to assess rule count, policy structure, naming consistency and address object reuse. Identified over 2,400 rules in HQ FortiGate with 70+% unused or redundant.
- **Segmentation mapping:** Compared VLANs, subnets,and VRFs against logical business zones (e.g., teller systems, back office, admin, guest). Confirmed lack of policy enforcement between business zones.
- **Traffic flow capture:** Used packet captures, NetFlow and FortiAnalyzer logs to observe traffic paths, focusing on inter-branch, internal server and cloud-destined flows. Noted over 80% of internal east/west traffic was unrestricted.
- **Cloud access review:** Evaluated Azure and SaaS connectivity. Validated that hairpinning of Microsoft 365 and Teams traffic through HQ increased latency and reduced fault tolerance.
- **Performance benchmarking:** Performed synthetic tests and baseline checks across 7 branch-to-HQ paths. Observed congestion during core banking app batch windows.
- **Security control review:** Validated logging, NAT policy usage and consistency of IPS/AV signatures. Determined that branch firewall logging was non-uniform and alerting thresholds were inconsistently applied.
- **AI workload planning session:** Conducted a strategic session with IT and compliance leads to understand upcoming AI/ML use cases, data sensitivity classifications and infrastructure targets.

All work was documented in alignment with Threadfin's structured AI Network Readiness Framework.

KEY FINDINGS & OBSERVATIONS

- **Segmentation gaps:** VLANs exist but do not reflect true business functions. Little to no ACL enforcement between zones.
- **East/west blind spots:** No inspection or monitoring between internal servers, creating exposure to lateral movement risks.
- **Firewall complexity:** Overly permissive access across legacy firewall policies; inconsistent use of address groups or naming standards.
- **Traffic bottlenecks:** Azure and SaaS traffic hairpinned through HQ firewalls, impacting Teams, SharePoint and Outlook Online performance.
- **Lack of monitoring & alerting:** FortiAnalyzer is logging selectively but isn't generating actionable insights due to misconfigured thresholds.
- **Branch variability:** Security configurations vary by branch, increasing audit complexity and creating uneven protections.
- **AI use case constraints:** Planned AI-based fraud detection and behavioral modeling workloads require low-latency, segmented environments with telemetry—none of which currently exist.
- **No SD-WAN:** MPLS is reliable but expensive and inflexible. Lack of SD-WAN capabilities limits path optimization and branch-to-cloud flexibility.

Threadfin's AI-Ready Network Assessment QuickStart

REMEDIATION RECOMMENDATIONS

Short-Term (0–90 Days)

- Firewall cleanup & policy audit
  - Remove redundant rules and address objects
  - Introduce consistent naming conventions and object grouping
  - Implement monthly audit process
- Define business-aligned zones
  - Design production, back office, teller, call center and guest zones with explicit access policies
  - Map ACLs and firewall rules to business function and intent
- Microsegmentation planning
  - Select initial pilot zones for segmentation (e.g., teller systems, internal servers)
  - Build zone-based trust boundaries and validate inter-zone requirements
- FortiAnalyzer tuning
  - Normalize log collection across FortiGates
  - Create alerting policies for lateral movement and east/west anomalies
  - Integrate with SIEM for unified monitoring
- SaaS routing optimization
  - Introduce local internet breakout for Microsoft 365, Teams and critical SaaS services
  - Apply DNS and egress policies to support optimal cloud access
- Adopt zero trust foundations
  - Enforce identity-based access controls on internal systems
  - Require MFA and compliant device posture for sensitive access (internal and remote)
- SD-WAN feasibility study
  - Evaluate vendors and pilot potential configurations
  - Determine cloud-onramp strategy and cost modeling

Long-Term (90–270 Days)

- Deploy microsegmentation
  - Implement zone-specific inspection and policy enforcement
  - Expand from pilot zones to full branch and data center scope
- SD-WAN rollout
  - Replace MPLS at prioritized branches and HQ
  - Leverage dynamic path selection, centralized orchestration and cloud prioritization
- AI workload readiness
  - Create secure enclaves for AI model operations and telemetry
  - Apply data classification, logging and encryption to support model training integrity
- Ongoing policy management & training
  - Establish lifecycle for policy updates and firewall reviews
  - Upskill network team in SD-WAN, microsegmentation and zero trust strategies

threadfin.com | info@threadfin.com | 904.473.4840

CASE STUDY | QUICKSTART

Threadfin's AI-Ready Network Assessment QuickStart

COMPREHENSIVE ENGAGEMENT SUMMARY

Threadfin's AI-Ready Network Assessment provided Frontier Fidelity with a deep and actionable view of its network architecture. Through targeted technical workshops, hands-on firewall analysis and structured traffic mapping, we uncovered the foundational gaps that would hinder secure, high-performance AI adoption.

The final output included prioritized recommendations, architecture visuals, policy diagrams and a roadmap that empowers Frontier's internal teams to act with clarity and urgency. This engagement not only evaluated their current state —it helped shift the conversation from reactive maintenance to forward-looking network modernization, aligned with business growth, compliance obligations and intelligent workload strategies.

threadfin

threadfin.com | info@threadfin.com | 904.473.4840