WHITE PAPER

AIStorm

# ThreatTrace Financial Services Case Studies

How large financial institutions strengthened APT, ransomware, phishing and zero-day detection through network visibility, built-in sandbox analysis and centralized security operations.

**Enterprise APT Monitoring • Network Detection • Sandbox Analysis**

# Table of Contents

# Executive Overview

Financial institutions operate high-value, highly regulated environments where advanced persistent threats (APTs), ransomware, phishing and zero-day exploitation can create significant operational and data-security risk. These banking cases show how ThreatTrace improved advanced-threat visibility, investigation and security-operations efficiency.

ThreatTrace combines network threat detection, traffic analysis, threat intelligence, and a built-in Sandbox in one platform. Suspicious files and objects identified from network traffic can be automatically submitted to the Sandbox for deeper static and dynamic analysis, allowing results to be correlated back into the investigation workflow.

# Case 1 | Tier 1 Bank APT Defense

## Business & Security Requirements

- Complex APT techniques combined with compliance requirements for APT defense under China's Classified Protection (Dengbao) standards.
- Limited security operations staffing and an urgent need to improve automated incident-response efficiency.
- Continued emergence of phishing campaigns and ransomware attacks.

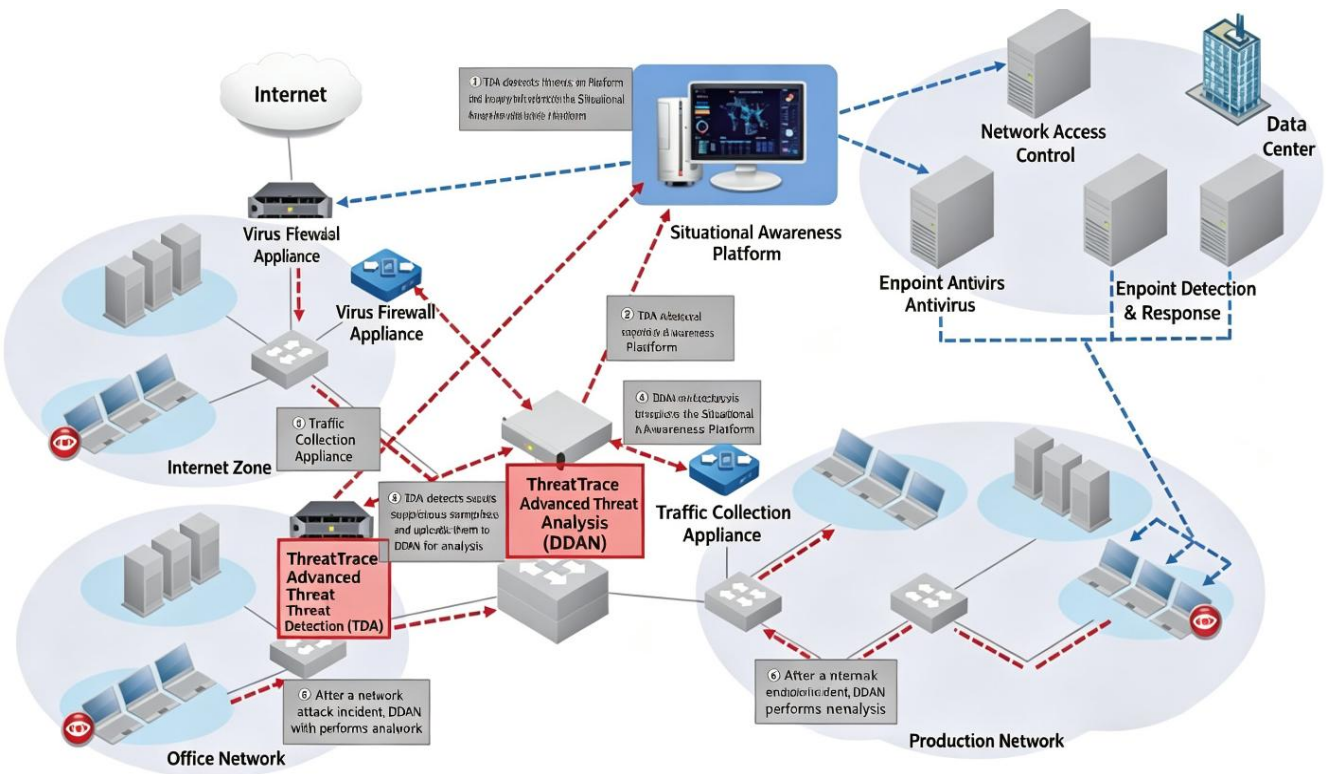
## Deployment Scope

ThreatTrace network sensors were deployed at branch intranet connections, branch-to-HQ interfaces, data center internal networks, and data center internet egress points. ThreatTrace built-in Sandbox were deployed in the data center operations-management zone to perform deep analysis of suspicious objects submitted by ThreatTrace network sensors across locations and return the analysis results. A centralized log-management platform collected, analyzed, and visualized logs generated by ThreatTrace.

# Case 1 | Tier 1 Bank APT Defense

## Business Value

- Integration of ThreatTrace strengthened enterprise-wide advanced-threat protection capabilities.
- Automated processing improved closed-loop security-incident handling efficiency.




*Case 1 Deployment Architecture*

# Case 2 | National Bank – Multi-Site Monitoring

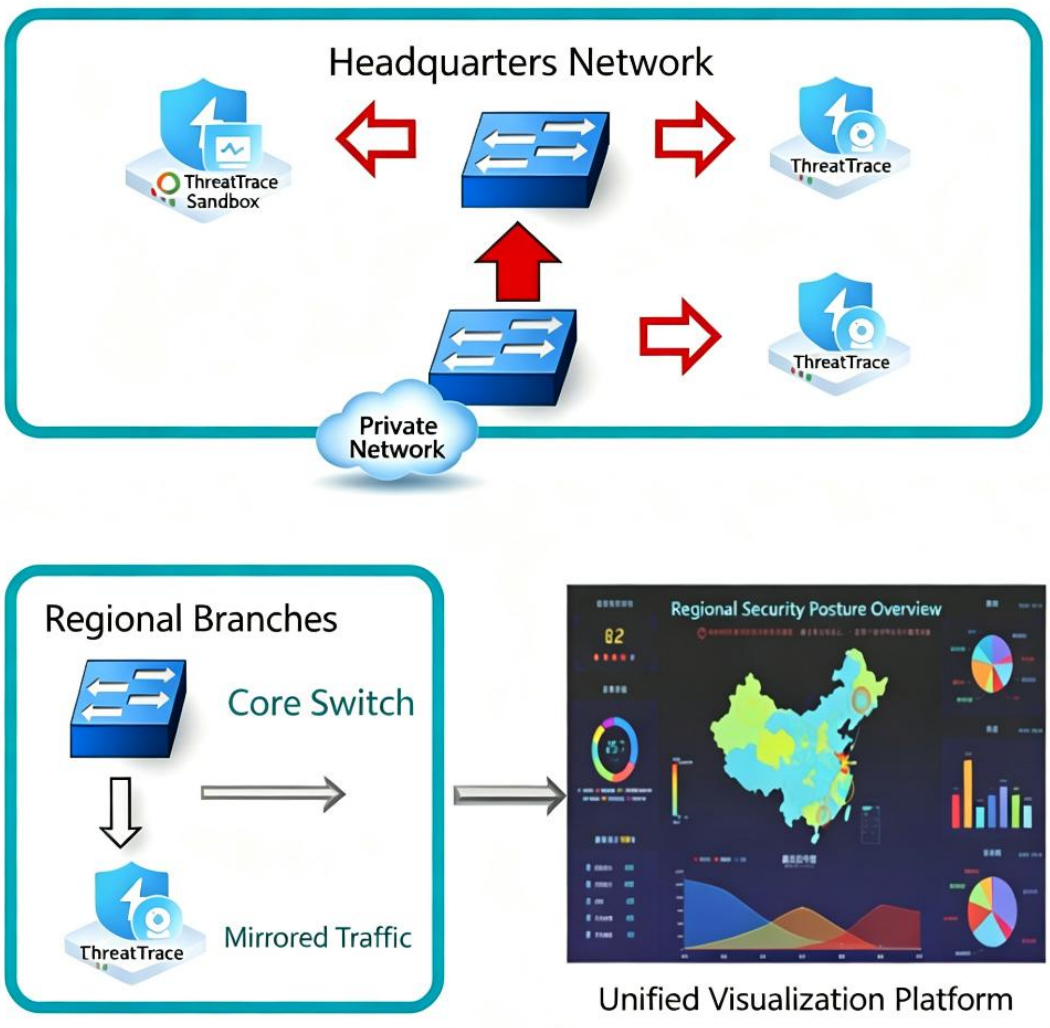
## Business & Security Requirements

Advanced Persistent Threat (APT) attacks often target high-value users and sensitive data. For financial institutions, even comprehensive defense-in-depth architectures can face difficulty preventing internet-originated intrusions and data exfiltration, particularly from APTs, ransomware, and zero-day exploit campaigns.

Against the backdrop of China's Cybersecurity Law, the project called for an APT monitoring capability that could discover advanced threats hidden within the network, support rapid detection and attribution, trace intrusion paths and attack scenarios, and help reduce losses caused by security threats.

# Case 2 | National Bank – Multi-Site Monitoring

## Business & Security Requirements




*Case 2 Monitoring Architecture*

# Case 2 | National Bank – Multi-Site Monitoring

## Project Outcomes

| Metric | Outcome |
|---|---|
| Average data traffic analyzed monthly by ThreatTrace during the deployment year | ~300 TB |
| Threat alerts generated | 300,000+ |
| Malicious IP addresses identified | 2,000+ |
| Threat events flagged as requiring attention | 30+ |
| Files processed monthly by ThreatTrace built-in Sandbox, with approximately 50 classified as high risk | 1.5M+ |
| Alerts related to business server IPs detected by AsiaInfo (AIStorm) APT monitoring in 2022 | 20,000+ |

# Case 2 | National Bank – Multi-Site Monitoring

## Business Value

- Accelerates investigation and coordinated response.
- Strengthens threat traceability and attack attribution.
- Enables timely countermeasures, including IP blocking.
- Protects critical assets from malicious traffic.
- Demonstrates security readiness during inspections.

# Key Takeaways for Financial Instituitions

## Improve Visibility Across Critical Network Points

Strategic placement of network probes at branches, HQ interfaces, data centers, and internet egress points expands visibility into suspicious activity.

## Combine Network Detection with deep file analysis

Integration between ThreatTrace allows suspicious objects detected on the network to undergo deeper sandbox analysis.

## Centralize Investigation and Reporting

Centralized log collection and situational-awareness workflows help security teams correlate findings and communicate security posture.

## Use Automation to Scale Security Operations

Automated analysis and processing can reduce the burden on limited security operations teams and improve closed-loop incident handling.

# Conclusion

These banking deployments demonstrate a layered approach to advanced-threat monitoring: network visibility through ThreatTrace, deeper suspicious-object analysis through ThreatTrace built-in Sandbox, and centralized operations for correlation, investigation and reporting.

For financial institutions facing sophisticated threats and demanding compliance environments, this architecture offers a practical model for strengthening detection and improving security-operations efficiency.

## Request a Demo

Discover how ThreatTrace can strengthen advanced-threat visibility and incident-response operations across your environment.

Visit www.aistorm.com or contact your AIStorm representative.