ChiefNET

CHIEFNET OT SHIELD · USE CASE

Securing Financial Services Infrastructure

Unidirectional Data Transfer for Core Banking, Payments, Trading and Data Centre Systems

Banking · Payments · Trading

Document reference	Version	Date	Published by
CN/OTS/UC/FINSERV/v1.0	1.0	June 2026	ChiefNET Private Limited

Contents

1. Executive Summary
2. Industry Context: Cybersecurity Challenges in Financial Services
3. ChiefNET OT Shield: Solution Overview
4. Reference Architecture
5. Detailed Use Cases
6. Compliance & Standards Alignment
7. Business Value
8. ChiefNET OT Shield vs. Traditional Firewalls
9. Technical Capability Snapshot
10. Deployment & Engagement Model
11. Conclusion

Also available online at chiefnet.io/use-cases/ot-shield/financial-services/

Executive Summary

Banks, payment processors and financial market infrastructure operate systems where availability and integrity are non-negotiable – core banking systems, payment switches, ATM networks and trading platforms must run continuously and cannot tolerate the kind of compromise that a single reversible network path can introduce. Yet these same institutions must feed fraud analytics, regulatory reporting and enterprise data warehouses with near-real-time transaction data, creating exactly the kind of IT/OT-style boundary that data diode technology was built to secure.

ChiefNET OT Shield is a hardware-enforced data diode purpose-built to close that gap. It allows transaction logs, payment switch data, trading feeds and infrastructure telemetry to flow out of the core banking or payments environment into fraud analytics, regulatory reporting and data warehouse systems, while making it physically impossible for any command, malware or intrusion attempt to flow back in. There is no firewall rule to misconfigure and no firmware to patch under strict change-control windows; isolation is built into the hardware itself.

This document presents a use-case-driven view of how ChiefNET OT Shield applies to financial services environments – covering reference architecture, detailed use cases, regulatory alignment, and the business case for deployment across data centres, branches and payment infrastructure.

> **Why this matters for financial institutions**
>
> High-profile financial sector breaches, including the 2016 Bangladesh Bank incident where attackers used compromised SWIFT credentials to attempt fraudulent transfers, have shown that a reversible path into payment messaging infrastructure can translate directly into financial loss. A one-way data export path removes that reversible path entirely for the systems it protects.

Industry Context: Cybersecurity Challenges in Financial Services

A Sector Built on Continuous Availability and Trust

Core banking systems, payment switches and trading platforms are engineered for continuous, high-integrity operation – a few minutes of downtime or a single fraudulent transaction can have material financial and reputational consequences. At the same time, banks are under constant pressure to feed fraud detection, regulatory reporting and data warehouse systems with near-real-time transaction data, which historically has meant bidirectional connectivity between core systems and the broader IT environment.

A Well-Documented Threat History

Financial services remains one of the most heavily targeted sectors for both cybercrime and state-linked actors, given the direct monetary incentive. The 2016 Bangladesh Bank heist, in which attackers used compromised credentials and malware to send fraudulent SWIFT payment instructions, demonstrated how a reversible connection into payment messaging systems can be exploited for direct financial theft. Ransomware and business email compromise campaigns against banks and payment processors have continued at a steady pace, frequently entering through a compromised endpoint on the general IT network before attempting to reach core systems.

Why General-Purpose IT Security Falls Short

- Firewalls and VPNs are software-defined and bidirectional by design – a misconfigured rule, an unpatched CVE, or a stolen credential can open a path back into core banking or payment systems.
- Patch cycles that are routine in general IT are tightly controlled in core banking and payment environments, where change windows are limited and unplanned downtime is unacceptable.
- Financial messaging and settlement protocols carry direct monetary value, making them a high-incentive target for protocol-level and credential-based attacks.
- Many institutions operate legacy core banking platforms alongside modern digital channels, creating complex network paths that are difficult to fully segment with rules alone.

Regulatory and Standards Drivers

Financial institutions operate under some of the most detailed cybersecurity mandates of any sector, and regulators increasingly expect demonstrable network segmentation for critical systems:

- **RBI Cyber Security Framework (India):** requires banks to implement network segmentation, restrict connectivity to critical systems, and demonstrate board-level oversight of cybersecurity controls.
- **SWIFT Customer Security Programme (CSP):** mandates specific controls around segregating the SWIFT messaging environment from the broader corporate network to reduce fraud risk.
- **PCI-DSS:** requires network segmentation to isolate cardholder data environments from other systems, reducing the scope and risk of payment card data exposure.
- **SEBI / Stock Exchange Cybersecurity Guidelines (India):** set expectations for trading and settlement system security, including segregation of critical trading infrastructure.
- **IT Act 2000 & CERT-In Advisories (India):** reinforce baseline security hygiene and incident-reporting obligations for banking and financial critical information infrastructure.

ChiefNET OT Shield: Solution Overview

ChiefNET OT Shield is a purpose-built cybersecurity appliance combining a hardware-enforced data diode with a hardened, cloud-managed communications platform. It is designed to sit precisely at the boundary between core banking, payment or trading systems and the fraud analytics, reporting or data warehouse systems that need visibility into them.

Core Architecture

- Physical transmitter (TX) module on the secure/restricted side and a physically separate receiver (RX) module on the monitoring/enterprise side, joined only through an optical, one-way link.
- No physical mechanism exists for signals to travel from the RX side back to the TX side – isolation is enforced by hardware, not by a rule set that can be disabled or bypassed.
- A hardened operating system on both sides minimises attack surface and removes the general-purpose services that create most software vulnerabilities.

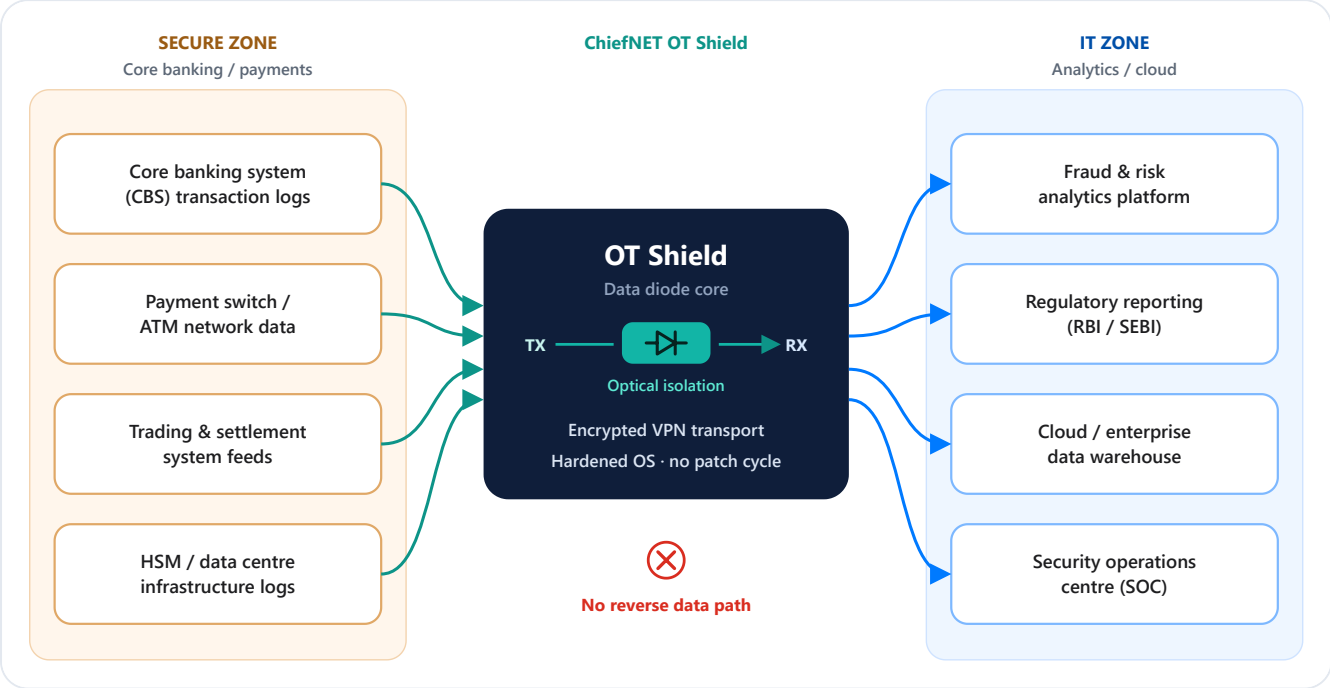
Key Capabilities

- **Native protocol support:** BACnet, Modbus, MQTT, OPC UA and industrial UDP (broadcast/multicast/anycast), covering data centre infrastructure and facility telemetry alongside application-level exports.
- **File and log transfer:** UDP file transfer, Syslog and HTTP PUT for transaction logs, settlement reports and infrastructure event data.
- **Encrypted VPN transport:** data exiting the diode is carried to fraud analytics, regulatory reporting or data warehouse endpoints over a hardened, encrypted tunnel, without reopening a return path.
- **Dual WAN / 4G-5G failover:** on the monitoring (RX) side, ensuring uninterrupted delivery of transaction and infrastructure data even where fixed connectivity is degraded.
- **Built-in SD-WAN functionality:** for institutions with many branches or data centres, enabling secure interconnection with head office while keeping core systems isolated from the broader network.
- **Centralised cloud orchestration:** zero-touch and pre-provisioning, fleet-wide monitoring, alerting and dashboards – essential for institutions managing many branches and processing centres.
- **Zero patch burden:** because isolation is physical rather than rule-based, there is no firewall ruleset or reverse-path exploit to patch against – reducing change-control overhead on core banking systems.

Reference Architecture

Single-Site Deployment – Data Centre / Core Banking Environment

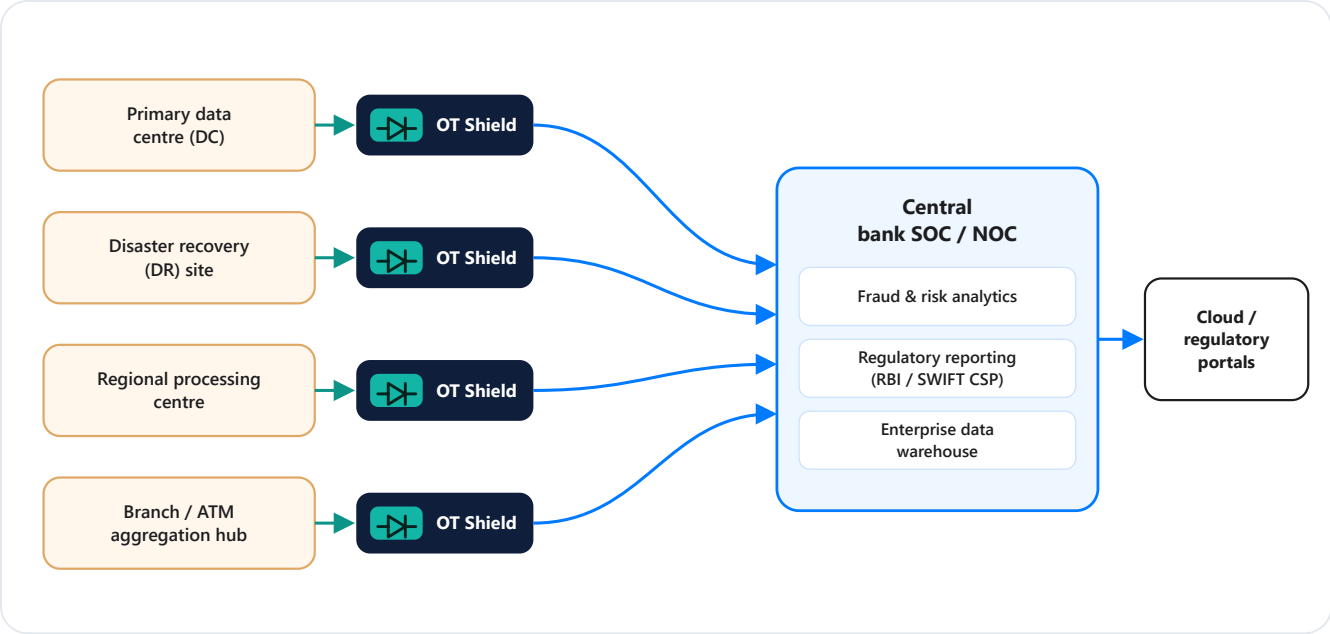
At a data centre or core processing site, ChiefNET OT Shield sits between the secure zone (core banking transaction logs, payment switch and ATM network data, trading and settlement feeds, HSM/data centre infrastructure logs) and the IT zone (fraud and risk analytics, regulatory reporting, enterprise data warehouse, SOC). All operational data leaves the secure zone through the diode's transmitter; nothing can traverse back.



Single-site reference architecture – unidirectional data flow from core banking/payment networks to analytics and reporting systems

Multi-Site Deployment Across Data Centres and Branches

Institutions operating a primary data centre, disaster recovery site, regional processing centres and branch networks can deploy one OT Shield per site, provisioned and monitored from a single cloud console, while each site's isolation guarantee remains entirely local and independent.



Multi-site deployment – data centres and branches converging on a central bank SOC/NOC

Detailed Use Cases

The following use cases illustrate how ChiefNET OT Shield is applied across core banking, payments, trading and data centre environments.

USE CASE 5.1

Core Banking Transaction Log Export for Fraud Analytics

Core Banking & Fraud Prevention

Challenge	Fraud and risk teams need near-real-time transaction data from the core banking system to detect anomalous activity, but the core banking environment must remain isolated from general IT to protect transaction integrity.
OT Shield solution	OT Shield exports core banking transaction logs one-way to a fraud and risk analytics platform over an encrypted VPN, with zero possibility of any command or query being sent back into the core banking system.
Outcome	✓ Near-real-time fraud detection without exposing the core banking system ✓ Core banking environment remains fully isolated from analytics infrastructure ✓ Supports scaling fraud analytics without increasing core system risk

USE CASE 5.2

Payment Switch & ATM Network Monitoring

Payments & Card Networks

Challenge	Payment operations teams need visibility into payment switch and ATM network health and transaction volumes for monitoring and reconciliation, but the payment switch environment is a high-value target that must not accept inbound connections from monitoring systems.
OT Shield solution	OT Shield forwards payment switch and ATM network telemetry one-way to a monitoring and reconciliation platform, supporting UDP and file-transfer protocols without any inbound path into the payment switch environment.
Outcome	✓ Real-time payment operations visibility without payment switch exposure ✓ Reduces attack surface on one of the institution's highest-value systems ✓ Supports faster reconciliation and anomaly detection

USE CASE 5.3

Trading & Settlement System Data Feed for Risk Management

Capital Markets & Trading

Challenge	Risk management teams need trading and settlement data to monitor exposure and compliance in near-real-time, but trading and settlement systems require strict isolation to maintain market integrity and prevent unauthorised order manipulation.
OT Shield solution	OT Shield exports trading and settlement feeds one-way to risk management and compliance monitoring systems, ensuring the trading environment cannot receive any inbound command from the risk platform.
Outcome	✓ Real-time risk and compliance visibility without trading system exposure ✓ Market integrity protected through hardware-enforced one-way isolation ✓ Simplifies audit evidence for exchange and regulator reviews

USE CASE 5.4

Data Centre Infrastructure & HSM Monitoring

Data Centre & Cryptographic Infrastructure

Challenge	Infrastructure teams need visibility into data centre power, environmental and Hardware Security Module (HSM) status for operational monitoring, but these systems underpin the institution's cryptographic and processing infrastructure and must remain tightly isolated.
OT Shield solution	OT Shield exports infrastructure and HSM status telemetry one-way to a centralised data centre monitoring platform, following the same zone/conduit segmentation principles used in critical infrastructure.
Outcome	✓ Centralised infrastructure visibility without exposing cryptographic systems ✓ Consistent segmentation approach across data centres ✓ Simplifies compliance with data centre security audits

USE CASE 5.5

Multi-Branch & Multi-DC Regulatory Reporting Aggregation

Regulatory Reporting (RBI / SEBI / SWIFT CSP)

Challenge	Institutions must submit periodic transaction, risk and compliance data to regulators from multiple data centres and processing sites, and must also demonstrate network segregation under frameworks such as the RBI Cyber Security Framework and SWIFT CSP.
OT Shield solution	OT Shield provides both the compliance evidence (a physically enforced, documented one-way boundary) and the mechanism for automated aggregation of regulatory data from multiple sites into central reporting systems.
Outcome	✓ Simplifies audits by providing a hardware-verifiable segregation control ✓ Automates recurring regulatory data submissions across sites ✓ Reduces audit preparation effort across data centres and branches

USE CASE 5.6

Disaster Recovery (DR) Site Replication Monitoring

Business Continuity & DR

Challenge	Business continuity teams need to monitor replication status and data integrity between the primary data centre and DR site, without creating a reversible path that could be exploited to compromise both sites simultaneously.
OT Shield solution	OT Shield exports replication status and integrity telemetry one-way from the primary site to a central monitoring platform, ensuring the primary and DR environments remain protected from any inbound path introduced by the monitoring layer.
Outcome	✓ Continuous DR readiness visibility without introducing a cross-site attack path ✓ Primary and DR environments retain independent, hardware-enforced isolation ✓ Supports business continuity audit and testing requirements

Compliance & Standards Alignment

The table below maps ChiefNET OT Shield capabilities to the regulatory and standards expectations most relevant to financial institutions.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
RBI Cyber Security Framework (India)	Implement network segmentation and restrict connectivity to critical banking systems.	Hardware data diode enforces one-way transfer, providing a demonstrable segmentation control for critical systems.
SWIFT Customer Security Programme (CSP)	Segregate the SWIFT messaging environment from the broader corporate network.	OT Shield provides physically enforced segregation between payment messaging infrastructure and reporting/analytics systems.
PCI-DSS	Segment cardholder data environments from other systems.	Supports scope reduction by isolating cardholder data environment exports through a one-way hardware boundary.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
SEBI / Stock Exchange Cybersecurity Guidelines	Segregate critical trading and settlement infrastructure.	OT Shield enforces a one-way conduit between trading systems and risk/compliance monitoring platforms.
IT Act 2000 / CERT-In Advisories	Maintain baseline security hygiene and incident reporting for financial critical infrastructure.	Reduces the attack surface that leads to reportable incidents; simplifies audit evidence.

Business Value

Business Driver	Impact of ChiefNET OT Shield
Transaction integrity & availability	Removes the most common remote-attack vector into core banking and payment systems, reducing risk of fraud or intrusion-driven outages.
Regulatory audit readiness	Provides a hardware-verifiable segregation control that is straightforward to demonstrate to RBI, SEBI and SWIFT auditors.
Operational cost	Eliminates recurring firewall patch cycles and associated change-control overhead on core banking systems.
Digital banking pace	Allows fraud analytics, data warehouse and reporting initiatives to proceed without re-architecting core systems.
Multi-site scalability	Centralised, zero-touch provisioning supports rollout across many branches and data centres from a single management platform.
Incident response	Rapid, low-risk access to transaction and infrastructure logs speeds up investigation after a security event.

ChiefNET OT Shield vs. Traditional Firewalls

In financial services, where transaction integrity has direct monetary consequences and change windows on core systems are tightly controlled, the distinction between rule-based and hardware-enforced isolation is a first-order design decision.

Dimension	ChiefNET OT Shield	Traditional Firewall
Data directionality	One-way, physically enforced	Two-way, governed by software rules
Patch / maintenance burden	None – isolation is hardware, not firmware	Frequent patching, often needing tightly controlled change windows

Dimension	ChiefNET OT Shield	Traditional Firewall
Misconfiguration risk	Not applicable – no rule set to misconfigure	Common cause of real-world financial sector breaches
Resistance to remote exploitation	Near-total – no reverse path exists to exploit	Moderate; depends on rule hygiene and patch currency
Fit for core banking / payment systems	Purpose-built for this class of asset	Adequate for general IT; not ideal for core systems
Audit / compliance evidence	Physically demonstrable segregation	Requires ongoing rule and log review to evidence

Technical Capability Snapshot

Capability	Specification
Throughput	Up to 1 Gbps
Isolation	100% one-way, optical / hardware-enforced physical air gap
Software exploit surface on reverse path	Zero – no reverse channel exists
Protocols supported	BACnet, Modbus, MQTT, OPC UA, industrial UDP (broadcast/multicast/anycast)
Data / file transfer	UDP file transfer, Syslog, HTTP PUT
Transport security	Encrypted VPN tunnel from RX side to analytics/reporting endpoint
WAN connectivity (RX side)	Dual WAN with 4G/5G failover for uninterrupted delivery
Management	Cloud-hosted controller, zero-touch and pre-provisioning, fleet dashboards and alerting
Operating system	Hardened OS, minimised attack surface, no routine patch cycle required
Additional networking	Built-in SD-WAN for secure multi-site interconnection alongside core system isolation

Deployment & Engagement Model

ChiefNET recommends a phased engagement for financial services deployments, allowing institutions to validate the solution at one representative data centre or branch before wider rollout.

Phase 1 – Assessment & Design

- Site survey of the target data centre or branch: network topology, protocols in use, existing firewall/VPN posture.
- Identification of required data points (transaction logs, payment switch data, trading feeds) and target analytics/reporting destinations.
- Reference architecture finalised against RBI, SWIFT CSP and PCI-DSS segmentation requirements as applicable.

Phase 2 – Pilot Deployment

- OT Shield installed at one representative data centre or branch, configured for the identified protocols and data flows.
- Validation of one-way data delivery, VPN transport and dashboard visibility with operations and risk teams.
- Compliance walkthrough to confirm alignment with the institution's cybersecurity policy and applicable regulations.

Phase 3 – Fleet Rollout (site-dependent)

- Zero-touch provisioning used to scale deployment across remaining data centres and branches.
- Central bank SOC/NOC dashboards extended to provide institution-wide monitoring and alerting.
- Documentation and audit evidence packaged for regulatory and internal compliance reviews.

Phase 4 – Ongoing Support

- ChiefNET provides device health monitoring, remote diagnostics support and periodic architecture reviews as the institution's monitoring and analytics needs evolve.

Conclusion

Financial institutions face a structural challenge: the same connectivity that enables modern fraud analytics, regulatory reporting and digital banking also expands the attack surface of systems where a compromise translates directly into financial loss. ChiefNET OT Shield resolves this tension directly – not by adding another rule set to manage, but by making the reverse path physically impossible.

Across core banking, payments, trading and data centre environments, the use cases in this document show a consistent pattern: transaction and infrastructure data flows out for analytics, reporting and monitoring, while command-and-control risk is removed at the hardware level. For institutions balancing digital transformation against the non-negotiable integrity requirements of financial systems, that combination – visibility without exposure – is the foundation ChiefNET OT Shield is built to provide.

Next Step

ChiefNET recommends starting with a site assessment and pilot deployment at one representative data centre or branch, validating data delivery and compliance alignment before scaling across the institution.

ChiefNET

About ChiefNET Private Limited

ChiefNET Private Limited, founded in 2020 and headquartered in Coimbatore, India, builds secure networking products for enterprises and critical infrastructure: ChiefNET SD-WAN, a cloud-managed network platform for multi-site organisations, and ChiefNET OT Shield, a hardware-enforced data diode for operational technology. ChiefNET product series are Make in India certified.

---

contact@chiefnet.io · chiefnet.io
DVP Building, First Floor, No. 4, Kalapatti Main Road, Civil Aerodrome Post, Nehru Nagar West, Coimbatore, Tamil Nadu 641014, India