ChiefNET

CHIEFNET OT SHIELD · USE CASE

Industry Vertical & Cross-Functional Use Cases

Extending Unidirectional OT-to-IT Protection Across Additional Industry Verticals and Cross-Cutting Security Functions

Oil & Gas · Water · Transport · and more

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

Contents

1. Executive Summary
2. ChiefNET OT Shield
3. Universal Reference Architecture
4. Industry Coverage Overview
5. Industry Vertical Use Cases
6. Cross-Functional Use Cases
7. Compliance & Standards Alignment Across Sectors
8. Business Value
9. ChiefNET OT Shield vs. Traditional Firewalls / VPNs
10. Technical Capability Snapshot
11. Deployment & Engagement Model
12. Conclusion

Also available online at chiefnet.io/use-cases/ot-shield/additional-industries/

Executive Summary

ChiefNET OT Shield has already been documented in detail for five sectors – Power Generation & Grid, Industrial Control Systems (ICS), Defence, Healthcare, and Financial Services. The underlying pattern in every case is the same: a hardware-enforced data diode that lets operational data flow out of a restricted or safety-critical network for monitoring, analytics and compliance, while making it physically impossible for anything to flow back in.

That same pattern applies well beyond those five sectors, and also cuts across sectors as a set of reusable security functions in their own right. This document collects both: additional industry verticals where ChiefNET OT Shield solves the same fundamental problem – safe one-way data export from a restricted network – and cross-functional use cases that are not tied to any single industry, such as ransomware-resilient backup, SIEM log aggregation, and third-party monitoring access.

Together with the five sector-specific documents, this gives a complete picture of where ChiefNET OT Shield applies across an enterprise's critical infrastructure, industrial, government, healthcare and financial estate – and of the security functions it enables regardless of which industry is asking.

> **How to use this document**
>
> Each use case below follows the same Challenge / Solution / Outcome format as the sector-specific documents, but in a more condensed form suitable for a broad reference. Where a prospect's need matches one of these use cases closely, ChiefNET can expand it into a full standalone use case document on request.

ChiefNET OT Shield

ChiefNET OT Shield is a hardware-enforced data diode combining a physical transmitter (TX) on the restricted/OT side and a physically separate receiver (RX) on the monitoring/IT 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.

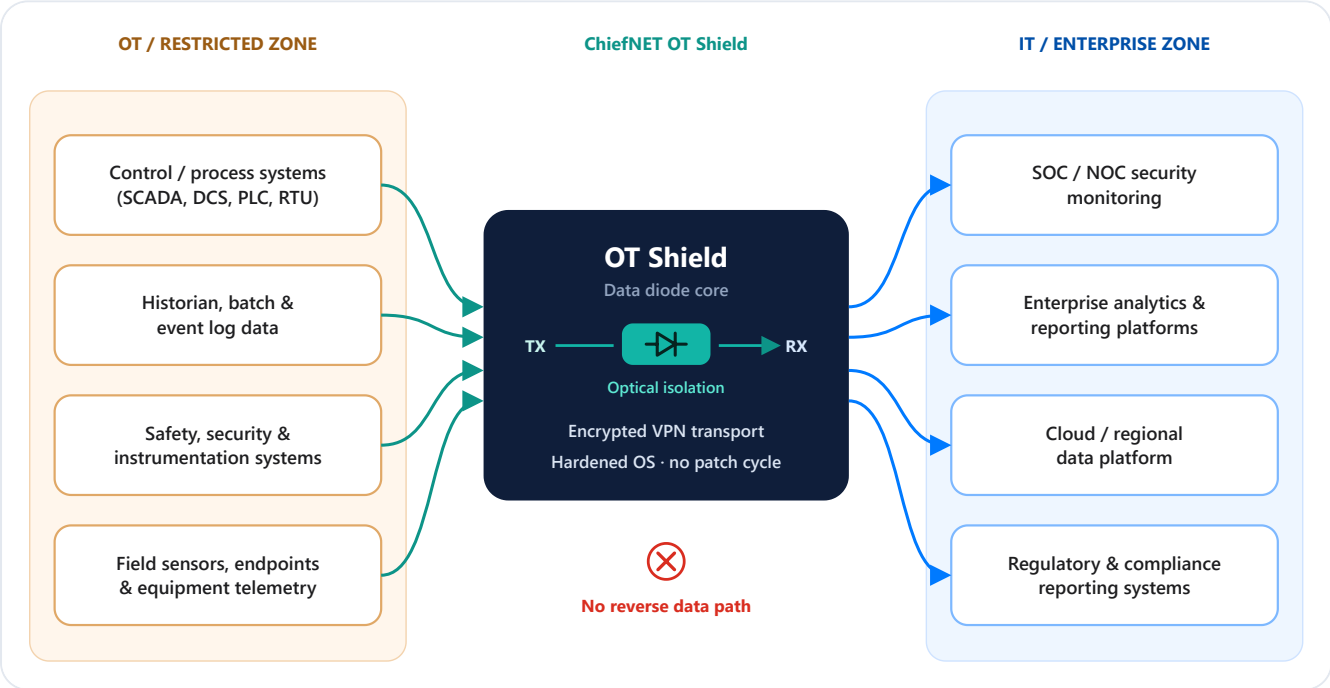
Key Capabilities

- **Native protocol support:** BACnet, Modbus, MQTT, OPC UA and industrial UDP (broadcast/multicast/anycast).
- **File and log transfer:** UDP file transfer, Syslog and HTTP PUT for historian exports, event logs and file-based records.

- **Encrypted VPN transport:** data exiting the diode is carried to its destination over a hardened, encrypted tunnel.
- **Dual WAN / 4G-5G failover:** on the monitoring (RX) side, for uninterrupted delivery even over unreliable connectivity.
- **Built-in SD-WAN:** for multi-site organisations, securely interconnecting sites while keeping each site's restricted network isolated.
- **Centralised cloud orchestration:** zero-touch and pre-provisioning, fleet-wide monitoring, alerting and dashboards.
- **Zero patch burden:** isolation is physical, so there is no firewall ruleset or reverse-path exploit to patch against.

Universal Reference Architecture

Regardless of industry, the architecture pattern is identical: a restricted or safety-critical zone containing control, safety, or transaction systems; ChiefNET OT Shield as the one-way conduit; and an enterprise or monitoring zone containing the analytics, reporting and compliance systems that consume the exported data.

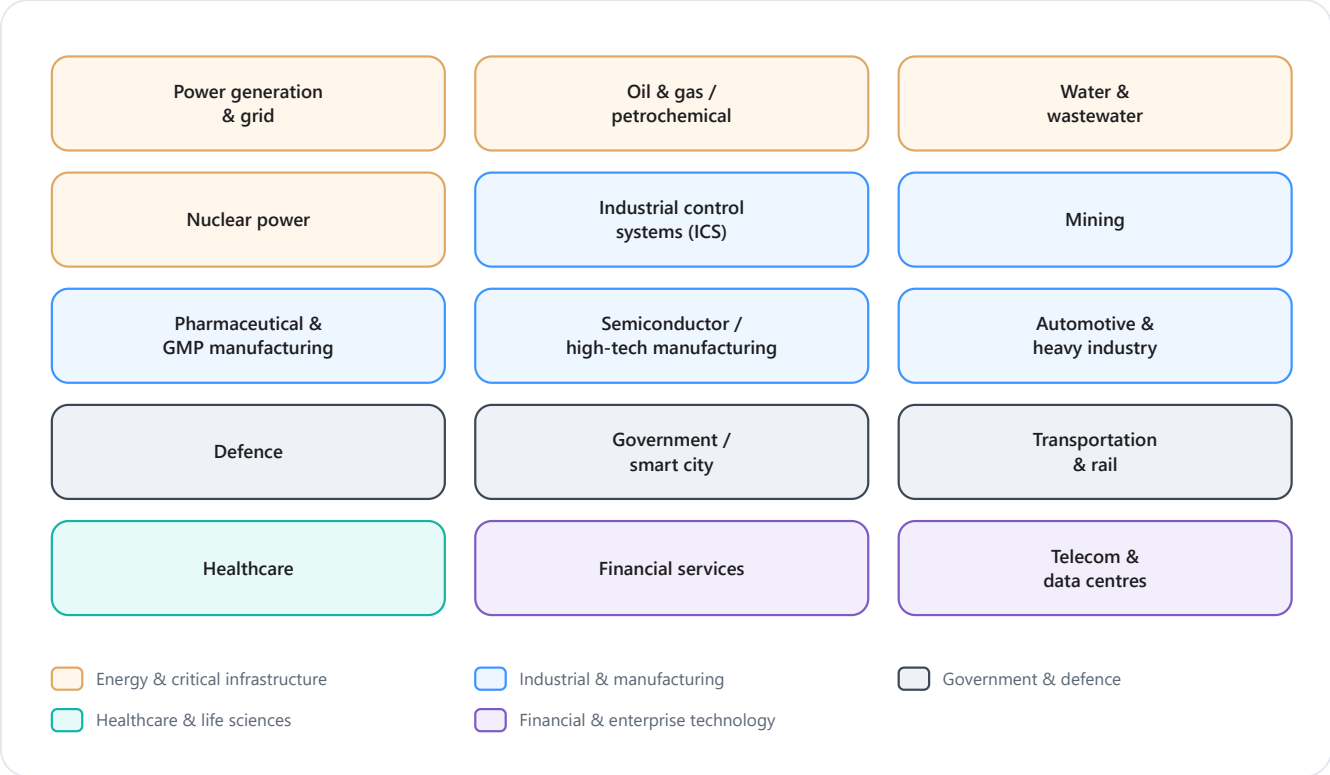


Universal single-site reference architecture, applicable across all verticals in this document

The use cases that follow simply change what sits in the left-hand (restricted) and right-hand (enterprise/monitoring) boxes – the isolation guarantee in the middle never changes.

Industry Coverage Overview

ChiefNET OT Shield is now documented across fifteen industry verticals in total – five with dedicated, in-depth use case documents, and ten more covered in this supplementary document. The map below shows the full portfolio.



ChiefNET OT Shield industry coverage across critical infrastructure, industrial, government, healthcare and financial sectors

Sections 5 and 6 of this document detail the ten additional verticals and the five cross-functional use cases respectively. For Power Generation & Grid, ICS, Defence, Healthcare and Financial Services, refer to the dedicated use case documents already provided.

Industry Vertical Use Cases

The following ten verticals apply the same hardware-enforced, one-way data export pattern used in the dedicated Power Generation & Grid, ICS, Defence, Healthcare and Financial Services documents – adapted to the specific systems and regulatory drivers of each industry.

USE CASE 5.1

Pipeline & Refinery SCADA / Historian Export

Oil & Gas / Petrochemical

Challenge	Pipeline control centres and refineries need real-time SCADA and historian data for production optimisation, leak detection analytics and HSE reporting, but pipeline and refinery control networks are high-consequence targets that must not accept inbound connections.
OT Shield solution	OT Shield exports pipeline SCADA telemetry, tank farm levels and refinery DCS historian data one-way to production optimisation, leak-detection and HSE reporting systems, using Modbus/OPC UA/UDP support with zero possibility of command write-back.
Outcome	✓ Real-time production and HSE visibility without exposing pipeline/refinery control ✓ Supports leak-detection analytics fed by continuous telemetry ✓ Control network remains fully isolated across remote and unmanned sites

USE CASE 5.2

Water & Wastewater Treatment Plant Monitoring

Water & Wastewater Utilities

Challenge	Public utilities must report treatment quality and process data to regulators and central operations, but treatment plant PLC/SCADA systems directly control chemical dosing and public health-critical processes.
OT Shield solution	OT Shield forwards treatment process data, chlorine dosing levels and pump station telemetry one-way to central operations and regulatory reporting systems, keeping dosing and control logic fully isolated from any external network.
Outcome	✓ Continuous regulatory and quality reporting without touching dosing control ✓ Protects a public-health-critical process from remote manipulation ✓ Scales across many distributed treatment and pump sites

USE CASE 5.3

Reactor Protection & Plant Information System Export

Nuclear Power

Challenge	Nuclear plant information systems and regulators require continuous access to reactor protection and safety system data, but these are the most safety-critical systems in the facility and must never accept any inbound signal.
OT Shield solution	OT Shield provides one-way export from reactor protection and safety instrumentation to the plant information system and regulatory reporting platform – a role consistent with the original, longest-standing use case for hardware data diodes in critical infrastructure.
Outcome	✓ Continuous safety-system visibility with zero reverse-path risk ✓ Aligns with the highest-assurance segregation expectations in the sector ✓ Supports regulator and plant-information-system reporting simultaneously

USE CASE 5.4

Railway Signalling & Metro SCADA Data Export

Transportation & Rail

Challenge	Railway and metro operators need signalling status, interlocking and asset telemetry at central control for performance monitoring and predictive maintenance, but signalling and interlocking systems are safety-of-life systems requiring strict isolation.
OT Shield solution	OT Shield exports signalling status, interlocking event logs and rolling-stock telemetry one-way to central control and asset-management platforms, preserving complete isolation of the signalling network.
Outcome	✓ Central visibility into signalling and asset health without safety-system exposure ✓ Supports predictive maintenance for rolling stock and track assets ✓ Consistent architecture across stations, depots and control centres

USE CASE 5.5

Remote Mine Site SCADA & Fleet Telemetry

Mining

Challenge	Mining operators need production, safety and fleet telemetry from remote or underground sites at head office, but mine-site SCADA and haulage/conveyor control systems are often unmanned and connected over long-haul or satellite links vulnerable to interception.
OT Shield solution	OT Shield, paired with dual-WAN/4G-5G failover, transmits production, ventilation-safety and fleet-management telemetry one-way from the mine site to head office, keeping site control systems isolated even over public or satellite backhaul.
Outcome	✓ Continuous production and safety visibility from remote, unmanned sites ✓ Site control systems remain isolated even over long-haul or satellite links ✓ Zero-touch provisioning simplifies rollout across dispersed mine sites

USE CASE 5.6

Batch Record & Process Historian Export for GMP Compliance

Pharmaceutical & GMP Manufacturing

Challenge	Pharmaceutical manufacturers must retain and report validated batch records and process data for regulatory (GMP-equivalent) compliance, but the validated production control system cannot be modified or exposed without triggering costly re-validation.
OT Shield solution	OT Shield exports batch records, process historian data and equipment logs one-way to a quality and compliance reporting system, without any change to the validated control system that would trigger re-validation.
Outcome	✓ Regulatory batch reporting achieved without disturbing validated systems ✓ Avoids re-validation costs associated with control-system changes ✓ Consistent compliance evidence across multiple production lines

USE CASE 5.7

Fab Equipment Telemetry & Yield Data Export

Semiconductor / High-Tech Manufacturing

Challenge	Fabs need equipment telemetry and yield data for process engineering and IP-sensitive analytics, but fab tool networks carry highly proprietary process recipes that must never be exposed to inbound access.
OT Shield solution	OT Shield exports equipment telemetry and yield data one-way to process engineering and analytics platforms, protecting proprietary process IP by design rather than relying solely on access control policy.
Outcome	✓ Yield and process analytics enabled without IP exposure risk ✓ Fab tool network protected from inbound access by hardware design ✓ Supports multi-fab data aggregation for engineering benchmarking

USE CASE 5.8

Carrier-Grade Network Element & Data Centre Monitoring

Telecom & Data Centre / Cloud Providers

Challenge	Telecom operators and data centre providers need performance and security telemetry from core network elements and infrastructure for NOC monitoring, but core network elements are high-value targets that must not accept inbound monitoring connections.
OT Shield solution	OT Shield exports performance, security and environmental telemetry one-way from core network elements and data centre infrastructure to the NOC/SOC, without granting the monitoring platform any path back into core infrastructure.
Outcome	✓ Real-time NOC/SOC visibility without core network exposure ✓ Reduces attack surface on carrier-grade and data centre infrastructure ✓ Scales across multiple sites and points of presence

USE CASE 5.9

Traffic Management & Public Safety System Reporting

Government / Smart City

Challenge	City traffic management, public safety and e-governance backend systems need to feed dashboards and reporting portals, but these systems often control physical infrastructure (traffic signals, public safety alerts) that must remain isolated from public-facing networks.
OT Shield solution	OT Shield exports traffic and public-safety system data one-way to city dashboards, reporting portals and e-governance backends, keeping the systems that control physical infrastructure isolated from any public-facing or inbound path.
Outcome	✓ Public dashboards and reporting enabled without exposing control systems ✓ Protects safety-of-life traffic and public safety infrastructure ✓ Supports e-governance data-sharing mandates without new attack surface

USE CASE 5.10

Robotics Cell Telemetry & Supplier IP Protection

Automotive & Heavy Industry Manufacturing

Challenge	Automotive and heavy-industry manufacturers want production-line telemetry for OEE and quality analytics, and sometimes need to share limited data with suppliers, but robotics cell and line-control networks carry proprietary process IP that must not be exposed.
OT Shield solution	OT Shield exports robotics cell and production-line telemetry one-way to OEE/quality analytics platforms and controlled supplier data-sharing portals, protecting proprietary line-control IP from any inbound access.
Outcome	✓ OEE and quality analytics enabled without exposing line-control IP ✓ Supports controlled supplier data sharing without direct network access ✓ Consistent protection across multiple production lines and plants

Cross-Functional Use Cases

The following five use cases are not tied to any single industry. They describe security functions that ChiefNET OT Shield enables regardless of sector – and that frequently apply on top of any of the industry-specific use cases already documented.

USE CASE 6.1

SIEM / Security Log Aggregation

Cross-Sector – Security Operations

Challenge	Security teams want OT security and event logs flowing into a central SIEM for correlation and threat detection, but connecting a SIEM bidirectionally to OT – or to multiple OT networks – creates a single point of compromise that could reach every connected OT environment.
OT Shield solution	OT Shield forwards OT security logs and events one-way into the SIEM via Syslog/UDP, so the SIEM (or an attacker who compromises it) can never use that connection to reach back into any OT network it monitors.
Outcome	✓ Centralised threat correlation without creating a path back into OT ✓ Removes the SIEM as a potential pivot point into multiple OT networks ✓ Scales safely as more OT sites are added to central monitoring

USE CASE 6.2

Air-Gapped Backup & Ransomware-Resilient Vaulting

Cross-Sector – Business Continuity

Challenge	Organisations need offsite backups that survive a ransomware attack on production systems, but backup systems reachable bidirectionally from production are frequently encrypted or deleted by the same attacker that compromises production.
OT Shield solution	OT Shield replicates critical data one-way into an isolated backup vault; because the vault has no inbound path from production, ransomware or an attacker that fully compromises production cannot reach, encrypt or delete the vaulted copies.
Outcome	✓ Backup copies survive even a total compromise of production systems ✓ Directly addresses the primary way modern ransomware defeats backups ✓ Applicable on top of any industry-specific OT Shield deployment

USE CASE 6.3

Inter-Agency / Cross-Domain Government Data Sharing

Cross-Sector – Government

Challenge	Government agencies often need to move data between networks with different trust or classification levels – for example from a secure operational network to a lower-trust reporting or public-facing system – without creating a bridge between the two domains.
OT Shield solution	OT Shield provides a physically enforced one-way path from the higher-trust domain to the lower-trust domain, allowing approved data to move across without ever permitting a connection in the reverse direction.
Outcome	✓ Enables inter-agency and public reporting without bridging trust domains ✓ Physically enforced control suitable for cross-domain accreditation ✓ Reusable pattern across defence, smart-city and public-sector deployments

USE CASE 6.4

Managed Security Service Provider (MSSP) Monitoring Access

Cross-Sector – Outsourced Security Operations

Challenge	Organisations that outsource OT security monitoring to an MSSP need to give that third party visibility into OT telemetry and alerts, but granting an external party any inbound access into OT expands the organisation's attack surface to include the MSSP's own security posture.
OT Shield solution	OT Shield gives the MSSP a one-way feed of the telemetry and alerts it needs to monitor, with no inbound path from the MSSP (or anyone who compromises the MSSP) back into the client's OT environment.
Outcome	✓ Third-party monitoring enabled without inheriting the MSSP's risk ✓ Client OT environment protected even if the MSSP itself is compromised ✓ Simplifies contractual and audit language around third-party access

USE CASE 6.5

Chain-of-Custody / Forensic Log Archiving

Cross-Sector – Legal & Forensic Integrity

Challenge	Legal, audit and forensic teams need OT and security logs archived in a way that can be trusted as evidence – but logs that remain reachable and writable from the production network can be argued to have been altered.
OT Shield solution	OT Shield exports logs one-way into a write-once forensic archive that has no path back to production, supporting a defensible chain of custody because the archived logs cannot have been reached or altered from the production side after export.
Outcome	✓ Stronger evidentiary standing for logs used in investigations or litigation ✓ Archive integrity is a property of the architecture, not just policy ✓ Applicable as an add-on to any of the industry-specific deployments

Compliance & Standards Alignment Across Sectors

While each industry has its own specific regulatory framework (documented in the sector-specific use case documents), the standards below recur across most of the additional verticals and cross-functional use cases in this document.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
IEC 62443 (Zones & Conduits)	Segment industrial and automation control systems into security zones connected by controlled conduits.	OT Shield functions as a physically-enforced conduit between zones with only one permitted direction of flow.
NIST SP 800-82 / NIST Cybersecurity Framework	Recommends unidirectional gateways at high-consequence OT/IT boundaries; supports the Protect and Recover functions.	Hardware data diode directly implements the unidirectional gateway control, and underpins ransomware-resilient backup (Recover).

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
ISO/IEC 27001 (Information Security Management)	Requires documented network segmentation and access control as part of an information security management system.	Provides a hardware-verifiable segregation control that is straightforward to evidence in an ISMS audit.
Sector-specific regulation (GMP, HSE, telecom licensing, etc.)	Require demonstrable protection of safety-critical, proprietary or licensed systems.	One-way export satisfies segregation expectations without modifying the underlying regulated or validated system.
Chain-of-custody / evidentiary standards	Require that archived logs and records be demonstrably unaltered after capture.	Physical one-way export to a write-only archive supports a defensible chain of custody.

Business Value

Business Driver	Impact of ChiefNET OT Shield
Ransomware resilience	Air-gapped, one-way backup vaulting ensures a clean recovery copy survives even a total production compromise.
Third-party risk reduction	MSSP and vendor monitoring access can be granted without inheriting the third party's own security risk.
Regulatory & audit readiness	A hardware-verifiable segregation control is straightforward to demonstrate across ISO 27001, IEC 62443 and sector-specific audits.
Cross-domain data sharing	Enables government, defence and enterprise data sharing across trust boundaries without bridging them.
Portfolio consistency	A single architectural pattern scales across fifteen industry verticals, simplifying training, support and proposal development.
Operational cost	Eliminates recurring firewall patch cycles and associated outage windows across every use case in this document.

ChiefNET OT Shield vs. Traditional Firewalls / VPNs

Across every use case in this document – whether an industry vertical or a cross-cutting security function – the same structural advantage applies: hardware-enforced isolation cannot be bypassed by a configuration error, stolen credential, or software exploit.

Dimension	ChiefNET OT Shield	Traditional Firewall / VPN
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 outage windows
Misconfiguration risk	Not applicable – no rule set to misconfigure	Common root cause of real-world breaches
Backup / archive integrity	Physically unreachable from production once exported	Vulnerable to attackers who compromise production credentials
Third-party access risk	Third party receives data with no path back to source	Third-party compromise can become a path into the source network
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 destination 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 isolation

Deployment & Engagement Model

Regardless of vertical or use case, ChiefNET recommends the same phased engagement: validate on one representative use case, then scale.

Phase 1 – Assessment & Design

- Identify the specific restricted system(s) and the destination system(s) that need one-way data delivery.
- Confirm protocols, data volumes and any sector-specific compliance requirements relevant to the use case.

Phase 2 – Pilot Deployment

- OT Shield installed and configured for the identified use case; one-way delivery and transport security validated with stakeholders.

Phase 3 – Scale-Out (use-case dependent)

- Zero-touch provisioning used to extend the same pattern across additional sites, systems or use cases.

Phase 4 – Ongoing Support

- ChiefNET provides device health monitoring, remote diagnostics and periodic architecture reviews as needs evolve.

Conclusion

The use cases in this document – spanning ten additional industry verticals and five cross-functional security scenarios – all rest on the same underlying principle already demonstrated across Power Generation & Grid, ICS, Defence, Healthcare and Financial Services: operational or sensitive data should be able to leave a restricted network for monitoring, analytics and compliance, without that network ever being reachable from the outside.

Whether the restricted system is a nuclear reactor protection system, a fab tool network, a backup vault, or a third-party MSSP connection, the architecture does not change – only what sits on either side of it. That consistency is what allows ChiefNET OT Shield to scale across fifteen industry verticals and a growing set of cross-cutting security functions from a single, well-understood product.

Next Step

Where any use case in this document closely matches an active opportunity, ChiefNET can expand it into a full standalone use case document – with dedicated architecture diagrams, compliance mapping and business case – in the same format as the five sector-specific documents already provided.

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