LUSQUAN B.V.

PROTECTING YOU NOT EXPOSING YOU

PUBLICATION PUB-TSHIELD-INFO-001

TSHIELD

Enterprise Cyber Defence Information Pack

Visibility. Detection. Controlled response. Evidence.

A SELF-CONTAINED DEFENCE PLATFORM

Transparent network enforcement

Operational security intelligence

Incident ownership and automation

EDITION

2026.1

CLASSIFICATION

PUBLIC

lusquan.com/tshield-information

PUBLICATION CONTROL

A real pack with explicit evidence boundaries

This document is designed for decision-makers, technical evaluators, procurement teams and operational security leaders.

CONTROLLED

Publication identity

Stable reference, edition, classification and public verification path.

HONEST

Capability integrity

Every material feature is marked by delivery status rather than presented as universally available.

AVAILABLE NOW	Implemented in the current product baseline.
VALIDATED	Implemented and exercised in controlled production tests.
INTEGRATION-DEPENDENT	Requires compatible telemetry, placement or third-party integration.
PLANNED	Defined product direction; not represented as delivered.
CONCEPTUAL	Research architecture or scenario requiring validation.

THE RULE THAT GOVERNS THIS PACK

TShield is described by what it can demonstrate - not by what marketing language might imply.

No security product can guarantee prevention. Outcomes depend on architecture, configuration, telemetry and human response.

EXECUTIVE BRIEF

One operational layer across visibility, control and response

TShield combines transparent network enforcement with monitoring, alert correlation, incident ownership, controlled automation and retained evidence.

SEE

Network and operational activity

Observe behaviour across protected boundaries.

DECIDE

Correlated risk and priority

Convert weak signals into an investigation.

ACT

Controlled, accountable response

Assign, approve, contain and prove.

Designed for

- Public-sector and municipal environments
- Critical infrastructure and distributed enterprises
- Organisations seeking local control and evidence-driven operations

THE OPERATING PROBLEM

Security tools generate signals. Organisations need outcomes.

A firewall alert, log entry or anomaly has limited value if nobody owns it, its urgency is unclear, or the response cannot be reconstructed.

FRAGMENTED
Separate devices and consoles

→

OVERLOADED
High alert volume

→

UNOWNED
No accountable responder

→

UNPROVEN
Incomplete evidence

TShield operating thesis

Connect the security event to ownership, decision and evidence.

OUTCOME

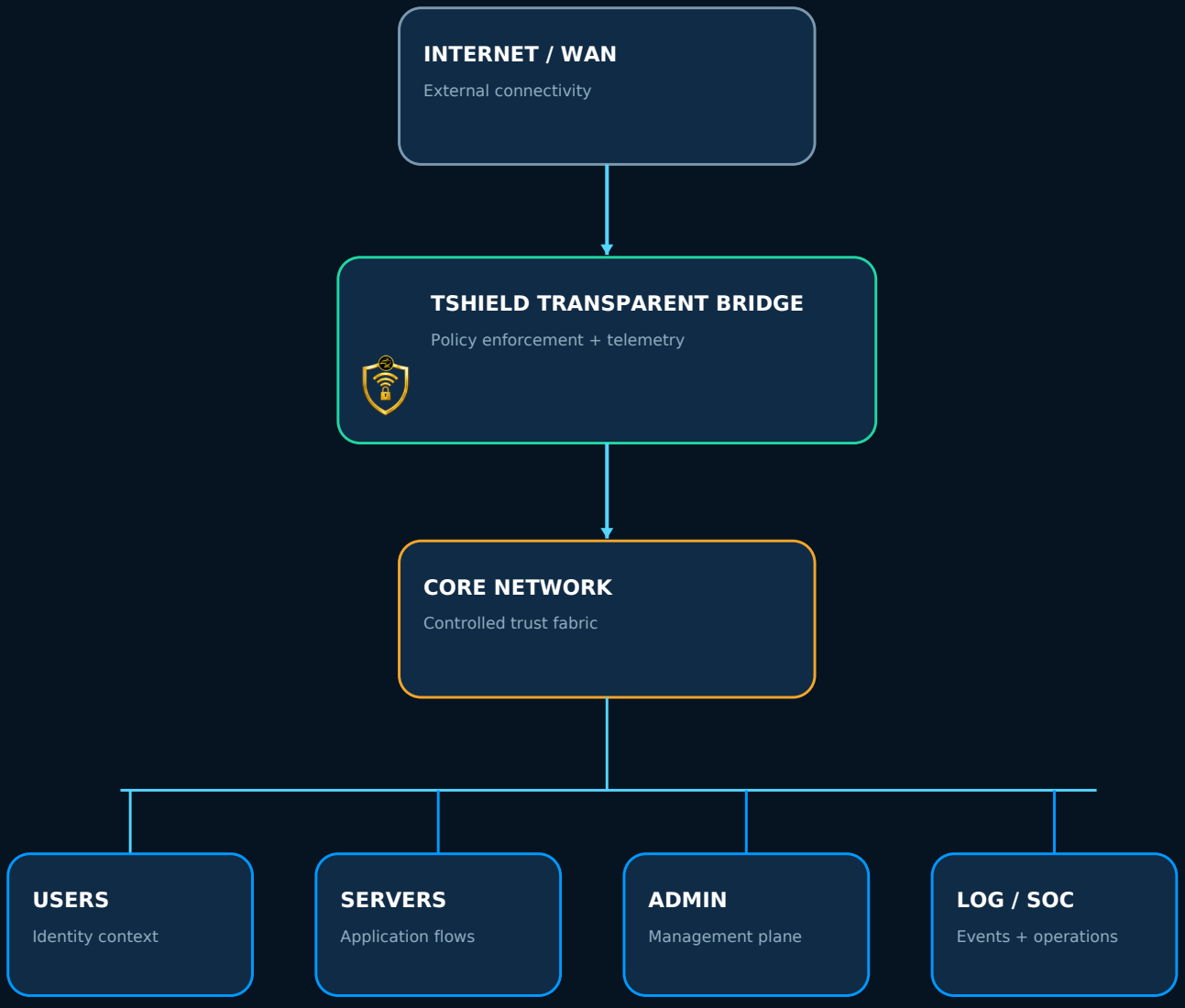
Business result

Shorter time to investigation, clearer ownership, controlled containment and a retained chronology for governance and improvement.

ARCHITECTURE OVERVIEW

Transparent enforcement with an operational control plane

TShield is positioned at relevant trust boundaries and connects network evidence to security operations.



PLACEMENT PRINCIPLE

Monitor the boundaries that matter - not merely the Internet edge.

Internal segmentation, administrative paths and outbound traffic can provide essential context.

TRANSPARENT BRIDGE

Protection without redesigning the entire network

A transparent deployment can sit between existing network elements while preserving the organisation's addressing plan.

Visibility

Observe flows, sources, destinations and changes.

Enforcement

Apply bounded firewall and access-control policies.

Continuity

Introduce controls with a deliberate rollback design.

Evidence

Retain events and response history for review.

DEPLOYMENT CAUTION

Inline placement must be engineered for availability, capacity, bypass and recovery.

No critical environment should adopt a new enforcement point without a documented failure and rollback model.

OPERATING MODEL

From signal to closed incident

The platform is designed to keep detection, ownership, escalation, response and evidence connected.

CORE VALUE

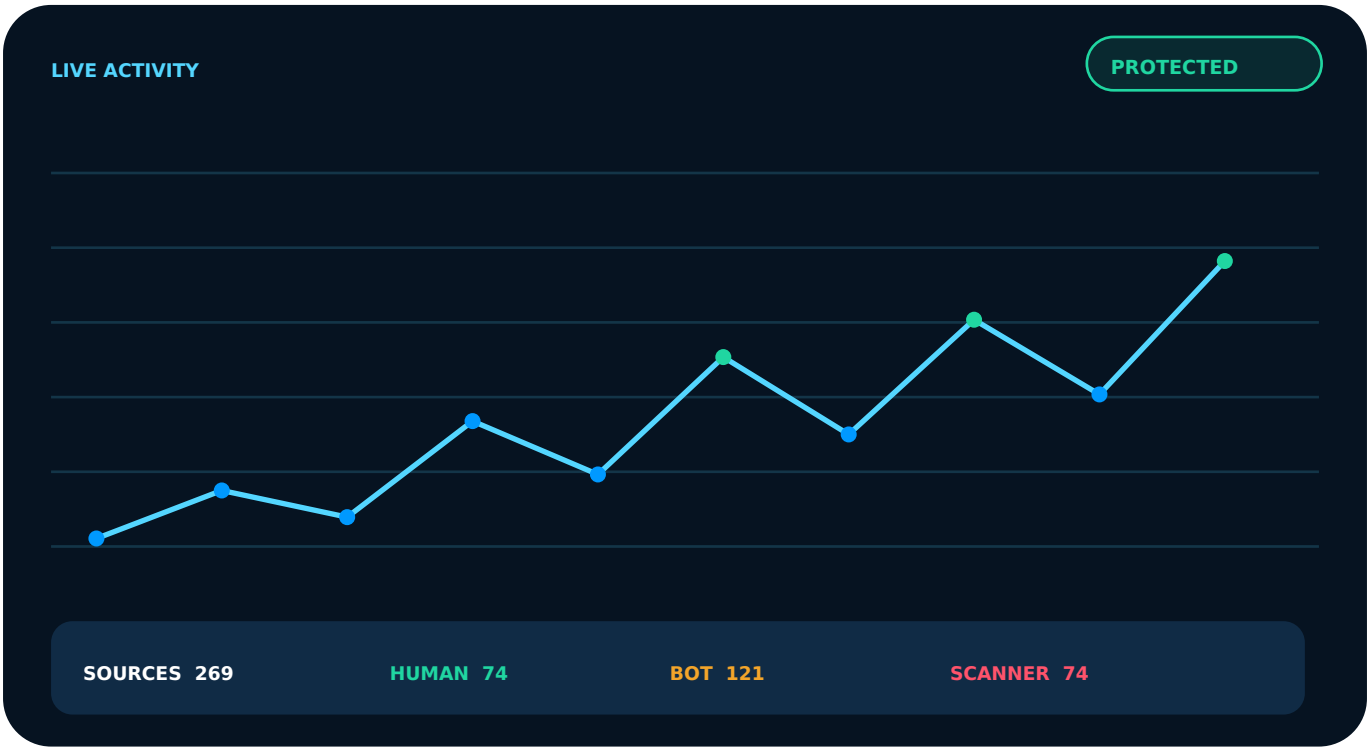
An alert becomes an accountable work item - not an isolated notification.

Assignments, timelines, decisions and response actions remain connected to the incident record.

OPERATIONAL VISIBILITY

See behaviour, not only blocked packets

Dashboards and investigation views turn network events into context that operators can evaluate.



- Live traffic and event views
- Source and destination investigation
- Geographic and behavioural context
- Bot and scanner differentiation
- Panels designed for security operations

DETECTION AND CORRELATION

Weak signals become stronger together

Network, destination, timing, identity context and rule outcomes can be combined into one incident hypothesis.

- Rule-driven and behavioural indicators can coexist.
- Correlation should reduce noise, not conceal underlying evidence.
- Detection quality depends on telemetry coverage and tuned baselines.
- A human operator remains necessary for ambiguous or high-impact decisions.

INCIDENT TICKETING

Every material incident needs an owner and a clock

TShield connects security evidence to queues, assignments, timelines and service-level escalation.

VALIDATED

Service-Level Agreement operations

Timers, escalation and queue ownership reduce the chance that a critical incident remains unseen or unresolved.

- Assignment history and timeline
- Tenant, appliance, queue and team context
- Protected records and evidence-aware operations
- Escalation without silent ticket abandonment

CONTROLLED AUTOMATION

Speed and governance do not have to be opposites

Security Orchestration, Automation and Response (SOAR) can accelerate repeatable work while retaining approval gates for sensitive actions.

HUMAN APPROVAL GATE

Is the proposed containment safe?

Approve · reject · amend · collect more evidence

Low-risk automation

Enrichment, evidence collection and notifications.

Approval-gated action

Isolation or policy changes affecting important systems.

Failure handling

Explicit failed state, logs and accountable follow-up.

Audit trail

Who authorised what, when and with which evidence.

EVIDENCE AND REPORTING

Can the organisation explain what happened?

Operational evidence should support investigation, management review, regulatory assessment and continuous improvement.

10:02	**ANOMALY**	Unexpected outbound behaviour
10:04	**INCIDENT**	Signals correlated
10:07	**OWNER**	SOC analyst assigned
10:12	**ACTION**	Containment approved
10:18	**RESULT**	Transfer interrupted

ACCOUNTABLE

Evidence package

Alert source, affected asset, timeline, assignments, comments, approvals, automated actions, outcomes and retained telemetry

LIMIT

TShield cannot recreate events that connected systems never generated or retained.

Evidence design must begin before an incident, not after the record is already missing.

DEPLOYMENT MODELS

Start with the boundary, scale with the mission

The correct design depends on traffic paths, risk, operational ownership, resilience requirements and available telemetry.

SINGLE SITE

One protected edge

Local appliance + operations

MULTI-ZONE

Several trust boundaries

Perimeter + internal segments

MULTI-SITE

Branches or facilities

Distributed sensors + central view

EVALUATION

Bounded pilot

Passive first, controlled activation

DESIGN RULE

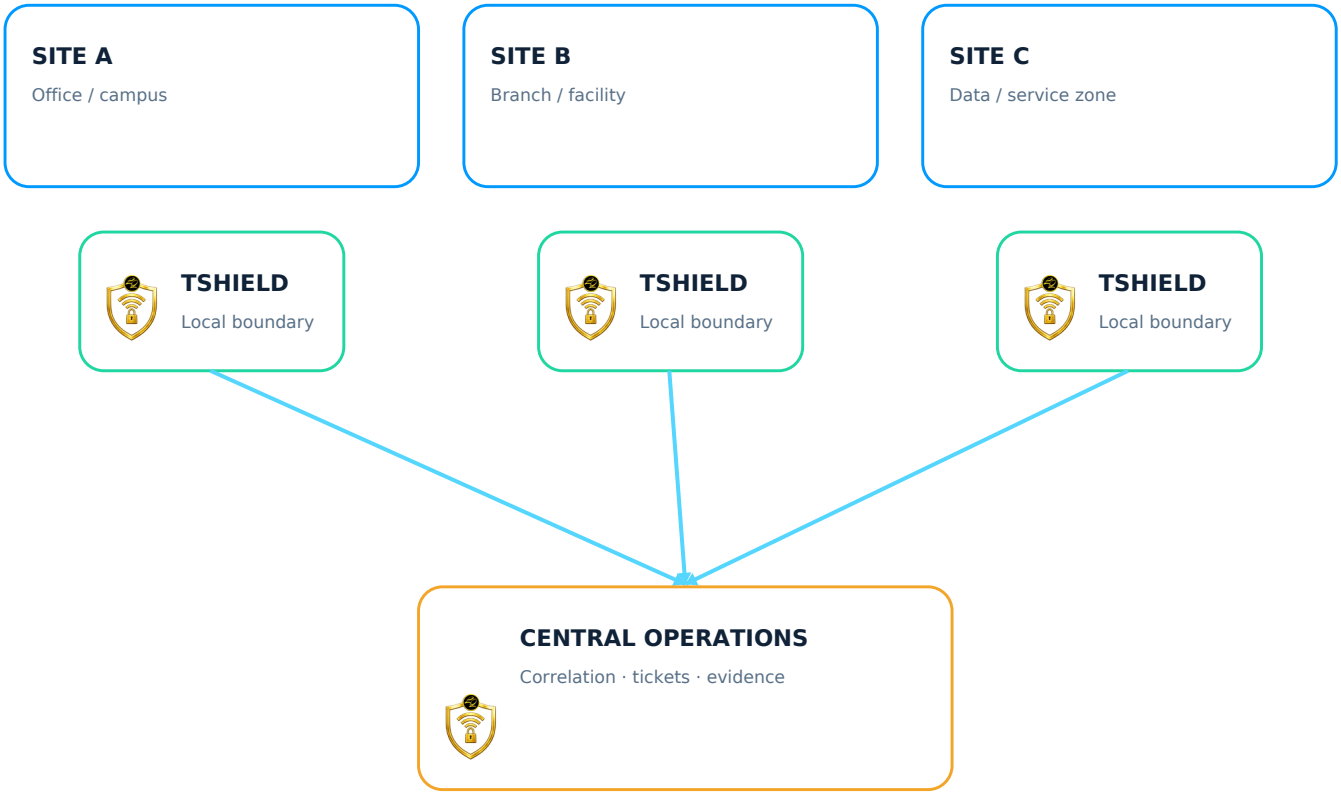
A proof of value should answer defined questions with measurable evidence.

Do not begin with uncontrolled automation or undefined success criteria.

DISTRIBUTED OPERATIONS

Local enforcement, shared situational awareness

A multi-site model can preserve site-level control while centralising incident context and governance.



- Local policies remain aligned to each site's risk and availability needs.
- Events can be normalised and prioritised centrally.
- Incident ownership can span appliances, tenants, queues and teams.
- Central visibility is a deployment model, not a claim of unlimited automatic compatibility.

GOVERNMENT AND PUBLIC SERVICES

Protect the service, the citizen and the record

Public-sector security must address confidentiality, integrity, availability and the ability to demonstrate accountable handling.

CITIZEN DATA

Identity, financial and case information

SERVICE CONTINUITY

Benefits, permits and public access

ADMINISTRATIVE CONTROL

Privileged and management paths

ACCOUNTABILITY

Evidence, timelines and oversight

Potential contribution

- Segment sensitive service environments
- Observe unusual administration and data movement
- Correlate exceptions into owned incidents
- Apply approval-gated response where safe
- Retain evidence for governance and improvement

MUNICIPAL OPERATIONAL ASSURANCE

When a digital record enters the wrong envelope

Public reporting describes a 2026 ISD Brabantse Wal benefit-statement mailing incident. The root cause was not publicly established at publication time.

HONEST BOUNDARY

TShield cannot independently see a document placed in the wrong physical envelope.

Primary prevention requires output matching, reconciliation, exception quarantine and controlled release.

POSSIBLE

Integration-dependent role

Ingest job and machine exceptions, correlate failed reconciliation, create a ticket, start an SLA clock and preserve the response record.

CONCEPTUAL

Concept direction

Government DataGuard could validate document, recipient and authorised channel relationships if reliable application data and governance exist.

Read the full independent case study

lusquan.com/case-studies/isd-brabantse-wal-data-breach-2026

SECTOR APPLICATIONS

One operating model, different risk boundaries

TShield capabilities must be mapped to each sector's mission, topology, safety constraints and regulatory obligations.

GOVERNMENT

Citizen services

TELECOM

Distributed infrastructure

AVIATION

High-consequence operations

FINANCE

Identity and data movement

HEALTHCARE

Sensitive data + availability

EDUCATION

Open, diverse environments

DO NOT COPY-PASTE SECURITY ARCHITECTURE

A hospital, airport, university and municipality cannot share the same containment assumptions.

Pilot design must reflect operational harm, lawful processing, ownership and safe-response limits.

CAPABILITY STATUS

What this edition represents

Status reflects the current internally validated product baseline and identified integration boundaries; it is not third-party certification.

Transparent bridge and firewall policy	VALIDATED
Traffic, metrics and investigation views	VALIDATED
Alert rules and email processing	VALIDATED
Incident ticketing, assignment and SLA	VALIDATED
SOAR lifecycle and approval gates	VALIDATED
Wireless radio-frequency monitoring	INTEGRATION-DEPENDENT
Identity and endpoint containment	INTEGRATION-DEPENDENT
Central multi-appliance operations	PLANNED
Government DataGuard recipient matching	CONCEPTUAL

PILOT PROGRAMME

Prove value in bounded stages

A credible evaluation begins with questions, baselines and rollback - then advances toward controlled enforcement.

01	**DISCOVER**	Topology, assets, risks and owners
02	**OBSERVE**	Passive telemetry and normal behaviour
03	**TUNE**	Rules, severity and false positives
04	**OPERATE**	Tickets, SLA and response exercises
05	**EVALUATE**	Coverage, time, evidence and gaps

MEASURE

Detection coverage · time to triage · ownership · false positives · evidence completeness

A pilot should finish with a decision record, not merely a demonstration.

IMPLEMENTATION REQUIREMENTS

What a technical evaluation needs

The appliance is only one part of an operational security capability.

NETWORK

Documented traffic path, interface role, addressing, capacity and bypass.

TELEMETRY

Defined sources, retention, lawful purpose and data minimisation.

OPERATIONS

Named owners, queues, severity model, escalation and on-call expectations.

RESPONSE

Approved actions, safety constraints, recovery and rollback.

GOVERNANCE

Privacy, audit, change control, supplier duties and evidence access.

RESILIENCE

Power, storage, backup, monitoring and failure-mode planning.

BUYER DUE DILIGENCE

Questions a serious evaluation should answer

LUSQUAN welcomes architecture, security, privacy and operational scrutiny.

01 Which exact capabilities are included in the proposed release?

02 Which claims are internally validated, integration-dependent or planned?

03 Where will appliances be placed and what failure modes are acceptable?

04 Which data is collected, retained and accessible to whom?

05 How are updates, backups, keys and administrative access governed?

06 Which response actions are automatic and which require approval?

07 How will detection coverage and false positives be measured?

08 What are the rollback, support and evidence-export arrangements?

PROCUREMENT PRINCIPLE

Require demonstrable controls, explicit exclusions and evidence of safe operation.

WHAT TSHIELD CANNOT GUARANTEE

Credibility requires limits

Security resilience is layered. TShield strengthens selected layers and does not replace the rest of the control environment.

- No appliance can guarantee that compromise or data loss will never occur.
- TShield does not replace identity management, endpoint protection, patching or backups.
- It cannot inspect physical documents or envelope contents without specialised external controls.
- It cannot infer business relationships that source systems do not reliably expose.
- Detection depends on placement, visibility, baselines, configuration and response.
- Automated containment can create operational harm if poorly governed.
- Wireless monitoring requires compatible and reliably operating radio hardware.
- Roadmap and conceptual capabilities must not be purchased as delivered features.

THE DEFENSIBLE PROMISE

More opportunities to observe, restrict, respond and prove.

Not perfect prevention - measurable operational resilience.

EVIDENCE LIBRARY

Real incidents. Explicit analytical boundaries.

The TShield case-study library distinguishes public facts from defensive reconstruction and never implies deployment where none is reported.

CS-NL-001

ISD Brabantse Wal data breach

Government · Netherlands

UC-SPECIAL-001

When Trust Fails - Xfinity

Telecommunications · United States

CS-CARIBBEAN-001

TSTT RansomEXX cyberattack

Telecommunications · Caribbean

CS-AFRICA-001

Namibia Airports cyberattack

Aviation · Africa

CS-AFRICA-002

Standard Bank data incident

Finance · Africa

CS-AFRICA-003

Nigeria CAC cyberattack

Government registry · Africa

Explore the full library

lusquan.com/case-studies

START WITH A QUESTION

What must your organisation

be able to detect, contain and prove?

REQUEST A TECHNICAL EVALUATION

Architecture workshop · bounded pilot · deployment consultation

lusquan.com/tshield-information

PUBLICATION

PUB-TSHIELD-INFO-001

EDITION

2026.1

LUSQUAN B.V.

PROTECTING YOU NOT EXPOSING YOU