SENDĀTRIX

SDX Technical Publications

SDX-TP-002

$5,000 Independent Security Evaluation

Evaluating the Structural Protection Model

Official Evaluation Methodology, Award Conditions, and Evidence Requirements

Can Protected Information remain protected after administrative compromise?

SENDĀTRIX invites the cybersecurity community to answer that question through independent technical evaluation.

Version 1.1 | August 2026

Greenville, North Carolina, USA | sendatrix.com

Publication Information

Publication	SDX-TP-002
Title	$5,000 Independent Security Evaluation
Subtitle	Evaluating the Structural Protection Model
Version	1.1
Publication Date	August 2026
Publisher	SENDĀTRIX — Greenville, North Carolina, USA
Website	sendatrix.com
Patent	U.S. Patent No. 9,405,927

This publication defines the architectural proposition, evaluation methodology, evidence requirements, and award conditions for the Independent Security Evaluation of the C Chains™ implementation of the Structural Protection Model.

Table of Contents

Executive One-Page Summary

The Problem

Modern cybersecurity has become highly effective at reducing unauthorized access through firewalls, encryption, identity management, privileged access management, endpoint protection, monitoring, and Zero Trust architectures. These technologies remain essential.

However, many significant data breaches become catastrophic only after an attacker—or an authorized insider—obtains elevated administrative privileges. At that point, Administrative Authority often becomes practical authority to reconstruct Protected Information.

This publication examines whether that assumption is architecturally necessary.

The Architectural Proposition

The Structural Protection Model separates Administrative Authority from Reconstruction Authority through a Distributed Trust Architecture.

Its objective is not to prevent every compromise. Its objective is to ensure that compromise of a single trusted component does not automatically permit Unauthorized Reconstruction of Protected Information.

C Chains™ is SENDĀTRIX's implementation of this architectural model.

Independent Evaluation

SENDĀTRIX invites qualified security professionals, penetration testers, forensic analysts, researchers, database professionals, and security organizations to independently evaluate the implementation using accepted professional methodologies.

Can Protected Information be reconstructed outside the authorization model established by the Structural Protection Model?

Evaluation Award

A $5,000 USD award will be granted if an evaluator successfully demonstrates Unauthorized Reconstruction of Protected Information under the published evaluation conditions and the findings are independently verified.

Core Principle

Administrative Authority is not, by itself, Reconstruction Authority.

Scope and Intended Audience

Purpose

This publication defines the architectural proposition, evaluation methodology, evidence requirements, and award conditions for the Independent Security Evaluation of the C Chains™ implementation of the Structural Protection Model.

It is intended to provide evaluators with a common understanding of the objectives, scope, and success criteria governing the published evaluation.

This publication is not a software user guide, deployment manual, programming reference, or implementation specification. Those subjects are addressed separately within the SDX Technical Publications Series.

Intended Audience

This publication is intended for:

- Chief Information Security Officers (CISOs)
- Chief Information Officers (CIOs)
- Security architects
- Penetration testers
- Digital forensic analysts
- Database administrators
- Security researchers
- Risk and compliance professionals
- Independent security assessment organizations
- Academic researchers evaluating security architectures

Although a technical background is helpful, the publication is written to be understandable by decision-makers responsible for evaluating enterprise security architectures.

Scope

This publication evaluates one architectural proposition:

Can Protected Information remain protected after Administrative Authority has been compromised or legitimately exercised?

Accordingly, the publication focuses upon:

- The Structural Protection Model
- The C Chains™ implementation
- Independent evaluation methodology
- Evidence requirements
- Evaluation success criteria
- Award conditions

The publication does not attempt to document every implementation detail, deployment configuration, or operational procedure. Those topics are intentionally addressed in companion publications.

Document Organization

This publication is organized into three parts:

Part I — Architectural Foundation

Defines the problem being addressed and introduces the Structural Protection Model.

Part II — Implementation

Describes how C Chains™ implements the Structural Protection Model.

Part III — Independent Evaluation

Defines the methodology, evaluation environment, evidence requirements, award conditions, and supporting publications.

Publication Objective

The objective of this publication is neither to persuade nor to market. Its purpose is to define a technical proposition with sufficient clarity that it may be independently evaluated, challenged, reproduced, and verified using accepted professional security practices.

Preface

Every significant advancement in cybersecurity has challenged an assumption that was once considered unavoidable.

Firewalls challenged unrestricted network connectivity.

Encryption challenged plaintext storage.

Multi-factor authentication challenged password-only identity.

Zero Trust challenged implicit trust within enterprise networks.

Yet one architectural assumption has remained largely unchanged.

Once Administrative Authority has been compromised—or legitimately exercised—Protected Information is generally assumed to become recoverable.

This publication examines whether that assumption is necessarily true.

It introduces the principles of Structural Protection, defines the architectural hypothesis being evaluated, and describes the conditions under which SENDĀTRIX invites independent technical examination.

The purpose of this publication is not to replace established cybersecurity practices.

Firewalls, encryption, identity management, privileged access management, endpoint protection, and Zero Trust remain essential components of modern security programs.

Structural Protection begins where those controls reach their practical limit.

It asks a different question.

What continues protecting Protected Information after Administrative Authority has been obtained?

The answer proposed by this publication is the Structural Protection Model, implemented by C Chains™.

Whether that model withstands independent scrutiny is not a matter of opinion.

It is a matter of evidence.

Executive Summary

Modern cybersecurity has become increasingly effective at preventing unauthorized access to information.

Organizations invest heavily in identity management, encryption, privileged access management, network segmentation, monitoring, endpoint protection, and Zero Trust architectures.

These controls reduce risk and remain essential.

However, many of the most damaging security incidents occur only after an attacker obtains elevated privileges or compromises a trusted administrative account.

At that point, traditional architectures frequently assume that the authority required to administer systems also provides the authority required to reconstruct Protected Information.

The Structural Protection Model challenges that assumption.

Rather than concentrating trust within a single administrative domain, Structural Protection separates the authority required to operate systems from the authority required to reconstruct Protected Information.

This distinction is fundamental.

Administrative Authority is not, by itself, Reconstruction Authority.

C Chains™ implements this principle through a Distributed Trust Architecture that separates operational responsibilities across independently controlled components.

The objective is not to prevent every compromise.

The objective is to ensure that compromise of one trusted component does not automatically permit Unauthorized Reconstruction of Protected Information.

This publication defines the architectural hypothesis, evaluation methodology, evidence requirements, and award conditions for an Independent Security Evaluation of that objective.

SENDĀTRIX invites qualified security professionals, researchers, penetration testers, forensic analysts, database professionals, and security organizations to examine the architecture using accepted professional methodologies.

If an evaluator demonstrates Unauthorized Reconstruction of Protected Information under the published evaluation conditions, and the findings can be independently reproduced, SENDĀTRIX will award $5,000 USD.

1. The Fundamental Question

Every security architecture is ultimately built upon a set of assumptions.

The assumption examined by this publication is straightforward.

Should compromise of Administrative Authority automatically result in Reconstruction Authority?

For decades, enterprise systems have largely answered this question yes.

If an attacker acquires sufficient administrative control over the database, operating system, cloud infrastructure, or application environment, the Protected Information managed by those systems is generally assumed to become recoverable.

This publication proposes a different architectural model.

Rather than asking whether administrative compromise can always be prevented, it asks whether administrative compromise must inevitably result in Unauthorized Reconstruction.

That question defines the scope of this Independent Security Evaluation.

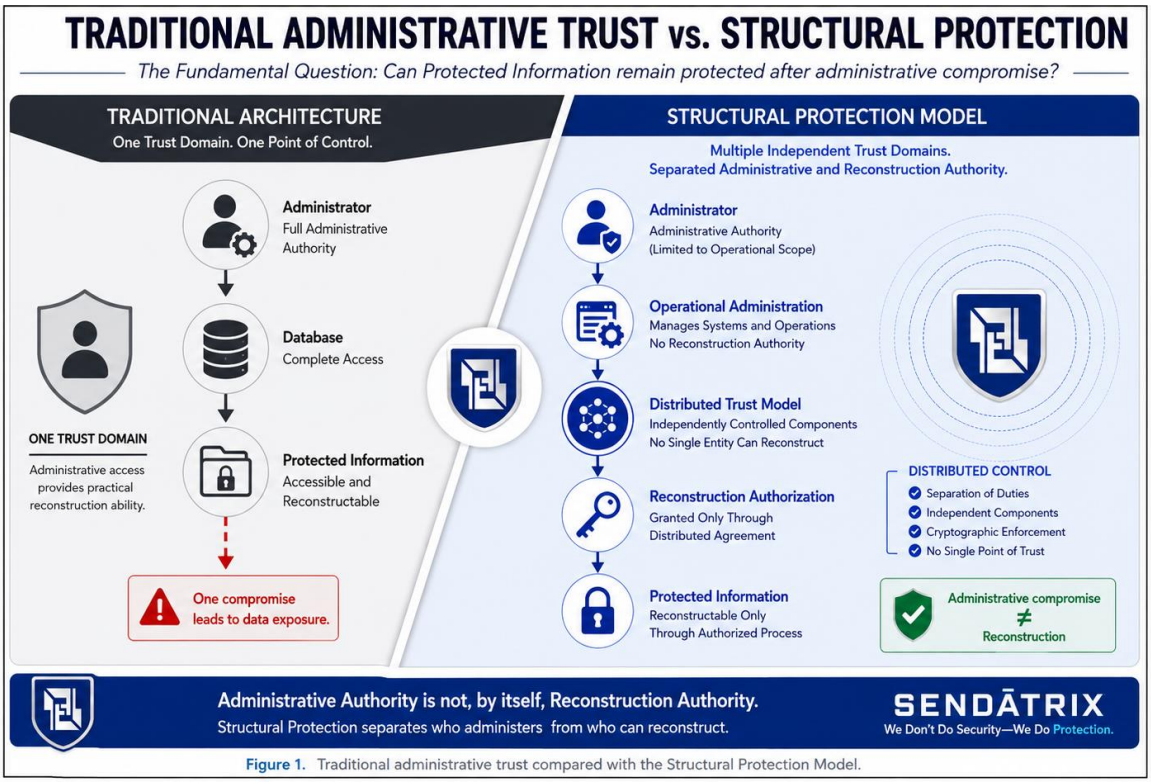


Figure 1. Traditional administrative trust compared with the Structural Protection Model.

2. The Structural Protection Model

Introduction

Traditional cybersecurity is designed to reduce the likelihood of compromise.

Firewalls restrict network access.

Encryption protects stored information.

Authentication verifies identity.

Authorization controls access.

Monitoring and auditing help detect misuse.

These technologies remain essential and continue to evolve.

The Structural Protection Model does not replace these controls.

Instead, it addresses a different architectural question.

What protects Protected Information after traditional security controls have been bypassed, compromised, or legitimately exercised through Administrative Authority?

The Structural Protection Model proposes that the answer should not depend upon continued trust in any single administrator, database, server, application, or security boundary.

Instead, it separates the authority required to reconstruct Protected Information from the authority required to administer the systems that support it.

This principle forms the foundation of Structural Protection.

The Central Principle

The Structural Protection Model is based upon one fundamental architectural objective.

Administrative Authority should not, by itself, constitute Reconstruction Authority.

In many traditional architectures, these two forms of authority are effectively combined.

An individual entrusted with administering the environment frequently possesses, either directly or indirectly, the practical ability to view, recover, or reconstruct Protected Information.

The Structural Protection Model intentionally separates these responsibilities.

Administrative responsibilities remain necessary.

Systems must still be installed, maintained, monitored, backed up, and supported.

However, performing those responsibilities should not automatically grant the authority required to reconstruct Protected Information.

This distinction represents a fundamental shift in architectural philosophy.

Rather than asking “Who can administer the system?”, the Structural Protection Model asks:

Who should be capable of reconstructing Protected Information, under what conditions, and with what independent authorization?

Design Principles

The Structural Protection Model is guided by six architectural principles.

1. Separate Administrative Authority from Reconstruction Authority

Operational administration and information reconstruction represent different responsibilities and should be treated independently.

2. Distribute Trust

No single architectural component should possess sufficient information or authority to independently reconstruct Protected Information.

3. Protect Information Structurally

Protection should result from the architecture itself rather than relying exclusively upon administrative policy or operational trust.

4. Assume Compromise

The model assumes that privileged accounts, applications, servers, or infrastructure components may eventually be compromised. The objective is to reduce the consequences of those events rather than assuming they can always be prevented.

5. Require Independent Authorization

Reconstruction of Protected Information should require authorization beyond ordinary administrative control and should occur only through defined operational processes.

6. Preserve Operational Functionality

Security should not unnecessarily interfere with normal business operations. Authorized users should continue performing legitimate work while Protected Information remains structurally protected.

Distributed Trust Architecture

The Structural Protection Model is implemented through a Distributed Trust Architecture.

Rather than concentrating responsibility within a single database, application, or administrative domain, the architecture distributes responsibility across independently controlled components.

Each component performs a specific function within the protection process.

No individual component is intended to possess sufficient information or authority to independently reconstruct Protected Information.

As a result, compromise of one trusted component does not automatically invalidate the protection model.

The objective is not to eliminate trust.

The objective is to distribute trust in a manner that reduces the consequences of compromise.

Relationship to C Chains™

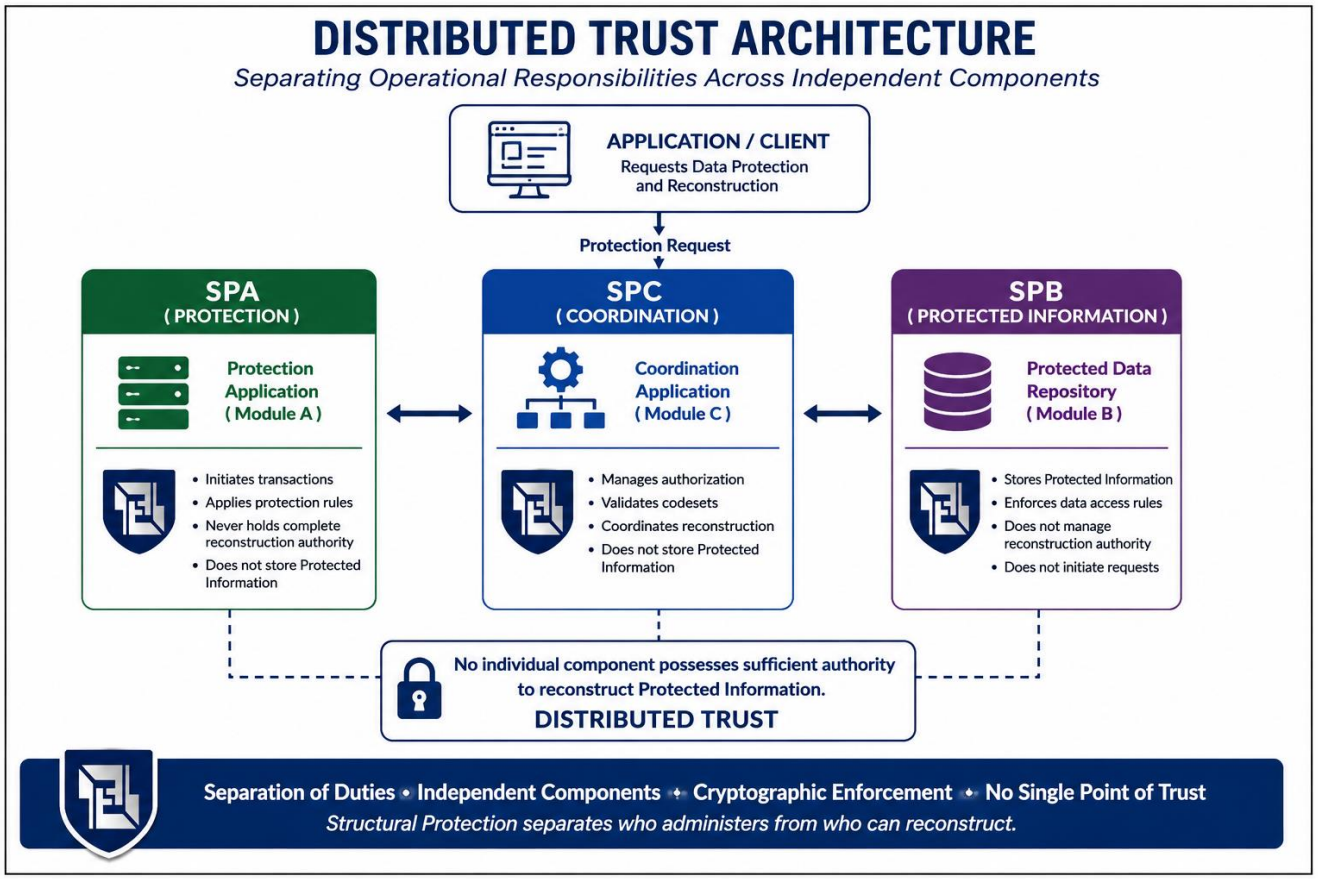
Structural Protection is an architectural model.

C Chains™ is SENDĀTRIX's implementation of that model.

The Independent Security Evaluation described in this publication examines whether the C Chains™ implementation successfully achieves the objectives of the Structural Protection Model under the published evaluation conditions.

Accordingly, the evaluation is not intended to determine whether the concept of Structural Protection is desirable.

It is intended to determine whether the implemented architecture withstands independent technical examination.



3. The C Chains™ Implementation

The preceding chapter introduced the principles of the Structural Protection Model. This chapter describes how those principles are implemented by the C Chains™ architecture.

The purpose of this publication is not to document every technical detail of the implementation. Rather, it provides sufficient context for evaluators to understand the architectural objectives being examined during the Independent Security Evaluation.

Comprehensive implementation details are provided in SDX-TP-003 — C Chains™ Security Architecture Guide.

Architectural Objective

The C Chains™ implementation was designed to achieve one primary objective.

Prevent Unauthorized Reconstruction of Protected Information through compromise of any single trusted component.

To accomplish this objective, the implementation separates operational responsibilities across independently controlled architectural components.

Each component performs a defined function within the overall protection process.

No individual component is intended to possess sufficient information or authority to independently reconstruct Protected Information.

This separation represents the practical implementation of the Structural Protection Model.

Operational Overview

At a high level, the protection process consists of four activities:

1. Identification of information designated for Structural Protection.
2. Protection of that information through the C Chains™ architecture.
3. Operational use of applications and databases without routine exposure of Protected Information.
4. Controlled reconstruction of Protected Information only through authorized operational processes.

The details of these activities are implementation-specific and are described within the accompanying Structural Protection Architecture Guide.

For the purposes of this publication, it is sufficient to understand that reconstruction is intended to occur only when all required architectural conditions have been satisfied.

Distributed Responsibilities

The implementation distributes operational responsibilities across independent architectural components rather than concentrating them within a single database, server, or administrative domain.

These responsibilities include, among others:

- Protection processing
- Protected Information storage
- Authorization and coordination
- Operational application support
- Audit and accountability

The evaluator is encouraged to determine whether this separation of responsibility is sufficient to achieve the objectives described by the Structural Protection Model.

Reconstruction

One of the first questions evaluators typically ask is straightforward.

If Protected Information has been structurally protected, how is it reconstructed when legitimately required?

The answer is equally important.

C Chains™ is not intended to prevent authorized business operations.

Rather, it is designed to ensure that reconstruction occurs only through the defined authorization process established by the architecture.

Authorized users continue performing legitimate operational tasks.

The architecture determines whether the conditions necessary for reconstruction have been satisfied before Protected Information is made available for the requested operation.

Consequently, the Independent Security Evaluation is not concerned with whether reconstruction occurs.

It is concerned with whether reconstruction can occur outside the intended authorization model.

That distinction is central to the Independent Security Evaluation.

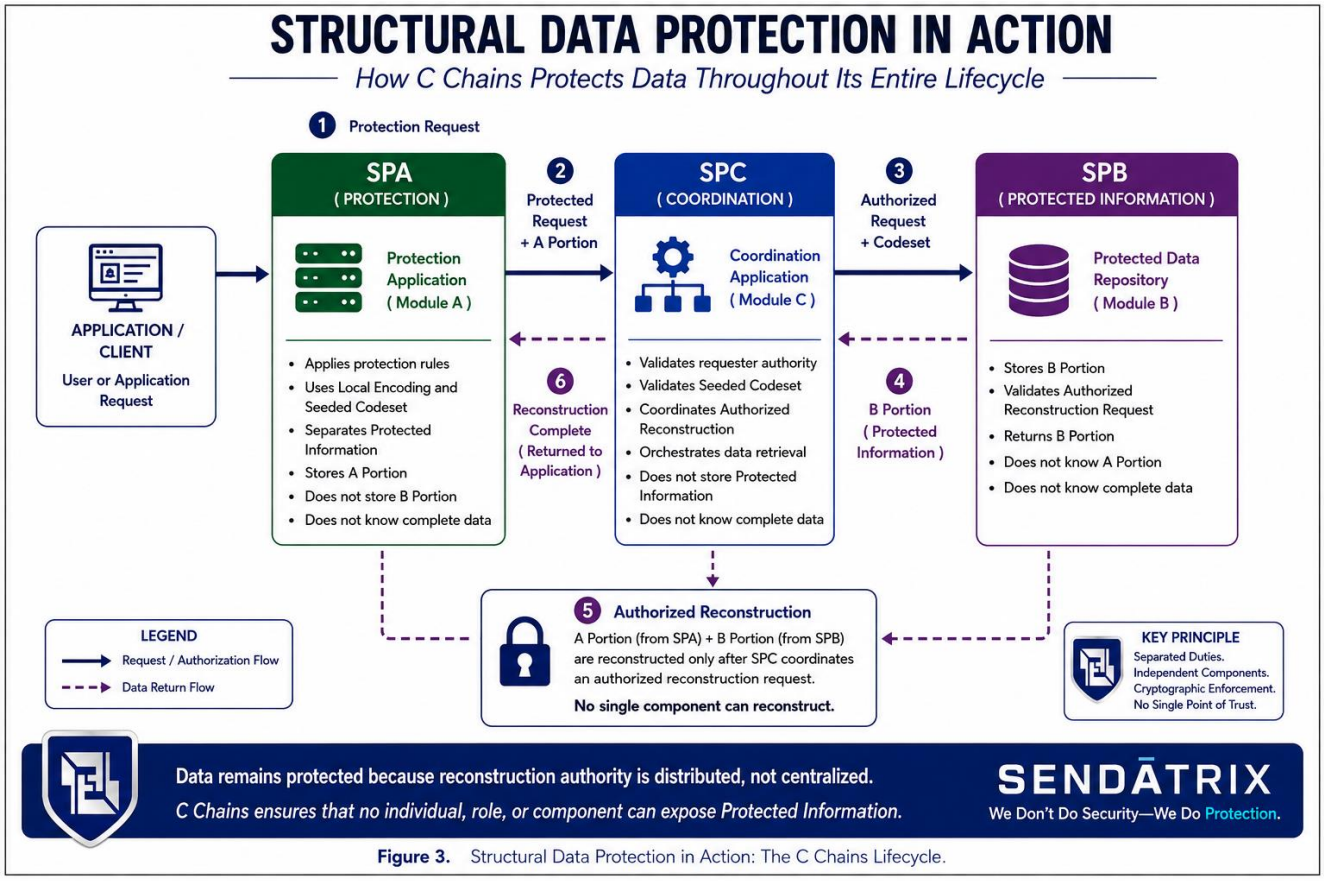


Figure 3. Structural Data Protection in Action: The C Chains Lifecycle.

What Is Being Evaluated

The evaluation described in this publication is intentionally focused.

Evaluators are not being asked to determine whether the C Chains™ software is entirely free of defects.

Nor are they being asked to certify every aspect of the implementation.

Instead, they are asked to examine a specific architectural proposition.

Can Protected Information be reconstructed without satisfying the Structural Protection Model implemented by C Chains™?

The answer to that question—not the presence or absence of unrelated software defects—determines the outcome of the Independent Security Evaluation.

Transition to Evaluation

The remaining chapters describe how this architectural proposition will be evaluated, the evidence required to support evaluation findings, and the conditions under which SENDĀTRIX will recognize a successful demonstration of Unauthorized Reconstruction.

4. Independent Security Evaluation

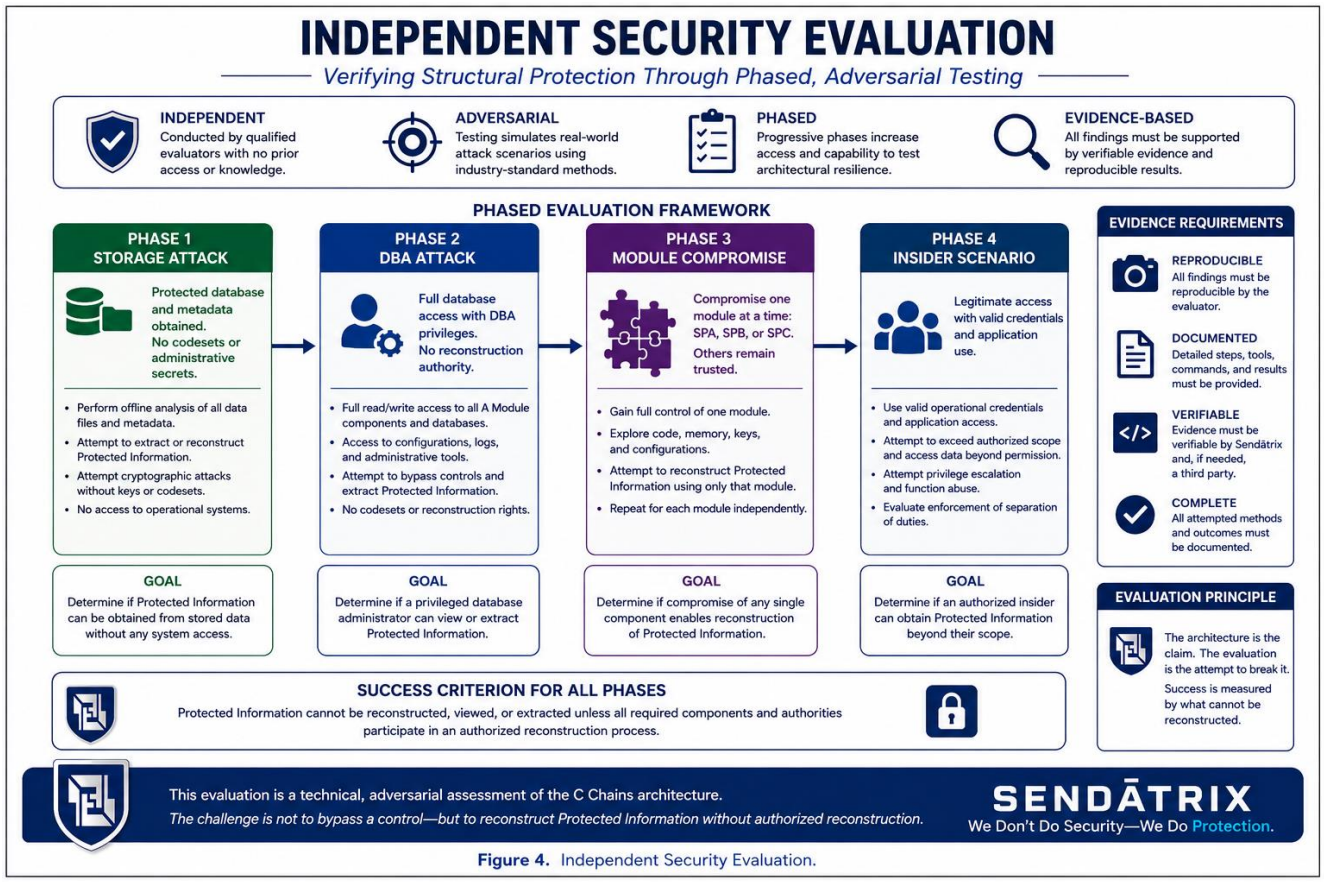


Figure 4. Independent Security Evaluation.

The purpose of an Independent Security Evaluation is to determine whether the C Chains™ implementation successfully achieves the objectives of the Structural Protection Model under realistic and technically rigorous conditions.

The evaluation is not intended to validate marketing claims, demonstrate product features, or certify software quality.

Its purpose is straightforward.

Can Protected Information be reconstructed without satisfying the architectural requirements established by the Structural Protection Model?

That question defines the evaluation.

Evaluation Philosophy

This publication intentionally distinguishes between system compromise and architectural compromise.

Modern software systems are complex.

Operating systems contain defects.

Applications evolve.

Configuration errors occur.

Administrative credentials may be compromised.

Professional evaluators are encouraged to examine all of these areas.

However, discovery of implementation defects does not automatically invalidate the Structural Protection Model.

Likewise, successful compromise of a server, database instance, administrative account, or application does not, by itself, constitute a successful outcome under this evaluation.

The defining question remains:

Does the compromise permit Unauthorized Reconstruction of Protected Information?

If the answer is no, the architecture has continued to perform its intended function despite the compromise.

If the answer is yes, the evaluator has identified an architectural failure that warrants independent verification.

Scope of Evaluation

SENDĀTRIX does not prescribe a preferred testing methodology.

Evaluators are encouraged to apply the same professional judgment, creativity, and technical rigor they would employ during a commercial security engagement.

Depending upon the objectives of the evaluation, this may include:

- Architectural analysis
- Penetration testing
- PostgreSQL forensic examination
- Operating system analysis
- Reverse engineering
- Source code review
- Memory analysis
- Network protocol analysis
- Backup examination
- Insider threat scenarios
- Multi-stage attack chains
- Reconstruction analysis

The evaluation is intentionally outcome-oriented rather than methodology-oriented.

The objective is not to determine how an evaluator attempts to defeat the architecture.

The objective is to determine whether the architecture can be defeated.

Evaluation Environment

The evaluation should provide sufficient access to permit meaningful examination of the implementation.

Depending upon the agreed scope, evaluators may be granted administrative authority over the operational database environment, access to supporting software components, documentation, configuration information, and other resources necessary to conduct a professional evaluation.

SENDĀTRIX does not intend to restrict legitimate examination of the implementation.

If an evaluator believes that a particular forensic technique, database artifact, operating system feature, or software analysis method may contribute to Unauthorized Reconstruction, its examination is encouraged.

The purpose of this evaluation is independent scrutiny—not constrained testing.

Evaluation Success

The outcome of the Independent Security Evaluation is determined by one criterion.

Has the evaluator demonstrated Unauthorized Reconstruction of Protected Information outside the authorization model defined by the Structural Protection Model?

Discovery of software defects, implementation weaknesses, or operational recommendations is valuable and welcomed.

However, those findings alone do not constitute a successful evaluation under the published award conditions.

Only demonstrated Unauthorized Reconstruction satisfies the primary objective of this evaluation.

Relationship to the C Chains™ Security Architecture Guide

This publication defines what is being evaluated.

Detailed evaluation methodology, evidence collection practices, reporting standards, and technical guidance for evaluators are provided in SDX-TP-003 — C Chains™ Security Architecture Guide, particularly Chapters 6 through 8.

SDX-TP-003 — C Chains™ Security Architecture Guide

Professional evaluators conducting formal assessments should consult those chapters together with the requirements defined in this publication.

5. Evaluation Environment

The Independent Security Evaluation is intended to provide qualified evaluators with sufficient access to meaningfully examine the C Chains™ implementation and determine whether the objectives of the Structural Protection Model have been achieved.

The purpose of the evaluation environment is not to restrict legitimate technical examination.

Its purpose is to clearly define the conditions under which evaluation findings will be interpreted and independently verified.

Evaluation Objectives

The evaluation environment should provide evaluators with the access necessary to determine whether Protected Information can be reconstructed outside the intended authorization model.

Evaluators are encouraged to approach the system using the same methodologies, tools, and analytical techniques they would employ during a professional security engagement.

SENDĀTRIX does not prescribe a preferred methodology.

The evaluation is intentionally designed to encourage independent thinking, technical rigor, and professional judgment.

Administrative Access

Where appropriate, evaluators may be granted privileged administrative access to the operational environment supporting the evaluation.

Depending upon the agreed scope of testing, this may include administrative authority over:

- The operating system
- The PostgreSQL database
- Database administration tools
- Configuration files
- Supporting software components
- Application executables
- Log files
- Backup media

Administrative authority is intentionally included because the purpose of the evaluation is to determine whether elevated privilege alone permits Unauthorized Reconstruction of Protected Information.

Database Examination

Evaluators are specifically encouraged to examine PostgreSQL using accepted administrative and forensic techniques.

This examination may include, but is not limited to:

- Database schema
- Table structures
- Views
- Stored procedures
- Functions
- Trigger definitions
- System catalogs
- WAL (Write-Ahead Log) records
- Heap pages
- Dead tuples
- Transaction metadata
- Index structures
- Backup files
- Database logs
- Administrative configuration
- Internal PostgreSQL artifacts

No PostgreSQL artifact is considered outside the intended scope of examination unless explicitly excluded as part of a mutually agreed evaluation.

Software Examination

Where source code, executable programs, supporting utilities, or configuration files are provided, evaluators are encouraged to perform any legitimate software analysis they believe appropriate.

Examples include:

- Static analysis
- Dynamic analysis
- Reverse engineering
- Debugging

- Memory inspection
- Binary analysis
- Protocol analysis

The objective is not to limit examination of the implementation.

The objective is to determine whether any combination of these techniques enables Unauthorized Reconstruction.

Scope of Authority

The evaluation should clearly distinguish between compromise of:

- A single architectural component
- Multiple independently trusted components
- Legitimate operational authority
- Administrative Authority
- Reconstruction Authority

This distinction is fundamental to the Structural Protection Model.

Evaluation findings should identify not only what was compromised, but whether that compromise was sufficient to bypass the architectural separation of trust upon which the Structural Protection Model is based.

Clarification

SENDĀTRIX welcomes rigorous technical examination.

If an evaluator believes that a particular forensic technique, software analysis method, database artifact, operating system feature, or administrative capability may contribute to Unauthorized Reconstruction, its examination is encouraged.

The objective of the Independent Security Evaluation is not constrained testing.

It is independent scrutiny.

6. Evidence Requirements and Success Criteria

Figure 5. Evidence Requirements and Success Criteria.

The purpose of the Independent Security Evaluation is to determine whether the C Chains™ implementation fulfills the architectural objectives of the Structural Protection Model.

Accordingly, the outcome of the evaluation is determined not by the discovery of software defects alone, but by the evaluator's ability to demonstrate Unauthorized Reconstruction of Protected Information under the published evaluation conditions.

This distinction is fundamental to the evaluation.

Evidence Requirements

Evaluation findings should be supported by sufficient technical evidence to permit independent review, analysis, and reproduction.

The objective of the evidence is not simply to document observations, but to demonstrate the methodology by which the reported outcome was achieved.

Depending upon the nature of the evaluation, supporting evidence may include:

- A technical description of the methodology employed
- The sequence of actions leading to the reported result
- SQL statements, scripts, or supporting utilities
- Source code or executable modifications, where applicable
- Screenshots or video recordings
- Packet captures
- Operating system and application logs

- PostgreSQL artifacts and forensic findings
- Memory analysis
- Backup analysis
- Reconstructed Protected Information
- Any additional material necessary to independently reproduce the reported results

The specific format of the evidence is less important than its completeness, clarity, and reproducibility.

Independent Verification

Before an evaluation is considered complete, SENDĀTRIX reserves the right to independently review, reproduce, or observe the reported findings.

The purpose of this verification is not to challenge the evaluator's conclusions.

Rather, it is to ensure that the reported methodology consistently produces the reported outcome under the agreed evaluation conditions.

Repeatability is an essential characteristic of every successful technical evaluation.

Evaluation Outcomes

Evaluation findings generally fall into one of four categories.

Architectural Success

The evaluator demonstrates Unauthorized Reconstruction of Protected Information outside the authorization model established by the Structural Protection Model.

If independently verified, this represents a successful outcome under the terms of the Independent Security Evaluation.

Implementation Findings

The evaluator identifies software defects, programming errors, configuration weaknesses, documentation issues, or operational recommendations that do not enable Unauthorized Reconstruction.

These findings are valuable, will be documented, and may result in improvements to the implementation.

However, they do not constitute an architectural failure.

Operational Findings

The evaluator identifies deployment practices, administrative procedures, or environmental conditions that may increase operational risk.

Such findings contribute to improving deployment guidance and operational best practices but should be distinguished from architectural deficiencies.

Observations and Recommendations

The evaluator offers recommendations regarding usability, documentation, deployment, performance, monitoring, or future enhancements.

These observations are welcomed as part of the Independent Security Evaluation process and may influence future versions of the implementation or supporting publications.

Success Criterion

The Independent Security Evaluation is built upon one defining question.

Has the evaluator demonstrated Unauthorized Reconstruction of Protected Information without satisfying the requirements of the Structural Protection Model?

If the answer is yes, the evaluator has successfully demonstrated an architectural failure under the published evaluation conditions.

If the answer is no, the evaluation provides additional evidence supporting the effectiveness of the Structural Protection Model within the scope examined.

This criterion distinguishes architectural evaluation from conventional software testing.

The evaluation is not intended to determine whether software defects exist.

It is intended to determine whether those defects ultimately defeat the Structural Protection Model.

Relationship to the C Chains™ Security Architecture Guide

This publication defines the evidence necessary to evaluate the architectural hypothesis.

Detailed procedures for evaluation methodology, evidence collection, reporting, and validation are provided in SDX-TP-003 — C Chains™ Security Architecture Guide, particularly Chapters 6 through 8.

SDX-TP-003 — C Chains™ Security Architecture Guide

Professional evaluators conducting formal assessments should consult those chapters together with the requirements defined in this publication.

Evaluation Principle

The Independent Security Evaluation recognizes that valuable findings may exist even when the Structural Protection Model is not defeated.

Implementation improvements, operational recommendations, deployment guidance, documentation corrections, and usability observations all contribute to the continued evolution of the C Chains™ implementation.

The primary objective of this publication, however, remains the independent evaluation of one architectural proposition:

Can Protected Information be reconstructed outside the authorization model established by the Structural Protection Model?

7. The Evaluation Award

The purpose of the $5,000 Independent Security Evaluation Award is to encourage objective, evidence-based examination of the C Chains™ implementation and the Structural Protection Model.

The award is intended to recognize a successful demonstration of Unauthorized Reconstruction of Protected Information under the published evaluation conditions.

It is not intended to reward the discovery of ordinary software defects, implementation errors, or operational recommendations unless those findings directly result in Unauthorized Reconstruction.

Eligibility

The evaluation is open to qualified security professionals, penetration testers, forensic analysts, researchers, academic institutions, and security organizations possessing the technical expertise necessary to conduct an independent assessment.

Evaluators may work individually or as members of a team.

Award Determination

To qualify for the award, an evaluator must:

- Demonstrate Unauthorized Reconstruction of Protected Information under the published evaluation conditions.
- Provide sufficient technical evidence to permit independent verification.
- Demonstrate that the reported methodology consistently produces the reported outcome.
- Cooperate with the independent verification process described in this publication.

Successful completion of these requirements constitutes a successful Independent Security Evaluation under the terms of this publication.

Independent Verification

Prior to the award being granted, SENDĀTRIX reserves the right to independently reproduce or observe the reported findings.

The purpose of this verification is not to dispute the evaluator's work, but to confirm that the reported methodology consistently produces the reported results.

Responsible Disclosure

Evaluators are encouraged to provide findings directly to SENDĀTRIX before public disclosure to allow sufficient opportunity for independent verification.

SENDĀTRIX is committed to acknowledging valid findings and recognizing successful evaluators in accordance with the published award conditions.

Recognition

Upon successful independent verification, SENDĀTRIX will publicly acknowledge the evaluator's achievement and award the published $5,000 USD evaluation award.

The purpose of this recognition is to encourage continued independent examination of the Structural Protection Model and to advance evidence-based discussion within the cybersecurity community.

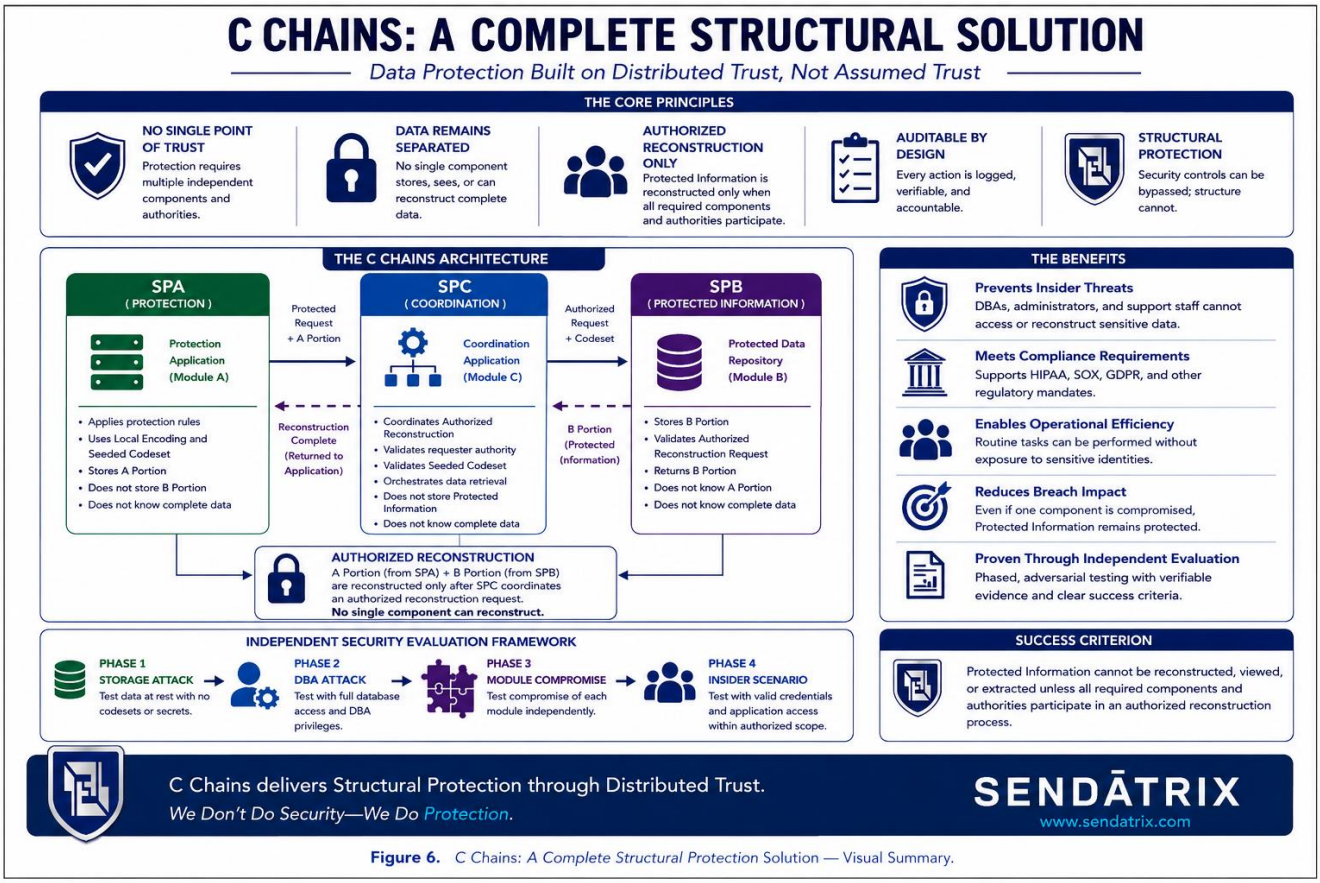


Figure 6. *C Chains: A Complete Structural Protection Solution — Visual Summary.*

8. Closing Statement

For decades, cybersecurity has sought to answer one fundamental question.

How do we prevent compromise?

That question remains essential.

Firewalls, encryption, Zero Trust architectures, privileged access management, endpoint protection, and continuous monitoring all represent significant advances toward reducing organizational risk.

The Structural Protection Model asks a different question.

What continues protecting Protected Information after compromise has occurred?

This publication does not suggest that compromise is inevitable.

Nor does it suggest that traditional cybersecurity controls are insufficient.

Rather, it recognizes that modern security architecture should continue protecting Protected Information even when privileged authority has been obtained through compromise or legitimate administrative control.

Whether the Structural Protection Model achieves that objective should not be determined through marketing claims, opinion, or theoretical discussion.

It should be determined through independent technical evaluation.

That is the purpose of this publication.

SENDĀTRIX invites the cybersecurity community to examine the implementation, challenge its assumptions, evaluate its architecture, and publish evidence-based conclusions.

Scientific progress depends upon independent examination.

Security architecture should be no different.

We welcome that examination.

9. Related Publications

This publication is one element of the SDX Technical Publications Series, which documents the principles, implementation, evaluation methodology, and operational practices associated with the Structural Protection Model and its implementation through C Chains™.

Readers seeking additional technical information are encouraged to consult the following companion publications.

SDX-TP-001 — Industry Perspectives on Trust, Database Security, and Structural Protection

A collection of industry viewpoints examining privileged access, insider threats, database administration, administrative trust, and the continuing challenge of protecting sensitive information after privileged compromise.

SDX-TP-003 — C Chains™ Security Architecture Guide

Describes the architecture, Distributed Trust Architecture, implementation concepts, operational workflow, and engineering principles underlying the C Chains™ implementation.

Additional publications, implementation guides, deployment references, research papers, and case studies will be released as the SDX Technical Publications Series continues to expand.

Revision History

Version	Date	Description
1.0	August 2026	Initial publication of the Independent Security Evaluation.
1.1	August 2026	Corrected companion-publication references to SDX-TP-003 and removed the nonexistent SDX-TP-004 reference.

Copyright