VERIDIAN LLC

Securing the Data That Matters Most

How the Zero Trust Data Security Platform Protects Healthcare, Financial Services, and Commercial Enterprises

WHITE PAPER

$97.8B
Healthcare Cybersecurity Market by 2031

$60.4B
BFSI Cybersecurity Market by 2030

$1.76M
Savings per Breach with Zero Trust

PREPARED BY
Veridian LLC

DATE
July 2026

PARTNER
NVIDIA

Table of Contents

1. The Problem: Data Is Under Siege

Every 39 seconds, an organization somewhere in the world suffers a cyber attack. The targets are not random — attackers pursue the data with the highest monetization value: patient health records that sell for hundreds of dollars each on the dark web, financial account credentials that enable immediate fraud, and material non-public information that powers insider trading. The industries that hold this data — healthcare and financial services — are the two most expensive sectors in which to suffer a breach.

$7.42M	$5.56M	$4.44M
Avg. Healthcare Breach Cost	Avg. Financial Breach Cost	Global Average Breach Cost

Source: IBM Cost of a Data Breach Report 2025

Traditional cybersecurity tools protect the perimeter — firewalls, VPNs, endpoint detection. But once an attacker (or a malicious insider) gains access, they inherit broad visibility into sensitive data. The perimeter model assumes trust after authentication. In healthcare, this means a registration clerk can view psychotherapy notes. In finance, a trader can access SAR filings. The problem is not access control — it is the *granularity* of access control.

Zero Trust Architecture eliminates implicit trust. But most Zero Trust implementations operate at the network or application layer — deciding whether a user can reach a server or an API endpoint. They do not address what happens *after* access is granted. They do not enforce which specific data fields a user can see within a record. Veridian's Zero Trust Data Security Platform does.

2. The Market Opportunity

The ZT DSP operates at the intersection of three rapidly expanding markets: healthcare cybersecurity, financial services cybersecurity, and zero trust architecture. Together, these markets represent a combined addressable opportunity exceeding $250 billion by 2031.

2.1 Healthcare Cybersecurity — $97.8B by 2031

The global healthcare cybersecurity market is projected to grow from $42.3 billion in 2026 to $97.8 billion by 2031, representing an 18.26% CAGR. This growth is driven by the rapid digitization of electronic health records, the expansion of telemedicine, and increasingly aggressive regulatory enforcement. Healthcare has been the most expensive industry for data breaches for 14 consecutive years. HIPAA penalties can reach $2.1 million per violation category per year, and class-action settlements routinely exceed $10 million.

Source: Mordor Intelligence, Healthcare Cybersecurity Market Report (May 2026)

2.2 Financial Services Cybersecurity — $60.4B by 2030

The BFSI cybersecurity market is forecast to reach $60.4 billion by 2030, growing at a 10% CAGR from $37.5 billion in 2025. Regulatory pressure is the primary catalyst — the SEC, FINRA, and global regulators imposed $542 million in compliance fines in Q1 2026 alone, with data privacy and operational risk enforcement surging. Open banking APIs, real-time payments, and institutional trading platforms create attack surfaces that traditional perimeter security cannot adequately protect.

Source: MarketsandMarkets, BFSI Cybersecurity Market Report (2025)

2.3 Zero Trust Architecture — $92B+ by 2030

The global zero trust security market reached approximately $42 billion in 2025 and is projected to exceed $92 billion by 2030 at a 15-17% CAGR. Federal mandates (Executive Order 14028, OMB M-22-09) and enterprise adoption (63% of organizations have partially implemented zero trust) are driving sustained investment. However, only 10% of large enterprises will achieve mature zero trust programs by 2026 — indicating massive runway for solutions that deliver measurable, field-level enforcement rather than entry-level controls.

The ROI of Zero Trust

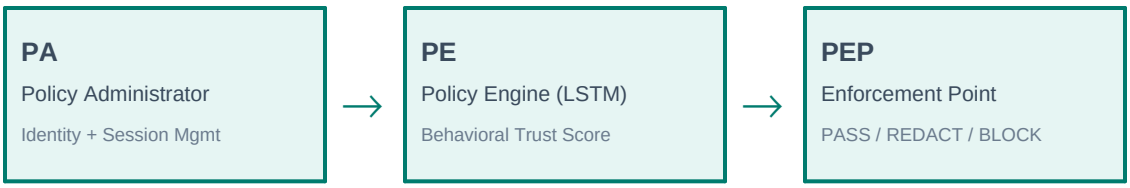
Organizations deploying zero trust architecture saved an average of **$1.76 million per breach** compared to non-adopters — a 39.6% cost reduction. Companies using AI-driven security automation detected breaches in **51 days vs. the 241-day global average**, an 79% acceleration in detection speed.

Source: IBM Cost of a Data Breach Report 2025

3. The Veridian Solution: Field-Level Zero Trust

The Veridian Zero Trust Data Security Platform is the only solution that enforces Zero Trust principles at the individual data field level. While other products decide whether a user can access a database, an API, or a file share, the ZT DSP decides whether a user can see each specific field within each specific record — in real time, on every request.

3.1 How It Works



Every data access request passes through three stages. The **Policy Administrator** verifies identity using X.509 certificates and device fingerprints. The **Policy Engine** evaluates behavioral patterns using an LSTM neural network, producing a continuous trust score from 0 to 1. The **Policy Enforcement Point** applies field-level decisions — PASS (show the value), REDACT (mask it), or BLOCK (hide it entirely) — based on the user's role, trust score, and the loaded schema.

3.2 Schema-Agnostic: One Engine, Every Vertical

The ZT DSP's most commercially significant advantage is that it requires **zero code changes** to move between verticals. The same PA, PE, and PEP code paths that protect naval classified data protect patient health records and financial trading data. The only component that changes is a JSON schema file — a configuration document that defines which fields exist, how they are enforced, and which roles can see them. A new vertical deployment is a new JSON file, not a new product.

3.3 AI-Driven Behavioral Trust Scoring

Static role-based access control (RBAC) cannot detect a legitimate user acting illegitimately. The ZT DSP's LSTM neural network continuously evaluates six behavioral features — access rate, access pattern diversity, time of access, data volume, failed attempt ratio, and idle duration — to produce a real-time trust score. This score drives a four-tier graduated response:

Tier	Trust Score	Response
PASS	>= 0.75	Full access per role/schema — normal operations
WARN	0.50 - 0.74	Access granted; session flagged for monitoring
INSPECT	0.25 - 0.49	Access granted; held for human review before release
TERMINATE	< 0.25	All fields blocked; session killed immediately

This graduated model means the platform does not choose between "let them in" and "lock them out." It applies proportional enforcement that tightens as risk increases — from logging, to human review, to automatic termination.

4. Healthcare: Stopping the $7.42M Breach

Healthcare suffers more expensive data breaches than any other industry — $7.42 million on average, driven by the high value of medical records, HIPAA's mandatory notification requirements, and the operational disruption of patient care. The ZT DSP's healthcare deployment enforces HIPAA's Minimum Necessary standard at the individual field level, ensuring every clinician sees exactly the data they need for patient care — and nothing more.

4.1 The Scenario — Memorial General Hospital

Consider a 500-bed teaching hospital with 2,400 staff members accessing electronic health records across 10 departments. The ZT DSP schema defines 31 fields per patient record with role-based enforcement across 8 clinical roles:

Role	Fields Visible	Key Restrictions
Physician	26 / 31	Substance abuse REDACTED (42 CFR Pt 2); genetic data BLOCKED (GINA)
Nurse	21 / 31	SSN, billing, psychotherapy notes, genetic data BLOCKED
Billing	12 / 31	Clinical data BLOCKED; insurance and demographics only
Front Desk	9 / 31	Name, DOB, contact info only; all clinical data BLOCKED

4.2 Without ZT DSP vs. With ZT DSP

Insider Threat: Registration Clerk Accesses Celebrity Records

Without ZT DSP

Registration clerk Marcus, passed over for promotion, opens 47 patient charts in 12 minutes at 2:17 AM seeking a celebrity's records to sell. Traditional access controls allow it — he has a valid login with chart access. The breach goes undetected for **73 days** until a tabloid publishes. Result: **$4.2 million** in HIPAA fines, legal costs, and class-action settlement. OCR investigation. Reputation damage.

With ZT DSP

> The LSTM detects the anomaly within minutes. Off-hours access + volume spike drops trust to 0.62 (WARN). By chart #8, trust hits 0.38 (INSPECT) — compliance is alerted, audit trail is max-verbosity. By chart #14, trust hits 0.19 — **TERMINATE**. Session killed. Marcus saw only his permitted 9 fields across all attempts — never the clinical data he sought. Total exposure time: **5 minutes**. Data exfiltrated: **zero**. HIPAA breach notification required: **none**. Cost: **$0**.

4.3 HIPAA Compliance — Built In, Not Bolted On

The ZT DSP does not require a separate compliance layer. Every enforcement decision — every field PASS, REDACT, or BLOCK — is logged to a WORM-compatible audit trail with UTC timestamps, satisfying HIPAA 164.312(b) audit controls. The schema itself encodes regulatory requirements: substance abuse records carry REDACT enforcement per 42 CFR Part 2, genetic data is BLOCKED per GINA, and psychotherapy notes are BLOCKED per 164.508(a)(2). Compliance is a property of the schema, not a separate workflow.

5. Financial Services: Enforcing the Chinese Wall

Financial institutions face a unique challenge: they must simultaneously protect client data, prevent insider trading, enforce information barriers between business units, maintain SAR confidentiality, and produce granular audit trails for SEC and FINRA examination — all while enabling high-speed trading operations. The average financial services breach costs $5.56 million, and 68% of insider threats in finance originate from employees with legitimate access.

5.1 The Scenario — Meridian Capital Group

Consider a composite financial institution spanning equities trading, fixed income, wealth management, investment banking advisory, prime brokerage, compliance, and back office. The ZT DSP schema defines 31 fields with enforcement across 5 institutional roles:

Role	Fields Visible	Key Restrictions
Trader	11 / 31	Client PII BLOCKED; MNPI BLOCKED (Chinese Wall); SAR BLOCKED
Compliance Officer	22 / 31	Broadest access; MNPI visible; SAR visible for investigation

Relationship Mgr	13 / 31	Client-facing data; no trading data, no MNPI, no SAR
Admin	20 / 31	Operational access; SSN visible for tax reporting (1099/W-9)

5.2 Without ZT DSP vs. With ZT DSP

Information Barrier Breach: Trader Seeks MNPI for Front-Running

Without ZT DSP

Equities trader Marcus queries 47 wealth management client accounts outside his desk coverage in 12 minutes, then attempts to access M&A; deal data. Traditional systems log the queries but do not block them in real time. The information barrier is breached. Result: SEC investigation, **$50M+ regulatory penalty exposure**, FINRA enforcement action, potential criminal insider trading charges, and reputational damage that costs institutional client relationships.

With ZT DSP

The LSTM detects the volume spike at 11:30 AM. Trust drops to 0.32 (INSPECT) — compliance analyst Diana Park is alerted in real time. When Marcus tries to access MNPI deal data, the schema-level BLOCK fires regardless of trust score — MNPI has an empty roles_allowed array. Trust crashes to 0.09 — **TERMINATE**. Total exposure: **8 minutes**. Data exfiltrated: **zero**. Meanwhile, 2,400 other sessions operated uninterrupted with **zero false positives**.

5.3 Regulatory Coverage — SEC to PCI DSS

Framework	ZT DSP Enforcement
SEC Rule 17a-4	Per-field audit trail with WORM-compatible timestamps (6-year retention)
FINRA Rule 3110	Role-based enforcement documented per record for supervisory review
SOX 302/404	Per-field enforcement log with threat tags for internal control testing
GLBA Safeguards	PII fields (SSN, address, phone) restricted to authorized roles only
BSA/AML	SAR filings hard-BLOCKED from all inline roles (anti-tipping compliance)
PCI DSS v4.0	Card numbers REDACTED at field level; token reference retained (Req 3.4)

SEC Info Barriers	MNPI deal data BLOCKED with empty roles_allowed (Chinese Wall enforced)

6. Commercial Market Expansion

The schema-agnostic architecture means every regulated industry with sensitive field-level data is an addressable market. The ZT DSP requires zero code changes per vertical — only a new JSON schema file. This creates an expansion model where new verticals are configuration deployments, not engineering projects.

Vertical	Regulatory Driver	Key Protected Fields	Status
Naval / DoD	NIST 800-207, CMMC 2.0	Classified mission data, personnel records	Deployed
Healthcare	HIPAA, 42 CFR Part 2, GINA	PHI, substance abuse, genetic data	Validated
Financial Services	SEC, FINRA, SOX, GLBA, PCI	MNPI, SAR filings, PCI card data	Validated
Defense / Intelligence	ITAR, EAR, ICD 503	Multi-classification data, SCI	Roadmap
Energy / Utilities	NERC CIP, TSA SD	SCADA controls, critical infrastructure	Roadmap
Government / FedRAMP	FedRAMP, FISMA, NIST	PII, CUI, tax records	Roadmap

Each new vertical follows the same deployment pattern: define the fields, set enforcement actions (PASS / REDACT / BLOCK), assign roles, and deploy. The engine handles identity management, behavioral trust scoring, field-level enforcement, and audit trail generation identically across all verticals. This architecture enables rapid go-to-market with minimal engineering cost per new vertical.

7. Competitive Differentiation

The cybersecurity market is crowded at the network and endpoint layers. The ZT DSP competes in a fundamentally different category — data-level enforcement — where the competitive landscape is sparse and the regulatory demand is growing.

Capability	Traditional ZTNA / SASE	DLP / CASB	Veridian ZT DSP
Enforcement granularity	Network / application	File / content pattern	Individual data field
Real-time behavioral trust scoring	No	No	Yes (LSTM neural network)
Graduated response (PASS/WARN/INSPECT/TERM)	Binary (allow/deny)	Binary (allow/block)	4-tier graduated
Schema-agnostic multi-vertical	No	Limited	Yes (JSON schema only)
Hardware acceleration (DPU/SmartNIC)	No	No	NVIDIA BlueField-3
Per-field audit trail (WORM-compatible)	No	Partial	Yes
Insider threat detection (behavioral)	Limited	No	Yes (6-feature LSTM)

No existing product combines field-level enforcement, AI behavioral trust scoring, schema-agnostic multi-vertical deployment, hardware acceleration, and WORM-compatible per-field audit trails in a single platform. The ZT DSP occupies a category of one.

8. The Investment Thesis

$250B+
Combined TAM Across 3 Markets

18.3%
Healthcare Cyber CAGR to 2031

39.6%
Breach Cost Reduction with Zero Trust

Veridian's ZT DSP addresses a structural gap in the cybersecurity market that grows wider with every new regulation, every breach headline, and every digital transformation initiative. The investment thesis rests on five pillars:

- **Massive, growing TAM.** Healthcare cybersecurity ($97.8B by 2031), financial services cybersecurity ($60.4B by 2030), and zero trust architecture ($92B+ by 2030) are all expanding at double-digit CAGRs, driven by regulatory mandates that are tightening, not loosening.

- **Regulatory tailwinds.** HIPAA enforcement is intensifying. SEC/FINRA imposed $542M in compliance fines in Q1 2026. Executive Order 14028 mandates Zero Trust for federal agencies. Every new regulation increases demand for the ZT DSP's field-level enforcement and audit capabilities.
- **Schema-agnostic scalability.** New vertical deployments require zero code changes — only a JSON schema file. This means engineering cost per new vertical approaches zero while revenue per vertical is independent. The marginal cost of expansion is a configuration file.
- **Hardware moat.** NVIDIA BlueField-3 DPU integration moves enforcement from the application layer to the NIC, enabling sub-millisecond latency at line rate. This hardware integration creates a technical moat that software-only competitors cannot replicate without similar DPU partnerships.
- **Proven across domains.** The same engine has been validated for DoD naval operations, healthcare (HIPAA/42 CFR Part 2/GINA), and financial services (SEC/FINRA/SOX/GLBA/BSA-AML/PCI DSS). Three domains, zero code changes. This is not a theoretical architecture — it is a working platform with simulation-validated enforcement across regulated verticals.

9. Next Steps

Veridian LLC invites prospective partners, enterprise customers, and investors to explore the Zero Trust Data Security Platform through the following engagement paths:

Engagement	Description	Audience
Technical Briefing	90-minute deep dive into platform architecture and live demonstration	CISOs, CTOs, Security Architects
Vertical Assessment	Map your organization's regulatory requirements to a ZT DSP schema	Compliance Officers, Data Protection Officers
Proof of Concept	Deploy ZT DSP in a sandbox environment with your data model	Engineering Teams, Security Operations
Investment Discussion	Market opportunity, growth strategy, and partnership models	Investors, Strategic Partners, Board

About Veridian LLC

Veridian LLC specializes in Zero Trust cybersecurity, AI-driven data protection, and secure application development for federal and commercial clients.

For technical briefings, partnership inquiries, or investment discussions, contact us at **veridianllc.com**.

Sources

- *IBM, Cost of a Data Breach Report 2025*
- *Mordor Intelligence, Healthcare Cybersecurity Market Report (May 2026)*
- *MarketsandMarkets, BFSI Cybersecurity Market Report (2025)*
- *Grand View Research, Zero Trust Security Market Report (2026)*
- *Axis Intelligence, Zero Trust Statistics 2026*
- *GlobeNewsWire, ZTNA Market Surges to $4.18B (July 2026)*
- *Gartner, Zero Trust Adoption Survey (2024)*
- *SEC, Enforcement Results for Fiscal Year 2025 (Press Release 2026-34)*
- *FINRA, 2026 Regulatory Oversight Report*