SERIES A

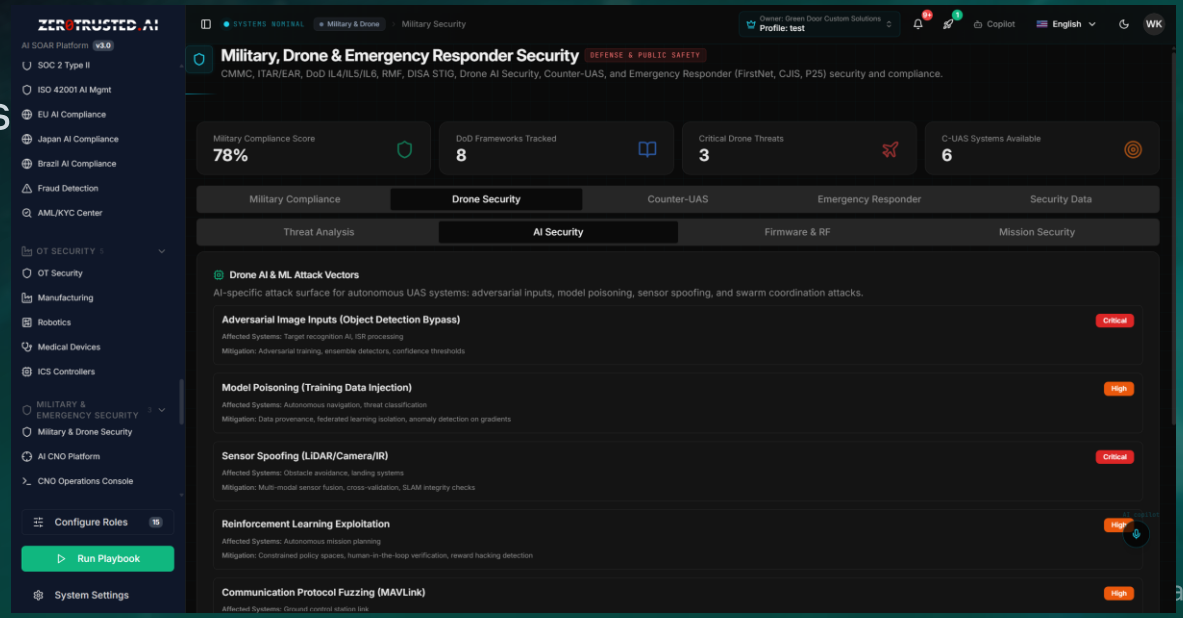
ZeroTrusted.ai AI SOAR / AI Firewall

Autonomous AI Security Operations

290+ AI Supervisor / Worker / Guardian Agents / 400 Command Line Tools / Over 50 AI Regulations / Defense Offense / Drone /OT

Defensive AI Infrastructure for Government & Critical Industry

Zero Trust for AI · AI Firewall · AI Governance · AI HealthCheck



September 2026

THE PROBLEM

Ungoverned AI & Uncontrolled Security Costs

No Control Over AI or Agents – Not Even the AI Companies

- **Security & Privacy Gaps**
  AI systems bypass traditional identity, network, and data controls. Shadow AI ingests sensitive data without oversight. You need to be aware of “everything” in AI attacks.
- **Reliability at Risk**
  Foreign and hostile models trained on stolen U.S. and enterprise data. Compliance frameworks don't protect inference or agent traffic. Agents are not controlled, tested or monitored.
- **62% Experimenting, Only 23% Scaled**
  Enterprises are adopting AI agents but governance gaps prevent production deployment.

Advanced AI Attack Surface Growth **+340%**

Mission Tools Too Expensive in the AI Age

- **Enterprise AI Implementation**
  $5,000 - $250,000+ for initial deployment depending on complexity and scale – plus expert employees
- **Annual Maintenance Burden**
  15-30% of initial build cost annually for infrastructure, monitoring, retraining, and support.
- **Spiraling Shadow AI Costs**
  Departments spinning up AI projects without oversight leads to rapidly spiraling costs and security vulnerabilities.

Fragmented Solutions **5-7 Vendors**

The Gap: Organizations need a unified, cost-effective solution that provides complete AI governance without the enterprise price tag.

MARKET TIMING

Why Now: The AI Security Imperative

Government Adoption

AI is being operationalized inside DoD, IC, DOT, FAA, and critical infrastructure. Models making high-impact decisions without auditability.

59
Federal AI regulations in 2025

AI Agent Explosion

62% of enterprises experimenting with AI agents, but only 23% have scaled. Governance gaps are the primary blocker.

39%
Report EBIT impact from AI

Attack Surface

Every ungoverned AI deployment is a new attack surface and intelligence target. Zero-day vulnerabilities tripled in 2024.

33%
Ransomware of all breaches

Explosive Market Growth

AI Governance	SOAR Market	Zero Trust Security	Enterprise AI Adoption
$308M	$2.22B	$42.3B	88%
2025 → $3.6B 2033	2026	2025 → $148.7B 2034	Regular AI use (2025)
36% CAGR	18.5% Growth	14.8% CAGR	Up from 78% in 2024

The Need: The U.S. and allies need a Zero Trust layer at the AI runtime, not just at the perimeter. Executive Order mandates zero trust for all federal agencies.

VALUE PROPOSITION

Everything You Need - Including the AI Agents

Complete Platform

Defensive AI infrastructure in one unified platform. No need for 5-7 different vendors. Everything from firewall to governance to compliance.

- ✓ AI Firewall + Gateway + HealthCheck
- ✓ Unified governance dashboard
- ✓ Single vendor, single contract

290+ AI Agents Working For You

Autonomous AI Supervisor and Guardian Agents that actively do the security work - not just monitor. Self-healing, self-optimizing defense. Plus all the tools to do the work – over 30 security tools working together with AI Agents.

- ✓ Autonomous threat detection & response
- ✓ Continuous policy enforcement
- ✓ No human intervention required

Model Agnostic

Works with any AI system - internal, open-source, commercial models. No vendor lock-in.

Deploy Once

Governs continuously with no code changes to existing applications. Instant protection.

Cost Effective

Fraction of the cost of enterprise AI security stacks. Predictable pricing model.

The Promise: Deploy AI at speed without sacrificing security, privacy, or ethics. The only platform that gives you both the tools AND the AI agents to do the work.

OUR SOLUTION

AI SOAR Platform

ZEROTRUSTED.AI

Core Platform Components

AI Firewall

Inline runtime enforcement for prompts, responses, and agent actions with real-time blocking / Shadow AI / Prompt / Data Protection

AI HealthCheck

Continuous monitoring for drift, hallucination, and policy violations across all AI systems

AI Gateway

Zero Trust control for MCP, A2A, and API-based AI agent traffic

Chain-of-Custody

Cryptographically verifiable audit trail for compliance and forensics

60+ AI Supervisor & Guardian Agents

Supervisor	Guardian	Response	Compliance
Monitor & Coordinate	Enforce & Block	Auto Remediate	Audit & Report

Agent Capabilities

- **Autonomous Threat Detection**
  Real-time analysis of all AI interactions
- **Self-Healing Response**
  Automated threat response without human intervention / Long term memory / full testing and remediation platform
- **Policy Enforcement**
  Continuous guardrail application
- **Drift Detection**
  Monitor model behavior changes over time
- **Hallucination Blocking**
  Prevent false or misleading outputs
- **Compliance Monitoring**
  Continuous audit for regulations

290+

Specialized AI Agents with over 400 CLI tools

Working 24/7 to protect your AI

Zero Trust at AI Runtime

Deployment Architecture

1 Deploy Once

Single deployment governs continuously across all AI systems. No code changes to existing applications. STIGed / On-Premis / Gov Cloud / Private Cloud

2 Independent Guardrails

Enforcement doesn't depend on LLM vendor's ethics or T&Cs. Your policies, your control. Shadow AI, Embedded AI, Data Drift – all AI NIST / MIT AI Risk

3 Session Isolation

Encryption and policy enforcement at the inference layer. Complete data protection.

Technical Differentiation

Runtime Zero Trust Engine

Not just static scanning - continuous runtime enforcement with real-time response capabilities. Then AI Guards to verify.

Cryptographic Verification

Verifiable session and transaction logging for inference events. Tamper-proof audit trails. Full Chain of Custod

Model Agnostic

Protects internal, open-source, and commercial models. No vendor lock-in, complete flexibility. We help customers retain their fine tuning and training

Compliance Aligned

Continuous AI HealthCheck aligned with NIST AI RMF, MIT AI Risk, and emerging AI regulations.

Environment Coverage

LLMs · SLMs · RAG · VectorDB · AI Agents · Cloud · Hybrid · Air-Gapped

Compliance Frameworks

- NIST AI RMF
- EU AI Act
- ISO 42001
- FedRAMP
- MIT AI Risk
- SOC 2

COMPETITIVE ADVANTAGE

Owning the Defensive Layer

Active vs. Passive

Only platform combining AI SOAR with 60+ autonomous AI agents that actively do security work.

Competitors
Passive monitoring tools that alert but don't act

National Security

First-mover in AI-native defensive infrastructure with government-grade security and compliance.

Competitors
Generic enterprise tools not built for classified environments

Audit Capability

Cryptographically verifiable session and transaction logging for inference events.

Competitors
Standard logging without cryptographic verification

Strategic Positioning

No Vendor Lock-in

Model-agnostic governance works with any AI system. Customers maintain complete flexibility and avoid dependency on single vendors.

Purpose-Built

Built from ground up for national security and regulated industries. Every feature designed with compliance and audit requirements in mind.

Palantir secured **Data & Decisions** → CrowdStrike secured **Endpoints** → ZeroTrusted.ai secures **AI Itself**

290+	0	100%	<100ms
AI Agents	Code Changes	Model Agnostic	Response Time

Distributors & Resellers

ZERØTRUSTED.AI

Revenue Streams

Platform Subscriptions

Primary

AI SOAR platform components: Firewall, Gateway, HealthCheck, Agent Fleet, AI SOAR – for MSSPs/Large Multinationals, Gov

Tiered Governance

Secondary

Pricing for regulated enterprises and federal agencies based on AI maturity

Professional Services

Services

AI compliance deployment, NIST/FedRAMP/EU AI framework mapping

Channel Strategy

Federal Integrators
IC, DoD, and Civ Federal

Cybersecurity VARs
Regional security partners

Cloud Marketplaces
AWS, Azure, GCP

Defense Primes
LAI Focused

Go-to-Market Model

1. **Channel-First Strategy**
   Distributors and resellers drive 70%+ of revenue. Focus on federal integrators with existing government relationships.
2. **Strategic Partnerships**
   Co-sell agreements with cloud providers (AWS, Azure, GCP, Red Hat) and defense primes for bundled solutions.
3. **Milestone-Based Pricing**
   Pricing aligned with customer AI maturity journey - start small, scale as AI adoption grows.
4. **Land & Expand**
   Initial pilot in one department, expand across agency/enterprise as value is demonstrated.

70%+	12-18	90%+
Channel Revenue	Month CAC Payback	Gross Margins

MARKET FOCUS

Target Markets & Traction

Target Markets

Primary: DoD & IC

High Priority

U.S. Department of Defense and Intelligence Community AI programs. Pentagon-focused initiatives and OTA contracting activity.

Secondary: Civilian Agencies

Growing

DOT, FAA, and other civilian agencies adopting AI in high-compliance missions.

Critical Infrastructure / Highly Regulated

Expansion

Energy, telecom, healthcare, finance, and transportation sectors.

Global Markets

- Brazil (LGPD)
- Japan
- EU (AI Act)
- Five Eyes

Current Traction

DoD AI Pilots

Active pilots including Pentagon-focused initiatives and OTA contracting activity

IC Pilots Re-initiated

Post-DOGE focus on AI security and governance within Intelligence Community

Gartner Recognition

TRiSM recognition as innovative AI governance and security solution - 2024 / 2025 /2026

Product Hunt and Enterprise Security Top AI Firewall #1

Product of the Day and global SaaS recognition

International Expansion

Brazil (LGPD) and Japan deployments for regulated AI

5+
Active Pilots

3
Countries

OUR TEAM

World-Class AI Security Experts

5 AI Developers

Core Engineering Team

- **LLM Security Specialists**
  Deep expertise in securing large language models and AI systems
- **Autonomous Agent Engineers**
  Building self-healing, self-optimizing AI security agents
- **Defensive AI Systems**
  Experience building AI that protects against AI-driven threats

2 Tech Founders

Leadership & Vision

- **Zero Trust Architecture**
  Deep expertise in zero trust security frameworks and implementation
- **National Security Experience**
  Background in DoD, IC, and classified AI deployments
- **Enterprise AI Deployment**
  Track record of scaling AI systems at Fortune 500 companies

Combined Expertise

DoD & IC	Fortune 500	AI Research	Advisors
National Security	Enterprise Security	Cutting Edge ML	Former CISOs

7 Total Team Members - Small, elite team focused on execution

Hiring for key roles

SERIES A

Current Status & The Ask

ZERØTRUSTED.AI

Current Status

Product

AI SOAR platform with 60+ AI agents in production. Validated with DoD/IC pilots. Over $1.3 Million Founders Investment

Traction

Active pilots with national security customers, Gartner recognition, international expansion.

Team

7 total (5 AI developers + 2 founders). Hiring for sales, customer success, and engineering.

IP

Proprietary Zero Trust engine for AI runtime, cryptographic logging technology, agent framework.

The Ask: Series A - 2027

Series A Funding Round

$8-12M

To accelerate growth and market leadership

Use of Funds

1. **Expand DoD/IC Delivery**
   Scale implementation teams for national security customers
2. **Accelerate R&D**
   Agent control, MCP/A2A governance, next-gen capabilities
3. **Scale GTM**
   Federal integrators, channel partners, enterprise sales, support for International Partners
4. **Market Positioning**
   De facto defensive AI infrastructure for U.S. and allies

18-24	3-5x	Q3
Month Runway	Revenue Growth	2026 Target

THE FUTURE OF SECURE AI

ZEROTRUSTED.AI

Securing the Future of AI

AI is now a **sovereign asset** and a potential **weapon system**.

It must be governed with the same rigor as other national security systems. ZeroTrusted.ai provides the defensive AI infrastructure that governments and critical industries need to deploy AI at speed without sacrificing security, privacy, or ethics.

290+ AI Agents
Autonomous Defense

National Security
Government Grade

36% CAGR Market
$3.6B by 2033

Join us in building the future of secure AI.

contact@zerotrusted.ai

zerotrusted.ai

ZEROTRUSTED.AI