Tonic

Agentic CTEM Platform

The Architecture Powering Continuous Exposure Reduction

March 2026

The Challenge

Modern security programs operate across dozens of disconnected tools. Vulnerability scanners, cloud platforms, identity systems, ticketing tools, and asset inventories each provide a partial view of the organization's security posture. Yet none of them maintain a complete and continuously updated understanding of the enterprise exposure landscape.

As a result, security teams struggle with several persistent challenges:

- Thousands of vulnerabilities with unclear prioritization
- Risk signals scattered across multiple systems
- Manual investigation required to understand context
- Remediation efforts that fail to measurably reduce exposure

Most existing security platforms provide **visibility and scoring,** but they stop short of enabling **continuous exposure reduction.** To solve this problem, organizations need a system that can continuously:

- Synthesize security and enterprise context
- Reason about exposure and risk
- Coordinate remediation across teams
- Validate that risk is actually reduced

This is the goal of **Tonic's Agentic CTEM Platform**.

The Tonic Agentic CTEM Platform

The Tonic platform introduces a new architecture designed to continuously transform fragmented security signals into **risk decisions and remediation outcomes**. The platform consists of two primary architectural layers:

Security Data Fabric

The contextual intelligence layer that continuously synthesizes security and enterprise data.

Decision & Execution Layer

The operational layer where AI agents and applications drive exposure reduction across the organization.

Together, these layers form a **closed-loop exposure reduction system.**

Architecture Overview

The Tonic architecture is built around six core components:

Security Data Fabric

Data Foundation

A self-improving security data fabric that ingests, reconciles, and normalizes signals from across the enterprise.

Context Engine

Extracts business, operational, and adversarial context from both structured and unstructured sources.

Exposure Intelligence

A multi-dimensional exposure graph that models relationships across assets, exposures, identities, and business services.

Let’s dig in.

Decision & Execution Layer

Agentic Control Plane

The governance layer controlling what agents can access and execute, enforcing permissions and human oversight.

Tonic Applications & MCP

The operational interface where security teams investigate exposure, coordinate remediation, and manage workflows.

Tonic Agents & Third-Party Agents

Domain-specific AI agents that continuously prioritize, coordinate, and validate exposure reduction at scale.

Exposure Intelligence

A Living Model of Enterprise Risk

At the core of the platform sits **Exposure Intelligence**. Exposure Intelligence is a continuously evolving graph that connects technical findings with business context. By reasoning across this graph, the platform can determine:

- Which exposures truly matter
- Which business systems are affected
- How attackers could exploit weaknesses
- Which teams are responsible for remediation
- Whether remediation actions actually reduced risk

This allows organizations to move beyond **generic severity scores** toward **context-driven exposure decisions.**

Decision & Execution Layer

Turning Intelligence into Risk Reduction

While the Security Data Fabric maintains understanding of the environment, the **Decision & Execution Layer** ensures that exposure intelligence leads to action.

Agentic Control Plane

The Agentic Control Plane governs how automation operates within the environment. It enforces:

- Access permissions
- Approval workflows for high-risk actions
- Execution policies
- Complete auditability

This ensures that AI agents operate safely and transparently within enterprise environments.

Tonic Applications & MCP

The application layer allows security teams to operate the platform through:

- Exposure investigation workflows
- Remediation coordination tools
- Integrations with existing security and IT systems

Through MCP-powered integrations, Tonic can operate directly within the tools teams already use.

Tonic Agents & Third-Party Agents

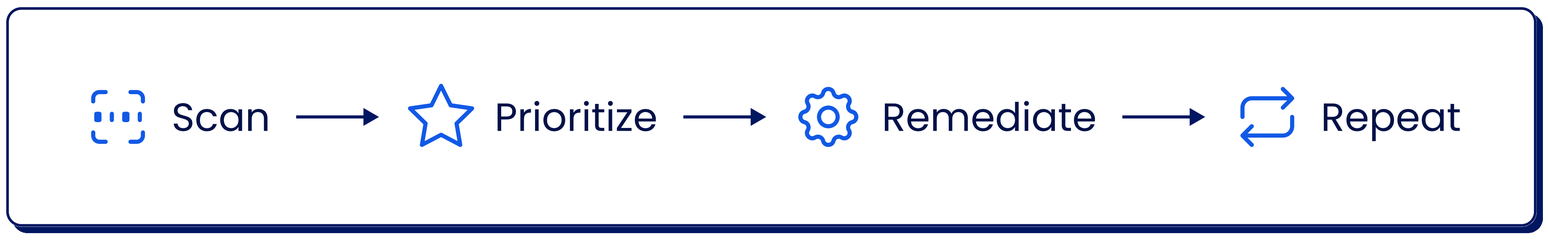
Domain-specific agents operate continuously across the environment to drive exposure reduction. These agents:

- Analyze exposure intelligence
- Prioritize remediation actions
- Coordinate work across teams
- Validate remediation outcomes

Agents can operate across both native Tonic capabilities and third-party tools, allowing organizations to orchestrate remediation across complex environments.

Continuous Exposure Reduction

Traditional vulnerability management operates as a **periodic workflow:**



The Tonic architecture enables a **continuous exposure reduction loop:**

Signals are ingested from across the enterprise

- Context is extracted and reconciled
- Exposure intelligence is generated
- Agents coordinate remediation
- Risk reduction is validated
- And the model continuously updates

This closed-loop architecture ensures that exposure management becomes an **ongoing operational process rather than periodic analysis.**

The Architecture of Agentic Exposure Management

Security teams today are overwhelmed by fragmented data and disconnected tools. The future of security operations requires systems that can **continuously maintain context and coordinate action across the enterprise.**

The Tonic Agentic CTEM Platform provides this foundation. By combining a self-maintaining Security Data Fabric with governable AI agents and operational applications, organizations gain the ability to:

Prioritize what truly matters

Coordinate remediation across teams

Continuously validate risk reduction

This architecture enables a new model of security operations: **Agentic Exposure Management.**