

Agentic Exposure Management

Fix the exposures that matter most – at machine speed

Stop managing vulnerabilities. Start reducing risk.

Tonic's AI-native Exposure Management platform turns fragmented security and IT signals into clear, **business-aligned** risk decisions and **orchestrates remediation to completion.**

Instead of static scoring, dashboards and ticket factories, Tonic operates as a **decision and execution engine** that continuously prioritizes what matters most and ensures real exposure reduction, with humans firmly in control.

Benefits

Reduce Risk, Respond Faster

Continuously focus on what matters and drive remediation to completion

Reclaim Expert Time

Agents handle investigation and coordination while teams focus on judgment

Turn Decisions into Action

Eliminate friction across security, IT, and the business with clear ownership

Get Clarity and Control

Replace generic scores with a business-led view leaders can act on

Why Vulnerability Management is Broken



Most security breaches don't happen because vulnerabilities were not detected.

Breaches happen because vulnerabilities were mismanaged - misprioritized or remediated too late

Industry studies consistently rank vulnerability exploitation among the top causes of breaches.

End-to-End Agentic Exposure Management Platform

Tonic replaces legacy vulnerability management with four continuous, agent-driven capabilities



1. Collect

Tonic Data Engineer
Agentic ingestion & sense-making

- Connect any source/data/environment
- Harmonizes and reconciles data continuously
- Detects drift, gaps, and stale signals
- Resolves assets, identities and exposures into one graph



2. Contextualize

Tonic Navigator
Agents that understand the business & the attackers

- Determines business criticality
- Identifies asset owners and fixers
- Analyzes reachability, exploitability, and blast radius
- Infers missing context and updates continuously as environments change



3. Prioritize

Tonic Exposure Analyst
Transparent, adaptive risk decisions

- Continuously re-ranks millions of findings
- Factors business impact, adversarial signals, and asset resilience
- Re-prioritizes as conditions change
- Fully explainable and customizable



4. Act

Tonic Mobilization Coordinator
Autonomous remediation orchestration & validation

- Routes fixes to owners across teams and tools
 - Injects context and remediation guidance
 - Tracks and validates completion
 - Manages exceptions, mitigation and approvals
- From recommendations & Tickets to verified outcomes & follow-through**

Measurable Impact

Customers are already seeing:

90%

Reduction in exposures requiring remediation

80%

Remediation automatically assigned and orchestrated

50%

Faster remediation of business-critical risk

35%

Security team capacity reclaimed

Eliminate Exposures with Six Degrees of Context™

Business context

Determine how critical the asset is, the business processes it supports, and the potential impact if compromised.

Organizational Context

Identify which department, team and individuals “own” the asset and are responsible for fixing issues on it.

Geographical Context

Pinpoint where the asset is located and how specific physical and local circumstances affect its security.

Operational Context

Ascertain the function of the asset in daily operations, how resilient is it, and what are its interdependencies with other entities.

Temporal Context

Know the lifecycle stage of the asset, and its history of vulnerabilities, incidents and configuration changes.

Adversarial Context

Assess the likelihood that a threat actor will be able to reach the asset and cause harm.

“Tonic is a game-changer. It used to take days to identify an exposed asset and understand the potential risk to the business if exploited. With Tonic it takes minutes.”

Mark Fournier, CIO & CISO



UNITED STATES
SENATE FEDERAL
CREDIT UNION

Trusted by



UNITED STATES
SENATE FEDERAL
CREDIT UNION



About Tonic Security

Tonic Security delivers an end-to-end agentic decision and execution platform for exposure management. Its AI-native solution continuously transforms fragmented security and IT signals into business-aligned risk decisions and verified remediation outcomes. By combining a self-maintaining security Data Fabric with governable agentic workflows, Tonic enables organizations to move from vulnerability management to continuous risk reduction at scale. Leading enterprises rely on Tonic to cut remediation time, eliminate noise, and measurably reduce exposure across their attack surface.

To learn more visit www.tonicsecurity.com.