

Elevate Your Exposure Management with Powerful Context

Tonic solves a critical challenge every security team faces: the inability to cut through the noise and quickly determine which vulnerabilities matter, how they impact the business, and which risks require immediate attention.

Tonic leverages domain-specific AI agents and a unique data fabric to uncover and prioritize exposures with actionable context, enabling teams to make quick, informed decisions across complex digital ecosystems.

Benefits

Reduce Risk, Respond Faster

Reduce the exposure window for remediating vulnerabilities and triaging alerts.

Work Faster, Not Harder

Stop wasting time on false positives, reduce tool pivots, and enhance collaboration between security, IT, and business stakeholders.

Optimize Operational Efficiency

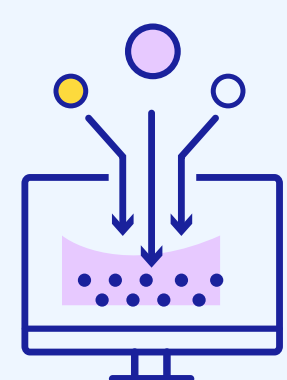
Enhance efficiency while minimizing dependencies on homegrown systems, manual collection processes, and information outside the security teams.

See the Big Picture

Move beyond technical visibility and generic security scores to attain a business-led perspective of your security team.

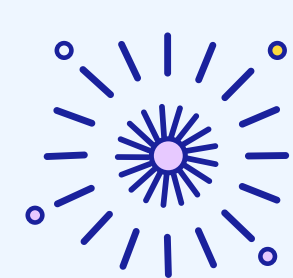
Unified Exposure Management Platform

The first context-driven Exposure Management platform that offers superior visibility so you to focus on the findings that are relevant to your business in four steps



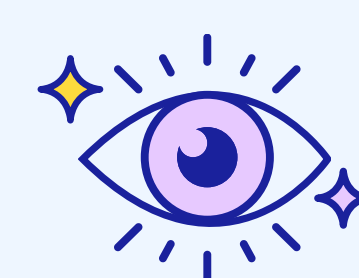
Collect

Connect any source, upload any file, ingest any data – structured or unstructured – across hybrid, distributed and diverse environments.



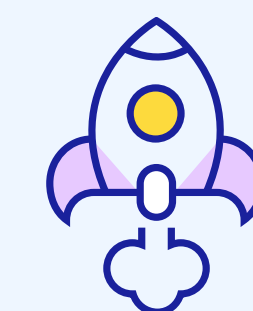
Contextualize

Super-charge triage and analysis of vulnerabilities and threats by quickly establishing context, and consuming it anywhere.



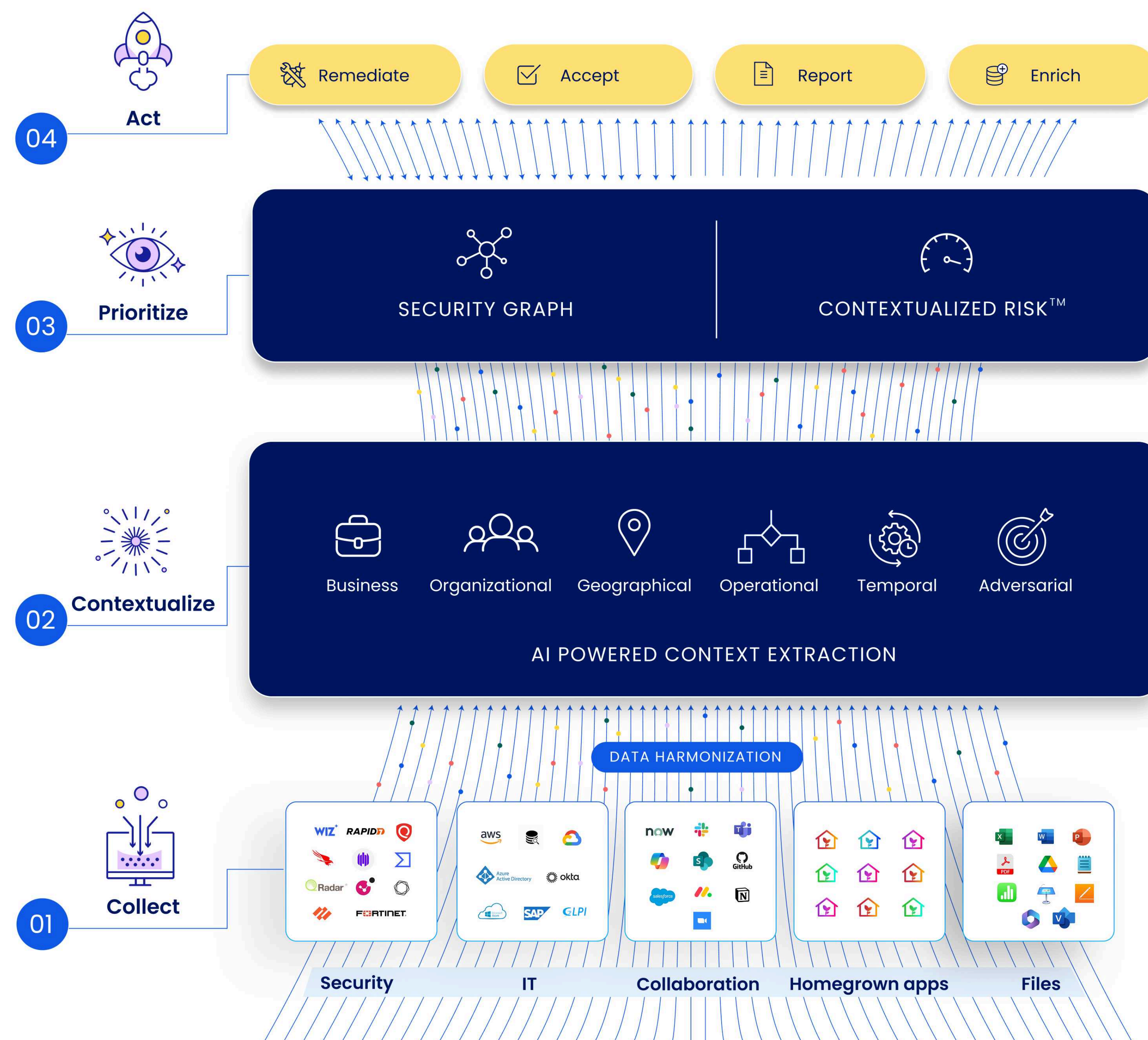
Prioritize

Know your Contextualized Risk – View and prioritize the main risks to your business in a single pane of glass.



Act

Confidently manage and automate remediation and reporting, while enriching systems of record with context.



“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



50%

Reduction in MTTR to business critical exposures

20%

Time saved per week on contextualizing findings and triaging alerts

90%

Reduction in exposures requiring remediation

80%

Assets enriched with ownership

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 it is, 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.

About Tonic Security

Tonic is reshaping Exposure and Vulnerability Management by providing the context security teams need to accelerate prioritization and remediation of vulnerabilities and threats. Powered by Agentic AI and a security Data Fabric, Tonic extracts meaningful and actionable context from unstructured organizational knowledge and threat intelligence, empowering security teams with superior visibility, dramatic reduction in false positives, and a sharp focus on findings that matter. Leading organizations, including Fortune 500 companies, rely on Tonic to slash remediation time and reduce risk to key business processes. **To learn more visit www.tonicsecurity.com.**