Software Analyst Cyber Research

OCTOBER 2025

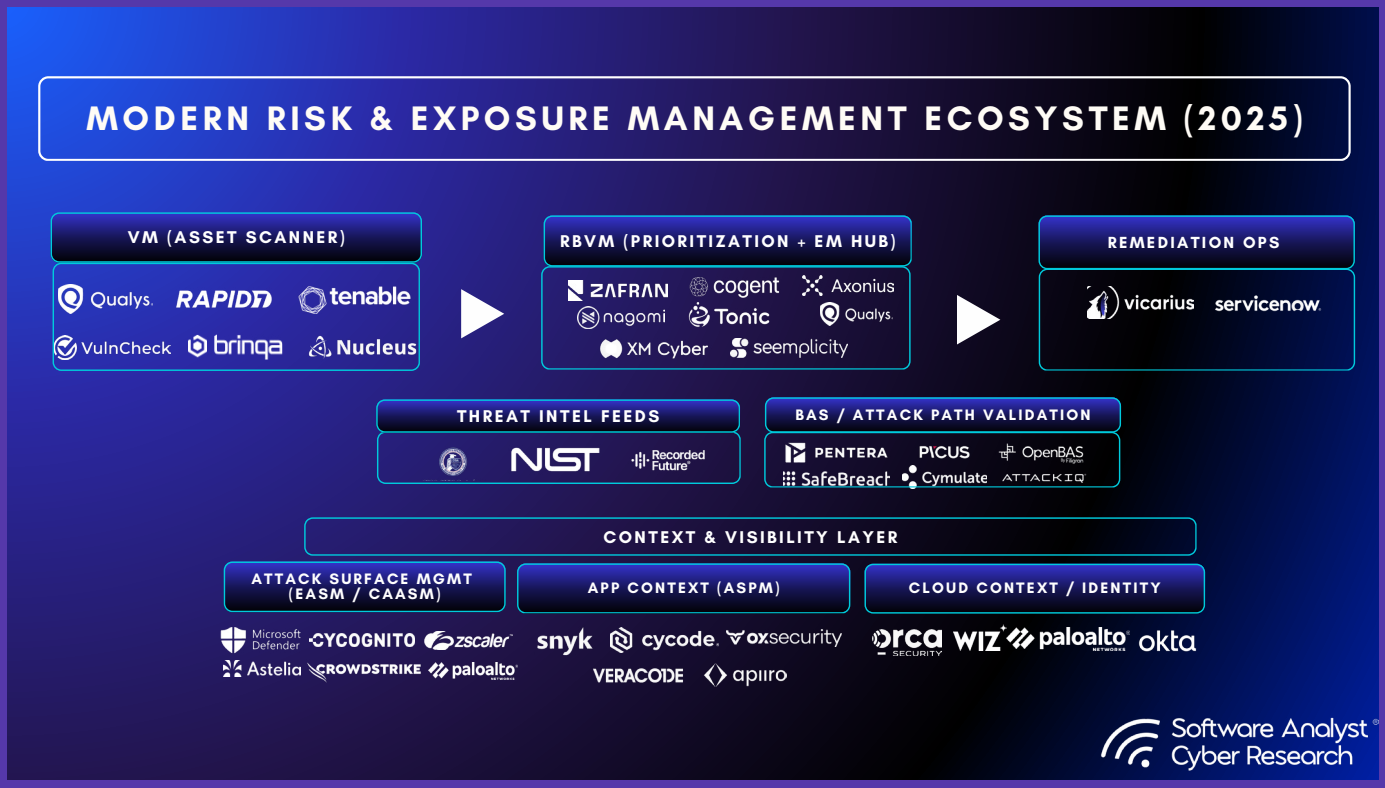
Tonic

SACR 2025

EMERGING INNOVATOR

MODERN RISK AND EXPOSURE MANAGEMENT

2025 MODERN RISK AND EXPOSURE MANAGEMENT PLATFORMS



Disclaimer

The purpose of this image is to provide a high-level depiction of various risk and exposure management categories, and it is not intended to rank the vendors (many of them cross categories in capabilities). It is also not all-inclusive, but rather based on the vendors we have interacted with in some capacity.

Table of Contents

Introduction

Vulnerability management is not what it was in the 2000s. Factors like CVSS scores, vulnerability counts, and the number of resolved CVEs are no longer the primary standards. Today, organizations do not need reminders to scan their resources for vulnerabilities because most already do so. The main struggle now is prioritization: knowing what truly matters, understanding the impact of not fixing it, and showing how to quickly address it.

In 2025, the combination of faster attacker breakout times, the use of AI to scale exploits, expanding attack surfaces, and increased board-level scrutiny and liability for CISOs has made exposure management a top organizational priority. As a result, the traditional ways of defining exposure or risk and calculating the probability of exploit have been evolving.

Practitioners are asking deeper questions to justify risk scores, the ***what***, ***why***, and ***how***: what factors constitute an evolved definition of "exposure," why this matters to their organization, and how to remediate this risk to deliver measurable outcomes to the board.

The market has responded accordingly. Vendors are quickly converging categories: Vulnerability Management (VM), Risk-Based Vulnerability Management (RBVM), Attack Surface Management (ASM), Cyber Asset Attack Surface Management (CAASM), Application Security Posture Management (ASPM), and Breach and Attack Simulation (BAS). These capabilities, under the CTEM umbrella, are now integrated within modern risk and exposure management platforms.

To bring key insights into this market, we conducted a deep dive into the world of risk prioritization and exposure management. We interviewed practitioners and security leaders from both large and small organizations to understand their primary concerns around risk and exposure. We also analyzed vendors that categorize themselves under the CTEM umbrella to assess how they have evolved in addressing practitioner concerns.

The goal of this report is to articulate practitioner concerns, assess how leading vendors are addressing them, present unbiased findings from platform deep dives, in-depth questionnaires, and customer interviews, and produce a practical framework for organizations looking to operationalize risk management.

This report highlights the major trends shaping exposure management in 2025 and their impact on security teams. We examine how exposure programs deliver value today, where they must evolve, and the characteristics that distinguish modern platforms. The analysis focuses on vendor convergence across VM, ASM, CAASM, and CNAPP, the shift toward exploitability and runtime-driven prioritization, and the growing role of automation and AI in defining **Modern Risk and Exposure Management** Platforms.

To maintain vendor neutrality, we examined practitioner perspectives, vendor strategies, customer references, and independent market research. To ground these concepts in practical assessment, we evaluated vendors using our **DDPER** (**Deployment, Data Collection, Prioritization, Exposure, Remediation**) framework.

The report also provides a **step-by-step practitioner guide** to selecting the best risk and exposure management solution for organizational needs. It is designed to separate utility from hype and provide security leaders with a clear framework for evaluating exposure and risk in their environments.

Actionable Insights

- **Risk and Exposure Management is being redefined**

Modern exposure platforms are challenging how exposure was calculated in the past by moving past configuration reads and performing true network reachability, ingesting context from unstructured data sources and even looking at social chatter for probability of exploitation beyond KEV and EPSS databases.

- **AI and automation are maturing into core utilities:**

AI agents are shifting from hype to function, assisting with ownership mapping, remediation orchestration, and contextual analysis to reduce operational overhead and mean time to remediation (MTTR).

- **Capability convergence is accelerating:**

VM, RBVM, ASM, CAASM, ASPM, BAS, CTEM and CNAPP are merging into unified Risk and Exposure Management platforms, providing dynamic scoring, context driven exposure reduction loops.

- **Aggregator style platforms are rising**

Aggregator-style exposure management platforms focus on consolidating data from multiple scanners, posture tools, and threat feeds into a single normalized risk view. They excel in organizations with mature, diverse toolsets.

- **Pure scanning platforms prioritize depth and native visibility**

Pure scanning or unified platforms perform their own continuous scanning across cloud, infrastructure, identity, and application layers. They offer immediate visibility and control, eliminating dependency on external data sources.

- **Remediation operations bridge security and IT**

Leading platforms now include bi directional ticketing, fix aggregation, SLA tracking, and automated verification to ensure findings translate into measurable risk reduction.

- **Board reporting is outcome based, not activity based**

Success metrics now track risk reduction, exposure trends, and exploitability validation, not the number of vulnerabilities fixed or scans completed.

- **Market divergence is emerging**

Platforms are evolving into two broader categories, aggregators that unify multi tool data for contextual prioritization, and in-house scanning platforms that integrate scanning, analytics, and automated remediation in-house.

- **Practical guide to selecting the right solution**

The Practitioner's Guide helps organizations choose and implement the right exposure management solution by outlining a clear, step-by-step framework to assess needs and then rank vendors against those needs to pick the right solution.

- **SACR Prediction**

Aggregator platforms are adding lightweight in-house scanning to reduce reliance on external tools and offer a single source of truth. Meanwhile, pure-play scanners are expanding into contextual analytics and automated remediation. Both are converging toward autonomous, outcome-driven exposure management focused on measurable risk reduction.

Quick Recap on Industry Definitions

Taken together, these challenges show why vulnerability management has had to evolve. The industry's definitions have shifted over time as well: from traditional Vulnerability Management to Risk-Based approaches, to more unified pipelines, to Continuous Threat Exposure Management. Before outlining the priorities security leaders are setting for 2025, it is important to establish this progression and align on the definitions of the different models in the vulnerability management world.

1. VM (Vulnerability Management)

This is the basic foundation. It includes a program for scanning all assets for vulnerabilities and providing a list of vulnerabilities with priorities that are based on CVSS scores. This does not take any other environmental factors into account.

2. Risk-Based Vulnerability Management (RBVM)

An evolution of VM that integrates "risk" to prioritize remediation. Key inputs include exploit intelligence from databases such as the Known Exploited Vulnerabilities (KEV) catalog, which identifies what is being exploited **now**, and the Exploit Prediction Scoring System (EPSS), which identifies what is **likely to be exploited soon**.

3. Unified Vulnerability Management (UVM)

A consolidated approach to vulnerability management that ingests vulnerability findings from multiple sources, normalizes and deduplicates them and helps with prioritization based on centralized view.

4. Attack Surface Management (ASM)

It maps every internet-facing asset and service, ties each one back to its owner, and calls out exposures like open ports, misconfigurations, leaked credentials, or expired certificates. The goal isn't just visibility, it's also validation. When combined with Breach and Attack Simulation (BAS), security teams can understand which exposures are truly exploitable.

5. Application Security Posture Management (ASPM)

ASPM gathers data from every part of the application lifecycle, including SAST, DAST, SCA, secrets management, IaC, supply chain, cloud configurations, and runtime environments, to give teams a unified view of risk. But it is not just about visibility. ASPM adds asset posture context, clarifies ownership, and connects with existing workflows.

6. Continuous Threat Exposure Management (CTEM)

A term defined by Gartner for a program defined with continuous identification, validation, prioritization, and reduction of exposures across the enterprise attack surface. Emphasizes ongoing discovery, business context, attack-path validation, and measurable reduction of exposure.

Evolution of Vulnerability Management into Exposure Management

Vulnerability management used to mean running periodic scans that generated long lists of issues, with severity ranked mainly by CVSS scores. That approach no longer fits. The modern cloud-native applications, dynamic infrastructure, and a constantly shifting threat landscape has changed expectations. What organizations want are solutions that move beyond static feeds and config reads, providing prioritization that reflects real exploitability and business context, platforms under the CTEM umbrella are evolving to address these needs, thus leading to the evolution of Modern Risk and Exposure Management Platforms.

Factors that led to Modernization

Before diving into the key characteristics of modern risk and exposure management platforms, it's important to understand the factors that led to the evolution of vulnerability management into broader and more advanced exposure management platforms. Understanding these gives you the lens through which to judge what "modern" really means in 2025.

1. Noise and Alert Fatigue: From Detection Overload to Decision Overload

Most traditional vulnerability tools still behave like finding lists, not risk reducers. They provide good insights on the vulnerabilities discovered, maybe even provide context on exploit based on KEV or EPSS feeds but less details in terms of active risk pertaining to that specific customer's environment. The result is alert fatigue, missed SLAs, and growing backlogs that neither reflect true risk nor move remediation forward in a measurable way.

2. Shallow Prioritization and Context Gaps: Fixing What's Visible, Missing What's Critical

In legacy vulnerability platforms, risk ranking often leans on external signals (CVSS scores, EPSS, KEV) without factoring in internal context like network exposure, identity privileges, runtime state, or asset criticality. This drives mis-prioritization, where teams spend cycles fixing non-exploitable issues while missing real attack paths. Not having exploitability or reachability analysis leaves security teams with a long list of vulnerability issues with misaligned priorities.

3. Activity Over Outcomes: Doing More, Achieving Less

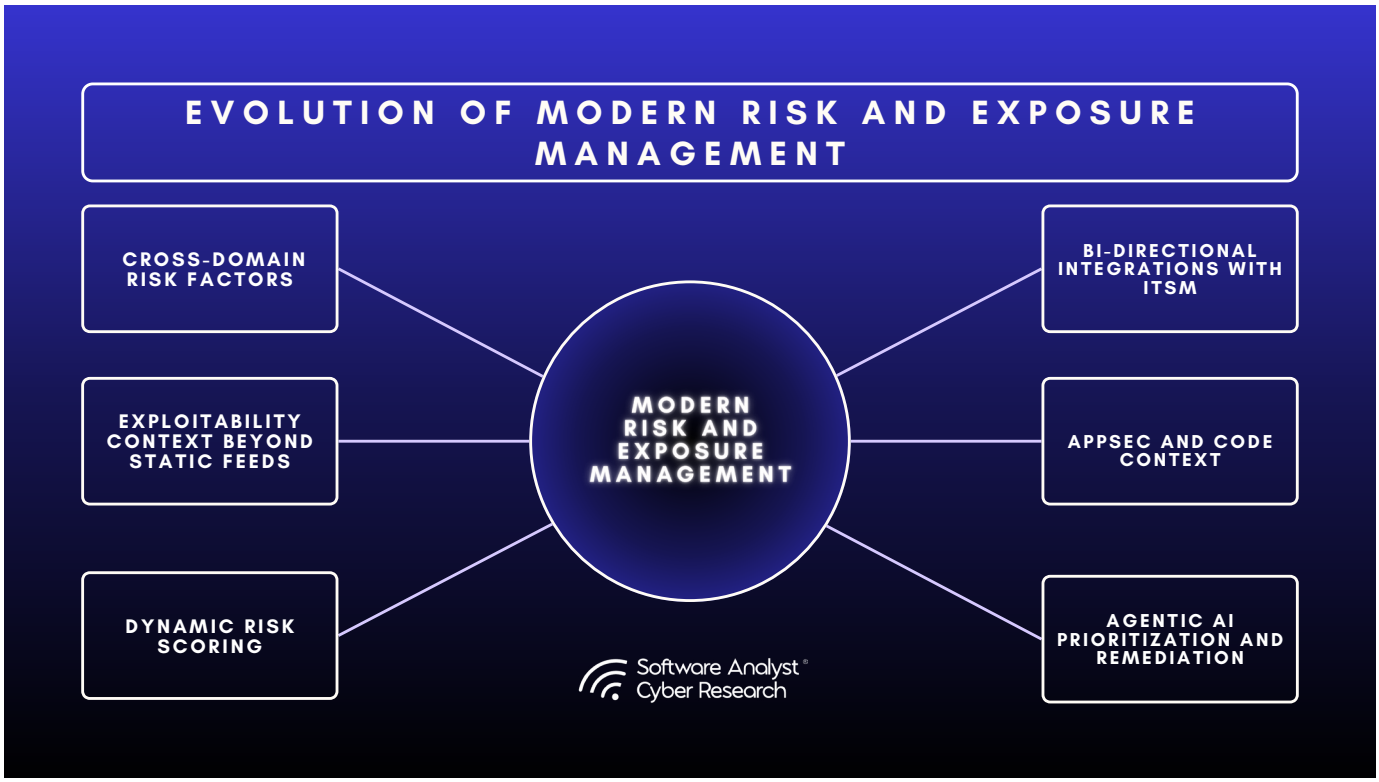
Dashboards that highlight the number of CVEs fixed rather than actual risk reduction create a false sense of progress. Activity metrics are not risk metrics. Without environment-aware prioritization, workflows optimize for throughput instead of impact, widening the gap between security teams focused on reducing exposure and engineering teams measured on delivery, not ticket counts.

4. Data Integrity and Trust Challenges: Proving More, Fixing Less

Conflicting feeds, backports, and false positives can waste time that should be spent accurately remediating risks. Discovering more vulnerabilities is no longer an automatic proof of a better scanner, as false positives often consume more practitioner time to resolve than addressing actual risk. Practitioners want platforms that reduce false positives and duplicates to improve trust and the accuracy of risk assessment.

Introducing Modern Risk and Exposure Management Platforms

There are several key ways we see vulnerability risk and exposure management being redefined in 2025, driven by practitioner concerns, pro-active security modeling, fast-paced threat landscape and introduction of AI from hype to utility. Modern risk exposure management platforms transform past approaches to defining exposure with exploit context derived beyond static configuration reads, true network reachability analysis via simulations, probability of exploit beyond static feeds like EPSS and KEV, social intelligence derived from internet chatter, bi-directional integrations with ticketing platforms to reduce stale risk states and AI-assisted prioritization and remediation. They unify asset intelligence, threat context, business data, and automation to measure, explain, and act on real risk. Here are some new trends related to how vendors are approaching vulnerability risk and exposure management in 2025 -



Control Optimization to Contextual Exposure Modeling

Modern platforms incorporate runtime verification, network reachability, exploit intelligence, presence of compensating controls and business context to measure true exploitability rather than just relying on exposure presence via asset configuration.

Unstructured Data Sources

We are also seeing an emergence of analyzing unstructured data sources to gain additional context about the business criticality of an asset based on information from sources such as ITSM and ticketing systems, collaboration platforms like slack, knowledge repositories and dev tools.

Exploitability Beyond Feeds

Some modern platforms are looking beyond exploitability databases like KEV and EPSS, using social, community, and open-source chatter to detect exploit trends early, feeding those signals into exploitability scoring and contextual risk models

Focus on Remediation

Modern platforms are turning AI from hype to utility by using AI agents for decision automation to perform correlation, ownership resolution, and remediation orchestration. There is still some hesitancy on how much AI should be involved in this process, however clients of these vendors have shared positive feedback.

AppSec and Code Context

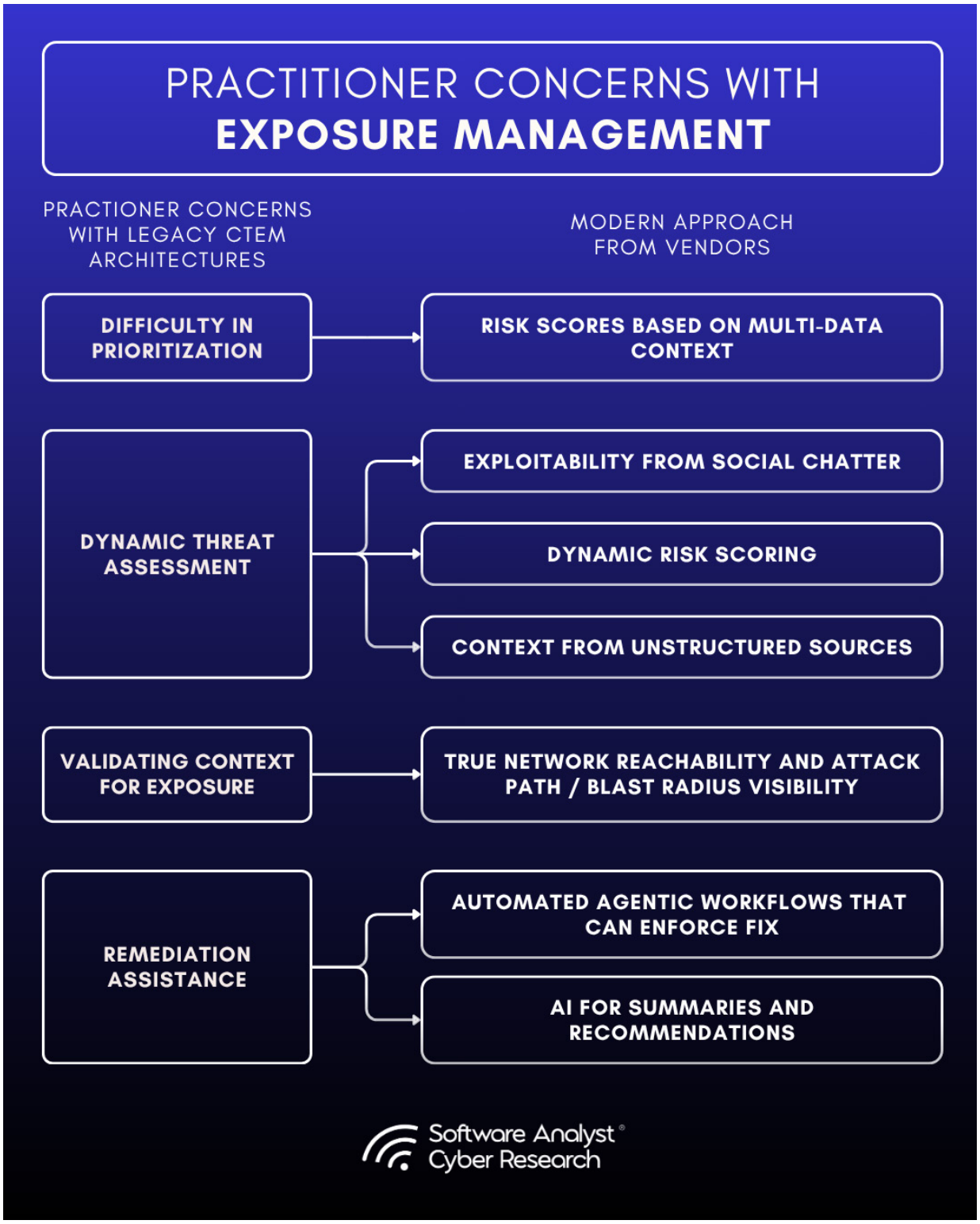
Modern platforms are shifting from infrastructure-centric vulnerability scanning to **u**nified exposure management that connects code, cloud, and runtime layers in a single risk model. By integrating application-security signals from SAST, DAST, SCA, and code repositories with contextual and runtime data, they link vulnerabilities in production back to their source. This convergence is turning exposure management into a **code-to-cloud discipline**, aligning exploitability insights, developer ownership, and remediation workflows within one continuous loop for proactive security.

Process Graphs

Attack paths are becoming common, but we are seeing a rising trend of visualizing business process graphs combined with exposure context.

Key Trends in Risk and Exposure Management in 2025

We interviewed practitioners and asked them about their priorities in this evolving vulnerability management scope and what pain points they would really like to see addressed. We then mapped these against the practical ways vendors are solving these concerns to give you insights on the key trends on Risk and Exposure Management platforms.



Risk vs Coverage

In 2025, the bottleneck isn't whether you can scan everything. Most orgs already run multiple scanners. The result is fragmented visibility and higher operational overhead. The real challenge is unifying visibility and prioritizing true risk across fragmented environments. In short, risk priority is now a popular pain point over raw coverage.

Leaders emphasized the need for **comprehensive visibility with contextualized risk priorities across all assets** in increasingly dynamic environments. Practitioners consistently voiced the need for a **single, unified coverage model** that can give them visibility with an easy onboarding experience.

How vendors are addressing this -

- Unified Visibility: Providing comprehensive coverage across all asset types including containers, code repositories, virtual machines, and cloud workloads in dynamic environments.
- Broad Data Ingestion: Aggregating insights from multiple feeds such as threat intelligence feeds, exploitability databases, and third-party scanners for a consolidated risk view.
- Beyond CVEs: Expanding scope to include insights on asset posture, coverage gaps, cloud security posture, identity exposure, data, business context and network context to create a complete picture of organizational risk.

Dynamic Threat Assessment

Crowdstrike's global threat report 2025 reports the fastest **eCrime breakout at 51 seconds**, with average lateral movement occurring in under an hour. 79% of detections were malware-free, emphasizing identity and living-off-the-land tradecraft. Mandiant's *M-Trends 2025* report shows **global median dwell time rose to 11 days.** Add to this the rise in third-party and supply-chain exposure, plus the scale of GenAI-driven attacks, and the picture is clear: exposures have never been faster to exploit or broader in impact.

Defenders need platforms that can keep pace. That means staying current with the latest threats and delivering immediate context when a new vulnerability emerges. Security leaders want fast, clear answers to the question: *"Am I impacted by this zero-day, and how high are the chances of its exploit in my environment?"* Addressing that requires tools that combine discovery with business context and exposure validation so teams can focus on what matters most - fixing.

As one security leader said, "Don't just show me what's wrong, show me what I need to prioritize right now with the limited resources I have and show my team how to fix it".

How vendors are addressing this -

- **Context-driven exploitability analysis:** Increasing validation of exploitability based on attack paths, blast radius and other impact driven factors.
- **AI-assisted or agentic remediation workflows:** Findings are automatically converted into tickets with full context and step-by-step guidance, routed to the correct asset owners via bi-directional integrations with ServiceNow or Jira to maintain true risk states.

Context for Exposure

If all we ever looked at was the severity rating that comes bundled with a vulnerability feed, every organization would end up with the same flat priority list. But reality does not work that way. Risk is not one size fits all; it is shaped by whether an asset is exposed to the internet, whether it is reachable, and how that environment is actually configured.

That is why a blanket score does not cut it. Two companies could have the same critical vulnerability, but for one it is buried behind layered defenses, while for the other it is sitting on a wide open asset in production. The stakes and the urgency are entirely different.

Security leaders do not just want to know what is theoretically severe; they want to know what is practically severe for **their** environment. Context, exposure, reachability, and attack surface are the layers that make vulnerability prioritization meaningful. Without them, security teams struggle to understand what truly demands urgent action in their environment.

Security leaders want dashboards that reflect context. Board metrics must show risk reduction, not just CVE counts. The priority is reducing exposure and protecting critical assets by ranking issues with reachability, exploit intel, control posture, coverage gaps and business impact.

How vendors are addressing this -

- **Reachability Context:** Evaluating internet-facing assets, their network reachability, lateral movement paths, and overall attack path / blast radius.
- **Business Criticality:** Prioritizing based on data sensitivity (PII) and business context such as production environment impact.
- **Compensating Controls:** Factoring in network segmentation, EDR coverage, WAF protections, or IAM policy conditions to refine true exposure.
- **Exploit Intelligence:** Integrating live threat data from CISA KEV, EPSS, and exploit feeds to identify active exploitation and probable attack vectors.
- **Layered Prioritization:** Combining reachability, exploit intelligence, and attack path context to establish a more accurate, risk-based remediation order.

Remediation Assistance

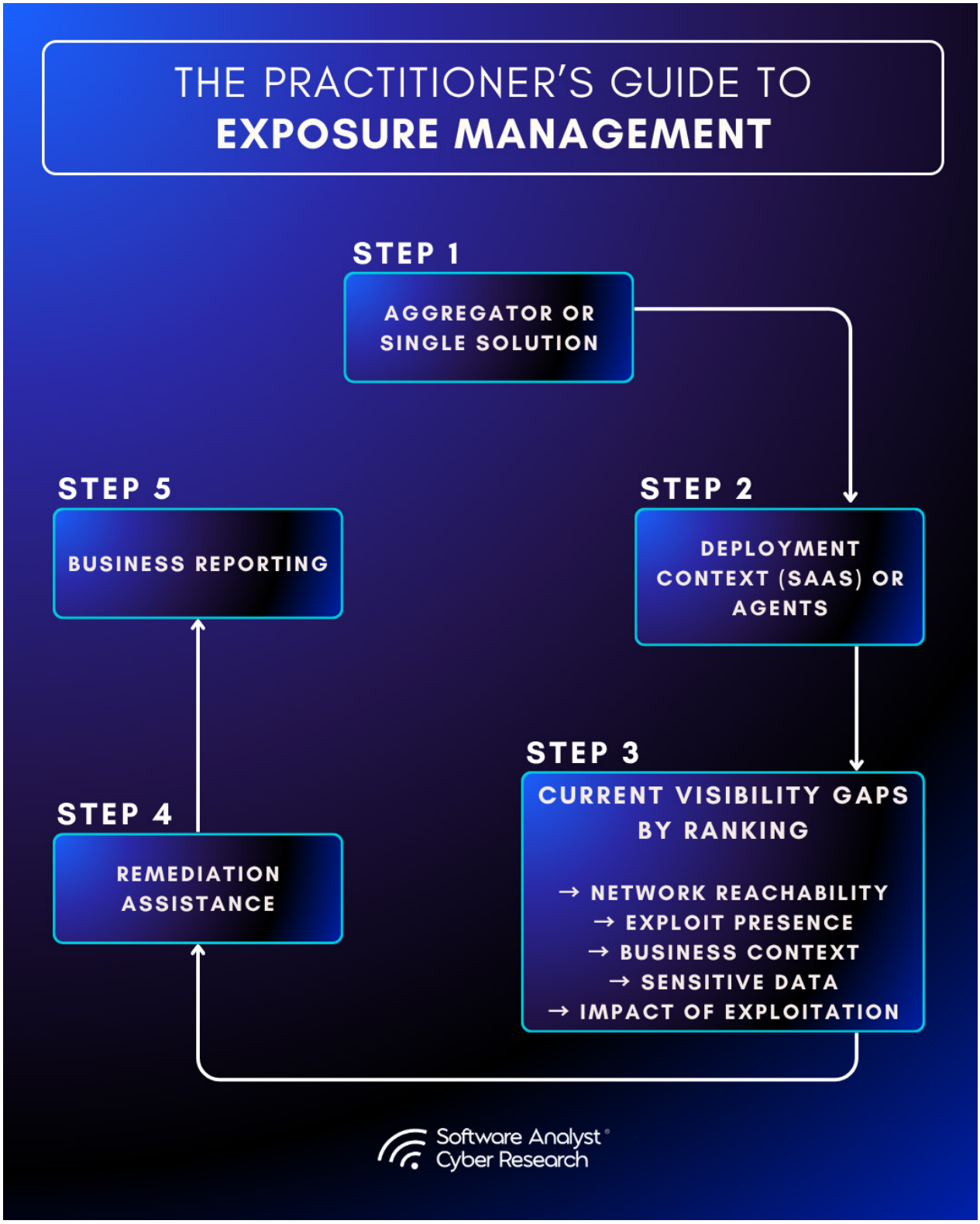
In our interviews, leaders consistently said discovery is easy; fixing is the bottleneck. Platforms that help prioritize what to remediate next and integrate directly into workflows (e.g., ServiceNow, Jira) are seen as genuinely helpful. Dedicated FTEs (Full Time Employees) for operating security platforms is a norm that is breaking in the world of AI capabilities reducing the operational overhead. Practitioners want platforms that can enhance the operator's experience and reduce the overhead on their teams.

How vendors are addressing this -

- **"Ops-Ready" Recommendations:** Clear, technically precise steps written for operations teams, bridging communication gaps between security and development teams.
- **Smart workflow automation:** Auto-assign tickets, bi-directional integrations with ticketing platforms to assess true risk state and track progress, was valued higher than just visualization.

Practitioner's Guide to the Right Solution

Step by Step Framework to Identify which solution fits best for your organization's use cases



Step 1: Unification or Single Solution

The first step is determining whether your organization requires an aggregator or a single-platform coverage model.

Aggregator platforms consolidate findings from multiple scanners, cloud tools, and vulnerability systems into one unified remediation pipeline. These are ideal if you have a mature tool stack but struggle with normalization, deduplication, and operational orchestration.

Unified exposure platforms provide native scanning or posture assessment along with correlation and remediation workflows. These are typically preferred when consolidation and simplified deployment are higher priorities than maintaining multiple overlapping tools.

Step 2: Deployment Context

Check whether the solution fits the deployment model that is preferable in your organization.

Regulated or Sovereign Data Requirements: If operating in sectors such as finance, healthcare, or critical infrastructure, confirm that vendors can support on-premises or air-gapped deployment. Some modern platforms remain SaaS-only, which may not align with strict residency mandates.

Agentless vs. Agent-Based Collection: Evaluate whether you can deploy agents across workloads, endpoints, or cloud assets. Many platforms now use read-only APIs or network sensors to achieve visibility without agents.

Integration Overhead: Platforms with prebuilt connectors for scanners, ITSM, EDR, and cloud providers reduce time-to-value significantly.

Step 3: Map Current Visibility Gaps by Priority

Before evaluating features, document where your current exposure visibility is weakest.

Establish a top-down priority list across the following five visibility domains:

Area: Network Reachability Assessment

Guiding Question: Can you easily determine which vulnerabilities are externally reachable or exposed through internal routing?

(Look at vendors that excel in true network reachability via active simulation or other techniques)

Area: Exploit Presence

Guiding Question: Do you have real-time insights into exploitability factors?

(Look at vendors that go beyond EPSS and KEV feeds to determine probability of exploit)

Area: Business Context

Guiding Question: Can you easily connect technical assets to business criticality, owners, and sensitivity levels?

(Look at vendors that excel in deriving context, sometimes even looking at unstructured data sources or dev tools)

Area: Sensitive Data Visibility

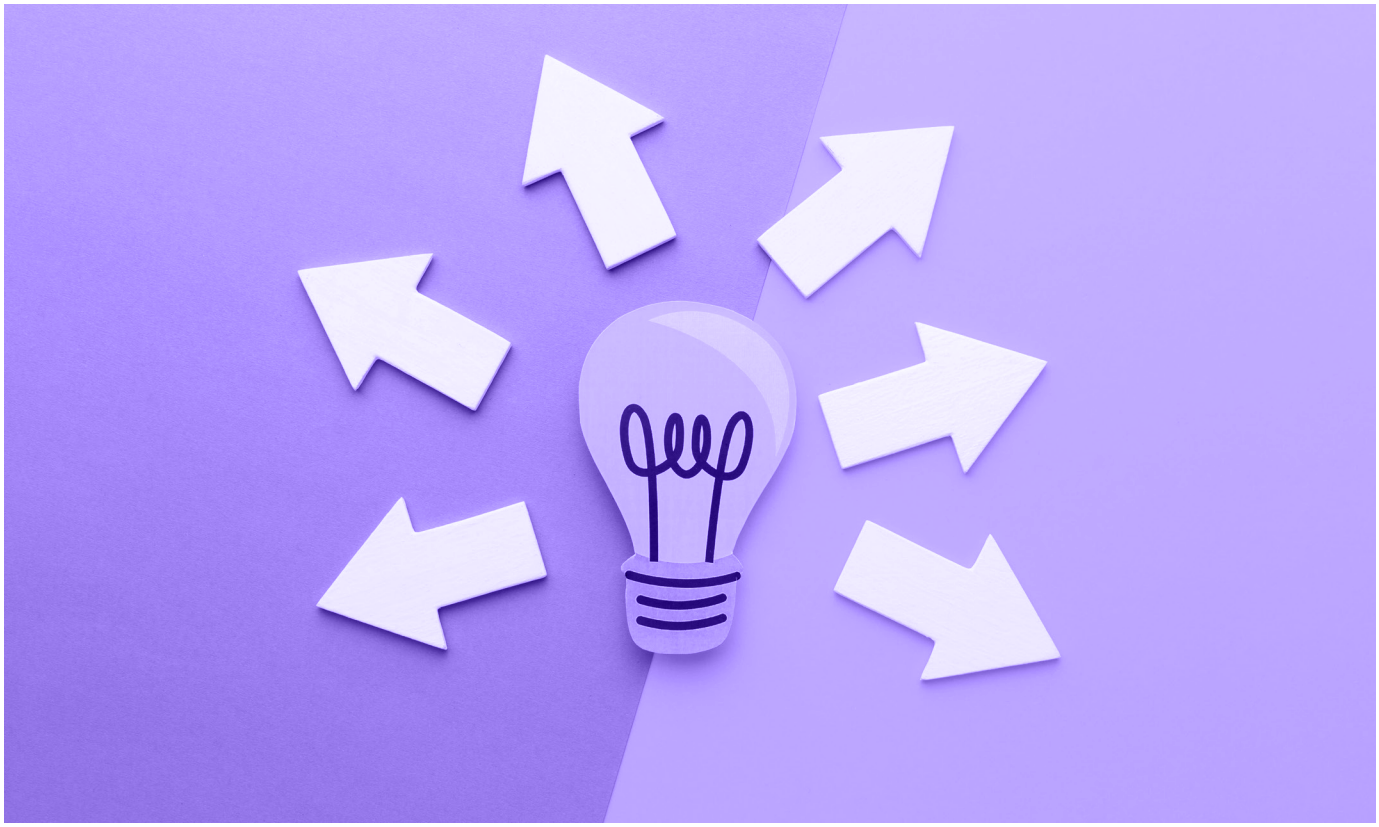
Guiding Question: Are you able to easily identify assets with critical / sensitive data in it?

(Look at vendors that can provide in-depth data scanning (DSPM) capabilities beyond config reads)

Guiding Question: Impact of Exploitation

Can you easily visualize how one compromise could traverse identities, network, and data?

(Look at vendors with exploit paths and blast radius visibility)



Step 4: Evaluate Remediation Assistance

After prioritization, there is still the need for remediation which is your responsibility. It's important to learn what assistance these platforms can provide in remediation operations.

Modern solutions now offer Remediation Operations (RemOps) or workflow automation that connect security and IT directly.

- **Automated Ticketing:** Platforms generate and route contextualized remediation tickets directly into Jira or ServiceNow with ownership and SLA metadata.
- **Task Consolidation:** Multiple CVEs or misconfigurations are merged into a single "fix item," reducing duplicate effort.
- **Verification Loop:** Closed tickets are automatically revalidated via telemetry syncs to ensure exposures are truly resolved.

Step 5: Business Reporting

This may not be an important factor for you if you create customized dashboards outside of the security tooling you use. However, if you do need this visibility from within the platform then you should consider these factors :

- **Custom Reporting and Dashboards:** Look for platforms that allow dynamic filtering by context such as environment, business unit, or SLA.
- **Residual Risk Metrics:** Ability to quantify how compensating controls reduce risk even before patch deployment.
- **Natural Language Summaries:** Some platforms generate narrative summaries or executive-ready visuals automatically, aligning technical exposure with business impact.

Vendor Assessment Framework

Vision (Not a weighing factor)

What is the vision of the company for future readiness? What areas do they see their platform evolving?

Vendors

To understand key innovations pertaining to vulnerability risk and exposure management platforms in 2025, we did a deep dive into 10 vendors through in-depth product briefings, customer interviews and in-depth questionnaires, beyond marketing materials. We focused on core differentiators, and the approach they're taking in addressing risk prioritization and exposure visibility concerns.

TOP VENDORS ANALYZED

ZAFRAN
XM Cyber
cogent
Tonic
nagomi
Axonius
seemplicity
Astelia
orca SECURITY


Tonic

Tonic Security

Tonic Security is a cybersecurity startup that recently emerged from stealth. Tonic focuses on reducing exposure by combining asset discovery, organizational context, threat intelligence, business impact assessment, and adversarial validation to prioritize remediation efforts.

Tonic's approach to exposure management centers on an AI Data Fabric and a security knowledge graph that ingest structured and unstructured data, add business context, and cut false positives so teams can focus on issues that materially impact the organization.

Key capabilities include large-scale data collection and harmonization, contextualization of findings with business impact, business process graphs and agentic workflows that accelerate mobilization from finding to fix. The platform aims to reduce tool pivots, provide a business-led view of posture, and slash remediation time across vulnerability and exposure workflows.

Mapping Tonic Security's capabilities against our analysis framework

Voice of the Customer

A customer of Tonic sent us their reasoning for choosing Tonic security for their exposure management program. His opinions below -

Life before Tonic

Before adopting Tonic, customer's risk and exposure management program faced several key limitations and critical gaps:

Lack of Business Contextual Intelligence, siloed data: Critical business and operational data were scattered across systems like Jira, Confluence, Office365 emails/Teams, and GLPI, limiting visibility and slowing down decision-making. Manual Processes, Limited Business Alignment: Security tools lacked the ability to map technical findings to business impact, making it hard to prioritize based on risk to key processes. Compliance Blind Spots and Fragmented Data Sources

"Asset intelligence was slow and fragmented. Enriching assets with actionable context took hours or days and happened frequently, making triage and prioritization inefficient.. Much of the vulnerability management relied on manual collection and correlation, which increased response times and reduced agility... Security tools lacked the ability to map technical findings to business impact, making it hard to prioritize based on risk to key processes. Risk data was scattered across multiple systems, making it difficult to get a unified view of exposure."

Why Tonic

"AI-Powered Business Contextualization: Its data fabric automatically analytics extracts and harmonizes context across business, organizational, and operational dimensions, enabling faster and more accurate triage

- **Efficiency and Focus:** Our team moved into "beast mode," achieving more with existing tools, reducing false positives, and gaining control over information silos
- **Automated Insights:** AI-driven analytics that surface hidden risks and provide actionable recommendations without manual intervention.
- **Unified Risk Intelligence:** A centralized platform that aggregates and normalizes data across silos, giving us a real-time, holistic view of risk exposure.
- **Trustworthy Reasoning:** Tonic's transparent and explainable logic gave you confidence in its outputs, allowing for decisive action without second-guessing

- **Accelerated Remediation:** Mean Time to Respond (MTTR) dropped significantly, and ownership of assets became clearer, improving accountability and reducing exposure windows"

What they would like to see more

"Deeper Integration with On-Prem Systems: Expand and streamline integration with Jira, Confluence, and other legacy systems to ensure full context extraction across hybrid environments. In addition, adding seamless ingestion of vendor and supply chain risk data to expand exposure visibility beyond internal systems

Enhanced Visualization of Business Blast Radius: Improve the UI/UX for mapping asset impact on business processes - make it more intuitive and actionable for both technical and non-technical stakeholders with customizable dashboards and Predictive Risk Alerts

Continuous Feedback Loop for Context Accuracy: Introduce mechanisms for users to validate and refine the context Tonic generates, ensuring it evolves with organizational changes and remains aligned with business priorities"

Deployment

Tonic supports flexible deployment options, including SaaS, on-premises, and fully self-hosted air-gapped deployments, particularly suited for regulated sectors such as financial services. Their default preference is SaaS deployment.

Data Collection and Correlation

Tonic aggregates and deduplicates data from a wide range of sources, including ITSM systems, CMDBs, EDR/XDR tools, IDPs, virtualization, and backup platforms. Beyond standard integrations with existing vulnerability scanners, Tonic also natively scans, ingests, indexes, and analyzes unstructured data sources, such as institutional wikis, collaboration tools, and messaging systems, to discover assets and extract business/organizational context (e.g., asset criticality). This enables discovery of assets beyond regular methods, with automatic contextualization.

- Data sources and collection:
  - Vulnerability scanners (e.g., Tenable, Qualys, Rapid7), ITSM and ticketing systems (e.g., ServiceNow, Jira), EDR/XDR tools (e.g., CrowdStrike, SentinelOne), Identity providers and CMDB platforms, Collaboration and knowledge management systems (e.g., Confluence, Slack, Microsoft Teams, Google Workspace), Virtualization and backup solutions.

Prioritization and Risk Factors

Tonic Security moves beyond CVSS scoring by taking into account -

- **Business Context:** Unlike traditional methods of deriving business context, such as from asset labels and asset config, Tonic derives context automatically from unstructured data sources and messaging platforms by considering additional factors like:
  - Asset criticality.
  - Business processes enabled by assets (hosts, applications).
  - Number of high privileged users logged in.
  - Sensitive data that may reside on the asset.
- **Ownership Context:** Ownership at the individual, team and departmental levels, structural dependencies, and hierarchy alignment.
- **Operational Context:** Asset function, patch status, system dependencies, and business process posture maturity (a unique differentiator).
- **Temporal Context:** Recency of detection, exploitation timelines, change frequency, patch cadence, as well as asset lifecycle and history.
- **Network Reachability:** Reachability of assets (e.g., internet exposure derived from asset and network config.)
- **External Feeds:** Exploitability of findings (e.g., KEV, EPSS and other databases), threat intelligence insights, and resilience of assets/control gaps (e.g., lacking recent backup or missing EDR agents).

Tonic consolidates all ingested data into contextualized views: business, organizational, geographical, operational, temporal, and adversarial, forming its "Six Degrees of Context" framework. A key differentiator is its ability to automatically extract business, operational, and organizational context from unstructured sources such as ITSM tickets, Notion, Slack, Confluence, and email, without needing manual input. This allows automated inference of asset criticality, role, and interdependencies across the application ecosystem, enabling dynamic and accurate prioritization.

Exploitability Assessment

- **Core Differentiator:** Tonic integrates with ITSM, EDR and other security systems for asset discovery, and extends visibility into institutional knowledge bases and collaboration tools to uncover shadow assets and exposures. Its integrations with internal knowledge bases and collaboration tools help surface assets and dependencies that exist outside conventional inventories. For example, Tonic can identify assets referenced in IT tickets or business continuity plans that are missed by conventional scanners.

Another differentiator is Tonic's business dashboard which provides a high-level, process-centric view of risk, helping CISOs and GRC teams understand how business operations map to security exposure.

- **Explainability:** The platform includes a confidence algorithm that validates the reliability of attributed context within its knowledge graph. It evaluates data volume, recency, source credibility, coherence, coverage, and user feedback to generate a transparency score. This provides visibility into how trustworthy contextual information is. It also validates the reachability of assets and simulates potential business impact through blast radius visualization.

Tonic allows organizations to define data source precedence (for example, ServiceNow as the system of record) to reconcile conflicting data inputs. A human feedback loop enhances recommendation mechanism, allowing users to validate or challenge attributions, enabling the model to improve reliability and accuracy over time.

Remediation and True Risk State

- Enables end-to-end remediation workflows by identifying responsible owners, initiating tickets, tracking fixes, and managing exceptions through compensating controls or risk acceptance processes.
- Uses agentic automation to help security teams understand remediation progress and the impact of changes.
- Integrates with ticketing and workflow systems such as Jira and ServiceNow to support automatic task assignment, ticket creation, exception handling, and remediation tracking.
- Employs domain-specific agentic AI to enrich downstream systems like CMDBs and SIEMs, keeping contextual data consistent as exposures evolve.
- Maintains an accurate view of asset risk by verifying remediation outcomes through integrations with scanning and patching tools, and identifying root causes when discrepancies occur.

Vision

Tonic's vision centers on making context the core principle of exposure management. By helping security teams determine what truly matters and why, and by mapping risk to business processes, the platform aims to reduce data noise, improve cross-functional communication, and streamline decision-making.

Analyst Take

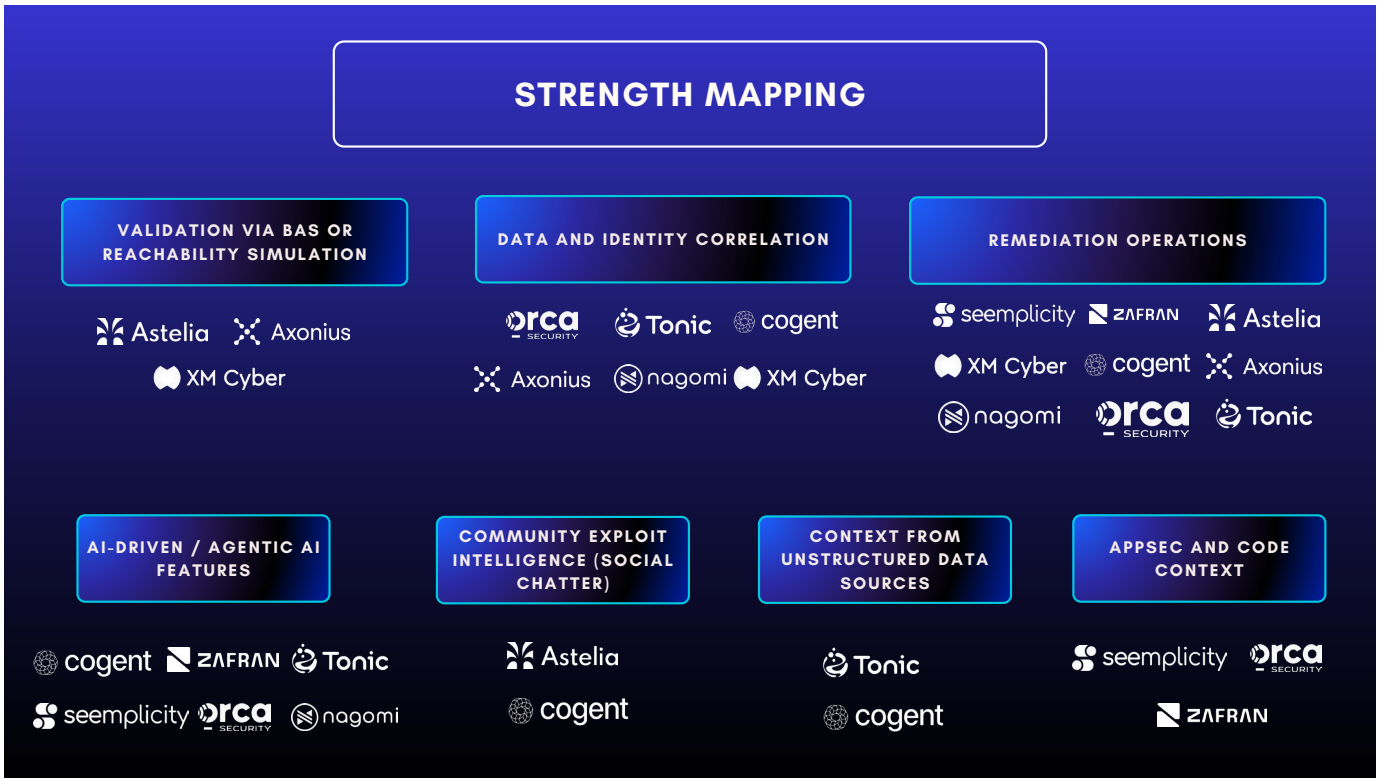
There are the strengths and areas to watch in our opinion

Strengths

- **Automatic business context from unstructured data:** Tonic extracts and normalizes context from tickets, wikis, Slack/ Teams, email, and docs to auto-populate business, operational, and organizational context for each asset, uncover shadow assets, and classify crown jewels without manual input.
- **Confidence scoring with transparent evidence and human feedback:** A confidence algorithm scores each attribution using data volume, recency, source quality, coherence, and coverage, while users can upvote or downvote and suggest corrections to continuously improve accuracy.
- **Flexible Deployment Options:** SaaS, on-prem, and airgapped
- **Process Graphs:** Mapping exposure to process graphs
- **Automation & Remediation Workflow:** Domain specific agentic AI provides strong automation capability to drive down MTTR but also keep other relevant systems and teams up to date as exposure changes.

Areas to Watch

- **Lack of Validation Phase Capability:** Full attack path analysis is described as upcoming, so current depth of validation may be insufficient for teams seeking proof of exploit paths.
- **Reliance on installed tools and data within:** Value is driven by ingesting many third-party sources and unstructured content. Gaps, conflicting feeds, or weak data hygiene can reduce accuracy.



Vulnerability Risk and Exposure Management - SACR Prediction

Looking ahead we see the evolution of vulnerability and risk management platforms in two directions

Aggregators expanding in-house scanning

Aggregator-style platforms or unified vulnerability management platforms, which today focus on normalizing and correlating data from third-party scanners, CNAPPs, and posture tools will increasingly introduce in-house scanning capabilities. This trend addresses the needs of organizations that either:

- Lack an existing vulnerability management stack, or
- Want a single-source-of-truth without relying on external data dependencies.

Expect vendors that have historically positioned themselves as “aggregator and unified VM layers” to develop lightweight agentless scanning modules for basic asset discovery and vulnerability enumeration. These capabilities will complement their correlation and remediation engines, giving them dual value as both aggregator and source of vulnerability intelligence.

Pure-Play Platforms moving up the stack

Meanwhile, pure-play vulnerability and exposure platforms that already provide native scanning and posture management will continue expanding upward into contextual analytics and remediation orchestration. They will evolve from point scanners into autonomous exposure management suites capable of:

- Correlating vulnerability, identity, data posture and network context;
- Going deeper on runtime exploitability to challenge the aggregators; and
- Investing heavily in agentic AI for automating remediation workflows

This evolution will be driven by customer demand for outcome-based risk reduction metrics, not volume-based vulnerability counts.

Conclusion

Vulnerability management and the need for reducing alert fatigue by prioritizing true risk continues to be a core requirement for organizations. The traditional KPIs of CVSS scores and vulnerability counts no longer represent success; instead, measurable risk reduction, exploitability validation, and remediation velocity define modern maturity.

The convergence of historically distinct categories VM, RBVM, ASM, CAASM, ASPM, CNAPP, and BAS, with an evolution beyond CTEM capabilities - under the modern risk and exposure management umbrella reflects how practitioners and threat actors now operate. The evolution described in this report signals that exposure management is becoming the connective tissue between asset intelligence, control validation, and remediation operations.

Software Analyst®
Cyber Research

business

personal

softwareanalyst.io

SACR®

Trusted research. Sharp insights. Real conversation.

CISO	VENDOR
SECURITY TEAMS	INVESTORS