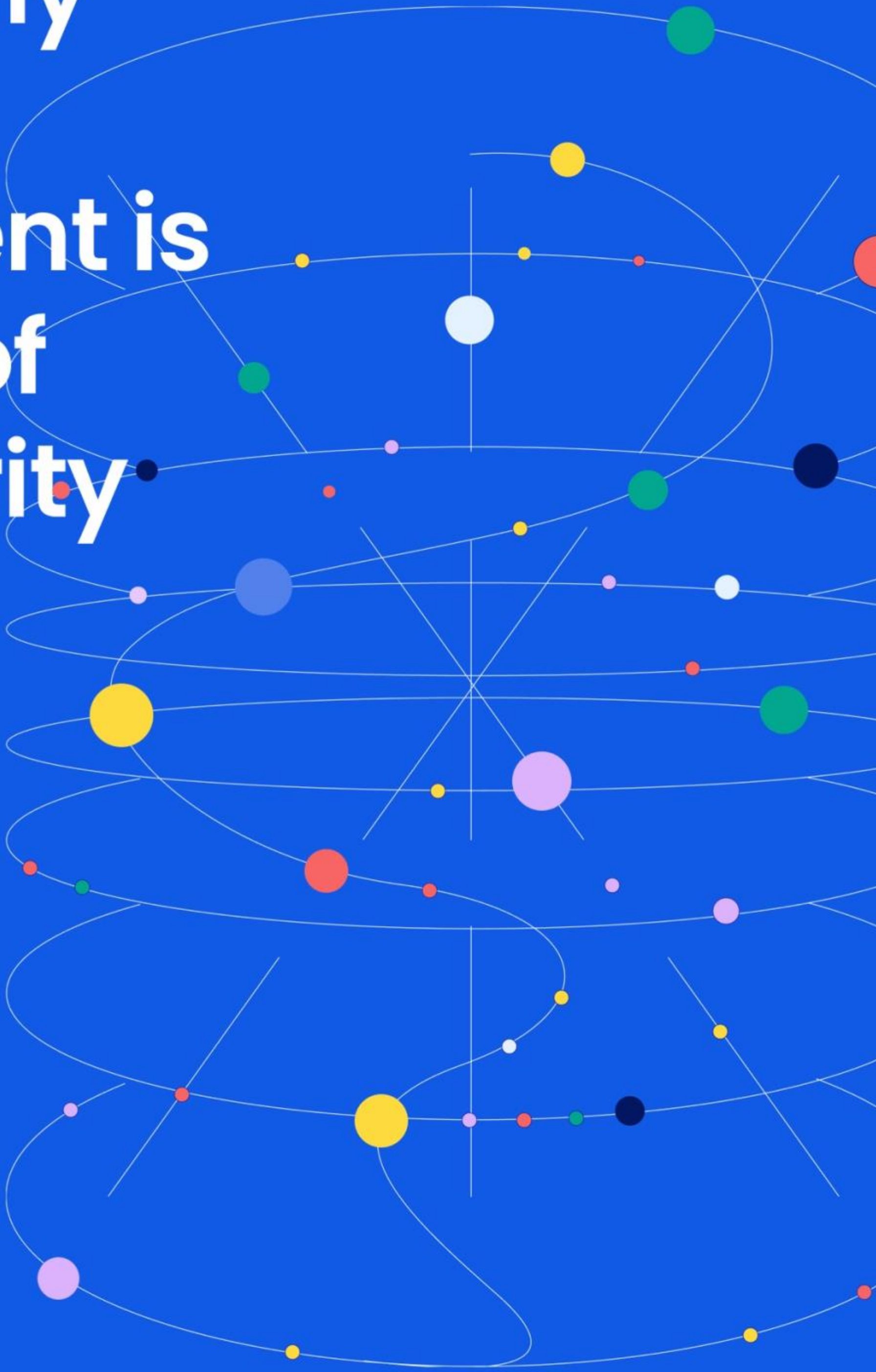
From Chaos to Context: Why Exposure Management is the Future of Cybersecurity

TONIC BROCHURE



Tonic

www.tonicsecurity.com

The Limits of Traditional Vulnerability Management

Security leaders are no strangers to vulnerability management. For over two decades, VM has been the frontline mechanism for discovering and fixing potential weaknesses in IT systems. Yet, despite advancements in scanning tools and vulnerability databases, breaches continue to rise. Why? Because the attack surface has exploded beyond what traditional VM can handle.

With the rise of cloud-native architectures, hybrid workforces, SaaS sprawl, and ephemeral infrastructure, organizations now operate in environments that change daily, sometimes hourly. Traditional VM was designed for static environments where monthly or quarterly scanning cycles were enough. That model is obsolete.

Further complicating matters is the overwhelming number of vulnerabilities discovered each year - over 40,000 reported in 2024 alone! But not all vulnerabilities pose equal risk. Most are never exploited. The problem isn't identifying vulnerabilities; it's identifying which ones matter and responding in time. This is where vulnerability management breaks down: it generates too much noise, lacks contextual awareness, and struggles to prioritize in line with business risk.

Why Exposure Management Is a Necessary Evolution

Gartner predicts that by 2026, organizations that prioritize their security investments based on a Continuous Threat Exposure Management (CTEM) program will be three times less likely to experience a breach. It further predicts that by 2028, organizations enriching SOC data with exposure information will halve the frequency and impact of cyberattacks.

Exposure management is not just a rebranding exercise. It represents a necessary and strategic evolution of cybersecurity operations. Rather than focusing solely on identifying software flaws, exposure management broadens scope to cover new areas of the attack surface, encompasses disparate types of findings, and continuously enriches them with multi-dimensional context. It looks at how those flaws intersect with assets, business processes, threat intelligence, and real-world attacker behavior.

Exposure management asks a different set of questions: Which assets are exposed right now? Are they business critical? Is there an exploit available? Are we seeing activity related to this vulnerability in the wild? Do compensating controls exist? These are the questions that define actual cyber risk.

This broader, contextual approach requires a shift in tools, processes, and mindset. It also demands better collaboration across the organization. Exposure management is a team sport. Security, infrastructure, DevOps, and business stakeholders must work together to reduce meaningful risk, not just fix issues that scanners surface.

Exposure Management solutions:

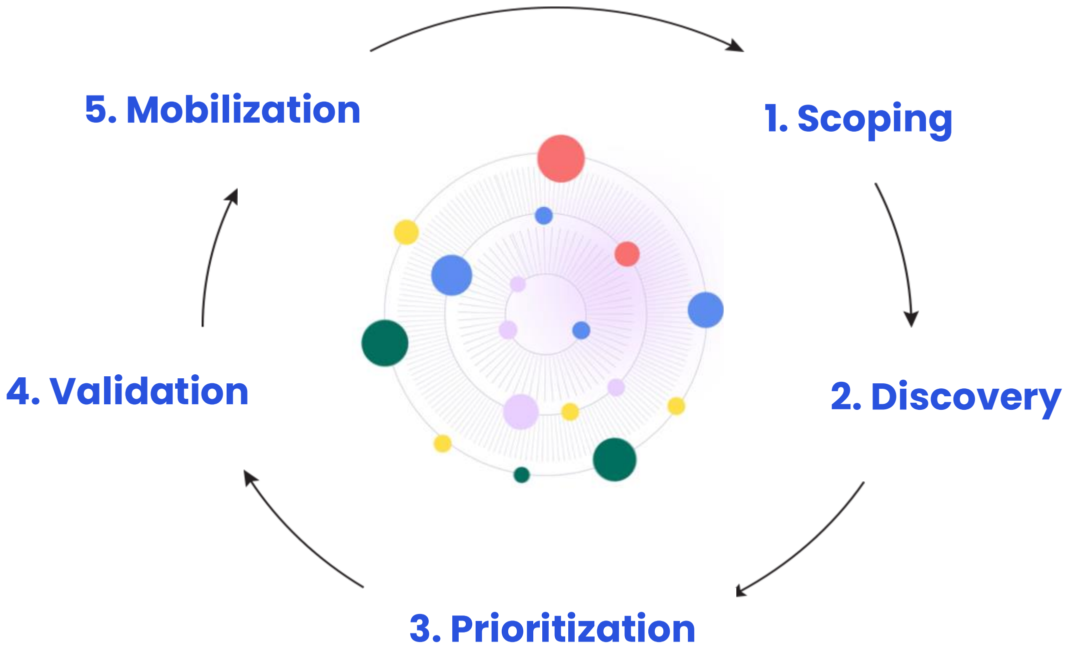
- Natively deliver or integrate with discovery capabilities that enumerate exposures.
- Continuously identify and prioritize exposures across a broad range of asset classes.
- Provide a comprehensive and centralized approach to identifying, assessing, prioritizing, and remediating exposures.
- Streamline workflows, ensures visibility into the security posture, and ensures a consistent, scalable response to vulnerabilities across on-premises, cloud, and hybrid environments.

The following table summarizes the main differences between traditional Vulnerabilitity Management and modern Exposure Management:

Aspect	Exposure Management	Vulnerability Manangement
Scope	Broader focus on all types of exposures (e.g., misconfigurations, security control gaps, unprotected secrets, credentials, etc.)	Narrower focus on software vulnerabilities (e.g., CVEs).
Approach	Holistic and strategic. Aims to assess the organization's entire attack surface.	Tactical and operational. Focused on patching and mitigating specific software issues.
Assets Covered	Includes applications, network configurations, IoT devices, shadow IT, cloud environments, etc.	Primarily focused on software systems, devices, and applications with known vulnerabilities.
Threat Sources	Looks at both known and unknown exposures that could lead to exploitation.	Targets primarily known vulnerabilities documented in databases like NIST's CVE.
Context	Leverages multi-dimensional, meaningful and actionable context, to inform and direct scoping, triage, prioritization and remediation.	Focuses on the vulnerabilities and treats them based on generic scores (e.g., CVSS).
Tools and Techniques	Involves asset management, attack surface management (ASM), penetration testing, Endpoint Detection and Response (EDR), external risk monitoring, posture management, and risk prioritization.	Utilizes vulnerability scanners.

Implementing Continuous Threat Exposure Management (CTEM)

Gartner's CTEM framework provides a structured methodology for making exposure management operational. At its core, CTEM is about continuously assessing the exposure level of your digital environment, validating real risk, and ensuring timely remediation. It is not a product - it is a program.



CTEM is composed of five phases:

1. **Scoping**: This is the foundation. Organizations must define what they want to protect, what their risk appetite is, and which systems are most critical to operations. Business alignment is essential; without it, prioritization will be misaligned.
2. **Discovery**: You can't protect what you don't know. Discovery must include known and unknown assets, cloud workloads, shadow IT, SaaS applications, APIs, and development infrastructure. Tools like CAASM and EASM help build this inventory.
3. **Prioritization**: This is where exposure management substantially diverges most from traditional VM. It's not just about severity - it's about context. Prioritization includes reachability, threat intelligence, likelihood of exploit, business impact, and resilience, among other factors.
4. **Validation**: This step is important but often skipped. Use attack simulation, red teaming, or purple teaming to validate whether the exposure is exploitable in your specific environment. Validation turns theory into actionable reality.

5. **Mobilization**: Remediation efforts must be tracked, measured, and supported with process ownership. Exceptions must be managed, timelines enforced, and workflows automated. This phase ensures exposures are actually closed and risk is reduced.

The following table summarizes the key characteristics of the five phases of CTEM:

#	Phase	Key Questions	Description	Key Actions
1	**Scoping**	What part of the attack surface should be protected and at what level? Is our strategy improving, or are we losing ground?	Define critical assets and resources that require protection, to ensure alignment with business priorities and risk tolerance.	• Evaluate SLA and metrics. • Address underlying issues. • Assess the proactive security posture. • Adjust scope.
2	**Discovery**	Which assets are affected?	Identify and assess the organization's attack surface, uncovering vulnerabilities, misconfigurations, and other security issues across all assets	• Compile a comprehensive inventory of all IT assets. • Conduct regular exposure assessments to identify potential weaknesses.
3	**Prioritization**	What is the risk to the business?	Determine the risk to the assets, and order the findings based on impact, probability and other factors.	• Contextualize and valuate assets. • Gauge adversarial exposure. • Rate vulnerabilities and assets.
4	**Validation**	Can the exposure be exploited? Has the exposure been effectively resolved?	Confirm the exploitability of identified exposures through controlled simulations of attacker techniques. Verify the effectiveness of the actions by conducting follow-up assessments.	• Model and simulate adversarial tactics. • Rescan and validate.
5	**Mobilization**	Are we addressing the most critical exposures first?	Implement the necessary measures to take action to prevent, detect and respond to existing or potential exposures.	• Remediate/mitigate, transfer, accept, or avoid. • Identify high-impact fixes. • Assign fixers and route tickets. • Manage exceptions and apply compensating controls.

The Role of AI and Automation in Exposure Management

AI is a critical enabler for modern exposure management. Tonic uses AI to correlate telemetry from across your ecosystem, enriching it with external threat intelligence and internal organizational knowledge. This allows for better risk scoring, faster triage, and more intelligent remediation planning.

Our AI agents also support simulation and validation. They can suggest potential attack paths, estimate blast radius, and highlight the most probable routes an attacker might take. Natural language generation tools help translate technical risk into business-friendly summaries, empowering CISOs to communicate effectively with boards and executives.

Ultimately, AI doesn't replace analysts - it augments them. By removing manual, repetitive tasks and adding intelligence to prioritization, AI ensures security teams spend their time where it matters most.

The Strategic Business Value of Exposure Management

CISOs today sit at the intersection of security, operations, and business leadership. They are expected to manage risk, enable growth, ensure compliance, and respond to incidents, while demonstrating ROI. Exposure management helps meet these demands.

It improves focus by ensuring limited resources go to the most important problems. It enhances collaboration by creating a shared language across security and operations. It supports automation by integrating with ITSM, CMDBs, CI/CD pipelines, and cloud-native workflows.

Most importantly, it aligns cybersecurity with business value. By focusing on actual exposures rather than hypothetical/generic vulnerabilities, security teams can assess and communicate risk in a way that resonates with business decision-makers.

How Tonic Makes Exposure Management Real

Tonic is purpose-built for exposure management. Our platform supports the full CTEM lifecycle, and we've worked with companies across industries to help them shift from reactive VM to proactive exposure management. With Tonic, you don't just see risk. You act on it.

At Tonic, we're here to help you navigate that shift. We provide the platform, the insights, and the support to turn exposure management from aspiration to execution.

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**