



DISCOVER WHY CTEM IS A TOP 10 SECURITY TREND

AND WHY CISOs ARE ADOPTING IT

EXECUTIVE SUMMARY

Continuous Threat Exposure Management (CTEM), recognized by Gartner as a top strategic security trend, marks a fundamental shift in cybersecurity, from managing vulnerabilities to continuously reducing real-world exposure.

This whitepaper outlines a more advanced approach to CTEM, one that moves beyond fragmented tools, static severity scoring, and ticket-driven reporting.

Effective CTEM requires:

- Unified, continuous exposure visibility across IT, cloud, SaaS, and hybrid environments
- Exploitability-driven prioritization grounded in threat intelligence, control context, and business impact
- Autonomous reprioritization as attack conditions and asset exposure change
- Control validation and measurable exposure burndown, independent of ticket volume
- Orchestrated remediation workflows that reduce friction between security and IT

The next evolution of CTEM is intelligent, agent-driven execution that continuously reasons about risk and drives measurable reduction in exposure.

The impact is measurable. At Carvana, their shift to autonomous CTEM led to a 40% reduction in breach likelihood that yielded a 200% ROI.

The future of CTEM isn't more dashboards. It's autonomous execution that continuously reduces real exposure.

INTRODUCTION

Gartner has identified Continuous Threat Exposure Management (CTEM) as one of the top 10 technology trends. At the same time, Forrester points towards Proactive Security Platforms as the hail mary rescue for the exposure management noise that drowns for vulnerability management leaders.

CTEM transforms traditional vulnerability management by expanding the scope beyond CVEs to include all sources of threat exposure, such as:

- Misconfigurations
- Open ports
- Weak encryption
- Control gaps

CTEM also introduces risk-based prioritization, shifting focus from volume to business impact, which adds a crucial missing layer to exposure management.

“

The volume of discovered assets and vulnerabilities is not success in and of itself; it's far more valuable to accurately scope based on business risk and potential impact.

Gartner®

Predicts 2023:

Enterprises Must Expand from Threat to Exposure Management

”

WHAT IS CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM)?

CTEM represents a proactive, continuous approach to cybersecurity. Unlike traditional vulnerability management, which relies on periodic scans, CTEM enables:

- Continuous monitoring across IT, cloud, and IoT
- Real-time detection of new exposures
- Dynamic response to an evolving threat landscape

CTEM shifts security teams from reactive remediation to ongoing cyber resilience.



CTEM'S FIVE STEPS TO EXPOSURE MANAGEMENT

- **Scope**
Define and continuously assess your organization's attack surface
- **Discovery**
Establish a discovery process to identify assets, vulnerabilities, misconfigurations, and more.
- **Prioritize**
Focus on the threats most likely to be exploited, not just those with the highest CVSS score.
- **Validate**
Determine whether existing controls and response plans are sufficient to protect the business.
- **Mobilize**
Operationalize findings by aligning people, processes, and technology to remove remediation friction.

ARE YOU READY FOR CTEM?

The Ultimate Checklist

If you answer “yes” to half or more, you’re ready to adopt CTEM.

1. Vulnerability Prioritization

- ☐ Are zero-days consuming disproportionate time and resources?
- ☐ Do you rely solely on CVSS or EPSS?

2. Workflow Efficiency

- ☐ Do IT teams request more remediation context?
- ☐ Are patches identified manually?

3. Reporting & Metrics

- ☐ Is success measured by volume closed rather than risk reduced?
- ☐ Does leadership ask for ROI or business impact?

4. Integration & Automation

- ☐ Do you lack a unified view across IT, cloud, and IoT?
- ☐ Is data fragmented across tools, assets, third parties, and more?

5. Strategic Alignment

- ☐ Is vulnerability management tied to enterprise risk reduction?
- ☐ Is business impact on the roadmap?

6. Stakeholder Communication

- ☐ Can security outcomes be explained to non-technical leaders?
- ☐ Do you want to quantify cyber risk financially?

7. Continuous Improvement

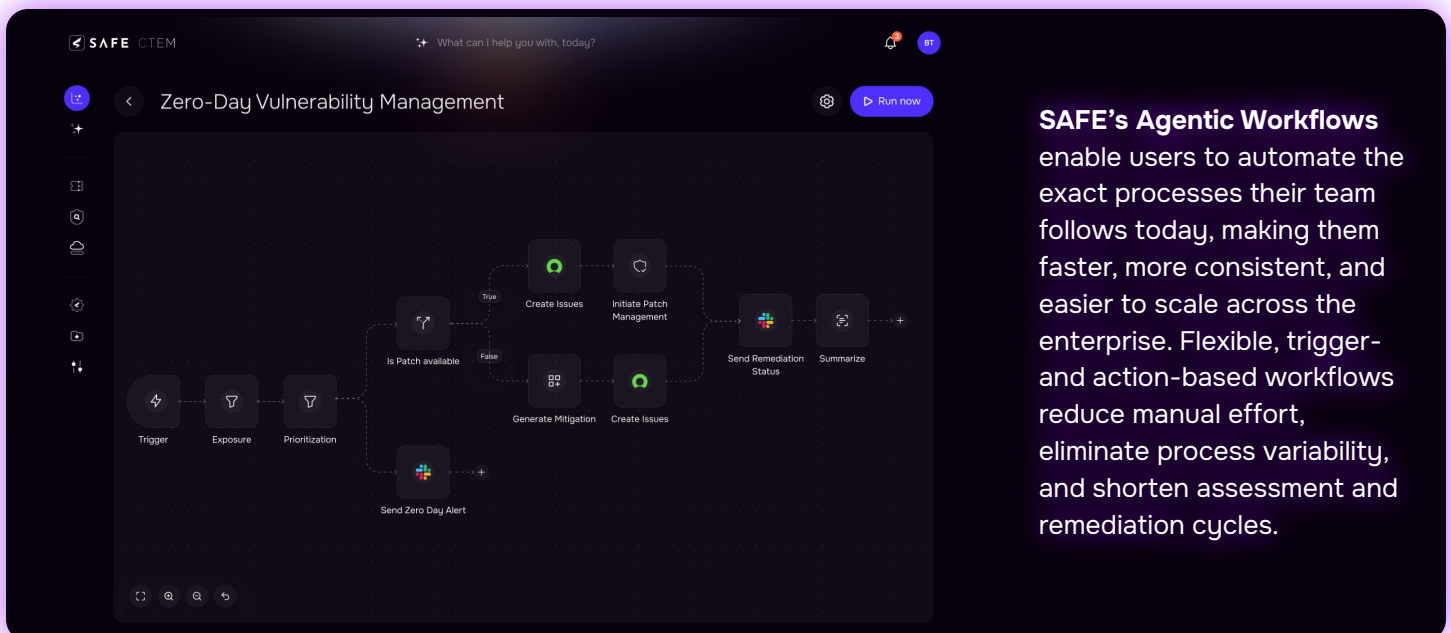
- ☐ Do you want peer benchmarking?
- ☐ Is there executive appetite for continuous security maturity?

How SAFE Helps Enterprises Move From Reactive Exposure Management to Autonomous CTEM

Continuous Threat Exposure Management (CTEM) was designed to move security beyond periodic scanning and toward continuous, risk-driven exposure reduction. Most organizations still rely on manual correlation across fragmented tools, severity-based prioritization, and ticket-driven reporting. Analysts are expected to reason across asset context, exploitability, threat intelligence, and compensating controls at machine scale. To make CTEM work, the approach must shift from manual analysis to **autonomous, agentic execution**:

- Continuous, unified exposure visibility
- Exploitability-driven prioritization
- Stable priorities that enable action
- Measurable exposure burndown
- Automated remediation orchestration

The next evolution of CTEM is autonomous, where intelligent agents continuously reason, prioritize, and drive exposure reduction in real time. As an established leader in Cyber Risk Quantification (CROQ), SAFE uniquely connects technical exposure to measurable business impact, enabling organizations to focus remediation on what truly reduces enterprise risk.



A Clear Comparison of How SAFE Transforms CTEM

Challenge	Stage	Legacy CTEM	Autonomous SAFE CTEM
Scoping	Scope of Coverage	Primarily CVEs	Covers all exposures: CVEs, misconfigurations, identity risk, attack paths, control gaps
	Asset Visibility	Fragmented, siloed asset views	Full attack surface visibility across IT, cloud, SaaS, hybrid
	Data Correlation	Manual reconciliation across tools	Aggregates, consolidates, normalizes, and de-duplicates telemetry from scanners, EDR, cloud control planes, CMDBs, SaaS APIs
	Risk Context	Limited linkage to enterprise risk	Links exposures to actual business impact
Discovery	Detection Model	Periodic scanning	Continuous telemetry ingestion and real-time exposure inference
	Asset & Exposure Identification	Limited context on assets and controls	Comprehensive asset inventory with mapped vulnerabilities and mitigating controls
	Risk Thresholding	Static severity thresholds	Defined, organization-specific risk thresholds enforced across environments
Prioritization	Primary Focus	Tracks what is vulnerable	Focuses on what is exploitable and materially increases attack risk
	Prioritization Method	CVSS-based severity scoring	Exposure-first prioritization based on • Severity • Threat intelligence • Mitigating controls • Asset exposure & reachability • Business impact
	Threat Intelligence	Reactive or manual review	Continuous KEV & threat intel ingestion with automatic exposure reassessment
	Priority Stability	Frequent reshuffling of lists	Autonomous reprioritization only when exposure materially changes

Challenge	Stage	Legacy CTEM	Autonomous SAFE CTEM		
Validation	Control Effectiveness	Limited testing of real-world controls	Control effectiveness testing (MITRE Engenuity frameworks)		
	Coverage Analysis	Minimal insight into control gaps	Visibility into control coverage gaps mapped to exposure drivers		
	Governance Alignment	Separate governance process	Map exposures to policies, risk thresholds, and governance frameworks		
	Outcome Measurement	Volume-based, number of tickets closed	Measure exposure burndown independent of ticket closure . Also tracks Mean Time to Patch (MTTP) Mean Time to Remediate (MTTR) Mean Open Vulnerability Age (MOVA)		
Mobilization	Fix Identification	Manual research for patch or fix	Automated fix identification tied to exposure drivers		
	Remediation Execution	Manual ticketing & coordination	Agentic remediation workflows orchestrating patch and remediation campaigns		
	Ticketing Integration	Basic integrations	Autonomous ticket creation, routing, and ownership assignment based on asset and environment		
	Risk Acceptance	Ad hoc exception handling	Structured risk acceptance workflows tied to governance thresholds		
	Reporting	Static dashboards	Risk and exposure reporting tied to measurable exposure reduction and business impact		

SUCCESS STORY



CARVANA

 How Carvana Reduced Breach Likelihood by 40% within 9 months

Challenges

- Limited visibility across a cloud-first environment
- Vulnerability overload without business context
- Difficulty communicating cyber risk to executives and insurers

Carvana Got 200% ROI with SAFE CTEM:

- Shifted from vulnerability scanning to continuous, quantified cyber risk monitoring
- Enabled business-impact-based prioritization and executive-aligned decision making
- Achieved 40% reduction in Breach Likelihood
- Achieved 25% reduction in cyber insurance premiums
- Doubled cyber insurance coverage limits

“

SAFE's use of AI isn't just a gimmick like many security vendors. Their use of generative AI, deep learning, and classic machine learning techniques is a core part of the platform, enabling us to deeply understand, quantify, and rapidly reduce our cyber risk across our environment.

Dina Mathers, CISO

”

SHIFT FROM MANAGING FINDINGS TO AUTONOMOUSLY REDUCING EXPOSURE

In today's hybrid, high-velocity environments, exposure changes faster than human workflows can keep up. The future of CTEM isn't more analysis. It's autonomous execution.

Organizations adopting this model are seeing measurable impact:

- **Up to 90% reduction in vulnerability noise,**
- **Laser focus on the 1–5% of exposures that materially move enterprise risk.**
- **40–50% faster remediation cycles** through automated ticket orchestration, ownership routing, and validation

This is the shift from managing findings to reducing exposure at scale. The differentiators are clear:

- **Operational scale through automation; not analyst headcount.**
- **Agentic workflows that continuously reason, reprioritize, and mobilize action**
- **Measurable exposure burndown; not ticket closure metrics.**

SAFE's autonomous CTEM transforms security from reactive firefighting into a continuously adaptive, risk-reducing system. The organizations that embrace it won't just keep up with change. They will operationalize resilience and prove it. [Contact us to learn more.](#)



**VISIONARY IN EXPOSURE
MANAGEMENT**

GARTNER MAGIC QUADRANT, 2025



**CATEGORY LEADER
IN CRQ**

FORRESTER CRQ WAVE Q2, 2025



**LEADER IN THIRD PARTY
RISK MANAGEMENT**

LIMINAL LINK INDEX™ REPORT, 2025



**RESEARCH
SPONSOR**

MITRE ATT&CK, TOP CONTRIBUTOR

www.safe.security

getintouch@safe.security