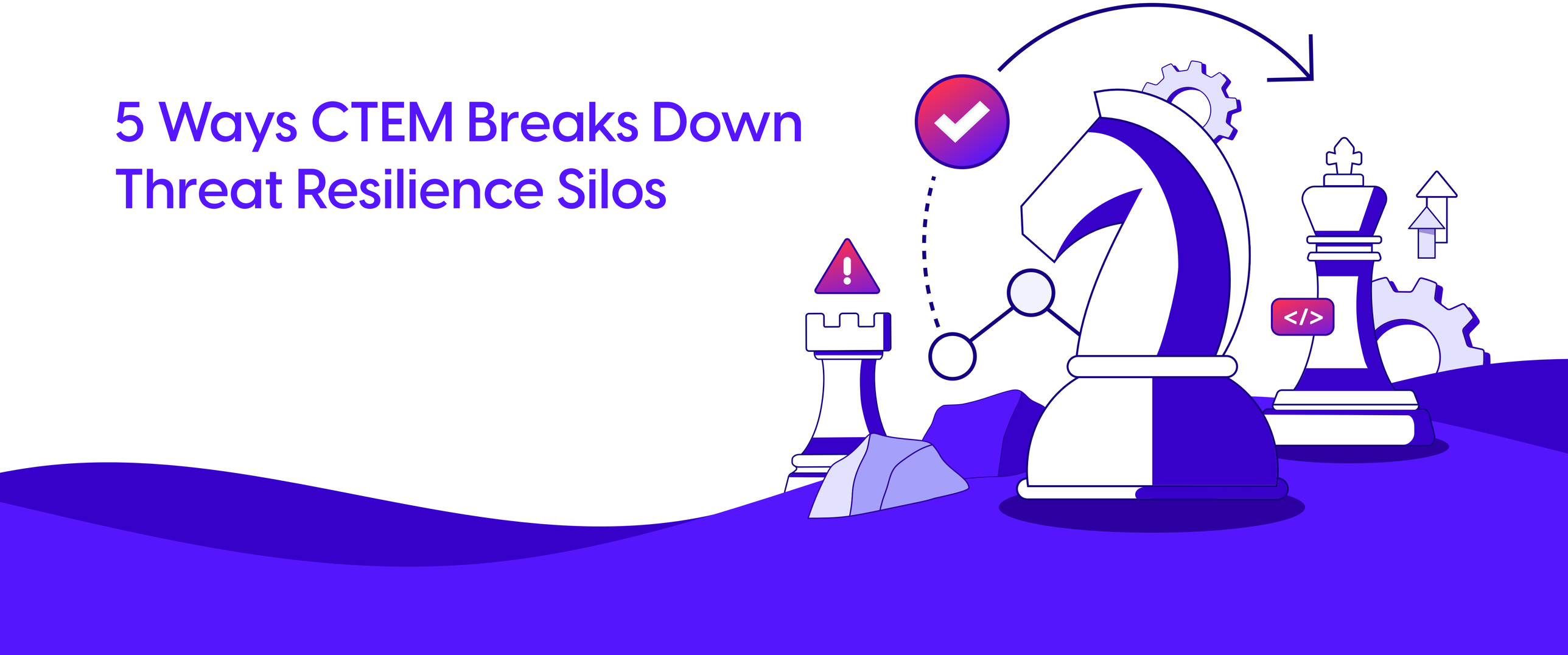
cymulate

5 Ways CTEM Breaks Down Threat Resilience Silos



Proven, proactive cybersecurity for all your teams

Security leaders today face a near-impossible equation: more threats, more tools and fewer clear answers. You can't patch everything, you can't chase every alert and you can't solely rely on reactive defenses.

Organizations implementing continuous threat exposure management (CTEM) will experience up to 50% fewer successful cyberattacks by 2028, according to Gartner. And 89% of CISOs plan to invest in CTEM in the next year according to the Cymulate 2025 Threat Exposure Validation Impact Report, recognizing it as the next evolution in proactive security.

CTEM doesn't just provide a technology framework; it enables the footprint for an organizational one, too. The hardest part isn't adopting new tools. It's breaking down silos between teams that historically operated in isolation.

This guide explores five key ways CTEM helps unite your security, IT and business stakeholders under one shared, validated view of risk. We'll also show how Cymulate operationalizes that collaboration to turn strategy into measurable, continuous resilience.

1 Establishing a common language of risk

Most CISOs don’t struggle with a lack of data. They struggle with too many disconnected sources of it. Vulnerability management tracks patch lists. Red teams test attack paths. SecOps monitors live incidents. Each team speaks its own language. Each has different priorities.

CTEM creates a shared framework and vocabulary for understanding risk. It’s anchored in what truly matters to the business.

- Vulnerability management identifies known weaknesses
- Red teams validate what attackers could actually exploit
- SecOps ensures active detection and response coverage
- Business unites what’s mission critical

How Cymulate helps

Cymulate unites these perspectives in one platform, consolidating data from vulnerability scanners, security controls and infrastructure into a single, correlated exposure view.
Each exposure is scored based on:

- Validation results (what can really be exploited)
- Active threat intelligence (who’s exploiting it now)
- Business context (what systems it impacts)

The result is a common language of validated risk that everyone, from the SOC analyst to the board, can understand and act on.

"Cymulate provides me cybersecurity visibility and resilience metrics enabling us to make data-driven decisions.”

Arkadiy Goykhberg
CISO, DMGT

2 Connecting red, blue and purple teams through continuous validation

Traditional vulnerability management assumes that every unpatched issue is dangerous. Red teams, on the other hand, know that only a subset of those issues can actually be exploited and that the real threat lies in how attackers chain exposures together.

CTEM bridges that gap through continuous validation, bringing the attacker's perspective into everyday decision-making.

Validation turns theoretical vulnerabilities into verified exposures. It proves what's exploitable, measures the potential blast radius and shows which controls are already mitigating risk.

How Cymulate helps

Cymulate offers industry-leading automated attack simulations that replicate real-world threats safely in production environments.

With full MITRE ATT@CK coverage and a daily threat feed of emerging campaigns, teams can continuously test their exposure to tactics adversaries are using right now.

- Red teams can automate attack paths and validate exploitability at scale
- SecOps can instantly see where detection or prevention failed
- Vulnerability management can focus remediation on validated weaknesses instead of CVSS scores

This continuous, automated validation closes the gap between assessment and action. It replaces assumptions with proof.

*By 2028, organizations that have implemented continuous threat exposure management with special focus on mobilization, across business units, will see at least a **50% reduction in successful cyberattacks***

Gartner

3 Prioritizing what demands immediate action

Once you've established what's truly exploitable, the next step is knowing what to do first.

CTEM's prioritization process is where cross-team collaboration delivers real value. It helps teams agree on which exposures pose the highest risk and which mitigation strategies will deliver the greatest impact.

The prioritization isn't static. It's dynamic and continuous, reflecting new threats, system changes and business priorities.

How Cymulate helps

Cymulate automatically scores and ranks exposures based on three dimensions:

- **Validated exploitability** — what's actually at risk
- **Threat intelligence correlation** — whether known exploits or active campaigns exist
- **Business impact** — what systems or data would be affected

From there, Cymulate recommends the most efficient next action:

- Apply a patch or configuration fix
- Implement a "virtual patch" through existing security controls
- Push custom detection rules directly to SIEM, EDR or XDR

This ensures that every action taken has measurable risk reduction, and every team knows why that action matters.

Cymulate Insight

On average, customers see a 52% reduction *in critical and high-severity vulnerabilities and a 30% improvement in threat prevention within CTEM supported by Cymulate.*

4 Maximizing the value of the tools you already own

The average enterprise security team uses 43 different tools, according to Gartner. Each generates alerts, logs and reports, but few integrate effectively.

The result? Duplicated effort, blind spots and wasted spend.

CTEM encourages organizations to focus on orchestration over accumulation, making the most of existing investments before adding new ones.

How Cymulate helps

Cymulate integrates directly with your current ecosystem, including vulnerability scanners, EDRs, SIEMs, SOAR and threat intelligence feeds.

Rather than adding more noise, it amplifies the signal across your existing stack by correlating and validating data from all sources.

- Use vulnerability data to understand the surface area
- Use red team simulations to validate real attack paths
- Use SecOps telemetry to confirm control effectiveness

Cymulate doesn't replace your existing tools. It helps them work together as a cohesive CTEM system. The next security tool you buy should not create another silo. It should make all your tools smarter.

"I use many security solutions, but Cymulate is a must if you want to ensure your organization is safe from cyber threats. It's easy to use, intuitive and the customer support is unparalleled."

Ariel Kashir
CISO, Hertz Israel

5 Measuring and communicating continuous improvement

The ultimate goal of CTEM is not just risk reduction. It's resilience validation.

CISOs need to show their organizations and boards that investments are paying off, controls are improving and exposure is shrinking over time.

CTEM provides the structure for continuous measurement, enabling leaders to demonstrate progress and maturity in quantifiable terms.

How Cymulate helps

Analytics dashboards from Cymulate help deliver always-updated, board-ready metrics that map directly to business and operational outcomes:

- Exposure reduction (validated, exploitable vulnerabilities)
- Prevention and detection rates (control effectiveness)
- MITRE ATT@CK coverage (breadth of tested defenses)
- Mean time to validation and mitigation (cycle efficiency)

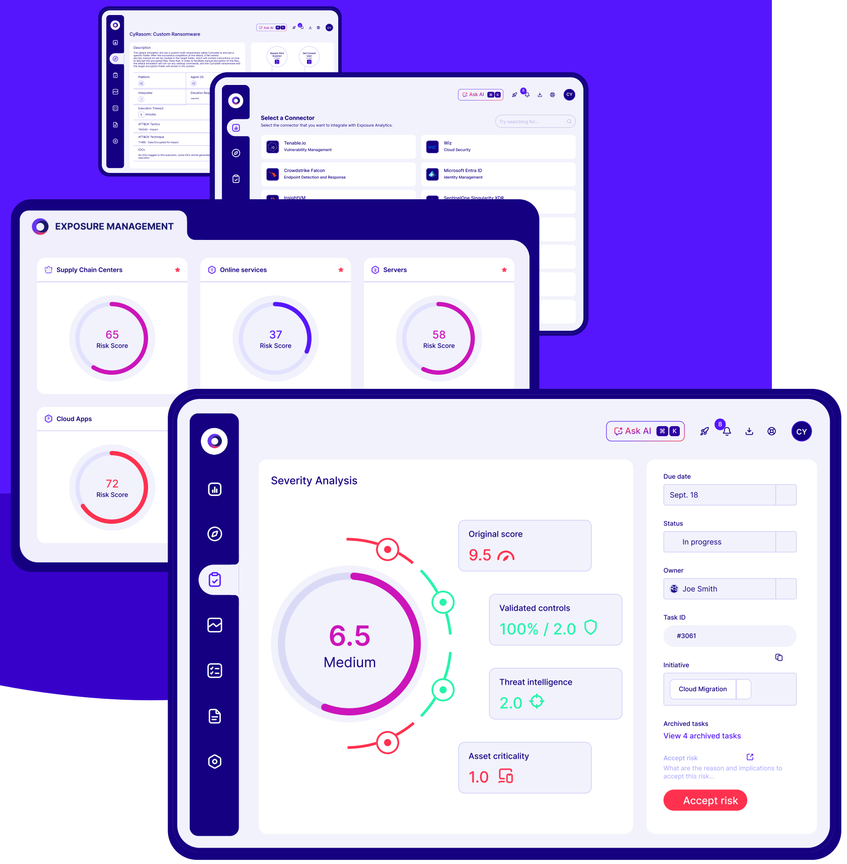
These insights empower CISOs to confidently answer the questions that matter the most:

- How exposed are we today?
- What has improved since last quarter?
- What are we doing next to improve resilience?

By turning CTEM data into measurable outcomes, Cymulate gives CISOs the evidence to demonstrate control maturity, investment ROI and readiness against evolving threats.

"We use the Cymulate reporting to track our improvement over time. We present this data visually to stakeholders who are not security experts in a way they can understand."

Dan Baylis
CISO, LV=



Breaking down silos, building continuous resilience

CTEM isn't just another framework. It's a new operating model for cybersecurity. By fostering collaboration across red, blue and business teams, CTEM transforms disconnected efforts into a unified, continuously improving security system. **Cymulate makes that transformation possible by operationalizing CTEM with:**

- **Continuous** validation of threats and defenses
- **Unified** exposure visibility across all tools
- **Automated** prioritization and remediation guidance
- **Quantifiable** metrics for board and executive reporting

The outcome is clear: teams working together toward the same goal, reducing risk that truly matters and proving resilience everyday. Break down silos. Build resilience. Start with Cymulate. Book a demo today to see it in action.

Start Your Live Demo

cymulate

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.