

# Think You're Secure? Prove It.

## 3 Reasons Why You Need Exposure Management



### The Proof Will Set You Free

**Your job isn't just to protect.** It's to prove—prove resilience, prove risk reduction and prove ROI on every security investment. Threats evolve daily and pressure from the boardroom grows relentlessly. The ultimate freedom comes not from more tools or more alerts, but from proof.

Proven threat resilience, enabled by exposure management, transforms your role. It frees you to operate with confidence and to say "Yes, we can scale," or "No, that risk isn't worth it"—with certainty. It's the freedom to lead from a position of knowledge, not assumption, thanks to continuous, data-driven and actionable proof. Here are three reasons why you need to change your strategy to one that shows proof your security systems will be resilient.

### Problem #1: You Can't Prove How Secure You Really Are

**The Challenge:** Boards want assurance. Business leaders want evidence. But without a reliable way to measure and validate your security posture, all you can offer is an educated guess. Traditional audits, compliance checks and red-teaming are too infrequent and limited in scope to keep up with today's threat landscape.

**The Cymulate Solution:** Cymulate continuously validates your defenses against real-world adversary tactics—across endpoints, networks, email and cloud. You gain:

- A quantified view of your current threat resilience posture
- The ability to translate technical results into business risk metrics
- Executive-level proof points to justify security investments and initiatives

### Problem #2: You're Prioritizing the Wrong Risks

**The Challenge:** Most security teams rely on severity scores to guide their remediation, but severity doesn't equal exploitability. Without knowing which exposures are actually viable for attackers in your environment, you risk wasting time on theoretical threats while critical gaps remain open.

**The Cymulate Solution:** Cymulate correlates your environment with real adversary behavior to surface what matters most by:

- Identifying exposures that real attackers could exploit
- Prioritizing remediation efforts based on actual risk, not just CVSS scores
- Avoiding wasting time and budget on low-impact vulnerabilities

#### Why Exposure Management Matters Now

**67%**

of businesses paid a ransom last year; nearly half experienced ransomware in the past 6 months  
(*Security Today, Cohesity*)

**47%**

of companies lost potential customers after a breach in 2024; 43% lost existing ones.  
(*Cyber Magazine*)

**Only 2%**

of organizations have achieved firm-wide cyber resilience—despite 66% ranking cyber risk as their top strategic concern.  
(*PWC*)

**Nearly half**

of all companies take 6+ days to recover from a cyber event.  
(*Cohesity*)

## Problem 3: Your Security Posture Is Always at Risk of Drifting

**The Challenge:** Security isn't static. Tools degrade. Configurations drift. New attack techniques emerge daily. Meanwhile, your teams are stretched thin, making it nearly impossible to keep everything tuned, current and aligned to the threat landscape.

**The Cymulate Solution:** Cymulate automates and streamlines the ongoing optimization of your controls and processes. Reduce MTTD/MTTR, improve detection coverage, leave fewer blind spots—and a posture that continuously adapts and improves with your business.

The platform:

- Continuously monitors prevention and detection system effectiveness
- Accelerates tuning through AI-powered detection engineering support
- Powers a full Continuous Threat Exposure Management (CTEM) program with dynamic threat-informed prioritization



*When leadership asks, "Can we take this risk?" your answer must be backed by proof, not hope.*

## The Cymulate Exposure Management Platform

Cymulate helps you prove, prioritize and optimize your threat resilience by continuously validating your security posture against real-world threats. We remove the guesswork from your security program by delivering a constantly updated view of where you stand—what threats you're prepared to stop, where you're exposed and how to fix it fast.

- **Validation** – Simulate attacks to prove current prevention and detection capabilities.
- **Prioritization** – Focus your teams on exposures that are actually exploitable in your environment.
- **Optimization** – Automate and guide remediation, configuration tuning and threat coverage expansion.

## Business Freedom Starts with Proof

The future of security isn't about reacting faster. It's about planning smarter. Reactive security doesn't scale. Resilient security does. With Cymulate, your teams validate, prioritize and optimize continuously. When leadership asks, "Can we take this risk?" your answer must be backed by proof, not hope.

### Real-World Use Cases That Matter

#### Threat Visibility & Validation

**What:** Simulate adversarial behavior to assess detection, prevention, and response

**Why it matters:** Provide security leaders with proof of resilience and clear threat posture reporting

#### Reduce Risk by Optimizing Controls

**What:** Uncover gaps in prevention and detection; validate exposure

**Why it matters:** Inform strategic planning, reduce business risk, and justify spend

#### Improve Detection Engineering Efficiency

**What:** Use AI to optimize alert logic and improve threat coverage

**Why it matters:** Boost SOC efficiency and reduce detection lag (MTTD/MTTR)

#### Enable a CTEM Program

**What:** Integrate exposure validation into continuous threat management

**Why it matters:** Get a full lifecycle view of threat exposure with real-world threat context

## About Cymulate

Cymulate, the leader in security and exposure validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit [www.cymulate.com](https://www.cymulate.com).