

SOLUTION BRIEF

Measure and Baseline Cyber Resilience

Measuring Cyber Resilience Requires Data

Security leaders lack data to establish a common baseline for assessing cyber resilience and measuring the outcomes of initiatives. Without clear, measurable data points, it's challenging to determine if resources are effectively reducing risk or simply maintaining the status quo, making it difficult to justify cybersecurity investments to stakeholders. Security leaders are increasingly under pressure to prove the impact of their programs, yet they often lack the data they need.

Security Validation Provides the Metrics and Evidence to Measure and Optimize Security

To deliver measurable results, you must start by evaluating the current state of your organization's defenses. The Cymulate Exposure Management Platform validates true threat exposure to baseline and measure security resilience and business risk. The platform's dynamic dashboards and reporting allow you to measure and communicate cyber resilience to executives, boards and their peers while prioritizing new investments and measuring improvement.

Dynamic dashboards and reporting

With Cymulate dynamic dashboards and reporting, you can gather insights from across the platform. These customized dashboards can be tailored to meet your specific needs and goals so you can visualize information that best suits your organization, updated in real time with the latest assessment metrics.

“Cymulate enables us to have data-driven conversations about cybersecurity. No more opinions. It's just the facts.”

- Dan Baylis, CISO, LV=

Solution Benefits



Track performance and trends

Understand how security measures are performing and where improvements can be made.



Make data-driven decisions

Gather actionable insights that inform security strategies and track their results.



Prove cyber resilience

Baseline security posture based on the attack surface, control efficacy and breach feasibility.

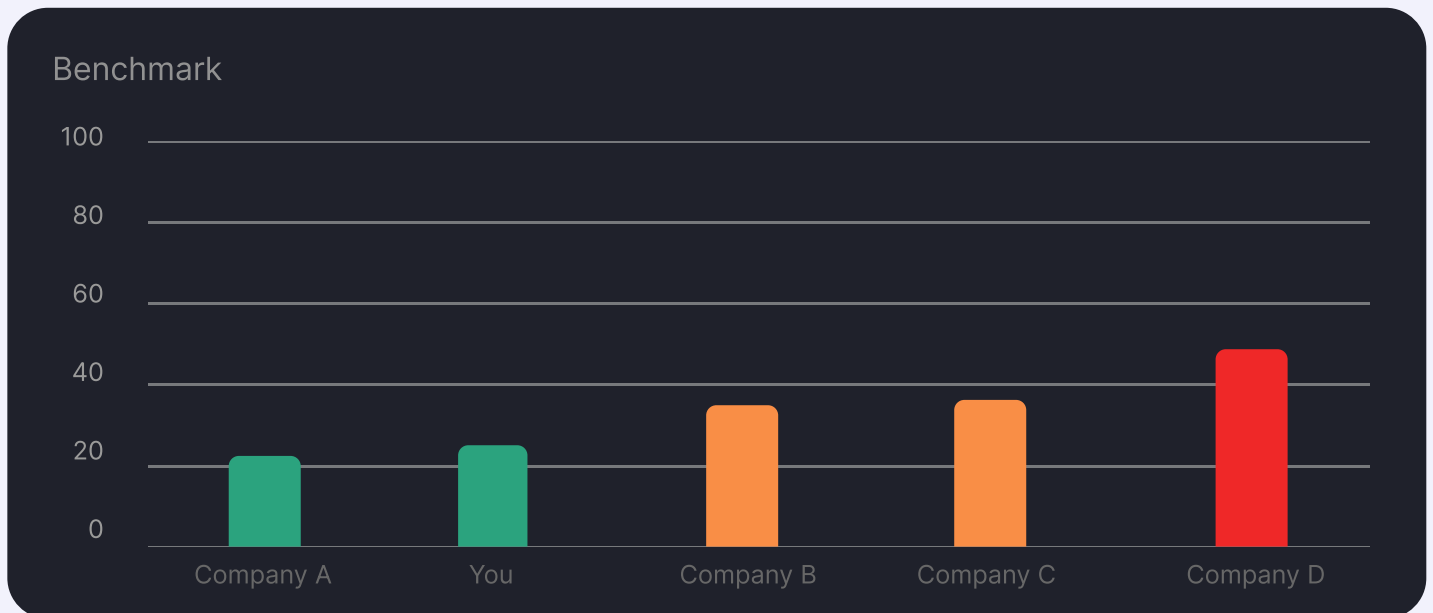


Increase communication

Translate technical metrics into business outcomes to ensure alignment with the executive team.

Industry benchmarks

Cymulate provides a quantifiable measurement of your organization's cyber resilience and control effectiveness relative to industry benchmarks. This comparison provides insights into how your organization's security measures align with industry norms and helps identify potential gaps or areas for improvement.



Cybersecurity framework alignment

Cymulate aligns with various cybersecurity frameworks, ensuring its methodologies adhere to industry standards for risk management and cybersecurity best practices. This alignment is crucial for organizations that comply with frameworks such as NIST 800-53, MITRE ATT&CK®, ISO, GDPR and SOC2 Type II.

Drift detection and management

Cymulate provides evidence-based, security effectiveness scoring based on assessments from breach and attack simulation and continuous automated red teaming. This measurement tracks security control performance and trends based on the historical data of previous assessments to give you a complete picture of your security defenses. The score considers control assessments that reflect the following:

- The evolution of new and active threats
- Control updates

About Cymulate

Cymulate, the leader in exposure management and security 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 500 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.

[Get a Demo](#)