

# Healthcare

Reducing threat exposure and attack impact.

## Healthcare Industry Under Attack

Security leaders in the healthcare industry face significant challenges as threat actors target valuable data and critical systems where any disruption impacts medical services and the complex nature of business operations.

While the average cost of a healthcare data breach reached \$10.93 million, threat actors know that healthcare providers will pay millions more in ransom payments to recover or maintain critical services.

**\$10.93M**  
Average Healthcare  
Data Breach Cost<sup>1</sup>

## Adopt the Attacker’s View to Harden Defenses

Healthcare organizations like Assuta Medical Center, Elara Caring, and Nemours know they must be prepared for the next attack, so they use Cymulate to continuously validate their cyber security controls and test their defensive posture.

The Cymulate security and exposure validation platform automates advanced offensive testing with the latest threat activity facing the healthcare industry. Each assessment includes remediation guidance with specific steps to update security configurations and tune controls.

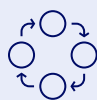
### Cymulate Security and Exposure Validation



Attack Surface  
Management



Breach & Attack  
Simulation



Continuous  
Automated  
Red Teaming

The Cymulate platform delivers automated offensive security testing with security controls integration and remediation guidance in a unified, easy-to-deploy SaaS solution.



### Assuta Medical Center

“Cymulate utilized their vast cyber knowledge and security experts to offer a complete solution that proactively challenges our overall security architecture.”

Tamir Ronen  
Chief Information Security Officer



### Elara Caring

“Cymulate is super easy to use and answers the tough boardroom questions. It is a force-multiplier for my small team. I can use it to easily test efficacy in a fire-and-forget automated manner.”

Eric Bowerman  
Chief Information Security Officer



### Healthcare Organization

“Cymulate enables us to test our defenses against the latest cyber threats as they emerge, prioritize remediation efforts, and improve our security team’s incident response skills.”

CISO, Healthcare Organization

## Defending at the Speed of Adversaries

Cybersecurity is a game of continuous improvement where healthcare organizations are adopting an offensive mindset to identify and fix their gaps and weaknesses before adversaries can find and exploit them.

Threat actors can gain initial access to a device on the network and then breakout and achieve lateral movement across your healthcare systems in just over 1 hour.

**62 mins**

Average eCrime  
Breakout Time<sup>2</sup>

Source: CrowdStrike Global Threat Report 2024<sup>2</sup>

## Defense that Can Take a Punch

Offensive testing provides proof and evidence of cyber resilience. The Cymulate platform continuously validates your security control effectiveness and attack path exposures with production-safe threat assessments to improve your security and prove resilience.

## Healthcare Customer Benefits

- Validate Defenses Against Emergent Threats
- Automate Continuous Security Testing
- Optimize Defenses with Remediation Guidance
- Prioritize Remediation Based on Real Threats

## Cymulate Named a Customers' Choice by Gartner Peer Insights



**4.7** out of  
★★★★★

**4.9** in support  
experience

**94%**  
of respondents willing to  
recommend Cymulate

## About Cymulate

Cymulate is the leader in exposure management and security validation. More than 500 customers worldwide rely on the Cymulate platform for continuous discovery, validation, prioritization, and guided remediation of security gaps before attackers can exploit them. For more information, visit [www.cymulate.com](http://www.cymulate.com).

## Why Healthcare Organizations Choose Cymulate?

### Ease of Deployment

Cymulate is a true SaaS platform, making it simple to deploy in your healthcare environment and accelerate the time to value to fully validate your security controls, identify high-priority areas of weakness, and provide mitigation guidance to improve your cyber posture.

### Depth of Attack Simulations

The Cymulate platform contains over 120,000 attack simulation resources created by Cymulate threat researchers and red team specialists, allowing healthcare providers to perform comprehensive testing and validation of their security controls using our automated suite of best practices and test scenarios.

### Immediate Threats Intel

The Cymulate Threat Research Group loads new test scenarios for the latest immediate threats discovered every single day, enabling the Cymulate platform to automatically validate and notify the healthcare security team of any exposure they may have to an active threat.

### Mitigation Guidance

Cymulate goes beyond simply identifying gaps and weaknesses in your security practices and controls by providing healthcare security teams with the guidance they need to mitigate threats and implement detection rules for the latest threat activity.

Contact us for a live demo

[Start Your Live Demo](#)

[info@cymulate.com](mailto:info@cymulate.com) | [www.cymulate.com](http://www.cymulate.com)