

INDUSTRY BRIEF

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
IBM Cost of a Data Breach 2023

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 validate their security controls and continuously test their defensive posture.

Cymulate exposure validation 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 Exposure Validation for Healthcare

With market-leading breach and attack simulation and automated red teaming, Cymulate helps healthcare security teams proactively uncover and remediate exposures before they can be exploited. By continuously assessing their controls, teams can optimize their defenses against new and evolving threats, protecting patient data and ensuring the resilience of healthcare operations.

Benefits

- Focus on true exposures
- Test and optimize security controls
- Battle-test your SOC and MSSP
- Measure and prove cyber resilience

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, CISO

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, CISO

Nemours Children's Health System

"Cymulate enables us to test Nemours' defences against the latest cyber threats as they emerge, prioritize remediation efforts, and improve our security team's incident response skills."

– Jim Loveless, CISO

Defending at the Speed of Adversaries

Cybersecurity is a continuous improvement journey, and healthcare organizations are adopting a proactive, offensive approach to stay ahead of threats.

Rather than waiting for breaches to occur, they're actively identifying and fixing security gaps before adversaries can exploit them. Today, attackers can gain initial access to a single device and move laterally across healthcare systems in just over an hour, making early detection and rapid response critical.

Prove and Optimize Threat Resilience

Offensive testing provides proof and evidence of cyber resilience. Cymulate continuously validates your security control effectiveness and attack path exposures with production-safe threat assessments that benchmark security resilience and identify gaps with actionable and automated mitigation to optimize security controls.

Why Healthcare Organizations Choose Cymulate



Ease of deployment

The SaaS-based platform is quick to deploy in healthcare environments, delivering immediate value by validation security controls, uncovering critical weaknesses and guiding mitigation to enhance cyber resilience.



Depth of attack simulation

Cymulate offers over 120,000 attack simulation crafted by experts, enabling healthcare providers to thoroughly test and validate security controls with best practices and scenarios.



24/7 threat feed

Cymulate Research Labs adds out-of-the-box test scenarios for the latest threats, automatically validating defenses and alerting healthcare teams about any new exposure.



Actionable & Automated Mitigation

Cymulate integrates with security controls and mobilizes healthcare teams to fine-tune controls and block active threats with both automated control updates and step-by-step recommended to optimize controls.

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.