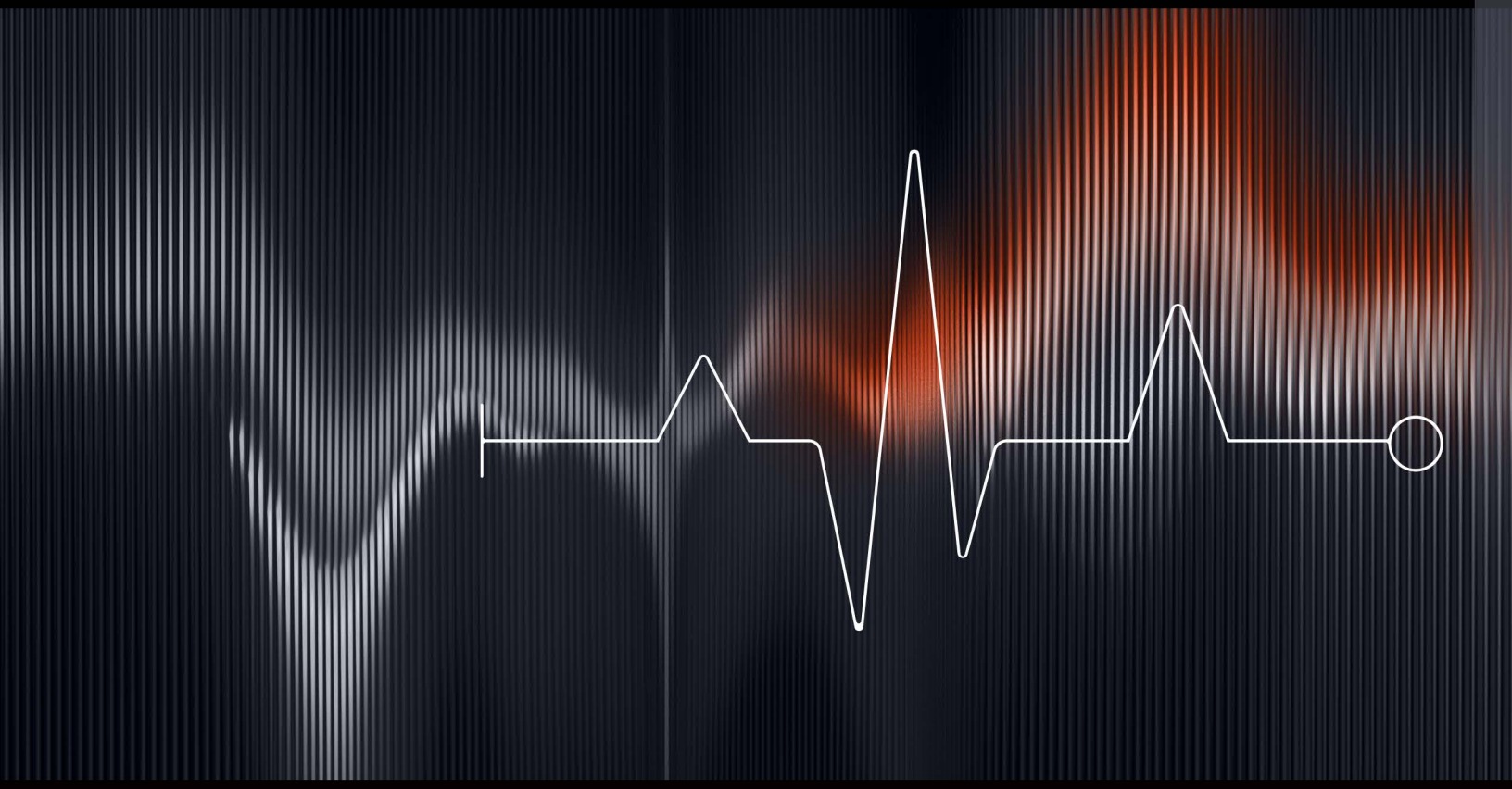
DATASHEET

SIMSPACE

CYBER RISK MANAGEMENT FOR HEALTHCARE ORGANIZATIONS



- SAFEGUARD PATIENT DATA
- MAINTAIN REGULATORY COMPLIANCE
- EVALUATE SECURITY TEAMS AND TECHNOLOGY

HEALTHCARE ORGANIZATIONS

SIMSPACE
SECURE WITH CONFIDENCE

As advances in modern medicine and technology have intersected to make treatment and therapy possible via the internet, healthcare organizations are embracing web-based digital operating models. While digital transformation initiatives help patients manage their own health and communicate with caregivers, they also introduce new cyber risk. And due to the high value of health records on the black market, healthcare organizations are often targeted by malicious actors.

To be competitive in the industry and maintain regulatory compliance, healthcare organizations need their security teams and technology stacks operating at peak performance, which requires continuous assessments to drive growth. In fact, certain regulatory frameworks like HITRUST specifically require firms to incorporate simulated events and exercises for thorough, realistic training.

reduce risk

Reducing cyber risk in healthcare starts with hands-on training and assessments

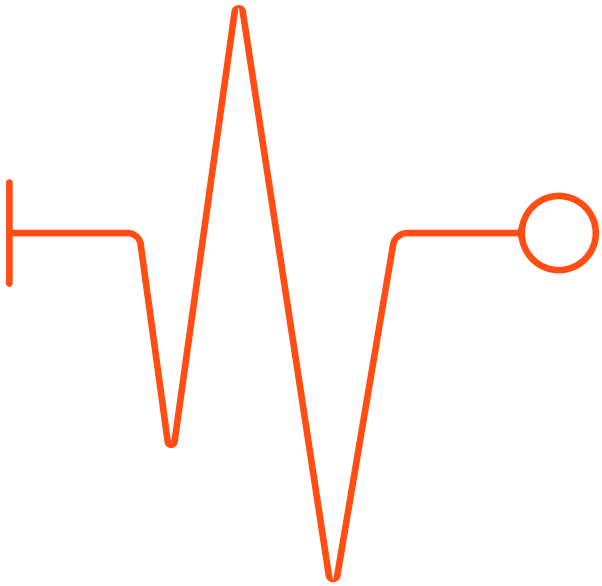
To meet strict compliance requirements and secure electronic protected health information (ePHI), it's critical to continually assess the performance of your security team and tech stack. With the SimSpace Cyber Risk Management Platform, you can use the most advanced commercially-available cyber range to evaluate your defenses against real-world attack scenarios.

32%
increase in individuals affected by data breaches[1]

82%
of reported data breaches affected healthcare providers[2]

113
hacking/IT incidents submitted to the Department of Health and Human Services Office for Civil Rights between 1/1/22 and 3/21/22[3]

assess the performance of your security team



[1] *2021 H2 Healthcare Data Breach Report | Critical Insight.* (2022). Critical Insight. https://cybersecurity.criticalinsight.com/2021_H2_HealthcareDataBreachReport

[2] *January 2022 Healthcare Breach Report.* Compliancy Group. (2022, April 5). https://compliancy-group.com/january-2022-healthcare-breach-report/

[3] *U.S. Department of Health & Human Services - Office for Civil Rights.* (2022). Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=6969879F75B929F19BA6DE1D7A9C5205

Build team readiness with SimSpace

- Establish a baseline for your security posture
- Train against new attacks and penetration testing scenarios to challenge and prepare your team
- Collect data and analytics to measure team performance
- Run more scenarios to improve your security posture and team proficiency

Maintain your (ISC)² certifications

You and your team can earn CPE credits by completing training courses on our cyber range platform, or by attending SimSpace virtual events.

build trust

Evaluate your people, processes and technology in a secure environment

People	Processes	Technology
Run realistic simulated attacks	**Optimize detection,** reponse and mitigation	**Evaluate your security tools** against advanced threats
Continually evaluate and improve team readiness	**Fine-tune your security** configurations and processes	**Model your production environment** to evaluate integrations and tool performance
Hire better candidates and train for specific roles	**Map security assessments to regulatory standards** like PCI DSS, HIPAA and HITRUST	**Apply life-like user and traffic emulation** for added realism

Balance security with efficiency

Before you introduce a new telehealth service, patient portal or electronic health record (EHR) system, help your organization's security leaders identify potential risks—without slowing down delivery:

Model scenarios in a secure, realistic environment

Evaluate products in depth before making a purchase

Understand how your security tools and policies impact delivery

Build security into applications, IoT devices and other IT infrastructure

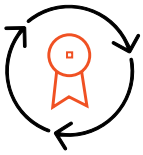
Test new patches prior to implementation

Business results

Keep telehealth and EHR systems online

Create competitive differentiation with your cybersecurity posture

Choose the right software vendors

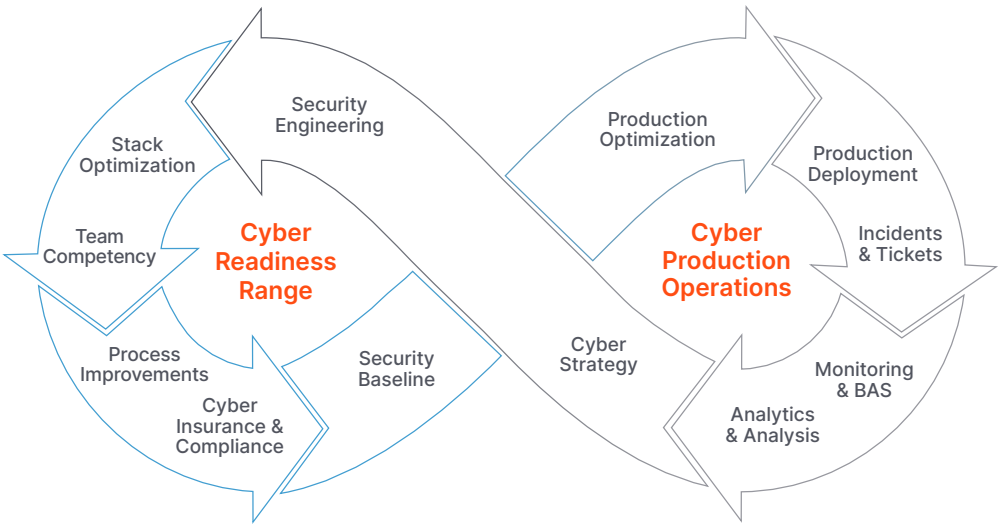


Stay compliant and negotiate lower cyber insurance premiums

Mitigate security risks when sharing data with clinicians, specialists, care givers and labs

Build patient trust

Make informed decisions throughout the cyber-maturity lifecycle



SimSpace Cyber Risk Management Platform features

- Open, customizable, high-fidelity platform
- Library of automated cyber crisis training content, APTs, insider threats and zero-day attacks
- Support for top open-source and commercial cybersecurity products
- Insights from our Professional Services team
- Pre-built, industry-specific network templates—hybrid cloud, ICS and SCADA
- Advanced user emulation for realism and more meaningful assessments
- Data-driven product evaluation and tech-stack tuning
- Maps to NICE 3.0, MITRE ATT&CK® and other regulatory frameworks

Why SimSpace?

Our exclusive cyber range provides healthcare organizations with an unparalleled platform for cyber risk assessments, product evaluation, real-world attack simulations and extensive individual and team readiness training. SimSpace helps you up-level your security posture and team competency so you can defend against evolving cyber threats with confidence. As a result, you'll be able to provide better care, protect patient data and stay compliant.

Capabilities supporting HIPAA and HITRUST requirements

Trusted by 5 of the Top 10 US banks

Chosen by the US Cyber Command

40% reduction in configuration related breaches

45% improvement in attack defense

48% improvement in time to detect attacks

Ready to learn more about how SimSpace can help you up-level your security posture? Click here to request a demo.