Healthcare Industry:
Reduce Your Risk of a Healthcare Data Breach

Healthcare data breaches are on the rise. Organizations face the challenge of safeguarding a large amount of sensitive information about their patients. The loss of Protected Health Information (PHI) incurs more than just heavy fines – affected patients may have to deal with identity theft or in some cases, medical harm.

125%

Criminal attacks on healthcare organizations are up 125% compared to 5 years ago, according to the Ponemon Institute (May 2015).

## Security Challenges Faced by Healthcare Organizations

- A motivated, organized and nimble adversary targeting highly valuable medical and identity information.

- Complex and distributed IT infrastructure with difficult to patch legacy systems and proprietary medical devices.

- An expanding attack surface with the adoption of BYOD, cloud-based email, and new technologies such as wearables.

- Overwhelming number of security alerts resulting in failure to spot genuine indicators of compromise.

- Significant regulatory expectations require increased focus and spend to comply with HIPAA Security and Privacy rules.

Reduce Your Risk of a Breach

Healthcare organizations need to manage a constantly changing IT environment. They need to understand their exposure across physical and virtual networks, cloud services, mobile devices, web applications, and medical systems. Risks need to be identified as they emerge and prioritized for remediation based on the threat landscape and the organization's unique needs.

Rapid7 Threat Exposure Management solutions can help you:

- Assess your network and infrastructure for vulnerabilities, configuration issues, controls gaps, and policy violations.

- Conduct a penetration test to uncover weaknesses and simulate phishing campaigns to improve security awareness.

- Dynamically scan your custom web applications for vulnerabilities and prioritize these for remediation.
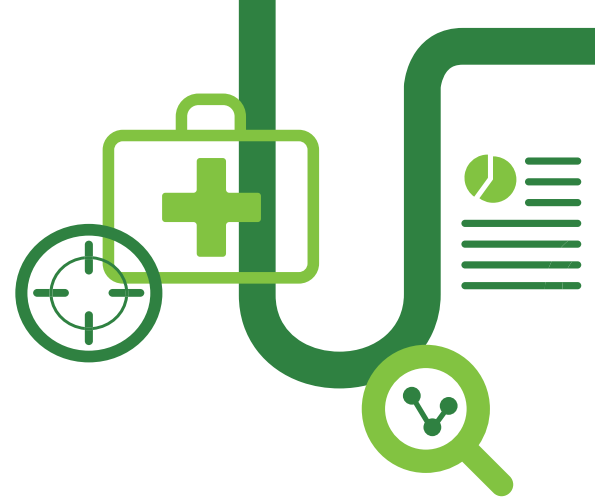
> "After eight months of running Nexpose and Metasploit… we had reduced risk exposure by more than 98%. That's particularly impressive when you consider the face that we brought on five new hospitals in that timeframe."

<div align="right">
Scott Erven
Manager, Information Security, Essentia Health
</div>

Keep Healthcare Data Safe from Attackers

Intruders are able to stay undetected on networks for an average 205 days (Mandiant 2015 Threat Report). During this time, cybercriminals are looking for PHI records, which command the highest prices on the black market. Healthcare organizations need to continuously monitor their network for indicators of compromise.

Rapid7 Incident Detection & Response solutions can help you:

- Detect stealthy attacks, including compromised credentials, lateral movement and phishing.

- Investigate security incidents faster with user context – stop attackers in their tracks before damage is done.

- Expose risky internal behavior across the network, endpoints, cloud services, and mobile devices.

Transform Your Security Program

The 2015 HIMSS Cybersecurity Survey reported that healthcare organizations are only moderately confident in their ability to protect their IT infrastructure and data. Healthcare organizations need a relevant, actionable, and sustainable cyber security program to improve their ability to protect against and respond to emerging threats.

Rapid7 Security Advisory Services can help you:

- Perform an assessment of your security program against a maturity model and HIPAA requirements.

- Develop a cyber security and incident response program to prepare your organization for relevant threats.

- Educate your employees to recognize security risks and understand their role in protecting PHI.

Simplify Your HIPAA Compliance Efforts

Over the past few years, HIPAA Security and Privacy rules have continued to evolve while personal and organizational fines for non-compliance have increased substantially. Rapid7 currently provides services to many HIPAA Covered Entities and Business Associates and meets the contractual obligations of a Business Associate.

Rapid7 solutions can help you comply with HIPAA requirements as follows:

- Use Nexpose and AppSpider to assess your network and applications for potential risks and vulnerabilities.

- Automatically generate reports showing compliance with built-in templates in Nexpose and AppSpider.

- Monitor critical assets containing PHI and detect unauthorized or malicious access with UserInsight.

- Use Metasploit to test the effectiveness of your technical safeguards and access controls.

- Identify gaps in your security program against HIPAA requirements and guidance on remediation.