

MEDICAL DEVICE PENETRATION TESTING

Relentlessly Future Focused, So You Can Be Too.

Discover and manage vulnerabilities on medical devices at every stage of development, implementation, and maintenance.

63% of healthcare companies have experienced one or more security incidents related to unmanaged and IoT devices. ([Forrester Report](#))

To add to this, the average 2022 cost of a healthcare data breach was **\$10.1 M.** ([IBM report](#))

In fact, medical device manufacturers must now prove that products meet cybersecurity standards for FDA approval according to 501(k) Premarket Notification. ([FDA Report](#))

NetSPI's IoT Penetration Testing is specifically designed for use cases in the medical device industry, leveraging our proven methodology from over 15,000 engagements and decades of manual testing experience, along with a deep understanding of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, FDA 501(k) Premarket Notification, ANSI, and more to not only meet, but exceed security recommendations.

“Solving these types of problems is a shared task between those responsible for configuring, maintaining, and operating the organization’s infrastructure as well as the users of this infrastructure,” said Dean Sittig, PhD, professor of biomedical informatics at the University of Texas Health Sciences Center at Houston. **“While preventing all ransomware attacks is not possible, there are a number of steps HCOs can take to reduce their risk as well as mitigate potential harm.”**

NetSPI's Medical Device Penetration Testing Process

1 Threat Model Potential Security Risks

- ◆ What is the scope of the device?
- ◆ What are the assets that need to be protected?
- ◆ What has access to the assets?
- ◆ How are we preventing the loss of the assets?
- ◆ How can we ensure availability and the integrity of the device?

2 Evaluate Using Proven Technology and Expert Pentesters

- ◆ Security requirements
- ◆ Threat mitigation
- ◆ Vulnerability testing
- ◆ Penetration testing
 - ◆ Network
 - ◆ Bluetooth
 - ◆ Wireless
 - ◆ Mobile
 - ◆ Cloud
 - ◆ Thick client
 - ◆ Medical

3 Deliver Actionable Findings and Support Remediation

- ◆ Expert human penetration testers
- ◆ Real-time findings reporting and remediation support
- ◆ Vulnerability validation and prioritization
- ◆ Track and trend findings
- ◆ Open API integration and more












To learn more about NetSPI's Medical Device Penetration Testing services, or any of our other offerings, visit www.netspi.com or [contact us](#).

About NetSPI

NetSPI is the leader in enterprise penetration testing and attack surface management. Today, NetSPI offers the most comprehensive suite of offensive security solutions – attack surface management, penetration testing as a service, and breach and attack simulation. Through a combination of technology innovation and human ingenuity NetSPI helps organizations discover, prioritize, and remediate security vulnerabilities. For over 20 years, NetSPI's global cybersecurity experts have been committed to securing the world's most prominent organizations, including nine of the top 10 U.S. banks, three of the five largest healthcare companies, the leading cloud providers, and many of the Fortune® 500.

Platform Driven, Human Delivered

RESOLVE | EAS | ASM

-  Application Pentesting
-  Cloud Pentesting
-  Network Pentesting
-  IoT Pentesting
-  Secure Code Review
-  Strategic Advisory
-  Red Team Testing
-  Social Engineering
-  Blockchain Pentesting