How NHS Royal Bolton Hospital Centralized Cybersecurity for Resilient Patient Data

Highlight Achievements

- Ability to run daily penetration tests providing a consistent security blanket
- Continuous penetration testing insights, identified vulnerabilities and suggested security improvements
- 30 minutes of using the Pentera Platform achieved the equivalent of 27 days of work

Background Information

Royal Bolton Hospital, part of the NHS network, manages a large and growing IT infrastructure that serves over 8,000 employees across 30 facilities, with plans to expand to 60 facilities. As an essential healthcare provider, Royal Bolton faced increasing cybersecurity risks, compounded by a reliance on multiple fragmented security tools. In search of a solution to unify its cybersecurity approach, the hospital partnered with Pentera to streamline operations, assess the effectiveness of its security stack, and strengthen its resilience against evolving threats.

The Challenge: The team struggled to manage cybersecurity across a complex infrastructure

Even for a security-conscious team, as your environment grows, different scripts get pushed to the back of your mind and old machines that are not in regular use can create additional attack surfaces causing you to lose control of some of the IT operations. As the Royal Bolton Hospital expanded and added new machines, users, and software, in tandem, the hospital network became more complex. This increasingly complex infrastructure required constant changes to their cybersecurity defense with the ongoing addition of new solutions and hardware. Manual penetration testing, as a way to validate cybersecurity effectiveness, is costly and only covers a segment of the network. It was insufficient as a solution for maintaining a completely secure network.

The Need: Continuous validation from an adversary's perspective

Royal Bolton required a solution that could continuously validate defenses, support NHS compliance, and ensure ongoing resilience without burdening their small IT team. In adherence with the UK compliance regulations, Royal Bolton ran routine penetration tests on their network once a year. Although not affected by the WannaCry attack in 2017, Royal Bolton's IT team understood the need to further invest in their cybersecurity defenses. With their ever-growing network, they realized the need to improve and challenge their resilience on a consistent basis using the adversary perspective.

The Solution: Centralized Security Validation

Royal Bolton was introduced to Pentera and requested to validate the solution and observe its value in their own environment before committing to purchase. The proof-of-concept was set for one day, and was concluded in just 5 hours.

The predefined success criteria were set at:

- Successful discovery & enumeration of hosts and devices within the IP range(s) selected
- Successful static vulnerability scanning and assessment
- Generating a prioritized list of pen-testing achievements within the selected segment(s)
- Display of the full attack vector for each pen-test achievement

The security team at Royal Bolton was able to review and analyze the results, the impact of a vulnerability, and the remediation options. Pentera generated a penetration test summary report that included an executive summary, a full action report, found vulnerabilities, and remediation suggestions (action items).

Penetration testing is a project. Vetting the vendor, scheduling the project, catering for logistics, hosting, and accompanying third-party ethical hackers. Pentera changed the game by performing the work of a penetration testing team without actually employing one. Royal Bolton was able to skip the resource-heavy, costly steps of logistics for continuous pentesting. Pentesting has become a standard and weekly procedure of the department that can now instantly audit every change in the network and test against the equivalent of a nation-sponsored hacker. Security team members can focus on their other tasks while Pentera runs in the background and when they are ready, review the vulnerabilities uncovered before prioritizing the necessary remediation.

The observed value as seen by the Royal Bolton IT security team was the complete visibility of vulnerabilities on an ongoing basis. The team could observe almost instantly the most crucial remediations that need to take place, and they could audit password and user privilege policies in the field. Bolton's IT team was now able to "stress test" their other cybersecurity tools and check their effectiveness, which they could not have done as easily before.

Result: Unified view of its attack surface and full context of exploitable paths

Pentera's platform provided long-term value through streamlined security functions, enabling cost reductions and eliminating the need for outsourced testing. The automated insights also validated previous security investments and guided strategic enhancements, supporting a continuously tested and adaptable security posture.

Targeted Vulnerability Prioritization
With a complex network, there is an immense number of theoretical vulnerabilities. With Pentera, you can see the most critical vulnerabilities and prioritize remediation. For Royal Bolton, this has resulted in the cybersecurity team being much more responsive and efficient in handling exploitable vulnerabilities.

Perpetual Security Resilience
Pentera allows companies to run automated penetration tests as needed. Unlike manual penetration testing on a set schedule, regular automated testing assures a state of perpetual security validation. For Royal Bolton, this ensures that all network-wide patches and fixes are tested for effectiveness immediately after rollout.

Cost Reduction
No longer having to contract a manual third-party pentesting team, the hospital has been able to save costs on keeping pentesting work in-house. They have also been able to generate efficiencies in their team by emulating attacks and getting the prioritization of fixes, the team can spend the needed time on the most breach-baring vulnerabilities.

Better Security Investment Decisions
With frequent and ever-evolving pen-testing practices, the hospital's IT security team can now validate the investment in security tools used in the past, optimize the use of current technology in place, and understand where additional investments need to take place based on the attack vectors that led to their crown jewels.

Compliance and Resource Optimization
Before Pentera, Royal Bolton met compliance requirements through their annual penetration test but didn't truly benefit from the activity. With Pentera, the hospital was able to schedule regular, automated penetration tests for the different network segments and continuously improve its cyber resilience by finding new vulnerabilities and checking remediation effectiveness. Automated validation ensured Royal Bolton met NHS compliance standards, allowing the IT team to focus on remediating verified vulnerabilities rather than conducting repetitive manual testing.

A Unified, Resilient Security Operation
By adopting Pentera, Royal Bolton transitioned from fragmented security processes to a unified, resilient cybersecurity model. As healthcare organizations face increasing cybersecurity demands, Pentera's platform offers a sustainable path to maintaining secure and adaptable protection across critical data environments.

"This solution opened our eyes. We were able to quickly close the most urgent security gaps. Pentera provides a security posture snapshot on-demand"

Brett Walmsley
Chief Technology Officer,
NHS

About Pentera

Pentera is the category leader for Automated Security Validation™, allowing any organization to test all cybersecurity layers, over all the attack surfaces, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.