Verified by Clutch

External Penetration Testing for Digital Healthcare Company

PROJECT DETAILS

- Cybersecurity
- Jan. - Feb. 2022
- $50,000 to $199,999

> *"We appreciated that they offered multiple alternative solutions to suit our budget."*

PROJECT SUMMARY

UN1QUELY conducted external penetration testing for a digital healthcare company's website and SaaS products. They performed a thorough security testing and identified potential risks in the infrastructure.

PROJECT FEEDBACK

UN1QUELY was able to identify more cybersecurity risks than the internal team could, and their team took the time to teach best practices throughout the engagement. Regular check-ins and feedback helped keep the project on track. Their expertise in the field was outstanding.

The Client

Please describe your company and your position there.

I'm running IT Security Operations for a digital healthcare SaaS company operating out of Germany and United States

The Challenge

For what projects/services did your company hire UN1QUELY?

We were looking for an external cybersecurity company to perform an external penetration test of our website and SaaS products (iOS/Android/API endpoints). Because we service the medical industry, we needed to make sure there were no potential data leaks or critical vulnerabilities.

Ema Dapčević
IT Security Operations, Kaia Health

Healthcare

201-500 Employees

Munich, Germany

CLIENT RATING

5.0
Overall Score

Quality:	5.0
Schedule:	5.0
Cost:	5.0
Would Refer:	5.0

The Approach

How did you select this vendor and what were the deciding factors?

We searched online for cybersecurity firms with proven high quality results and senior talent and shortlisted 5. After interviewing them, we chose this vendor based on their service package and experience.

Describe the project in detail and walk through the stages of the project.

They performed a thorough security testing of our website and mobile apps + backend, identifying potential risks in our infrastructure. They used OWASP Top 10 framework as a basis but went beyond the required scope to carry out penetration testing. After they finished, they delivered a report on all of our risks and provided a list of security recommendations. They maintained available via Slack Connect and offered free retests of identified vulnerabilities for 12 months after the report is issued. Their team was supporting ours in implementing the remediations after the engagement was over.

How many resources from the vendor's team worked with you, and what were their positions?

We had a project manager, 2 penetration testers, and a QA Engineer.

The Outcome

Can you share any outcomes from the project that demonstrate progress or success?

They were able to identify far more risks than our internal tests could, and their team is addressing those changes for us. Not only were they thorough, but they also took the time to teach us additional cybersecurity best practices.

How effective was the workflow between your team and theirs?

They kept us updated as they went through each round of testing, and their reports were easy to understand. Weekly check-ins and live chat on Slack helped us stay on schedule.

What did you find most impressive or unique about this company?

We appreciated that they offered multiple alternative solutions to suit our budget. That way, we could better prioritize how we spent our money.

Are there any areas for improvement or something they could have done differently?

Some of the testing took longer than we expected, but their in-depth process paid off in the end.