info@apriorit.com
www.apriorit.com

Case study

Improving a SaaS Cybersecurity Platform with Competitive Features and Quality

Our client is a worldwide provider of a SaaS-based cybersecurity platform. They have customers in the healthcare, automotive, industrial, and other sectors that demand nothing but the best from their partners.

To satisfy their customers' needs, comply with numerous laws and regulations, and ensure product growth, our client needed dedicated specialists with rare skills in several IT fields. Apriorit put together a team with relevant IT skills to fulfill their first request — implementing new features in a low-level vulnerability detection engine.

That was the start of a long-term collaboration that has resulted in many improvements to the platform's feature set, stability, and user experience.

The client

Our client delivers a SaaS cybersecurity platform for detecting and managing vulnerabilities. Thanks to its variety of features and reliability, the platform has become especially popular in the automotive, medical, and industrial sectors.

These sectors are fast-growing and innovative, and at the same time are very attractive to cybercriminals. Software suppliers must pay special attention to the security of their products to be several steps ahead of potential attackers and remain industry-compliant.

To deliver a competitive solution and expand it with the latest achievements in cyber protection, our client started looking for outside help with SaaS platform development and support.

The challenge

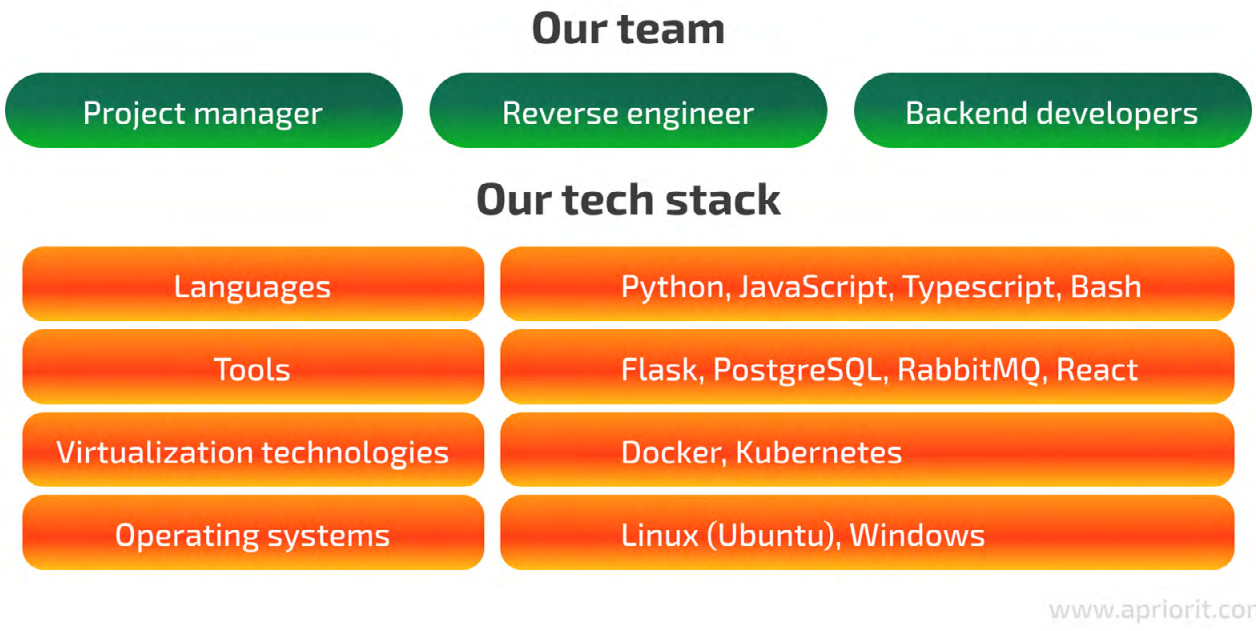
Because of the platform's complexity, the client required an outsourcing development team with a diverse and quite rare set of IT skills that could work as part of their team. With the help of this team, they hoped to solve the following challenges:

- Stay competitive by adding new features and support for more platforms
- Provide timely and efficient support to platform end users
- Improve the efficiency of the in-house team by automating internal processes
- Remain compliant with requirements within end users' industries

After evaluating their options, the client decided to go with Apriorit.

Our approach

To facilitate the project's development, we put together a team with a project manager, a reverse engineer, and backend developers with experience in the relevant technology stack. They work alongside our client's in-house team.



To make sure that our developers and the client's team are always on the same page, we introduced Scrum-based communications. The client can track the project's progress in weekly meetings, via Jira tasks, and by holding additional meetings to discuss complex issues. To resolve all day-to-day challenges, our developers communicate directly with in-house specialists.

The result

New functionalities and features have made the client's platform more stable, robust, and competitive. The client helps end users stay on top of their cybersecurity by helping them efficiently detect and manage more vulnerabilities. We have also helped the client improve end user satisfaction by working on support requests and the platform's user experience (UX).

The client is satisfied with the results of our work, and we continue to help them deliver the best possible product to their users.

How we did it

Initially, the client approached us with a request to extend the functionality of their platform's vulnerability detection engine. We worked as an independent team and presented the client with the results of our work.

1. Adding support for more platforms

Our client wanted to extend the capabilities of their platform's vulnerability detection engine. In particular, they needed it to support a wider variety of processor architectures.

We started with researching the existing engine code and the CPU architectures the client wanted to support. It turned out that to implement support for additional processor architectures, the client's platform required additional backend work.

We offered our client:

- a reverse engineer to research ways to add the required support
- Python developers to create new features and implement them in the existing product back end
- a project manager to coordinate work between our team and the client's team

The client was impressed with the quality and flexibility of our work as well as the diversity of our development expertise. They were looking for a partner who could help them support a Python-based back end, distributed cloud infrastructure, and orchestrated instances. Now our team works alongside QA specialists and our client's in-house development.

2. Providing timely and efficient support to platform end users

The client's platform is constantly growing and attracting new users, which led to more support tickets. We help the client's in-house team process these tickets on time by fixing bugs detected by end users, implementing per-request features, and making overall improvements to the SaaS cybersecurity platform.

In particular, we have:

- ***Developed functionality for uploading and managing custom firmware.*** End users can work with custom equipment to scan their firmware for vulnerabilities and manage security information in the SaaS platform.

- ***Added custom Jira integration.*** End users can gather all information about discovered vulnerabilities in Jira.

- ***Improved the product's user interface (UI).*** We implemented several changes suggested by end users that make the platform's UI more comfortable to use.

These improvements allowed the client to reduce the average ticket processing time and improve user satisfaction with the product.

3. Improving efficiency of the in-house team by automating internal processes.

The client's sales and business analysis team constantly collects a lot of information about their platform: common user interactions, use cases, most searched for vulnerabilities, etc. Gathering such data manually took a lot of time for specialists, so the client asked us to look into automation options.

We introduced automation algorithms that enabled the platform to gather and analyze data with little human involvement. The features that we added helped our client free the time of business analysts and sales specialists and allowed them to focus on more complex and valuable tasks such as delivering several internal and external web apps.

4. Meeting compliance requirements in end users' industries

Many of the platform's end users come from highly regulated industries like healthcare, automotive, and cybersecurity. Companies in such industries often work with highly sensitive data and must comply with numerous laws and regulations. To be able to work with such companies, our client has to comply with these laws and regulations as well as industry standards.

Since Apriorit has experience working with regulated industries, our client often consults with us on compliance issues. We have used our experience to:

- Research new vulnerabilities and ways to detect them
- Implement discovered detection methods on the client's platform
- Add audit logs for management-related events and actions
- Increase the number of available data analysis mechanisms, including password-finding and password analysis mechanisms

Our industry-related expertise helps the client keep their cybersecurity platform up to date with current compliance requirements. Our thorough and proactive approach to compliance helps our client attract new customers that work with sensitive data.

The impact

Our collaboration has allowed the client to make their platform more stable and competitive by fixing bugs and introducing new features. End users appreciate the quick fixes of reported issues and overall UI/UX improvements.

We continue to work closely with the client to understand their workflows, values, and priorities. Constant involvement and communication has allowed us to truly become a part of the client's team. Thanks to this, the client can focus on improving their platform without disruption to their internal processes.