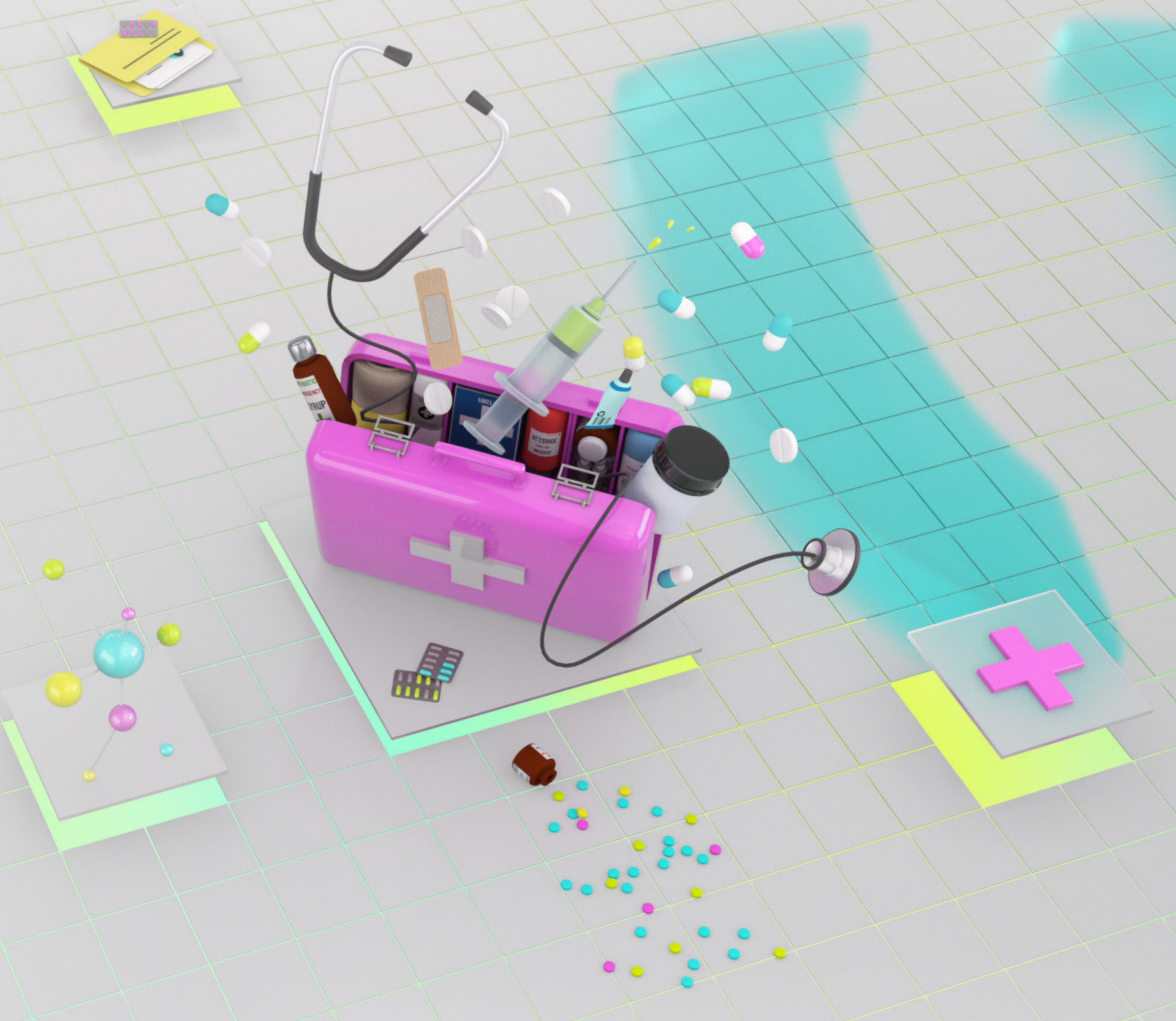
ADAPTIVE
SHIELD

SaaS Security in Healthcare

How the European e-Health Leader Implemented an Agile and Robust Program at Scale

Doctolib SUCCESS STORY



About Doctolib

Since 2013, Doctolib has been committed to one objective: Building the healthcare we all dream of, together with caregivers and patients. Doctolib powers 430,000 healthcare practitioners and helps 90 million people throughout Europe. With over 3,000 employees, Doctolib has a presence in more than 30 cities across France, as well as in Germany, Italy, and the Netherlands.

The company has a very large and mature security team, with three departments that focus on different areas of security: Product Security, Corporate Security, and Platform Security. SaaS security is led by the Corporate Security Team, which has a requisition security process in place to manage the onboarding and ongoing maintenance of all business-critical applications.

The SaaS Security Challenge

Doctolib originally used manual processes to manage and secure its SaaS applications, which resulted in a limited snapshot of its security posture. As the company adopted more apps, it realized that its current security and compliance management approach for the heavily regulated healthcare industry was inefficient and unscalable.

The Corporate Security team needed continuous visibility into configurations to ensure that the app remained secure and in compliance with relevant regulatory requirements. They also needed a better understanding of the thousands of users who accessed the applications and the third-party applications that were connected to improve functionality or workflow.

Other SaaS issues crept up.Teams were starting to onboard applications without the knowledge of the security team. The company recognized the need to improve collaboration with its business units if they hoped to tame “an untamable jungle” of SaaS apps.

At the time, Doctolib managed its cloud infrastructure with a Cloud Security Posture Management (CSPM) solution. They sought an equivalent solution to manage their rapidly growing SaaS stack.

SSPM Evaluation Process

In 2022, Doctolib conducted an RFP with all three leading SaaS Security Posture Management vendors. During the Proof of Concept (POC), they connected their most sensitive and complex applications to Adaptive Shield's SSPM platform.

After an extensive evaluation comparison process of all leading SSPM solutions on the market, Doctolib selected Adaptive Shield as their partner of choice. Adaptive Shield supported far more integrations out-of-the-box to provide full SaaS coverage, and its security checks were the most comprehensive. Adaptive Shield's platform was the only one that associated users with their devices, had an intuitive UI/UX, and simplified collaboration between the security team and app owners.

> With Adaptive Shield, we quickly implemented a strong zero trust policy across our entire SaaS ecosystem. The platform continuously strengthens our SaaS security by honing in on individual misconfigurations, governing identities, detecting shadow apps, and providing visibility into SaaS user devices."

François-Xavier Le Quéré
Corporate IT Senior Security Engineer at Doctolib

Kickstarting a Successful SaaS Security Program with Adaptive Shield

Doctolib went live with Adaptive Shield at the beginning of 2023. In an instant, the security team went from snapshot visibility provided by manual audits to continuous, deep visibility of all its critical applications. Adaptive Shield's Customer Success team assisted with the onboarding process, helping Doctolib define goals and KPIs, follow best practices, and involve the right personnel at each stage.

In addition to the top apps that were monitored during the POC, Doctolib quickly integrated all SaaS applications into the platform via API. For the first time, the organization could easily monitor users and their permissions and the third-party applications that were integrated into its SaaS stack.

Device management was a critical concern to Doctolib. Adaptive Shield's Crowdstrike integration enabled security team members to view Crowdstrike's zero trust scores and device critical vulnerabilities (CVE), while the device inventory associated each device with a user.

The security team granted its critical stakeholders access to the Adaptive Shield platform, including the GRC, Endpoint Management, Risk & Vulnerability Management, and SecOps teams, so they could regularly monitor their domains. They also onboarded Application Owners, to help them better understand the security issues impacted by configuration choices and collaborate with the security team to remediate issues.

Process and Results

Using Adaptive Shield, Doctolib drastically strengthened the posture of its SaaS stack in no time. It uses the platform on a daily basis to manage all aspects of SaaS security. The company was able to identify and mitigate misconfigurations that put its applications at risk and align app settings with compliance standards. In addition to the out-of-the-box security checks, Doctolib has created over 40 custom security checks to help align its applications with the company's security policy.

By monitoring users through the platform, Doctolib improved its deprovisioning capabilities, fully removing access from employees who were offboarded from the IdP, yet still had access to different SaaS applications.

Over the last year, Doctolib has continued to enhance its posture through Adaptive Shield's two new inventories. The Permissions Inventory provides them with granular visibility into user entitlements and access, allowing them to right-size user access. Meanwhile, the Data Inventory shows which files are shared publicly, helping them limit the potential for data leaks.

Today, Doctolib monitors a large number of integrations through the Adaptive Shield platform. The company strives for a 100% security posture score on every application and has quarterly reviews with app owners to discuss any failed security checks. The company has come a long way in taming its SaaS jungle.

Moving Forward

With their SaaS security prevention tools performing effectively, Doctolib is now in the process of integrating threat detection and response mechanisms and placing automated workflows through incorporating them into SOAR/SIEM systems. Moving forward, Doctolib also plans to connect and monitor homegrown custom applications with the Adaptive Shield platform.