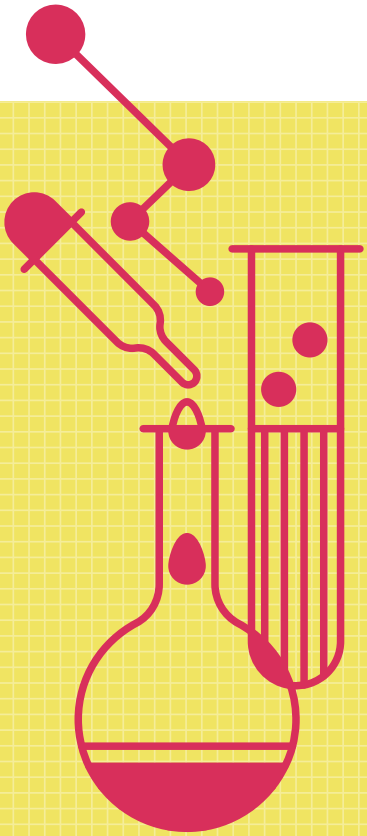
ADAPTIVE SHIELD

Case Study

Schrödinger

Schrödinger Increases SaaS Security Posture by 300% in Only 4 Months



About Schrödinger

For over thirty years, Schrödinger has been a leader in the pharmaceutical & biotechnology space and is the developer of predictive modeling software to accelerate pharma innovation. The company has doubled in size over the last two years, and currently has over 850 employees. In 2022, the company reported over $137M in revenue.

United States
New York

Industry
Pharma/Biotech

Employees
850+

Adaptive Shield's SSPM Offering Significantly Upgraded Schrödinger's Security Posture

The Challenge

As Schrödinger expanded, they increased their reliance on business-critical SaaS applications. The security team had used CASBs in previous roles but were frustrated by the high volume of false positives CASBs generated. Additionally, the team felt CASBs were expensive, created user friction, and added an unnecessary layer in securing SaaS applications. It left them exposed when dealing with SaaS misconfigurations, connected applications, Identity & Access governance, and risks deriving from SaaS user devices.

The team decided to dive into the security controls of each SaaS application. They would manually manage configurations and discover all connected applications. However, they quickly recognized this strategy was not scalable due to the large and ever-changing environment. The security team also realized they lacked visibility into each application, which were owned and managed by the business owners, and lacked context on how to prioritize and fix each configuration based on the level of risk.

> The Adaptive Shield platform helped us build and maintain a strong process in which we partner with the application owners, who are continuously engaged, to fix any security issues. Furthermore, it monitors each change, enabling the team to stay ahead of any configuration drift as it happens.

Jason Walton
Executive Director of Information Security

The Solution

Schrödinger turned to Adaptive Shield's SaaS Security Posture Management (SSPM) to monitor and manage the security of their SaaS stack. They were drawn to Adaptive Shield's leadership in the space, its robust platform's out-of-the-box SaaS-app integrations and capabilities around misconfiguration management and third-party connected apps.

Adaptive Shield's comprehensive security checks offered the type of insight Schrödinger needed for its SaaS stack. It quantified and deeply contextualized the level of risk in each configuration, and recommended settings that would improve the security posture for each application.

"The Adaptive Shield platform helped us build and maintain a strong process in which we partner with the application owners, who are continuously engaged, to fix any security issues," said Jason Walton, Executive Director of Information Security, Schrödinger. "Furthermore, it monitors each change, enabling the team to stay ahead of any configuration drift as it happens."

The platform also provided Schrödinger with visibility into connected applications. For the first time, the security team could easily monitor third-party applications and understand the level of risk posed based on the scopes granted to each app by employees.

Process and Results

Schrödinger deployed the Adaptive Shield platform and is currently using it to monitor 80% of the company's SaaS stack. When the platform launched, Schrödinger's initial security posture score was 20%. Within four months, the company dramatically improved its posture by 325%, to 85%, and is now able to maintain its high posture with minimal effort.

The team began by addressing high-impact misconfigurations that affected the most privileged users with access to the most sensitive data. Once those misconfigurations were managed, they focused their attention on settings that would impact larger sets of users. The security team took the same approach with third-party SaaS applications, identifying those apps with high permission scopes and a limited number of users. Once those applications were addressed, they turned their attention to other high-risk applications.

Schrödinger opted to remediate all issues within Adaptive Shield's platform rather than through external ticketing or alerting systems. Application owners have visibility into their own applications through RBAC (role-based access control), and have all the information they need to remediate misconfigurations and communicate with the security team. Today, Schrödinger uses Adaptive Shield to cover almost all of their SaaS stack, with plans to continue connecting newly acquired SaaS apps to the platform.

Moving Forward

Schrödinger is preparing to monitor additional SaaS applications through the Adaptive Shield platform and is planning to introduce Adaptive Shield's Data Leakage Protection and Threat Center to continue hardening its SaaS security.