CYE

Hyver Reduces Cyber Risk of File-Sharing **SaaS Provider** by 96%

A fast-growing consumer app company aimed to secure its users' privacy, but found critical gaps that weakened its cyber resilience.

The Challenge:

Minimize Potential Privacy Violations of Millions of Clients

Many successful SaaS companies are known for their fast growth. But growth is a double-edged sword; profits increase but so does responsibility and complexity. Companies with millions of clients must protect sensitive data, since failing to do so could result in data privacy regulatory fines amounting to hundreds of millions of dollars.

With a customer base of millions of active users, the client aimed to minimize the potentially massive business impact that privacy violations could cause.

The Solution:

Identify Attack Routes and Create Security Program

The client's CRO implemented Hyver to identify attack routes that put user privacy at risk and build a risk-based security program.

Hyver conducted a baseline assessment of the organization's security posture that covered the client's external attack surface, networks, and cloud environments. By analyzing findings across the client's attack routes, Hyver quantified the risk exposure according to likelihood and business impact.

Despite being a cloud-native, tech-savvy organization, the client had a massive attack surface and problematic policies and procedures that resulted in lower-than-average security maturity scores.

Excessive trust in early employees
Growing from seven employees to 7000 in six years, the client had to make fast organizational, IT, and security adjustments. Organizational culture adjustments took a backseat, and so did the principle of least privilege.

Hyver discovered this issue primarily in production environments, where early employees had access to everything. While this issue can lead to privacy violations, it can also lead to major disruptions, downtime, and breach of code integrity. Excessive trust in early employees is a major risk factor and is frequently seen in fast-growing SaaS companies.

Employee access to unlimited customer data
The second critical privacy finding was a lack of segmentation. To enable the business to move fast, the client allowed all employees to view every user's activity history and personal information. This provided malicious actors with thousands of potential entry points that could be used to obtain sensitive information.

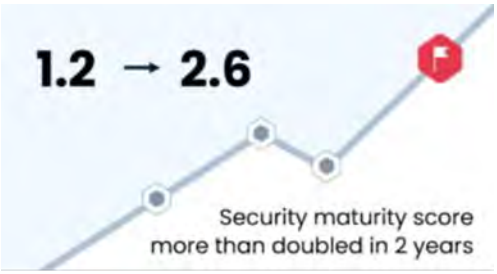
The Impact:

Dramatic Increase in Security Maturity and Robust Privacy

The conventional solution for both findings is a long-term architectural shift. However, since this can take years to design and implement, Hyver identified a short-term solution to reduce the risk exposure immediately.

Hyver focused on sensitive production environments. It limited the process so that only a few carefully selected individuals could conduct a code review and accept publishing changes. While this solution was a quick fix, it could not be a long-term strategy, as the individuals experienced a "review fatigue" and became (albeit intentionally) a bottleneck.

A second short-term solution was therefore implemented to segment employee access by region. With 26 countries, the risk was immediately reduced by 96%.



> **"It's nice to know our concerns are taken care of, which includes assets our team did not identify as top concerns. Hyver identified attack routes that boosted our maturity very fast and very efficiently."**
>
> The Client's Cyber Risk Officer

The conventional solution took longer—just under two years—to be fully implemented. Once the change was completed, the security maturity score rose dramatically, and the CRO's top concern about privacy was under control.

About CYE

CYE's optimized cyber risk quantification platform and expert guidance transform the way organizations manage cybersecurity. Using AI, machine learning, and innovative technology, CYE visualizes attack routes, quantifies, mitigates, and communicates cyber risk, and matures organizational cybersecurity posture. In doing so, CYE provides clear and relevant insights that empower companies to make effective cybersecurity decisions. The company serves organizations in multiple industries globally. Founded in 2012, with headquarters in Israel and operations around the world, CYE is funded by EQT Private Equity and 83North. Visit us at cyesec.com.

CYE