wallarm

miro | CASE STUDY

Miro Case Study

About Miro

Miro is the AI-powered innovation workspace that brings teams of all types together to collaborate more effectively to build the next big thing. It's their goal to help these teams go quickly from big ideas to execution through the delivery of a powerful and secure workspace that leverages AI at every stage.
But facilitating the collaboration that helps drive the creativity and intellectual property behind these organizations also comes with a responsibility to protect that data from malicious breaches and accidental or involuntary exposure. Wallarm has partnered with Miro to make sure their customers' data is secure around the clock while minimizing the operational impact on Miro so that they can stay focused on developing cutting edge capabilities and solutions for their rapidly growing user base.

More than **80M users** and **250,000 companies** collaborate in the Innovation Workspace

Several International Offices

G2 Leader

Founded in **2011**

Challenges

Miro has grown a thriving and dynamic business delivering digital collaboration and business transformation to organizations around the world. In order to gain and keep the trust of their customers, Miro has to not only deliver a stellar user experience that simplifies their work and accelerates innovation, they also have to ensure the safety and security of their customers' mission critical intellectual property.

With an AI-enabled and cloud-native enterprise platform powered by AWS, Miro needed a solution that would not only protect their customers' data, but also wouldn't have a negative impact on performance or the user experience. It also needs to fit into their current environment with minimal effort by integrating with their security, DevOps and BI solutions to adapt to their operating processes. And they wanted easy customization capabilities to ensure they were protected from rapidly evolving threats and zero-day attacks, without requiring extensive development cycles to write new detection rules.

Key Criteria

- Real time API and web application protection
- Zero day and API abuse detection
- Minimal impact on bandwidth
- Easy customization
- Integration with existing tools
- Minimal operating overhead

Solution

Wallarm was the first tool that Miro purchased to protect their APIs. One of the key drivers behind selecting Wallarm was its ability to provide real time API and web application protection, something that other vendors didn't do well at the time. Wallarm's flexibility was a key selling point early on. It allowed Miro to recognize immediate value through critical capabilities like DDoS mitigation, while also creating new rules to tackle other critical use cases, like bot enumeration. This ability to mitigate new threats quickly buys Miro engineers the time they need to deal with issues without having to worry about critical damage being done.

Evolving threat protection

Wallarm was originally implemented as Miro's only protection against DDoS and other web application attacks. It was their first line of defense, protecting them from a wide range of attacks without slowing application performance or impacting customer experience. Wallarm is specifically designed to deliver the kind of high performance, customizable protection that Miro requires, with the flexibility to provide continuous protection while adapting to Miro's dynamically changing security requirements. But as their business has grown, so has their security posture.

Miro now uses a multi-layered approach to protecting their web applications Wallarm is deployed in front of all of their services, behind the AWS WAF (application layer) & AWS Shield (infrastructure) which are deployed at the perimeter. Wallarm is more configurable than AWS, allowing it to detect a broader range of attacks more quickly. In the case of a high-volume attack like DDoS, Wallarm will detect it minutes before AWS and will provide the initial real time protection against the attack. Once the DDoS hits a certain volume and duration, AWS WAF takes over blocking the attack, allowing Wallarm to deliver detection and response for everything else with minimal impact on performance.

API Abuse/Zero Day Protection

Another critical capability that Wallarm delivers to Miro is protection from zero-day attacks and API abuse. When log4j was disclosed, Wallarm was able to quickly create specific rules to detect log4j attacks and was providing protection in under 3 hours. This was done without requiring Miro to create their own rules, delivering same day protection while removing a significant operational burden.

While Miro will sometimes create their own custom rules to address new and evolving threats, most of the time they are created for Miro by Wallarm. One of the greatest benefits that Miro cites about their partnership with Wallarm is the responsiveness of Wallarm Support Services, which helps them secure their APIs and applications with minimal effort.

Conclusion

Wallarm delivers real time API and application protection that can be easily customized to adapt to rapidly evolving attacks and zero day exploits, without requiring extensive time and effort from Miro's cybersecurity, engineering, or DevOps teams. By using Wallarm as a key component of their security posture, Miro can confidently deliver the API and web application protection that their customers demand to ensure that proprietary ideas, processes and collaborations are protected around the clock.

wallarm

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107