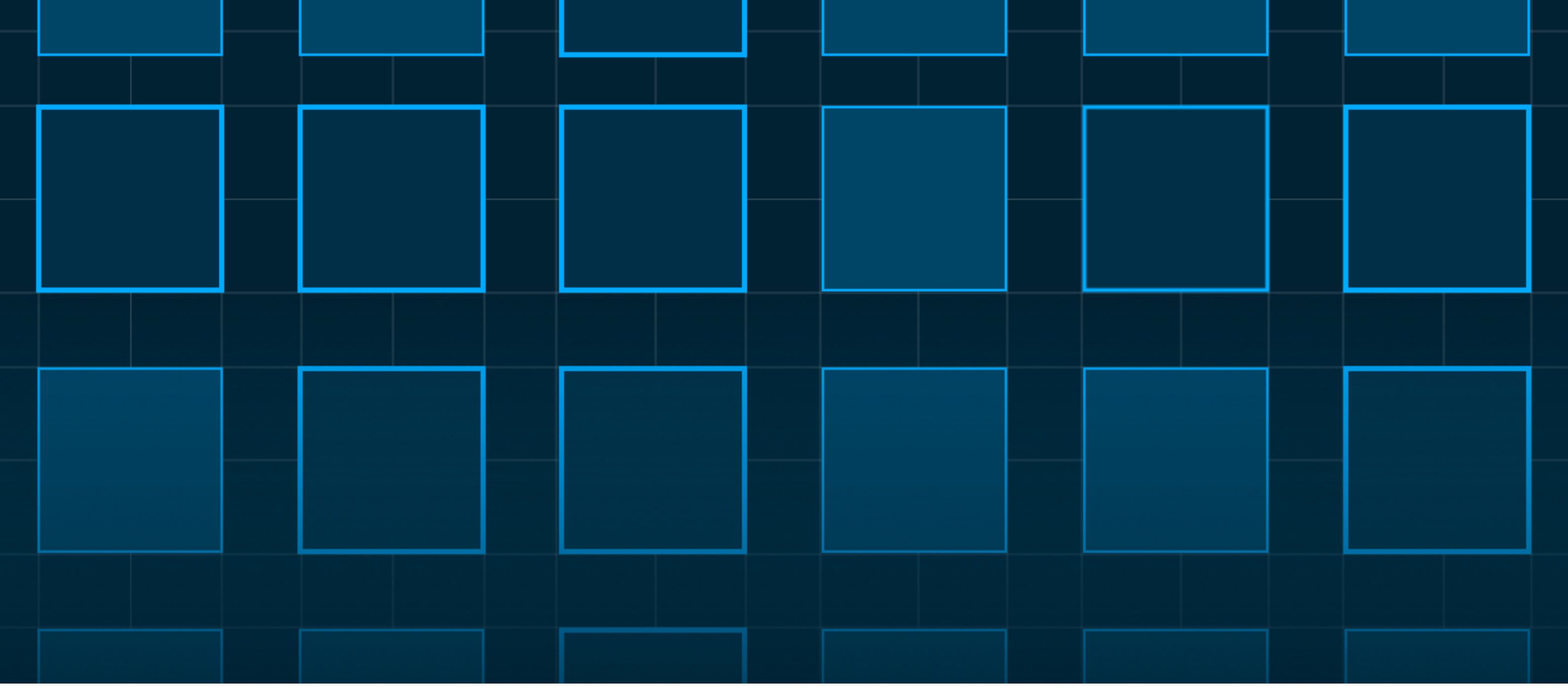

Your brand is safe with us

Bynder’s web application firewall

As part of our ongoing commitment to you and the security of your data, we have increased Bynder's security standards by implementing a web application firewall (WAF).

What does a WAF do?

A WAF monitors, filters, and blocks data packets as they travel to the Bynder web application or API. It adds additional security to protect both from common web exploits that may affect availability, compromise security, or consume excessive resources. By leveraging security features like DDOS protection or malicious URL filtering, the WAF monitors how traffic reaches the Bynder web applications or API. It applies sets of security rules that filter out specific traffic patterns and block common attack patterns, such as SQL injection or cross-site scripting.

How does it work?

A WAF analyzes Hypertext Transfer Protocol (HTTP) requests and applies rules that define which parts of each conversation are benign and which are malicious. Mainly, a WAF analyzes HTTP methods used when making HTTP requests, like GET and POST.

What does that mean for my organization?

It simply means that using Bynder is now more secure than ever. The advantage of using a WAF over traditional firewalls is that it offers greater visibility into application data that is communicated using the HTTP application layer. A WAF can prevent application layer attacks that normally bypass traditional network firewalls. Bynder already has a wide range of security measures in place for all customers, the WAF is specifically assigned to your portal(s) to add an additional layer of protection to it.

Implementing a WAF doesn't change the way in which our services are provided. For more information on this, please refer to our API documentation. https://bynder.docs.apiary.io/