Barracuda
Your journey, secured.

Go from zero to security in minutes.

Innovative SaaS-delivered WAF makes deployment and configuration fast and easy.

As your web presence becomes ever more critical to your operations, comprehensive application security is critical. But because of its complexity, it's too often overlooked, resulting in a chronic rise in data breaches.

Easy five step setup 1 Websites 2 IP Address 3 Backend Server 4 Select Mode 5 Change DNS

WAFs are notoriously complex to configure. For many businesses it is almost impossible to correctly configure a WAF without specialized resources. Even then, it may take days of work to get a WAF working in a typical production environment—a process that must be repeated whenever you deploy new or updated applications, resulting in unnecessary recurring costs.

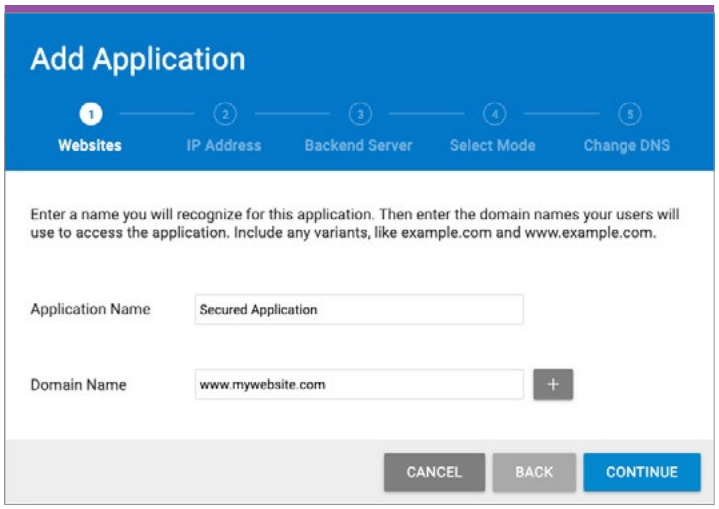
Barracuda WAF-as-a-Service brings the simplicity and ease-of-use of a SaaS model to application security. A simple, innovative 5-step configuration wizard gets you up and running—and your apps completely protected—in literally minutes. No specialized training or resources are required.

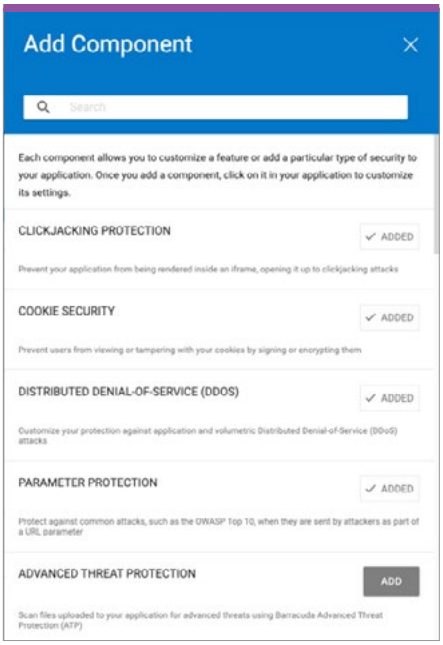
Barracuda WAF-as-a-Service has an amazingly simple and intuitive user interface, bringing application security within reach of every business. The configuration wizard is extremely easy to use.

At the same time, the solution makes no compromises when it comes to security features. Pre-configured policy templates secure most infrastructures, but you can also get hands-on, fine-tuning custom policy sets with highly detailed, granular control.

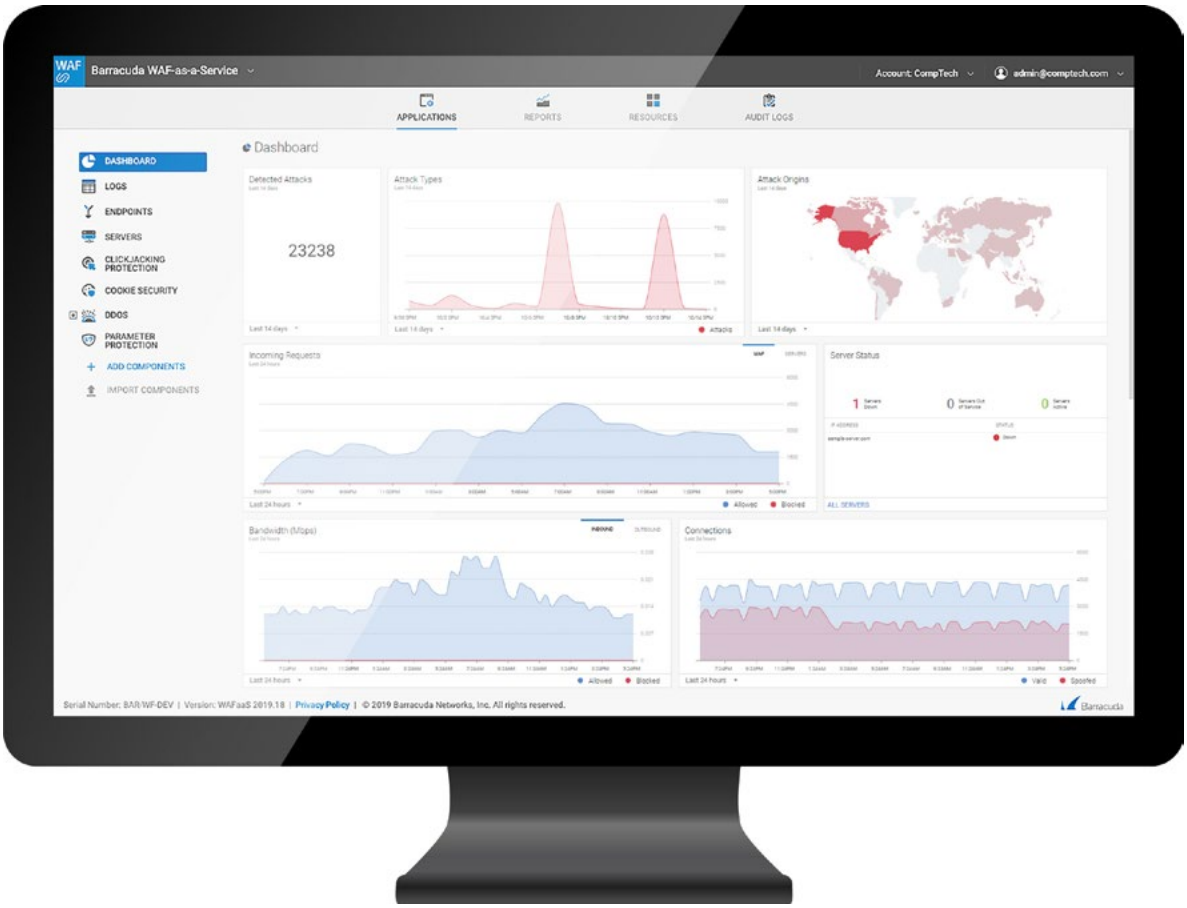
Facts about Web Application Firewalls (WAFs)

- WAFs are effective but complex solutions.
- WAFs traditionally require specialized training and resources.
- Misconfigured WAFs degrade user experience and impact business.

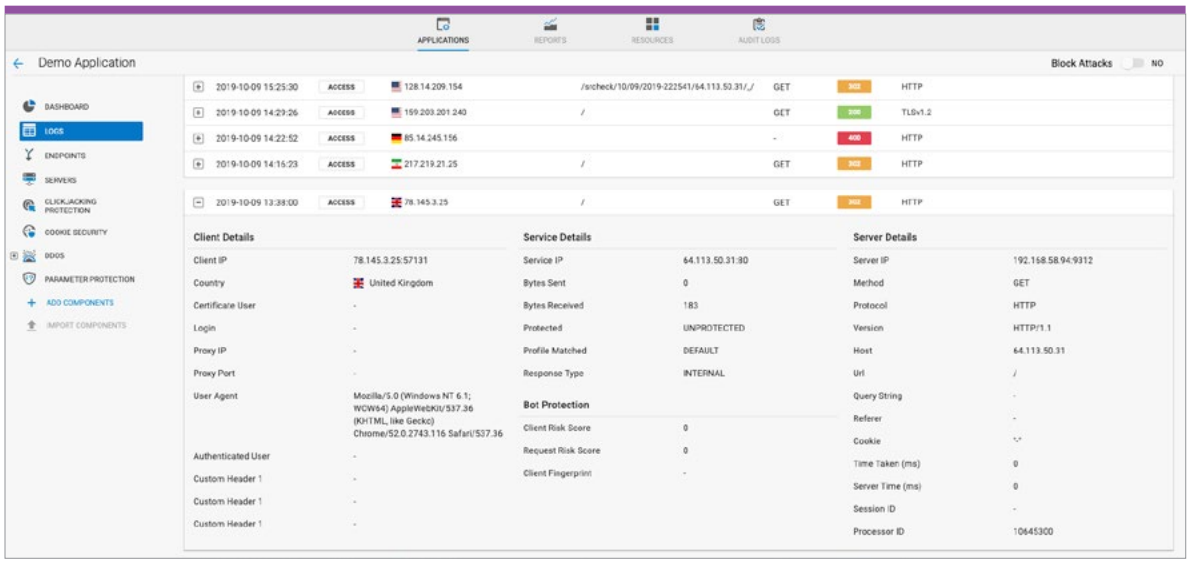




- The Add Component feature lets you specifically add only the components you need for more control, without cluttering the interface.
- Choose from dozens of components based on the specific needs of your application.
- Simply add the component and it will show up in the management interface, ready for you to configure.



- Rich analytics and logging capabilities give you critical information to support better security decisions.
- It's easy to drill down from high-level insights to highly detailed information when you need it.



Built-in DDoS protection

Unlike most WAF solutions, Barracuda WAF-as-a-Service includes full-spectrum L3 – L7 DDoS protection as an unmetered, no-extra-charge capability.

Simple yet powerful, Barracuda WAF-as-a-Service has the elastic scalability you need to secure a dynamic, changing app environment. It lets you take as much—or as little—control over policy details as you choose to.

Available add-ons for Barracuda WAF-as-a-Service

Barracuda's add-on offerings make WAF-as-a-Service even more comprehensive, by letting it detect and block zero-day malware and automated threats.

Advanced Threat Protection uses multi-layered and sandbox analysis to find and block advanced, zero-day malware and other threats.

Advanced Bot Protection delivers AI-based traffic scanning to detect and block malicious bots and automated threats while allowing legitimate bots and human traffic.

Barracuda
Your journey, secured.