# Web Application Firewall (WAF) FAQ

### Q: What does a Web Application Firewall do?

**A:** Generally speaking, a Web Application Firewall (WAF) is used to detect and protect web applications from attacks that try to exploit application vulnerabilities. To drill down on the explanation a bit, a WAF is responsible for inspecting the HTTP request and response based on predefined rules; processing preset actions against questionable HTTP requests/responses identified during the inspection phase or during the HTTP connection validity check; and logging the malicious HTTP requests/responses identified during inspection.

### Q: How does my WAF vendor acquire intelligence?

**A:** Neustar UltraWAF, in particular, relies on insights derived out of the Neustar Security Cloud and reliable third party sources, thereby providing a cohesive view to the threat landscape.

### Q: Who manages UltraWAF?

**A:** UltraWAF is intuitive and you can set it up to protect against the most common application attacks in minutes. Or if you would prefer, our dedicated provisioning team is available to assist you with UltraWAF configuration.

### Q: What is the false negative/positive rate on UltraWAF?

**A:** Every WAF is prone to false negatives and false positives. Unfortunately no WAF by itself will be able to tune out false negatives or false positives, but our SOC Provisioning Team will work with you to refine UltraWAF deployment and minimize the false positives or false negatives.

### Q: Does UltraWAF include protection against credential stuffing attacks?

**A:** Yes, Neustar UltraWAF provides always-on protection with flexible controls to mitigate brute force and credential stuffing attacks conducted by BOTnets.

### Q: Can UltraWAF virtually patch my application?

**A:** Yes. As the time to exploit a new vulnerability has declined from weeks to days to hours, being able to patch your applications against the newest vulnerabilities is critical to your security. Virtual patching with UltraWAF allows you to block traffic that looks to exploit vulnerabilities while giving you time to properly test patches in your environment. You can choose from thousands of pre-defined signatures that are frequently updated. If a signature is not yet available, UltraWAF allows you to define a customer signature based on SNORT or PCRE.

### Q: Can I create custom signatures?

**A:** Yes, if one is not available in the pre-defined signature list.

### Q:Does UltraWAF support an API?

**A:** Yes, all information available in the Web in the portal is abstracted through a publicly available version-controlled API. This includes configuration, reporting, and detailed violations logs

### Q: Is UltraWAF customizable based on the customers web applications?

**A:** Yes. We recognize that each customer environment is unique and not all applications may require all WAF security controls. UltraWAF can be customized for each unique environment.

### Q: Can UltraWAF work with existing hardware based load balancers?

**A:** Yes. One of the benefits of UltraWAF is that it's agnostic to your back end infrastructure, and works well even in cloud environments like AWS, Azure, etc.

**Q: How much traffic can UltraWAF support?**

**A:** UltraWAF is built upon our DDoS infrastructure which can handle up to 12+Tbps of traffic. This ensures our service can support a significant amount of traffic to meet your needs.

**Q: Does performance decrease when new/complex rules are added?**

**A:** No. UltraWAF does not impede performance as it is inline and has enormous scale since it's a distributed cloud platform.

**Q: Can UltraWAF integrate with my SIEM?**

**A:** Yes. SIEM integration can be achieved via the UltraWAF API that can take any and all log information in a structured format to allow the customer to easily integrate. Notification integration is also available via webhooks.

**Q: Can UltraWAF integrate with my ticketing system?**

**A:** Yes. UltraWAF can be integrated with ticketing systems via the UltraWAF API, webhooks, or email notifications.

**Q: What kind of Reporting does UltraWAF have?**

**A:** UltraWAF reports are available via the web portal or API and provide at a glance information about the most common attack vectors. Detailed violation logs and IP address enrichment provide important information about the source of the attacks. Reports can be exported into pdf, json, or csv formats as appropriate.

**Q: What kind of support does UltraWAF have?**

**A:** UltraWAF includes 24x7x365 phone/web/email support with direct access to our SOC engineers who can assist you with any questions you have about your configuration or attacks you may see.

**Q: Does UltraWAF provide detailed log information?**

**A:** Yes. UltraWAF logs all violations and makes header and user agent information visible for deeper investigation.

**Q: Does UltraWAF protect against BOTs?**

**A:** Yes. UltraBOT uses static and dynamic methods to detect malicious BOTs to keep your applications safe.

**Q: Does UltraWAF protect me against OWASP Top 10 attacks?**

**A:** Yes. UltraWAF protects against the most common application attacks including the OWASP top 10.

**Q: Can I create custom rules in UltraWAF?**

**A:** Yes. UltraWAF allows you to create many types of customizations including policy relaxation rules, rate and geo limits, custom signatures, as well as block and allow lists for IP addresses and known BOTs.

LEARN MORE

**Visit us here to learn more about how Neustar UltraWAF can support your security needs.**

Email: **security@team.neustar**

Call: **+1 855-898-0036 (US)** | **+44 1784 448444 (UK)**