Protect Web Apps and APIs on Azure with FortiWeb Cloud WAF-as-a-Service

Better security, less time and money

Legacy Web Application Firewalls (WAF) can’t keep up with a fast-changing world.

FortiWeb Cloud WAF-as-a-Service for Azure cuts costs and frees up time while improving protection.

The sad state of application security

43% of WAFs were disabled in Q4 2020, with 60% of those disabled for more than six months.

50% of WAFs had less than 5% of traffic being monitored.

The hours your team spends on…

Fortinet can save with…

Fault tolerance
Highly resilient cloud-based architecture

Load balancing
Integrated load-balancing engine

Capacity planning
Automatic scaling to match your app's needs

Manual tuning and configuration
Machine learning that adapts on the fly

Compute, network, and storage infrastructure for on-premises WAF

Managing false positives
Intelligent threat detection that eliminates false positives

Liberate the time and talent of your team

Managing legacy WAF requires an average of…

2.5 security administrators per week processing WAF alerts

45 hours per week tuning and configuring existing legacy WAF

16 hours per week writing new rules

Are you overspending on your WAF?

Average annual legacy WAF spend

$200,000

3 ways FortiWeb Cloud WAF-as-a-Service for Azure reduces your cost

Eliminate the need to over provision idle capacity to handle spikes.

Dramatically reduces manual configuration and management.

Provides CDN, Bot Mitigation, DDoS and API protection built in with simple, all-in-one pricing.

FortiWeb Cloud WAF for Azure makes business sense

Take it from our customers

We’ve found that FortiWeb WAF is a reliable and stable solution. The product is easy to manage, with a friendly GUI interface. Unlike other products, it uses machine learning, so it can identify users’ normal behavior.

Try FortiWeb Cloud WAF-as-a-Service for free on Azure Marketplace

Get started today