wallarm

How Wallarm can address Fintech Security challenges

98%

98% of the world top 100 Fintech startups are vulnerable to web & mobile application attacks

97%

97% of the mobile applications tested have at least two medium or high-risk vulnerabilities

56%

56% of mobile applications backends have serious misconfigurations in privacy issues related to SSL/TLS configuration & insufficient web server security hardening

62%

64% of the Fintech main websites failed PCI DSS compliance test

64%

64% of all Fintech main websites failed GDPR compliance

97/100

97 of 100 of the largest world banks are vulnerable to web & mobile attacks, enabling hackers to steal sensitive data

XSS

The most common website vulnerabilities are cross-site scripting (XSS), sensitive data exposure, and security misconfiguration – all are part of well-known OWASP top 10

Sources:
https://cynation.com/fintech-startups-struggle-to-battle-cyber-attacks/

wallarm

How Wallarm WAF can address web & applications security:

Ultra-low False Positives

98% of Wallarm customers use Wallarm WAF in fully blocking mode

Hear signal from the noise

Distinguishes real vulnerabilities from millions of irrelevant attacks

Easy to manage

Discovered Vulnerabilities are prioritized & reported in the Wallarm console UI & also can be dispatched to any supported integrations like Sumo Logic, Rapid7, Splunk, Slack, e-mail, OpsGenie, PagerDuty

Proven Enterprise scalable solution

hundreds of Fortune 500 customers supported

Hybrid architecture

Integrate Web & API protection right into publicly exposed endpoints without extending security perimeter. Wallarm cloud-based analytics backend allows to dynamically monitor WAF behavior and automatically adjust it to minimize false positives

Build-in Scanner

Allows to monitor the perimeter and find security issues in real-time

Platform agnostic

Bare metal, cloud providers, K8s, your own platform, or a mix of everything

Public Cloud friendly

Available as images on AWS & GCP

Machine Learning

Dynamic blocking rules instead of static signatures for each application. Continuously updated API-specific signature-free security rules generated by AI

External vulnerabilities scanner

With more than 120 security feeds connected

DevOps friendly

Chef, Puppet, Ansible, SaltStack, RESTful API for management

Low TCO

With Wallarm it will be easy to implement. You don't need any extra team effort except initial implementation. The rest of your cyber security protection will be done automatically

API protection

gRPC, REST, JSON, XML, SOAP and dozens more protocols supported without any configuration

Multi-platform deployment options

NGINX, NGINX Plus, Kubernetes Ingress, Kong API Gateway, AWS, GCP, Docker, Envoy

Multi-tenancy management

("Single pane of glass" approach): Unified web panel and API to manage all deployed application firewall instances. Perfect for large Enterprises & MSP's

Start your own Wallarm WAF demo at: **sales@wallarm.com** **www.wallarm.com**