TATA COMMUNICATIONS

# UNDERSTANDING WEB APPLICATION AND API PROTECTION (WAAP) FOR ENTERPRISES

## The challenges of securing modern web applications

In a world where businesses are digital-first, web services and apps are the most visible part of a business. As a result, they are relentlessly targeted by cyber criminals. The ever-increasing need for web applications and APIs, increases the complexity making them prime targets. Organisations grapple with a multitude of challenges in safeguarding these digital assets.  Some key challenges one encounters in protecting web apps and APIs are:

- **Lack of expertise:** Many organisations struggle to find and retain skilled cybersecurity professionals capable of implementing and managing sophisticated security solutions.
- **Complex security stack:** Managing multiple point solutions for different security needs can be overwhelming, leading to inefficiencies and increased costs.
- **Sophisticated cyber threats:** The increasing frequency and complexity of cyberattacks, such as DDoS, SQL injection, and API vulnerabilities, pose significant risks.
- **Regulatory compliance:** Adhering to evolving data privacy regulations like GDPR and CCPA while maintaining business operations is a daunting task.
- **High Total Cost of Ownership (TCO):** Investing in security infrastructure, personnel, and incident response capabilities can be expensive and time-consuming.

## The growing menace of web attacks

Here are some worrisome numbers:

- **94%** of applications had SQL injection vulnerability
- In 2022, DDoS attacks increased by **273%** YoY
- **92%** of organisations experienced API security incidents in 2022
- **90%** of web attack surface area are APIs

## The world is adopting WAAP

By 2026:

- **40%** of organisations will select a WAAP provider based on its advanced WAAP features
- > **40%** of organisations will consume WAAP using specialised providers, up from less than 10% in 2022

Source: Gartner

## The solution is Web Application and API Protection (WAAP)

***Cloud WAAP** is a category of security solutions designed to protect web applications irrespective of their hosted locations. Typically delivered as a service, cloud WAAP is offered as a series of security modules that provide protection from a broad range of runtime attacks* - **Gartner**

## How does WAAP work?

It works by using data from a wide array of threat intelligence sources. WAAP technology inspects and analyses incoming HTTP traffic at the edge of the network to identify and mitigate attacks such as SQL injection, distributed denial-of-service (DDoS), credential stuffing, API-based attacks, and many other forms of cybercrime.

TATA COMMUNICATIONS

## The core modules of WAAP

A comprehensive WAAP solution encompasses several key components to provide robust protection for your web applications and APIs:

**API protection:** Safeguard your APIs from unauthorised access and abuse through features like API discovery, inventory, and security posture management. Utilise advanced techniques such as automated traffic pattern learning and integration with OpenAPI specifications to ensure optimal protection.

**DDoS protection:** Defend your applications against a wide range of DDoS attacks, including volumetric (Layer 3,4), protocol, and application layer assaults (Layer 7), by leveraging advanced mitigation techniques and AI-driven threat detection.

**Web Application Firewall (WAF):** Protect your web applications from common vulnerabilities like SQL injection, cross-site scripting (XSS), and other exploits through advanced behavior analysis and AI-powered threat intelligence.

**Bot management:** Differentiate between legitimate and malicious bot traffic, preventing scraping, fraud, and other harmful activities while allowing beneficial bots to access your website.

## Deployment options for your WAAP solution

Choosing the right deployment model is crucial for optimising your WAAP strategy. On-premises deployments offer granular control but often come with higher costs and potential latency. Cloud-based solutions provide scalability and cost-efficiency but might introduce security concerns due to reliance on third-party providers. Hybrid deployments balance these factors by combining the strengths of both approaches. Carefully consider your organisation's specific needs, including security requirements, performance expectations, budget constraints, and IT resources, to determine the optimal deployment model for your WAAP solution.

## Top 5 best practices to consider when implementing a WAAP solution

Implementing a WAAP solution requires careful planning and execution to maximise its benefits. By following these best practices, organisations can effectively protect their web applications and APIs from evolving threats.

1. **Know your enemy:** Conduct a thorough threat assessment to identify potential vulnerabilities and tailor your WAAP solution accordingly.
2. **Build a strong foundation:** Establish clear security policies and procedures. Start with tier-3 or tier-2 applications as a proof of concept.
3. **Create a unified front:** Integrate your WAAP solution with existing security tools for comprehensive protection.
4. **Stay ahead of the curve:** Engage expert partners to continuously monitor your WAAP environment and adapt to evolving threats.
5. **Prepare for the worst:** Develop a comprehensive incident response plan to minimise the impact of potential breaches.

## WAAP will impact every industry

**BFSI:**

- Protect self-service customer web applications and portals
- Ensuring consistent application runtime

**E-commerce:**

- Limit server attacks and safeguard e-commerce transactions
- Secure payment gateways from DDoS and other attacks

**Manufacturing:**

- Secure both web and IIoT assets
- Detect and mitigate attacks to ensure supply chain continuity

**Schedule a consultation with our security experts now!**

**For more information, visit us at www.tatacommunicatons.com**

Follow us