

# Don't let your business get caught in the web

Anyone who needs to access a web application for work, wants to do so seamlessly and securely – so they don't put themselves, or the business, at risk. A web application firewall (WAF) filters, monitors, and blocks traffic to and from a web application to protect it from attack. By identifying typical usage patterns it can detect anything out of the ordinary. Our WAF solution uses superior Machine Learning and AI to protect your sensitive data and business critical web apps – helping avoid attacks and ensure industry compliance.

Many web-based applications are connected to databases with critical business information or personal data, making them prime targets for cybercriminals. Under new GDPR legislation, it's your job to protect sensitive data, but many companies don't have the security in place to demonstrate compliance.

Traditional network firewalls only offer protection at the network layer. They lack the sophistication required to protect against web-based attacks and unknown threats.

Finding, recruiting and retaining skilled resources to manage your WAF is costly and time-consuming, and if not done properly you're left vulnerable and open to attack. A managed service from BT allows you to free up your IT and security team. We will deploy, provision and monitor your web application firewall appliance ensuring you keep up with the latest threats.

Our Managed WAF solution is powered by Fortinet, the leading network and web application firewall provider. We offer a full implementation and in-life, round the clock support model for our solution, using a 'follow the sun' support approach. We can also optimise the service to make sure you get the reports you need to make the most of it.

## Improve web performance while safeguarding your brand

- **User experience**  
Cut application downtime and disruptive anti-bot measures to deliver a seamless user experience
- **Digital transformation**  
Increase the speed and agility of your web application growth to provide business benefits
- **Security**  
Eliminate data breaches due to web-application attacks
- **Data protection**  
Secure your internal and customer sensitive data sources
- **Service management**  
Focus on the needs of your business while we protect your business-critical web apps.

---

**43% of data breaches in 2019 could be traced back to attacks on web applications – more than double the results from the previous year<sup>1</sup>**

**20% of website requests are generated by malicious bots, capable of performing DoS attacks<sup>2</sup>**

1. Verizon: Data Breach Investigation Report, 2020  
2. ZDNet: Bad bots, 2019



# Filter, monitor, and block traffic to and from a web application

## Solution features

### Business application protection

Protect both internal and externally facing web applications by enforcing URL access and HTTP protocol constraints to sites and resources from outside protected domains – protecting against OWASP top 10 threats. And cut the number of false positives at the same time.

### Bot threat mitigation

Identify and block unwanted or malicious bot traffic that hits your application or network. This helps enhance the user experience by avoiding the need for verification. This feature protects against: scraping, account login abuse, fraudulent accounts and purchases, and other types of automated fraudulent behaviour.

### Machine learning

Our solution will automatically model web application behaviour to provide real-time protection for web servers. This means security teams spend less time manually tuning the WAF and creating exceptions based on false positives.

### DoS protection

Protect your networks against flood attacks by monitoring server requests and traffic sources. You can validate malicious IPs, limiting the number of connections users can make to a web application. This delivers a seamless experience across organisations and device networks for users.

### Man in the Browser (MitB)

Manual intervention from our Security Operations Centres (SOCs) helps protect sensitive user data from being snooped and stolen. This offers password field encryption and can scramble all susceptible field names.

## Why work with us?

We have teams of network security specialists spread around the globe, providing a 24 x 7 rapid reaction group.

### Benefit from a network of specialists

We've taken a strategic approach to ensure we deepen and expand our relationships with partners who complement our capabilities – to provide you with the best solutions we can.

### Application security management

We understand the challenge of both managing and securing business critical applications, from the moment of onboarding to the moment you're at risk of a security breach.

### Market leaders

BT is positioned as a leader in the IDC MarketScape for worldwide managed security services 2020 vendor assessment.

### Regulatory compliance

We're experienced in the compliance requirements that surround data regulation and can help you create policies that safeguard customer and employee information, ensuring you stay on track with your regulatory obligations.

## What could Managed Web Application Firewall from BT do for you?

Visit [bt.com/security](https://bt.com/security)

### Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract. © British Telecommunications plc 2020. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No: 1800000.

November 2020

