



## THIS IS WAF

### WHAT IS IT?

WAF is a acronym and stands for Web Application Firewalls. A WAF creates a shield between a web app and the Internet which can mitigate attacks.



### WHY SHOULD I CARE?

A web application firewall offers protection from layers 3 through 7. This is including network, transport, session, presentation, and application layers as well as cyber attacks.



### THIS IS HOW IT WORKS

A WAF operates through a set of different rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic.



### WHO IS IT FOR?

WAFs are useful to companies that provide products or services over the Internet such as e-commerce shopping, online banking and others and help your overall security environment.



### WHEN DOES IT MAKE SENSE?

If you want to maximizing throughput, ensuring the high availability of applications and API protection, protect you against bots, DoS or other cyber attacks, then a WAF is for you.



# VERSUS

## DIFFERENCE

### FACT 1

WAF solutions help to keep cyber attacks out of your organisations network by shielding your web applications.



### FACT 2

EDR solutions help to identify behaviour and activity on your endpoint to mitigate cyber attacks in your organization.



## //// Credits ////

This poster was created by Patrick in collaboration with Heike Ritter.

To learn more about Microsoft's EDR, go ahead and visit <https://aka.ms/mdatp>



## THIS IS EDR

### WHAT IS IT?

EDR stands for Endpoint Detection and Response. It records and stores behaviors, detect suspicious system behavior, provides information, blocks activity and provides remediation suggestions for the affected systems.



### WHY SHOULD I CARE?

EDR solutions automatically detect security incidents, contain them, investigate incidents and provide remediation guidance. It is a key pillar to everyone's security environment.



### THIS IS HOW IT WORKS

With a agent on the endpoint, this agent is monitoring and collecting data. With real-time analytics and when incoming data indicates a known type of security breach, it triggers an automatic response.



### WHO IS IT FOR?

Every organization and even every person should use an EDR solution as it is protecting connected devices in the organization's infrastructure.



### WHEN DOES IT MAKE SENSE?

In almost any scenario, an EDR solution makes sense especially as more endpoints are attached to networks within your environment to provide a overall secure endpoint.

