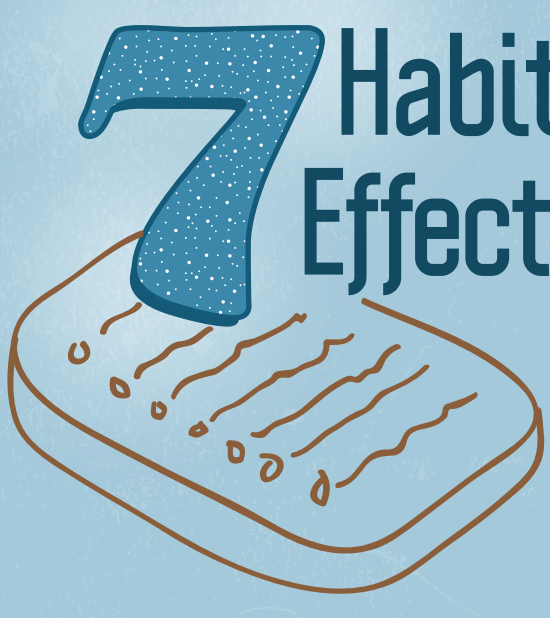
7 Habits of Highly Effective WAF

Web Application Firewall



Web application firewalls have been a critical part of securing external facing websites.

Organizations need to ensure that they deploy WAFs to ensure agile application layer protections. As network elements are unable to provide broad coverage for application layer issues, WAFs have become mandatory with the end security posture in mind.

This illustration helps you understand what you should be looking for in a WAF.

1 BE PROACTIVE

Key Paradigms According to **COVEY**

I am responsible for my behaviour and the choices I make in life

Key Application Security Paradigms

Vendor must provide WAF-as-a-Service, accept the responsibility of making WAF work for the customer, refine it as needed, and develop proactive defence mechanisms.

2 BEGIN WITH THE END IN MIND

Key Paradigms According to **COVEY**

I will create results mentally before beginning any activity

Key Application Security Paradigms

WAF vendor must configure the WAF rule-set to ensure minimal false alerts, goal must be to improve security posture without degradation of user experience

3 PUT FIRST THINGS FIRST

Key Paradigms According to **COVEY**

Focus on Truly important and say no to unimportant

Key Application Security Paradigms

Protecting against Critical known issues - Effective virtual patching - should be first priority of WAF deployments

4 THINK WIN-WIN

Key Paradigms According to **COVEY**

Effective, long-term relationships require mutual benefit

Key Application Security Paradigms

WAFs need to be able to demonstrate ROI while improving security posture of the application

5 SEEK FIRST TO UNDERSTAND THEN TO BE UNDERSTOOD

Key Paradigms According to **COVEY**

Diagnosis must precede prescription

Key Application Security Paradigms

Ability to provide detail forensics, logging any suspicious activities and providing enhancements based on application nuances is key feature of WAF core rule set improvement

6 SYNERGIZE

Key Paradigms According to **COVEY**

The whole is greater than the sum of parts

Key Application Security Paradigms

WAFs must be leveraged to develop a total application security posture, combine deployments of WAFs along with application scanning and secure coding practices to get a holistic application security program.

7 SHARPEN THE SAW

Key Paradigms According to **COVEY**

Results require constant improvement/development of resources

Key Application Security Paradigms

Constant update and monitoring of WAF Core Rules sets, getting intimate with application and user behaviour via forensics on legal/suspicious/illegal user actions