QUANN PROTECT

QUANN INTELLIGENT WEB APPLICATION FIREWALL

Protecting web applications against known and unknown threats using attack logic analysis

For many businesses, web applications are primarily the interface with customers. As businesses are now moving towards the digital landscape, web applications now play an essential role in today's business world. While businesses embrace web applications to meet business demands, they risk exposing sensitive data like customers' information or payment details to threat actors.

There is a rise in efficacy and volume of web attacks as threat actors evolve and prowl for their next victims. Vulnerabilities in web applications could potentially allow attackers to gain access to the company's web servers and piggyback on the connections that the web servers have to laterally move throughout their customers' networks, thereby stealing and infecting files. Therefore, it is critical for businesses to ensure that their web applications are properly protected.

As part of your defence against Web-Bourne attacks, it is necessary to deploy a web application firewall (WAF).

QUANN INTELLIGENT WEB APPLICATION FIREWALL

Quann Intelligent Web Application Firewall (WAF) leads the way in protecting servers, applications and data from web-based attacks. Our behavioural engine ensures accurate detection of known and unknown attacks. Instead of looking for known web attacks and malware, Quann WAF moves up the attack chain to evaluate and categorise the behaviour of all incoming traffic. This results in a higher rate of detection and a lower rate of false positives, using a high performance behaviour engine which allows higher throughput and a reduced need for signature administration.

Unlike other security applications, Quann WAF understands the various protocols for web-based applications to detect and defend against malicious web attacks.

Capabilities

- Protect against known and unknown threats
- Scale according to your needs
- Easy to deploy
- Have an intuitive management console for day-to-day operations

FEATURES

Patented Logic Analysis Engine

- No signatures are required to recognise malicious intent. All packets and exact matching on specific characters related to similar known threats are analysed and will be denied if matched.
- This provides comprehensive protection against the OWASP (Open Web Application Security Project) Top 10 vulnerabilities and ensures PCI-DSS (Payment Card Industry Data Security Standard) compliance.
- The engine also offers complete protection against all types of Level 7 Distributed Denial-of-Service (DDoS) attacks.

Highly Intuitive Administration Console

- The console's graphic user interface (GUI) makes it easy for administrators to establish security policies.
- Preset rules for various compliance and audit requirements can be enforced with a few clicks, making deployment easy.
- The policies need not be altered even if the web application has been modified or if new attacks arise as we do not use signatures.
- Administrators can easily access detailed logs of threats that have been detected and blocked.
- Administrators are able to customise the counter-threat actions based on factors such as the nature of the threat, origin and time period.

BENEFITS

Provides comprehensive protection for web applications

With the pre-defined models to ensure widespread protection against malicious traffic, the Contents Classification and Evaluation Processing engine is used to protect your business from unknown threats. This is an effective defence against HTTP DDoS attacks with extremely low rates of false positives.

Addresses stringent web security requirements without compromising performance

Quann WAF ensures that systems continue to deliver stable high-end performance even with strict security policy settings, through engine optimisation and by making use of in-memory computing capabilities and bonding technology to increase bandwidth.

Enables businesses to get up to speed quickly with web applications protection

The solution is easy to install and configure using an intuitive and easy-to-use GUI console, which also helps to reduce the time spent on web security management. Protection is activated immediately upon installation, with minimal changes required to existing systems.

Provides flexibility to support different configurations and enterprise requirements

Quann WAF can be deployed in reverse proxy, inline or high-availability configuration modes, with various hardware models that can support small, medium, or large enterprises.

Powered by

Penta SECURITY

QUANN

THE ART AND SCIENCE OF BEING CYBER SECURE

For more information, please contact us at **info@quannsecurity.com**
or visit our website at **quannsecurity.com**