REAL-TIME WEB APPLICATION PROTECTION.

vAWF DATASHEET

VIRTUAL WEB APPLICATION FIREWALL

vAWF virtual Web application firewalls provide industry-leading Web application attack protection, ensuring continuity and high availability of Web applications while reducing security risks.

Array's vAWF virtual Web application firewalls extend beyond traditional firewalls and intrusion detection systems to provide comprehensive protection for business-critical Web applications. vAWF not only detects the complex Web application attacks of today, but also blocks the attack traffic in real time without affecting the normal flow of business data traffic. In addition, vAWF provides extremely fine-grained attack detection and analysis capabilities while protecting against the most common Web application threats including SQL injection attacks, Web page tampering, Web site malicious code, and disclosure of sensitive information.

Array's vAWF virtual Web application firewalls protect against the most widespread attack mechanisms while providing active incident response to halt hackers in their tracks, with post-incident analysis and diagnosis to provide guidance for strengthening servers against future attacks.

Available for common hypervisors, the vAWF virtual appliances are ideal for organizations seeking to benefit from the flexibility of virtual environments.

Highlights & Benefits

- Next-generation Web application firewall operates on multiple levels to protect vital Web servers and applications
- Continuous scanning for Web application vulnerabilities and for SQL injection or cross-site scripting and other threats within applications
- DDoS protection via brute force attacks mitigation
- Active incident response including detection, blocking and prevention of intrusion and other attacks, including zero-day detection by abnormal behavior analysis techniques
- Post-incident diagnosis and analysis of security issues to reduce overall security risk and maintain Web site credibility
- Highly refined rules library includes sophisticated protections such as information disclosure protection, embedded Trojan detection and protection, protocol integrity detection, keyword filtering and much more
- Comprehensive Layer 1 through 7 protection for Web servers at the network level, including packet-filtering, URL-based access control, blacklist/whitelist and other protection functions
- Web page tamper-proofing through centralized management and control of all Web tamperproofing endpoints, with content monitoring, synchronization and publish functions
- Customizable feature library and flexible configuration model to meet the needs of complex Web applications
- Comprehensive management portal provides visualized monitoring at the system, hardware, attack and tamper-proofing levels
- Guided configuration with exception rules to reduce installation complexity and errors
- Comprehensive management portal provides visualized monitoring at the system, hardware, attack and tamper-proofing levels
- Role-based authentication at the administrator level to secure configuration and data and allow for auditing
- Logging and log analysis with graphical representation and easy export of logs and statistics

Specifications

Hypervisor Support

- VMware ESXi 4.1 or later
- KVM 1.1.1-1.8.1 or later

Virtual Machine Requirements

- 2 Virtual CPUs
- 2GB RAM