In every enterprise/Government—from finance, industry, telecom, IT, and media to government—the internet is reaching deeper into business than ever before. Previously time-consuming tasks are automated with websites, online storefronts, document management systems, inventory, e-banking, and other applications that streamline workflows. But these same technologies also create new opportunities for cybercriminals. In this web-tech world, a variety of web/mobile, as well as ERP applications, help us to run the day to day operations. With this rapid growth of applications, grows the security vulnerabilities that lead to damage in your business.

The Verizon 2019 Data Breach Investigation Report (DBIR) states 41,686 security incidents, of which 2,013 were confirmed data breaches.

Most vulnerabilities in web applications result from developer errors. Traditional scanners, intrusion detection/prevention systems (IDS/IPS), and firewalls can’t always detect these advance web application attacks.

With this, comes the Array Web application Firewall providing top-notch protection, ensuring continuity and high availability of Web applications while reducing security risks.

Array WAF 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. Array Networks WAF provides wide-range of protection against all internet attack types that have been recognized by OWASP (including Top 10 attacks) and WASC, including SQLi, XSS, and XXE, as well as against HTTP Request Splitting, Clickjacking, and complicated client-side attacks (DOM-based XSS).
Continuous, real-time protection

Instead of applying the classical signature method, Array Networks WAF analyzes network traffic, logs and users’ actions, creating and constantly maintaining a real-time statistical model of the application during normal operation. It uses this model to detect abnormal system behavior. Together with other protection mechanisms, this ensures zero-day attacks are blocked without any special adjustment needed within the client.

Focus on major threats

Array Networks WAF automatically detects attack chains — from spying to data theft or backdoor setup. Instead of security specialists working through thousands of potential attacks, they receive alerts on only the most serious risks.

Advanced L7 DDoS Protection

On the basis of application stress metrics (RPS, response time, and errors rate), Array Networks WAF not only detects L7 DDoS attacks but can also predicts and prevents them. DDoS attacks are predicted, and security engineers are notified so that they can proactively implement the action plan without any business disruption. Array WAF’s extended range of features eliminates the need for third-party DDoS L7 monitoring tools.

Bot Mitigation

The automatic profiling of user behavior allows quick detection of automated attacks. But, because Array’s WAF does not block search bots, it doesn’t prevent sites being indexed.

Data Leakage Prevention

Array Networks helps all the outbound traffic to be monitored. The sensitive data is blocked (masked) automatically, without any interference of humans.

Maximum confidentiality for end-user data

Administrators create special rules to detect sensitive data such as payment card numbers, passport information, insurance details, etc. Furthermore, rules can be used to mask the information from third parties or even from administrators using Array’s WAF itself.

Proactive defense

Proactive defense of queries, data, and cookies allows blocking attacks such as CSRF, even if the developers have overlooked the necessary security tools.

Effective integration

Effective integration into one’s company’s information security management system that in turn helps to provide advanced multilayer protection.

Protection against security bypass

Array WAF ensures protection from the majority of firewall bypass methods including HPC (HTTP Parameter Contamination), HPP (HTTP Parameter Pollution).

Compliance with PCI DSS

Compliance with PCI DSS and other international, national, and corporate security standards.
HOW IT WORKS

Array Networks Web Application Firewall™ uses a multilayer defense scheme with many specialized modules to provide precise and impenetrable protection of web, mobile, and ERP applications.

Modules & Engines

- **User Tracking** permits the administrators to analyze session data as well as the geolocation of the user account that helps to get access to the protected application. Furthermore, Array Networks WAF™ can detect multiple unsuccessful login attempts and link such incidents together to quickly identify and block brute-force attacks.

- **Web Engine** is used for rapid verification of susceptibilities probed by attackers. It is considered as a built-in Dynamic Application Security Testing (DAST) module for active fingerprinting of application components (CMS, Frameworks, Libraries).

- **Passive Scan** passively fingerprints application components (CMS, Framework, Libraries, etc.) and detects known (CVE-based) susceptibilities and data leakage.

- **Normalization** helps rebuilds HTTP data and headers according to backend web application fingerprints (Web server, Language, Frameworks) to prevent protection bypass by HPP, HPC, and other data manipulation attacks.

- **Third-party Integration**: Array Networks WAF not only uses built-in AV engine and sensitive data detection rules but can also be integrated with external antivirus and DLP solutions for industrial protection. To fight massive DDoS attacks, Array Networks WAF can report the bots’ IP-addresses to external anti-DDoS solutions, such as Arbor.

- **Rule engine** allows the creation of custom rules, including for all known CVE susceptibilities. With additional geolocation tuning, it supports the creation of blocking rules and exclusions based on particular geolocations, providing targeted protection against attacks from specific areas.

- **WAF.js** is a JavaScript module for protection against client-side attacks (XSS, DOM XSS, DOM Clobbering, CSRF). It runs in the user’s browser every time a protected page is opened. The module also protects against robot programs of varying degrees of complexity, even those that can execute JavaScript by emulating the browser. WAF.js also detects hacking tools that are launched by clients when accessing the protected application.

- **Heuristics.** Based on self-learning artificial intelligence algorithms, Array Networks WAF regularly tracks request attributes to detect known and unknown attacks.

- **Correlation** helps to reduce the number of alerts and to highlight important incidents based on application fingerprints, vulnerabilities, user tracking, and attack history. This also builds attack chain metrics to simplify forensics.

- **Data masking** ensures the confidentiality of end-user data such as payment card numbers, passport data, insurance details, etc. It also supports web applications to continue functioning normally until any minor defects detected in them have been fixed.
Avx Series Network Functions Platform

AVX Series Network Functions Platforms host multiple Array and 3rd-party virtual appliances, providing the agility of cloud and virtualization with the guaranteed performance of dedicated appliances. It can host up to 32 fully independent virtual appliances (VAs) including Array load balancing, SSL VPN, WAN optimization and WAF as well as 3rd-party VAs from leading networking and security vendors.

Designed with managed service provider and enterprises in mind, the AVX Series enables data center consolidation without sacrificing the agility of cloud and virtualization or the performance of dedicated appliances. Uniquely capable of assigning dedicated CPU, SSL, memory and interface resources per VA, the AVX Series Platform is one stop solution to deliver guaranteed performance in shared environments.

Deployment Options

Array Networks Web Application Firewall can be deployed as a virtual function on AVX hardware appliance. Listed below are the modes as to how Array Networks Web Application Firewall can be deployed:

**IN-LINE MODE**
The in-line mode consists of three deployment schemes:

- Reverse Proxy
- Transparent Proxy
- L2 Bridge (detection mode only)

Traffic is routed through Array Networks Web Application Firewall, that dynamically detects and prevents attacks. Administrators can easily and quickly switch between Transparent Proxy and L2 Bridge via the Array WAF web interface.

**MIRROR MODE**
A router mirrors traffic to Array Networks Web Application Firewall, which then detects potential threats and alerts your existing security systems.

**OFFLINE MODE**
Array Networks Web Application Firewall examines logs for evidence of previous attacks for forensic analysis.

Setup and Configuration

The listed capabilities help Array Networks WAF to setup and configure in no time.

1. **Standard WSC wizards and convenient interface**: Administrators can use standard CLI scenarios and Array Networks WAF’s intuitive web interface in order to finalize deployment settings.

2. **Automatic detection of protected resources**: While utilizing Transparent Proxy, Bridge, and Mirror deployment modes administrators don’t have to remember all protected resources as they are detected automatically. After the preliminary product setup is complete, the UI displays information about all protected applications.
3. **Flexible security policies**: Array Networks WAF includes pre-defined security templates which in turn helps administrators to quickly set up required security policies that are defined as:
   
   i. By level of security (high, middle and low)
   
   ii. By hierarchy (a general policy for multiple apps or individual policies for each separate app)
   
   iii. By function (allowing different policies to be applied to each part of an app such as the public-facing elements, personal account, administration interface, etc.)

4. **Flexible settings within security policies**: Array Networks WAF includes a unified base of rules i.e. automatically applied to all security policies. Administrators can also apply several other system actions like blocking or logging to each rule, depending on the criticality of the protected application. This means administrators can control the level of Array Networks WAF protection at a granular level while significantly reducing the time and effort required for such fine-tuning.

5. **Auto-restore for system configuration**: If the system configuration fails, previously saved settings can be automatically restored. All the manual effort is reduced here.

6. **Ability to specify stored data length**: There is no need to store all data if certain parameters are of little long-term value. Administrators can specify which parts of lengthy data (Request POST Data, Matched arguments value, Request / Response headers) should be stored.

Lastly, Array Networks WAF offers in-depth finetuning capabilities to meet the needs of any kind of security hierarchy:

- Each app or set of apps can be protected by one or many policies
- Each policy or set of policies can be regulated by one or many rules
- Each rule or set of rules can trigger one or many actions
- Once all the settings are configured, they can be saved as a template for future use, eliminating repetitive configuration tasks.

**High Performance and Availability**

Array Networks WAF is designed keeping the high availability in mind that helps to deploy in active-active or active-passive mode. Enterprises can benefit from the kernel load balancing built-in to Array Networks WAF, as well as using an external load balancer.

- **Active-Active High Availability**: Active-Active cluster can be integrated with external load balancers. It helps creating a highly-performant and reliable application.

- **Active-Passive High Availability**: Active-Passive cluster supports two-node operations with built-in load balancing. It can be integrated with external load balancers.
# Product Specifications – AVX Series

<table>
<thead>
<tr>
<th></th>
<th>AVX5800</th>
<th>AVX7800</th>
<th>AVX9800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted VNF/VAs</td>
<td>1, 2, 4 or 8 (16 without performance guarantee)</td>
<td>2, 4, 8 or 16</td>
<td>4, 8, 16 or 32</td>
</tr>
<tr>
<td>Max. L4 Throughput</td>
<td>40G</td>
<td>80G</td>
<td>160G</td>
</tr>
<tr>
<td>Max. SSL TPS</td>
<td>40K</td>
<td>53K</td>
<td>110K</td>
</tr>
<tr>
<td>Max. ECC TPS</td>
<td>28K</td>
<td>38K</td>
<td>76K</td>
</tr>
<tr>
<td># of CPU Cores</td>
<td>4 (8 vCPUs)</td>
<td>12 (24 vCPUs)</td>
<td>20 (40 vCPUs)</td>
</tr>
<tr>
<td># of Cryptographic Engines</td>
<td>144</td>
<td>144</td>
<td>288</td>
</tr>
<tr>
<td>RAM</td>
<td>64GB</td>
<td>64/128 GB</td>
<td>128/256/512 GB</td>
</tr>
<tr>
<td>HDD</td>
<td>2TB (4TB option)</td>
<td>2TB (4TB option)</td>
<td>2TB (4TB option)</td>
</tr>
<tr>
<td>1 GbE (copper)</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>10 GbE Fiber (SFP+)</td>
<td>4</td>
<td>8</td>
<td>8 or 16 (option)</td>
</tr>
<tr>
<td>40 GbE Fiber (QSFP+)</td>
<td>-</td>
<td>2 (option)</td>
<td>4 or 8 (option)</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Dual Power: 1U - 17”W x 19.875” D x 1.75” H</td>
<td>Dual Power: 2U - 17” W x 22.5” D x 3.5” H</td>
<td></td>
</tr>
<tr>
<td>Typical Power Consumption (W)</td>
<td>174</td>
<td>281 - 449†</td>
<td>533 - 581†</td>
</tr>
<tr>
<td>BTUs/Hour</td>
<td>484</td>
<td>788 - 1249†</td>
<td>1443 - 1550†</td>
</tr>
<tr>
<td>Dimensions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>Dual Power: 19.8 lbs.</td>
<td>Dual Power: 28 lbs.</td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td>Operating Temperature: 0º to 45º C, Humidity: 0% to 90%, Non-condensing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>Gold, Silver and Bronze Level Support Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warranty</td>
<td>1 Year Hardware, 90 Days Software</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

†Note: Power consumption values may vary depending on specific configuration and usage conditions.