Automated Vulnerability Detection System

AVDS (Automated Vulnerability Detection System) is a network vulnerability assessment appliance. AVDS locates and exposes security breaches and vulnerabilities and lists their exact location and description along with suggested solutions.

With each scan, AVDS will automatically find new equipment and services and add them to the inspection schedule. It then tests every active node based on its characteristics and records responses creating a network security baseline.

AVDS is able to scan all IPs automatically, or schedule tests for specific IP addresses or segments at specific times. Each scan includes the widest range of security tests available today.

Security Appliance

The AVDS Scanner is a 19” 1U rack mount appliance. The dedicated appliance design provides fast scanning and allows the security administrator to focus on performing vulnerability assessments quickly and directly, without the worry of administering an operating system or a disparate suite of tools.

- Easy setup–up and running in about an hour
- Self-contained appliance–no integration with your existing hardware required
- No software or agents to install
- Appliance OS is hardened against attack

Focused Reporting

AVDS standard reports provide a comprehensive analysis of all vulnerabilities found grouped by risk severity. Every detected vulnerability contains technical information specific to that risk, including a short summary, severity, possible impact, recommended solution and relevant information such as links to software vendor patches. An Executive Summary section includes an overall summary for quick assessment of discovered risks.

Key Features

- Scans servers, routers, firewalls, switches, phones, operating systems–anything that speaks IP
- No software or agents to install or maintain
- Flexible scan frequency: scheduled or on-demand
- Differential reports–quickly spot new vulnerabilities, changes from security baseline and track remediation efforts over time
- Automatic daily vulnerability database updates–stay ahead of the latest threats
- 24/7 unlimited phone support with access to the Beyond Security network of security experts

"We now have the ability to scan at any time. Regular vulnerability assessments scans are like having sonar on our own network. We always know what is going on around us."

–Mike Gutknecht
Network Engineer
Rayovac Corporation
**Web Site Security Audits?**

AVDS performs internal and external scanning of networks consisting of any number of servers, services, ports or IP addresses.

For security scanning targeted at web sites, web servers, shopping carts and all Internet-facing IP addresses, scans can be done by our hosted AVDS servers and the results combined with local internal scan results for a comprehensive vulnerability report.

**Managed Service Providers**

Easily integrate AVDS with your existing infrastructure. Installed in a Security Operating Center (SOC), ASP farm, co-location or as an outsourced service, AVDS can become a part of your service offering quickly and with minimal capital outlay.

“AVDS graphically, unobtrusively and with great detail demonstrated to me the situation of our network/firewall and web server after scanning our system with a huge range of tests. Reports were sent to me that were concise and clear and then the technical staff of Beyond Security talked me through the results of the scans, interpreting areas with which I was unfamiliar and suggesting simple and precise fixes. From the moment of my first contact with Beyond Security, I have been impressed and enjoyed their friendliness, clear talking, approach to confidentiality and technical knowledge.”

–Paul Sheriff
IT Manager
City of Geraldton

---

**Differential Reports**

Differential reports show changes from the previous scan. New vulnerabilities, open ports, running services or new/removed hosts are listed, as well as a summary of any problems resolved since the last scan. Differential reports are a valuable tool to monitor changes to the security baseline and track remediation efforts over time.

**Distributed Architecture for Large Networks**

For large networks (from 2,000 to 2 million nodes), AVDS employs a distributed scanning architecture to effectively scan and manage vulnerability assessment and tracking from a single administration console. Multiple AVDS appliances on separate networks can connect to a centralized management system for distributed scanning and consolidated report collection.
New Vulnerabilities

With an average of 310 new operating system and application vulnerabilities announced each and every month regular active network scanning is essential. An automated, ongoing vulnerability assessment and management solution is your best option for the assessment and management of corporate network vulnerabilities.

“\textit{The information provided in the reports is very clear and concise. It explains to engineers what the problem is, where to look for more information, and how to fix it. “With these reports we can be sure after every change to the network if we are making the right change in terms of our security requirements.}

“We tried the free services. But when we piloted AVDS, we saw zero false positives and the differential reports make Management Reporting easy. These features are huge. They allow us to focus on delivering ICT services instead of chasing down vulnerabilities.”

–Cody Phang
Head of IT for the Australian Government National Capital Authority (NCA)

Vulnerability Checks

<table>
<thead>
<tr>
<th>Scans</th>
<th>Sample Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications</td>
<td>Apache, Microsoft IIS®, Oracle WebLogic®, IBM WebSphere®, Adobe ColdFusion®, shopping carts</td>
</tr>
<tr>
<td>Databases</td>
<td>Oracle®, MySQL, Microsoft SQL Server®, Lotus Notes®, DB2®</td>
</tr>
<tr>
<td>Network Systems</td>
<td>Routers, Firewalls, Switches/Hubs, Remote Access Servers, Wireless Access Points, IPsec, PPTP, DHCP, DNS, LDAP, SNMP, VPNs, FTP, SSH, TELNET, Modems, Anti-Virus Systems</td>
</tr>
<tr>
<td>Languages</td>
<td>SQL, ASP, PHP, CGI, JavaScript, PERL, Ruby, .NET</td>
</tr>
<tr>
<td>OSI Layer 7 Apps</td>
<td>Web server, Database server, Mail server, FTP server, Proxy server</td>
</tr>
</tbody>
</table>

Features

- Scans unlimited IP ranges to identify active IPs
- Quick Scan feature provides ad-hoc scans within seconds on individual nodes or network segments
- Schedule automatic daily/weekly/monthly scans
- Differential reporting highlights and automatically tests newly added IPs, ports and services
- Powerful search engine–quickly filter and search reported vulnerabilities
- Distributed scanning architecture for large networks and multiple AVDS appliances with enterprise-wide scans and consolidated reports
- Scan Profiles can check large networks quickly for a small subset of problems
- Non-intrusive and consumes minimal bandwidth. Scan rate can be limited by administrator to control bandwidth requirements
- Web browser administrative interface
- Scales to 2 million active IPs
- Automated daily updates of threat database
- Vulnerability database supplied by SecuriTeam Portal (www.securiteam.com), a industry respected security clearinghouse with over 2 million visits annually and 8,500 online articles
- 24/7 unlimited phone support with access to Beyond Security experts

Penetration Testing Replacement

Many organizations are required to perform periodic penetration testing on their networks and web sites. These tests are intrusive and costly. Further, with the rapid rate new vulnerabilities are discovered, exploited and made available to the hacker community at large, penetration test results can be rendered out of date as soon as they are complete. AVDS provides results equivalent to most penetration testing procedures, on demand and at a fraction of the cost.
Scanning Performance

<table>
<thead>
<tr>
<th></th>
<th>Default</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate of Scan (Packets/Second)</td>
<td>300</td>
<td>35</td>
<td>1200</td>
</tr>
<tr>
<td>Number of Sessions per Scan</td>
<td>8</td>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>Throughput per Scan (Kilobits / Second)</td>
<td>60</td>
<td>6</td>
<td>240</td>
</tr>
<tr>
<td>Average Scanning Time</td>
<td>Scans a typical Class C network in ~12 minutes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Appliance Hardware Specifications

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Factor</td>
<td>1U 19&quot; Rack Mount (with Dell Rapid/Versa Rails) or Mini Tower</td>
</tr>
<tr>
<td>Processor</td>
<td>Dual Core Xeon E3110</td>
</tr>
<tr>
<td>RAM</td>
<td>2GB DDR2, 800MHZ, 2X1G</td>
</tr>
<tr>
<td>Hard Disk</td>
<td>250GB, 7.2K RPM, SATA, 3Gbps, 3.5-in</td>
</tr>
<tr>
<td>NIC</td>
<td>2 Gigabit Ethernet ports</td>
</tr>
<tr>
<td>OS</td>
<td>Linux (hardened)</td>
</tr>
</tbody>
</table>

Requirements

- IE 6.0 or later, Mozilla Firefox 1.5 or later (for administrative console)
- IP address on your internal network

Contact Us

For more information, visit [www.beyondsecurity.com](http://www.beyondsecurity.com) or call us at +61 401 778 124

For pricing details, contact us at [steveh@beyondsecurity.com](mailto:steveh@beyondsecurity.com)