Benefits and Features for AVDS Vulnerability Management Solutions

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

Beyond Security has extensive experience and a clear advantage with larger applications.

Our solution consists of Scanners that scan the network and a Management Station that produces reports and manages the scanners. No matter how many scanners you have, or how dispersed they are in your network, you can simply manage everything through a single Management Station.

Self Contained: For sensitive information all data can be kept in house, which means there is no need to send to a 3rd party portal for analysis.

Users Hierarchy: Several different user levels are available: SuperAdmin, Admin, User: from simple read only user accounts that can be defined to only look at specific network segments to superadmin that has full privileges.

One of our key advantages is that we can scale with the same hardware and scan from the smallest network to the largest network. Meaning that you can start with 1 or 2 scanners reporting back to the management station and as you grow you can add scanners as you need them with out losing any of your initial investment. Installing a scanner is as simple as defining an IP address and gateway. We have customers that have started like this and ended up with dozens of scanners.

The reason we can scale so well and can support such large applications is because our solution was designed originally for Internet Service Providers, to enable them to scan a whole country using only 1 management station. (Examples to ISPs that are using us: Sprint, TiscaliWorldonline).

Some of our unique features for large applications are:

- Excellent reporting: 1) Executive Reports, 2) Summary Reports using Vulnerability Scoring, 3) Trend Reports, and 4) Detailed interactive reports that are intuitive with powerful search engines.

  Enables quick analysis of large networks.

- Asset Management, and Remediation: Asset management allows you to change the weight of IP devices, and how they effect the overall score of a network. For example, if the IIS servers are more critical than your network printers, you can lower the weight of the network printers and how it effects the overall vulnerability score of your organization or the specific subnet.

  More efficient and quicker remediation, as the reporting is the most accurate in the industry and will show which are the most critical

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

vulnerabilities to concentrate on.

The ADVS Ticketing system can help you manage your remediation. Once a vulnerability is assigned a ticket, it will remain open until the vulnerability is resolved, providing a very important remediation verification process – All patches are verified.

- Business Processes: An especially powerful feature for large organizations that are spread out over a wide geographic area. It enables you to place your scanners anywhere physically in an organization according to Business Processes and report back scanning results, aggregating all the same business processes back to the Management Station. Business Processes can be either based on Organizational structure or Technology.

  For example, you may have Scanners geographically dispersed from branch1 to branch300 all managed by a Management Station sitting in the SOC at HQ. The scanners from these 300 branch offices are defined to scan the following Business Processes: Operations, Purchasing, and Sales, and HR from branch1 to branch300. Or you can choose to scan all Operations, Purchasing, or all routers, or all Apache servers. All scan information is reported back to the one Management Station. You can also have any combination of different Processes sent together as one report.

- Flexible Hierarchical configurations: Enables you to assign specific or any combination of Business Processes to an individual or group to manage. Our Hierarchical configurations are the most flexible in the industry, providing all the requirements and flexibility needed when configuring complex network applications.

  For example, you can have Bob handle Business process 1, and Jim handle Business Process 2. and if there is a corporate policy requirement you can prevent either one from seeing the other. Then you can have David, who is in charge only see both organizations. This allows for local responsibility and oversight from different levels of management, which is all independent from where the scanners are located, whether in different buildings or different countries.

  One of the largest banks in South America is using AVDS. They have a complex application, and are taking advantage of our Flexible Hierarchical features. They have scanners going over the internet and through VPN tunnels connecting branches and subsidiaries worldwide.

- Compliance Management: Automatic and manual compliance reporting. For quick compliance inventory for Security Managers. There is no need to work with other tables or management. Completely built in enables engineers to quickly determine what IP hosts are safe.
  - Automatic: When your host's vulnerabilities have been fixed AVDS will automatically mark the compliance column in your reports, clearly showing which hosts are compliant and which are not immune from vulnerabilities.
  - Manually: AVDS enables interaction with your report to mark/sign off on individual IP hosts that has been determined to be compliant.. You can mark off, according to your specific security policy.

- Location of scanners:
  - Scanners are sometimes physically segmented by VLANs, VPN, and firewalls. In order to scan across these kinds of networks you can

Request a Free Evaluation

Our free 30-day evaluation includes an AVDS appliance and unlimited testing of up to 2,500 IP addresses.

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.

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

Contact Us

For more information, visit
www.beyondsecurity.com

Or call:

Hilton Loewenstein

+27 (0)11 609 9495

hilton@sekureit.co.za

open up firewall ports to allow the server to reach the whole network.

- WAN connections, if you do not want to scan over the WAN, just spread scanners on the local networks and have them all send the results back to HQ.
- Mixed: If you are going to scan a small remote branch with a few IPs it might be worthwhile to go through a VPN or WAN (the scanning takes only 1020 KB/s, but if you are going to scan an entire class B then it is recommended to put a separate scanner at the remote location. ADVS is flexible enough to let you choose the configuration that works for you.

- Protecting your information:All communication is encrypted over 3DES (Triple DES), and can be passed over HTTP or HTTPS, depending on the organization security policy. If the security policy is to have the Firewall check the content of all communications then you can use HTTP, as HTTP is more FW friendly. Alternative, you can have an extra level of security with HTTPS.

- Proxy Configuration: If your network does not allow a direct outbound connection, you can point the scanner to a proxy server.

- Push or Pull: Depending on the configuration you can have the scanner initiate a download Pull for updates from the management server, or the scanner can initiate a upload Push to start the update.

  For example, if the scanner is sitting behind a NAT then the scanner will need to 'Pull' and download the update from the IS.

- More than just a port scanner:
  - Performs security enforcement functions: Detects and reports default / short passwords, diskey connections, unauthorized services open, like shareware music, etc.
  - Checks for vulnerabilities on web applications like Oracle, SAP.
  - Banner analysis, Behavior Analysis, Weakened Exploit.

- Integration: AVDS was designed for easy, and quick integration. It has a standard and open API, and stores all data in XML format making it very easy to integrate. Many of our large customers have integrated AVDS with such management platforms as Remedy, RT ArcSite, and HP OpenView.

- References: ITW & ITAU, over 50k IPs each. SourceCorp (IT outsourcing) has over 150K IPs.
  - ITW scans 400 business units. They have integrated AVDS into their management system.
  - ITAU: One of the largest banks in South America
  - SourceCorp: Using AVDS in 4 locations in the US, all scanning constantly and producing daily/weekly technical reports and quarterly reports to the CIO that are presented annually to the company's CEO.