AVDS Key Features:

- Accurate scanning with near-zero false positives to save you time
- Pricing structure allows wide scan ranges; pay only for active IPs
- Reports designed for ease of use and efficient mitigation
- Simple set up and upkeep for low cost of operation
- PCI, CIS, SOX, HIPAA, ISO compliance reporting included in every system
- No host-based clients or agents required
- Penetration testing alternative, at lower cost.
- Automatic, daily vulnerability database updates – stay ahead of the latest threats

A Complete PCI Solution

Beyond Security is an Approved Scanning Vendor for the Payment Card Industry (PCI ASV) and PCI certification can be included in every installed AVDS system.

"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

Automated Vulnerability Detection System

AVDS™ is a complete network and web application Vulnerability Assessment product family. Its testing is the most accurate available and its reporting delivers exactly the information needed to repair the vulnerabilities that are most likely to cause data loss.

It will map and score your network to show you in real time which network components are most vulnerable to attack and where to start prioritizing your resources to secure your network efficiently.

AVDS scans everything that 'talks IP', automatically. Each scan includes the widest range of security tests available today and the AVDS test library is expanded to include new vulnerabilities daily, with updates hourly.

High Accuracy

AVDS tests the behavior of network hosts by recording their responses to carefully crafted queries delivering penetration test-like accuracy. No more huge reports packed with hard to resolve false positives. Most AVDS customers never experience a false positive report.

Most VA/VM systems depend heavily upon checking version numbers to deduce a possible security issue. This results in high error rates. The AVDS test library consists of behavior-based tests - not version checking. Behavior in response to a query is the only means of testing all the factors that are required to prove that a vulnerability exists.

Simplicity of Installation and Maintenance

AVDS is delivered as a turnkey solution and was designed with the functions most frequently used at easy reach. Drill-down user interface architecture facilitates getting to complex features you may only occasionally need and report details that are only occasionally used.

'Automated' is not just a part of the name. AVDS was designed from the ground up by practicing security experts who have felt the pain of running overly complex scanning systems. AVDS will reduce the time you spend running a scanning tool (or tools!) and increase the time you spend eliminating real network vulnerabilities.

Low Cost of Operation

The testing accuracy and ease-of-use is matched with an easy to understand, common sense licensing plan to produce the lowest scanning cost per IP in the VA marketplace. AVDS licenses are based on active IPs. This give you the freedom to set up fewer scans that span wider IP ranges without taking a license hit for every IP in the range.

With AVDS you will spend less time chasing vulnerabilities that don't exist, less time maintaining your VA solution and your licenses will go a lot farther, allowing you to scan more of your network for less.

Integration

Included with every system are the ready to use modules and advanced API that allows AVDS to talk with ticketing systems, SIEMs, WAF and all other systems that may need vulnerability data. There are no additional fees or support costs for establishing and maintain integration with other security systems.

Web App Testing:

Scan web applications and networks with the same solution. The AVDS web-application module includes an integrated crawler that tests every page of your site and every possible entry point against every family of security risk. It is the most in-depth, automated testing tool available, testing for code vulnerabilities such as SQL Injection, XSS (Cross Site Scripting), File Disclosure, Remote File Inclusion, PHP/ASP Code Injection, and Directory Traversal.

MSPs:

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

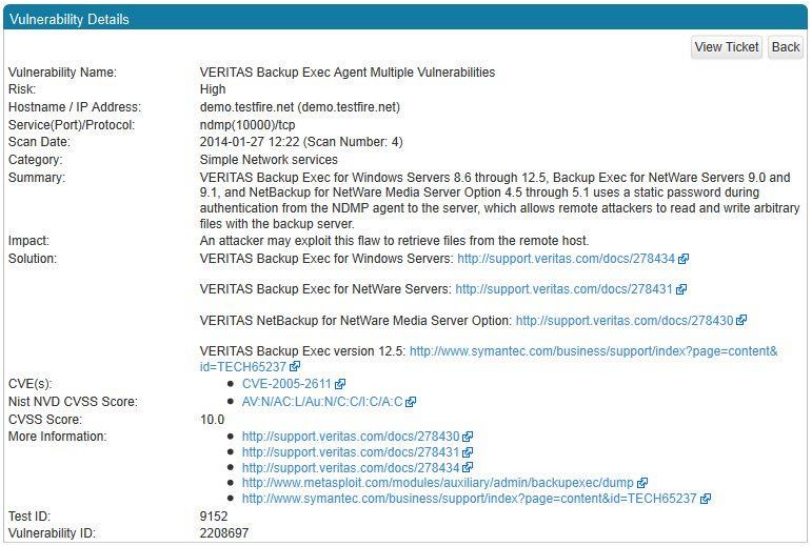
High Security

AVDS meets or exceeds the most rigorous corporate, government and military security standards for network scanning systems. It has been selected by Central Banks, Military units and Government entities in many countries to scan some of the most carefully secured networks in the world. No data of any kind is sent out of the network by AVDS. The operating system itself is a hardened, locked down version of Linux and all functions, including storage of results is self-contained. There is no known security requirement that AVDS has not met.

Focused, Actionable Reporting

AVDS standard reports provide a comprehensive analysis of all vulnerabilities found grouped by risk severity or by most severely compromised asset. Every report contains technical information specific to the risks discovered, including a summary, severity, possible impact, recommended solution and relevant information such as links to software vendor patches.

Reports are available on the management interface by browser with handy drill-down from the highest overview down to each individual contributing issue. Reports are provided in HTML, PDF, CSV, CIS and XML. An Executive Summary section includes an overall summary for quick assessment of discovered risks.



Vulnerability Details

View Ticket | Back

Vulnerability Name:	VERITAS Backup Exec Agent Multiple Vulnerabilities
Risk:	High
Hostname / IP Address:	demo.testfire.net (demo.testfire.net)
Service(Port)/Protocol:	ndmp(10000)/tcp
Scan Date:	2014-01-27 12:22 (Scan Number: 4)
Category:	Simple Network services
Summary:	VERITAS Backup Exec for Windows Servers 8.6 through 12.5, Backup Exec for NetWare Servers 9.0 and 9.1, and NetBackup for NetWare Media Server Option 4.5 through 5.1 uses a static password during authentication from the NDMP agent to the server, which allows remote attackers to read and write arbitrary files with the backup server.
Impact:	An attacker may exploit this flaw to retrieve files from the remote host.
Solution:	VERITAS Backup Exec for Windows Servers: http://support.veritas.com/docs/278434 VERITAS Backup Exec for NetWare Servers: http://support.veritas.com/docs/278431 VERITAS NetBackup for NetWare Media Server Option: http://support.veritas.com/docs/278430 VERITAS Backup Exec version 12.5: http://www.symantec.com/business/support/index?page=content&id=TECH65237
CVE(s):	• CVE-2005-2611
Nist NVD CVSS Score:	• AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Score:	10.0
More Information:	• http://support.veritas.com/docs/278430 • http://support.veritas.com/docs/278431 • http://support.veritas.com/docs/278434 • http://www.metasploit.com/modules/auxiliary/admin/backupexec/dump • http://www.symantec.com/business/support/index?page=content&id=TECH65237
Test ID:	9152
Vulnerability ID:	2208697

Differential Reports

Discover what changed on your network with each new scan. This popular report type will display new and removed hosts, the newest vulnerabilities, just opened, unexpected ports, newly installed vulnerable services, 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.

Custom Reporting Policies and Adjustable Scoring

Accurate Vulnerability Management requires flexibility in asset ranking and vulnerability severity scoring. Default reporting values in AVDS follow current best practices but allow administrators to adjust the relative importance of individual assets and/or vulnerabilities. Upgrade or downgrade specific assets or vulnerabilities and ensure that your remediation efforts are always focused on the right targets. Generate reports based on detailed company vulnerability policies.

Distributed Networks:

Handle hundreds of widely distributed business units from a single, central control point. Assign each security admin the rights to scan his own network, create and view his own reports. All scan results migrate up to the home office reports for a comprehensive overview of the security status of the entire organization and then drill down on how each unit is managing its assets and responding to local challenges.

New Vulnerabilities:

With over 300 new operating system and application vulnerabilities announced every month, regular network scanning is essential. An automated, ongoing vulnerability assessment and management solution is your best option for the elimination of all high-risk corporate network vulnerabilities.

"Previously, I have dealt with many (many) different scanning vendors in my 15+ years in IT-security. AVDS from Beyond Security is the first solution I could power up, configure and start doing useful scans within 15 minutes of my first session - awesome!"

Mikael Vingaard
Head of Research
Sec4IT

"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."

Cody Phang
National Capital Authority (NCA)
Australian Government

Penetration Testing Alternative

Penetration testing is the delivery of carefully crafted queries to secure a host or application response that proves the presence of a vulnerability. AVDS 'behavior based' focus does this with each scan, and replicates the efforts of a skilled security consultant. In fact, many consultants use AVDS as their primary discovery tool. A typical AVDS installation costs no more than an annual penetration test and has several advantages: Instead of one scan a year, do one a month at same cost and find new vulnerabilities months earlier; Automate testing to avoid the disruption caused by bringing in consultants; Get the same standard of testing every time, no variations in results.

Vulnerability Test Library

Beyond Security maintains its own complete library of behavior-based vulnerability tests that span the entire range of known network vulnerabilities. Updates to the library are done daily and every system in the world is updated hourly, automatically.

Scans	Sample Checks
Web Applications	All known web app vulnerabilities, such as SQL Injection, XSS (Cross Site Scripting), File Disclosure, Remote File Inclusion, PHP/ASP Code Injection, and Directory Traversal
Databases	Oracle®, MySQL, PostgreSQL, Microsoft SQL Server®, Lotus Notes®, DB2®
Network Systems	Routers, Firewalls, Switches/Hubs, Remote Access Servers, Wireless Access Points, IPsec, PPTP, DHCP, DNS, LDAP, SNMP, VPNs, FTP, SSH, TELNET, Modems, Anti-Virus Systems
Operating Systems	Microsoft® – all versions, Solaris®, AIX®, HP-UX®, SCO UnixWare®, BSD (OpenBSD, NetBSD), Linux – all distributions, AS/400®, VMS®, Mac OS X®, Novell NDS
Languages	SQL, ASP, PHP, Python, CGI, JavaScript, PERL, Ruby, .NET
OSI Layer 7 Apps	Web server, Database server, Mail server, FTP server, Proxy server

AVDS Features at a Glance

- Scan unlimited IP ranges and only pay for the active IPs on your network
- Network, web application, PCI, HIPAA, SOX and ISO in one solution.
- Quick Scan gets testing started in minutes
- Differential reporting highlights newly added IPs, ports and services
- Powerful search engine to 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.
- Web browser administrative interface
- Automated daily updates of threat database
- Vulnerability database supplied by SecuriTeam Portal (www.securiteam.com), an 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

Free Evaluation

Our free 30-day evaluation is available in most countries and includes an AVDS appliance with access to all features.

Compliance Features

AVDS reporting is designed to respond to PCI, CIS, SOX, HIPAA, ISO and all other compliance requirements. Beyond Security is an approved Scanning Vendor for the Payment Card Industry.

"We needed a way to discover and audit network assets, understand and prioritize current network vulnerabilities, then track and manage the remediation efforts over time. After a three month review of nearly ten different vulnerability scanning vendors we chose Beyond Security's AVDS. We had specifically selected AVDS because it would cause no disruption to our systems and required no installation of any new software on our systems."

–Gary Anton
VP of Strategic Sourcing and IT
Illinois Tool Works (ITW)

Contact Us:

www.beyondsecurity.com
sales@beyondsecurity.com

US: +1 800-801-2821

UK: +44 118-315-0005

France: +33(0)6 03 79 55 74

Korea: +82 70-8741-8885

China: +86 10-598-22245

India: +91 80-4040-7235

Singapore: +65 6850-5045

Scanning Performance

Given average network structure, a single AVDS scanner can test approximately 2500 active IPs a day at default settings. This default speed allows scanning production networks during working hours with no impact on user experience. Scan speed can be adjusted higher to get large networks completed during non-production hours.

	Default	Min	Max
Rate of Scan (Packets/Second)	300	35	1200
Number of Sessions per Scan	8	2	32
Throughput per Scan (Kilobits/Second)	60	6	240
Average Scanning Time	Typical Class C network in ~12 minutes		

Product Line

There is an AVDS product for every network and web application testing need. Hosted services are available for just a single web site. Network scanning product applications range from a single location with 100 active IPs to international corporations with hundreds of business units and hundreds of thousands of active IPs.

Product	Application
Hosted Scanning Service	Scan one or thousands of external IPs, PCI available
AVDSII	Up to 500 IPs in one network
AVDS	Unlimited IPs, networks, administrators,

Hardware and Virtual Machine Specifications

AVDS is available in a variety of form factors. The standard appliance is a 1U rackmount server. Portable units allow easy transport between business locations. Custom systems can be configured with any arrangement of redundant power supplies, RAID drive arrays and optical communication capabilities.

Form Factor	Components
Standard	1U 19” Rack Mount; Xeon E3-1220, 8GB UDIMM, 500GB SATA, 2 Gigabit ports,
Portable	7" x 7" x 1.4" / 18 x 18 x 3.5cm case, 3 Lbs., Pentium G4400T, 8GB DDR3L, 500GB SATA
Custom	2U 19” Rack Mount; Choice of processors, memory and redundant drives, ports and power supplies
Virtual Machine	For installation on cloud or existing servers

AVDS System Requirements

- Browser: Chrome, IE 6.0 or later, Firefox 1.5 or later (for administrative console)
- Appliance based installations require only an IP address on your internal network
- Power requirements vary by form factor, but all are Energy Star compliant