What's New in 4.4.0
==========
1. DAM - new platform support: DB2 LUW 9.5 and 9.7, MS SQL 2012, Teradata 14.
2. DAM+DVM - Server and sensor can run in FIPS 140-2 mode (certification pending). To configure FIPS mode see installation guide.
3. DAM+DVM - Server can run in 64bit mode (allowing you to use more than 2GB RAM). To run the server using 64bit JVM, install the server by running the setup executable with a /64 flag.
4. DAM - Added netIP and nethost identifiers - these identifiers show the network value of the host name and IP name (which in some cases differ from the values as reported by the DBMS).
5. DAM - Added the ability to alert when a minimum number of data rows is exceeded.
6. DAM - Exit codes (such as error codes) can now be reported and used in rules.
7. DVM - You can now run a report based on the last scan only (choose the filter named "last run results").
8. DVM - Added a new field to tests "memo". Unlike the description field, memo is not changed when the predefined tests are updated and does not appear in the test results.
9. DVM - Added the ability to filter and sort scans by the next run time.
10. DVM - default email scan action will send a summary of results. User can configure other ways of sending the results (e.g. email per result, change the email template, etc.).
11. DVM - when configuring a DBMS scan user, the user's privileges will be tested and an error message will be displayed when the user privileges are inadequate. The feature is not yet available for MySQL and PostgreSQL. The feature can be modified via custom properties.

What's New in 4.3.1
==========
1. DVM - Modify VA scan mail action - Scan summary will be sent

What's New in 4.3.0
==========
1. DAM - Support for Teradata 12, 13, 13.1
2. DAM - Support for MySQL 5.1 and 5.5 using a MySQL plug-in (see install guide).

What's New in 4.2.1
==========
1.DAM - Added the ability to send e-mail notification whenever a session termination occurs.
2.VA - Expanded XML API to include various vulnerability management tasks.
3.DAM - Fixed an issue where DML triggers were not created correctly on Oracle 9 platforms.
4.VA - Fixed a server performance problem that resulted in slowness when updating VA tests.

What's New in 4.2.0
==========
IMPORTANT NOTE FOR EXISTING CUSTOMERS: a new permission, “All OUs”, was added to the permissions scheme in preparation for a future enhancement. The new permission does not impact most users. However, if you have created users with limited database access, the new permission may impact these users’ permissions. Please contact technical support for further details.

1. DAM - added script signing, allowing signed transactions to bypass custom policy.
2. Reports - added dynamic systems reports mechanism and new preconfigured reports.
3. VA - Running database OS checks via SSH tunnel is now supported (see DBMS properties/advanced).
4. VA - Running database OS checks using a certificate is now supported (see DBMS properties/advanced).
5. VA - New limited VA scan permission allows limiting the user to clone/run/delete scans, selecting DBMSs and scheduling only.
6. General - added selective archive loading (load partial archives using a filter).
7. DAM - DBMS system report allows reporting on the dbms up time.

8. DAM - added revision differences report (see rule revision page).
9. VA - added new scan tests report, showing which tests passed and failed per scan.
10. General - added automatic backup of the HSQLDB backend database.
11. Scheduling - added the ability to schedule a single event.
12. DAM - Application Mapping added paging and sorting.
13. VA - PostgreSQL and SQL Azure now supported.
14. DAM - new property allows users to decide whether new vPatch rules will be enabled or disabled (vpatch.default.disabled=true or false).
15. VA - network scans can now be scheduled.
16. DAM - new support for active/passive clusters. This is enabled by default. When defining an active/active cluster go to DBMS properties and change the cluster to active/active.
17. General - added new filters in the DBMS screen.
18. General - password policy - added the ability to prevent the use of user name in the password.
19. VA - added export and import of custom tests and custom configuration of system tests.
20. General - added browser time out warning.
21. VA - improved weak password discovery, including a larger password dictionary. This may result in slower tests.

What's New in 4.1.0
==========
1. VA – added OS level tests (e.g. test permissions of the DBMS files and directories).
2. VA - added support for MySQL
3. VA - added support for Sybase vulnerability scanning
4. DAM - added support for MS SQL 2008 SP2.
5. DAM - added support for Oracle 10.2.0.5 and 11.2.0.2
6. VA - for Oracle – added the ability to import database names and parameters from tnsnames.ora files (in the DBMS tab)
7. DAM - Added ability to audit pre & post values for DML transactions using DML triggers.
8. Improved reports:
   a. Added summary reports including charts (Bar, Multi Bar, Pie
   b. Added report formats (now supported: XML, PDF, RTF, DOC, Excel, HTML)
9. VA - Advanced management for VA tests - manage & edit custom and predefined tests as well as add new test groups
10. DAM - Rule syntax expansion: added Exec_user. In addition to user and osuser keywords the exec_user has been added for Microsoft SQL Server. Exec_user is used when the login of the current session is changed or a statement is executed under a different user.
11. DAM - Added support for bind variables. Bind variables will now be shown in alerts. You can also write rules that include bind variable values. For example bindvar contains ‘obama’ will trigger an alert whenever the bind variable value will contain the string obama. Note that all values are treated as strings.
12. DAM - Alert times are now shown in both server local time and sensor local time (note – time based rules always refer to the sensor local time).
13. LDAP - added the ability to configure the cipher suite for LDAP over SSL.
14. DAM - When a sensor error occurs, a new indication will be shown in the sensor page (exclamation mark next to the relevant sensor).
15. DAM - Rule objects: added support for Regular Expressions in the dynamic object values.
16. VA - Scan results – added the ability to search within the data set results.
17. VA results – new state field will reveal whether a result is new (was not seen in the past), existing, or old (no longer exists).
18. VA – added the ability to exclude a DBMS from a specific test.
19. VA – added the ability to exclude users from the weak password tests.
20. VA – added clear indication whether a user with a weak password is open or locked.
21. Users can now configure which page will be open upon log in to the server (in the Permissions/users screen).
22. DAM - Added history record of sensor versions (in the system/history screen).
23. VA - Data discovery: you can now sample row data and search for data using regular expressions. See example in the User Manual.

Known Issues
==========
1. (No issue number) Exec_user: if sensor monitors a new session event when session executes with user different from original (e.g. sensor starts when session is already active) the user name will be set to exec user name, and exec user will be altered when session returns from the execution.
2. (No issue number) When using promiscuous mode on HPUX NICs: only one process may sniff the NIC and therefore the sensor may either prevent another sniffer from working or another sniffer may prevent the sensor from functioning correctly. Workaround – make sure that the NIC is not running in promiscuous mode.
3. (5021) When using Chrome - it is impossible to select print view twice (workaround - go to another screen and return to alerts).
This is due to a known Chrome issue:
http://code.google.com/p/chromium/issues/detail?id=16528
https://bugs.webkit.org/show_bug.cgi?id=28633
4. (No issue number) Non-English characters cannot be used in rules (e.g. if a table name is in non-english characters, it cannot be used in a rule). This is a known issue that will be resolved in a future release.
5. (No issue number) Because of limitations of SQL 2000 the following behavior is different from all other DBs:
SQL server 2000 does not enable the use of triggers, therefore there is no DDL trigger.
This means there is no delay of DDL commands (and termination will not necessarily happen before the transaction).
6. (1111) When setting the sensor machine's clock backward, all databases display as "none".
Workaround - restart the sensor.
7. (1927) When changing the Server time manually (e.g. when daylight savings time takes effect and the server doesn't change the time automatically) the Server's time may show incorrectly and alerts may also show incorrectly. Restarting the Server will resolve this issue.
8. (1083) Action scripts are not ignored by the sensor. This may cause database instability.
Workaround - when using action scripts user must be sure that the script does not trigger alerts (e.g. by creating an allow rule at the top of the policy).
9. (5604) Dashboard - in some cases (10min or hour time period) a refresh does not apply to the alert summary graph.
Workaround - choose a different time period