Security Reporter 3.1.0

M86 Security is pleased to announce the release of Security Reporter software version 3.1.0, available for downloading to a workstation and running as a virtual machine. This upgrade is compatible with an M86 Web Filter appliance running software version 4.0.10 or later, and/or an M86 Secure Web Gateway appliance running software version 9.2 or later.

WARNING: If upgrading an existing M86 appliance with this software release, M86 Security recommends scheduling the upgrade during non-peak hours. Since this software update includes a kernel upgrade for the operating system, once applied, this update cannot be uninstalled and the server will automatically reboot itself.

FREQUENTLY ASKED QUESTIONS

Q. What are the benefits of using SR Virtual instead of the SR Appliance option?
A. SR Virtual lets you use an existing computer to run the SR software image as a virtual machine, instead of installing and configuring a separate SR appliance. Virtualization is more cost effective in ensuring redundancy, failover and disaster recovery.

Q. Which type of server software is required in order to use SR Virtual?
A. M86 has tested VMware ESXi 4.1 and supports this software version, although other virtualization software may be used. Please consult with your M86 accounts representative or an M86 solutions engineer about software compatibility with SR Virtual.

Q. Can I use an SWG or a Web Filter with SR Virtual?
A. As with the SR Appliance version of the SR product, an SWG and/or Web Filter can be used with SR Virtual.

Q. Which report types are available for me if I have a Web Filter or a Secure Web Gateway (SWG) appliance, or both appliances?
A. Using a Web Filter, SR 3.0 (and higher) will generate real-time and productivity reports. Using an SWG, SR 3.0 (and higher) will generate productivity reports and security reports. If you are running both appliances, Web Filter log data will be used in your productivity reports.

Q. What type of content is included in security reports for an SWG user?
A. Log feeds from the SWG let you generate security reports showing blocked viruses, security policy violations, traffic analysis by content type, and security rules triggered. You can also generate a customized report for any of these options, including specific dates, break types, URLs, and user or IP criteria, and then export a PDF file of the generated report to designated email addresses.

(continued)

NEW FEATURES

Security Reporter Virtual now available

The new Security Reporter Virtual product is now available for running SR as a virtual machine.
- The following items are required for using SR Virtual:
  - Host computer on your network
  - VMware ESXi 4.1 server software and ESXi 4.1 client software
  - SR software image downloaded to your computer from a Content Delivery Network; this image comes in the following sizes: 500GB, 1TB, 2TB, 4TB, 6TB, 12TB.
- Optional items:
  - A SCSI/SAN storage device can be used with SR Virtual
  - A tap can be used for bandwidth monitoring
- In SR Virtual, the following differences are seen in the user interface of the System Configuration administrator console:
  - Backup screen is not available since the image is not FTPed.
  - Hardware Failure Detection screen displays the message: "Hardware Failure Detection is unavailable since this is not a RAID server."

Productivity reports enhanced with security report elements

Drill Down productivity reports (accessible via Report Manager: Reports > Drill Down Reports) have been enhanced with the look and feel of security reports, giving you greater flexibility in viewing reports in your browser.

Summary Drill Down Reports enhancements
The default summary drill down report panel now displays a split view of a graph and table showing the top six items in the bar chart, and a list of top records below. Mousing over a bar in the chart displays the name of the item depicted by that bar, and the corresponding page count total.
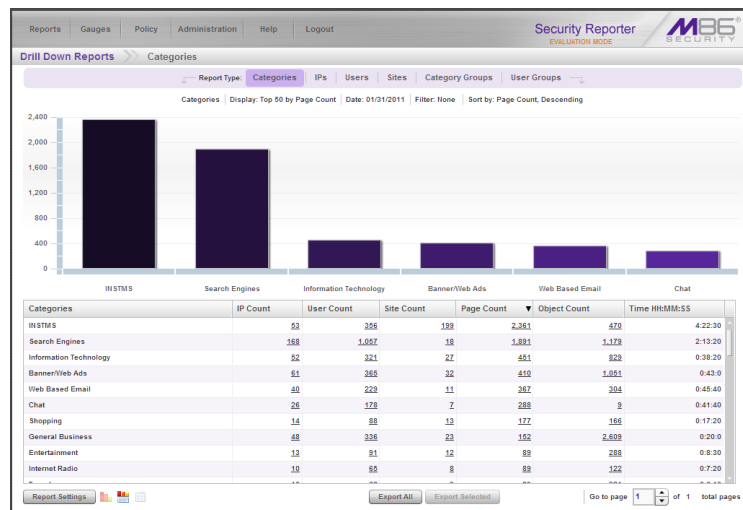
(continued)

Security Reporter 3.1.0

FAQs, continued

Q. Can I use more than one SWG to send logs to the SR?
A. Multiple SWG policy servers can now be set up to send logs to the SR.

NOTE: In SR 3.0, a known issue exists in which SR reports may be inaccurate in an environment in which multiple SWG policy servers send logs to the same SR. That issue has been resolved in this 3.1 software release. M86 recommends re-importing backed up archive logs and textmaps from each policy server after applying the 3.1 software update.

Q. Does SR 3.1 use different port numbers than the ones used in SR 3.0?
A. No, the same port numbers are used in this release. To access the reporting functions in SR 3.1, use port 8443. The administrator console, accessible via Administration > System Configuration, still uses port 8843.

Q. Which types of SR models are available if using a Web Filter and/or SWG?
A. SR models using 3.0 software (and higher) are as follows:
• Using a Web Filter, you have the option to use:
  • SR 300, 500, 700, or 730 Equus model, or
  • SR 705 or 735 IBM model.
• Using an SWG, you have the option to use an SR 705 or 735 IBM model.
• Using both a Web Filter and an SWG, you have the option to use an SR 705 or 735 IBM model.

Q. What are some of the differences between the SR models built by Equus and those built IBM?
A. All models built by Equus are 1U units, with the 300 series model half the width of a standard 1U unit. IBM models are 2U units. For the Equus 700 model, storage capacity is 1.5 TB. For the IBM 705 model, storage capacity is 2.3 TB. Attached storage options are available for Equus 730 and IBM 735 models using a Nexsan storage device:
• Basic storage: 3 TB storage for an SR 730 (Equus) model.
• Standard storage: 6 TB storage for an SR 730 (Equus) model or an SR 735 (IBM) model.
• Extended storage: 12 TB storage for an SR 730 (Equus) model or an SR 735 (IBM) model.

Productivity reports, continued

Summary Drill Down Reports enhancements
This report view can be modified by clicking one of three icons at the bottom left side of the panel:
• Clicking the bar chart icon displays only the bar graph
• Clicking the table icon displays only the table of records
• Clicking the split chart and table icon displays the default report view again
The checkboxes to the left of each record have been removed, and all buttons at the bottom of the panel have been replaced by the following objects:
• Report Settings menu includes the following options:
  • **Run** - Choosing this option opens the Run Report pop-up window, formerly named Modify Report, accessible via the Modify button. Specifying criteria in this pop-up window, and then clicking Run, updates the report view.
  • **Save** - Choosing this option opens the Save Report pop-up window
  • **Limited Detail Result** - Choosing this option opens the Limit Detail Result pop-up window.
• **Export All** button - Clicking this button (formerly named Export) opens the Export pop-up window with the Export option "All the rows on this report" specified. Formerly, all records would be exported if all checkboxes preceding records in the table were selected.
• **Export Selected** button - Select records to be exported by clicking the first column of each record you wish to select, and then clicking the activated Export Selected button to open the Export pop-up window, with the Export option "Only selected rows on this page" specified. Formerly, only records in the table with selected checkboxes would be exported.

Any column not containing statistical data no longer displays. For example, when using a Web Filter with this SR, the Bandwidth column which previously displayed zeroes will not display.

Detail Drill Down Reports enhancements
The default detail drill down report view displays the table of records with the following modifications:
• The Modify and Save buttons have been removed from the bottom of the panel, since these functions are now incorporated in the new Report Settings menu with the following options:
  • **Run** - Choosing this option opens the Run Report pop-up window, formerly named Modify Report, accessible via the Modify button. Specifying criteria in this pop-up window, and then clicking Run, updates the report view.
  • **Save** - Choosing this option opens the Save Report pop-up window. Previously, the Save button fulfilled this function.
• **Export All** button - Clicking this button (formerly named Export) opens the Export pop-up window. Previously, the Export button (now removed from the bottom of the panel) fulfilled this function.
• **Column visibility** button - Clicking this button still opens the Column visibility pop-up window, with the Cancel button in it now renamed "Close."

Report Wizard now accessible from Drill Down Reports menu
The Report Wizard for Drill Down Reports is now accessible via the Drill Down Reports menu (Report Manager: Reports > Drill Down Reports > Report Wizard). This restructuring follows the logic of the Report Wizard for Security Reports, which is accessible via the Security Reports menu.

Security Reporter 3.1.0

FAQs, continued

Q. Are real time reports available if I'm using an SWG?
A. Real time reports are only available if using a Web Filter. If you have both a Web Filter and an SWG, you will be able to use real time reports. The user interface for real time reports shows a dashboard with gauges for URL categories or ports, and end user Internet/network activity for each gauge in real time.

Productivity reports, continued

'Group By' term replaces 'Break Type'

The term "Group By" is now used throughout the user interface instead of "Break Type." The replacement affects the following areas in productivity reports:
• Drop-down menu name in Export pop-up window in summary and detail Drill Down Reports (Report Manager: Drill Down Reports > report > Export Selected or Export All button > Export pop-up box)
• Drop-down menu name in Save Report pop-up box, Advanced Options tab (Report Manager: Drill Down Reports > report > Report Settings > Save option)
• Drop-down menu name in Saved Report pop-up box, Advanced Options tab (Report Manager: Saved Reports panel)

General report enhancements
• For both summary and detail productivity Drill Down Reports, the tab for the selected Report Type remains highlighted, as it does in Security Reports
• For Summary Reports (Report Manager: Reports > Summary Reports), the selected Date Scope tab now remains highlighted in the report view panel
• When attempting to click a URL in a report view for a detail productivity or security report view, a warning dialog box now opens asking if you wish to proceed, given that clicking the link could launch malware on your machine if the end user accessed malware content at that URL
• The footer of the generated drill down productivity report or canned Sample Report now includes the time zone following the time in which the report was generated

Reports landing page: Summary Reports or Report Wizard

When logging in to the SR, instead of displaying the Dashboard, the landing page is now Summary Reports (Report Manager: Reports > Summary Reports) or the Drill Down Report Wizard (Report Manager: Reports > Drill Down Reports > Report Wizard)—the latter if permissions are not granted to the user to access Summary Reports. The Dashboard is still accessible by navigating to Report Manager: Reports > Dashboard.

Security Reports provide new tools, greater flexibility

Security reports have been enhanced to include some of the same features found in productivity drill down reports and report views:
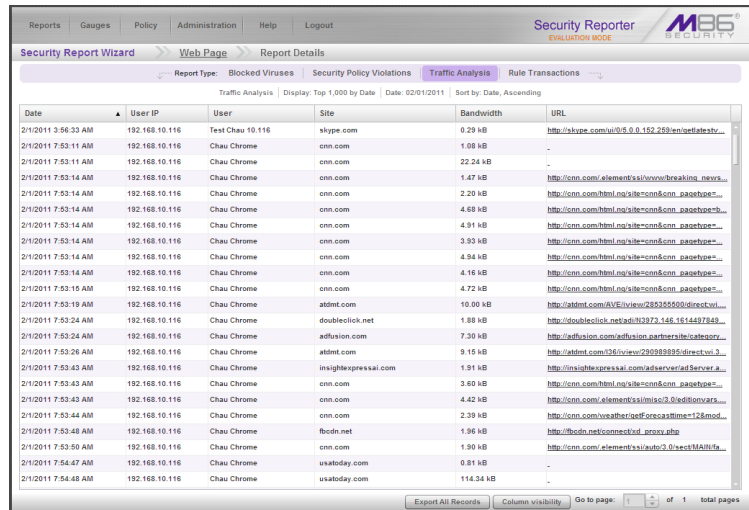• Beneath the tabs at the top of the report view, the following criteria now displays: Report type name, Display, Date, and Sort by criteria
• The Count column at far right has been renamed Hit Count in Blocked Viruses, Security Policy Violations, and Rule Transactions report views
• Break Type drop-down menu name has been changed to Group By, affecting the following areas in security reports:
  • Drop-down menu name in Export Report pop-up window (Report Manager: Reports > Security Reports > Export button)
  • Drop-down menu name in Report Wizard panel, Report Details frame (Report Manager: Reports > Security Reports > Report Wizard)
• Export Report pop-up box buttons have been renamed Email and Download (from Email Report and Download Report)
• Reports generated in the PDF format resemble productivity reports, including both a chart graph and rows of records below.

(continued)

Security Reporter 3.1.0

Security Reports, continued

Drill down and detail reports now available for Security Reports
- In a security report view, clicking a link in a column for a record lets you drill down to view additional information for that record, similar to the way productivity drill down reports function
- Clicking a Bandwidth or Hit Count column link generates a detail Security Report view that includes:
  - Rows of records in the report table
  - The Export All Records and Column visibility buttons as well as the page navigation tool for viewing additional pages in the report at the bottom of the report view

Security Report Wizard Schedule Settings link
In the Security Report Wizard panel (Report Manager: Reports > Security Reports > Report Wizard), the Schedule Settings button is now a link preceding—instead of following—the Save button at the bottom right of the panel.

Multiple SWG policy servers supported

More than one SWG policy server can now be used with an SR. When adding additional policy servers, the ID number to be assigned to the policy server auto-increments to the next consecutive number.

Wizard modifications
The following modifications were made to the SR Wizard to accommodate this feature:
- The view only ID field has been replaced by the Name entry field
- The view only Username field has been removed
- The Password field has been moved beneath the Remove button, and the Confirm Password field has been added beside this field
- The table includes only the Name and Description columns, consistent with the entry fields above

(continued)

Multiple Policy Servers, continued

Device Registry modifications
The following modifications were made to the Device Registry panel (Report Manager: Administration > Device Registry) to accommodate this feature:
- The New Policy Server button and pop-up box have been renamed New SWG Policy Server. The pop-up box includes the following modifications:
  - The explanatory text has been modified
  - Links are included for accessing the SWG User Guide to help you configure the SWG server to work with this SR
  - The Path information now displays above the SWG Device Type image. The Path includes the IP address of the SR preceded by double slashes '//' and followed by a single slash '/' and auto-incremented ID number assigned to the SWG. This Path information can be copied and pasted into the SWG user interface so the SWG can send logs to the SR being configured.
  - The view only ID and Username fields no longer display; in its place are the Name and Description entry fields. Entries saved for these fields display in the thumbnail image for the SWG device
  - The Password field is now followed by the Confirm Password field
  - For any subsequent SWG being added to the Device Registry, the New SWG Policy Server pop-up box does not include the Password fields
- The Edit Policy Server pop-up box has been renamed Edit SWG Policy Server
  - This pop-up box includes the Change Common Password button. Clicking this button takes you to the next pop-up page named Change Common SWG Policy Server(s) Password. Entering the passwords in these fields and clicking Change Password takes you back to the Edit SWG Policy Server page.
- If an SWG was removed from the Device Registry and subsequently added back in, a new ID number is assigned to that same SWG. (This new ID number needs to replace the original ID number entry for this SR in the SWG user interface.)

General Wizard enhancements
- The SR Wizard now displays larger font sizes
- Only Main Administrator frame settings are initially required. However, if a Web Filter or SWG is not added during this process, an alert box opens after logging in the user interface to inform you to set up a filtering device in the Device Registry. In this scenario, the Report Manager navigation bar does not include the Gauges selection; this would appear if a Web Filter is subsequently added in the Device Registry.
- The Language settings menu appears in the Main Administrator section, with English as the default selection if the browser is set to display text in the English language. The other two language setting selections are Traditional Chinese and Simplified Chinese.

General Device Registry enhancements
- The Device Registry panel (Report Manager: Administration > Device Registry) now displays larger thumbnail images and font sizes
- Spaces are now accepted when adding or editing Name and Description entries
- The Refresh Devices button has been renamed Refresh View, and the Sync All Devices button and pop-up box have been renamed Refresh Settings
- The Refresh Settings button only displays if a Web Filter is included in the Device Registry
- If adding the first Web Filter in the Device Registry subsequent to the SR Wizard installation process, be sure to indicate that this is the Source Web Filter (unless another Web Filter will be added as the Source), and specify the Bandwidth IP range for the SR to monitor
- If adding the first SWG in the Device Registry subsequent to the SR Wizard installation process, the Security Reports menu will be available the next time you log in to the Report Manager user interface

Security Reporter 3.1.0

Traditional and Simplified Chinese localization

The user interface of the SR has been translated to the Simplified Chinese (Mainland China) and Traditional Chinese (Taiwan) languages. The following features accommodate this enhancement:

- If a browser is already set to use either Simplified Chinese or Traditional Chinese, that language setting will automatically display in the user interface after applying this software update
- Language selection for English, Simplified Chinese, or Traditional Chinese can be made from the new Language drop-down menu in the following areas of the SR:
  - Main Administrator section of the SR Wizard screen
  - Admin Detail frame of the Admin Profiles panel (Report Manager: Administration > Admin Profiles)

Admin Profiles enhancements

The Admin Detail frame of the Admin Profiles panel (Administration > Admin Profiles) includes the following enhancements:

- The Full Name field entry is now optional
- The new Language setting drop-down menu now lets you choose the Traditional Chinese or Simplified Chinese language setting to display throughout the user interface. If making a language selection change, a warning message displays to inform you that the new language selection will be effective immediately, and may affect your ability to navigate the user interface if you are not familiar with that language.

New features accessible from the Report Manager banner

The Help tab in the Report Manager navigation bar now includes the following menu selections:

- Online Help: Choosing this selection opens the Security Reporter documentation page at M86Security.com, previously accessible by clicking Help
- About...: Choosing this selection opens a new pop-up window that provides information about the current software Version number applied to the SR, as well as the Serial number of the SR chassis

The Security Reporter logo in the Report Manager application is now clickable. Clicking 'Security Reporter' in the banner of any Report Manager panel takes you to the M86 Security public Web site.

Process for converting to Registered Mode simplified

For an SR in Evaluation Mode, the Report Manager banner now displays 'EVALUATION MODE' to remind you of the SR's current status. An SR in Evaluation Mode stores no more than three weeks of data. Activating the SR converts the unit to Registered Mode, in which the amount of data storage is contingent upon the current drive capacity available on the SR. The following areas of the user interface are affected by this enhancement:

- Report Manager banner includes the 'EVALUATION MODE' link:
  - Hovering over this link displays a tooltip explaining "Evaluation Mode"
  - Clicking this link takes you to the Server Status screen of the System Configuration administrator console, in which the SR Status pop-up window opens to let you change the server mode to Registered Mode.
- Server Information panel (Report Manager: Administration > Server Information) no longer displays the Mode status (EVALUATION - MAX DATA STORAGE 'X' WEEKS) for an SR in Evaluation Mode, since this indicator now displays in the banner.

(continued)

Security Reporter 3.1.0

Forgot Your Password lets you log in with a new password

If you are unable to log in the Security Reporter user interface because you forgot your password, this new feature lets you create a new password on demand. The following areas of the SR are affected by this feature:
- The Forgot your password? link has been added in the login window:
  - Entering your Username and then clicking the Forgot your password? link displays the Forgot Your Password? window.
  - In the Forgot Your Password? window, clicking Submit displays the alert window letting you know an email was sent to the email address on record for your account.
  - The dispatched email provides instructions and a link to access the Reset Your Password login window.
  - In the Reset Your Password login window, entering the New Password and Confirm Password, and then clicking Submit grants access to the SR user interface.

Default Report Settings enhancements for SWG users

The following modifications were made to the Default Report Settings panel (Report Manager: Administration > Default Report Settings):
- A note has been added to specify the Hide Unidentified IPs option does not affect Security Reports
- If using only an SWG with this SR, the Hide Uncategorized Category option does not display, since this feature is only pertinent to the Web Filter
- The new Combine Duplicate Names drop-down menu is used for specifying whether Security Reports will show duplicate report name entries under the same name, or if separate entries will display for duplicate names.

Object Count frame renamed Log Import Settings

The Object Count frame (System Configuration: Database > Optional Features) has been renamed Log Import Settings. The explanatory text therein has been modified to specify that the settings in this frame solely pertain to the Web Filter and not the SWG.

Registered trademark symbol replaces TM symbol

The M86 logo in the banner header of the user interface and in reports is now followed by the registered trademark symbol (an encircled 'R') instead of the former TM trademark symbol.

Download software updates to preview upcoming features

Software Update Setting and Software Update screens (accessible via System Configuration: Server menu) have been modified to accommodate new options available for reviewing pre-released software features. The following terms are used when referring to the three basic types of software downloads:
- GA (General Availability) - Official software release; recommended for production systems.
- LA (Limited Availability) - Production ready software made available in advance of an official software release; can be used in a production environment.
- Beta - Pre-released software made available for reviewing new features in an upcoming software release; not recommended for use in a production environment.

(continued)

Download software updates, continued

Software Update Setting screen

The Software Download Settings frame has been added to this screen and includes the option(s) to have Beta and/or Limited Availability software updates downloaded to your SR if you wish to preview upcoming software features
• By default, the Limited Availability option is enabled
• If enabling the Beta option, the Limited Availability option cannot be disabled
• Options to enable/disable Beta or Limited Availability software downloads can be modified at any time

Software Update screen

The following modifications have been made to this screen to accommodate the software preview feature:
• Type column has been added to the SR Software Updates frame (renamed from SR Patch Updates) and the SR Software Update History frame. This column precedes the Description column and specifies the type of software update (GA, LA, Beta) for each item included in the table.
  • A key describing Software Update Types displays at the bottom of the SR Software Update History frame

• LA and Beta software update links are included in the table(s) only if the option(s) to have LA and/or beta software updates download to the SR is/are enabled in the Software Update Settings screen
  • Only the latest software update is included in the SR Software Updates frame.
  • Once the beta software testing period has passed, only the latest LA software update displays in the table, if the request to have LA software updates downloaded is enabled

  NOTE: GA software updates will still automatically download to all active SR units.

• When choosing to apply either a Beta or LA software update for the first time, clicking Apply Now launches the Software Update Installation Key pop-up window requesting the entry of a valid installation key:
  • Typing in the valid installation key and clicking Enter opens a readme file that includes:
    • Explanation for the type of software update being requested (Beta, LA)
    • Checkbox that must be populated in order to enable the Yes button and proceed with the installation request process; the No button is active by default
  • Clicking Yes launches the EULA that must be accepted in order to apply the requested software update
  • If you do not have an installation key, clicking the "click here" link launches the login page at M86Security.com in which you authenticate yourself and verify user and server criteria in order to obtain the installation key

When enabling Beta and/or LA software update downloads, an email is sent to alert you to the availability of the latest Beta/LA software update.

Security Reporter 3.1.0

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and 16 million users worldwide. As one of the largest independent Internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information, and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

Logs for verifying software downloads and installation

A new log for verifying recent software downloads is available via the Software Update screen (System Configuration: Server > Software Update) and Database Status drop-down menu in the Tools screen (System Configuration: Database > Tools).

Software Update screen

The following items now display beneath the SR Software Update History table:
- Download Available Updates button - Clicking this button launches a request to Traveler to download any available software updates on demand, and opens a pop-up box that explains the screen needs to be refreshed in order to find out if there are new downloaded software updates available for installation.
- Link for viewing Software Installation Log - This link, formerly named "Software Update Log," accesses the Software Installation Log pop-up box that shows you the history of recently installed software updates.
- Link for viewing Software Download Log - Clicking this link opens the update log that shows you recent software download criteria.

Tools screen

The following software log menu selections are available from the Database Status menu:
- Software Installation Log - Formerly named "Software Update Log," choosing this menu selection and clicking View accesses the patch log that shows the history of recently installed software updates.
- Software Download Log - Choosing this menu selection and clicking View accesses the update log that shows the history of recent software download criteria.

Gauge Ranking panel column expansion

The column width in the Gauge Ranking panel (Report Manager: Gauges > Dashboard > gauge > Gauge Ranking) has expanded to accommodate the column headers in one row instead of stacking text, which increased the height of the column header.

Upgrades to operating system and Tomcat

This software release includes upgrades to the OS kernel and Apache Tomcat in order to address security vulnerability issues.

Resolved Known Issues

- Go to http://www.m86security.com/software/8e6/ts/sr-rki.html to view the resolved known issues for this software release.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**