radware

AlteonOS

RELEASE NOTES

Version 34.0.0.0
March 30, 2023

TABLE OF CONTENTS

CONTENT **4**

RELEASE SUMMARY **4**

SUPPORTED PLATFORMS AND MODULES **4**

UPGRADE PATH **5**

Before Upgrade – Important! 5

Additional Considerations 5

Downgrade 6

WHAT'S NEW IN 34.0.0.0 ..... **6**

GEL Support in Standalone Mode 6

Alteon Kubernetes Connector Enhancements 6

Overload Protection for Integrated WAF 8

Slowloris Attack Protection 8

Layer 7 Modification on HTTP/2 traffic 9

Out-of-the-box Certificate Pinned Sites List 9

Sideband and SecurePath Updates in Unified Events 10

GEL Dashboard Enhancements 10

Control and Export of Management Port Packet Capture from WBM 10

WHAT'S CHANGED IN 34.0.0.0 ..... **11**

UDP Stateless and TCP Services on the Same VIP 11

Integrated WAF SUS and GEO DB Update Via Proxy 11

Combined Image Upload Option Removed from WBM 11

Service and Real PPS Collection Interval 11

OpenSSL Upgrade 11

Integrated AppWall 11

API Security 11

Custom Pattern per Application Path 12

Server-Side Request Forgery 12

Multiple IPs Included in XFF HTTP Header 12

Global Security Event Suppression 12

Database Security Filter 12

Multiple Enhancements on AppWall REST API for DevOps 12

MAINTENANCE FIXES **13**

Fixed in 34.0.0.0 13

General Bug Fixes 13

AppWall Bug Fixes 15
KNOWN LIMITATIONS 16
RELATED DOCUMENTATION 16

CONTENT

Radware announces the release of AlteonOS version 34.0.0.0. These release notes describe new and changed features introduced in this version on top of version 33.5.3.0.

RELEASE SUMMARY

Release Date: March 30, 2023

Objective: Major software release that introduces and/or enhances a number of capabilities and solves a number of issues.

SUPPORTED PLATFORMS AND MODULES

This version is supported by the following platforms:

- 4208, 4208S
- 5208, 5208S
- 5424S, 5424SL, 5820S, 5820SL
- 6024, 6024S, 6024SL, 6024 FIPS II
- 6420p, 6420, 6420S, 6420SL
- 7612S, 7612SL
- 7220S, 7220SL
- 7100S, 7100SL, 7100DS
- 7700S, 7700SL, 7700DS
- 8420, 8420S, 8420SL
- 8820, 8820S, 8820SL
- 9800, 9800S, 9800SL
- Alteon VA running on VMware ESXi 6.0, 6.5, 6.7, 7.0, KVM, Hyper-V, and OpenXen
- Alteon VA on AWS
- Alteon VA on Azure
- Alteon VA on Nutanix
- Alteon VA on Oracle Cloud
- Alteon VA on Google Cloud

For more information on platform specifications, refer to the *Alteon Installation and Maintenance Guide*.

Alteon 34.0.0.0 is supported by APSolute Vision version 4.30 and later, and Cyber Controller 10.0 and later.

Integrated AppWall version: 7.6.19.0

OpenSSL version:

- FIPS II model: 1.0.2u
- S/SL models, standard models, and VA: 1.1.1t

UPGRADE PATH

You can upgrade to this AlteonOS from AlteonOS versions 28.*x*, 29.*x,* 30.x, 31.x, 32.x and 33.x.

General upgrade instructions are found in the *Alteon Installation and Maintenance Guide*.

Before Upgrade – Important!

1. Before performing an upgrade, back up your current configuration.
2. To ensure a successful upgrade, run the Upgrade Advisor Tool with your current configuration and the target version. Then, perform the required actions as instructed in the report output. The Upgrade Advisory Tool includes all the limitation and upgrade considerations specifically relevant to the source configuration, version, device details and target version. Make sure to update the Upgrade Advisory Tool DB before performing the analysis. The Upgrade Advisor Tool is available on the Customer Portal.
3. Read the Upgrade Limitations in these Release Notes for new upgrade limitations related to this version.

The following table describes the specific upgrade path from each version to 34.0.0.0:

Current Version	Upgrade Path	Notes
28.*x*	> 29.0.9.0 > 30.5.3.0 > this version	As an alternative, you can upgrade directly to 34.0.0.0 using the recovery process. **Note**: You must save the configuration before starting this process.
29.0.*x* (*x*=<8)	> 29.0.9.0 > 30.5.3.0 > this version	
29.0.*x* (*x* > 8)	> 30.5.3.0 > this version	
29.5.*x* (*x*=<7)	> 29.5.8.0 > 30.5.3.0 > this version	
29.5.*x* (*x*>7)	> 30.5.3.0 > this version	
30.*x* =< 30.5.2.0	> 30.5.3.0 > this version	
30.*x* > 30.5.2.0	Direct upgrade to this version	
31.*x*	Direct upgrade to this version	
32.*x*	Direct upgrade to this version	
33.x	Direct upgrade to this version	

Additional Considerations

Hypervisors (ADC-VX) running a certain version only support vADCs that run the same version or later.

Important!

- For Alteon 5208, 5424, 5820, 6024, 7612, 7220, and 9800, vADCs running this version require ADC-VX running at a minimum version 33.0.0.0.
- For Alteon 8420, vADCs running this version require ADC-VX running at a minimum version 33.0.1.0.
- For Alteon 6420, vADCs running this version require ADC-VX running at a minimum version 33.0.4.50.

Downgrade

Configuration rollback (downgrade) is not supported. The configuration should be saved before upgrading to a newer version. If you perform version rollback, Radware recommends the following procedure:

1. Set the configuration block for the next boot to **factory** (the management port setting can be kept).
2. Change the image for the next boot to the image to which you want to roll back.
3. Perform reboot.
4. After reboot, Alteon will run with the previous version with the factory default configuration.
5. Upload the configuration that was saved before the version upgrade

WHAT'S NEW IN 34.0.0.0

This section describes the new features and components introduced in this version on top of Alteon version 33.5.3.0.

GEL Support in Standalone Mode

Starting with this version, GEL is now available on a Standalone platform.

Now, entitlements can be allocated to VA, vADC, and Standalone platforms.

NFR ID: 221222-000039

Alteon Kubernetes Connector Enhancements

The Alteon Kubernetes Connector (AKC) provides a solution for Alteon integration with Kubernetes/OpenShift orchestration.

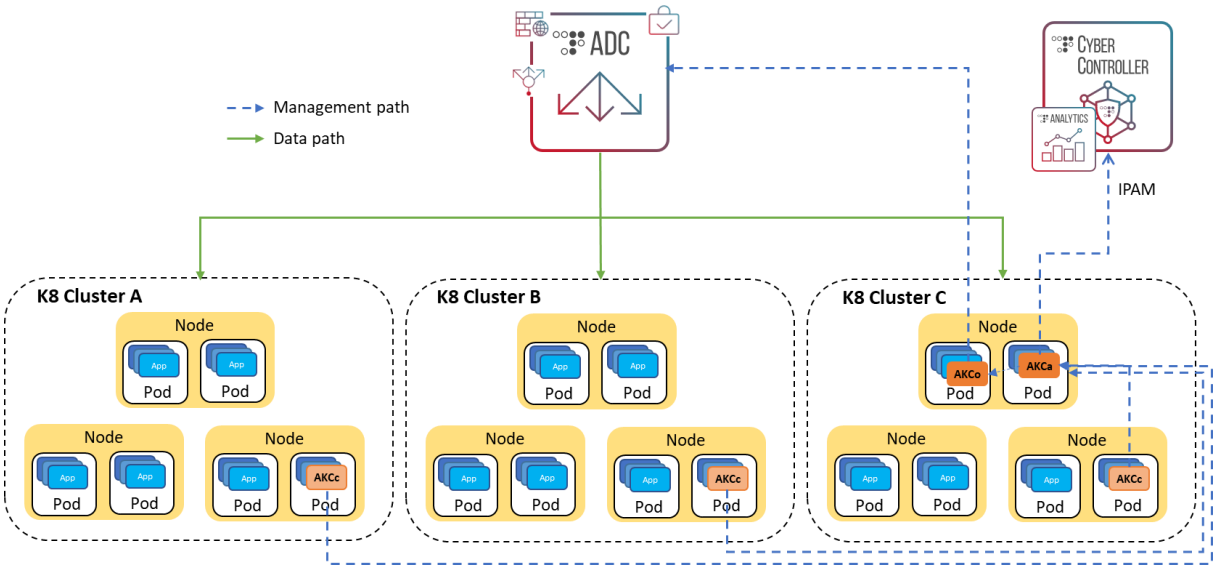
AKC runs inside the Kubernetes clusters, discovers services of type LoadBalancer and translates them to an Alteon ADC configuration. In addition, it monitors the cluster nodes and updates the Alteon configuration when nodes are removed or added to a cluster.

The AKC solution enables Alteon to load balance a service that is deployed in multiple Kubernetes clusters, using a single VIP.

The AKC has three components:

- The AKC Controller that monitors the service objects and nodes in the Kubernetes clusters. Such a component is required in each of the participating Kubernetes clusters.
- The AKC Aggregator that aggregates inputs from all the collectors and communicates the necessary configuration changes to the AKC Configurator. These components should be installed in only one of the clusters.
- The AKC Configurator that translates the changes to Alteon configuration file and pushes it to Alteon.

In addition, the solution uses the vDirect module in Cyber Controller/APSolute Vision, which handles the IPAM service, required to allocate the service IP (VIP) from an IP pool (currently a single pool supported).



In this version, the AKC has added support for the following Alteon capabilities for the services deployed in Kubernetes:

- SSL offload. To enable SSL offload, the following annotations can be used during service deployment to specify the SSL policy and certificate that should be used (these objects must be configured in Alteon before the service is deployed).
  - `akc.radware.com/sslpol: <ssl policy id>`
  - `akc.radware.com/cert: <certificate id>`
- The SecurePath connector that allows providing application security (Cloud WAF, API protection, and BoTM) for the deployed service. The following annotations can be used during service deployment to specify the SecurePath and Sideband policies necessary to activate SecurePath for its traffic (these objects must be configured in Alteon before the service is deployed).
  - `akc.radware.com/sideband: <sideband policy id>`
  - `akc.radware.com/secpath: <secpath policy id>`

Overload Protection for Integrated WAF

A new mechanism is now available to reduce the load on the WAF process in case of overload by bypassing WAF inspection for some of the transactions.

When the overload protection mechanism is enabled, it looks at the transactions sent within a 10-second sliding window, and when at least 1,000 transactions are received within such a window, the following occurs:

- If the WAF processing time of between 31% and 50% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 50% of the transactions.
- If the WAF processing time of between 51% and 75% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 10% of the transactions.
- If the WAF processing time of over 76% of the transactions within the window is higher than the user-specified threshold, Alteon will start sending to the WAF process only 1% of the transactions.
- Once 30% or less of the transactions within the window have a WAF processing time higher than the user-specified threshold, Alteon will go back to sending all the transactions to the WAF process.

To enable this mechanism, set the value of the **WAF Overload Threshold** parameter in the relevant virtual service or filter (by default it is disabled, meaning set to 0) as follows:

- From the CLI:
  - For a virtual service: `cfg/slb/virt <id>/service <port>/http/aw overload`
  - For a filter: `cfg/slb/filt <id>/aw overload`
- From the WBM
  - For a virtual service: Use the *New/Edit Virtual Service* pane > *Security* tab
  - For filter: New/Edit Filter page, Security tab

Note: Filters that have this mechanism enabled must be part of a Filter Set.

Slowloris Attack Protection

Slowloris is an application layer DDoS attack that uses partial HTTP requests to open connections between a single computer and a targeted Web server, and then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

Alteon can now protect itself and the application servers from a slowloris attack.

To activate the protection, configure the new **HTTP Headers Timeout** parameter for the virtual services or filters you want to protect. If all headers are not received within the specified time, the session is closed. The recommended value is 4000 msecs.

Notes:

- The Delayed Bind mode must be Force Proxy when the Slowloris protection is enabled.

- Filters that have this protection enabled must be part of a Filter Set.

Layer 7 Modification on HTTP/2 traffic

Header modification is now supported for HTTP/2 proxy traffic, via HTTP Modification Rules.

Notes:

- Each rule in the rule list must be a header modification rule.
- If the action is Insert, the rule must not contain a condition.
- If the action is Remove or Replace, the following headers cannot be replaced or removed (the values of the header can be changed):
  - Request: ":method", ":scheme", ":authority" and ":path"
  - Response: ":status"
- The header names must not contain uppercase characters.

NFR ID: 221123-000123

Out-of-the-box Certificate Pinned Sites List

Pinning is the process of associating a host with the expected X509 certificate or public key. This means the client (browser or app) knows which certificate to expect for a certain site, including who signed the certificate.

SSL inspection is not possible for a site with a pinned certificate, as the client will identify the signer of the certificate as not being the original signer, thus terminating the connection.

Traffic to these application domains should be configured for bypass in any SSL Inspection solution if the enterprise wishes to allow such traffic for its employees.

To simplify this for customers, Radware provides an out-of-the-box list of known sites with pinned certificates. The following out-of-the-box elements have been added:

- Data class bypass_hosts_list, which includes the list of known sites with pinned certificates
- Content class Cert_Pinning_Bypass_Sni of type SSL with the bypass_hosts_list data class attached
- Content class Cert_Pinning_Bypass_Hostnames of type HTTP with the bypass_hosts_list data class attached

To bypass the pinned sites, you need to configure the bypass filter and select the relevant Content Class (SNI for Transparent Proxy mode or Hostnames for Explicit Proxy mode).

All these out-of-the-box objects are editable:

- If the data class was edited, it can be reverted to the default.
- After version upgrades the list could be updated. In such cases, if the bypass_hosts_list data class was not edited it is automatically updated. If the data class was edited, it is not updated unless **Revert to Default** is performed.

NFR ID: 221011-000139

Sideband and SecurePath Updates in Unified Events

Unified events now include information related to Sideband and SecurePath (based on AppShape++ script SIDEBAND::add_action commands send_response and terminate_session):

- In SecurePath integration, if the request is identified as an attack and is responded to by Cloud WAF (without reaching the destination server), the event's *severity* is marked as "security" with *reason* "SecurePath Response"
- When generic sideband is used, if the request is responded to by the sideband server (without reaching the destination server), the event's *severity* is marked as "Normal" with *outcome* "Sideband Response"
- When the connection is terminated by the sideband, meaning that the client connection is closed by FIN/RST, the event's *severity* is marked as "Exception" with *outcome* "Failure" and *reason* "Connection Closed by Sideband".
- When there is a Sideband time out, meaning that the client connection is closed by FIN/RST, the event's *severity* is marked as "Exception" with *reason* "Sideband Failure".

GEL Dashboard Enhancements

The following GEL Dashboard enhancements are available starting with Cyber Controller version 10.1.1.0 for all supported Alteon versions:

- An instance's last validation time is now visible in the *Instances* table per the selected entitlement. By default, each instance validates its license with the license server every five (5) minutes.
- The validation status of the license allocated to the Alteon server is now available in the *Instances* table per selected entitlement. Values include:
  - Valid — The Alteon server has received revalidation from the LLS.
  - Revalidation Required — The Alteon license is still valid, but the Alteon server did not receive validation from the LLS for more than two (2) hours, half of the borrow period. If the Alteon server receives revalidation before the end of the four-hour borrow period, the status changes back to Valid.
- Sorting was added to the instance table per selected entitlement. By default, the table is sorted according to the validation status. The table can be sorted by each one of the columns in the table.

Control and Export of Management Port Packet Capture from WBM

You can now control and export the Management port packet capture from WBM.

NFR ID: 221102-000004

WHAT'S CHANGED IN 34.0.0.0

UDP Stateless and TCP Services on the Same VIP

You can now configure both a TCP service and an UDP stateless service on the same VIP and port.

NFR ID: 220520-000151

Integrated WAF SUS and GEO DB Update Via Proxy

Auto-updates for WAF SUS and GEO DB can now be performed through a Proxy server.

Use `/cfg/sys/mmgmt/awproxy` to set the interface to route the traffic to the proxy server. The management interface is defined by default.

NFR ID: 220601-000032

Combined Image Upload Option Removed from WBM

The Alteon combined image is utilized to install both ADC-VX and vADC instances for Alteon platforms in a single step. However, the option to upload a combined image has been removed from the WBM in this version and is only supported via the CLI. If you want to upload an image via WBM, you must upload the ADC-VX and vADC images separately.

Service and Real PPS Collection Interval

Starting with this version, the service and real PPS collection is enabled by default and collects the information every 20 minutes in .csv format. in addition, the interval can be now adjusted using the `/cfg/slb/adv/pps/interval` command.

OpenSSL Upgrade

The OpenSSL version was updated, for both the data and management path, to version 1.1.1t.

Note: Not relevant for FIPS II models.

Integrated AppWall

API Security

In this version multiple enhancements are provided for API Security protection:

- **Support for Preflight request (CORS mechanism):** Usually the preflight requests are automatically sent by browsers. This consists of sending automatic requests with the HTTP method OPTION and the header "Access-Control-Request-Method". If the method OPTION is not defined in the OpenAPI file description, the requests are blocked by the API protection. Support of preflight request will now accept these client requests coming from the browser.

- **Case insensitivity during the API Catalog endpoints inspection.** By default, the inspection is case sensitive. It can be deactivated to be case insensitive.
- **Circular reference**: OpenAPI files that include circular references are now supported.
- The **Forensics Security Events** present more detailed descriptions related to the nested parameters, for example into a JSON body.
- When a Security violation occurs, AppWall propose a more accurate and **advanced refinements option** that will improve the False Positive management.
- The **AppWall Techdata** has been updated to include the OpenAPI files that have been previously uploaded.

Custom Pattern per Application Path

Custom Patterns help to define a personal signature. Custom Patterns can now be defined per Application Path, not only globally.

Server-Side Request Forgery

The Unvalidated Redirect protection is improved in term of performance and security coverage.

Multiple IPs Included in XFF HTTP Header

In version 7.6.18.0, AppWall allowed globally configuring how to read XFF HTTP headers when they contain multiple IPs. From this version, this can be configured per AppWall Tunnel (referred to as SECWA in the Alteon WAF).

Global Security Event Suppression

AppWall provides mechanisms to protect from a Security Events flood:

- Automatic Event suppression configured manually per Security Event.
- Automatic Event suppression configured dynamically per Security Event.

In this version, AppWall provides an additional mechanism:

- Automatic Event suppression configured dynamically per multiple Security Events.

Database Security Filter

Database Filter inspection can be excluded for Query/Body Parameter names. The configuration is available globally or per Application Path.

Multiple Enhancements on AppWall REST API for DevOps

Multiple new AppWall REST APIs have been delivered.

For details, please consult the on-line product documentation.

MAINTENANCE FIXES

The following sections list the fixed bugs included in this release.

Fixed in 34.0.0.0

General Bug Fixes

Item	Description	Bug ID
1.	On a 6024 SL platform, as unable to give the response to a TCP-SYN message.	DE76488
2.	RSTP was not working properly	DE78382
3.	Could not configure filtpbkp in hot-standby mode. Modified the CLI validation to resolve the issue.	DE78555
4.	Interface 256 could not be selected for switch HA advertisements.	DE78894
5.	Using WBM, an update to the cipher list was greater than 256 characters and was not accepted.	DE78975 DE78982
6.	The Unit label for a rule level timeout was different between WBM and the CLI.	DE79014
7.	On DPDK virtual platforms, traffic passing thorough BWM shaping contracts caused invalid buffer access and caused the vADC to reboot.	DE79049
8.	There was high SP memory utilization during a low traffic period.	DE79060
9.	Getting the vADC partition size failed and caused the vADC to hang on restart.	DE79122
10.	After running /stats/slb/pip, the SNMP OID was missing from the output.	DE79222
11.	VPN connectivity failed because of the IKE and the ESP sessions being bound to different servers.	DE79231
12.	Could not enter the hyphen (-) character in the New Host to Replace field on the **Application Delivery > Virtual Services >Virtual Services of Selected Virtual Server > HTTP Content Modifications >HTTP Rules >URL Match & URL Action** pane.	DE79234
13.	The Root Bridge was not properly declared in MSTP.	DE79245
14.	Using WBM, the hard disk capacity displayed incorrectly because secondary disk size was not counted.	DE79254
15.	SNMP walk failed because the OID did not increase.	DE79433
16.	A vADC did not handle traffic when it became the master.	DE79515

Item	Description	Bug ID
17.	An AppShape++ script trying to insert a script greater than 50k characters into the cmdLogMP-1-1 file caused the device to reboot.	DE79544
18.	System analytics were sent with null data.	DE79612 DE79619
19.	There was an issue with FQDN and multiport applications because there was no server name for the FQDN ephemeral real server in the XML sent to AppXcel.	DE79729
20.	When setting the time zone by name and not changing the default NTP time zone, a warning is issued after the Apply.	DE79793 DE79800
21.	When clsaging both is enabled with tunnels, the device rebooted.	DE79831
22.	The application services engine was not synchronized with the current configuration and the change was not saved.	DE79844
23.	In an SLB and PIP environment, there was a discrepancy in the PIP statistics between /st/slb/pip and /st/slb/aux.	DE80128
24.	SANs fields greater than 1024 bytes were accepted while generating a CSR.	DE80145
25.	The traceroute response packet was sent by Alteon with the wrong interface.	DE80192
26.	After upgrading from version 30.5.3.0 to 32.4.6.0, VLANs displayed as Down.	DE80319
27.	After downloading and uploading a configuration via REST API, SlbNewCfgFQDNServerTable was empty.	DE80348
28.	An SSLi issue caused the device to reboot.	DE80415 DE80420
29.	An incorrect GSLB DNS query refused a response for non-existing domains.	DE80453
30.	Unexpected BFD behavior.	DE80466
31.	Logging the times command caused the device to reboot.	DE80605
32.	There was an AppShape++ namespace conflict when using rule Ids that end with digits.	DE80629
33.	SNMP trap 193 is returned for a disk space issue when it was not included it its MIB.	DE80689
34.	The Secured Web Applications (secwa) pane did not display on a standalone device.	DE80695

Item	Description	Bug ID
35.	On an ADC-VX, the MP caused a reboot.	DE80820
36.	From the CLI, could not connect to real server via Telnet.	DE81212
37.	Using WBM, could not change the protocol TCP/UDP for port 389.	DE81263
38.	The real server health checks treatment was delayed when an unavailable rlogging server was configured.	DE81271
39.	The label in the output regarding MP memory for the `/i/sys/capacity` command was not clear. Changed the label from “mp memory” to “total device memory”.	DE81369
40.	The last digit of the year was missing in the output for some OIDs because arrayLength-1 was assigned with a Null character.	DE81378
41.	A RADIUS UDP health check was sent for RADIUS AA instead of the expected TCP health check when a non-standard destination port was defined.	DE81519
42.	When there is a shared resource (file) that is being accessed by two different operations (for example, putcfg and snmp), there was a bug in the state machine that is responsible for the synchronization, causing the device to reboot.	DE81560
43.	There were DNS errors in the Alteon MP logs.dns due to DNS resolution not being case-insensitive.	DE81599
44.	Back-end SSL with client authentication using static RSA caused a bad MAC address.	DE81675

AppWall Bug Fixes

Item	Description	Bug ID
1.	Cannot change the tunnel operational mode to Passive.	DE78282
2.	Sensitive Parameters are not getting masked in Security Details but are getting masked in Raw Request Data.	DE78706
3.	AppWall GUI gets stuck and affects the Alteon GUI as well in versions 32.4.13 and 33.5.3 and 33.0.6.5.	DE79700
4.	Error in the GUI when accessing Vulnerabilities.	DE79955
5.	File Upload security filter is detecting false-positive.	DE80620
6.	AppWall is trimming requests payload based on Content-Length header value.	DE81172
7.	AppWall does not send complete hostname in the security syslog message.	DE81249

KNOWN LIMITATIONS

The list of known limitations, available to customers only, is available at the following link: https://support.radware.com/app/answers/answer_view/a_id/1036876

RELATED DOCUMENTATION

The following documentation is related to this version:

- *Alteon Installation and Maintenance Guide*
- *Alteon VA Installation and Maintenance Guide*
- *Alteon Getting Started Guide*
- *Alteon Web Based Management Application Guide*
- *Alteon Command Line Interface Application Guide*
- *Alteon Command Reference*
- *Alteon REST API User Guide*
- *Alteon AppShape++ SDK Guide*
- *AppWall for Alteon NG User Guide*
- *LinkProof for Alteon NG User Guide*
- *LinkProof NG User Guide*

North America	International
Radware Inc.	Radware Ltd.
575 Corporate Drive	22 Raoul Wallenberg St.
Mahwah, NJ 07430	Tel Aviv 69710, Israel
Tel: +1-888-234-5763	Tel: 972 3 766 8666