TEST REPORT

Tolly.

#212119
August 2012
Commissioned by EdgeWave Inc.
Testing Conducted in February 2009

EdgeWave ePrism Email Security 2800

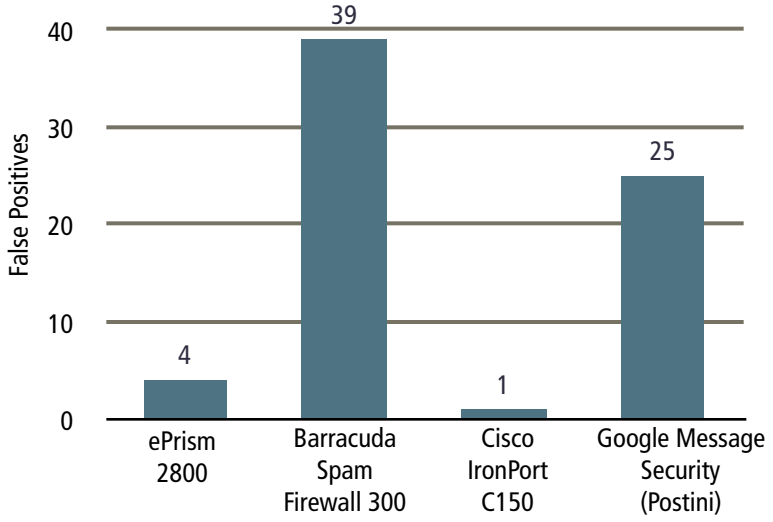
Anti-spam Effectiveness and Feature Comparison Versus Solutions from Barracuda, Cisco and Google

EXECUTIVE SUMMARY

EdgeWave's ePrism Email Security 2800 (2800) achieved a higher percentage of spam detection in this February 2009 test than Barracuda and Google offerings, and delivered performance on par with the Cisco IronPort C150, at a fraction of the cost per user mailbox.

The ePrism 2800 also resulted in up to 90% fewer false positives than Barracuda and Google offerings. Finally, it offers a hybrid solution combining appliance technology with hosted services for backup.

Total False Positives Generated in a Calendar Week by the Anti-spam Solutions Under Test



Source: Tolly, February 2009

Figure 1

THE BOTTOM LINE

The ePrism 2800:

1. Generates just one false positive in over 190,000 inbound messages
2. Blocks 99.991% of 760,470 spam messages with highly effective perimeter defenses and filter stack
3. Requires no filter tuning, with almost zero ongoing administration
4. Combines low cost and control of an onsite appliance with the proactive monitoring and reliability of a hosted service
5. Offers both hosted and appliance-based solutions for E-mail security protection

Results

Inbound Anti-spam Detection Accuracy

Anti-spam solutions must be able to accurately detect and block any unsolicited and/or malware-infested messages while delivering legitimate E-mails properly.

Tolly engineers tested the EdgeWave ePrism Email Security 2800 (referred to as ePrism 2800, hereafter) against Barracuda Networks' Spam Firewall 300 (referred to as Barracuda, hereafter), and Cisco Systems Inc.'s IronPort C150 Email Security Appliance (referred to as IronPort, hereafter), and a hosted service from Google Inc.'s Message Security, powered by Postini (referred to as Postini, hereafter.)

According to the respective vendors, the ePrism 2800 appliance supports 2,500-5,000 users, while the Barracuda Spam Firewall 300 appliance supports 300-1,000 users. Although the 2800 was tested against a Barracuda Spam Firewall

EdgeWave, Inc.

ePrism Email Security 2800

Anti-spam Effectiveness

Tolly. Certified

February 2009

Spam Processing Analysis of EdgeWave ePrism Email Security 2800 Compared to Products Tested from Barracuda, IronPort and Postini

Category	EdgeWave	Barracuda	IronPort	Postini
Inbound Messages Tested [1]	762,962	262,088	1,564,526	13,187
Legitimate messages	2,488	2,738	3,415	2,147
Total spam	760,470	259,311	1,561,110	11,015
Spam blocked correctly [2]	760,398	259,210	1,561,008	10,508
False negatives (Spam mistakenly classified as legitimate E-mail)	72	101	102	507
False positives (E-mail classified as spam but not actually spam)	4	39	1	25
Spam Detection Percentage	99.991%	99.961%	99.993%	95.397%
Spam Error Percentage	0.009%	0.039%	0.007%	4.603%
False Positive Rate [3] (as a ratio of legitimate messages)	1 in 622	1 in 70	1 in 3,415	1 in 86
False Positive Rate [4] (as a ratio of total inbound E-mail messages)	1 in 190,741	1 in 6,720	1 in 1,564,526	1 in 527

Note:

[1] Count of Inbound E-mail messages and spam blocked were taken from the management interfaces of the devices under test

[2] All products under test used different algorithms to calculate total E-mail volume processed in the presence of spam or legitimate E-mails addressed to multiple recipients, thereby resulting in a wide variation in the number of E-mails processed as reported by each product in its user interface, even though the total inbound E-mail volume remained fairly constant through the test duration

- Spam Detection Percentage = [(spam detected / Total spam) * 100]
- Spam Error Percentage = [(False Negatives / Total spam) * 100]
- False Positive Rate = [(False Positive / Total Legitimate Messages) * 100]

[3] This is the statistically accurate False Positive Rate definition.

[4] This is the common (yet technically inaccurate) practice in the industry to quote False Positive Rate as a ratio of all inbound E-mails handled.

Source: Tolly, February 2009

Figure 2

300, the Barracuda Spam Firewall 400 would be more appropriate hardware equivalent to the 2800. The IronPort C150 appliance was the base model Email security appliance from Cisco. The Postini hosted service was the most similar package to the other products under test.

Tests show that the ePrism 2800 delivered a highly effective spam block rate, coupled with a very low False Positive rate. The ePrism 2800 demonstrated superior anti-spam performance in terms of spam detection rate, false negatives and false positives compared to the Barracuda and Postini solutions; and was roughly on par with the IronPort C150 solution. See Figure 2 for more details.

While performance of the IronPort C150 is on par, EdgeWave's ePrism 2800 costs much less per mailbox for a 500-user scenario compared to the IronPort C150. For more details, see the "Cost per Mailbox" analysis table in Figure 3 below.

Test results show that the ePrism 2800 achieves a better overall spam detection rate (99.991% for 2800 vs 95.397% for Postini and 99.961% for Barracuda). The

Cost per Mailbox Analysis and Feature Set Comparison

Pricing	Barracuda Spam Firewall 200	Barracuda Spam Firewall 300	IronPort C150	Postini (Hosted)	ePrism 2505	ePrism 2800
Mailbox Capacity	51-500	1,000	500	500	100-500	5,000
Mailbox Count Priced	500	1,000	500	500	500	5,000
1 Year Price (MSRP)	$2,306.00	$3,006.00	$11,770.00	$6,000.00	$2,398.00	$7,298.00
1 Year Price/Mailbox	$4.61	$3.01	$23.54	$12.00	$4.80	$1.46
1 year price/Mailbox with Vx (or an equivalent) Technology	$9.22	$6.01	$47.08	N/A	$5.99	$1.83

Feature Set	Barracuda Spam Firewall 200	Barracuda Spam Firewall 300	IronPort C150	Postini (Hosted)	ePrism 2505	ePrism 2800
Basic Anti-spam and Anti-virus	✓	✓	✓	✓	✓	✓
Customized Branding	-	-	✓	✓	✓	✓
Per User Settings & Quarantine	-	✓	✓	✓	✓	✓
Onsite Clustering	-	-	$	N/A	✓	✓
Per Domain Settings	-	-	✓	✓	✓	✓
Vx Technology (or similar Load Sharing/Failover mechanism)	-	-	-	N/A	$	$

Key	✓	-	$	N/A
	Supported	Not Supported	Supported - requires additional license	NOT APPLICABLE

Note: All pricing information current as of February, 2009.

- All prices quoted are MSRP including all hardware, support and warranty costs, and assumes that solutions other than EdgeWave require TWO appliances to provide redundancy/load sharing capabilities similar to that offered by EdgeWave's Vx Technology
- MSRP for EdgeWave appliances provided by EdgeWave,Inc.
- MSRP for Barracuda appliances was taken from Barracuda's online purchase portal at https://www.barracudanetworks.com/ns/purchase/purchase.php
- MSRP for IronPort C150 appliance was obtained from an IronPort Authorized Gold Reseller in the month of April 2009
- MSRP for Google Message Security, powered by Postini was obtained from Google's product Web Site at http://www.google.com/postini/compare.html
- Feature set items were taken from official product data sheets

Source: Tolly, February 2009

Figure 3

ePrism 2800 was not only more effective at blocking spam messages, but also was more effective in recognizing good messages (fewer false positives). Postini classified 25 good messages out of 2,147 messages as spam, as did Barracuda with 39 out of 2,738 good messages; while the 2800 classified just four messages out of 2,488 messages.

Users should note that EdgeWave uses the same perimeter defenses, filter stack, user interface – identical technology – in both its appliances and hosted service. So buyers who prefer a hosted solution can take advantage of the better performing EdgeWave filter without having to switch to an appliance.

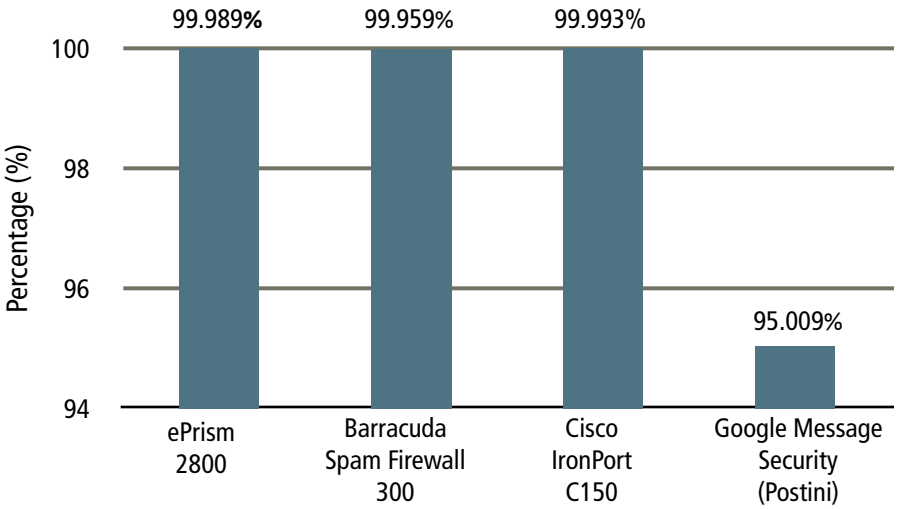
EdgeWave's Vx Technology

Tolly engineers examined EdgeWave's Vx Technology that combines cloud-based service hosted in EdgeWave's data centers distributed geographically, in conjunction with its on-premises hardware anti-spam gateway appliances, to deliver a hybrid anti-spam solution.

Using the Vx Technology, EdgeWave eliminates the need of multiple appliances for redundancy – saving users time and money by filtering E-mails in EdgeWave's data centers as needed in the event of a failure of the on-premises EdgeWave appliance.

Tolly engineers configured the ePrism 2800 appliance to use the Vx Technology, and then simulated an appliance failure by powering off the ePrism 2800 appliance. While the on-premises erism 2800 appliance was offline, engineers verified that spam E-mail continued to be filtered, and legitimate E-mails delivered to the Tolly E-mail server, as E-mails were getting delivered from EdgeWave's hosted servers using Vx Technology.

Daily Average Spam Detection Rate for EdgeWave ePrism Email Security 2800 and Competitors



Note: To clearly illustrate the relative performance levels of solutions tested, Y-axis scales from 94% to 100%

Source: Tolly, February 2009 Figure 4

Hands-on User Experience

Tolly engineers evaluated the user experience on each solution under test in terms of the ease of installation, management console options and functions available to network administrators, and the operational effort required to maintain each device up-to-date.

Initial installation and configuration of the ePrism 2800 appliance into the Tolly corporate network was easily accomplished in less than an hour. Once deployed, Tolly engineers found that the 2800 appliance required no tuning or time consuming ongoing management, often associated with anti-spam solutions.

The ePrism 2800 Web-based administration console was powerful and easy-to-use, and provided all the resources required by the network administrator to manage the solution, generate reports and manage the quarantine folder of the users.

Compared to the ePrism 2800, the Postini solution provided a limited tool set for the administrator to manage the user mailboxes, quarantine folders, report generation, etc. The Barracuda and IronPort solutions offered more administrative options than Postini, but were in turn more complicated to set up than the ePrism 2800.

To configure load sharing or redundancy for the anti-spam solutions, the Barracuda and IronPort solutions would require configuring two physical appliances. On the other hand, EdgeWave greatly simplified this operation by using the Vx Technology, which just required opening a couple of ports on the firewall, and configuring the appropriate changes in the DNS records for the corporate domain. In the case of

an on-site 2800 appliance overload or failure, the E-mail was automatically routed to EdgeWave servers and delivered to the E-mail server with no involvement of the administrator.

Test Setup & Methodology

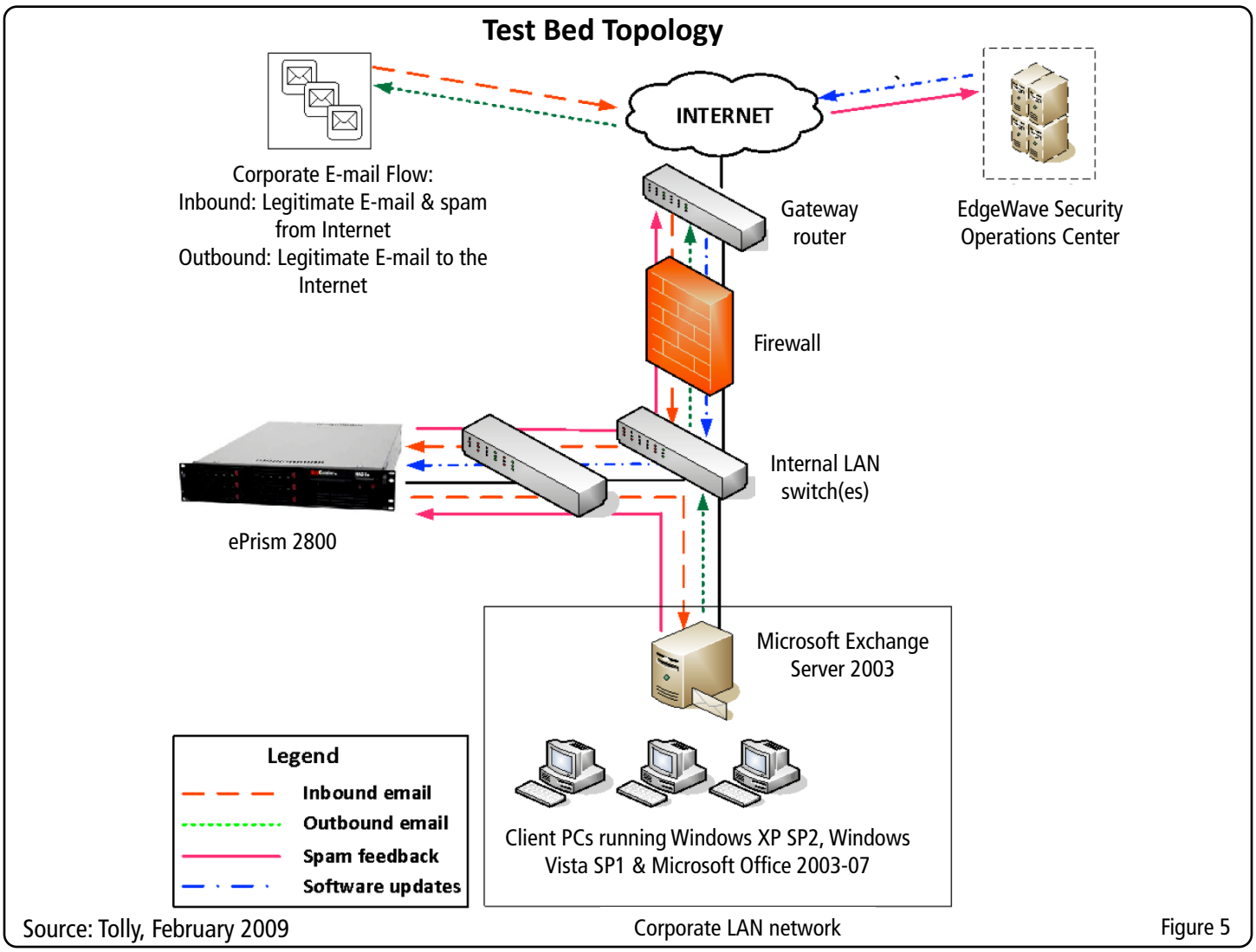
The ePrism 2800 Network Appliance was equipped with two 10/100/1000 Ethernet ports and 480 GB of storage capacity. The Barracuda Spam Firewall 300 was equipped with one 10/100 Base-T Ethernet port and 10 GB of storage. The IronPort C150 was equipped with two 10/100/1000 Ethernet ports and 160 GB of storage capacity.

Tolly engineers tested all platforms with a live E-mail stream of messages in order to test the capabilities and behavior of each product when they were deployed in a live network. This way, all inbound messages were kept intact without modifying sender information and/or SMTP session state.

The test bed consisted of Tolly's internal production network, which includes a Microsoft 2003 Exchange Server running on Window Server 2003 R2 with Active Directory, Juniper NetScreen firewall, ADTRAN NetVanta router, Brocade/ Foundry Network edge switch, etc.

The anti-spam solutions under test were deployed as an inbound anti-spam gateway to scan all incoming mail and relay it to the mail server. The client computers that received mail used the following OS components: Microsoft Windows XP SP2 or Microsoft Windows Vista SP1 and Microsoft Outlook 2003-07.

Tolly engineers modified existing MX record(s) in the corporate DNS server(s) to direct all mail traffic to the anti-spam solutions under test. Engineers applied



Source: Tolly, February 2009

Figure 5

the MX record modification 24 hours prior to starting the production testing so that the DNS update was propagated properly throughout the Internet.

Engineers configured all appliances behind the corporate firewall to analyze SMTP traffic prior to delivering it to the corporate Microsoft Exchange server. Engineers enabled the quarantine feature of all the products tested to quarantine spam. Tolly engineers also used the LDAP query feature available in each device under test to run recipient verification on The Tolly Group's Active Directory server. Each solution under test was configured to monitor all incoming E-mail messages for possible spam (unsolicited bulk E-mail) in the Tolly corporate network.

Engineers made sure that Internet access was made available to each platform to download any newly available anti-spam and anti-virus definitions, or new firmware updates.

The anti-spam solution under test then monitored inbound messages to detect any spam during a period of seven (7) calendar days continuously. Starting on a weekday morning, a new appliance under test was switched into Tolly's corporate network as the E-mail gateway and ending on the same weekday at the same time the following week.

At the beginning of the test any log files, White list, Black list, spam or spam statistics were deleted and the system was reset to factory default setting.

All appliances under test were connected to the Tolly live production network at all times to allow mail-digests to be delivered from the appliance under test to the MTA. Engineers configured different firewall rules to route traffic on port 25 to the appropriate appliance under test, and to allow outbound communication of the appliances under test to communicate with the vendor's servers to obtain software and filtering definition updates.

TOLLY™ common TEST PLAN SERIES

The test methodology used for this report relies upon test procedures, metrics and documentation practices as defined in Tolly Common Test Plan #1058 Anti-Spam Gateway.

To lear more about the Tolly Common Test Plan program visit:

CommonTestPlan.org

Engineers manually checked each user's Outlook inbox and quarantine folder on the anti-spam solution under test between 9:00 am to 11:00 am for any potential False Positives or any False Negatives, and to ensure that the users classified E-mails as legitimate or spam consistent with the test principles.

Metrics for an appliance deployed on Monday were counted on Tuesday morning between 9 am-11 am, and so on. Tolly engineers ensured that the E-mails (legitimate, spam, False Positives and False Negatives) were counted towards the correct product by double checking the unique header inserted by each of the solutions under tests.

Finally, engineers checked the solution under test log files or monitoring systems, as well as users' Outlook inbox, quarantine folders on the solution under test to verify how many messages were received, and how many E-mails were classified and blocked as spam.

Testing was conducted in succession, meaning that engineers first deployed the Postini anti-spam service for a calendar week, followed by Barracuda, then IronPort and then ePrism 2800 each successive week.

Production testing for the Postini service was conducted from 29 October to 04 November 2008; IronPort C150 was tested from 09 December to 15 December 2008; the Barracuda solution was tested from 17 December through 23 December 2008; and the ePrism 2800 testing occurred from 04 February to 10 February, 2009.

A total of 24 E-mail accounts were used for this test. E-mail messages were delivered to the Tolly corporate mail server. Each anti-spam appliance was configured three days prior to the actual production test. The purpose of this was to properly integrate and have the appliance learn the mail and spam characteristics of the Tolly corporate E-mail flow.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
You can reach the company via E-mail at sales@tolly.com, or via telephone at 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, Tolly personnel invited representatives from the competing companies - Barracuda Networks Inc., Cisco Systems, Inc. and Google Inc. to participate in the testing, and provided test plans for review and recommendation. None of the firms responded with interest to participate or provided comments for publication.

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

212119-spvttfm1-wt-2012-07-30-verC