MSExchange.org

MSExchange.org Gold Award ★★★★★

Microsoft MVP Brien Posey Takes a Look at InBoxer's Anti-Risk Appliance

MSExchange.org Gives InBoxer Its Gold Award For A "Perfect 5-Star Rating"

A perfect five-star rating, because it truly is a first-rate product.

Today there are numerous government regulations which require various types of organizations to archive all of their E-mail correspondences. While the scope of the mail retention requirements vary from one set of regulations to another, virtually all of the regulations require organizations to be able to sort and retrieve messages in response to a subpoena. It is this requirement that tends to complicate the otherwise relatively simple task of archiving messages.

There are numerous products and services available that can help organizations to comply with the various E-mail retention requirements. One such product is the InBoxer Anti-Risk Appliance.

The InBoxer Anti-Risk Appliance is designed to provide message archiving and eDiscovery capabilities to enterprise class organizations with up to 30,000 employees. InBoxer offers three different versions of their Anti-Risk Appliance. There is a rack-mounted hardware appliance, a virtual appliance that is designed to run within a virtual server, and a cloud-hosted appliance. For the purposes of this review, I decided to try out the cloud-hosted appliance.

The InBoxer Anti-Risk Appliance's Architecture

The initial setup process required me to provide InBoxer with access to my journaling mailbox. I have to admit that I was initially a bit apprehensive about granting InBoxer access to this mailbox since it was filled with sensitive data, but I felt better when I learned that InBoxer uses a secure datacenter, and that they use a separate virtual server for each customer.

If you really stop and think about it, it makes perfect sense for the InBoxer Anti-Risk Appliance to latch on to the journaling mailbox. Exchange Server is designed in such a way that allows an administrator to create a rule that places a copy of every message into the journal mailbox. The InBoxer Anti-Risk Appliance then downloads the journal mailbox's contents using a POP3 session.

While this approach provides the InBoxer Anti-Risk Appliance easy access to all of the E-mail messages

Brien Posey is an MCSE and has won the Microsoft MVP award six times. Brien has written more than 4,000 technical articles and written or contributed material to about three dozen books. In addition to his writing, Brien routinely speaks at IT conferences and is involved in a wide variety of other technology-related projects.

Brien served as CIO for a national chain of hospitals and healthcare companies. He has also served as a Network Administrator for the Department of Defense at Fort Knox, and for some of the nation's largest insurance companies.

flowing through the Exchange Server organization, there are some other, less obvious benefits to using this approach.

For starters, the InBoxer Anti-Risk Appliance downloads messages from the Exchange Server using the POP3 protocol. As you probably already know, POP3 is a universal messaging protocol that is supported by virtually all mail systems. As such, the InBoxer Anti-Risk Appliance could conceivably be used with mail systems other than Exchange Server, provided that the mail server provides a way to automatically copy each message to a target mailbox.

Another important advantage to the way that the InBoxer Anti-Risk Appliance retrieves mail from an Exchange Server is that the mail server's topology does not have to be restructured.

I have worked with a couple of other mail archiving products that required me to change my messaging topology so that the appliance could be placed between my firewall and my mail server. Not only is the restructuring process a little bit messy, but if the appliance fails then mail flow is disrupted.

Furthermore, I have seen more than one situation in which such an appliance became bogged down and either failed to archive some messages or slowed mail flow to a crawl. Since the InBoxer Anti-Risk Appliance simply downloads messages from the Exchange journal, these types of issues are of no concern.

> ***The appliance caught every "bait" message that I sent.***

The Setup Process

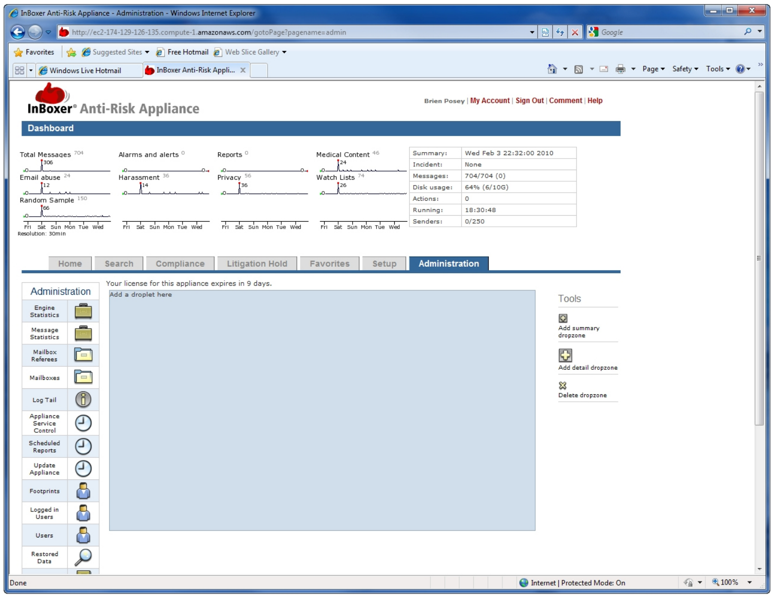
Being that I chose to review the cloud-hosted appliance, I did not have to worry about installing or configuring any software. Instead, a representative from InBoxer asked me to fill out an online form with a few key pieces of information about my Exchange Server organization. This information that the form asked for was very basic, so I was able to complete the form in less than five minutes, and without having to look anything up.

The only configuration task that I had to perform on my end was to enable Exchange Server's journaling feature. I am guessing that most larger organizations would not even have to worry about performing this step since such organizations would typically already have journaling enabled.

A day or two after submitting the required information to InBoxer, I received an E-mail message with a link to my cloud-hosted appliance. I was able to access my cloud-hosted appliance by clicking on the link and signing in using a set of credentials that I had provided to InBoxer.

Using the InBoxer Anti-Risk Appliance

After logging in, I was taken to the product's mail user interface, which you can see in Figure A. As you can see in the figure, the interface is divided into two sections. The upper section is the dashboard display. It allows you to get a quick idea of the types of messages that are passing through your mail servers.



Summary:	Wed Feb 3 22:32:00 2010
Incident:	None
Messages:	704/704 (0)
Disk usage:	64% (6/10G)
Actions:	0
Running:	18:30:48
Senders:	0/250

Your license for this appliance expires in 9 days.

Figure A: This is what the appliance's user interface looks like

The lower portion of the interface is where you can actually interact with the appliance. If you look at the lower left portion of the screen capture, you can see a series of icons. You can drag these icons to the blank area within the workspace to produce various types of reports.

Heuristic Filtering

The appliance is able to display the results instantly.

The primary feature that sets the InBoxer Anti-Risk Appliance apart from competing products is its filtering technology. The easiest way for me to explain how the appliance filters messages is to compare it to the way that a spam filter works.

As I am sure you know, most first generation spam filters were keyword based. In other words, if the filter encountered phrases such as online casino, discount pharmaceuticals, or mail order brides, then it could be relatively sure that the message was spam. Eventually though, the spammers realized that they had to stop using certain words and phrases if they wanted their messages to make it past the filters. In response to the spammers new tactics, many of the anti spam products began using heuristics.

The idea behind heuristics is that it is possible to determine whether or not a message is spam by looking at the message as a whole rather than looking for certain words or phrases. Anti spam product vendors began writing algorithms to analyze the characteristics of messages that were known to be spam, as well as the characteristics of legitimate messages. Eventually, it became possible to reliably determine whether or not a message was spam by examining the message's characteristics.

The InBoxer Anti-Risk Appliance's search feature works in a similar manner. Many of the eDiscovery products on the market require the use of key word searches. In some situations this approach works pretty well. For example, if you need to compile all of the messages sent to or from a certain company, then a key word search will definitely get the job done. Likewise, if you wanted to make sure that employees have not been using swear words in messages sent to the clients, then a keyword search would get the job done. Sometimes though, a keyword search just is not practical.

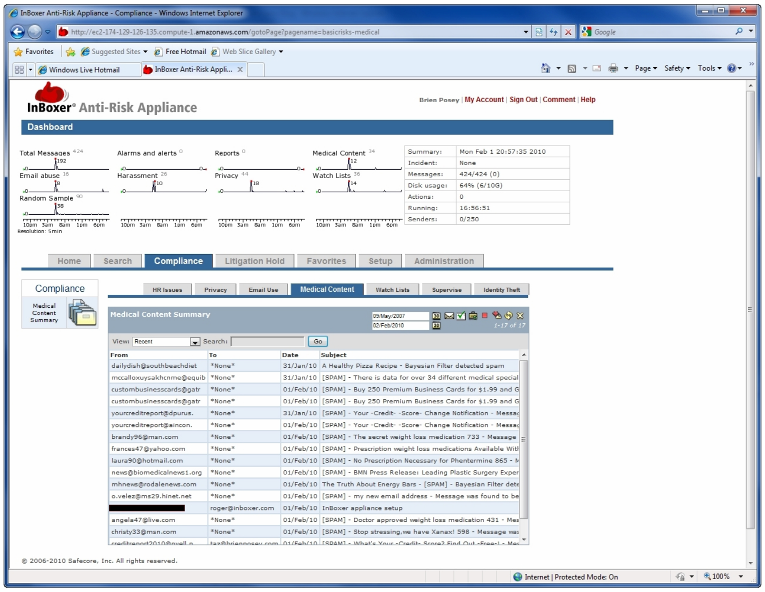
To give you an idea of what I am talking about, imagine that you decided that you needed to protect the organization from lawsuits by actively looking for any E-mail messages that could be deemed as harassment. How could you possibly look for E-mail harassment using a key word search? While you might be able to come up with a few good search terms, searching on those terms alone would not be a good solution because it would be far too easy for a message to slip through the cracks.

This is where the InBoxer Anti-Risk Appliance's filtering engine comes into play. The appliance uses heuristics to look at a message's characteristics. That way, the InBoxer Anti-Risk Appliance can determine whether or not a message's characteristics are consistent with known forms of harassment, rather than simply looking for keywords. Of course harassment is not the only thing that the InBoxer Anti-Risk Appliance can look for. The appliance contains numerous filters designed to look for things like privacy and HR issues.

While this approach to message filtering sounds good in theory, I was really curious as to how well it would work in the real world. What I found was that the InBoxer Anti-Risk Appliance tended to err on the side of caution. The appliance caught every "bait" message that I sent, but there were also some false positives.

To get a better idea of what I am talking about, take a look at Figure B. This figure shows the appliance's Medical Content filter. InBoxer included this filter in the appliance because HIPAA laws prohibit certain types of medical information from being disclosed. Being that I do not work in the medical field, I was really curious what this filter would uncover.

As you have probably noticed, most of the messages that the filter reported were spam. This brings up an important point. The InBoxer Anti-Risk Appliance is designed for use in large organizations with thousands of mailboxes. My own organization is nowhere near that large. This being the case, I configured my



InBoxer Anti-Risk Appliance - Compliance - Windows Internet Explorer

http://ec2-174-129-126-135.compute-1.amazonaws.com/gotoPage?pagename=basicrisks-medical

InBoxer® Anti-Risk Appliance

Brien Posey | My Account | Sign Out | Comment | Help

Dashboard

Summary:	Mon Feb 1 20:57:35 2010
Incident:	None
Messages:	424/424 (0)
Disk usage:	64% (6/10G)
Actions:	0
Running:	16:56:51
Senders:	0/250

Medical Content Summary

09/May/2007
02/Feb/2010
1-17 of 17

View: Recent Search: Go

From	To	Date	Subject
dailydish@southbeachdiet	*None*	31/Jan/10	A Healthy Pizza Recipe - Bayesian Filter detected spam
mccalloxuysakhcnme@equib	*None*	31/Jan/10	[SPAM] - There is data for over 34 different medical special
custombusinesscards@gatr	*None*	01/Feb/10	[SPAM] - Buy 250 Premium Business Cards for $1.99 and G
custombusinesscards@gatr	*None*	01/Feb/10	[SPAM] - Buy 250 Premium Business Cards for $1.99 and G
yourcreditreport@dpurus.	*None*	31/Jan/10	[SPAM] - Your -Credit- -Score- Change Notification - Messag
yourcreditreport@aincon.	*None*	01/Feb/10	[SPAM] - Your -Credit- -Score- Change Notification - Messag
brandy96@msn.com	*None*	01/Feb/10	[SPAM] - The secret weight loss medication 733 - Message
frances47@yahoo.com	*None*	01/Feb/10	[SPAM] - Prescription weight loss medications Available With
laura90@hotmail.com	*None*	01/Feb/10	[SPAM] - No Prescription Necessary for Phentermine 865 - M
news@biomedicalnews1.org	*None*	01/Feb/10	[SPAM] - BMN Press Release: Leading Plastic Surgery Exper
mhnews@rodalenews.com	*None*	01/Feb/10	The Truth About Energy Bars - [SPAM] - Bayesian Filter dete
o.velez@ms29.hinet.net	*None*	01/Feb/10	[SPAM] - my new email address - Message was found to be
[redacted]	roger@inboxer.com	01/Feb/10	InBoxer appliance setup
angela47@live.com	*None*	01/Feb/10	[SPAM] - Doctor approved weight loss medication 431 - Mes
christy33@msn.com	*None*	01/Feb/10	[SPAM] - Stop stressing,we have Xanax! 598 - Message was
creditreport2010@nvell.n	taz@brienposey.com	01/Feb/10	[SPAM] - What's Your -Credit- Score? Find Out -Free-! - Mes

© 2006-2010 Safecore, Inc. All rights reserved.

Figure B: The Medical Content Filter helps to ensure HIPAA compliance

Exchange Server to journal all of the messages passing through the transport pipeline; including spam. Doing so allowed me to test the appliance on a larger number of messages than I would have otherwise been able to. In the real world, it is important that you do not journal spam because, as you can see in the figure above, excessive spam can greatly skew the filter results.

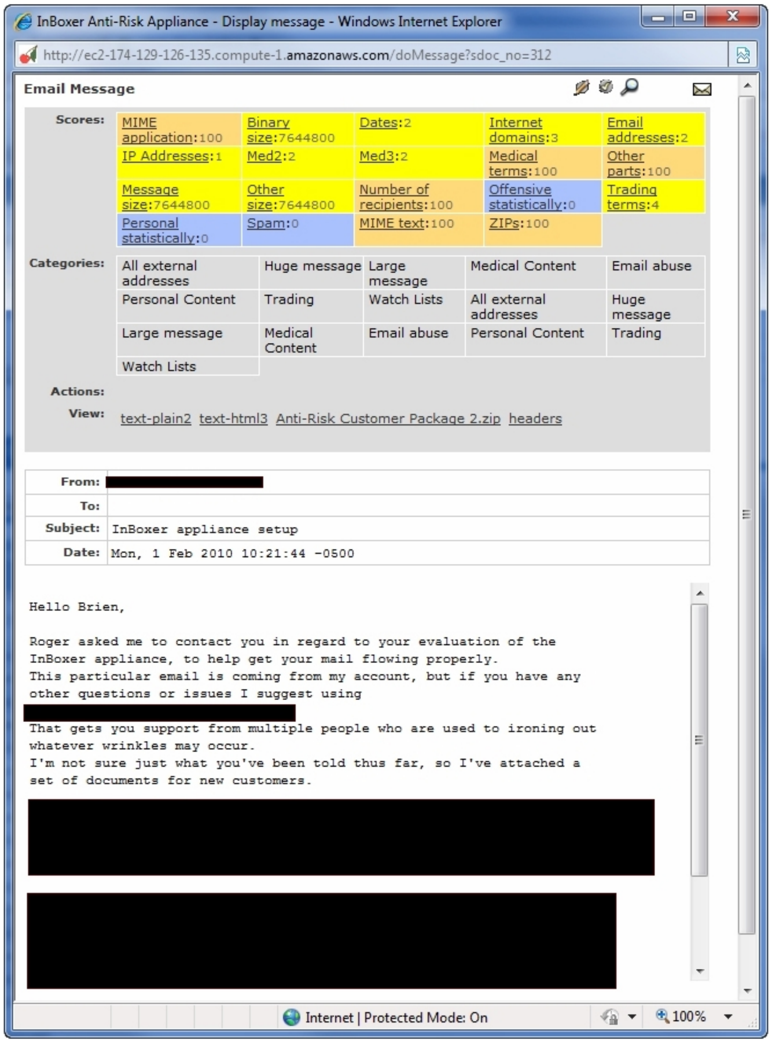
> ***I was impressed by the fact that the InBoxer appliance picked up on this message.***

With that said, it is pretty easy to see why most of these messages were flagged as containing medical content. The message's subject lines refer to everything from healthy pizza recipes to prescription weight loss. You might have noticed, though, that one of the messages has the subject line "InBoxer appliance setup". This was a message that someone at InBoxer had sent me in response to a question that I had about this review. I couldn't imagine how this message could possibly have been reported as containing medical content. Thankfully, the appliance allows you to click on a message's subject line and read the message.

If you look at Figure C, you can see the window that was displayed when I opened the message. The black sections are areas that I have blacked out to protect the sender's privacy. At any rate, you will notice that the message contains the phrase "ironing out whatever wrinkles may occur". The word "wrinkles" is what caused the message to be classified as containing medical content.

I have to say that I was impressed by the fact that the InBoxer appliance picked up on this message.

Although it was a false positive, the message very well could have contained medical information. The term "wrinkles" is not something that I would have thought to include



InBoxer Anti-Risk Appliance - Display message - Windows Internet Explorer

http://ec2-174-129-126-135.compute-1.amazonaws.com/doMessage?sdoc_no=312

Email Message

Scores:				
MIME application:100	Binary size:7644800	Dates:2	Internet domains:3	Email addresses:2
IP Addresses:1	Med2:2	Med3:2	Medical terms:100	Other parts:100
Message size:7644800	Other size:7644800	Number of recipients:100	Offensive statistically:0	Trading terms:4
Personal statistically:0	Spam:0	MIME text:100	ZIPs:100	

Categories:				
All external addresses	Huge message	Large message	Medical Content	Email abuse
Personal Content	Trading	Watch Lists	All external addresses	Huge message
Large message	Medical Content	Email abuse	Personal Content	Trading
Watch Lists				

Actions:

View: text-plain2 text-html3 Anti-Risk Customer Package 2.zip headers

From:	[redacted]
To:	
Subject:	InBoxer appliance setup
Date:	Mon, 1 Feb 2010 10:21:44 -0500

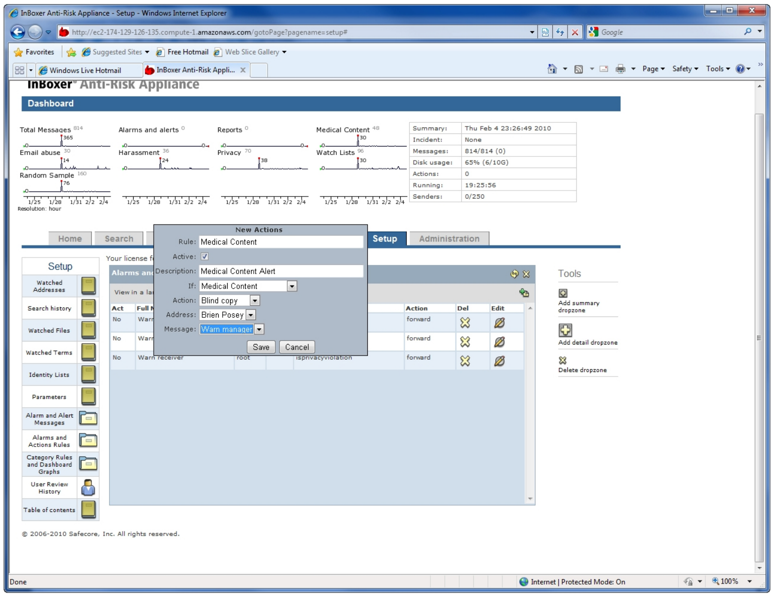
```
Hello Brien,

Roger asked me to contact you in regard to your evaluation of the
InBoxer appliance, to help get your mail flowing properly.
This particular email is coming from my account, but if you have any
other questions or issues I suggest using
[redacted]
That gets you support from multiple people who are used to ironing out
whatever wrinkles may occur.
I'm not sure just what you've been told thus far, so I've attached a
set of documents for new customers.
[redacted]

[redacted]
```

Figure C: The appliance allows you to open any message in a keyword search, and yet the appliance found it.

Although false positives can be frustrating at times, I believe that it is important for a product sold as an "Anti-Risk Appliance" to err on the side of caution rather than potentially overlooking messages.

Alerting

In the example above, I manually checked to see if any messages had been flagged as containing medical content. It does not have to be that way though. The appliance contains a very flexible alerting mechanism. For example, Figure D shows an alert that is triggered by messages containing medical content. In this case, if such a message is detected then the message is blind copied to a designated contact, and a manager is alerted.



InBoxer Anti-Risk Appliance - Setup - Windows Internet Explorer

http://ec2-174-129-126-135.compute-1.amazonaws.com/gotoPage?pagename=setup#

Summary:	Thu Feb 4 23:26:49 2010
Incident:	None
Messages:	814/814 (0)
Disk usage:	65% (6/10G)
Actions:	0
Running:	19:25:56
Senders:	0/250

New Actions

Rule: Medical Content

Active: ☑

Description: Medical Content Alert

If: Medical Content

Action: Blind copy

Address: Brien Posey

Message: Warn manager

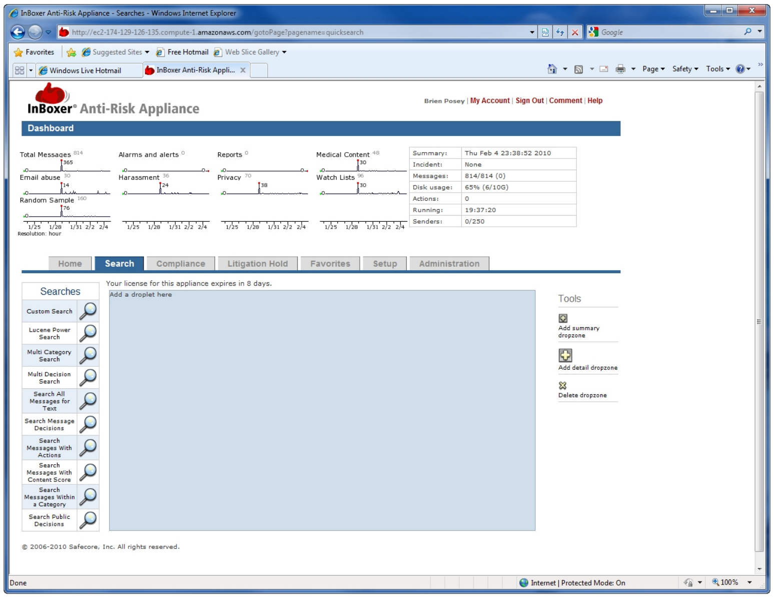
© 2006-2010 Safecore, Inc. All rights reserved.

Figure D: The InBoxer Anti-Risk Appliance can generate alerts when certain types of messages are detected

Indexing

One of the big problems with many eDiscovery applications is that queries tend to be really slow. The InBoxer Anti-Risk Appliance seems to solve this problem though, through the use of something called Pre-Search. Pre-Search executes more than eighty of the most common queries in the background. That way, whenever an administrator performs one of the more common queries, the appliance is able to display the results instantly.

Of course this does not mean that administrators are limited to performing the most common search queries. In fact, the InBoxer Anti-Risk Appliance includes a multitude of different search utilities, as shown in Figure E. These utilities allow administrators to perform anything from natural language searches, to content category searches, to complex custom searches. During my testing, I experimented with several different types of searches. I found that the appliance returned my search results very quickly, even when I searched on something that was outside of the norm.



InBoxer Anti-Risk Appliance - Searches - Windows Internet Explorer

http://ec2-174-129-126-135.compute-1.amazonaws.com/gotoPage?pagename=quicksearch

Summary:	Thu Feb 4 23:38:52 2010
Incident:	None
Messages:	814/814 (0)
Disk usage:	65% (6/10G)
Actions:	0
Running:	19:37:20
Senders:	0/250

Your license for this appliance expires in 8 days.

© 2006-2010 Safecore, Inc. All rights reserved.

Figure E: The InBoxer Anti-Risk Appliance offers a plethora of search tools

Conclusion

In conclusion, I found the InBoxer Anti-Risk Appliance to be a solid and reliable product. The user interface was very intuitive, and the feature set seemed to be very well thought out. Sadly, there are several nice features that I was unable to discuss due to space limitations. These features include things like litigation hold and audit trails.

A solid and reliable product... a perfect score.

I am always reluctant to give the products that I review a perfect score, because I fear that perfect scores will be perceived as personal bias. In this case though, I have to give the InBoxer Anti-Risk Appliance a perfect five-star rating, because it truly is a first-rate product.

TechGenix

Original review text may be found at:
http://www.msexchange.org/articles_tutorials/product-reviews/inboxer-product-review.html

InBoxer

InBoxer
One Van de Graaff Drive | Burlington, MA 01803 USA
U.S.: 781 272 1140 | UK: 0871 733 6293 | www.inboxer.com