

myhosting.com CEO and President Tony Yustein is passionate and opinionated about Windows web hosting. A former regional director for Microsoft, Yustein founded Toronto's SoftCom Technology in 1997, and has built it into a significant player in both web hosting and webmail. In an interview with Rich Miller, Yustein shares his views on Microsoft's approach to hosting and security, and the road ahead for webmail and spam.

Q. In April myhosting.com introduced a "blended hosting environment" for shared hosting customers that includes both Windows and Linux accounts within a single plan. You'd previously been a Windows-only provider. What led you to add Linux hosting, and to adopt this particular approach?

A. Simply put, demand from our customers. Our experience with our customers showed us that it's not the operating system which drives their choices, but the availability of the applications. Most popular web applications are either in Perl or PHP and use MySQL. We had two options: either install Perl, PHP and MySQL on Windows platform, or offer our customers the native platform which these tools are developed on. This is the main reason we decided to offer a native Linux offering at no additional cost to our web hosting customers. So they get 2 for the price of 1, both Windows Server 2003 and Linux under the same account.

Q. What type of customers are most interested in the blended hosting environment, and how are they using it?

A. Customers who use Microsoft FrontPage to design their pages but also want to run enhanced web applications which utilize PHP, Perl and MySQL are the ones who activate their free Linux account. They combine the power of ASP.Net and PHP on their native environments to create the best website possible.

Q. You used to work at Microsoft, and have been a strong proponent of Windows hosting and the .net initiative. At the same time, you were recently quoted in Business Week as saying that Microsoft has "lost its perspective, concentration, and vision in operating systems." What's your analysis of the strengths and weaknesses of Microsoft's hosting products and strategy?

A. Unfortunately, I feel so passionate about Microsoft that I can not be politically correct

when I criticize my friends at Microsoft. After all Mr. Gates is the reason why I got into the IT industry in the first place. I think somewhere up at the ranks of Microsoft executives, there was a decision made that the shared hosting market was not their top priority. Nobody at Microsoft will publicly accept this, but I think it's the truth. Microsoft wanted to concentrate on dedicated Windows hosting, which drives more revenue per customer, and is also much easier to support in a technical way. I can clearly see that Windows Server 2003 was designed to support dedicated hosting, and shared hosting was not a priority in the total design.

As an example, you can not run Microsoft Access databases for shared hosting environment under the fully secure option of ASP.Net environment. This is driving many of our customers mad. Many hosting companies disable full security just to enable Access support under ASP.Net, but as a byproduct of this, customers can see each other's files on a shared environment. That's one of the reasons why people want to use MySQL - because they don't need the power of Microsoft SQL, and they can't use Access under ASP.Net. On the other hand, Microsoft Exchange server is very well designed and suited for shared hosting environments. Actually we are working on a very large scale Microsoft Exchange project, but it seems like I'm off the Christmas card list at Microsoft because nobody is returning my calls.

Q. How would you assess Microsoft's short-term and long-term approaches to its Internet security issues?

A. This is the toughest question. I think there is more that Microsoft can do in the short term. I don't want to get too technical, but there are methods where Microsoft can ban a compromised DLL to execute under Windows, but they haven't utilized those yet. To give an example, a faulty FrontPage server extension DLL which was identified to have buffer overflow security problems, can still be uploaded by a hosting customer in a non-privileged directory, which results in the buffer overflow creating privileged accounts for the hacker. To disable this you have to disable file upload, which is of course out of question in a hosting environment. For the long term, we have Longhorn on the horizon, and we will have to wait and see.

Q. In recent months, myhosting.com has consistently been among the 10 most reliable hosting providers tracked by Netcraft, and the best-performing provider running its site on

Windows Server 2003. What, in your experience, are the key factors in delivering this level of reliability with Windows Server 2003?

A. Again, Windows Server 2003 is a perfect solution for dedicated hosting. It's extremely reliable with the new IIS 6 and has very nice auto recovery options for the web sites. Of course, we know how to tweak this to perform the best. We have extensive know-how about the Windows platform developed over the last eight years.

Q. SoftCom also owns and operates mail2web.com, which allows users to fetch email via the web. Many ISPs now offer webmail access to their users, and the Net's best-known brands are major players. What are the key competitive issues in the webmail business, and how is mail2web differentiating itself?

A. mail2web.com is a very important component of our business. It was developed eight years ago out of an actual necessity I had which involved firewalls and access to my private e-mail while at work. The key differentiator for mail2web.com is that we do not provide a new e-mail address for mail2web.com users. All the ISPs who provide web based e-mail systems are providing the e-mail space and name as well. Even though we do that through myhosting.com, mail2web.com's focus is how to access e-mail already stored on a POP3 or IMAP system. This focus enabled us to fine tune and develop a very special know-how for web based access to e-mail. mail2web.com's priority is to make it as easy as possible for the user to access their e-mail. That's why the interface is very clean, light and free of Java or ActiveX components.

Millions of users now use mail2web.com through their PDAs, mobile phones, Internet kiosks and basically any Internet connected computer anywhere in the world. We see that many of the ISPs who have their web based e-mail retrieval services do not maintain these very well. Most of the time they are not reachable, and even when they are reachable they do not perform well. That's why many customer support agents who work for those ISPs, recommend mail2web.com when everything else fails. Also, imitation is considered the best method of flattery and everybody knows mail2web.com is the real deal in this market. It's available in 16 languages, it's free, and it has users from more than 190 countries and more than 14 million unique users. Alexa rates it in the top 500 of all the global web sites in the world. And have I mentioned it's free? :-)



AUGUST 2004

Q. Which approaches to the spam problem do you find most promising? What's your outlook on spam management for hosting e-mail providers?

A. The only approach which will work is to stop the spam at the source, period. I think most of the MPs in various countries don't have an e-mail address; otherwise we would be seeing more legislation about preventing spam. I find it impractical to charge people to send e-mail, or to develop technology to block spam. Why should we create another industry like the antivirus industry? It's simply not needed if we can stop the spam at the source.

It's simple as stopping petty crime; you just need the right legislation and the right enforcement. Meanwhile, I value the technologies like DSPAM which is an open-source statistical anti-spam filter. I suggest that e-mail hosting providers drop the virus containing messages and do not forward any outgoing traffic which has spam or viruses by enabling outgoing checks as well as incoming checks. Also, it's not that difficult to find which networks these spammers are using and the problem can be dealt on the network peering level as well. Unfortunately, more spam means more bandwidth revenue, more hard disk space revenue for ISPs and more revenue for anti-spam software companies. ISPs should realize it is not ethical to turn a blind eye to the spam problem because it brings some more revenue and should act responsibly to cut the spam at the source.