UNDER THE BRIM AT THE LINUX LEADERS

RED HAT

It's the world's best-known Linux brand, but its move to Enterprise Linux angered as many as it pleased. Just what is it about Red Hat that has made it so successful, and where is it going in the coming years?

As one of the largest and most well-known Linux companies, Red Hat is a success story that few people really know that much about. As a Linux distribution, it was founded back in 1994 by Mark Ewing, an entrepreneur who used to wear his grandfather's red Cornell lacrosse hat whilst at Carnegie Mellon. It then merged with ACC Corporation in 1995 (when ACC's owner, Bob Young, moved up to CEO of Red Hat), and merged again with Cygnus Solutions in 1999. But it's only been since 2002, when Red Hat Linux Advanced Server was first launched, that Red Hat's real forte came to light.

Since moving to its Enterprise Linux strategy, Red Hat has gone from strength to strength. Its home-user product, Red Hat Linux, was spun off into the Fedora Project in September 2003, so Red Hat's primary focus is now enterprise customers. Fedora is its test bed for new technologies and enthusiast use, which means that Red Hat's Enterprise Linux line – consisting of Desktop, for client machines; WS, for high-end workstations; ES, for departmental servers; and AS, for mission-critical servers – always uses tested, certified, rock-solid code that can be relied upon.

Red Hat has also worked hard to promote its service model, which has revolutionised the OS marketplace. The Red Hat Network (RHN) is where users can download their software CDs, patches, and documentation all in one place, as well as access all Red Hat's support options. Big companies such as Rackspace proudly boast to prospective customers that they have more certified Red Hat technicians than any other managed hosting company, while developers such as Discreet – which is porting all its applications to Linux – are choosing Red Hat Enterprise Linux as *the* supported OS.

This is the market position most companies can only dream of, but its one that Matthew Szulik – Red Hat's CEO, Chairman and President – has worked hard for. Since Szulik took over from Bob Young as CEO in 1999, Red Hat has launched the RHN, introduced its Enterprise Linux strategy and the Fedora Project, opened up a large R&D facility in Massachusetts, and even seen its share prices go higher than Sun Microsystems.

Eight out of the top ten global investment banks are already Red Hat customers, and now that the new Red Hat Desktop has been launched, you'd be forgiven for wondering how Red Hat can top its achievements. We were curious too, so we caught up with Matthew Szulik after the announcement of Red Hat Desktop to talk about that decision, Fedora, training, and whether or not Red Hat can now make a product he'd be comfortable letting his mother-in-law use...

LINUX PRO: **Red Hat has had an interesting dalliance with the desktop market. You always had Red Hat Linux providing for home users, but there was almost a retreat when it was spun off into Fedora. Has this been a linear progression towards your goals, or has there been some sort of change of plan?**

MATTHEW SZULIK: Let me give you my perspectives, and we can maybe debate it. First of all, if you go back to Red Hat 5.0, or near that, to 4.0, 5.0, 5.1, 5.2, which all had the retail channel for distribution – Dixons, CompUSA, *etc.* I think it ran on anything that an end-user wanted it to. You had a technically

literate person who would either download it or go to a retail outlet because they've heard about this thing called Linux, and they had the technical aptitude to install it.

I think – not by design – there was this marketplace where it was used as a client operating system by a technically literate person: it wasn't a productivity suite at that time. I was using *PINE* and *Emacs* back in '96 and '95, so clearly from an end-user perspective it wasn't a productivity suite at all; but it was the retail channel of distribution that made it available – that positioned it as a client operating system. It wasn't strategy, it wasn't focused, it was just through distribution that it ended up there.

What ended up happening was that that technology started to find its way into the enterprise market, and we were starting to find customers looking to put Oracle 9i on Red Hat Linux 9 – there was no certification, there was no testing, there was no there was no development model to take this product that was being updated and enhanced and thrown out into the retail channel three or four times a year. That had no relationship with what an enterprise computing buyer wanted to use. The worst part was becoming a branding nightmare: customers – from the enterprise to governments – were putting DB2 or SAP on it and becoming increasingly frustrated by it. It was great technology, but it was never built to be an enterprise-class OS, so we had to make two decisions: the Fedora decision, as everyone is now familiar with, but second of all we had to learn how to build – as an Open Source community and a vendor – a worldwide development model and service model for an enterprise-class operating system.

And I think a lot of commentators are amazed at how naïve people are about the complexities about building an operating system that's enterprise-class; especially the fact that it's going into environments today that may have an EMC component, that's interfacing through Infiniband or iSCSI, it's running or a 64-bit Intel or AMD architecture. The service competency, the application competency, and the integration competency around this thing that some people still think of as a free OS is incredibly hard, and expensive to maintain.

We had to make sure that we did a good job at servicing that kind of customer, and I think we're getting there after two-and-a-half years in the enterprise.

The other issue is among all the talk of the Linux client, whether it's Lindows, or Xandros, Lycoris, or all the rest of these guys... God love 'em that they're doing what they're doing. The issue is: how do you monetize that? How do you build a financial relationship so that you're able to pay the money for that product to be serviced? We are a publicly traded company, and I have that responsibility. Over the last three or four years, guys like Havoc Pennington have been going out and visiting customers, only to be told, *"We don't want better word processing, we don't want a better spellchecker, and our pivot tables work just fine. But you know what? Our cost of administration is going up quarter over quarter, year over year."* A large university in the US got hit by one of the recent viruses, and had to reboot its entire server network over 19 universities. The school was down and without email for four days. The message to us is, *"Solve the security problem and I'll pay you money. Build more automation and into my system administration practices."*

These became recurring themes. We believe that if we could provide parity in the productivity suites – the improvements in *Mozilla,* such as the UML tools that have been built-in, a lot of the security improvements that have been built into the X Windows system, going on to things like ExecShield (more on this later), the 2.6 kernel and SELinux. We think we've got value there at a very low price for the enterprise and government buyer.

"I WAS USING *PINE* AND *EMACS* BACK IN '96 AND '95, SO CLEARLY FROM AN END-USER PERSPECTIVE, RED HAT WASN'T A PRODUCTIVITY SUITE AT ALL."

RED HAT APPLICATIONS

Tailoring your flavour

BEYOND THE STOCK THREE versions of RHEL, there is also a small selection of other products that add more functionality. The current line-up includes *Cluster Suite, Content Management System, Developer Suite,* and *Portal Server*, each of which seamlessly plug-in to various editions of RHEL and build upon the existing functionality. *Cluster Suite* was previously bundled with RHEL 2.1 AS, but it was reportedly spun off into a separate product as of RHEL 3 so that Red Hat could better judge the extent to which it was being used and thereby predict how much money to invest in future work.

Now that Red Hat has completed its acquisition of Sistina Software (makers of *LVM* – the *Linux Volume Management* software), it's now only a matter of time before Red Hat launches a new member of their application family based upon Sistina's *GFS* product, which is the enterprise-level version of *LVM*. Combined with *Cluster Suite*, this new clustered filesystem support will really put RHEL at the cutting edge and give businesses that extra competitive advantage in the storage marketplace.

It was never an issue of "if", it was always "when". If you look at our hiring practices over the last few years, you'll see that we have selectively gone out to recruit the best in the world, the same way we did with the Linux kernel.

***LXP:* Obviously it was quite difficult for Red Hat to get away from the 'six-monthly hit' of your releases...**

MS: Inside the company, I call that *"the heroin addiction of Red Hat"*!

***LXP:* Now that you're away from that, you have more time to think and more time to plan. A few years ago, training made up a substantial amount of your revenue, but now there's also subscription. Is this business model going to change again over the new few years?**

MS: I don't want to bore you with the economic intricacies of the business, but this is a great story that should be told to other entrepreneurs. If you look at our retail business a few years ago, it was the dominant part of our revenue stream. Today, it's almost gone. That was a conscious strategy to get rid of the addiction, because it was causing enormous customer dissatisfaction. Plus, it's very expensive to sell your products through retail channels and distribution – you've got a lot of people between you and the customer, so there was very little left for Red Hat.

Learning services continue to be an important area of investment for Red Hat. There's a guy called Pete Childers, who's built this program from the ground up – he's been at Red Hat for six years. It's really an outstanding product: we now have online self-certification, and a pre-assessment program so that you can get a good idea of your skill level before you start, and then build your skills appropriately. Learning resources like our consulting services will continue to be an important part of our business, but at the core we're still a technology and software company.

***LXP:* How many Red Hat Certified Engineers (RHCEs) do you have now?**

MS: I think it's around 10,000 – a very large number – so it's an experiment in an evolving market, which is now moving into areas of greater sophistication. We purchased a company called Sistina, which brought us a very robust clustered filesystem. We're starting to get into

the storage and storage management markets for Linux, so it's kind of amazing that we're now building highly strategic, robust, critical information systems.

***LXP:* In RHEL 2.1, the clustering services were actually built into the AS product. In RHEL 3, it's now a separate purchase. SUSE's new Enterprise Server product is slated to have clustering built-in, so what made you want to remove it?**

MS: The main reason was that we found customers simply weren't using it – it floored us! We asked people if they knew whether they had it, and the answer was usually *"No"*.

***LXP:* But it's still an important market for the future?**

MS: I think it's a critically important market, but timing is key – what we've learnt is that although the functionality was there, the customer wasn't ready to receive it: it didn't matter how good the code was.

***LXP:* Going back to your overall strategy, would it be fair to say that Red Hat is focusing on subscription-based computing?**

MS: Absolutely. That happened in 1997 – we figured that the bet was that customers would want to have always-on, always-reliable, always-secure information systems, and we felt that the proprietary technology didn't do that. We took a big gamble, and we were one of the first to roll out a subscription model so that the customer gets continuous improvement of the product as fast as it becomes available.

***LXP:* In RHEL 2.1, products were more mature, whereas in RHEL 3 some products were released just weeks before final release. Was this a conscious decision?**

MS: The big issue for the enterprise market is stability, so all of our decisions are now focused on stability – maintaining binary compatibility so we're not breaking ISV applications – important when you consider that we're going into some highly sophisticated environments; for instance, there's a large investment bank with over 12,000 servers that runs all its mortgage and banking transactions on Red Hat Linux.

A big public issue that we faced recently was backporting some of the 2.6 kernel functions. That doesn't happen by accident – that happens because we want to make damn sure that it's certified and it's tested with the ISV applications before it's rolled out to our customers . SUSE has been doing that too – it's not a new idea by any means, but security and stability in the operating environment is pre-eminent.

"IF YOU LOOK AT OUR RETAIL BUSINESS A FEW YEARS AGO, IT WAS THE DOMINANT PART OF OUR REVENUE STREAM. TODAY, IT'S ALMOST GONE."

Now, having said that, this is why we introduced Fedora – there will always be customers who want the latest and greatest, there always will be developers who want the very latest version of *The GIMP*, and we want continue to introduce new technologies like SELinux to get that out there and let developers work on it and hack on it – even though there's no expectation for certification on it – then move that technology upstream once it has been stabilised.

***LXP:* Would you say you share a close relationship with Oracle and other ISVs?**

MS: I think the advancement we're making on our business processes relationships is good, because these vendors have global responsibilities. Whether it's Veritas, Oracle, or IBM, they have global responsibilities, technical certification, hardware certification and driver support; and it's really, really expensive to support. I think it's really cool that we all work hard to ensure that ISVs continue to support Linux.

LXP: So will Red Hat Desktop (RHD) be something your mother-in-law will be able to use?

MS: My mother-in-law will use it in the next thirty days!

***LXP:* Does *she* know that yet?**

MS: I just had this discussion with her on Sunday! If you've used the Red Hat Network, you'll know it's a pretty cool piece of technology, and for the right customer I think it's going to be a very good improvement.

***LXP:* With the Enterprise Desktop, do you think there's a bigger market for it in Europe than in the US?**

MS: Definitely, which is why we launched it in London!

***LXP:* Why do you think that is?**

MS: I think a lot of US companies took hold of the Microsoft Software Assurance scheme, and as a result made very large financial commitments to Microsoft. Those contracts continue until 2006 or 2007, and that will

WHAT'S COMING IN RHEL 4?

Gazing into Red Hat's crystal ball...

THOUGH RED HAT ENTERPRISE LINUX ONLY went on sale late last year, Red Hat has long been working on its successor: Red Hat Enterprise Linux 4. This release will be based on Fedora Core 2, which means that features such as SELinux and ExecShield are incorporated as standard, but it will also feature a 2.6 kernel and a system built using *GCC 3.4*. As this is a big step forward, libraries to enable full system compatibility with RHEL 3 will be bundled as standard, and it may also include RHEL 2.1 compatibility libraries also, so that products written for any of the three versions will work flawlessly on RHEL 4.

Still to be finalised as yet is the exact version numbers of the supporting apps, but it will definitely include latest stable releases of GNOME, *Mozilla*, *Evolution*, and other usual suspects. Also in the air is the exact set of SELinux policies to be shipped as standard – this will have a great impact on the flexibility and learning-curve of SELinux on deployed machines; but to begin with, we expect many administrators will just use the default policy that essentially disables SELinux. Furthermore, Red Hat may well make newer policies available through the Red Hat Network after the product has shipped.

Red Hat's partners already have the alpha release of RHEL 4, and the beta program is set to kick off in September. All being well, the final product should ship early in 2005 – surprisingly hot on the heels of RHEL 3. But, given the number of backports of features from the 2.6 kernel that are currently in RHEL 3, it's probably not so much work to make the upgrade once SELinux and ExecShield are finalised!

probably turn out to be a positive thing for Red Hat because there are a lot of CIOs and a lot of enterprise and government customers who are looking at what they spent and are not happy with that. Customers are not dumb – they know what it feels like to be taken advantage of!

Secondly, there are still many Windows 95/98 and NT 4.0 machines that have yet to be upgraded – they have no Active Directory presence. Look at the kind of improvements that are happening – the usability of the product, the directory services, the security that's becoming increasingly available. It's happening just like the Linux OS did – it's improving by the minute.

I think Europe – because of the lack of legacy – is going to move forward, open-minded, towards Open Source software. There are also the countries that have just recently joined the EU, as well as India, China and Russia – our best developers come from Europe, hands-down.

***LXP:* In the Red Hat Desktop announcement, you said that it would lower TCO, but one of the biggest factors in TCO is the cost of support. What new improvements are there in RHD that are going to make it easier to manage on a company-wide basis?**

MS: One helpful feature is *Kickstart*, which is the ability to build another system image based upon an installation. That functionality itself – which is now two years old – has helped more system administrators than we know: it gets rid of the Microsoft problem of making an image for each server. Imagine that functionality being extended to the client, for example. I think when we start to see the SELinux kernel being introduced with policy management, I think that's really making a statement, really servicing the needs of management infrastructure.

Today, if you look at why we have so many security violations, it's not that the technology hasn't been made available, but that administrators are overworked: having to do too many manual tasks, when then could be doing work on more strategic activities. Consider the client administration tools in RHN – the dependency model, the ability to clone, the provisioning for desktop environments – all of these are really compelling features that can reduce the manpower required to support the environment, and it's important to do that from a managed service.

LXP: That sounds like quite a similar vision to what we have heard of late from Sun Microsystems, where the Networked Computer idea is touted.

MS: I think the idea of a networked computer is an old idea. Ken Olson, in the Digital Equipment days, also had some of the same vision in the late 1970s and early 1980s. What I think is really interesting is that the complexity of networked devices continues to grow exponentially, as you add things like Blackberry devices and Palms; and now there's an increasing amount of content, whether that be images, or sound, video, and voice. So, I think what we're witnessing is a move back to central administration. I think compute power, failover is getting better – having a second failover is becoming a reality.

I think the big issue between Sun, Novell, and all the rest of them is that they are proprietary software companies. At the end of the day, when you spread everything apart, you have one proprietary implementation, whether that's from Sun, Novell, Microsoft, or whoever; and one is Open Source. The customer will have to choose which paradigm they want to buy into: do they want to buy into lock-in, the extortion of the Software Assurance program, the whole issue about the Java ONE client, and all the relationships you have to buy into to become a part of that infrastructure? Or, would you rather be like the EU now, and not require a passport to go from country to country, be able to use a common currency, and have your information in a neutral format? My view is that, based on the demand that I can see from our customers, that they are increasingly moving towards an Open Source vendor.

It's quite a change – I'd be quite surprised to see a customer go from Microsoft to Sun or Microsoft to Novell, because that's just going from one proprietary tie-in to another.

***LXP:* Do you think smaller businesses and startups are now generally aware enough to be sold on the ideology of Open Source in addition to the TCO?**

MS: It would be my hope that they wouldn't buy into the ideology straight away, because the rule is that these fledglings die young and often, sadly. If you're starting a new business, you are probably going to outsource some of the things that are not your competencies – as much as you might love technology, you have choices to make. If you're trying to build a sales force, you can get your servers through the likes of SalesForce.com for X dollars per month, and never have to install software, and Yahoo! can provide all the functionality of email services that you want. These are choices that are practical, versus having to rebuild the network, hire a systems administrator, having to build all your email clients, deal with all the issues of security – many people are just going to outsource things that aren't their immediate priorities until their business is at a more sustainable level.

PERFECT PARTNERS

How Red Hat drives deployment through its partners

ALTHOUGH RED HAT IS A BIG BRAND, IT'S actually quite a small company. So, to help Red Hat reach the largest range of customers, it has a wide selection of partners that provide certification and also channel distribution. Beyond that, there are also distribution partners and value-added resellers that ship out systems based on Red Hat's range, and Red Hat is currently in the process of introducing several more of these.

The premier hardware partners – such as IBM, HP, Dell, and Fujitsu Siemens – preload and OEM Red Hat's software; and usually also provide support for the products direct to customers, so that they only have one number to call. Each of these partners also has service contracts direct with Red Hat, so that they can collaborate on any difficult support issues. Furthermore, Red Hat can take part in its partners' marketing strategies, which helps get its message across without breaking the bank.

Software partners – such as Oracle, Veritas, BEA, and SAP – also work with Red Hat to certify that their software runs on Red Hat systems. Again, these partners can – and do – also provide technical support direct to their customers as part of their value-add. By having such a large variety of hardware and software vendors – all of which receive early releases of Enterprise Linux so they can provide feedback and certify their products – Red Hat has managed to produce a strong ecosystem for customers of all varieties without having to compromise its all-important vendor-neutral stance.

SUPPORT AND PEACE OF MIND FOR THE MASSES

Red Hat Network is so much more than just patches

INCLUDED WITH EACH PURCHASE OF Red Hat software is a one-year subscription to the Red Hat Network, which in turn gives you technical support. Each product comes in three flavours: Basic, Standard, and Premium. While the products are the same, it's the level of support that changes.

The Basic edition is just that: people who don't really want technical support for one reason or another, and so it's the cheapest option. Unsurprisingly, though, the vast majority of customers do opt to purchase either the Standard or Premium options, both of which come with much better support. Someone who has purchased RHEL 3 AS Premium, for example, gets a full year of 24/7 Web support, 24/7 telephone support on severity 1, and guaranteed one-hour turnaround for telephone support issues, which is pretty incredible for just £1750.

What's more – unlike some other support contracts – the range of what's supported is huge: for that money, a customer gets unlimited support for installation and configuration, OS debugging, kernel optimisation and configuration, *Bash* scripting, backup, security, various servers (web, FTP, mail, *Samba etc*), directory services and lots more for the whole year. It also includes full support for Red Hat-certified third-party applications as well as desktop assistance.

Although some smaller businesses might balk at the initial purchase cost, clearly it's worth it as purchasing a five-incident 'support pack' from Microsoft is £675, and that's only available 8am-6pm, Monday to Friday.

Linux Pro tried out Red Hat's support anonymously – the phone was picked up within two rings, and was answered by an engineer fluent in several languages. When your IT infrastructure hits a problem and your business is at risk, no one wants to wait until next morning for help. In this situation – or even just because the connection to the new networked printer is slow – it's good to know you can have someone on the line in just a matter of minutes. Red Hat provides technical support in nine languages from three primary support centers (UK, USA and Australia). All Red Hat support engineers are RHCE qualified, and 70 per cent of calls placed to Red Hat are resolved on the spot.

« I think it's going to take a while, but a lot of small business is starting to buy into the Open Source ethos once they are more established. To start with, they don't have any computers on their premises except the terminals they are using to access email, but Open Source will become more and more widely used as a direct result of the advanced capability of the technology and the price it has.

***LXP:* At the Red Hat Desktop launch, VMware was there talking about how it plans to support it. But VMware isn't Open Source, and neither is Java – how do you reconcile these two against the fact that Red Hat is an entirely GPLed distro? And why use *VMware* when CodeWeavers' *CrossOver Office* is available?**

MS: The issue about CodeWeavers is, *"How do we keep the code moving forward?"* That's the problem. Our whole development model is based on speed, and being able to service the customer. So, if Red Hat started adding the CodeWeavers' implementation of *WINE*, my great fear – and I think I speak for all our engineers on this – is that you end up making a couple of hundred thousand dollars, and then you've got about 25 customers and something happens to CodeWeavers that makes the code go in the opposite direction. Red Hat then has to service 25 customers who have given us money for technology that's not even being kept up. We don't like that relationship with a customer – we just don't want that to happen.

Every day, there's some new piece of technology that someone wants to include in their distro, but our big issue is, *"How do we continue to service the customer over the long-term?"* The 2.1 RHEL distro has to be maintained for five to seven years – once you start to think about the commitment we're making to our customers and you start to add any crazy technology in there, we've got to maintain that for five to seven years – that's a long time. I think a lot of customers don't get that, and the tech media tends to play that up a bit – *"Why don't you do this?"* Or *"Why don't you ship and install this because Company A or Company B does?"* After two years, we'll see how happy those companies are.

With regard to Java, we've been very involved in the Open Source Java initiative for some time, and we're continuing to work really hard to see if there's an opportunity to create an Open Source Java. That's our end goal. We're shipping BEA's *JRockit*, we're shipping an IBM *Java Virtual Machine*, but it's on a separate CD and not part of the core Linux distribution.

We've approached Scott McNealy about this, and we've approached Jonathan Schwartz as well, both over a year ago; and we worked hard with the whole Sun organisation on this topic. It wasn't so much that we thought it would benefit Red Hat, it was that we thought it would create exponentially better applications for customers. Obviously they didn't see it that way...

***LXP:* What are you thoughts on Mono?**

RH: I think Miguel di Icaza is an incredibly creative guy, and what he's done is a great testimony to his ability to gather support around a pretty neat idea. But I think that if he were here, the broad term of Mono doesn't speak to the real challenge of some of the more specifics, such as issues of class structures, how to deal with the CLI. I think it remains to be seen how far Microsoft will let that go to become truly compliant and the Microsoft .NET framework.

Our preference would be to see an Open Source Java implementation that was royalty-free, that would be put into the public domain, and that could be used as the basis for some pretty basic technology without having to worry about the patents and royalty issues associated with Mono.

***LXP:* How do you see the competition between GNOME and KDE playing out?**

RH: We went through this before at Red Hat. It was a cultural shift in the company, because it didn't really matter what I thought. In fact, some of the engineers were trying to make the issue religious, and I had spent enough time in front of customers and ISVs to realise that my opinion didn't really matter – it was their opinion. I think we got behind GNOME when the interest in KDE and the Open Source community was very high, and I can remember a lot of the engineers wouldn't talk to me for a month or so after the decision – I was the biggest jerk in the building. Bigger than I am now!

As a result, the decisions we make are driven less by religion and are more about what customers want. It's certainly going to be a very hard problem to solve, because there's an ISV community that wants consistency and a common metaphor. Although we have the option to switch between GNOME and KDE in RHEL 3, all of the security, all of the infrastructure support is around GNOME – being driven by customers.

***LXP:* Now that Novell has purchased Ximian, would you say that Novell has the inside track on development of *Evolution* and the *Exchange Connector*?**

RH: We've thought through that too. We have a couple of guys who are pretty confident they could do the same thing from an engineering perspective, but it would be proprietary. If we wanted to get onto that proprietary track, we'd need to have four or five dedicated engineers to move the technology forward; without leveraging the community model, you'd need to service the customer consistently, and there's the issue of potential patent infringements – those are just rat holes that we've chosen, as a company, never to go down.

If a customer wants that kind of capability, there are products like *Scalix*, produced by a pretty neat young company. That's something we sell, and if customers want it we're happy to co-promote it. But the proprietary trap is just not something we find consistent within our model.

***LXP:* With its *OpenExchange Server* product, SUSE has a full alternative to *MS Exchange* that can provide calendaring, email, and other groupware. Is this not an area that interests Red Hat?**

MS: Once again, I think SUSE did this a couple of years ago with Lotus – the German company got itself in a very large development overhead project there. It takes a lot of money and a very large amount of resources to support that. Then SUSE developed its own implementation to create a revenue stream. So now all of a sudden you've got this very divergent product-line – the Lotus product-line, the internally developed groupware system.

How do you build consistency into the user experience? How do you have consistency in your development? And, most importantly, how are you consistent in your service model?

> **"RHEL 3 IS THE MANIFESTATION OF A LOT OF BIG IDEAS. WHAT'S BEHIND IT IS A MUCH BROADER VIEW OF WHAT THE OPEN SOURCE ARCHITECTURE IS."**
>
> **PAUL SALAZAR, MARKETING DIRECTOR FOR RED HAT EMEA**

TRAINING AND CERTIFICATION

What makes Red Hat Certified Engineers so valuable?

THERE ARE NOW OVER 10,000 RED HAT Certified Engineers (RHCEs) worldwide, with a further 2,500 qualifying each year. Although the largest single contingent is in the USA, EMEA is a close second, and growing fast. It's no surprise: RHCEs earn up to 40 per cent more than non-RHCE staff, and in 2002 the qualification came first in an independent survey of IT certification quality.

Perhaps the key to RHCE's success is that – unlike many other certifications – the testing is entirely practical: there are no multiple-choice questions, and no extraneous questions that push a specific agenda. Instead, the qualification tests only how well an individual can administer and maintain a set of machines running Red Hat Linux.

As the test doesn't bias towards any particular application running on Linux, it's popular in a wide variety of sectors – from large finance and telco corporations through to SMB organisations that require their technical staff to have a proven Linux competency. The qualifications also make up part of Red Hat's larger Enterprise Linux strategy – each qualification is directly attached to the release of the product commercially available at the time the certification was earned, and remains valid for that product as well as the next major release. For example, certificates earned on Red Hat Enterprise Linux 3 will be current until the release of Red Hat Enterprise Linux 5. Even when RHEL 5 is released, the qualification never expires – it just doesn't apply to that release.

Thanks to this popularity, Red Hat's training division – Global Learning Services – now makes up 20 per cent of Red Hat's overall revenue. Many of the classes are run directly by one of Red Hat's staff instructors in about 100 cities worldwide. Elsewhere, members of the Red Hat Certified Partner Programme run courses of equal quality.

In the future, the Red Hat training system can only expand. Originally it was just the RHCE qualification, but in January 2003 that was expanded to include the Red Hat Certified Technician exam, which is a slightly lower-level certification that covers a large chunk of the more comprehensive RHCE exam. Also, Red Hat has also now launched a new certification – the Red Hat Certified Architect – pitched even higher than RHCE, focusing primarily on skills surrounding systems deployment and management, performance tuning, storage management and other enterprise-level skills.

Note: all prices quoted here are including UK VAT

RHCE track (for someone with no Unix/Linux background):

Red Hat Linux Essentials – 4 days £1295
Red Hat system Administration with RHCT – 4.5 days £1450
Red Hat Networking and Security – 4 days £1295
RHCE Certification Exam – 1 day £485

Rapid Track to RHCE (for those with excellent Unix system administration skills):

Rapid Track to RHCE – 5 days including RHCE exam – £1599

Red Hat Certified Architect (for advanced administrators working in the enterprise):

Red Hat Enterprise Deployment and Systems Management – £1860
Red Hat Enterprise Storage Management – £2220
Red Hat Enterprise System Monitoring and Performance tuning – £1860
Red Hat Enterprise Directory Services and Authentication – £1750

Local contact information – Red Hat Europe

Tel +44 (0)1483 734 909
email **training-eu@redhat.com**
web **www.europe.redhat.com/training**

I think it's interesting when you look at the legacies of these two companies, because they both started out at almost at the same time, and they both have made very different choices along the way. But I think the single characteristic that defines Red Hat has been its unfailing commitment to its collaborative, Open Source, GPL-based model. When you stay committed that way – as painful as it has been sometimes, admittedly – you avoid falling into those short-term traps of *"How do I make money?"* And then afterwards, *"How the heck do we support this customer base?"*

"WE'VE GOT A LOT OF YOUNG AND ENTHUSIASTIC DEVELOPERS WHO WANT TO USE FEDORA AND DEVELOP FEDORA, AND WE'RE VERY HAPPY FOR THEM TO DO THAT."

The RHEL 3 product that we released in October 2003 has seven architectures off of one code base. We don't worry about any of the rhetoric coming from SUSE that you might have seen in the press or its PR announcements. Why? The customers know – the sophisticated customers that we sell to – that *has* to be more efficient and cheaper for you to service, because it makes sense. And I think as a result, the ISVs appreciate that because we can build them a multi-route technical roadmap. I think that's the way great companies are going – not for the short-term of making a new product and making someone happy for 15 minutes.

***LXP:* Though you can go to redhat.com and download RHEL 3 for free as long as you don't mind missing the support, not many people realise that you offer this. How do you go about combating that belief?**

MS: It's kind of ironic, because I visit our customers and I see the complex environments they're running in right now, and RHEL is a small part of what they're buying right now. You're at Amazon.com, and you're running a HPC cluster that does financial models with Hyperion software running on RHEL 3, and at peak holiday season there's a problem and they think it's a kernel-locking problem. How many people in the world can solve that and get it turned around in six hours for you? The price of the OS is small money – it's nothing compared to the brand promise, the responsiveness, the quality of the personnel; all of the things that aren't that sexy to talk about in print, but the reality is that's what our customers are really paying for.

We have had 87,000 new subscribers in the last 90 days from 5,000 new customers, many of which are highly sophisticated companies. We think that's what they're paying for. So, yeah, anyone can download the bits for free and they can knock themselves out with it and have a great time, but I think if you're going to run it in a professional environment, what we offer is relatively small money.

***LXP:* Is that quite evenly spread, or was it someone like IBM buying 80,000 by themselves?**

MS: No, no. Surprisingly there were a couple of large hosting companies, but beyond that it was pretty evenly spread.

***LXP:* Now that official support for Red Hat Linux 9 has ended, do you still hear much from users about it and older products?**

MS: Actually, it amazes me. I was at a conference in Toronto, Canada, and I had people come up to me who were running Red Hat Linux 5.2 or 6.0, who were very happy. They'd come up to me and say, *"I'm never going to pay you any money at all, because this is a great piece of software."* And I thought that was great! They're using Open Source software, they're not using the proprietary alternative, they're getting great value out of it, and I think they're very happy. That's the whole point of Open Source software, isn't it? It's not to continue to extort money out of them because each release needs a hardware upgrade.

***LXP:* Did you get many people who used Red Hat 7.x, with the infamous GCC 2.96, coming up to thank you?**

MS: I remember that very clearly, but, you know, that was technically the right decision. The community didn't like it, but technically it was the right decision, and the evidence of that bore out – same as with the Fedora decision. Young people in the company made the Fedora decision, that wasn't something that came from the 'suits'. It came from the engineers, the people working on it; and a result we took a lot of abuse about cancelling the Red Hat Linux product and replacing it with Fedora. But now I'm amazed at the support Fedora is getting.

So, it was our engineers who just said that there was a better way to solve this problem. We cannibalised nine million dollars worth of revenue, because to do that – to create Fedora – we *had* to take the retail product out of circulation. That was a big gamble – how many publicly trading companies will take out nine million dollars of revenue without knowing how to replace it? To say, *"We're going to put it all back into the Open Source community with Fedora"* was a big gamble.

***LXP:* There's still some discussion about whether Fedora is really a community product, owing to the fact that many of the developers work for Red Hat. Also SELinux was in Fedora Core 2 tests 1 and 2, but not in test 3 because most consumers wouldn't need it – some say this implies Red Hat is using Fedora users as guinea pigs.**

MS: The secret story to that misconception is just simply a lack of infrastructure – we've got a lot of young and enthusiastic developers who want to use Fedora and want to develop Fedora, and we're very happy for them to do that.

MAKING LINUX SECURE

Open Source is much more secure than proprietary software, because there's so many more people working to protect it!

With a five-year support life on each member of the Red Hat Enterprise Linux family, no choices about security are left to chance. As the Red Hat Network is the core of Red Hat's security notification and distribution, encouraging users to keep their systems up-to-date is a constant task for a large team of people dedicated to patching holes, fixing buffer overflows, and stopping malicious crackers before they get to you.

Linux Pro spoke to Mark Cox, the leader of Red Hat's security response team, about how security decisions are made at Red Hat and the importance of end-user education...

***LINUX PRO:* What kind of trade-off is there between releasing new software that has the features end-users want, and releasing old software that's known to be more mature and stable?**

MARK COX: We've been Apache Software Foundation (ASF) members since early 1995, and we spent a lot of time thinking, *"Should we upgrade people from the1.3 release, which is stable, secure, and just works, to 2.0, which doesn't have any real new features that people need?"* It works maybe a little bit faster, but not a huge amount – maybe 10 per cent, depending on the system. For a 10 per cent improvement, you can just throw another machine in the mix.

Apache 2.0 also had problems with things like PHP, which doesn't support threading, and some of the more popular modules hadn't been ported yet, so we weren't sure whether we should stick with 1.3 or move to 2.0. Obviously, we had to make that decision at some point, because sooner or later the ASF was going to stop supporting 1.3. There are still going to be security issues about, and we need to fix them, and we have many *Apache* folks in-house who did that upgrading work – we actually made it stable for Red Hat Linux 8, which switched completely to *Apache 2*, dropping 1.3.

Again, we wanted to get people to use *Apache 2* so that we could make it more stable, because Netcraft was showing really tiny *Apache 2* numbers compared to 1.3, because there really was no business benefit to people upgrading. More people using it meant more testing, and we could give our code fixes back to the community. People knew that new features would only be available in *Apache 2*, and we wanted to give them that before security updates ended for 1.3.

PARTNERS

Some Red Hat partners such as Oracle handle technical support for versions of Red Hat they provide to their customers. Does that make your job harder?

MC: THE FIXES HAVE TO come out in the right way – people are expecting to get fixes via the RHN. How the fix actually gets into the RHN – whether that's from an Oracle engineer or if someone at SUSE shares it with us via the vendor partnership we have, doesn't really matter – the fix is going to be deployed via RHN if it's a Red Hat product, so we audit it, test it, and then we sign it.

***LXP:* How does your support for *Apache 1.3* tie in with your five-year lifecycle plan?**

MC: Well, actually it's *at least* five years!

***LXP:* So even if the ASF decided to stop producing fixes for *Apache 1.3* in six months, you'll carry on supporting it until the end of the RHEL 2.1 support lifecycle?**

MC: We will continue to provide support and security fixes.

***LXP:* That sounds very expensive for Red Hat...**

MC: Well, it is and it isn't. There are other vendors in the same position as us, and when it comes to security updates, we share information and we share security backports from *Apache 2* on a daily basis. SUSE, Mandrake, Debian, some of the BSDs, and Red Hat all co-operate with security issues – perhaps one guy in one of the companies will do the actual patch, but we'll all help peer review it to make sure the quality is high. No one wants to remake patches over and over again, so we co-operate really closely with all these guys, and a lot of them are still using *Apache1.3*.

***LXP:* As patches came out for RHEL 2.1, the number of security-related bugs declined. Do you see that spiking again now that RHEL3 adoption is picking up?**

MC: Yeah, we expect to see it spike a little, but only as a result of more people looking at and using the new code.

LXP: With RHEL 3, *Apache 2* is the only option – 1.3 isn't included on the CDs. Wouldn't it have been better to give people the choice?

MC: We believe that *Apache 2* is stable enough that we can support our users to do everything they could do with 1.3.

***LXP:* As the products in RHEL 2.1 were generally older and more mature, would you say you've seen more vulnerabilities in RHEL 3?**

"ONLY RECENTLY ONE VENDOR RELEASED A PATCH FOR A VULNERABILITY THAT WAS FIXED IN *APACHE* OVER A YEAR BEFORE."

MARK COX, RED HAT SECURITY

MC: Actually no, I've seen less. Within the entire lifecycle of RHEL 2.1 to date, there have been 21 critical security issues. With RHEL 3, since it came out, there has been just one issue, and this year there has been zero. From that alone, it's clear that RHEL 3 is a more secure base.

***LXP:* How do you see your security response panning out for Enterprise Linux 4?**

MC: One of the things we've been doing is working really closely with NISCC (the National Infrastructure Security Co-ordination Centre), who are the guys in the UK government who are worried about the key critical infrastructure.

"IF YOU HAVE A FLAW IN YOUR KERNEL, BOTH SELINUX AND EXECSHIELD AREN'T GOING TO HELP YOU."

They've been looking at protocols, and working with us and other vendors to do tests on protocols such as SSL. The aim of this relationship is to help define what the threats are, particularly on Linux, and we're developing this to make sure that ourselves and other vendors have a place to go to work together on these and other issues.

***LXP:* How do you combat the tide of belief about Linux being immune to everything?**

MC: We've been trying to improve user education in a number of ways. First, one of the problems with Open Source software is that so many vendors ship patches – if there's a vulnerability found in *Apache*, you'll see 20 or 30 vendor announcements spread out. In fact, only recently one vendor released a patch for a vulnerability that was fixed in *Apache* over a year before! As a result, it can be hard for an end-user who's looking at *BugTraq* or the press to know what the issues are, whether it affects them, whether their distribution has fixed it, and for someone to work through all that, download the patch, and apply it... It's really hard.

So what we want to do is explain to people, if you're using a Red Hat distribution, come to us, and look at what we say about the security issues. We try to make our advisories clear so that people understand what the issues are, whether we've fixed them, as well as backporting information. What we really try to do these days is backport security fixes, but again that causes problems when people see that they're not running the latest version of a particular release.

For example, the ASF might say *"you need1.3.29 to be protected from this particular vulnerability"*, and people come to us and say, *"You're only on1.3.23!"* Some tools such as *Nessus* don't even look for the vulnerability, they just check the server header for a version number and go by that, which can result in many false positives. We need to get that education across too – that's why we got involved with CVE (Common Vulnerabilities and Exposures), as it makes sure we all use common names for a given issue. This also lets us more easily assign severities to issues – for example, if you're running a Red Hat system, the severity of an *Apache* bug is likely to be different than if you're running a Debian system because we package things differently.

PATCHES

Are the patches that are available on RHN available to non-subscribers?

MC: WE ALREADY MAKE ALL our source RPMs available for free on our website, whether you subscribe to RHN or not. So if we do a fix for *Apache*, we'll put those source RPMs on our website.

***LXP:* At the same time as they become available to subscribers?**

MC: Oh yeah, at exactly the same time they become available to subscribers. Not so much for *Apache*, but for other products that are GPLed – it's essential for us to do. We always share our fixes with the other relevant vendors anyway, so most vendors will tend to have their patches out at about the same time.

***LXP:* Juergen Geck of SUSE highlighted the backports issue recently, and it definitely does make life harder when version numbers can't be used to assess vulnerability. How are you tackling this?**

MC: One interesting project we're working on is to have a local security analysis tool that scans your system and automatically reports which patches you're missing. Behind the scenes, it knows about that system, it knows about *RPM*, it has information from us about which versions fix which vulnerabilities, and from all that data it can help you find and patch your system. Ideally we want to get that working over a network so that you can check and patch all your systems across a network from just one computer.

We'd rather people ran a tool like that than a tool like Nessus, which doesn't know how to check for individual vulnerabilities. The thing that got me was that the first time I ran *Nessus* it said, *"You're running an old version of* Apache*"*, and it also said, *"Your server is returning a version header, which can give the bad guys an idea of what vulnerabilities you have on your system – turn it off"*. So I turned it off, and then *Nessus* didn't work because it was looking for the version number to work out what vulnerabilities affected me!

So, user education is partly about getting people to patch regularly, but it's also about helping people understand what patches they need. Red Hat Network (RHN) does this partially already because it looks at RPM version numbers and such, but it doesn't break that down into individual vulnerabilities.

***LXP:* To what extent do RH and other vendors work together when writing vulnerability announcements?**

MC: Well, we do need to work closer with them. For example, there's a vulnerability in the Ext3 filesystem that came out last week when some of the vendors disclosed it. It's a vulnerability that when it creates Ext3 superblocks, there's a way that some uninitialised kernel memory might appear in these blocks. And when you actually look at how you'd exploit it, you'd have to be root – because you'd have to have access to the raw device. All you'd find is a few bytes of uninitialised kernel memory, so it could come from anywhere. So what we're saying is: root can access some bits of kernel memory – not a huge issue.

However, someone thought that this could be an issue *if* you had cryptographic keys in memory and they weren't cleared up by the program, so it wasn't a very good program because it wasn't clearing its memory, and you don't have any swapping, because if they got swapped to disk then you'd also be able to read them. And then that got written up as the advisory: *"Flaw in the Ext3 filesystem could allow compromise of cryptographic keys"*.

***LXP:* SUSE got EAL 2 (Evaluation Assurance Level 2 of the Common Criteria from the US National Institute for Standards and Technology – NIST) before you and already has EAL 3. What do you make of that?**

MC: EAL isn't designed to be a competitive advantage for anybody; it's designed to open up markets – EAL 3 opens up certain markets, EAL 4 opens up certain markets as well. It was just SUSE's choice of certification: it went with IBM through a German test, and we went with Oracle through a UK test.

RED HAT ENTERPRISE LINUX 3 – UNLEASH THE POWER OF LINUX KERNEL 2.6

New features and capabilities

Feature	In Linux 2.6 kernel	In Red Hat Enterprise Linux 3	Provides:
Native Posix Thread Library (NPTL)	Yes	Yes	High performance POSIX compliant multi-threading
Kernel IPSec	Yes	Yes	*IPSec* layer available for use by kernel modules
Asynchronous I/O (AIO)	Yes	Yes	Improved application performance
O(1) Scheduler	Yes	Yes	Highly scalable SMP scheduler
OProfile	Yes	Yes	CPU-hardware-based performance monitoring
kksymoops	Yes	Yes	Improved kernel bug reporting
Reverse Map Virtual Memory (rmap VM)	Yes	Yes	Performance improvement in memory constrained systems
HugeTLBFS	Yes	Yes	Performance improvement for large virtual memory applications (*eg* Databases)
Remap_file_pages	Yes	Yes	Kernel memory optimisation for shared memory applications
2.6 Network stack features (IGMPv3, Ipv6, etc.)	Yes	Yes	Improved network performance and messaging
IPvs	Yes	Yes	Network load balancing
Access Control Lists (ACLs)	Yes	Yes	Improved file system security management
4GB-4GB memory split	No	Yes	Greatly increased x86 physical memory support and larger application address space
Scheduler support for hyperthreaded CPUs	No	Yes	Improved hyperthreaded CPU performance. (2.6 implementation not yet comparable)
Block I/O (BIO) block layer	Yes	No	Major rewrite of the I/O subsystem (stabilisation and driver support in progress)
Support for > 2TB file system	Yes	No	Support for very large volumes. Red Hat Enterprise Linux 3 supports up to 1TB
New I/O elevators	Yes	No	Fine tuning for I/O subsystem performance (stabilisation in progress)
Interactive scheduler response tuning	Yes	No	Scheduler improvements for interactive tasks (stabilisation in progress)

The whole point of EAL isn't that it's more secure, it just says that you meet a certain target that was set down. Microsoft has EAL 4, for example, so it would be a useless certification if it was saying that Microsoft products were more secure in totality than Red Hat or SUSE Linux! In EAL 3, for example, NIST looks at your development processes and some of your security response processes, so it's a useful certification to have. But it doesn't mean that SUSE is more secure because it had EAL 3 before us – you don't change the product in order to get EAL certification, except to add auditing.

***LXP:* Would you say there's a trade-off between making software easy enough so that people can use it and actually giving it a proper security model?**

MC: This was the reason we created ExecShield. At the time there we lots of non-executable stack patches available for Linux at the time, some commercial and some free, but we wanted to make sure that our solution wasn't invasive to the user – that it wouldn't break anything. Or, that if it absolutely had to break something, that we knew how it was going to break and we could pre-empt it. We didn't want people to have to recompile their applications or things like that. One of engineers wrote ExecShield based on these criteria.

Now, it's not going to catch *every* stack overflow but it does a good enough job that it's raising the bar. If you can raise the bar without having any negative effects – and this had none, and it's been in the Fedora Core for quite a while now – then it's an improvement. ExecShield stopped several vulnerabilities that were posted on full disclosure lists, without affecting people.

So, yes, there is a compromise. With Fedora Core 2, we shipped SELinux, and we're still working on what SELinux policy we ship with RHEL 4. In this situation we can't ship with the most secure policies because things just won't work for people.

VULNERABILITIES

What would you say are actually the most vulnerable parts of a standard Linux distro?

MC: THAT DEPENDS ON what you consider to be vulnerable. If you're running a system as a web server, then you care about all your web applications, and if you're running a mail server you care about *Sendmail*. With regards to what's likely to be most vulnerable, it's probably the kernel. And that's despite our work on SELinux and ExecShield, because if you have a flaw in your kernel both SELinux and ExecShield aren't going to help you.

***LXP:* To what extent is the new code that is being added to RHEL 3 backported from development on what will eventually become RHEL 4?**

MC: We employ lots and lots of folks who work on various versions of *Apache* and the kernel, and lots of the stuff we backport is stuff that we wrote – things that we wrote and we put into our kernel early. For example, PIE (Position-Independent Executables) is the idea that when something loads into memory, all the bits that load load at slightly different locations each time. It adds a little bit of overhead, of course, but no more than 10 per cent.

The idea is that if you have a vulnerability that has a buffer overflow offset built into it, anyone posting to a full disclosure list will include a table saying, *"Red Hat Linux 8, with X version of Apache, here's the offset"*. Some of these things are one-shot events – if you don't get the offset right the first time, the system dies and that's your chance gone. Things that like *Apache* are probably not the best example, because when an *Apache* child process dies, it gets respawned. But with PIE, it gets respawned at slightly different locations, so every time you try exploiting things they re-appear at different locations. It's not going to solve it, but it's going to make it a bit harder for some exploits to work – a lot harder for the script kiddies.

***LXP:* Can PIE be disabled?**

MC: No. This is because it's compiled in to each of the programs. The speed overhead is really minimal – again, no more than 10 per cent.