# Leveraging Linux and Managed Services

## To Lock Out Cyber Criminals and Keep Your Systems Humming

By CJ Fearnley, LinuxForce, Inc.

## The Challenge of Computer Security

To quote and expand upon a popular commercial, rust never sleeps and neither do cyber-miscreants. Beyond death and taxes, you can count on continued attempts to compromise your IT systems for reasons ranging from mischief to internal employee discord to corporate sabotage or the now rampant threat of theft and fraud. According to the most recent CSI/FBI Computer Crime and Security Survey,[1] "the percentage of organizations reporting computer intrusions to law enforcement has reversed its multi-year decline, standing at 25 percent as compared with 20 percent in the previous two years." This might not seem terribly alarming but for the fact that many more organizations never report intrusions to avoid negative publicity and other undesirable business impacts. In fact, participants in the study report that over the past year they have experienced myriad attacks on their systems ranging from virus attacks (65 percent) to Web site defacement (59 percent), system penetration (15 percent), denial of service attacks (25 percent) and more. More recently, organizational apprehensions have been elevated by the increasing spate of zero-day attacks (attacks which target unknown or undisclosed software vulnerabilities and for which no fix is immediately available).

In our practice at LinuxForce, we are frequently contacted by organizations whose Web servers have been commandeered and employed to promote products and services other than those offered by their own businesses, or whose e-mail servers are suddenly running very sluggishly because, as it turns out, someone has taken control of the servers to send out a profusion of spam messages, thus seriously delaying the delivery of the organization's own e-mail.

So what are you to do in the face of this unrelenting onslaught in order to stave off malicious attacks and the damage they can do to your organization's bottom line, reputation, customer relationships, and to the threat they pose to your survival?

## All Enterprises Are Vulnerable

Spammers, saboteurs, identity thiefs, and other cyber-villains are nothing if not clever, resourceful and persistent. As a result, all enterprises are vulnerable to their exploits. While it's true that organizations are increasingly devoting more time and resources to security, it's rarely enough to stay ahead of the attackers.

In fairness, most small and medium-sized organizations simply don't have the staff or budget resources to address security on a full-time basis. Even large enterprises are often hard pressed to do this.

To ensure maximum uptime, you have to proactively inspect your systems around the clock to detect anomalies that could indicate an imminent problem. You have to perform timely upgrades, anticipate potential failures, carry out a variety of proactive and reactive maintenance duties, and audit your IT environment 24/7 to ensure policy and best practices are continually followed. Particularly in the case of security, fending off or limiting the impact of threats requires constant vigilance and an ongoing improvement and layering of security technology and policies.

Simply deploying firewalls and virus protection and applying periodic upgrades will not keep the cyber-hoodlums at bay.

And then, of course, there is the issue of the operating system you're running. Some operating systems — Linux, in particular — are less vulnerable than others, such as Windows.

[1] CSI/FBI Computer Crime and Security Survey; `http://www.GoCSI.com`

## Starting With a Linux Foundation

It is no secret that the Windows operating system is quite porous and open to a variety of cyber-attacks. Nor is it a mystery why vendors running the gamut from IBM to HP to Oracle and others have embraced Linux in recent years. Our own experience with Linux has clearly validated our dedication to delivering and maintaining reliable, robust, scalable and affordable Linux systems. Systems we've developed and maintain provide unrivaled dependability, flexibility and security, and clients with previous experience running other operating systems can see a dramatic difference.

That said, we also know it is not enough — even with a Linux-based system — to merely install it with other open source software and let it run, while only performing periodic upgrades. The key to realizing increased productivity, savings[2], security and positive business results is continuous systems monitoring and continuous systems and software improvement.

## Managed Services vs. DIY

Many organizations are reluctant to outsource any IT work having to do with security despite the fact that they have insufficient IT staff or whose staff lack the necessary skills to do the job right. Many organizations are reluctant to outsource any IT work having to do with security. While at first this may seem to make sense, closer consideration often leads to a reappraisal. If your organization's IT staff is lean, as is so often the case these days, particularly in small and midsize companies, you really can't afford to divert them from activities that will enhance your competitive advantage to deal with monitoring and managing utility services. Even large organizations often prefer to focus their IT professionals on activities that will advance the fortunes of the business instead of administering generic servers.

That realization is compounded when you examine the scope of the task. What you really need is a comprehensive, proactive systems administration infrastructure. That means scanning your systems around the clock, deploying and continuously adding multiple layers of protection to stymie would-be intruders. Not only will the multiple strata protect you even if one layer fails. But by complicating the lives of those who would do your business harm, you make it costly and risky for the cyber-criminals to persevere with attacking your systems. In addition, you need to comprehensively audit your services to identify potential avenues of attack and assess the best method of defense for each. You also need to continually improve your best practices to stay ahead of the ever-evolving threat, since as Buckminster Fuller said "change is normal." Moreover, you have to track every aberration that your systems inspection software identifies to ensure that you are secure and functional. Finally, you have to constantly review and build-out your monitoring system to ensure that it detects more and more inadmissible behavior.

Can your organization adequately address all of the facets needed to prosecute the twin defenses of adding layer upon layer of safeguards and reviewing systems operations continuously and meticulously to ensure your business is protected? For most organizations it is simpler and less expensive to offload these challenges and complications to a dedicated, Linux-based managed services partner.

## Practical Solutions

Faced with the calls we so often receive regarding problems with mail and Web servers, we have developed two, innovative, open source-based products to protect our clients' IT systems and help ensure their optimal performance in the service of their business objectives. Each of these products embodies our central principles that systems must be monitored and audited constantly and deterrents to attacks must be layered and continuously improved.

[2] "The cost benefits of deploying on Linux are dramatic" from `http://www.cio.com/archive/071506/open_source.html`

### Remote Responder℠

To ensure maximum uptime, you have to proactively monitor your systems around the clock to detect signs of possible trouble. You have to do timely upgrades, anticipate potential failures, perform a multitude of proactive and reactive maintenance duties and audit your IT environment to ensure policy and best practices are continually employed.

Even the most perfectly architected, most robust system can fall victim to cyber-attacks, be they viruses, unauthorized intrusions or some other threat. LinuxForce developed Remote Responder℠ to ensure maximum uptime by monitoring your systems around the clock to detect anomalies that could indicate an impending problem.

This automated, comprehensive monitoring and systems administration service can save you money, increase your efficiency, and most important, keep your systems humming along. Among the remote systems monitoring and testing performed by Remote Responder℠ are: continuous service level monitoring, e-mail monitoring, network availability and performance testing, response time monitoring (especially for web sites), and services availability (WWW, SMTP, ssh, ftp, etc.). When an abnormality is detected, e-mail and/or pager alerts are sent.

The Remote Responder℠ service also includes routine maintenance, auditing and tweaking of your systems, application of required security-related upgrades and configurations as soon as vendors release tested and proven fixes, implementation and maintenance of an intrusion detection system, a host-based firewall, and ongoing security scans and audits.

Our service frees you to focus on your core business activities and allows your in-house IT staff to work on revenue-generating development projects. You may learn more about Remote Responder℠ at `http://www.LinuxForce.net/remoteresponder.html`.

### LinuxForceMail℠

Because so many of the attacks on your systems are perpetrated through e-mail, we have developed a solution to specifically identify and prevent them. LinuxForceMail℠ is a multi-tiered, anti-abuse service that blocks and removes as much as 99.4% of unwanted e-mail. It is delivered as Software as a Service (SaaS), with remotely provided systems administration via Remote Responder℠.

The LinuxForceMail℠ service includes: continual updating of comprehensive aggressive SMTP-time hygiene rules, continual updating of open-source ClamAV (anti-virus) and Spamassassin (content filtering) rules, security upgrades promptly as they become available, 24/7 service monitoring, proactive maintenance, and regular statistical reports.

Additionally, while LinuxForceMail℠ can sit in front of your Microsoft Exchange, Lotus Notes or other mail server to filter and protect your e-mail system around-the-clock, it can also function as your complete e-mail system. You may learn more about LinuxForceMail℠ at `http://www.LinuxForce.net/mail`.

## Act Now

There is no evidence and no reason to believe that cyber-attacks are going to do anything other than increase over time. And unless you're willing to risk your business on the belief that what has happened to the majority of businesses won't happen to yours, you must act now to secure your IT systems.

Our recommendation is to partner with a managed services company dedicated to continuously improve upon security best practices to simplify your IT operations and keep the miscreants at bay. And therein lies your edge.

*CJ Fearnley is President and CEO of LinuxForce, Inc., a leading technology services provider specializing in the development, implementation, management and support of Linux-based systems, with a particular expertise in Debian GNU/Linux. He may be reached at `cjf@LinuxForce.net`.*