Guardian Digital Presents EnGarde Linux

Mar 16th, 21:58 UTC

EnGarde is the next generation in Linux security by providing a complete suite of e-business services, intrusion alert capabilities, improved authentication and access control utilizing strong cryptography, and complete SSL secure Web-based administration capabilities.

EnGarde Secure Linux Website

Imagine a cohesive suite of Open Source applications converging to provide the level of security required for corporate environments as well as security-conscious Internet users.

Imagine the ability to manage and create secure Web sites, configure DNS, e-mail, SSL certificates, and other administrative tasks using a secure Web-based front-end.

Now visualize the ability to create complete e-business storefronts. This suite of applications would then provide all the components necessary for an organization to securely conduct business on the Web, perform the function of a network intrusion detection system, and securely host Web sites.

That is precisely what Guardian Digital has done with the creation of EnGarde, an easy-to-use, low maintenance, ultra high secure Linux server distribution. On March 30, 2001, at 00:01 EST, Guardian Digital, the Open Source security company, will unveil EnGarde Finestra, a stable and revolutionary release like none before it.

Robust and highly secure, EnGarde provides a comprehensive suite of tools designed to maintain data integrity and increase the level of assurance necessary to entrust to it your corporate assets.

EnGarde protects against many forms of attack, not just a particular form of vulnerability. It is also not just a repackaged version of another distribution that claims to be secure. EnGarde is a collection of best-of-breed applications from many sources tuned to provide exactly what is necessary to maintain a secure Internet presence.

Features:

- **Kernel and Host Security:**
  The security of the kernel and the host itself have been significantly improved. Advanced forms of data integrity management and assurance, provided by the Linux Intrusion Detection System and other means, offers the ability to control all access to system resources, even preventing a root compromise from subverting the security of the entire system. Protection from many forms of buffer overflows at the kernel level gives administrators a lead on any potential vulnerabilities that may occur.

- **Browser-based Administration:**
  Browser-based administration can be performed using the Guardian Digital WebTool. The GD WebTool provides security through a 1024-bit SSL connection and allows an administrator to perform 100% of the functions using a Web browser that could previously only be performed from the command line.

- **Built-in E-Commerce:**
  Secure E-Commerce sites can be painlessly created using the GD WebTool and integrated SSL support. Creation of SSL certificates and maintenance of them can be automatically managed through the GD WebTool.

- **Web Services:**
  All Web functions are controllable through through the GD WebTool. The creation of thousands of SSL and standard virtual Web sites can be easily managed and maintained. Access to CGI and Server-Side scripts can also be controlled.

- **Guardian Digital Secure Update:**
  Registered users can use the Guardian Digital Update Tool to automatically be alerted to new security updates and packages, and provide the user with the ability to proactively update the system from the Guardian Digital secure Web site.

- **Intrusion Detection and Prevention:**
  The intrusion detection features will detect and notify users of possible threats and security related events. Network intrusion detection using "snort" is pre-configured, easy-to-use and production-ready. Integrated and Web-managable Tripwire ensures the system is always being monitored and administrator notified upon the first indication of unauthorized activity.

- **Domain Name Services:**
  Guardian Digital's EnGarde Linux can manage DNS for thousands of domains for external users trying to access virtual Web sites, as well as DNS for internal users. This is all configurable using the GD WebTool.

- **Electronic Mail Server:**
  The included e-mail server has been engineered to provide security and stability and can control e-mail for hundreds of domains with the click of a mouse. Mail can then be retrieved in a secure format using conventional mail clients. The Web-based management enables administrators to create thousands of virtual e-mail domains on

the same host simply and effectively. Additional security improvements have been made including protection from common threats as well as restricting unsolicted e-mail.

- **Secured IMAP and POP3:**
  SSL Secure IMAP and POP3 are fully supported to help increase the security of personal e-mail. This also provides the ability to securely read e-mail from a remote location.

- **Secure Shell Accounts:**
  The Secure Shell provides a secure encrypted communications link with Guardian Digital's EnGarde Linux from a remote location, eliminating the risk previously found in other remote access methods such as telnet. Key management and access control can be performed using the GD WebTool.

- **Web Server Aliasing:**
  EnGarde includes the ability to create thousands of virtual Web sites from the same IP address. Creating and managing SSL Web sites is equally as effortless.

- **System Logging and Auditing:**
  Extensive logging is performed to ensure that the system has access to the latest system information. Daily summaries sent via e-mail to an administrator ensures the system is in correct working order.

For further information on EnGarde Linux, Guardian Digital, or the Guardian Digital Linux Lockbox e-business server appliance featuring EnGarde Linux, please visit us on the Web at http://www.GuardianDigital.com, e-mail us at info@guardiandigital.com or reach us by calling toll-free **1-866-GDLINUX**.

Guardian Digital, Inc. is the primary sponsor of LinuxSecurity.com.
