Guardian Digital

Pioneering. Open Source. Security.

www.GuardianDigital.com
1-866-GDLINUX

Guardian Digital EnGarde Secure Linux

The Design of the Secure Linux Platform

Users familiar with the history of Linux have become accustomed to its stability, versatility, and scalability. Now, with EnGarde Secure Linux, Guardian Digital has added unsurpassed security.

Engineered from the ground up with specific regard to security, EnGarde Secure Linux incorporates intrusion alert capabilities, a complete suite of eBusiness applications using AllCommerce, mail and DNS management for an entire organization, improved authentication and access control, strong cryptography, and complete SSL secure Web-based administration capabilities.

EnGarde Secure Linux is the perfect platform for developing an online presence that requires a high degree of security.

Using tools from the best open source security projects on the Internet, EnGarde forms a secure host platform for developing a firewall and proxy server, act as an intrusion detection device, and handle common Internet functions such as Web, DNS and electronic mail.

EnGarde Secure Linux was created by Guardian Digital, Inc., the first full-service open source security company. Guardian Digital is focused on the intelligent growth of secure open source security solutions for Linux, including the Guardian Digital Linux Lockbox, a secure turnkey eBusiness server appliance featuring specially optimized and configured EnGarde.

Security is pervasive. No longer is it the case that a company can purchase or contract an eBusiness solution without great concern for the assurance and integrity for the data and information contained within it. Guardian Digital solutions are engineered with security as a primary concern, providing that high degree of assurance required to conduct business on the Web today.

Security issues are a critical component of doing business on the Internet, especially among data-sensitive businesses. Guardian Digital fills the void for applications that are used in areas where security, reliability, and data integrity are of the utmost importance.

EnGarde provides a high level of defense against intruders gaining local access and engaging in destructive activities. Every component of EnGarde has been scrutinized to ensure it provides the most robust and secure candidate available for the task. It is not a repackaged version of another distribution, but rather a unique collection of the best open source tools available, coupled with the security and networking expertise of the Guardian Digital engineers.

Global electronic commerce and networking requires assurance that the integrity of your organization's data is maintained. EnGarde addresses these challenges by providing a comprehensive suite of tools to mitigate the risk of intrusion, as well as detecting an anomolous event should one occur.

No longer is it possible to conduct business communications on the Internet without specific regard to security. Organizations need a robust and easily managed security infrastructure that must satisfy a demanding set of user requirements, while ensuring performance and transaction security.

Feature Overview

EnGarde Secure Linux addresses the needs of small organizations wishing to develop a secure Internet presence, as well as large organizations wishing to conduct eBusiness on the Web.

Issues involving availability, performance, integrity, and privacy have been addressed with EnGarde. EnGarde improves the security of existing versions of Linux in several critical areas with:

- Advanced forms of data integrity management and assurance
- Intrusion alert and prevention capabilities
- Reduction of any threat should an administrative account be compromised
- Real-time and around-the-clock remote notification of immediate security threats via e-mail or pager
- Security control center that provides automatic notification of security and application updates
- Improved authentication and access control utilizing strong cryptography

Easy to use, robust, and highly secure, EnGarde is built on the latest stable technology and includes all the components necessary to manage all Internet functions.

Secure Web-based Management

The Guardian Digital WebTool provides basic system administrative functions via a secure web browser using HTTPS (HTTP over SSL). Designed to simplify complex network administration tasks, the GD WebTool provides the ability to create virtual Web sites, manage e-mail and DNS domains, create SSL certificates required for secure transactions, manage users and groups, monitor system information, and much more.

Virtual Web Site Hosting

The Virtual Host Management component of the GD WebTool allows you to perform all administrative functions necessary to set up and manage hundreds of standard Web sites or even an SSL-enabled Web sites.

Creating a virtual host has never been easier. Simply fill out five fields and click on “Create.” Additionally, you can generate SSL certificates necessary to perform secure transactions over the Web, and even generate a database specifically for that Web site.

The MySQL database, PHP, perl, and CGI capabilities are also integrated and available for rapid Web-site development.

Create secure corporate firewall and router gateway

A firewall is an essential part of any Internet presence. EnGarde Secure Linux provides administrators with a secure foundation on which to build a secure firewall and accompanying network intrusion detection device. Using the ipchains tool, experienced Linux administrators can build a packet filtering firewall required for network security.

Manage DNS and Electronic Mail

Management of thousands of electronic mail domains can be controlled using the GD WebTool Web interface, seamlessly integrating with DNS to make the process extremely easy.

EnGarde Secure Linux enables administrators that have no prior knowledge of Internet techniques and configuration files to have a domain set up and configured in minutes.

Even the process of receiving mail is done securely with EnGarde. EnGarde virtually eliminates the threat of eavesdropping through the use of the same technology that is used to provide transaction security to Web sites.

Using standard mail client programs such as Netscape, Outlook or Eudora, users can continue to receive mail as they normally do, but their passwords and the content of the mail itself is encrypted with the use of SSL.

Build secure eBusiness storefronts easily and securely

EnGarde Secure Linux provides the ability to get online securely, quickly and completely. EnGarde is truly “eBusiness ready”, and includes all the components necessary to create an online presence within minutes and start populating it with an organization’s products.

It includes the ability to automatically generate the necessary SSL server certificate to be sent to an authority such as Verisign or Thwate, then inserted into the Web configuration to provide secure transaction ability.

The AllCommerce suite of eBusiness applications is the industry’s only enterprise-level e-commerce solution that fully integrates front-end functionality with warehouse operations. Businesses of all types can effectively manage site content, orders, inventory and warehouse facilities all from a clean, intuitive user interface.

Robust Host Intrusion Detection solution

The Linux Intrusion Detection System (LIDS) implements an additional level of access control above and beyond what is normally included with the Linux kernel. This Mandatory Access Control mechanism prevents at a kernel level users (including root) from accessing resources they have not explicitly been given permission to access.

The host intrusion detection included with EnGarde is pre-configured for your system. Experienced Linux users can tweak the level of notification, control the level of access to system resources, as well as numerous other system parameters. It requires no additional configuration as a part of standard system operation.

Through the use of the Web-manageable Tripwire host integrity database, users can maintain data integrity and increase the level of assurance required to be on the Web today. Tripwire is software that monitors all file changes, verifies the integrity of data at rest on network servers, and notifies administrators of any violations.

The network-based intrusion detection provides a commercial quality system that can monitor network activity for not only the host on which it runs, but also entire networks.

Detailed network statistics and system reporting

System logging is the looking glass into suspicious activity. Indications of pending system and network issues as well as information on prospective intrusion attempts can easily be analyzed. Extensive logging of internal and external operations utilizing a system with a high level of granularity, allowing storage and analysis of very general event groups or very specific ones.

Track network access, proactively monitor corporate activity EnGarde Secure Linux allows you to monitor access to your Web and email servers and generate graphical reports to develop trends, usage reports on hourly, daily, weekly or monthly hits to your Web sites.

Design Philosophy

Security involves tradeoffs. Mitigating the risks with finding the right level of functionality and performance is always a challenge.

EnGarde utilizes the principle of least privilege. The secure design employed in EnGarde acknowledges the possibility of undiscovered flaws, and takes steps to minimize the security impact these flaws can have. Every part of the system has been closely examined to ensure the programs run with only the privilege it needs and no more.

Additionally, programs that are not directly essential to normal operation are either not enabled by default or simply not included at all. EnGarde users can easily customize the default installation with their favorite applications above what is included from the wealth of pre-existing tools from the Internet.

Every component of EnGarde has been evaluated to ensure it is the best choice with regard to performance, security, stability, and functionality. Only after it meets these criteria is it selected to be included, with additional inspection and security modifications by the Guardian Digital engineers.

The Open Source nature of EnGarde allows for critical peer review of all of our software, improving the product and making it more secure.

EnGarde Addresses eBusiness

Despite a slowdown in growth during 2001, particularly for the first six months, e-commerce sales will increase 57 percent this year compared to 2000, according to an upcoming report by research firm eMarketer. They have concluded that online business will total US$65.9 billion in 2001.

EnGarde Secure Linux provides the ability to get online securely, quickly and completely. Support for the creation of SSL certificates, secure virtual domains and the ability to create complete eBusiness storefronts using AllCommerce marks EnGarde Secure Linux as the only Open Source platform that is completely eBusiness ready.

Using the Web-based management to create a secure virtual host, users can create an online presence within minutes and begin to populate it with their products.

It also contains the ability to generate SSL-enabled Web site just as easily. After it is created you can either generate a new certificate and key pair or upload an existing one, making site migration easier then ever and getting your new secure site up in as little time possible.

A Certificate Signing Request (CSR) can be generated which can then be sent to a certificate authority such as Verisign or Thawte, then imported into your Web site without touching the command-line.

The AllCommerce suite of eBusiness applications is the industry's only enterprise-level e-commerce solution that fully integrates front-end functionality with warehouse operations. Businesses of all types can effectively manage site content, orders, inventory and warehouse facilities—all from a clean, intuitive user interface.

AllCommerce contains a sophisticated database system that gives the administrator great flexibility, power and speed. Web content is delivered to the consumer from information bound at run time. The Web is literally spun out of customers' responses.

EnGarde implements all of the current AllCommerce features, including:

- Store creation can be done in minutes via the GD WebTool interface. You can have a basic site up and running, ready to be populated with sales items in under 5 minutes!
- AllCommerce is designed for flexibility and usability. Every Web page that appears to a user is generated from templates. Changing these templates takes effect over the entire site making customization as easy as could be.
- The AllCommerce search engine is one of the most advanced search engines available. The search engine learns common phrases and syntax. As the AllCommerce store ages, the search engine gets more intelligent, making your users shopping experience even easier.
- The administrative back-end interface allows for extremely easy maintenance of their e-commerce store. Adding items, checking up on orders and stocking inventory can all be done from this single interface.

The GD WebTool can be used to build a working storefront created from default HTML templates linked to a MySQL database. Items for purchase can be entered into the virtual store. Based on submitted store data and the templates, EnGarde will generate the interactive storefront. Never is it necessary to interact directly with the database.

Simple and Secure Web Management

The Guardian Digital WebTool provides basic system administrative functions via a standard web browser using HTTPS (HTTP over SSL). All of the functionality is modularized making the codebase very easy to expand upon. New and customized features can be added very easily.

The unique functions of the GD WebTool can be outlined as follows:

- **Virtual Host Management**: The Virtual Host Management module allows you to perform all the administrative functions necessary to set up and manage a production Web site.
- **System Management**: The System Management module allows you to perform all normal system administrative functions easily. You can add or delete users and assign them to different groups, set up virtual Ethernet interfaces, and configure network time services.
- **System Status Monitor**: The System Status Monitor allows you to view real-time statistics of your system. You can view various logs to see what is going on and see what processes are currently running sorted by username, memory usage, or CPU usage. You can also view disk and network utilization.
- **Security**: The Security module allows you to perform all security-related functions to your machine. The ability to generate SSL certificates, SSH public and private keys, change passwords and perform IP access control functions are also performed here.
- **Guardian Digital Update**: The Guardian Digital Secure Network and Security Control Center enable EnGarde users to have immediate access to system and security updates, support services, and new features.
- **System Backup**: The System Backup module allows you to perform various backup functions such as backup creation, backup restoration, and viewing what files have changed since the backup. When a backup is created you can either save it to the machine itself (for later restoration) or even download it for off-machine archival.

The WebTool communicates exclusively over HTTPS. HTTPS is an implementation of HTTP (Hypertext Transfer Protocol) over SSL (Secure Socket Layer). This allows for a secure connection by encrypting all the traffic between the client and the GD WebTool.

SSL also provides another layer of authenticity because of the certificate involved. The Guardian Digital Certificate Authority (CA) signs this certificate so the user can be sure that they are in fact connected to the GD WebTool rather then a subject in a man-in-the-middle attack.

To enhance the value of the certificate, the user can download and install the Guardian Digital CA directly into their Web browser. If they ever attempt to connect to the WebTool and the certificate presented is not signed by Guardian Digital, they will receive a warning. This warning is an indication of a potential man-in-the-middle attack.

The GD WebTool also provides IP-based access control. Before the user is even presented with the login screen, they must be coming from a pre-defined, trusted IP address or network.

Host Security

Security of the host itself has been significantly improved. Enforcement of longer user passwords, control of expiration dates, and utilization of the latest in advanced forms of cryptography as a means of authentication, close one of the most common and easily exploitable means of intrusion. Advanced forms of authentication permits only authorized users to execute pre-specified privileged commands.

Obtaining access to a local user is one of the first things that system intruders attempt, while on their way to exploiting the root account. Local attacks are attacks that occur once access to the machine has been achieved.

EnGarde reduces the threat normally posed by intruders that gain local access. Significant improvements have been made to reduce the threat from buffer overflows, local and remote denial of service attacks, attacks resulting from improperly configured services, and “default allow” configurations.

To provide the necessary level of security to perform these functions, EnGarde employs the following host security measures:

- **Linux Intrusion Detection System**: The Linux Intrusion Detection System (LIDS) implements an additional level of access control above and beyond what is normally included with the Linux kernel. This Mandatory Access Control mechanism prevents at a kernel level users (including root) from accessing resources they have not explicitly been given permission to access. This means that, for example, even the root user can’t replace trusted binaries such as /bin/login with a Trojan version should the root account be compromised.

- **Extensive Access Control**: The GD WebTool has an entire section devoted to managing access control. This provides the ability to control who is authorized to connect to the server using OpenSSH, and from where they can connect. EnGarde is configured by default to not allow access to any system resources unless otherwise explicitly granted access.

- **Openwall Project**: The Openwall project is an effort to audit source code for potential security vulnerabilities. They have created several kernel security improvements that prevent many types of buffer overflows, restrict symbolic hard links created to files in /tmp not owned by the user, restrict the amount of information available to a user in /proc, provide better management of shared memory segments not in use, and more.

Host Security

- **Restrictive File Permissions**: File and directory permissions are the basic means for providing security on a system. They are also the last line of defense against an unauthorized user reading or modifying information that does not belong to them. Maintaining file and filesystem integrity is essential to host security.

  Every system binary on the system has been evaluated to ensure it has only the level of access required. Less than ten binaries on the system run with superuser privileges regardless of the user executing the command. The “set user ID” file permission attribute, when applied to files owned by root, are especially vulnerable to buffer overflows, format string attacks, and other exploits that can result in complete compromise of the system. All of the system configuration and initialization files that contain sensitive data are only readable by administrative accounts. Log files are also only readable by administrative accounts.

  Unless the user is the owner or in the “admin” group these files are inaccessible. Using access control lists, administrators can even hide files from view on the filesystem, effectively removing any access to all but trusted system commands.

- **Process Accounting**: EnGarde comes with a process accounting package installed that includes the “accton”, “ac”, “lastcomm” and “sa” programs. These provide data and summaries of user times and command usage to further the ability to track user activities.

- **Capabilities**: The ability to remove the dependence on the root user is an extremely powerful notion. As you know, the “root” user normally has complete control over all functions of a Linux box. Binding to a privileged port, loading kernel modules, and managing filesystems are examples of things that typically can only be done by root. If a regular user needed to run the “ping” command, for example, it was necessary to make it run with the privileges of the root user. The ping binary needs root privileges in order to open a raw socket (an operation managed by the kernel) to create the necessary ICMP packet for the echo request.

  Capabilities split up the all powerful root privilege into lots of sometimes orthogonal privileges. By using capabilities to ensure we only have the privilege needed, again limiting the potential damage of security holes.

  Many of the network daemons and processes on an EnGarde system utilize this advanced security technique including vsFTPd, postfix, and xntpd.

- **Chroot Jails**: Normally, network daemons have access to system devices, the filesystem, and standard system binaries and libraries. Using a “chroot jail”, a process can be relegated to a specific region of the filesystem and only that region. This effectively limits the resources available to the particular program. Combined with running a daemon as a standard user and not as root, this adds a significant additional layer of security to the system. Should the daemon be compromised, it will still have a restricted view of the system, limiting the amount of damage that can be done.

  The Postfix, vsFTPd, xntpd, BIND, MySQL, and Snort processes all run either as a non-root user or in a chroot jail.

- **Pluggable Authentication Modules**: EnGarde makes extensive use of Pluggable Authentication Modules. This provides a highly configurable authentication and limitation scheme on a service by service basis as well as general user access. Among many of the common security implementations of PAM, EnGarde also restricts user resource consumption as a defense against denial of service attacks and to enforce MD5 password hashes to all PAM aware services. PAM is used to control both local and remote access.

Network Security

The days have passed when one could distinguish the end of the local desktop computer and the beginning of a computer to which it is connected. EnGarde treats network connections as originating from hosts from which we have no control, and makes extensive use of advanced security methods to prevent remote attacks and limit the impact should the system be compromised.

EnGarde reduces the threat normally posed by intruders that attempt unauthorized remote access. Significant improvements have been made to reduce the threat from IP, DNS, and mail spoofing attacks, SYN flood and other bandwidth consumption attacks, and information leakage.

There are a number of significant improvements EnGarde has made to network security significantly limiting the impact on the integrity of the system should it be compromised.

- **Secure Remote Access**: The use of the Secure Shell as the only means of remote shell access provides strong authentication as well as an encrypted tunnel to protect data privacy.

- **SSL-enabled Administrative Access**: Access to the GD WebTool system administrative menu is strictly controlled with the use of strong encryption, a server certificate signed by Guardian Digital, and IP access control.

- **Insecure Services Excluded**: The lack of inclusion of services normally associated with not having strong authentication such as telnet and rsh prevent one of the most common forms of vulnerability.

- **Extensive use of Advanced Security Techniques**: The use of “capabilities” and “chroot jails” as next generation security enhancements prevent network daemons from accessing protected system resources, effectively relegating them to the level of privilege of a normal user.

- **Least Privileges**: Running services as a normal user wherever possible serves to limit the exposure of the system to unauthorized attempts to access reserved system files and resources.

Virtual Web Hosting

The Virtual Host Management component of the GD WebTool allows you to perform all the administrative functions necessary to set up and manage a standard Web site or an SSL-enabled Web site. Creating a virtual host has never been easier. You simply fill in a few simple fields and click “Create”. Optionally, it is also possible to create a database for this virtual host by providing a username and password for MySQL. The WebTool takes care of the MySQL grant tables.

Providing your organization with an SSL-enabled Web site is just as easy. After it is created you can either generate a new certificate and key pair or upload an existing one, making site migration easier then ever and getting your new secure site up in as little time possible.

If you want to get your certificate signed by a certificate authority such as Verisign or Thawte, you can generate your Certificate Signing Request in the GD WebTool.

The GD WebTool allows you to edit document options, error pages, and aliases and redirects.

By leveraging the AllCommerce package, you can create a complete eBusiness store by following three simple steps. The GD WebTool sets up the directory structure, database, and file permissions automatically. You can follow simple links to edit the store’s configuration and populate it with items.

The Virtual Host Management module also allows you to set up Web site log analysis. You can define how often you want the log analysis to be run and users that can access the summary screens.

Intrusion Detection

EnGarde Secure Linux includes numerous enhancements to both network and host intrusion detection capabilities. The inclusion of system host intrusion prevention features marks EnGarde as the only Linux distribution to provide protection from security events that may occur, as well as detection and notification of potentially threatening events. The network intrusion detection features provide the capability to turn an EnGarde Secure Linux installation into a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks equivalent to expensive commercial systems.

The Linux Intrusion Detection System (LIDS) implements an additional level of access control above and beyond what is normally included with the Linux kernel. This Mandatory Access Control mechanism prevents at a kernel level users (including root) from accessing resources they have not explicitly been given permission to access. This means that, for example, even the root user can't replace trusted binaries such as <tt>/bin/login</tt> with a Trojan version should the root account be compromised. This attempt will then be reported to the system administrator via e-mail or even sent to a pager or cell phone.

Additionally, LIDS can perform these other security functions:

- **Log Auditing**: Logs are kept of all system activity and can be easily referenced.
- **Improved access control**: A fine degree of control over every system resource and file is possible. Based upon a pre-defined access control list, only certain users or programs are permitted read and write access to files and resources.
- **Ease-of-use**: Using the GD WebTool, LIDS appears transparent and will not hinder system usage.

The host intrusion detection included with EnGarde is pre-configured for your system. Experienced Linux users can tweak the level of notification, control the level of access to system resources, as well as numerous other system parameters. It requires no additional configuration as a part of standard system operation.

Through the use of the Web-manageable Tripwire host integrity database, users can maintain data integrity and increase the level of assurance required to be on the Web today. Tripwire is software that monitors all file changes, verifies the integrity of data at rest on network servers, and notifies administrators of any violations. This additional level of protection can be used to monitor changes to Web site data, critical system files, and even changes in hardware conditions.

The network-based intrusion detection utilizing Snort provides a commercial quality system that can monitor network activity for not only the host on which it runs, but also entire networks. Snort produces easy-to-read reports that can be used to alert an administrator to potential network probes and intrusions. Now used by thousands of people, Snort is surely to become the de facto open source network intrusion detection device of the future.

The ever-increasing amount of Internet crackers, armed with “ready-to-run” exploits, as well as the sophisticated attacker that’s intent on defacing your web page necessitates the use of a method to track their activity and alert you to this.

Until now, intrusion detection devices were either dedicated-use commercial products, or not real-time and difficult to install. Snort is the solution for monitoring small TCP/IP networks where it is not cost-effective to deploy commercial products. Snort is an easy-to-use, “lightweight”, and very functional alternative.

Intrusion Detection

Among the wealth of features included with Snort include:

- Detect and alert based on pattern matching for threats including buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other portscanners, well-known backdoors and system vulnerabilities, DDoS clients, and many more
- Use syslog, SMB “WinPopUp” messages, or a file to alert an administrator
- Develop new rules quickly once the pattern (attack signature) is known for the vulnerability
- Record packets in their human-readable form from the offending IP address in a hierarchial directory structure
- Used as a “passive trap” to record the presence of traffic that should not be found on a network, such as NFS or Napster connections
- Used on an existing workstation to monitor a home DSL connection, or on a dedicated server to monitor a corporate web site

Intrusion detection devices are an integral part of any network. The Internet is constantly evolving, and new vulnerabilities and exploits are found regularly. They provide an additional level of protection to detect the presence of an intruder, and help to provide accountability for the attacker’s actions.

Secure Remote Connectivity

Standard Linux systems include support for legacy protocols such as telnet and the Berkeley r-commands that lack any modern form of authentication. EnGarde permits only encrypted remote access, effectively creating a virtual private network between the client and the EnGarde server. Through the use of OpenSSH and the GD WebTool that can be used to generate the necessary public and private keys, users can securely connect to an EnGarde system from anywhere on the Internet.

Even the GD WebTool itself employs SSL certificates as the only means of access. The GD WebTool communicates exclusively over HTTPS. HTTPS is an implementation of HTTP (Hypertext Transfer Protocol) over SSL (Secure Socket Layer). This allows for a “secure” connection by encrypting all the traffic between the client and the GD WebTool.

SSL also provides another layer of authenticy because of the certificate involved. This certificate is signed by the Guardian Digital Certificate Authority (CA) so the user can be sure that they are in fact connected to the WebTool rather then a subject in a man-in-the-middle attack.

The GD WebTool also provides IP-based access control. Before the user is even presented with the login screen, they must be coming from a pre-defined, trusted IP address or network. If they are not, they are given an access denied page.

The use of the vsFTPd marks EnGarde Secure Linux as the only distribution to include and provide full support for the next generation in secure FTP services. This ‘very secure’ FTP daemon was developed from the ground up with specific regards to security, and takes advantage of cutting edge security technologies. Unique to vsFTPd is its use of a secure initial design, strong inter-process communication facilities, “capabilities”, a “chroot jail”, attention to trust relationships that may be dangerous, and secure buffer handling to avoid many types of potential buffer overflows.

EnGarde and AllCommerce Support

Guardian Digital provides comprehensive system support for your enterprise. Our security and support operation center is available to guide customers with specialized service requirements. Network and system health monitoring, combined with security policy review, and our Security Control Center that provides automatic notification of security and application updates, helps to maintain the necessary level of security required to conduct business on the Web.

Guardian Digital can help bridge the support gap between the fast-paced nature of the Internet, open source software development, security, and commerce. Guardian Digital has the Linux expertise and personalized service required to ensure the Linux solutions we provide enable your business to quickly and effectively build a secure eBusiness presence. Our network and security engineers have the authoritative answers to resolve your most difficult concerns.

The Guardian Digital Network, including the Security Control Center, provides users of EnGarde with automatic notification and installation of software and security improvements, increasing reliability and productivity, while dramatically lowering maintenance costs.

Using the SSL-enabled Web interface integrated within EnGarde, users can receive instant notification of security events, proactive software updates, and download new products and features.

Services including software and security updates, network and system health monitoring, security policy review and verification, site planning and implementation combine to simplify network management, increase productivity, reduce total cost of ownership, all come together to form a single source for support and security services.

System and Security Updates

One of the most important aspects of security is keeping up to date with the latest software packages and bug fixes. Using the latest software will greatly increase the overall security of your system. Included with EnGarde is a utility that will allow you to easily and securely keep your system up to date.

The GD Update utility is a section of the GD WebTool that will determine what new software is available, and install any updated software. You will be prompted to authorize all changes.

All new packages are downloaded directly from Guardian Digital via an SSL secured connection to insure the highest degree of security and data integrity.

Secure Electronic Mail

EnGarde runs the Postfix mail server due to its merits as a more secure mail system. Postfix was developed by Wietse Venema, author of TCP Wrapper and many other security programs that have become a staple of modern Linux systems. Postfix was developed with security as a primary focus, and leverages a number of advanced techniques to improve its resiliency to attack. Postfix differs from other common mail servers quite a bit, in that:

"There is no direct path from the network to the security-sensitive local delivery programs - an intruder has to break through several other programs first. Postfix does not even trust the contents of its own queue files, or the contents of its own IPC messages. Postfix filters sender-provided information before exporting it via environment variables. Last but not least, no Postfix program is set-uid."

Additionally, Postfix runs in a controlled environment, called a "chroot jail", with fixed low privileges that permit it only access to a restricted set of system resources, not the entire pool of system resources, where the potential of system compromise is greatest. With the additional change of running the Postfix processes as a standard user without root privileges, Postfix is sure to be the most secure mail server to date.

Postfix has also been configured to restrict what hosts can relay their mail through the mail system, and supports restrictions on what mail is allowed to come in. Postfix implements the usual suspects including blacklists, RBL lookups, and HELO/sender DNS lookups.

Management of thousands of mail domains can be controlled using the GD WebTool Web interface, seamlessly integrating with DNS to make the process extremely easy.

Even the process of receiving mail is done securely with EnGarde. Conventional methods of receiving e-mail, including IMAP4 and POP3, are insecure and permit e-mail to be easily intercepted and read. EnGarde virtually eliminates this threat by using SIMAP4 and SPOP3.

Using standard mail client programs such as Netscape, Outlook or Eudora, users can continue to receive mail as they normally do, but their passwords and the content of the mail itself is encrypted with the use of SSL 128-bit encryption before it is sent, virtually ensuring its secure delivery. For this reason, standard unsecured POP3 and IMAP4 aren't even configured.

Among the features of the mail delivery system include:

- Only encrypted e-mail is transmitted to a users e-mail client. Ordinary Linux distributions transmit passwords and e-mail content in unencrypted form, allowing anyone to snoop on the connection and easily read a users mail.

- The encryption methods applied here also prove user and server authentication so a user always knows they are communicating with a trusted server.

- Secure e-mail via IMAP and POP3 over SSL is supported in almost all of today's most popular e-mail clients in Windows, Mac OS and Linux operating systems.

Secure System Logging and Auditing

System logging is the looking glass into suspicious activity. Indications of pending system and network issues as well as information on prospective intrusion attempts can easily be analyized. Extensive logging of internal and external operations utilizing a system with a high level of granularity, allowing storage and analysis of very general event groups or very specific ones.

The importance of secure and reliable system logging cannot be underestimated. Extensive system logs are kept so past system activity can be easily monitored. EnGarde includes the syslog-ng system logging daemon and swatch, the log processing program, to separate system and security messages, making it easier to isolate normal system messages from messages that may require further attention.

The GD WebTool can then be used to view system information in an easily readable format. System activities can also be configured to be e-mailed the administrator on a daily basis.

This daily summary breaks down important daily information, such as root logins, SSH logins, and failed root logins into an easy to read format to help you stay on top of your EnGarde system's daily activities. These daily summaries are delivered every night to you via e-mail.

- Daily summaries are kept and can be archived in e-mail of each days system activities
- Logs are audited as the come in and organized through the GD WebTool in a user-friendly fashion
- Each day logs are rotated and archived for up to seven days.
- With some basic system knowledge logs can be manipulated to filter customized data

Secure Domain Name Services

Maintaining large DNS zones can be an administrator's worst nightmare. With the GD WebTool, you never have to touch configure files again. The GD WebTool allows you to create forward and reverse master zones, along with slave zones. It also provides consistency in the configuration files, ensuring that no security or configuration option is ever overlooked or left in an insecure setting.

Additionally, EnGarde adds a significant number of improvements to standard configurations. Among these changes include:

- Access Control: Extensive access control modifications have been made to prevent all but authorized users from transferring zone information by default, as well as performing queries on non-public domains.
- Least Privileges: Configured to run as a non-privileged user, the server is severely limited in the information to which it has access. This significantly reduces the overall impact should the system be compromised as a result of a vulnerability. Additionally, it runs in a restricted chroot jail, greatly improving the resiliency to attack.
- Reliable Logging: The additional logging enabled by default provides an administrator with a detailed account of zone transfers, operating system issues, security-specific messages, and service statistics.

Further Information

EnGarde Secure Linux is currently available for download under the GNU General Public License from the EnGarde Linux homepage and worldwide network of mirrors.

Please visit us on the Web at http://www.EnGardeLinux.org for download information, up to date news and resources, and support guidance.

EnGarde Secure Linux is also commercially supported by Guardian Digital. Orders include a printed manual, free installation support, and a trial subscription to the Guardian Digital secure online network services.

Guardian Digital provides a complete range of support options including incident-based and contractual, as well as AllCommerce development and support.

For pre-configured server appliance solutions featuring customized EnGarde Secure Linux, and further information about Guardian Digital, please visit us on the Web at http://www.GuardianDigital.com.

Guardian Digital

Pioneering. Open Source. Security.

www.GuardianDigital.com

1-866-GDLINUX

To learn more, visit us on the Web at
www.GuardianDigital.com or call 1-866-GD-LINUX.