

# Secure By Design: How Guardian Digital Secures EnGarde Secure Linux

## 1. Introduction to Guardian Digital and EnGarde Secure Linux

### 1.1. Pioneering Open Source Security in an Insecure World

Since its inception in 1999, Guardian Digital has been revolutionizing the way companies conduct business over the Internet. Guardian Digital recognized from its beginnings that the Internet, conceived and expanded with little regard for security, required a new and more disciplined set of Internet services and tools if businesses were to remain secure. Guardian Digital was among the first to realize that this secure Internet infrastructure could best be constructed using the resources of the rapidly expanding open source software community. The result of these insights is EnGarde Secure Linux, an efficient, easy-to-use and cost-effective Internet services platform offering an unparalleled level of built-in security.

### 1.2. Guardian Digital and the Open Security Model

The explosive growth of the Internet during the late 1990s was fueled by the rise of open Internet standards, open source software and the Linux operating system. To create EnGarde Secure Linux, Guardian Digital brought together the work of its engineering team and the contributions of the world community of open source security enthusiasts and professionals. Guardian Digital recognized that the open source model also provided the best approach to the problem of maintaining security in the relentlessly dynamic environment of the Internet. By making every element of EnGarde Secure Linux freely available for inspection by security professionals and enthusiasts throughout the world, Guardian Digital ensures that any security vulnerabilities in EnGarde Secure Linux will be rapidly found and corrected. And by freely distributing EnGarde Secure Linux to the community, Guardian Digital subjects its services to the harsh realities of Internet service and receives constant feedback from thousands of users around the world in every imaginable business setting. The result is secure and enterprise-ready platform for delivering enterprise-class services.

### 1.3. What is EnGarde Secure Linux?

By joining a disciplined, professional approach to security with the resources and tools of the open source community, Guardian Digital has created EnGarde Secure Linux, the perfect platform for developing a highly-secure online presence. EnGarde Secure Linux is not just another "repackaged" Linux distribution, but a unique collection of the best open source tools, selected and integrated by Guardian Digital's engineering team. EnGarde Secure Linux builds on kernel-level security policies and incorporates a wide range of proven security tools like host and network intrusion detection to deliver the most secure available open source platform for any Internet service, from Web and mail services to FTP and proxy services.

## 2. Design Philosophy

Guardian Digital builds EnGarde Secure Linux on the principle that security is the first priority of a modern operating system and must therefore be considered in every element of its design. This is very different from the more common practice of "hardening" a system by attempting to remove security vulnerabilities after the system is complete, for example by restricting permissions or closing ports. To achieve an unparalleled level of security, EnGarde Secure Linux tailors its system following the principle of "least privilege" in which every program and service is given only the privileges and access it needs to do its job, and no more.

Many operating systems compromise both security and function by offering a "server" system that is in fact only a stripped-down version of their basic desktop system. Guardian Digital has built EnGarde as a server system only, choosing, installing, and enabling only those services that are needed to provide efficient Internet or network services. Despite this selective approach, however, EnGarde is not a single-purpose tool like many "appliance" hardware boxes, but is instead a complete system of service offerings, one that Guardian Digital constantly enhances through the selective addition of open source services.

The security of EnGarde is further enhanced by its open source nature. Every component of EnGarde is evaluated, not just by the skilled members of the Guardian Digital engineering team, but by programmers, security experts, and users all over the world who quickly detect any security flaws and help provide fixes.

### **3. Feature Overview**

EnGarde Secure Linux achieves its unique built-in security by drawing on the worldwide resources of the open source community, selecting "best of breed" open source security tools and then carefully configuring these tools for maximum security. These tools include:

- **SELinux kernel-level security**

EnGarde Secure Linux uses SELinux, a system of kernel-level security tools originally developed by the NSA (National Security Agency) to control access by processes and programs to only those resources they need to do their jobs, thereby preventing the large-scale damage that intrusions and compromises can wreak on traditional computer systems.

- **Guardian Digital WebTool remote administration**

EnGarde Secure Linux is designed for secure and convenient remote administration using Guardian Digital's custom-designed interface, the WebTool. The WebTool streamlines and simplifies all common system administration tasks, and guides the user in maintaining securely configured Internet services.

- **Guardian Digital Secure Network**

Users of EnGarde Secure Linux receive program updates and security patches through the Guardian Digital Secure Network (GDSN) using the Guardian Digital WebTool, thereby ensuring that their EnGarde systems remain secure.

- **Intrusion Detection**

EnGarde Secure Linux uses the best available open source tools to detect both actual system attacks and potential threats using the both local host-based detection systems and systems that detect network-based threats.

- **Secure Internet services**

EnGarde Secure Linux selects the best available open source programs like Apache, Postfix, and vsFTPd and then configures them for maximum security, functionality, and productivity using the Guardian Digital WebTool.

## **4. Security at the Kernel and Security Enhanced Linux (SELinux)**

EnGarde Secure Linux begins its defense in depth at the kernel, a level neglected by many supposedly secure systems, through the comprehensive application of security policies using Security Enhanced Linux (SELinux). Although released in its current form relatively recently, SELinux has a substantial heritage as part of a decades-long effort to develop inherently secure or "trusted" operating systems. This largely academic effort culminated in the development and subsequent public release by the National Security Agency (NSA) of SELinux. The release of this previously closely-guarded security framework was both a complete surprise to the open source community and a watershed in open source security development.

Guardian Digital was among the first in the open source community to realize the revolutionary potential of SELinux policies for building a truly secure operating system. Soon after the release of SELinux, Guardian Digital committed itself to the ambitious goal of applying SELinux policies to every element of its secure operating system and to every service it offered. Guardian Digital achieved this goal with the release of EnGarde Secure Linux 3.0, among the first and most thorough implementations of SELinux.

### **4.1. The Hazards of "root" Access**

The most serious system compromises occur through "privilege escalation" when an intruder gains access to an ordinary local account and then leverages it to obtain root access. In traditional systems, the intruder then has unrestricted access to all system resources and the game is over: the intruder is beyond the reach of anti-intrusion and other conventional security measures.

EnGarde Secure Linux changes the rules of the game by re-architecting the Linux security model to govern the activities of every system activity through a set of security policies. No system user, not even root, has unlimited power to alter critical files or carry out critical functions. Every command must be within the scope of a policy-defined "role" and, in contrast to an unmodified system, there is no easy means by which a process or program started by one role can acquire the powers of another role without specific policy authorization.

### **4.2. "Mandatory Access Control": Limiting The Damage from Security Breaches**

EnGarde Secure Linux, through the use of SELinux policies, exchanges this insecure practice of granting access to resources based on the privileges of the user running a program, for example a Web server, for one based on granting the program only the resources it needs to carry out its functions. This mandatory policy-based limitation on program activity prevents intrusions and compromises from being readily turned into destructive attacks on the system as a whole.

### **4.3. "Targeted" SELinux implementations vs. "Comprehensive" EnGarde Secure Linux**

Although other Linux distributions make use of SELinux policies, most apply them only to selected parts of the system and to certain "critical" applications. Some open source systems do this because their security policies must be made to fit desktop systems, which have entirely different security requirements and run a much wider variety of software.

Guardian Digital, by contrast, examines every package it includes in its installation or offers through the Guardian Digital WebTool and creates an appropriate SELinux Policy Module for each application, ensuring that every program runs in a carefully secured environment.

## **5. Security and the User Experience: The Guardian Digital WebTool**

Security in EnGarde Secure Linux extends from the unseen policies applied at the kernel by SELinux to the most mundane day-to-day aspects of system administration--the province of the Guardian Digital WebTool. The WebTool allows the user to perform all basic administration remotely using a standard browser over an encrypted SSL connection to the EnGarde server. The WebTool's carefully designed interface hides the abstract decisions involved in securely managing Internet services and guides the user through maintaining a securely configured system.

### **5.1. Limiting Access to Services**

All operating systems that show any concern for security begin with secure default settings, limited access to system resources, and "default-deny policies". EnGarde Secure Linux goes further by managing its system through an interface designed to enforce and maintain security without involving the user in the details--the Guardian Digital WebTool. EnGarde draws a clear distinction between services that need to be immediately available to all users and from all locations, like Web and mail service, and those that need to be tightly restricted by default. Before the latter services can even be run, the administrator must specify access by user and IP address.

For similar reasons, and also in contrast to most systems, the WebTool turns off all but a few essential services at startup until the user designates those services she wishes to run at system startup.

### **5.2. The EnGarde Secure Linux Secure Services Portfolio**

EnGarde Secure Linux differs from other platforms for network and Internet services not so much in the services it offers, but in the secure environment in which they operate. EnGarde chooses programs from the most secure available open source offerings and through the WebTool ensures that they are accessed and managed securely.

#### **5.2.1. Encryption and Passwords the Guardian Digital Way**

Secure communication begins with a secure login. EnGarde Secure Linux enforces encrypted passwords for every service it offers, with the exception of FTP, a service for which secure alternatives like SFTP and SCP are readily available. For truly secure communication by critical services, EnGarde builds in encryption behind the scenes wherever needed. For public Internet services like Web and mail service, EnGarde makes it as easy to set up SSL-enabled services as it is to set up non-secure services. An HTTPS virtual host, for example, can be created using the WebTool simply by selecting the "SSL-enabled" option. The WebTool goes a step further in the creation of mail service and removes even the option of automatically creating a non-SSL POP or IMAP server, requiring encrypted SPOP and SIMAP. And for the Guardian Digital WebTool administration, the most critical secure service of all, EnGarde also mandates a secure SSL connection.

#### **5.2.2. Secure Web server**

Setting up and configuring a secure Web server can be a complex process, and one full of security pitfalls for the unwary. Creating secure SSL-enabled sites avoids the serious vulnerabilities common to most Web sites, but this process can be especially difficult. EnGarde Secure Linux, through the Guardian Digital WebTool, makes it possible to create secure SSL-enabled sites in only a few more steps than it takes to create ordinary Web sites. The WebTool also avoids many other mis-configurations and insecurities associated with creating a Web site by managing the setup of DNS service and the creation of an associated database when these are desired.

### 5.2.3. Secure Mail Transport and Delivery

Mail servers are also notoriously difficult to set up and prone to security-damaging misconfiguration. EnGarde Secure Linux, through the WebTool, reduces the creation of secure virtual mail domains to a few steps while maintaining secure default settings. Unlike most mail servers, EnGarde mail servers are configured by default to use secure SSL-enabled connections to mail clients. The WebTool also simplifies the setup of EnGarde's mail servers as relays, a sometimes tricky operation in conventionally-managed mail servers and eliminates security flaws caused by common misconfigurations like creating "open relay" servers.

### 5.2.4. Secure Databases

Although databases are an integral part of modern Internet services and are a common companion to Web services, many systems require the user to install and configure database support independently of other services and run the risk of introducing security vulnerabilities. EnGarde Secure Linux, through the WebTool, relieves the user of this burden by making it easy to setup a MySQL database at the same time that she creates each Web Virtual Host while at the same time maintaining secure default settings.

### 5.2.5. Secure Shell access (SSH)

Although EnGarde Secure Linux is designed so that all necessary system administration and security functions can be performed through the WebTool, there are some activities, like file management on the Web server, and even some obscure configuration tasks that are best performed through shell commands. EnGarde provides secure shell access (SSH) for this purpose and makes SSH easy to set up through seamless use of the WebTool's key-generation capability. EnGarde eliminates potentially insecure access to the shell by making SSH the only means of access.

### 5.2.6. Other services managed by the WebTool

#### 5.2.6.1. vsFTPD and "very secure" FTP service

The most notorious Achilles heel of traditional Internet servers is the FTP service. EnGarde Secure Linux protects its server by selecting and installing vsFTPD, an FTP server designed from the ground up for secure file transfer through the use of secure default settings, "chroot jails" to limit user access, and careful attention to issues like buffer overflows. The WebTool ensures that only secure defaults are presented to the user, for example by requiring the user to turn on access to potentially insecure features like anonymous FTP access.

#### 5.2.6.2. Firewall Service

Every secure server needs basic firewall protection from network attacks. EnGarde Secure Linux provides a firewall service that is conveniently set up and managed through the WebTool. The WebTool's Firewall module allows the administrator to define interfaces, create and delete firewall rules, and implement features like IP forwarding and masquerading to enhance the security of the protected network.

#### 5.2.6.3. Secure DNS (Domain Name Service)

Domain name service is critical to the function of all other Internet services and is complex and difficult to configure in standard installations, especially on networks with many zones. By placing DNS setup and configuration under the control of the WebTool, Guardian Digital makes it easy to create forward and reverse master zones, as well as slave zones, and manage zone transfers. The WebTool also helps the administrator avoid common misconfigurations and insecure settings,

carefully restricting potentially dangerous zone transfers by default. EnGarde further protects the DNS service by running it in a "chroot jail" thereby limiting the potential damage from compromises to the Web server. EnGarde helps the administrator guard against DNS attacks through customized system logs that separately report zone transfers, system issues, security-specific messages and service statistics relating to DNS Server.

Finally, Guardian Digital ensures that DNS service remains secure and correctly configured through regular updates using the Guardian Digital Secure Network.

#### *5.2.6.4. Proxy Services*

Guardian Digital works constantly to expand the services supported by the EnGarde platform. Guardian Digital's latest service offering is based on the open source Squid caching proxy server and brings an extra level of security for those using the service, while significantly improving the performance of Web, FTP and other network services. By intercepting and passing along traffic between network clients like Web browsers and services on the public Internet, the proxy server gives the EnGarde administrator fine-grained control over each user's access to the Internet, along with the ability to filter Web access and examine other Internet traffic for potential dangers. Using the WebTool, the EnGarde administrator can easily configure both the security features and the performance-enhancing caching features of the proxy server.

#### *5.2.6.5. Backup and UPS support*

No system is secure without the ability to recover quickly from system damage and compromise by restoring files or entire systems from a reliable backup. Instead of leaving choice of backup systems and the selection of files to the user, as many operating systems do, Guardian Digital includes in the WebTool a backup module that automatically selects the most critical files for backup and directs the backup to a user-selected directory.

Another small but important administrative detail often left up to the system user is UPS (Uninterruptible Power Supply) support for the system hardware. Here again, Guardian Digital integrates and configures an appropriate open source tool to allow the system user to monitor and configure the way in which the UPS manages power interruptions.

## **6. Defense in Depth: Intrusion Detection and EnGarde Secure Linux**

Layered security means not just preventing attacks and limiting their damage but also taking proactive measures to identify potential threats and detect malicious activities before they can cause further damage. Since attackers almost always leave traces of their activities, EnGarde monitors both the server itself and its network interfaces for signs that an attack is threatened or is actually taking place.

### **6.1. Network-based Intrusion Detection**

Detecting potential attacks and compromises begins by monitoring the network interfaces for signs of trouble. EnGarde deploys the Snort network intrusion detection system to examine network traffic in real time, searching for signs of a variety of attacks and probes, from buffer overflows to port scans. To this external network monitoring, EnGarde adds its own custom open source tool, NetDiff. NetDiff logs and reports changes in the status of the server's network ports to alert the administrator to newly-opened ports that may be the result intrusions or compromises.

## **6.2. Secure System Logging, Host-based Intrusion Detection and the WebTool**

No network-based system can detect all intrusions and not all intrusions can be detected by automated tools. EnGarde helps the user monitor the system for signs of suspicious activity by introducing a secure system for maintaining and analyzing system logs, and then adding host-based intrusion detection.

### **6.2.1. Secure and Reliable System Logging**

EnGarde extensively logs all internal and external system activities and uses open source log analysis tools to separate ordinary system messages from security messages requiring special attention. Through the Guardian Digital WebTool, the administrator can view system information in an easily readable format. EnGarde generates daily log summaries that highlight important security information like attempted root logins and delivers them every night via email so that the administrator can investigate and correct these vulnerabilities.

### **6.2.2. Host-based intrusion detection**

EnGarde builds on its infrastructure of secure and accessible logs, adding a open source host-based intrusion detection system that, in addition to examining log files, identifies and checks critical system files using checksum information to reveal traces left by system attacks and compromise. These intrusion detection systems are particularly helpful in revealing the presence of a rootkit, the tool of choice for many system attacks. It should be noted here that unlike most other systems, EnGarde provides an essentially complete defense to rootkit attacks, detected or undetected, through the use of SELinux policies.

## **7. Security Threats and the EnGarde Secure Linux Response**

The harshest reality of system security, and not just of computer systems, is that not all attacks can be anticipated, or even imagined, and that attacks that can be anticipated cannot always be prevented. EnGarde Secure Linux confronts this reality by using threat detection and containment to prevent or minimize the damage caused by attacks and intrusions. Instead of attempting to create rules and strategies for every conceivable security threat, EnGarde extends across the board the firewall principle of "default-deny"--sometimes expressed as "that which is not expressly permitted is forbidden". As has been emphasized previously, this is the only effective response to so-called "zero-day" threats for which no response has yet been devised.

Here are some examples of how EnGarde responds to common types of attacks and compromises.

### **7.1. Configuration-related compromises**

As computer systems and their environment grow more complicated, the effort required to configure, update and maintain them increases dramatically, along with the potential for inadvertently creating serious security vulnerabilities. EnGarde Secure Linux relieves its users of as much of this burden as possible by placing all administration under the control of the Guardian Digital WebTool. The WebTool then presents only secure default settings to the administrator and eliminates choices that could have disastrous security effects.

Secure defaults are not the only protection afforded by the WebTool. Many dangerous misconfigurations, like the open relay mail server described earlier, arise when system administrators are confronted with service problems, especially in an emergency, and are forced to experiment with system settings in attempt to resolve problems. This can result in "temporary

changes" like "world-writable" permissions or applications that run as root. The WebTool makes it virtually impossible to make changes like these that can seriously impact the security of the system.

Most common day-to-day configuration vulnerabilities, however, come from failing to keep up with system upgrades and security patches. Many systems either require the user to find and apply the necessary upgrades and patches, a tedious and error-prone process, or they drown the user in a torrent of upgrades, many of which create problems of their own. EnGarde Secure Linux eliminates this vulnerability by providing carefully selected and managed upgrades through the Guardian Digital Secure Network.

## **7.2. Server Host-based compromises**

Attacks on the server are met by EnGarde Secure Linux with a variety of defense in depth strategies designed to detect intrusions and minimize the damage they can cause. The first line of defense in EnGarde Secure Linux is Guardian Digital's commitment to secure coding and security best-practices in building EnGarde. For example, experts believe that buffer overflows, which are the result of poor programming practices, are the starting point for a majority of system compromises. By carefully choosing and implementing the packages that make up EnGarde, and by eliminating known vulnerabilities through regular updates through the GDSN, EnGarde eliminates many of these coding-related vulnerabilities. Since these vulnerabilities can never be entirely eliminated, however, EnGarde deploys a variety of defenses to prevent code executed through the successful exploitation of a buffer overflow from leading to further compromise.

EnGarde detects attempts to run unauthorized code or alter system files through the use of carefully-configured open source intrusion detection software. Even if the effects of the unauthorized code are not detected, or the administrator takes no action, the potential intrusion is still trapped by EnGarde's SELinux policy restrictions. These restrictions prevent the unauthorized program from gaining root powers through "privilege escalation" or from accessing files needed to operate or to communicate over network ports. This combination of intrusion detection and policy restriction will thwart the most common and damaging of host exploits, the rootkit, since even a successful and undetected buffer overflow exploitation cannot gain the root status needed to launch a successful attack on the system.

## **7.3. Network attacks**

EnGarde Secure Linux also uses a variety of strategies to deal with attacks originating from the server's network. EnGarde's first line of defense to these attacks is to detect and report anomalous or suspicious network activity through the use of the Snort intrusion detection program. Snort examines network packets to look for the "signatures" of potential network threats and notifies the user when they are detected. Since Snort, an open source tool, is only effective when its set of rules is kept up-to-date, EnGarde, through the GDSN, keeps Snort supplied with the very latest rules.

EnGarde also helps reduce network vulnerabilities resulting from improper network configurations like inadvertently opened network ports by including its own network port status utility, NetDiff, which runs the Nmap port scanner at regular intervals, compares the results, and reports changes that could open EnGarde to network attacks. While these techniques cannot prevent network attacks like "Denial of Service" attacks that overload the server by exploiting flaws in the network protocols themselves, it does allow the EnGarde user to react quickly to potential or actual network attacks and prevent serious service interruptions.

## **7.4. Snooping and Eavesdropping**

Not all attackers are bent on causing damage to the system. Instead, many are attempting to steal private information by listening to the system's communications within the server or over the network. One common follow-up to rootkit intrusions, for example, is to install "keylogger" programs that record the system user's keyboard input to steal passwords. Another

example is network "sniffing" commonly used to intercept passwords to outside systems as well as sensitive personal information like financial data and social security numbers. EnGarde presents several defenses to this kind of unauthorized listening. First, EnGarde makes it difficult or impossible for a would-be listener to install and run "snooping" software on the system by using the combination of detection and access restrictions described above. More important, though, EnGarde prevents the listener from finding anything intelligible to listen to by using encryption for every sensitive communication and every important service.

## **8. Security, Consistency and the Guardian Digital Secure Network (GDSN) Promise**

In order to remain secure, any system must have a method for maintaining, upgrading and enhancing the system to keep it in a consistent and predictable state. Many open source systems fail in this respect because they rely on the user to find and apply, sometimes haphazardly, a variety of packages and updates. EnGarde Secure Linux derives its stability and consistency from the work of Guardian Digital's team of security engineers, who carefully select and tailor all alterations to EnGarde with security in mind, while making sure that changes do not cause unexpected changes to other parts of the system. The GDSN is Guardian Digital's promise to EnGarde users that EnGarde will always continue to behave as expected and that upgrades and changes will enhance and not impair EnGarde's security and functionality.

### **8.1. Upgrades and Security Patches**

The GDSN makes system and program upgrades and security patches conveniently available through the WebTool's Updates module so that all upgrades are available from a single source. Guardian Digital evaluates every patch and upgrade in the context of the system as a whole to make sure that it does not change existing configurations.

### **8.2. Enhancements and Adding New Services**

Rather than expecting EnGarde users to install individual packages and deal with any resulting dependencies and interactions, and their resulting security implications, Guardian Digital configures complete services for installation and makes them available through the WebTool. Guardian Digital constantly adds value to EnGarde by expanding the range of Internet and intranet services offered in EnGarde, for example through the recent introduction of the Squid proxy service and the planned introduction of VPN (Virtual Private Network) and VoIP (Voice over IP) services.

## **9. Summary**

Users of Linux and other open source systems have long taken for granted their stability, versatility and scalability. Guardian Digital has now added the missing element--security that is comprehensive, seamlessly integrated and easily maintained. By implementing SELinux policies at the kernel to regulate applications and processes, EnGarde protects the system against the previously unknown "zero-day" attacks to which most systems fall prey and limits the damage caused by even the most "successful" exploits. EnGarde Secure Linux extends its strategy of defense in depth by adding network defenses like network intrusion detection and encrypted public Internet services, as well as defenses at the server itself, including host-based intrusion detection and secure logging features. The keystone of EnGarde's secure architecture is the Guardian Digital WebTool, which provides encrypted remote administration and guides the administrator in maintaining secure configurations while preventing a wide range of potentially insecure and damaging misconfigurations. EnGarde closes the security loop by offering program updates, security patches, and installation of additional secure service packages through the Guardian Digital Secure Network.

