Secure By Design: How Guardian Digital Secures EnGarde Secure Linux (ABSTRACT)

ABSTRACT

1. What is EnGarde Secure Linux?

EnGarde Secure Linux is not just another "repackaged" Linux distribution, but a modern open source system built from the ground up to provide secure services in the threatening world of the modern Internet. EnGarde Secure Linux is the creation of Guardian Digital, Inc. a pioneer in open source security since 1999, and has been developed since then in collaboration with the worldwide community of open source security enthusiasts and professionals. Guardian Digital provides a secure and consistent environment for EnGarde Secure Linux through the Guardian Digital WebTool and the Guardian Digital Secure Network. A server-only system, EnGarde Secure Linux is administered securely and remotely using the WebTool, a custom interface that both simplifies server administration and guides the system user in maintaining a secure configurations for all of the services that comprise EnGarde. The Guardian Digital Secure Network maintains the consistency and security of EnGarde by providing system upgrades and security patches that have been constructed by Guardian Digital's engineering team to relieve the user of the burden of maintaining the system in a consistent and secure state.

2. Defense In Depth In EnGarde Secure Linux

Security is the primary consideration in designing every element of EnGarde Secure Linux. Guardian Digital applies basic security principles like "least privilege", "no unnecessary services" and "default-deny" rules to every level of EnGarde from access to kernel itself to defense of the network perimeter. Security begins with the selection of the best available open source packages, chosen and tailored for maximum security and following software security best-practices. The next level of protection comes from a complete re-engineering of the standard Linux security model using Security Enhanced Linux (SELinux). SELinux implements the principle of "Mandatory Access Control" which places each program and process under the control of its own SELinux policy, limiting its access to files and resources and effectively containing any intrusions or compromises. EnGarde Secure Linux builds on this secure foundation by placing all administration of EnGarde and its services under the control of the Guardian Digital WebTool. The Guardian Digital WebTool is a secure, remote graphical administration interface that is carefully tailored, not just to simplify administration, but to help maintain secure practices and configurations. For example, EnGarde, through the WebTool, limits user and IP access by default for most services like FTP file transfers and POP/IMAP mail retrieval. For services that must be publicly accessible like Web service and mail transport, the WebTool offers simple setup of SSL-enabled encrypted services. The WebTool also mandates secure practices like encrypted passwords and prevents hazardous configurations like open mail relays. EnGarde Secure Linux extends its secure environment through the use of a carefully integrated selection of the best open source security tools for detecting compromises and intrusions at all levels. EnGarde generates special security-focused system logs to help the administrator identify potential compromises, and adds to this host-based intrusion detection tools. EnGarde monitors the system for potential network compromises and intrusions using the open source Snort intrusion detection system, adding its own NetDiff port status monitoring software.

3. Summary

Linux and open source systems have long been renowned for their stability, versatility and scalability. EnGarde Secure Linux adds the feature crucial to providing services on the modern Internet -- security. Guardian Digital builds security into every element of EnGarde by selecting the best available open source tools and services available and configuring them with security as the top priority. Recognizing that security can only be maintained in a consistent and stable environment, Guardian Digital relieves the user of the burden of "hardening" the system and following secure practices by designing

secure administration into its WebTool and by updating and securing the system through the Guardian Digital Secure Network. For an in-depth exploration of the EnGarde Secure Linux security environment, see the full version of this document at http://www.engardelinux.org/doc/other/wmes/wmes.html.