



RED HAT ENTERPRISE LINUX SECURITY



A POWERFUL COLLECTION OF RED HAT ENTERPRISE LINUX SECURITY TOOLS

Computing security has never been more important. Increasing regulations, differing requirements from international locales, and sophisticated attacks all contribute to serious challenges that call for thorough solutions. Red Hat has deep security experience, and provides the technology and consulting that you require.

Comprehensive security not only covers a broad range of solutions, it also offers strategies for managing systems today and into the future. Attention to security must be pervasive across all of the technologies a company uses and across all of the functionality that a company provides. There are fundamental elements of any sound security solution that must be observed, including:

- **Access:** Security starts with who can access your systems, and what role each user will play. Systems must offer convenient identity management through enterprise directories, authentication of that identity through authoritative sources, and definition of roles and allowable actions through enforced access control.
- **Activities:** Once identified, systems must ensure that users can only perform actions that are consistent with their roles. Protecting access or modification of data - while in storage and in transit is critical.
- **Auditing:** The system must be able to track and document users' actions to meet compliance requirements, to document complex activities, and to identify unauthorized actions that may have occurred through software failures or hacking.

In this series of security subsystem profiles, we will focus on some of the most important and fundamental Red Hat security technologies and services.

SECURITY AND AUDITING AS A DEVELOPMENT PARADIGM

Red Hat advocates a pro-active security approach. At Red Hat, security is part of the requirements that define a project, the architecture that structures a design, and the technologies that implement that design. Security is integrated into a system as thoroughly as any other business requirement.

SELinux separates policy definition from implementation of those policies, allowing creation of the policy rules that define and constrain system behavior while a system is being designed. Not only will those rules more accurately define a system's behavior, they will make developers more aware of the ramifications of security design decisions.



Auditing a system's behavior not only benefits a production system, but it also provides useful information while a system is being developed. Just like programmers profile program runtime activity to identify where optimization is required, auditing a program's interaction with the operating system reveals critical profile information such as use of file system and network resources. When auditing is performed early in a development project, it is more likely to guide that development at greatly reduced costs.

Red Hat not only prevents security breaches in real-time, but it also prevent them as early as possible.

RED HAT SECURITY TECHNOLOGIES

The following overview provides an introduction to some of the Red Hat Enterprise Linux technologies that solve critical security problems.

SSSD	The SSSD (System Security Services Daemon) provides access to remote identity and authentication mechanisms (e.g., LDAP, NIS, Samba, and IPA). In addition to aggregating those mechanisms into a common interface, it provides caching so that on-the-road users can be authenticated even while working offline. (For more information, see Red Hat Enterprise Linux Security Series: SSSD)
SELinux	SELinux can enforce the access rights of every user, application, process, and file within a Red Hat system to a degree previously unavailable in enterprise operating systems. It ensures that any application behaves as intended with very low performance overhead. (For more Information, see Red Hat Enterprise Linux Security Series: SELinux)
VPNs	Red Hat provides native tools based on the IPsec protocol suite for setting up secure VPNs for network-to-network and "road warrior" communications. Also, specific applications can have their network communications encrypted by using stunnel, a TLS/SSL tunneling service. (For more information, see Red Hat Enterprise Linux Security Series: VPNs on Red Hat Enterprise Linux)
Audit	The Red Hat Auditing System allows users to gather wide-reaching data about Red Hat Enterprise Linux system operation and generate summary reports that help monitor and manage system and user behavior. (For more information, see Red Hat Enterprise Linux Security Series: The Audit System)



RED HAT NETWORK

Red Hat Network allows administrators to efficiently manage (perform patch management, updates, monitoring and maintenance) the systems on their networks via a simple user interface. The ability to manage multiple systems, verify configuration details, and quickly apply updates and patches minimizes risks of attacks. (For more information, see [HYPERLINK "http://rhn.redhat.com/help/about.pxt"](http://rhn.redhat.com/help/about.pxt)<http://rhn.redhat.com/help/about.pxt>)

Red Hat
Enterprise Linux
Updates and Patches

Red Hat releases software updates and patches that address bugs, provide enhancements, and remedy security vulnerabilities. The strength and responsiveness of the open source community and Red Hat's engineers ensures that all issues are resolved quickly. (For more information see <http://www.redhat.com/security/updates/>)

CERTIFICATION OF RED HAT TECHNOLOGIES

Red Hat Enterprise Linux meets stringent security expectations, and has achieved the following security certifications:

- Red Hat Enterprise Linux has achieved Common Criteria certification at Evaluation Assurance Level 4 (EAL4+) for Labeled Security Protection Profile (LSPP), Controlled Access Protection Profile (CAPP), and Role-Based Access Control Protection Profile (RBAC).
- JBoss Enterprise Application Platform 4.3 has achieved Common Criteria certification at Evaluation Assurance Level (EAL) 2+ (augmented for flaw remediation).
- Red Hat Enterprise Linux 5.2 is one of only four operating systems on the DISA Approved Products Lists for IPv6. This makes Red Hat Enterprise Linux one of only 4 operating systems with this certification.

These Red Hat technology certifications are backed by Red Hat specialists who have proven their advanced skills in using Red Hat Enterprise Linux. Security experts with up-to-date and hands-on experience with Red Hat's systems are available to help you meet your business challenges.



GLOSSARY OF ACRONYMS

AVC	Access Vector Cache	NSS	Name Service Switch
DCID 6/3	Directory of Central Intelligence Directive	PAM	Pluggable Authentication Modules
DISA STIG	Defense Information Systems Agency, Security Technical Implementation Guide	PCI-DSS	Payment Card Industry - Data Security Standard
FLASK	Flux Advanced Security Kernel	PSK	Pre Shared Key
IPA	Identity, Policy, Audit	RBAC	Role-Based Access Control
LDAP	Lightweight Directory Access Protocol	SLIDE	Eclipse-based IDE for police development
LSM	Linux Security Modules	SOX	Sarbanes-Oxley
MAC	Mandatory Access Control	SSSD	System Security Services Daemon
MCS	Multi-Category Security	TCB	Trusted Computing Base
MLS	Multi-Level Security	TCSEC	Trusted Computer System Evaluation Criteria (aka, Orange Book)
NISPOM	National Industrial Security Program Operating Manual		

HYPERLINK "<http://www.niap-ccevs.org/cc-scheme/st/vid10165/>"www.niap-ccevs.org/cc-scheme/st/vid10165/

HYPERLINK "<http://www.commoncriteriportal.org/>"www.commoncriteriportal.org

HYPERLINK "<http://www.redhat.com/certification/rhcss/>"www.redhat.com/certification/rhcss/



RED HAT SALES AND INQUIRIES

NORTH AMERICA

1-888-REDHAT1

www.redhat.com

ASIA PACIFIC

+65 6490 4200

www.apac.redhat.com

apac@redhat.com

EUROPE, MIDDLE EAST AND AFRICA

00800 7334 2835

www.europe.redhat.com

europe@redhat.com

LATIN AMERICA

+54 11 4341 6200

www.latam.redhat.com

info-latam@redhat.com