



# **SECURITY** **BLANKET**

BY TCS  
TM

**The Operating System Lock  
Down Solution for Linux**

# The Challenge: Meeting Organizational Security Requirements

## Linux Operating System Security

Operating system (OS) security is a priority for System Administrators and most agree that it is not an easy process. It can be a time consuming and difficult process that varies from OS to OS. Security Blanket™ from Trusted Computer Solutions (TCS) is an easy-to-use, flexible tool that helps System Administrators securely configure Red Hat® Enterprise Linux® (RHEL), CentOS, and Oracle® Enterprise Linux (OEL) versions 4 and 5 operating systems—a process known as system lock down or system hardening—while saving time, money, and frustration.

## The Importance of System Lock Down

Research shows that System Administrators agree; staying ahead of the OS security game comes down to three sets of practices that really work: server hygiene, server patching, and access control. Server hygiene is directly related to hardening and standardizing servers using a security policy or guidelines, such as those defined by the Center for Internet Security (CIS), the SANS (SysAdmin, Audit, Network, Security)<sup>1</sup> Institute, and the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). In addition to adhering to policy, the server's security configuration must provide the desired up time and stability needed for applications and users. Locking down an OS to ensure security without reducing functionality for users and applications can be time consuming and expensive. As a result, security configuration is often overlooked so that installations and implementations can stay on schedule.

*“Many of the vulnerabilities we identify are because the operating systems are not securely configured. Usually, vendors set their operating system configurations in the least secure manner in order to facilitate installation and implementation.”*

- “Q&A: Federal Information Security Isn't Just About FISMA Compliance, Auditor Says,” by Jaikumar Vijayan, *ComputerWorld*, June 14, 2007

## The System Lock Down Dilemma

According to Forrester Research, only 45% of IT organizations secure all of their systems and 26% do not secure all of their Internet-facing servers.<sup>2</sup> Additionally, half of the Linux® servers in use today are manually locked down—a process that is time consuming and prone to human error. As indicated in the table below, System Administrators are using a variety of costly, time consuming, and inadequate means to lock down their Linux servers.

Server Lock Down Methods			
Method	Cost	Productivity	Ease-of-Use
Hire consulting	Expensive	Need to manage the process	Yes
Attend training	Expensive	Manual cross-reference to security policy or guidelines; prone to error; time consuming	No
Manual configuration	Time	Manual cross-reference to security policy or guidelines; prone to error; time consuming	No
Rely on complex lock down scripts	Time	Manual cross-reference to security policy or guidelines; time consuming	No
Open source lock down tools	Free	Partially meets guidelines; tracking updates required	No
Do nothing	Inexpensive	Ineffective and highly vulnerable	Yes

Typical server lock down methods.

<sup>1</sup> <http://www.sans.org/top20>

<sup>2</sup> Forrester Research, “State of Server Operating System Security 2007: Admins Patch an Average of Eight Days Late,” June 2007

# The Solution: Quick, Automated Lock Down with Security Blanket

## An Intuitive Graphical Users Interface Makes It Faster and Easier

Security Blanket is a software tool that automatically assesses and locks down your system. It also allows quick “undo” for actions that compromise system functionality. Security Blanket is easy to use with an intuitive graphical user interface, or a pure command line interface, enabling the System Administrator to perform security assessments and security configurations through scan, apply, and undo activities. Assessment and baseline reporting allow the System Administrator to capture a server’s security state and compare an earlier baseline with the current security state, providing valuable compliancy information.

Below are scan results. The failures are related to Security Blanket modules, which comprise multiple guidelines. For example, one Security Blanket module might address four STIG guidelines and two CIS guidelines.

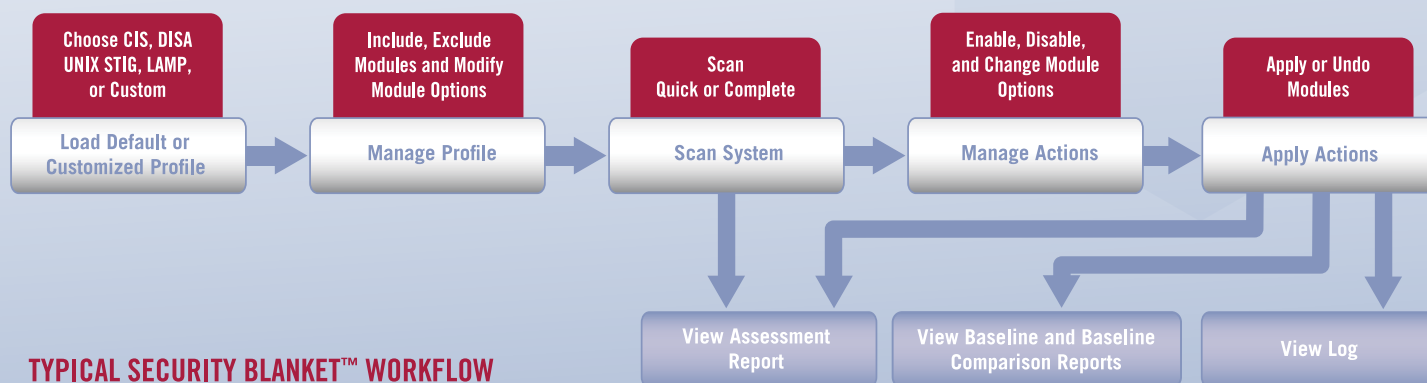
Scan Results (Complete)					
Profile	Time (secs)	Pass	N/A <sup>3</sup>	Failed	Total
CIS	41	31	15	62	108
DISA UNIX STIG	43	52	24	89	165

Total Available Modules to Users: 173

Severity Breakdown of Failed Modules				
Profile	Medium	High	Severe	Total
CIS	39	15	8	62
DISA UNIX STIG	59	17	13	89

These benchmark results were run on a RHEL5 OS installed “out of the box.”  
Proving ease of installation is a trade off with security.

Security Blanket supports a compliancy model that includes both assessment and remediation. The product was designed to meet the challenge of giving System Administrator’s an automated tool that provides compliancy to the lock down guidelines defined by the DISA UNIX STIGs, CIS, and the SANS<sup>4</sup> Institute’s Top 20 guidelines for ensuring certain configurations such as Linux, Apache, MySQL, and PHP (LAMP). Additionally, Security Blanket aids in providing required security controls to support Federal Information Security Management Act (FISMA) guidelines.



### TYPICAL SECURITY BLANKET™ WORKFLOW

Security Blanket workflow is flexible and easy to navigate.

<sup>3</sup> The N/A notation refers to DISA UNIX STIG security requirements that cannot be addressed by a software solution. The Security Blanket User’s Guide clearly documents the STIGs that cannot be addressed by this product and why they cannot be addressed.

<sup>4</sup> <http://www.sans.org/top20>

## Best-of-Breed Industry Guidelines for Security

Security Blanket was designed to adhere to the industry's best-of-breed security lock down guidelines.

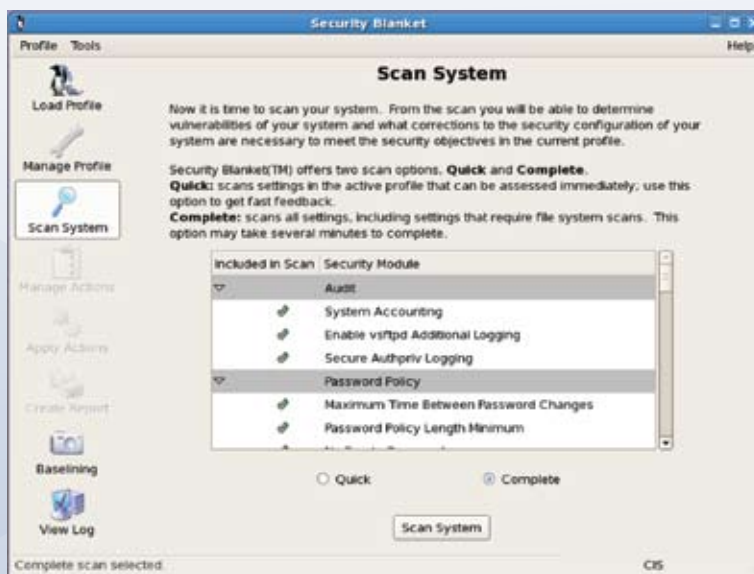


Security Blanket has undergone evaluation and received certification by CIS for the Red Hat Enterprise Linux benchmark. Security Blanket provides full DISA UNIX STIG compliancy and contains a LAMP profile based on the SANS<sup>5</sup> Institute's defined risks associated with using PHP; the CIS Linux and MySQL benchmarks; and the DISA UNIX STIGs.

### System Assessment

A System Administrator can choose a pre-defined profile that meets the security requirements of CIS, DISA UNIX STIGs, and SANS<sup>5</sup> guidelines, or can customize one of these profiles by selecting or deselecting modules. System Administrators can apply actions as an entire profile, a subset of a profile, or individual security modules.

Administrators have a choice between a quick scan and a complete scan. The difference is that the complete scan includes file system scans. Performance for both scans is well within reasonable time expectations.



The System Administrator can deselect any security module from the scan process.

*“Very interesting product. I utilize open source for a lot of Community Bank’s Credit Unions—this tool will certainly help quickly harden the boxes before production use.”*

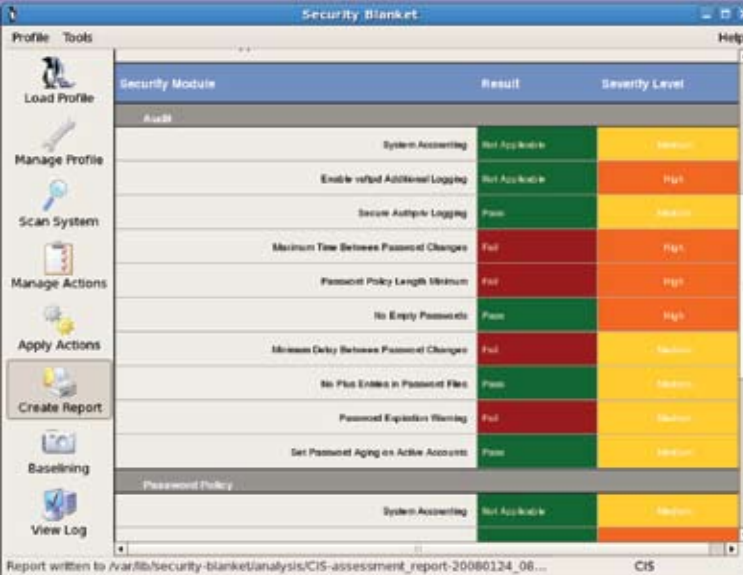
-TCS Security Blanket Client

<sup>5</sup> <http://www.sans.org/top20>

## Remediation

The Assessment Report provides conformance indicators that show how the system matches up against the security guidelines in the profile. The Administrator can choose to correct all conformance issues or bypass certain corrections in meeting the needs of the particular system installation or security policy.

Modules address specific security requirements found in industry guidelines. Online documentation includes cross-references from a specific requirement in an industry guideline to the applicable Security Blanket module.



Security Module	Result	Severity Level
<b>Audit</b>		
System Accounting	Not Applicable	Medium
Enable verbose Additional Logging	Not Applicable	High
Secure Auditfile Logging	Pass	Medium
Maximum Time Between Password Changes	Fail	High
Password Policy Length Minimum	Fail	High
No Empty Passwords	Pass	High
Minimum Delay Between Password Changes	Fail	Medium
No Plus Entries in Password File	Pass	Medium
Password Expiration Warning	Fail	Medium
Set Password Aging on Active Accounts	Pass	Medium
<b>Password Policy</b>		
System Accounting	Not Applicable	Medium

System Administrators can easily and quickly see how this server complied with the designated security modules.

## Security Blanket Benefits

**Easy to use assessment and remediation tool.** Security Blanket offers an intuitive graphical user interface (or pure command line interface) to run system scans (assessments) and then automatically apply actions to configure the OS.

**Easy-to-manage security profiles.** Security modules make up a security profile and the intuitive interface allows for loading and managing security profiles. Predefined security profiles are provided in the standard application. If your organization requires specific security policy guidelines; enabling modules, disabling modules, or changing module parameters, profiles can be customized.

**Clear and concise descriptions and tips are provided for every security module.** Additionally, Security Blanket provides a cross-reference between modules to the guidelines it satisfies. This cross-reference can be invaluable when a System Administrator requires data for a security audit.

**Easy-to-manage actions for remediation.** Security modules can be selected or deselected within a profile to manage what will be configured during remediation.

**Automatic lock down.** The System Administrator can click “Apply” or execute the apply command to configure the OS with the chosen profile. Additionally, an automated undo capability can be selected for specific modules, or an entire profile, to return to the previous system state.

**Low price point.** Security Blanket is priced on a single server license model with a low price point that enables IT shops with only a few Linux servers to take advantage of the product’s functionality in an affordable way. IT shops with a larger number of Linux servers can contact TCS for quantity discounts.

## Reporting and Logging

- An Assessment Report provides “pass,” “fail,” and “not applicable” status for every module in the selected profile. The Assessment Report also indicates the severity level of the module’s impact on the security state of the system.
- Detailed logging of scanning and system changes include data such as each file’s previous permissions and the permissions Security Blanket set when actions were applied.
- Baseline reporting captures the state of the system at a point in time. The baseline reporting feature includes the ability to compare current system states to past states and identify changes in hardware, networks, files, and software. The Baseline Report functionality and content was designed to meet the DISA Field Security Office recommendation for routine confirmation of a system baseline.
- Reports are generated in XML format allowing System Administrators to create customized reports.



Baseline reporting allows for the comparison of the current system state.

## Security Blanket Operational Characteristics

Security Blanket is designed for minimal operational and hardware intrusion, and sensitivity to an administrator’s needs when deploying new Linux OS distributions:

- A small disk footprint (<2MB) and lightweight memory usage.
- The only additional software required is the Python bindings to the XSLT system library for reporting.
- Supports Red Hat Enterprise Linux versions 4 and 5 and the open source counterparts, CentOS 4 and 5, as well as Oracle Enterprise Linux 4 and 5.
- Supports both 32 bit and 64 bit architectures.
- No outside connectivity is required.
- Administrator’s choice of full GUI or pure command line interface.
- Runs only when initiated. It is not required for Security Blanket to be running all the time.
- Batch jobs can be run to periodically scan, report, and apply.
- Security Blanket User’s Guide and module documentation are integrated with the Red Hat online help system. The documentation is also available in PDF format from the Security Blanket website.

## About Trusted Computer Solutions, Inc.

Founded in 1994, Trusted Computer Solutions (TCS) provides commercial and government organizations with solutions for securely sharing and protecting critical information assets. TCS has deep experience in developing solutions to support the Linux community. The company's flagship commercial product, Security Blanket, provides Linux users with an automated software tool that allows users to easily lock down an installed Linux operating system and periodically check the system security. TCS has over thirteen years of experience in building security solutions that meet the most stringent security conformance requirements as mandated by the Federal government. TCS is headquartered in Herndon, VA, with offices in Urbana, IL and San Antonio, TX. For more information, visit [www.TrustedCS.com](http://www.TrustedCS.com).

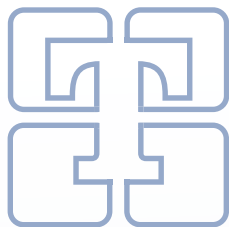


*"Did a brief evaluation of your product and I liked what I saw. The description of the Modules, the ease of use of the tool—I just thought it was very good."*

-TCS Security Blanket Client

[www.TrustedCS.com/securityblanket](http://www.TrustedCS.com/securityblanket)





**TCS Corporate Office**

2350 Corporate Park Drive, Suite 500  
Herndon, VA 20171  
1-866-230-1307

**TCS Trusted Operating Systems Lab**

2021 S. First St, Suite 207  
Champaign, IL 61820  
217.384.0028

**TCS Texas Office**

10010 San Pedro, Suite 220  
San Antonio, TX 78216  
210.340.3151

Security Blanket is a trademark of Trusted Computer Solutions, Inc. Linux is a registered trademark of Linus Torvalds.  
All other trademarks and registered trademarks are the property of their respective owners.