Manual operating system (OS) hardening, or lock down, is still the most common method for securing systems. In fact, 53% of System Administrators are still securing systems manually\(^1\). The action of manually locking down systems is typically performed by writing lines of code, or scripts, to run on each system. Manually locking down a single machine can take hours, if not days, to complete. Multiply that time by the number of systems in your organization, and locking down the entire enterprise can take a significant amount of time that System Administrators could use to perform more mission critical tasks.

Once all the systems in your enterprise have been hardened, they must also be maintained according to the security policies set by your organization, which can change over time. That means interpreting new guidelines, developing or editing scripts, and then re-hardening those systems. The bottom line: considerable time spent maintaining a hardened security state.

As much as 42% of System Administrators’ time is spent writing programs and scripts to automate such tasks\(^2\).

Not all systems require the same levels of security. There could be different security needs based on the business use of each machine. For instance, government agencies and many corporate organizations require systems to be hardened using the Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide (STIG). Servers that handle credit card transaction information may require following the Payment Card Industry Data Security Standards (PCI DSS) guidelines. Keeping up with the many different published security guidelines as they are updated and maintaining your systems over their life span can be a full-time job for System Administrators. Shouldn’t they be focused on more productive tasks such as troubleshooting IT service requests, adding new applications and users, and managing asset inventory?

---

1 Survey from Large Installation System Administrator (LISA) conference, 2010
2 Survey from Large Installation System Administrator (LISA) conference, 2010
Security Blanket, by Raytheon Cyber Products, is an automated OS hardening tool which enables System Administrators to quickly and consistently lock down Linux® and Solaris® OSs. Whether the OS is on bare metal hardware or implemented as a virtual instance, Security Blanket can lock it down in minutes. For convenience and to ensure consistency, systems can be grouped together by the required security policy. The policy can then be applied to all systems in the group at the same time. Managing systems in groups allows for assessments, baselines, and reporting to be performed quickly and effortlessly.

**Consistency and Predictability**

The Administration Console makes it easy to configure systems into groups with identical security lock down requirements. The ability to apply security policy to groups of servers is critical for ensuring consistency within the organization. As new systems are added to the group, or as policies change, apply the designated security policy to the whole group, with one click. Regularly assessing the security posture of the group provides verification that systems are being secured appropriately and within prescribed change management guidelines. It is easy to identify when systems vary from expected results.

**Minimal Impact on Network and Personnel Resources**

Security Blanket was developed to minimally impact hardware implementations and simplify deployment of new OS distributions.

- Console-to-client communications using Simple Object Access Protocol (SOAP) messages using HTTP over Transport Layer Security (TLS) for secure and encrypted communications
- IPv4 and IPv6 simultaneous network support
- 32- and 64-bit architecture support

**Intuitive Interface**

Security Blanket employs an intuitive user interface for managing OSs. Little to no training is necessary to effectively lock down your enterprise. Personnel with no Linux or Solaris expertise can secure new OSs as they are added to your environment.

**Not Just a Hardening Tool**

Although Security Blanket was primarily developed to automate the manual process of hardening OSs, it has evolved to do so much more. System Administrators can perform various assessment, hardening, baseline and reporting functions with a single click.

**Scan** - Assess system configurations against prescribed security profiles and report results using “pass/fail/not applicable” indicators for each security module.

**Apply** – Automatically configure the OS to meet the selected hardening guideline creating a state of lock down or compliance.

**Undo** – Automatically reverse the most recent configuration performed, restoring the OS to the prior system configuration.

**Baseline** – Take a snapshot of the system configuration at a given point in time. Providing a baseline is often required by security auditors and is highly recommended in many of the industry standard OS security guidelines.

**Scheduling** – Pre-set automatic lock down actions or report generation for off-peak times, or regularly scheduled days to alleviate System Administrators from having to perform these functions during their standard working hours.

**Reporting That Ensures Audit Compliance**

It is no longer enough to just secure your OS. You also need proof that systems are successfully locked down and remain secure. This evidence is easily created using the robust reporting capabilities within Security Blanket.

Reports are delivered in a variety of formats to include PDF, HTML, text, and CSV (for importing into spreadsheets). Additionally, since reports are generated using Extensible Markup Language (XML), System Administrators can customize reports by writing their own XSLT (Extensible Stylesheet Language Transformations) stylesheet or import the report data into existing reporting tools.

**Assessment Reports** - The Assessment Report displays the results of a scan and can be run against individual servers or a group of servers. The report displays a result for each module with a “pass” or “fail” indicator.

**Baseline and Baseline Comparison Reports** - Baseline Reports capture a snapshot of a client’s system configuration. The Baseline Comparison Report compares the current system state to a prior Baseline Report and identifies changes in hardware, files, software, and network access configurations.

**Detailed Logging** - All actions performed by individual clients, or by the Administration Console are logged for any detailed analysis that may be needed. Client logs provide insight as to exactly how the OS is being configured. Logging can identify previous file permissions and the permissions set when lock down actions were applied. Console logging tracks all actions performed by the Administration Console which provides accountability for updates and changes to OS configurations.

**Profile Comparison Report** - The Profile Comparison Report provides the ability to view and compare two security profiles. This capability greatly assists with the evaluation process when deciding which profiles are most applicable to your organization. It also helps in developing custom profiles to meet organizational security objectives.
Apply and Undo Reports -
The Apply and Undo Reports display the successful completion of each function (apply or undo) at each security module level.

Comprehensive Documentation
The Security Blanket Administration Guide and the Security Blanket Modules Guide are extensive documents inherent in the product. The Administration guide provides detailed information about Security Blanket, the installation process, and user information. The Modules guide provides descriptions for each security module, the location of the configuration setting for each OS, and any configuration change that will be invoked when applied. It also provides a valuable cross reference to each pre-defined security profile.

Published Guidelines
Security guidelines have been developed by industry leaders using their extensive knowledge and research regarding the best practices for securing OSs. The adoption of these best practices, throughout government and industry, is becoming more prevalent, and even mandated, as security breaches and data leaks increase. Evaluating, interpreting, and implementing these guidelines can be a confusing and cumbersome endeavor. Using these industry guidelines as a reference, Security Blanket has developed security profiles that are compatible with the suggested lock down technical controls. Profiles are a compilation of individual technical controls and settings, known as modules. Additionally, Security Blanket provides the capability to customize guidelines for your organization using any security profiles as a starting template, or allows you to build your own security profile from scratch using a combination of security modules from the database. As security guidelines are updated, modules and profiles are evaluated for necessary changes and updated accordingly. Updated profiles are available to all customers with active maintenance agreements.

Security Blanket and SELinux Support
Security Blanket supports the most commonly deployed versions of Linux and Solaris OSs as well as Red Hat® Enterprise Linux® default SELinux policy known as “targeted”. Security Blanket locks down non-SELinux OSs as well as those which have SELinux disabled. When SELinux is enabled and using the targeted policy, both the “enforcing” and “permissive” modes are supported. Security Blanket is proactively updated following any new OS release and offered to clients with current maintenance agreements for no additional cost.

Operational Management
Role Based Access Control (RBAC) is incorporated to ensure that users perform operations that are appropriate for their specific roles. For example, System Administrators with responsibility for lock down and policy assurance may have a higher level functional authority than Security Officers who may only need access to reports.

Integration for Enhanced Functionality
Security Blanket provides the ability to communicate with external third-party applications through a variety of protocols. Its comprehensive Baseline Report contains key system information valuable to applications such as patch management, configuration management, and inventory management. It utilizes a plug-in architecture to allow the simple addition of new protocols and interfaces to communicate with

### Supported Operating Systems Include:
- Red Hat Enterprise Linux v4, 5, and 6; includes v5 for IBM® System z®
- CentOS v4, 5, and 6
- Oracle® Enterprise Linux (OEL) v4, 5, and 6
- Solaris™ 10
- Novell® SUSE® Linux and openSUSE Linux 10 and 11; includes SUSE 10 and 11 for IBM System z
- Fedora™ 10, 11, 12, and 13

### Security Industry Leader/Author | Referenced Guideline
--- | ---
Department of Homeland Security (DHS) | DHS Linux Configuration Guidance
Director of Central Intelligence Directive (DCID) 6/3 | DCID 6/3
National Industrial Security Program (NISP) | National Industrial Security Program Operating Manual (NISPOM), Chapter 8
Payment Card Industry (PCI) | Data Security Standard (DSS)
SANS Institute | Top 20 Security Risks as related to Linux, Apache™, My SQL, and PHP (LAMP) and Solaris, Apache, MySQL and PHP (SAMP)
SANS Institute | Consensus Audit Guidelines (CAG) Top 20 Critical Controls
National Security Agency (NSA) | NSA Guide - Guide to the Configuration of Red Hat Enterprise Linux 5

Figure 2: Industry Guidelines Referenced in Security Blanket
applications. For example, an email plug-in supports the generation of email notifications following completion of key events.

**Platform Options**

Security Blanket supports the x86 (32- and 64-bit) Red Hat Enterprise Linux v4/5/6 (and CentOS/Oracle equivalents), Novell SUSE Linux v10/11, openSUSE v10/11, and Fedora v10/11/12/13 distributions. Red Hat Enterprise Linux v/5/6 and SUSE v10/11 are also supported on the IBM System z mainframe. Solaris 10 is supported on both x86 and SPARC® platforms. Implementations can run natively or as virtual machines within most hypervisor environments.

**What Our Customers Are Saying**

“I was able to lock down all 18 of my classified servers in one day. Prior to using Security Blanket, locking down one server would have taken an entire week. Now that I am using this tool, I have more time to focus on mission-critical tasks and projects.”

**Principal Field Support Engineer, National Test Range**

“The product efficiently does exactly what it says it does. It provides an assessment to tell you what is non-compliant on a server and then automatically fixes it so that the server is compliant.”

**Keith Arthur, Technical Team Lead, Unique Communication Solutions**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“I was able to lock down all 18 of my classified servers in one day. Prior to using Security Blanket, locking down one server would have taken an entire week. Now that I am using this tool, I have more time to focus on mission-critical tasks and projects.”

**Principal Field Support Engineer, National Test Range**

“The product efficiently does exactly what it says it does. It provides an assessment to tell you what is non-compliant on a server and then automatically fixes it so that the server is compliant.”

**Keith Arthur, Technical Team Lead, Unique Communication Solutions**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“I was able to lock down all 18 of my classified servers in one day. Prior to using Security Blanket, locking down one server would have taken an entire week. Now that I am using this tool, I have more time to focus on mission-critical tasks and projects.”

**Principal Field Support Engineer, National Test Range**

“The product efficiently does exactly what it says it does. It provides an assessment to tell you what is non-compliant on a server and then automatically fixes it so that the server is compliant.”

**Keith Arthur, Technical Team Lead, Unique Communication Solutions**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**

“I was able to lock down all 18 of my classified servers in one day. Prior to using Security Blanket, locking down one server would have taken an entire week. Now that I am using this tool, I have more time to focus on mission-critical tasks and projects.”

**Principal Field Support Engineer, National Test Range**

“The product efficiently does exactly what it says it does. It provides an assessment to tell you what is non-compliant on a server and then automatically fixes it so that the server is compliant.”

**Keith Arthur, Technical Team Lead, Unique Communication Solutions**

“We estimate that we have been able to save 40-60 hours in the development of the initial security configuration that we use for all of our Linux systems. With each new system deployment, we are saving between 4-6 hours per system. The time savings alone is a huge benefit, but knowing that our systems are DISA STIG compliant is especially beneficial for our clients.”

**Larry Pakieser, Chief Operating Officer, GBprotect**