



hp data sheet

hp Safeguard software enhanced asset protection for NonStop servers

features at a glance

- Authentication, authorization, and auditing
- Application, data, and device protection
- Fine-grained subject/object access control
- Open architecture
- Partner extensions

Although Internet attacks get the most press, the majority of security breaches actually come from insiders who already have access to your systems, according to a study by Ernst and Young. To address this problem, security experts recommend that only the minimum required access be granted to authenticated users to help minimize insider data theft.

HP Safeguard security management software, running on the HP NonStop platform, implements a fine-grained subject/object access control mechanism that allows you to more tightly control access to NonStop system resources. Users can establish and maintain a chosen level of protection for their own data, or you can limit the use of protection to your security administrators. With Safeguard software, you can establish control selectively—without impeding application or user productivity—through authentication, authorization, and auditing.



authentication

Safeguard software complements and extends the native security features of the NonStop system. Although the NonStop system also authenticates requests for entry into the system, Safeguard software adds advanced support for UNIX® type user names, account expiration, temporary access suspension and restoration, password history, minimum password length, password change intervals, and automatic user account suspension after excessive logon failures.



You can configure Safeguard software to help reduce help desk calls by issuing a warning to users when their password expiration date approaches, and by extending a post-expiration grace period to users. The authentication service lets users conveniently change passwords during logon and provides information to help them determine if their passwords have been compromised.

authorization

Safeguard software can improve server availability by reserving resources for critical production applications, ensuring that application servers are accessed only by authorized clients, and protecting critical data from unauthorized or accidental modification. Authorized users can exercise control over objects such as disk files; disk volumes and subvolumes; devices such as printers, tape drives, connected PCs, and communications lines; and even client/server interprocess communications.

You establish the protection of an object by creating one or more access control lists (ACLs) for it. An ACL contains subjects or groups of subjects (users) and the access they are permitted to the object. Access authorities are read, write, execute, create, purge, or owner. ACLs also can explicitly deny access to designated

individuals and groups. Safeguard software allows different authorization privileges to be assigned to the same user, depending on whether the user is connected locally or remotely. This model ensures that users are given only the minimal access required.

auditing

In addition to reporting logon attempts, Safeguard software audits access to objects and changes to the security settings for those objects. Auditing features allow your security administrators to

- Detect unauthorized system access
- Detect unauthorized security setting changes
- Discourage users from abusing their authorized power
- Verify that policies are being followed

Security administrators can specify the objects and the types of access to be audited. The security administrator decides how much or how little system activity will be recorded for later review.

Safeguard software can be configured to log each attempt to access an object, as well as logging the initiation of communications between client/server application processes. Each audit record includes such information as the object name, date and time of the access attempt, the user account, and whether the attempt was authorized or denied. When initiating or altering Safeguard protection, you can use a warning-only mode so that production applications are not negatively affected.

Safeguard software also logs changes made to an object's ACLs. This record can be reviewed by management and auditors to verify that security administrator activity conforms to established management policies.



availability and manageability

Safeguard software provides an extra level of server availability by preventing intentional or accidental modification of critical NonStop system files, application databases, and programs by disgruntled employees or other insiders. It can enforce operational policies that reserve process names for specific production applications, preventing unauthorized users and test programs from accessing them.

open architecture

Safeguard software has a rich set of documented application program interfaces (APIs) available to security administrators. These APIs allow you to customize the software according to your needs and enable you to improve administrative productivity by simplifying complex and repetitive tasks.

security partners

There are dozens of HP partner enhancements available for Safeguard software. Customers can take advantage of valuable off-the-shelf features such as single sign-on; support for RSA SecureID tokens; graphical interfaces; enhanced logging and reporting; limiting authorization to specific times, locations, and access devices; and granularity to the individual command level of system utilities. Frequent interaction with these partners allows HP to understand what new APIs should be made available to increase the functionality of Safeguard software. For more information on HP security partners and their offerings, visit nonstop.compaq.com/security and select Safeguard Software.

ordering information

product ID	description
9750	Safeguard software

specifications

system requirements	
hardware	Any NonStop server (some features may be available only on NonStop S-series servers)
software	NonStop Kernel operating system, any supported software release



For more information, go to www.hp.com/go/nonstop.

March 2003, first published May 2001. UNIX is a registered trademark of The Open Group. All other product names mentioned herein may be trademarks of their respective companies. HP shall not be liable for technical or editorial errors or omissions contained herein. The information is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

5981-6166EN

©2003 Hewlett-Packard Development Company, L.P.