Powered by
NAVER CLOUD PLATFORM

HIWARE PAM

HIWARE Privileged Access Management for System

Do you have an accident caused by someone else's change of system settings?

HIWARE enables the complete management and supervision of users by controlling all accesses and operations monitoring work details in real-time and saving log records.

Have you ever forgotten your system ID's password?

HIWARE centrally manages passwords of IT infrastructure systems and enhances security through password policies.

AS-IS

- Weak of authentication / authority
- Indiscriminate server connection
- User fault
- Poor monitoring

Inadequate prevention

- Unable to trace the cause of the accident
- Cost for recovery
- Compliance violation
- Fall in brand value

Without customer service

TO-BE

- Strengthen user authentication
- Access authority management
- Command control
- Real-time control and monitoring

Precaution

- Analysis cause of accident and response
- Manage task record / log
- Deal with compliance
- Improved external reliability

With customer service

PCI-DSS COMPLIANCE

- Limit access to system components and cardholder data to only those individuals whose job requires such access.
  - Define access needs for each role, including
  - Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
  - Assign access based on individual personnel's job classification and function.
  - Require documented approval by authorized parties specifying required privileges.

- Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
  - Coverage of all system components
  - Assignment of privileges to individuals based on job classification and function

- Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.
  - Assign all users a unique ID before allowing them to access system components or cardholder data.
  - Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
  - Immediately revoke access for any terminated users.
  - Remove/disable inactive user accounts within 90 days.
  - Manage IDs used by third parties to access, support, or maintain system components via remote access.
  - Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
  - If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

- In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users.

- Implement two-factor authentication for all remote network access that originates from outside the network, by employees, administrators, and third parties including vendor access for support or maintenance.

- Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.

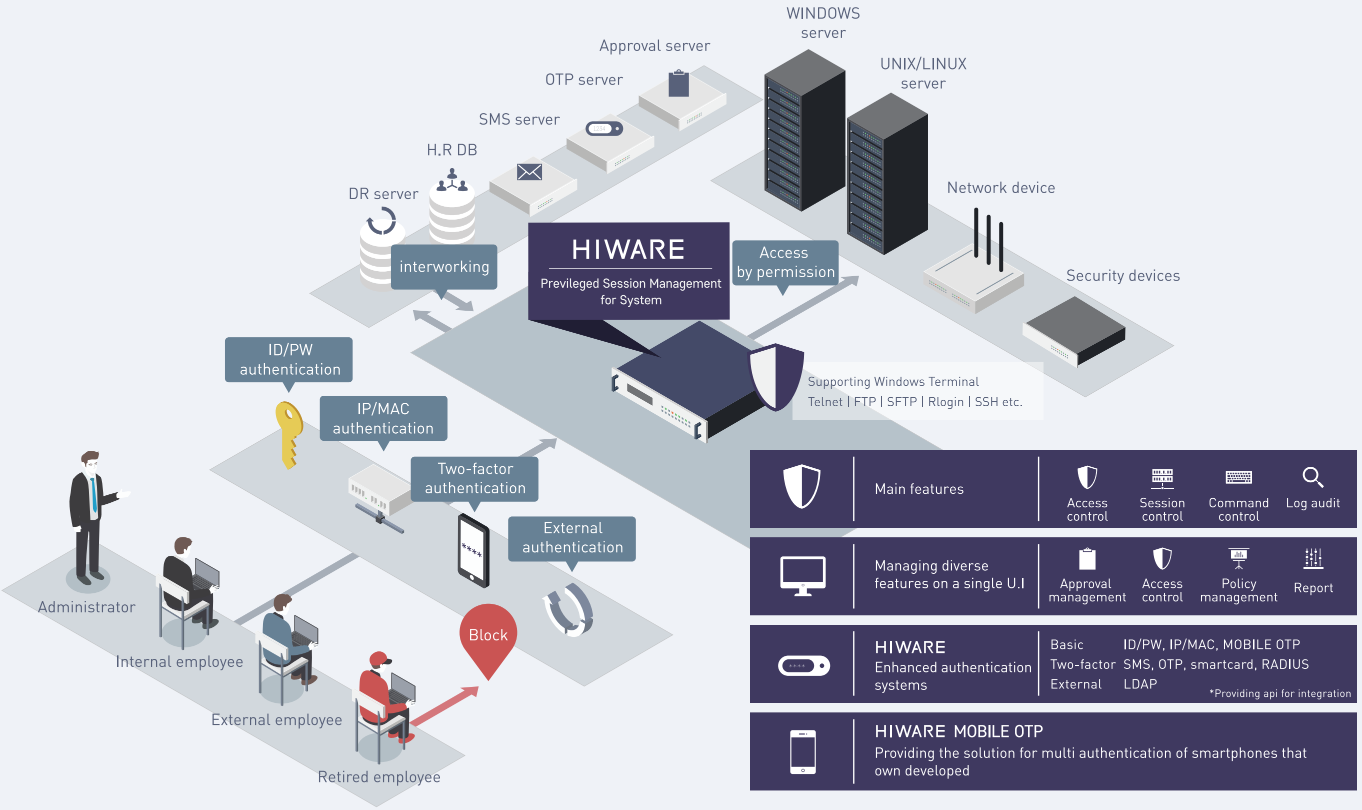
- All access to any database containing cardholder data must be restricted (PSM for Database)

Powered by

NAVER
CLOUD
PLATFORM

HIWARE PAM

HIWARE Privileged Access Management for System



Supporting Windows Terminal
Telnet | FTP | SFTP | Rlogin | SSH etc.

Main features	Access control	Session control	Command control	Log audit
Managing diverse features on a single U.I	Approval management	Access control	Policy management	Report

HIWARE
Enhanced authentication systems

Basic	ID/PW, IP/MAC, MOBILE OTP
Two-factor	SMS, OTP, smartcard, RADIUS
External	LDAP

*Providing api for integration

HIWARE MOBILE OTP
Providing the solution for multi authentication of smartphones that own developed

Task log record / audit

- Detailed task audit log
- Statics by user/equipment/command
- Various audit report
- Image logging for the GUI environment

Enhanced user authentication

- Block unregistered IP/MAC access
- Support various authentication API (OTP, LDAP, ARS, SMS, etc)
- Support mobile OTP

Access control

- Control central access authority (IP, MAC, 2-factor authentication)
- Centralize all remote access
- Support various protocols (Telnet, SSH, FTP, SFTP, RDP, etc.)
- Access control alarm and automatic access blocking unauthorized user

Command control

- Command control (White-list/Black-list)
- Manage command audit/notification
- Block session when using dangerous command
- Manage all used commands

Real-time session control

- Dashboard of real-time session/statics
- Real-time monitoring for session
- Block illegal user session
- Idle session timeout

Tel : +82-(0)70-8672-8155 | **Email :** shhan@s2lab.co.kr

www.s2lab.co.kr/hiware