H www.lsware.com B blog.lsware.co.kr

Integrated Modular Server Security and Management Solution

Omniguard

GS 1grade

KONEPS

UPV Account Mgmt. Solution

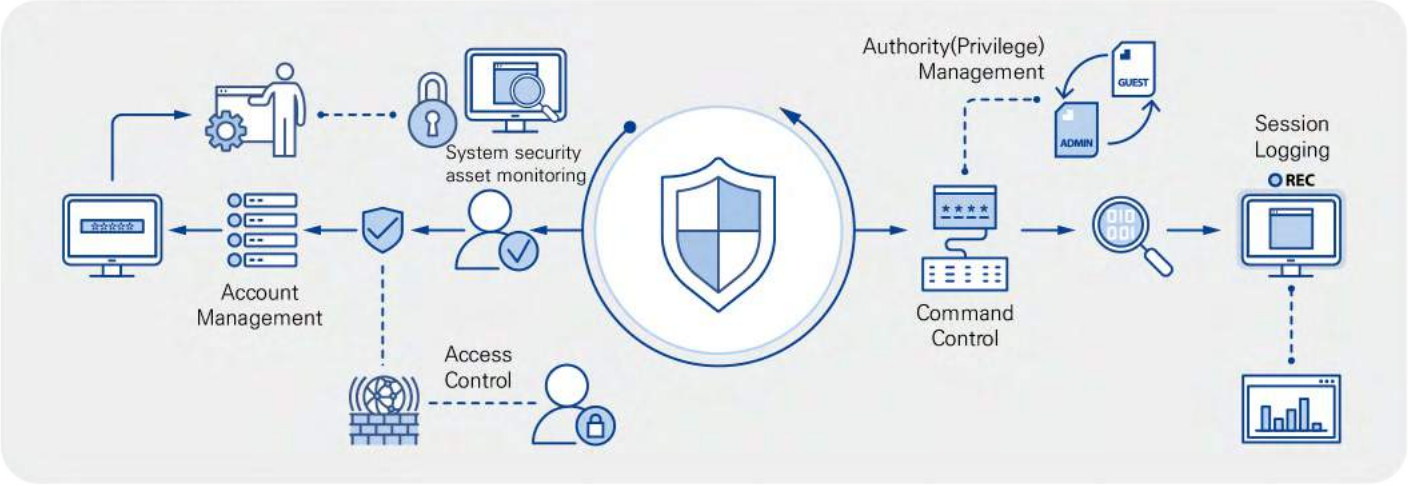
UAC Access Control Solution

UCC Authority Mgmt. & Audit Trail Solution

USAM System Security Asset Monitoring Solution

Omniguard, our next-generation server security solution, provides guaranteed stability as well as various functions, such as account management, access control, session logging, authority management, command control, and system security asset monitoring for each module. Not only that, but it also provides convenience for selective builds while minimizing the impact on the OS and limiting the impact on the system with zero kernel modifications.

Omniguard operation process



Overview

Breach of Internal Confidential Information and Increase in Various Attacks

- The need to secure the traceability for accountability in terms of security arises due to the account sharing
- It is necessary to control behaviors that undermine the integrity of key system information or data
- Contemplating about company-wide countermeasures for system access
- It is needed to establish countermeasures for each system

Growing Management Tasks and Costs

- Increase in the variety of servers and subjects to be managed
- Growing demand for rapid resolution on the password and resource-related issues
- Increasing importance of security asset status management in the system

Increased Need for Efficient Account and Authority Management

- The workload increases when managing and changing passwords due to the manual account management
- It is difficult to check the status of account use and account security policies
- The risk of security incidents rises due to unauthorized access to the system by users or illegal command input.
- It is difficult to identify the cause in case of a failure or an incident due to scattered logs of sessions

Needs for Compliance with Legal and Regulatory Requirements and Respond to Audits

- Technical and Administrative Personal Information Safeguard and Security Standard
- Regulation on Supervision of Electronic Financial Transactions
- Personal Information & Information Security Management System(ISMS-P)

LSware

LSware Inc. 18th floor, Daeseong D-polis Building A, 606, Seobusaet-gil, Geumcheon-gu, Seoul, Republic of Korea, 08504
TEL +82-2-6919-0321 FAX +82-2-6919-0329

Expected Benefits from Omniguard

Key Features of Omniguard

Central Management

- Integrated management of heterogeneous servers
- Batch application and monitoring of system account policies
- Providing a single web console

Account Management

- Providing the creation, change, and deletion of heterogeneous server accounts
- Password policy management
- Unlocking locked accounts
- Applying a batch security policy to the accounts subject to management

Session Logging

- User Session Screen Logging /Save session screen in playable format
- Windows: FTP/TELNET connection logging, remote terminal session logging
- UNIX/Linux: Telnet/SSH/xterm/SU/Console connection logging
- Providing the status of sessions accessed by users

Access Control

- Service (Telnet, FTP, rexec, ssh, rlogin, CDE, etc.) access control (by user/group)
- Remote terminal and port access control (by IP/user/group)
- OTP authentication support when accessing the system
- Distributing access authority according to the policy

Command Control

- Controlling violation commands in various service environments
- Providing various blocking methods when a violation command is entered (session blocking, command cancellation, message output)
- Setting the command control policy(by user/group)

Authority (Privilege) Management

- Account authority delegation(User/Group)
- Record usage history for delegated privileges

System security asset monitor

- Monitors forgery and tampering of files and registry changes
- Network service status monitoring
- Monitoring server operating environment software installation information

Mapping for Core Elements, Laws, and Guidelines

Core Elements	Key Certification Guidelines
Information Security Management System (ISMS)	• Including control items in Article 19-10 (Access Control), such as limiting the number of failed logins/access user authentication/password complexity in items such as user authentication, password management, user registration, and authorization
Personal Information Security Management System (PIMS)	• Article 8 (Technical Protection Measures) In consideration of legal requirements and external threat factors, the password management procedures for personal information handlers, users, and information principals (users) shall be established and implemented. Accounts and authorities (privileges) granted to the personal information and personal information processing systems for special purposes shall be identified and separately controlled.
Regulation on Supervision of Electronic Financial Transactions	• Article 32 (Management of Passwords of Internal Users) A finance company or electronic financial business entity shall reflect the following matters in the information processing system in order to prevent the leakage of the passwords of internal users. • Article 13 (Computational Data Protection Measures) User accounts and passwords shall be assigned to each individual, and their registration, change, and deletion shall be systematically managed.

※ Relevant laws and regulations
Ministry of Science and ICT "Notification on Personal Information Security Management System Certification, etc."
Korea Communications Commission "Notification on Personal Information Security Management System Certification, etc."
Financial Services Commission "Regulation on Supervision of Electronic Financial Transactions"