

Centralization and Automation of Repetitive Management Tasks to Improve Work Efficiency and Security through HIWARE

"Since the introduction of HIWARE, OS account management convenience and security have improved significantly."

Senior Security Manager at HYOSUNG



Success Story

INDUSTRY

Manufacturing

SOLUTION

- HIWARE Privileged Access System Management
- HIWARE Identity Management



OVERVIEW

Integrated Access, Identity Management and Password Management Deployment. Fully Interoperable with OTP, HR and company portals.

RESULTS

- **Protocol Fix**
Manual administration of system security tasks creates a risk of human error and creates a work overload for IT administrators
- **Resolution Method**
Centralization and automation of PAM, IM tasks. Access and management logs provided
- **Connectivity**
Strengthened security, increased management efficiency, and security audit & compliance requirements were satisfied.

ISSUES TO SOLVE

Previously Hyosung Co., Ltd. did not use access control and account management solutions. The IT administrator was manually managing systems, accounts and passwords. Because repetitive management tasks such as the creation, change, and deletion of accounts and passwords was performed manually, the administrator's work was overloaded and there was a major risk of security accidents due to human error. System permission requests and approval tasks were also done through the administrator's e-mail without a separate request/approval system. Therefore, there was a possibility that omissions could occur in the verification and processing process. Additionally, the time for sending and receiving email was wasted unnecessarily, creating an inefficient environment with low productivity.

The biggest problem was that since the accounts were manually managed, it was difficult to monitor the real-time status of unauthorized accounts such as those for terminated employees, employees on a leave of absence, or randomly created accounts.

In order to solve these problems, Hyosung Co., Ltd. needed a centralized and automated solution that is compliant with ISMS certification, and audit activities that included a request/approval system and usage logs.

ACHIEVING RESULTS

NETAND centralized and automated user access control and account management tasks that were previously decentralized and performed manually by using HIWARE to integrate access, identity, and password management. When accessing HIWARE, user authentication is reinforced with 2-factor authentication OTP. Password sharing and theft is prevented with an automatic login function that does not expose system passwords to users when accessing servers. Users are given different system access and task privileges.

Detailed logs are recorded of users who accessed the system, when they accessed it, and what accounts were used to access the system; enabling quick identification of the cause in the event of a problem. Through integration with the HR system, life-cycle management such as account creation/modification/deletion and account authority inheritance tasks are automated when position transfer occurs according to policies set by administrators. In addition, accounts for employees on leave of absence and terminated employees are automatically locked/deleted to block security accidents caused by account theft.

Additionally, we built a password management solution along with the Integrated Access and Identity Management solution to automatically issue/change/revoke system passwords, and apply hard-coded password changes for 900 Windows Job Scheduling accounts in Windows servers. By linking HIWARE with the request/approval portal, authorization tasks that were done through email could be easily performed through a single integrated UI and a unified approval process, similar to access control and identity management tasks.

All user access, actions, and administrator's account and password management logs are all kept, and various reports are generated to prepare for security and ISMS certification audits.



About NETAND

NETAND, is a Network Security Solutions Company that enables organizations to strengthen security insight through market leading Privileged Access Management solution, on-premises and in the cloud. For more information about NETAND visit netand.io.

NETAND FOR BETTER TOMORROW

By automating user access control and identity management tasks that were done manually, the workload of the IT administrator has been reduced, increasing work efficiency significantly. In terms of security, user authentication, automatic detection and blockage of unauthorized accounts has strengthened security. In particular, it became possible to prevent a lapse in security and prevent accidents that could occur due to mistakes caused by heavy workloads. Monitoring requirements for compliance with laws such as the Personal Information Protection Act and the Information and Communication Network Act have also been satisfied. The access history report function has made it easy to respond to ISMS certification inspections and group security audits.