

HIWARE

HIWARE Privileged Access Management for DBMS

HIWARE Identity Management for DBMS



Contents

HIWARE, an integrated PAM solution which has adopted the latest technologies such as artificial intelligence and cloud, is the flagship product of NETAND that has developed various solutions with the best technology.

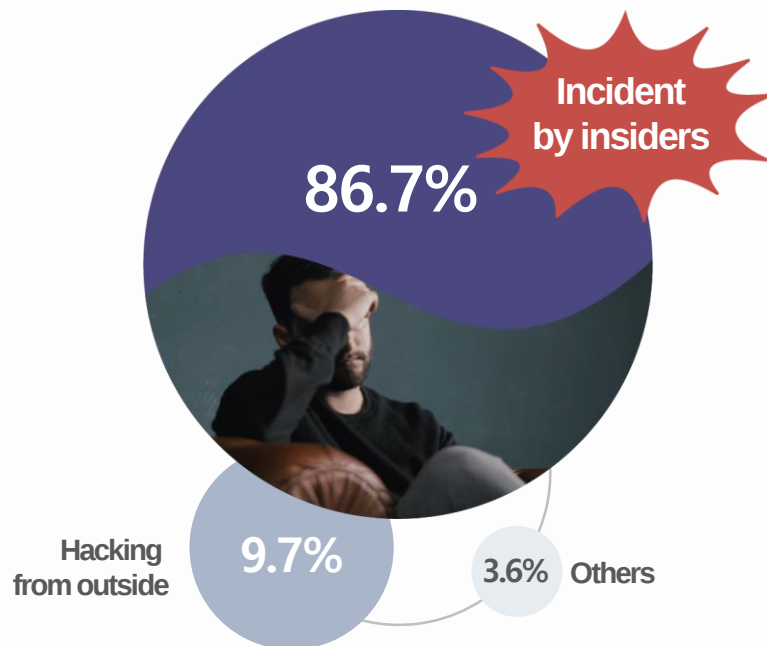
- 01 Background**
- 02 Strengths of Products**
- 03 HIWARE Product Line-up**
- 04 Privileged Access Management for DBMS**
- 05 Identity Management for DBMS**
- 06 References / Success Story / Company Overview**

The beginning and the end of security is “HUMAN”

Complicated and diverse security threats to IT infrastructure have been growing and **most of security incidents are caused by insiders who have their eyes on loopholes of security** created due to neglect as various kinds of security incidents prove.

Additionally, damage of the incidents becomes greater owing to poor response and slow recovery.

Causes of information security incidents



source: ponemon institute 2016

Information Security Incident Examples

- Brute access to IT infrastructure database
- Impossible to prevent insiders who being malicious actions/mistakes
- Poor response to audits by higher-level organizations and security compliance issues
- **Leading to security incidents**
- Difficulties in analyzing causes of incidents and recovery of incidents
- Spending a lot of effort/time writing materials and audit reports

The core of PAM security is “Control” and “Audit”

AS-IS



Incomplete user authentication for accessing database

Possible to unauthorized access databases by stealing passwords if users can be authorized only with passwords



Poor management of authorities to access database

Information leak or database errors due to rash and unauthorized Access



Possible to execute risky query in case of remote control of database

database errors by someone who input risky commands by mistake or maliciously



Poor management of audit reports about Access history and job logs

Impossible to monitor and track down after security incidents
Spending heavy efforts and long time writing audit report

TO-BE



Stronger user authentication

Stronger databases to authorize users through IP/MAC authentication and double authentication



Control of authorities to access database

Thoroughly preventing security incidents in advance by giving different authorities to users depending on policies and controlling access time



Control of database query

Minimizing human errors through provisioning of commands by control, logging, and alert features when input commands



Log record/audit report

Stronger monitoring and tracking with logs of every job Improving efficiency of supporting audit by providing integrated reports of authorities and account status

The first step of IM security is thorough “Management” of accounts and authorities

AS-IS



Poor management of ID integration of different database

Impossible to identify status of entire accounts and difficulties in integrated management



Lower regulated management with complexity passwords and frequency of the password change

Increasing risk of password exposure



Manual creation, assignment, and collection of ID

Burden due to manual works and risk of human errors



Disorganized the status of identities which is Retired Employees or dormant accounts

Data leak and security incidents caused by theft of accounts of Retired employees or dormant accounts

TO-BE



Smart Integrated ID management

Effective integrated management of every account through periodical automatic collection and synchronization



Improving highly regulated Password management

Maintaining consistent security policies and preventing password leak by implementing the policy of integrating passwords for heterogeneous devices



Automatic ID life-cycle management

Improving efficiency at work by automatically managing creation and collection of accounts



Management of unauthorized account

Prevention and detection of Insider threats by unauthorized accounts they had created

Upgrade Your Thinking

Providing amazing convenience of use

Our solution does not simply provide features of security.

It is the next generation Access control solution considering security, convenience of use, and efficiency at work.

This easy but strong solution changes users' thought that a security solution is inconvenient to use.



Responsive U.I



Dynamic dashboard



Management feature to inform what a user should do

Notification

Bookmark

Personal widget

Real-time data statistics

Making work environment smarter and more stable

Solutions have to change, following rapidly changing business environment and IT infrastructure. HIWARE is the next Access control solution which perfectly supports not only users' work environment but also diverse IT infrastructure such as cloud and network segmentation.

Create a smart work environment in a rapidly changing IT environment under security threat without concerns about security.

User Environment

✓ Cross browsing



✓ Multi-languages



✓ Windows / MAC



✓ IPv6

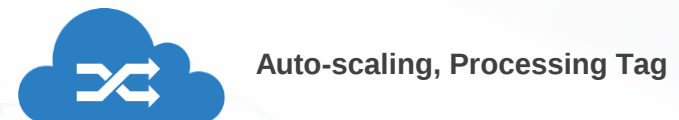


Infrastructure

✓ Network segmentation



✓ Cloud environment



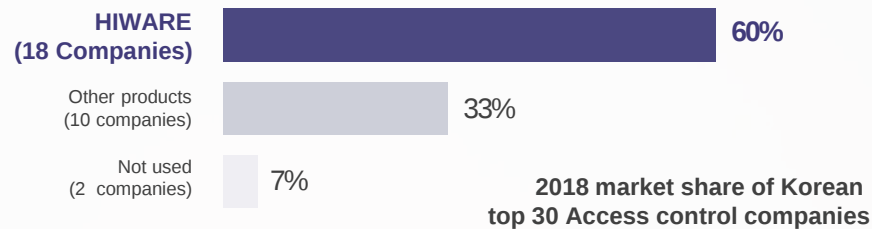
Auto-scaling, Processing Tag

Providing the best service and quality that you have never experienced

The first and the best Access control solution in Korea for last 10 years. You are the best so the best solution goes with you. **This solution will upgrade your experience of using the solution** since it is the best solution that you have never experienced and the company's engineers provide the best service.

✓ Top market share in Korea access management

No.1



2018 Korean company ranking: http://www.ceoscore.co.kr/pop_preview.php

✓ TOP market share in Korea identity management

No.1

Total sales of domestic IM/PAM market in 2019

KISIA
<2019 survey on domestic information security industry >
IM/EAM total sales



✓ Professional staff



- 10 years of technology and know-how
- Korea's highest level of professional manpower work environment.

✓ Global partner network & business

Providing services swiftly and accurately anytime anywhere



- Cooperating with 50 global partners in 20 countries
- 10 clients including SMART, the largest telecommunication service provider in the Philippines, in the world
- Operating a corporation and the R&D center in' San Francisco in the US

Implementing the top-tier security management based on integration of identity management and privilege Access management

Not only identity management but also controlling authorities to Access databases and do jobs through the concerned account is required for stronger and efficient security.

HIWARE Identity management



Account life-cycle management



Password management



Integrated policy management



Retired employee / illegal account management

HIWARE Identity management + HIWARE Access management



Integrated UI



Approval database



Policy setting



Audit report



Privilege Access Management

- Access control
- Command control
- Access control
- Log audit



Identity Management

- Life-cycle management
- Password management
- Integrated account management
- Illegal account management



Integrated UI



Simplified work processes



Account authority management



Strengthening maintenance stability



Dormant account management

HIWARE

NETAND., Ltd. of the top-tier technology and variety of experience supplies **HIWARE, a package of integrated Identity and Access Management(IAM)** which consists of seven products managing security of IT infrastructure and databases of companies and institutions.

Standard

1. HIWARE Privileged Access Management for database v6.0
2. HIWARE Identity Management for database v6.0

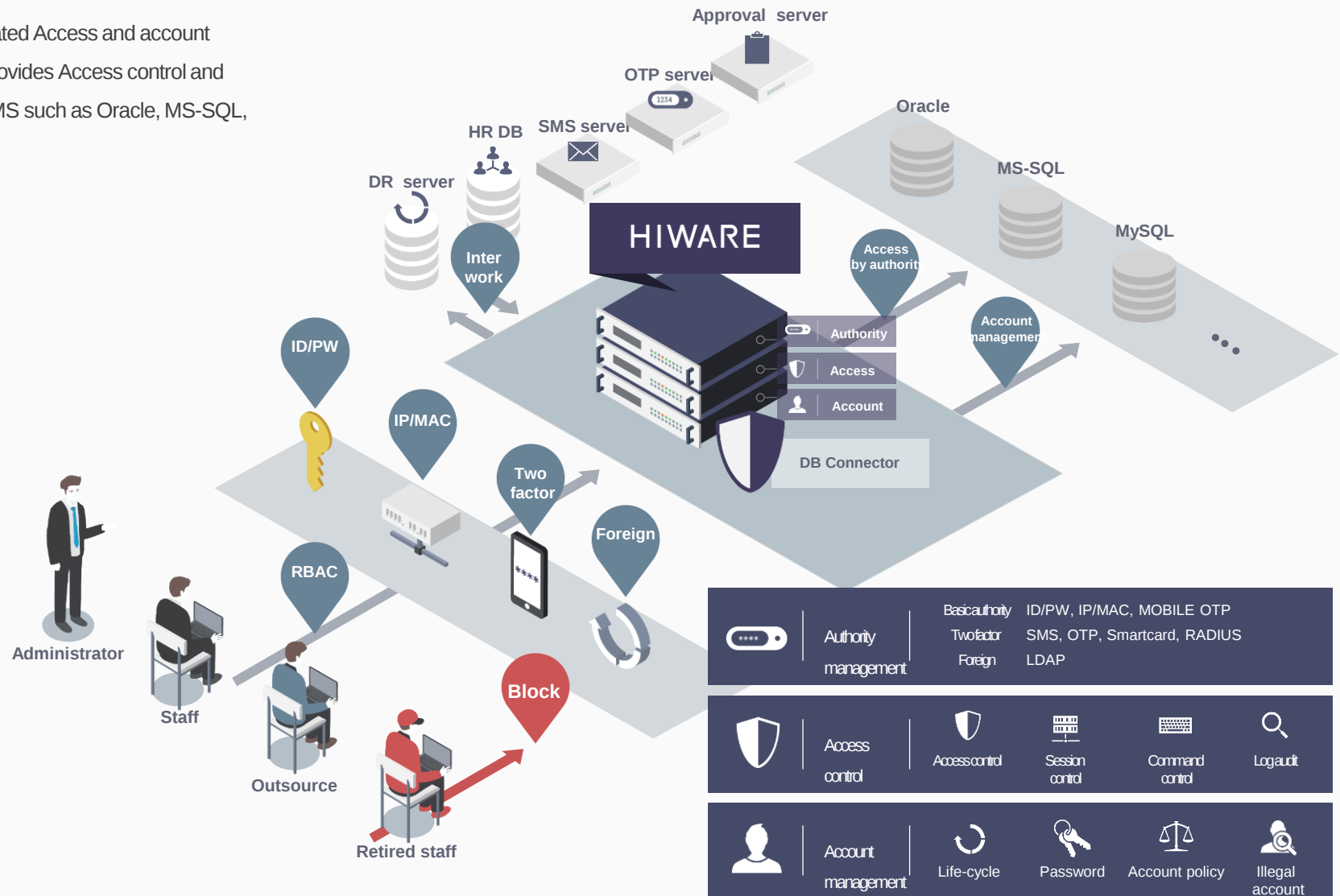
Scalable

3. HIWARE Privileged Access Management for Database v6.0
4. HIWARE Identity Management for Database v6.0
5. HIWARE Identity Management for Active Directory v6.0
6. HIWARE Mobile One Time Password v6.0
7. HIWARE Threat Analytics v6.0



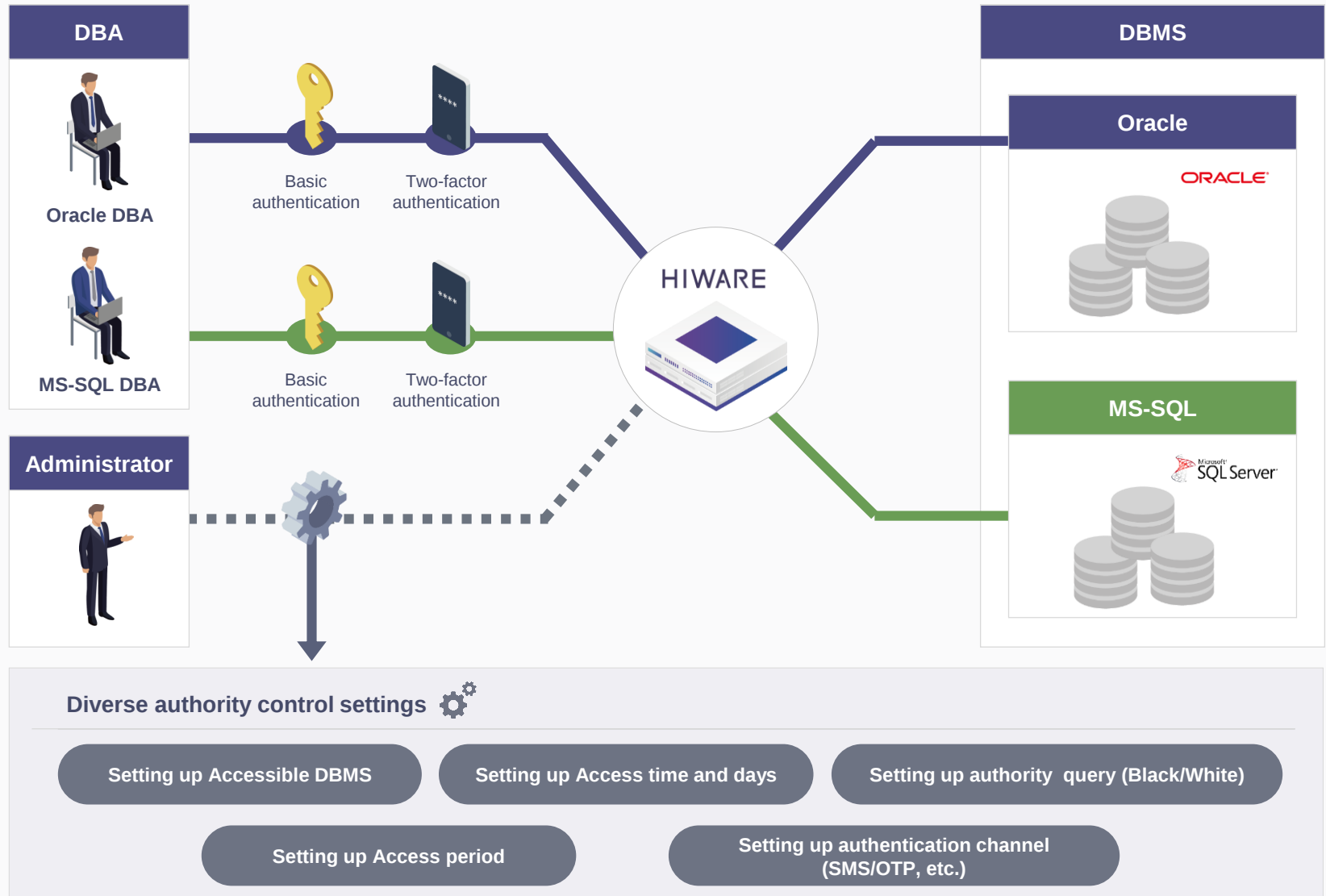
HIWARE PAM for DBMS v6.0

HIWARE PAM for DBMS is an integrated Access and account authority management solution that provides Access control and account management for various DBMS such as Oracle, MS-SQL, and MySQL.



DBMS Access authority control

- ✓ Access authority control by user
- ✓ Reinforce authentication (Two Factor)
- ✓ Access time control
- ✓ Automatic login to DBMS



DBMS query control

✓ query control
(permitted/prohibited)

✓ Managing monitoring/
blocking/notification of query

✓ Requesting approval of
important query

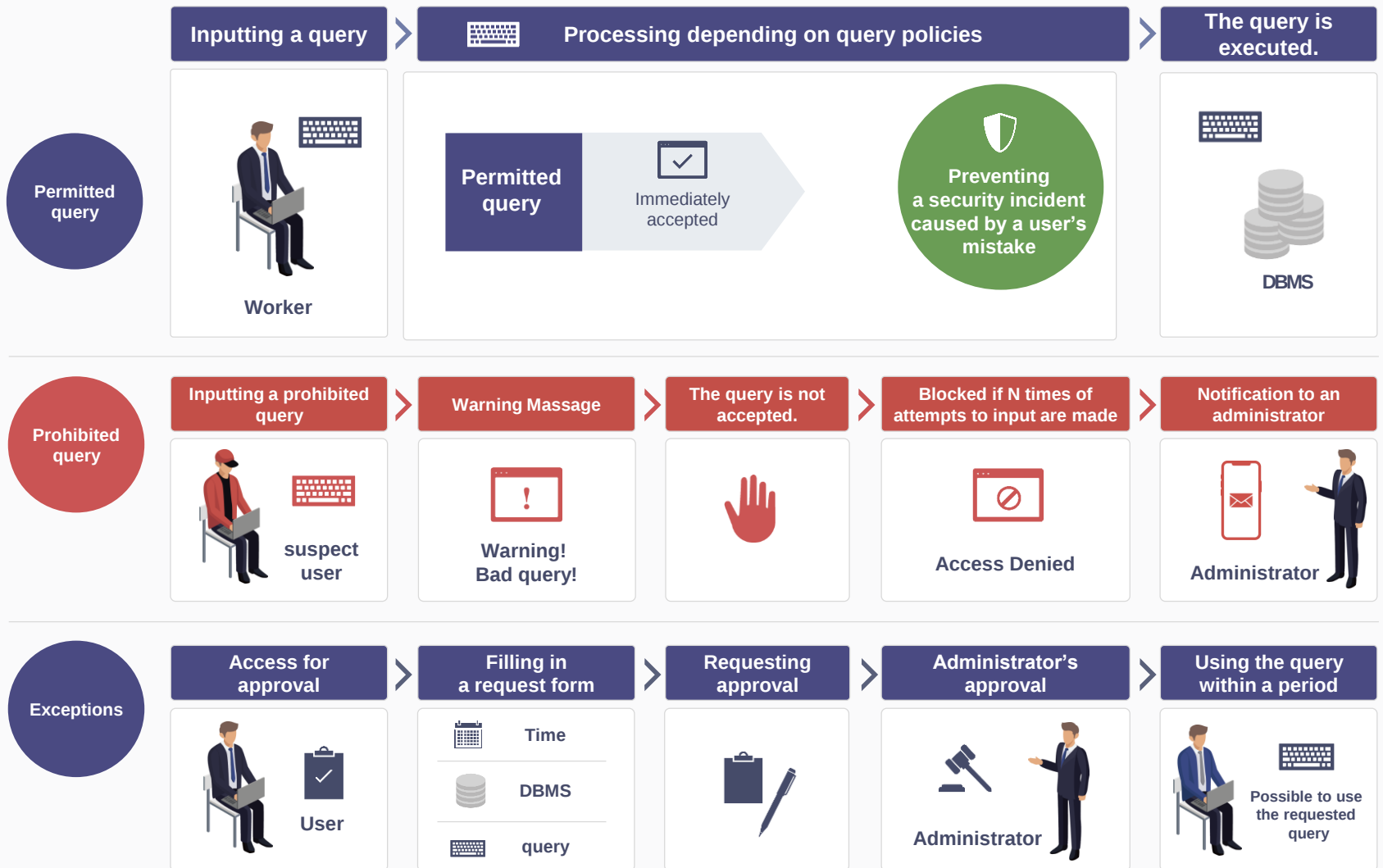
✓ Managing query usage history

Control query type

- **QUERY** : SELECT, DESC, WITH,...
- **DML** : INSERT, UPDATE,...
- **DDL** : CREATE, DROP,...
- **DCL** : GRANT, REVOKE,...
- **PL/SQL** : BEGIN, REVOKE,...

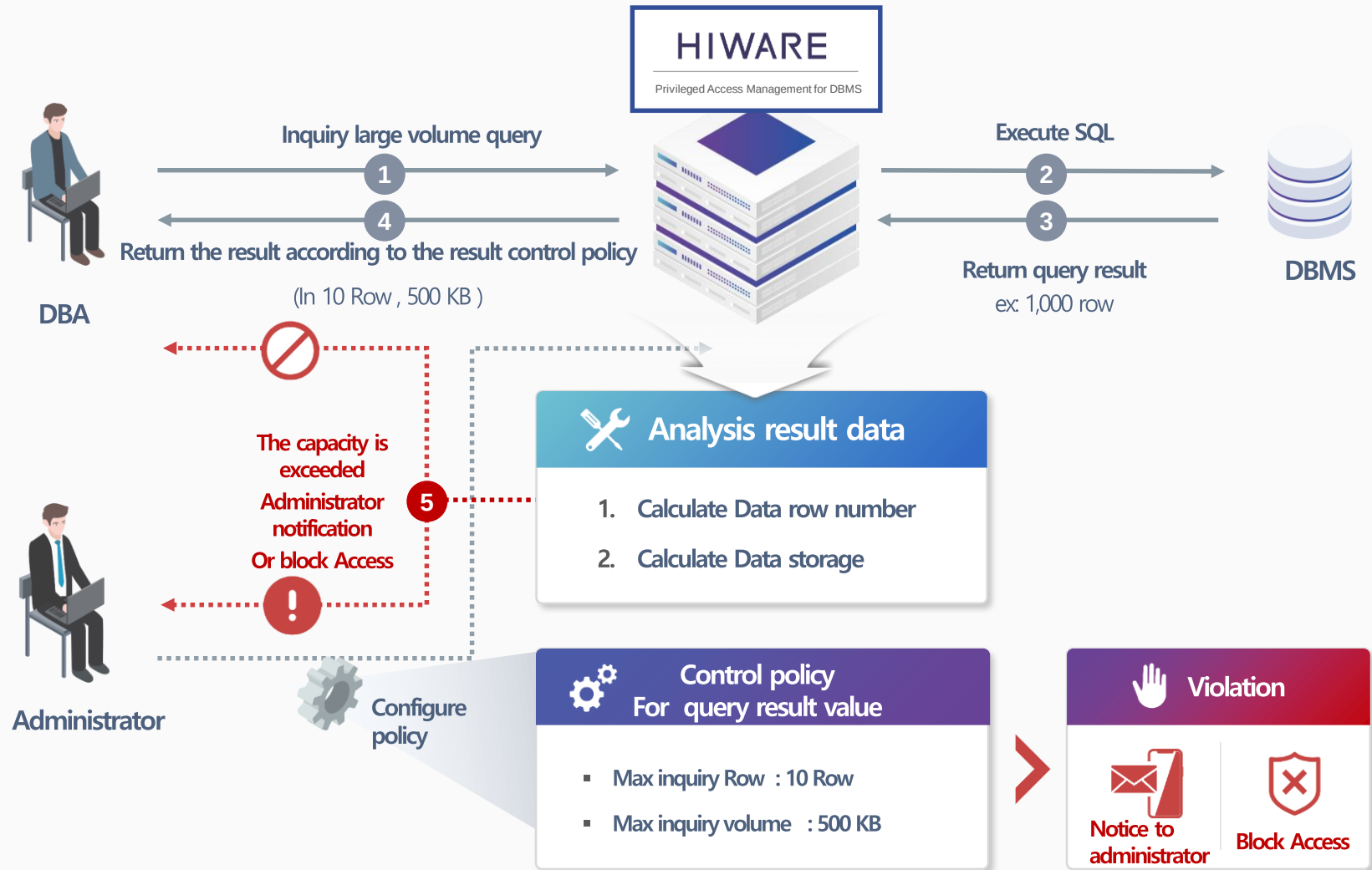
Control query context (pattern)

- **Template #1 : Social number**
-> ^\d{2}(0[1-9]|1[0-2])(0[1-9]|[12][0-9]|[3][01])\d{4}-[1-4][0-9]{6}
- **Template #1 : Email**
-> (Ww+W.)*Ww+@(Ww+W.)+[A-Za-z]
- **Template #1 : IP address**
-> ((([0-9])|([1-9]\d{1})|([1]\d{2})|([2][0-4]\d)|([25][0-5]))\d{3}([0-9])|([1-9]\d{1})|([1]\d{2})|([2][0-4]\d)|([25][0-5]))



Control result data(1/2)

- ✓ Control large volume data
- ✓ Control data inquiry number
- ✓ Masking sensitive data
- ✓ Notification to administrator

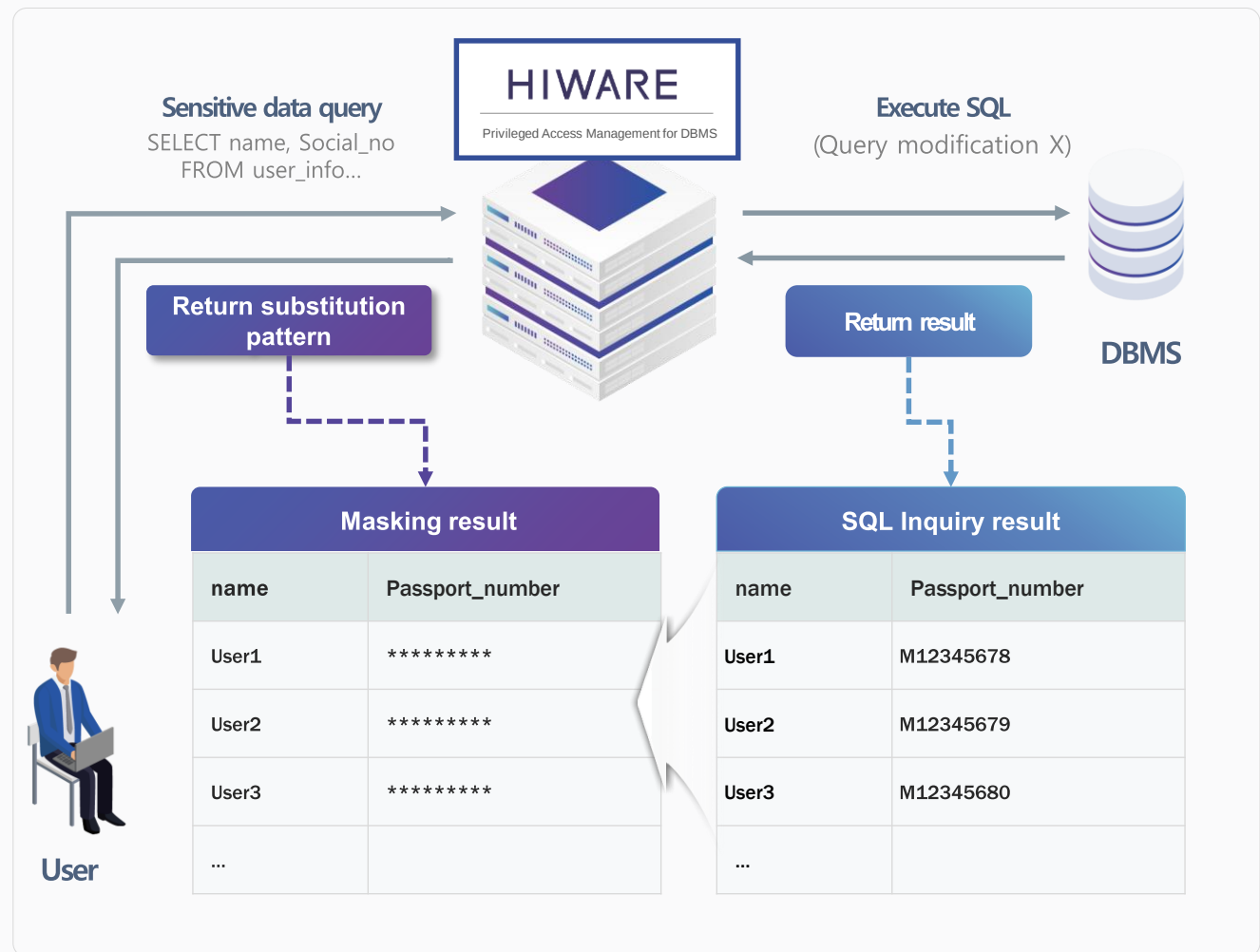


Control result data(2/2)

< Define Masking pattern >		
Masking Name	Masking pattern	Substitution pattern
Cell phone number	(01[016789])-(1-9)[0-9]{2,3})-(0-9){4}	010-****-****
Social number	^\d{2}(0[1-9] 1[0-2])(0[1-9] 1[12][0-9] 3[01])\1-4[0-9]{6}	*****-*****
Credit card number	[1-9][0-9]{3}-[0-9]{4}-[0-9]{4}-[0-9]{4}	****-****-****-****
...		



Configure policy



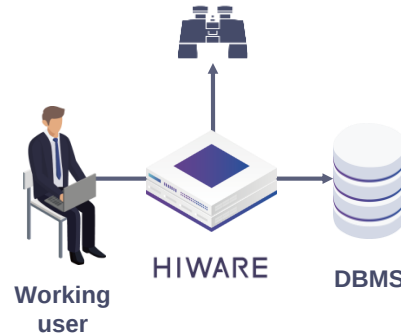
DBMS log / audit

- Logging information of auditing work details
- Diverse statistics and audit reports
- Various search filters
- Statistics by user/DBMS/query
- Inquiry query result

Logging

Monitoring all events after Access

Auditing work details in real time



Logging audit information of work details



Detailed history management

Providing various search filters

Access history by user

Change history by DBMS

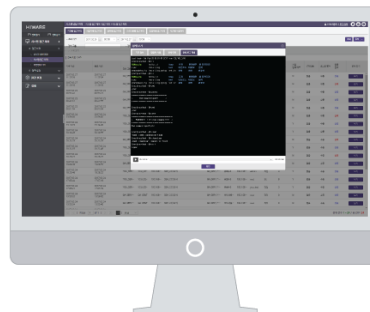
Usage history by query

History of work details

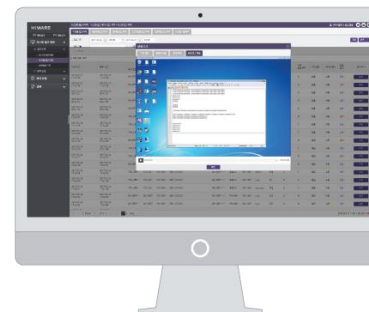
Searching diverse history

Auditing

Auditing variety of work details



[TEXT audit] Displaying texts by query



[Video audit] Displaying video by query



[Dashboard] Multivariate statistics

Account life-cycle policy management

✓ Automatic collection/
synchronization of accounts

✓ Provisioning management
(create/change/delete)

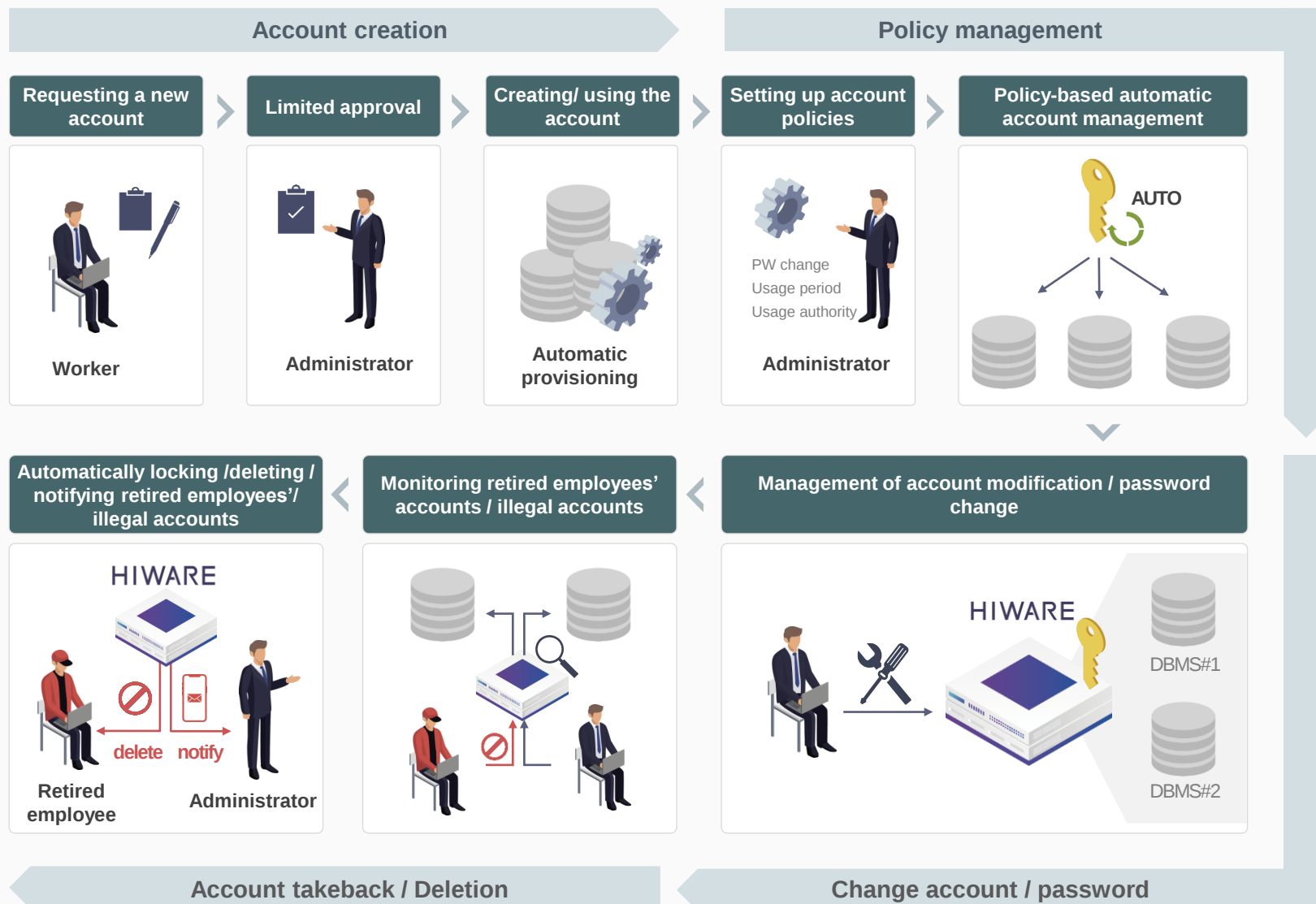
✓ Suspension in Implementing
policies

✓ Handling accounts at once

✓ Personal setting
(password / unlock)

✓ Providing solutions to
normalize accounts depending
on their status

✓ Tracking down change history
by account



Password policy management

✓ Password complexity management

✓ Management of password change frequency

✓ Automatic/manual/random change of passwords

✓ Password management report

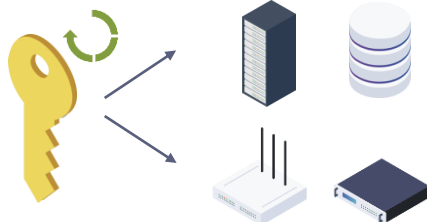
✓ Password change history management

Setting up password policies



Administrator

Automatic change of passwords based on policies



Automatic provisioning of accounts



Reporting change history



Administrator

Efficiency in managing passwords



Automatic change

Automatically changing on a scheduled date



Manual change

Directly changing by booking change on a certain date



Bulk change

Changing all passwords at once

Security of passwords



Random change of passwords

Randomly changing by setting up complexity



Setting up complexity of passwords

Numbers, capital letters, special characters, etc.

Password management report



Password management report

(The report that passwords can be viewed)



Password change history

Password change history report



History of access passwords

Report on the history of viewing passwords

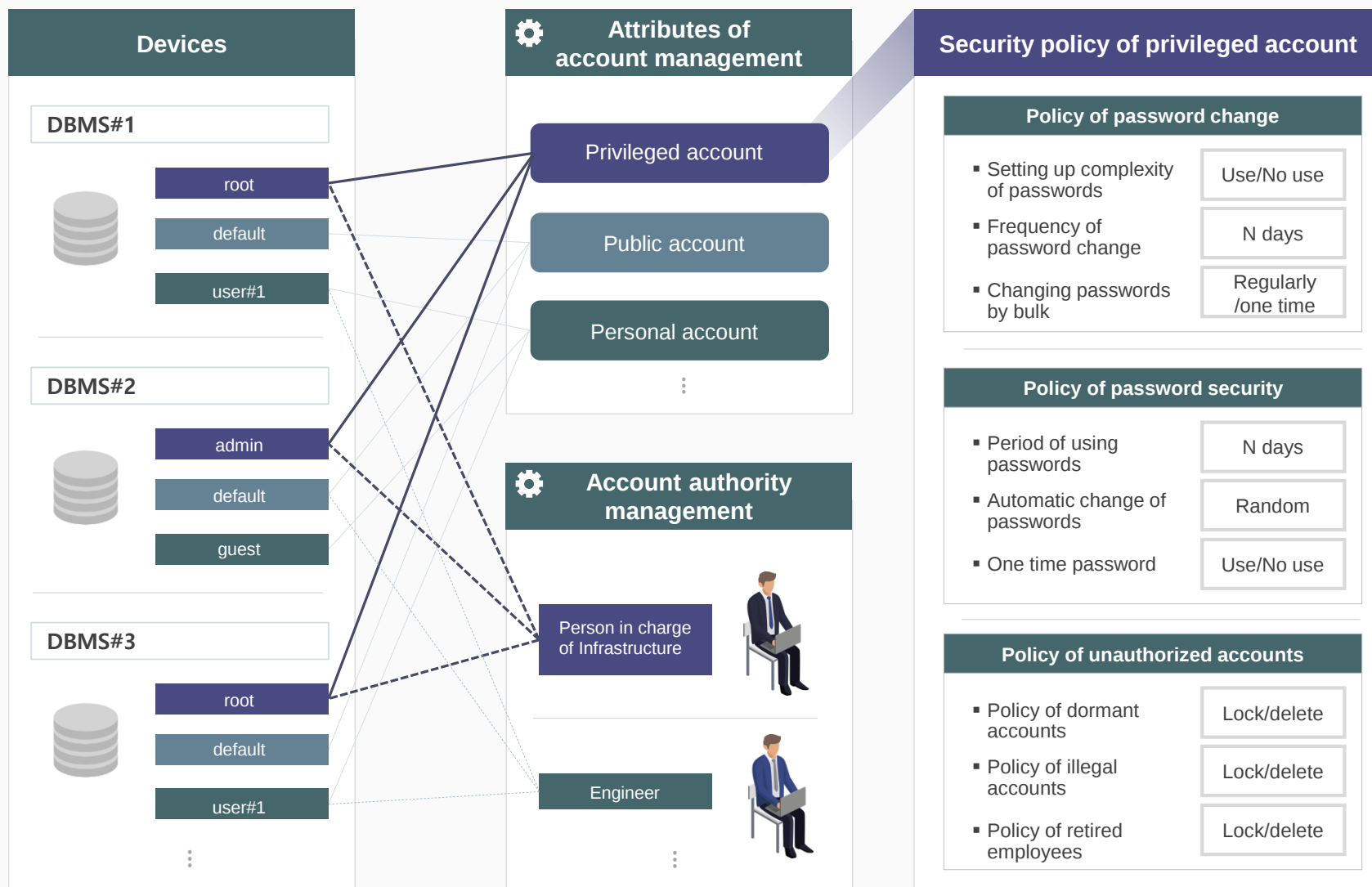
Integrated management of account policies

✓ Integrated management of accounts for heterogeneous DBMSs

✓ Establishing policies to manage by account attribute

✓ Providing overview for administrator of integrated accounts

✓ Policies to standardize accounts



Management of retired employees / inactive / illegal accounts

✓ Managing Retired employees' accounts

✓ Detecting, automatically deleting / locking unauthorized accounts

✓ Managing ghost accounts

✓ Managing broken accounts

✓ Managing history of Unauthorized accounts

Retired employees

Retired employees' accounts



Account deleted in the HR DBMS since the worker left the company
> **Automatically blocked through integration with the HR DBMS**

Illegal

Unauthorized accounts



Ghost

Created illegal account which is in a DBMS but not registered



Broken

Deleted unauthorized account which is registered but not in a DBMS

DBMS



DBMS#1



DBMS#2



DBMS#3



DBMS#4



Lock



Delete



Notify

Administrator



References

Global Clients

 Philippine SMART Communications	 Cambodia ACLEDA Bank	 Philippine RCBC Savings Bank	 Philippine Robinsons Land Corporation
--	---	---	--

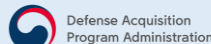
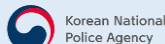
Manufacturing / Businesses

Finance

Public

						central administrative agency of Korea
						
						

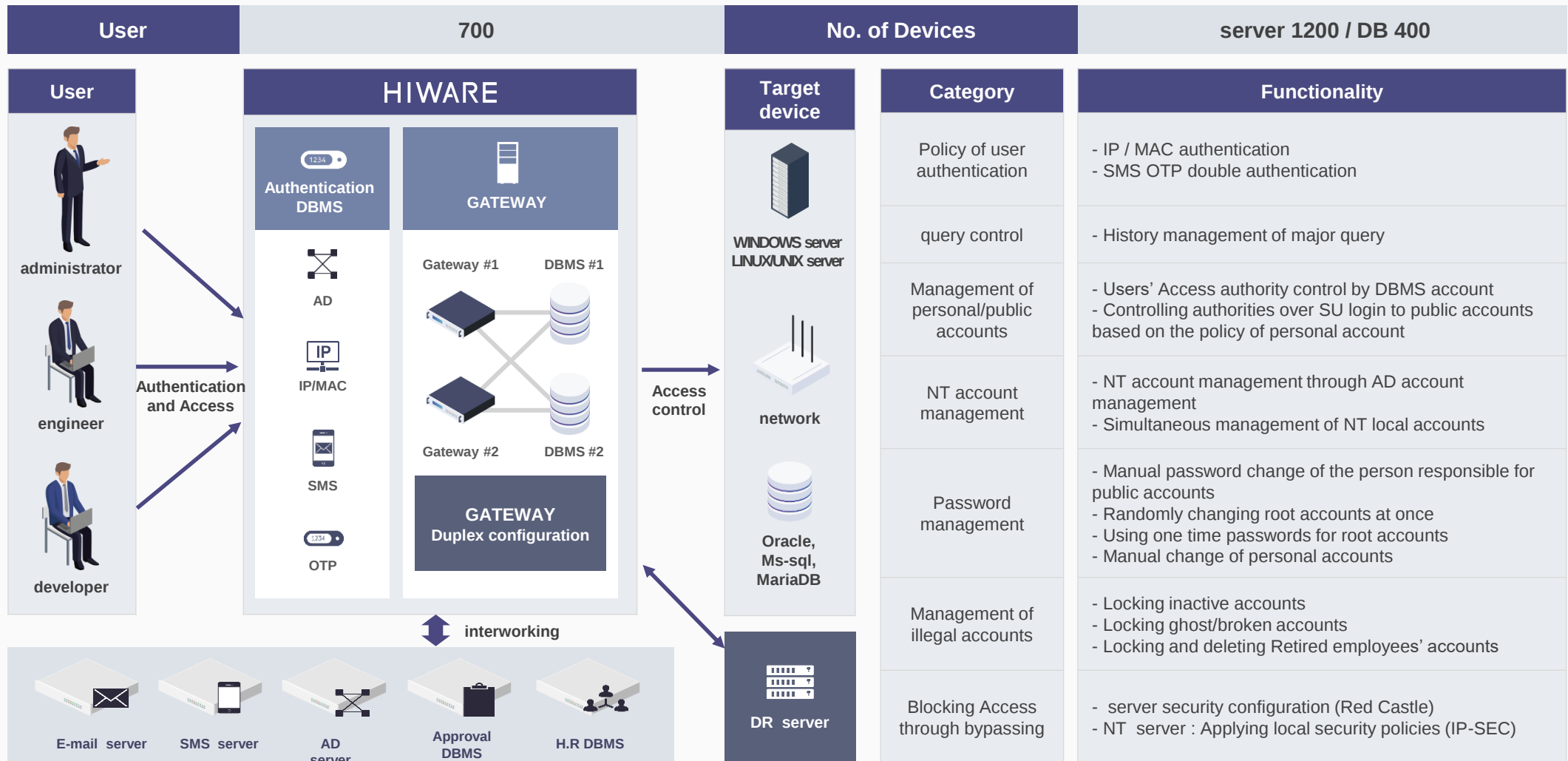
Broadcasting/telecommunications

					
---	---	---	---	---	---

... And, more than 500 clients at home and abroad

Success Story

In this case, both DBMS Privileged Access management solution and identity management solution are established together and they are integrated with diverse authentication DBMS to strengthen security and improve stability through dualization of gateways. Also, the solutions are integrated with the client's existing in-house DBMSs such as HR DBMS, approval DBMS, and the server for managing automation to implement a single interface and enhance convenience of use and efficiency at work at the same time.



“NETAND”, the company creating values beyond network

Korean top researchers in the company are studying and developing more advanced technologies based on their expertise of IT security and operating and management solutions which has been accumulated through abundant experience with diverse clients even at this moment to continuously secure clients' high credibility and satisfaction.

NETAND will be the company which creates forward-looking values, considering the past, the present, and a better future, at the point of contact between people and networks.

Category	Details
Name	NETAND., Ltd.
CEO	Shin Ho-cheol
Business areas	Software development, supply of device Access control DBMS and identity management for DBMS
Address	10 th floor, Hanam Building, Yeouido-dong, Yeongdeungpo-gu, Seoul
Contact	02) 2661- 10 FAX 02) 2661-1420 http://www.netand.co.kr
Employees	122 employees (50 researchers / 40 engineers)
Year of foundation	Jan. 2 nd , 2007
Certification/awards	Certified as a venture enterprise/ Certified by INNO-BIZ / GS certification / CC certification / New SW product award

Certification / Awards



INNO-BIZ certificate of small-and-medium enterprise with innovative technology



Certificate of venture enterprise



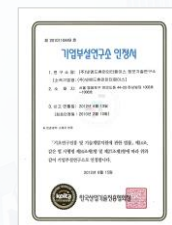
Certificate of a patent



CC Certificate



Certificate of software quality (GS)



Certificate of research institute under a company

Thank you