

클라우드 환경에서의 PC/모바일 사용자 접근 관리

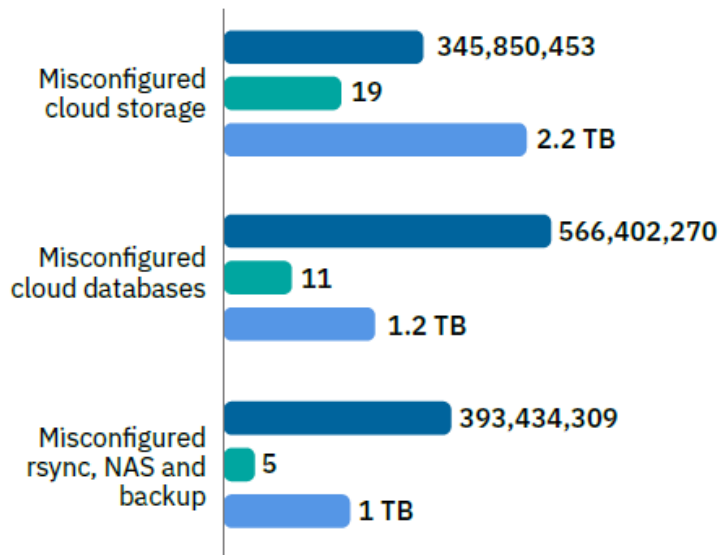
IBM SECURITY ACCESS MANAGER ENTERPRISE EDITION



박형근 실장 (phk@kr.ibm.com)

클라우드 보안 사고 유형

Notable cloud service misconfiguration incidents in 2017



■ Records breached
 ■ Number of incidents
 ■ Amount of data

Figure 9: Notable cloud service misconfiguration incidents in 2017.

IBM X-Force Threat Intelligence Index 2018



AWS S3 버킷 설정 오류
이름, 전화번호, 성별,
비밀번호, **이메일 주소** 등
고객 5만명 개인정보 유출



클라우드 상의 아파치
에어플로우(Apache Airflow)
서버 설정 오류로 **FTP**
크리덴셜과 SQL 비밀번호,
AWS 비밀 액세스 키, 비밀번호
정보 다량 유출



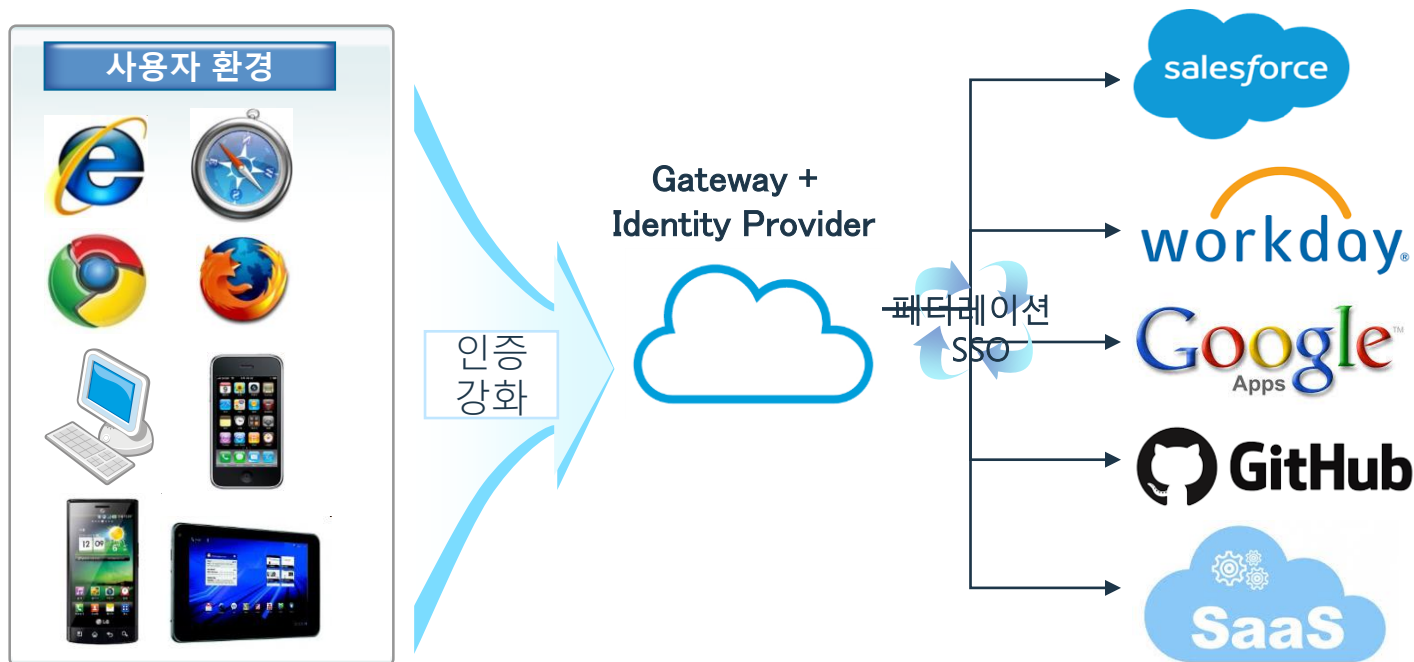
AWS S3 버킷 설정 오류로
비밀 API 데이터와 **인증 계정,**
디크립션 키, 고객 정보 등
유출

내부자 위협 + 클라우드



클라우드 접근 관리를 위한 아이덴티티 프로바이더 활용

클라우드 접근 관리를 위해 사용자 접점인 게이트웨이와 아이덴티티 프로바이더가 결합된 IBM Security Access Manager Enterprise Edition을 활용합니다.



클라우드 접근 관리

인터넷 상에서 자유롭게 접근 가능한 퍼블릭 클라우드와 서비스형 소프트웨어(SaaS) 환경에서 사용자 접근을 관리할 수 있을까?

회사 내에서만 특정 서비스(SaaS)에 접근 가능하고 그 외에는 접근 차단할 수 있나요?

악성 IP (Reputation) 데이터베이스를 기반으로 접근을 차단할 수 있나요?

주말에는 접근을 차단할 수 있나요?

업무 시간에만 접근을 허용할 수 있나요?

SaaS마다 다른 접근 정책을 적용할 수 있나요?



클라우드 접근 관리

POP Properties

General Attach IP Auth Extended Attributes

POP Name

CloudPublicIPControl

Description

Cloud Public IP based Control

☒ Warn Only On Policy Violation

Audit Level

- ☒ Permit
☒ Deny
☒ Error
☒ Admin

Quality of Protection

Privacy ▾

Time of Day Access

- ☐ Sunday
☒ Monday
☒ Tuesday
☒ Wednesday
☒ Thursday
☒ Friday
☐ Saturday

☐ All Day

☒ Between hours of: Start Time: 8 ▾ 00 ▾

End Time: 19 ▾ 00 ▾

☒ Local Time ☐ UTC Time

POP Properties

General Attach IP Auth Extended Attributes

POP Name

CloudPublicIPControl

List of all IP Auth

Create...

Delete

Select	Network	Netmask	Authentication Level
	Any Other Network		0
☐	211.212.202.54	255.255.255.255	Forbidden
☐	172.31.24.4	255.255.255.255	Forbidden

Create IP Authentication

POP Name

CloudPublicIPControl

* Network

☐ Any Other Network

* Netmask

* Authentication Level

0 ☐ Forbidden

Create

Cancel

클라우드 접근 관리

Access Policies - Access_Policy_Dump

```
importClass(Packages.com.ibm.security.access.policy.decision.Decision);
importClass(Packages.com.ibm.security.access.policy.decision.HtmlPageDenyDecisionHandler);
importPackage(Packages.com.tivoli.am.fim.trustserver.sts.utilities);

//This access policy denys the user from running a successful Single Sign On, print all the context information such

var AllowedIPRanges = [
    ['14.63.75.1','14.63.75.126'],
    ['221.149.38.1','221.149.38.254'],
    ['221.149.39.1','221.149.39.254'],
    ['210.13.75.57','210.13.75.62'],
    ['182.18.15.89','182.18.15.94'],
    ['4.16.175.57','4.16.175.62'],
    ['114.203.208.1','114.203.208.254'],
    ['185.46.212.88','185.46.212.88'],
    ['104.129.202.1','104.129.203.254'],
    ['165.225.34.1','165.225.35.254'],
    ['165.225.50.1','165.225.51.254']
];
```

클라우드 접근 관리

Manage Application Databases

General Configuration

IP Reputation Database:

☒ Auto Update

IBM Security Access Manager

LogoutHelpLanguage

IBM.

HomeAppliance Dashboard

MonitorAnalysis and Diagnostics

SecureMobile Settings

ManageSystem Settings

Access ControlPoliciesResourcesAttributesObligations

SaveCancel

Name:Check Risk Score and Malware

Description:Permit access if low risk score and ip reputation is not malware

Subjects

Rules (1)Precedence: PermitAttributes: Optional

1. If All are true (

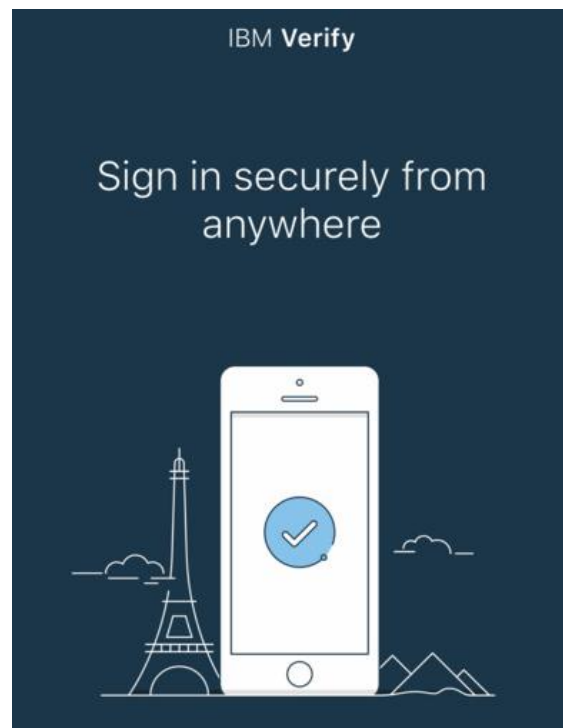
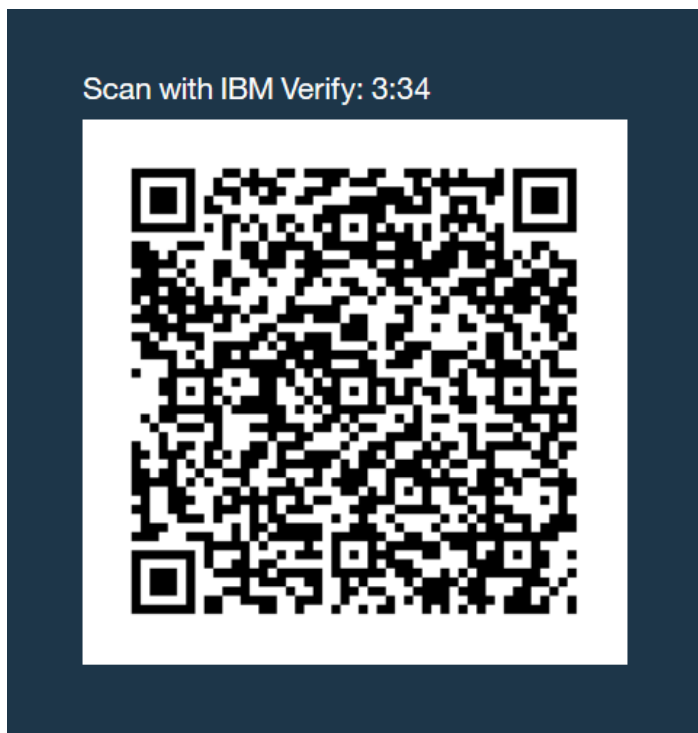
riskScore<=50andnot ipReputation has member Malware

) Then Permit

OKCancel

클라우드 인증 - QR 인증 혹은 패스워드리스

인터넷 상에서 자유롭게 접근 가능한 퍼블릭 클라우드와 서비스형 소프트웨어(SaaS) 환경에서 사용자 계정 정보 유출이나 도용의 문제를 QR 코드 기반 인증 혹은 패스워드리스 인증으로 해결해 보자!!



클라우드 싱글사인온

인터넷 상에서 자유롭게 접근 가능한 퍼블릭 클라우드와 서비스형 소프트웨어(SaaS) 환경에서 사용자 경험을 높이기 위한 싱글사인온 지원을 위해 웹 서비스 표준 인증 방식(SAML, OAuth, OIDC, JWT, OpenID 등)과 필요하다면 계정 관리도 지원합니다.

* 참조: <http://www-01.ibm.com/support/docview.wss?uid=swg21970379>



서비스 목록
Login ID: test1@ibmtest.net Group: sales Login IP: 211.212.202.54
<u>Sales Force</u> <u>이메일(Gmail)</u> <u>메신저(Slack)</u> <u>개발허브(GitHub)</u> <u>인프라(AWS Web Console)</u> <u>금융서비스</u>
<u>패스워드 변경</u> <u>로그아웃</u>

클라우드 인프라 접근 제어

인터넷 상에서 자유롭게 접근 가능한 가상 머신에 대해 패스워드 관리, SSH 키 관리, 그리고 사용자 행위 모니터링(세션 레코딩)을 수행합니다.

Secret Server

Search Secrets

Search

HOME

TOOLS

ADMIN

REPORTS

?

An update is available (10.5.000003)

Advanced | Basic

+ Content

Browse

Reporting Dashboard

Find Folder

< All Folders >

Personal Folders

Critical Accounts

Linux Systems

Router Devices

Service Accounts

SQL Server Accounts

Windows Systems

Advanced

Secret	Folder	Template
☐ iamlab.ibm.com\wina...	Windows Systems	Active Directory Acco...
☐ iamlab.ibm.com\wina...	Windows Systems	AD Account - Fixed M...
☐ iamlab.ibm.com\wind...	Windows Systems	Active Directory Acco...
☐ Windows Client Admi...	Windows Systems	Windows Account

Page 1 of 1 100 View 1 - 4 of 4

< Select Bulk Operation >

Create Secret

Create New

< Select >

Favorite Secrets

CENTOS Root Account

Expired Secrets

iamlab.ibm.com\privmanager

iamlab.ibm.com\secretserver

iamlab.ibm.com\windowsadmin1

Secret Template Distribution

Session Monitoring

Request Management

클라우드 인프라 접근 제어

인터넷 상에서 자유롭게 접근 가능한 가상 머신에 대해 패스워드 관리, SSH 키 관리, 그리고 사용자 행위 모니터링(세션 레코딩)을 수행합니다.

Session Playback Search

Search Filters

Search Across

- Secret Name ☒
- Secret Items ☒
- Username ☒
- Proxy Session Client Data ☐
- RDP Keystroke Data ☒

Date

Last 30 Days

Status

All

Launcher Type

All

Showing 1 to 10 of 53  

Page

CentOS SSH Key Rotation - Accessed By admin
PuTTY   · 12/3/2018 05:06 PM· 0:00:44
192.168.42.11
[View Secret](#)



CentOS SSH Key Rotation - Accessed By admin
PuTTY   · 12/3/2018 05:02 PM· 0:03:36
192.168.42.11
[View Secret](#)



CentOS SSH Key Rotation - Accessed By admin
PuTTY   · 12/3/2018 05:01 PM· 0:00:26
192.168.42.11
[View Secret](#)



클라우드 인프라 접근 제어

인터넷 상에서 자유롭게 접근 가능한 가상 머신에 대해 패스워드 관리, SSH 키 관리, 그리고 사용자 행위 모니터링(세션 레코딩)을 수행합니다.

Watch Session Recording

Session Summary

Session Secret: [CentOS SSH Key Rotation](#)
Machine: 192.168.42.11

Session User: admin
Launcher Used: PuTTY

Session Start: 12/3/2018 05:06 PM
Session End: 12/3/2018 05:07 PM

Search Session Activity

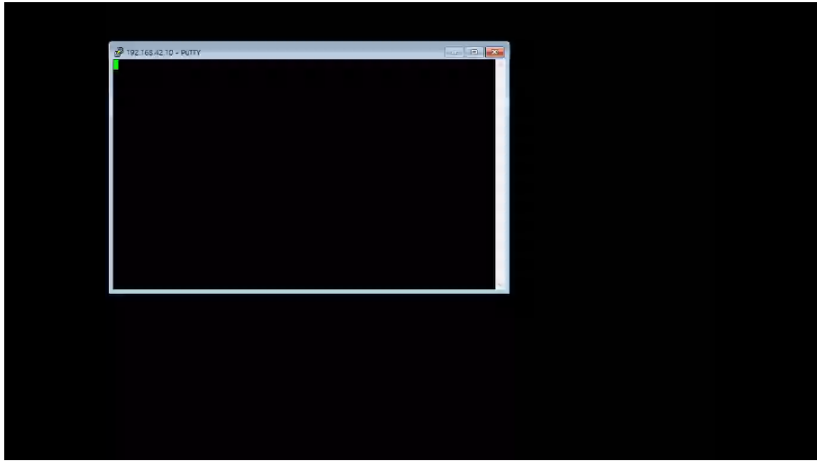
Activity Type:

Keystroke

Keyword:

Elapsed	Type	Activity	Jump To
00:00:01	1		
00:00:01	cmd1 -al		
00:00:13	cmd1		
00:00:13	pwd		
00:00:13	cmd1 -sdjflsdjfls		
00:00:13	cd ..		
00:00:13	exit		

[View entire SSH Session Log](#)



클라우드 인프라 접근 제어

인터넷 상에서 자유롭게 접근 가능한 가상 머신에 대해 패스워드 관리, SSH 키 관리, 그리고 사용자 행위 모니터링(세션 레코딩)을 수행합니다.

Change Password Remotely

By clicking the change button, the password on the remote device will be queued for an immediate change.

Secret Name

CentOS SSH Key Rotation

Next Password



Generate

SSH Key



Generate New SSH Key

Next Private Key Passphrase



Generate

클라우드 인프라 접근 제어

인터넷 상에서 자유롭게 접근 가능한 가상 머신에 대해 패스워드 관리, SSH 키 관리, 그리고 사용자 행위 모니터링(세션 레코딩)을 수행합니다.

AutoChange Schedule



The AutoChange Schedule will be saved and run in Secret Server's time zone which is current

- ☐ Daily
- ☐ Weekly
- ☒ Monthly
- ☐ None

☐ Day of every (months).

☒ The of every * (months).

Starting on: Changing at:

Only change password when Secret is expired ☐

IBM 클라우드 보안 프레임워크





THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.