

차세대 특권 계정 및 접근 관리

IBM SECRET SERVER



윤우희 이사 (wh.yoon@escare.co.kr)

DEC, 2018

ES-CARE 소개



주식회사 에스케어 (ESCARE Co.,Ltd.)는
기업을 보호하기 위한 인간중심의 프로세스 변화를 추구합니다.

금융권 / 글로벌 기업 정보보안 파트너

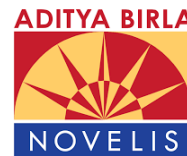


Finance	KDB 산업은행	Standard Chartered SC 제일은행	우리은행
中國銀行 BANK OF CHINA	中国建设银行 China Construction Bank	Bank 中国光大银行 CHINA EVERBRIGHT BANK	K bank
kakaobank	Prudential	수호천사동양생명	Cigna. 라이나생명
KB 투자증권	IBK 투자증권	유진투자증권	ktb 투자증권
현대증권	KG Inicis	DEUTSCH FINANCIAL	모기지파트너스 MORTGAGE PARTNERS
르노캐피탈	C&V Asset Management Corp.	대한민국 No.1 롯데렌터카	JT 캐피탈
우리카드	대신증권 Daishin Securities		

금융권 / 글로벌 기업 정보보안 파트너



AMOREPACIFIC



2018 글로벌 위협 보고서



Figure I: The Global Risks Landscape 2018



- 2016년에 기업들은 **40억 건 이상의 데이터 유출 피해를 발견**했습니다. 이 수치는 이전 두 해의 총 합계를 초과합니다.
- 사이버 공격의 재정적 비용이 증가하고 있습니다. 7개국 254개 기업을 대상으로 실시한 2017년의 한 조사에 따르면 사이버 공격에 대응하는 데 드는 연간 비용은 기업당 1,170만달러로 **전년 대비 27.4% 증가**했습니다.
- 향후 5년간** 기업의 사이버범죄 피해 비용은 **8조 달러에** 이를 것으로 예상됩니다.

80 %

의 침입이 권한 있는
자격 증명을 포함합니다.

- 2016 Forrester Wave
Privileged Identity Management

75 %

의 침입이 내부자 위협
및 남용을 포함합니다.

- 2016 IBM Security Index
Security Index Report

85 %

의 침입이 손상된
엔드포인트를 포함합니다.

- 2016 SANS Report

IN THE NEWS

“Yahoo! Hack! How it Took Just One-Click...”

“Do you know spear-phishing was the only secret weapon behind the biggest data breach in the history? It’s true, as one of the Yahoo employees fell victim to a simple phishing attack and clicked one wrong link that let the hackers gain a foothold in the company’s internal networks.”

- The Hacker News
March 2017
Phishing / Account Theft

IN THE NEWS

“Who is Anthony... and why is Google suing him?”

“The lawsuit filed... accuses him of stealing 14,000 confidential files about [their] self-driving technology, including detailed designs of proprietary circuit boards and the laser ranging LiDAR systems, when he was employed there”

- The Hacker News
March 2017
Insider Theft

IN THE NEWS

“Hacking Attack Has Security Experts Scrambling to Contain Fallout.”

“The global efforts came less than a day after malicious software, transmitted via email and stolen from the National Security Agency, targeted vulnerabilities in computer systems in almost 100 countries in one of the largest “ransomware” attacks on record.”

- New York Times
May 2017
WannaCry Attack

2018 글로벌 위협 보고서

[시스템 계정 관리 현황]

- 20%의 조직은 권한 있는 계정의 **기본 암호를 변경한 적이 없습니다.**
- 30%의 조직은 **계정과 암호를 공유합니다.**
- 40%의 조직은 관리자 계정과 일반계정 계정에 대해 **동일한 보안권한을 사용합니다.**
- 50%의 조직은 권한 있는 계정 활동을 **감사하지 않습니다.**

2018 글로벌 위협 보고서

[시스템 계정 관리 현황]

- 70%의 조직은 **권한 있는 노출된 계정을 발견하지 못하고 있으며, 40%는 이러한 계정을 발견하기 위해 아무것도 하지 않습니다.**
- 55%는 직원이 **퇴사한 후 퇴사 직원의 액세스를 해지하지 못합니다.**
- 70%는 권한 계정에 대한 **비 인가자의 접근을 제한하지 못합니다.**
- 51%는 권한 계정에 대한 **보안 로그인 프로세스를 사용하지 못합니다.**

무엇이 문제인가?



- **80%** 의 보안 사고 모두 특권 계정과 관련!!!
- **54%** 의 기업에서 특권 계정 관리 위해 종이나 엑셀 사용!!!
- **특권 계정**
시스템(root), DBA, Network Admin, 어플리케이션 최고 관리자, 기업 소셜 계정 등

¹ The Forrester Wave: Privileged Identity Management, Q3 2016

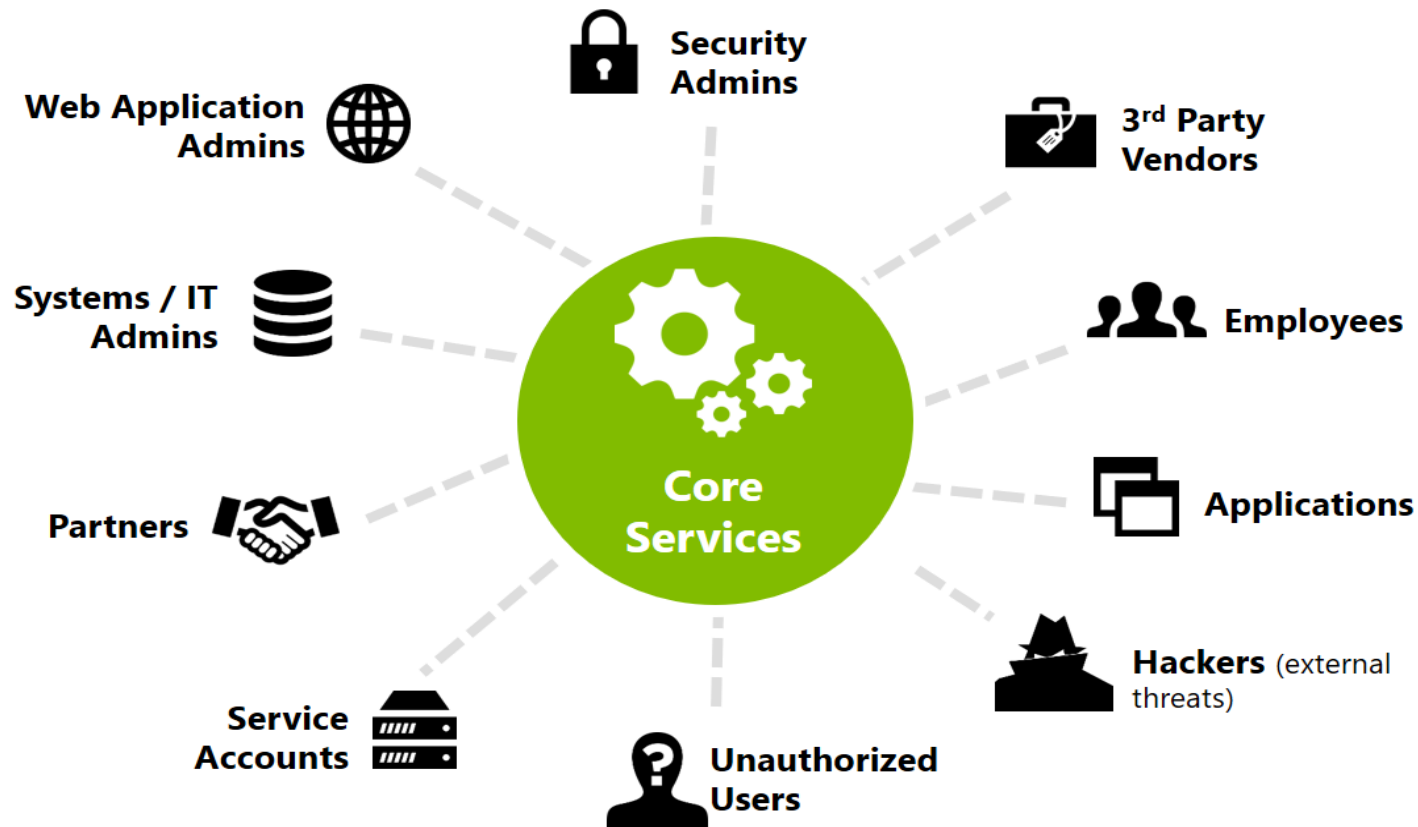
² Dimensional Research Global PAM Survey 2017

무엇이 문제인가?

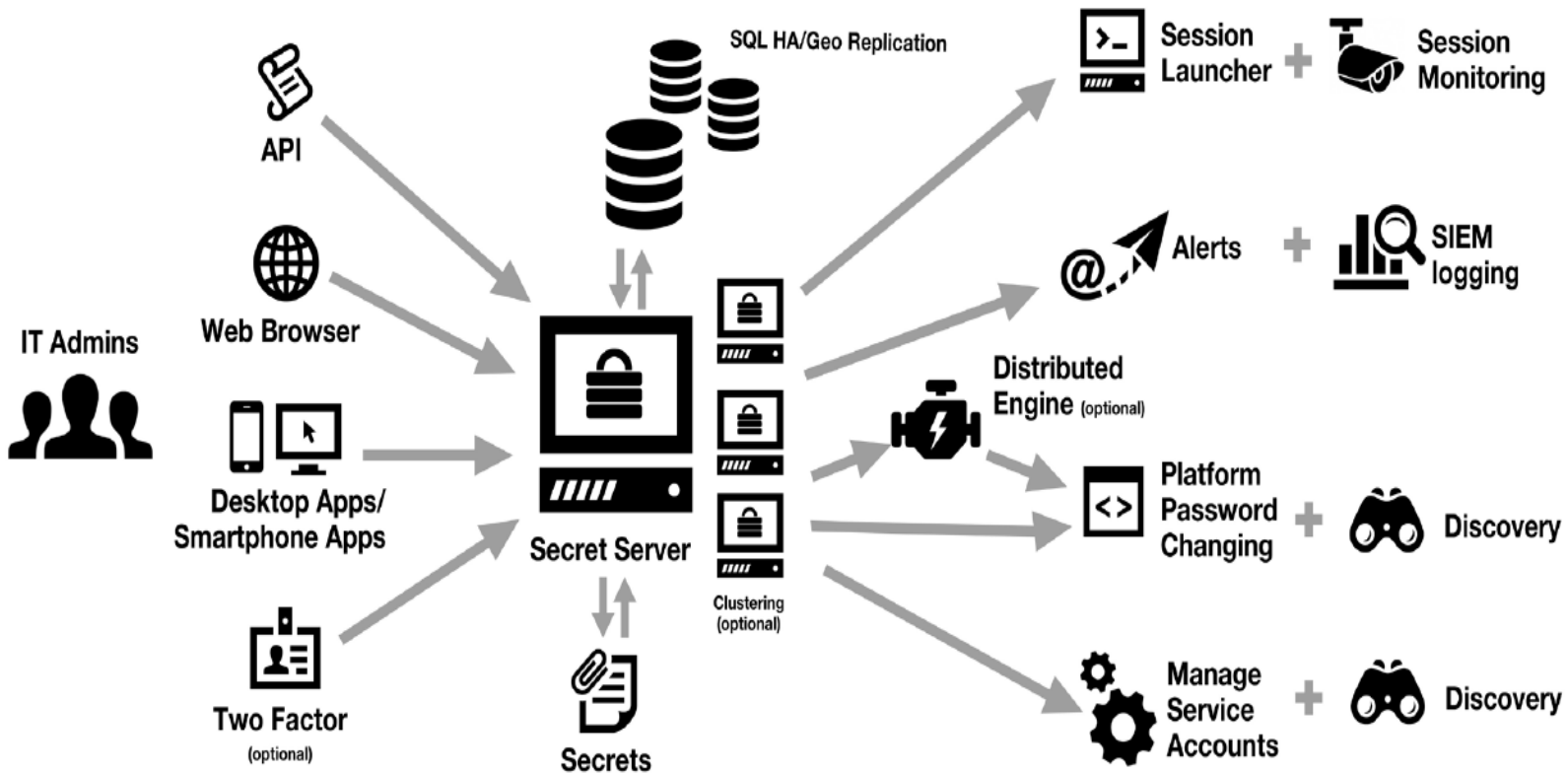


- 어디에 있는지 모르는, 관리되지 않는 특권 계정 존재
- IT 관리자들 사이에 특권 계정의 공유 사용.
- 비밀번호 혹은 SSH 키가 변경되지 않음.
- 멀티 팩터 인증이 강제화 되지 않음
- 대부분 작업에 과도하게 높은 수준의 특권 접근
- 어플리케이션 통제 미약

권한 계정 관리 및 통제 대상



권한 계정 관리 및 통제 방식



패스워드 변경 관리 대상 및 방안

- Secret Server는 규정 준수를 위해 일정에 따라 권한 계정 암호 변경을 자동화 합니다.
 - Secret Server의 기본 암호 변경 및 만료 일정은 관리자 정의에 의하여 변경 됩니다.
 - 일반적 IT 자산 패스워드 변경 지원이 내장되어 있으며 빠른 구축을 지원합니다.
-
- | | |
|--|---|
| <ul style="list-style-type: none">• Windows Local Administrator Accounts• Active Directory / LDAP• Microsoft SQL Server• Unix / Linux• VMWare ESXi• Cisco• Juniper• Blue Coat• Sybase• MySQL• Oracle | <ul style="list-style-type: none">• z/OS Mainframe• SAP• Cloud<ul style="list-style-type: none">- Google, Salesforce, Amazon, Office365• Any SSH, Telnet, or ODBC interface. |
| | <p>[Custom Integration]</p> <ul style="list-style-type: none">- AS/400, Linux / Mac, Check Point, Enterasys, Dell DRAC |



IBM의 사이버 공격 방어 전략!!!!

보다 더 안전한
패스워드 관리

보호 대상
엔드포인트

통제된
접근



권한 계정 통제 완벽한 기능 제공

쉬운 사용 | 완전한 E2E

권한 계정 관리

Secret Server

어플리케이션 권한 관리

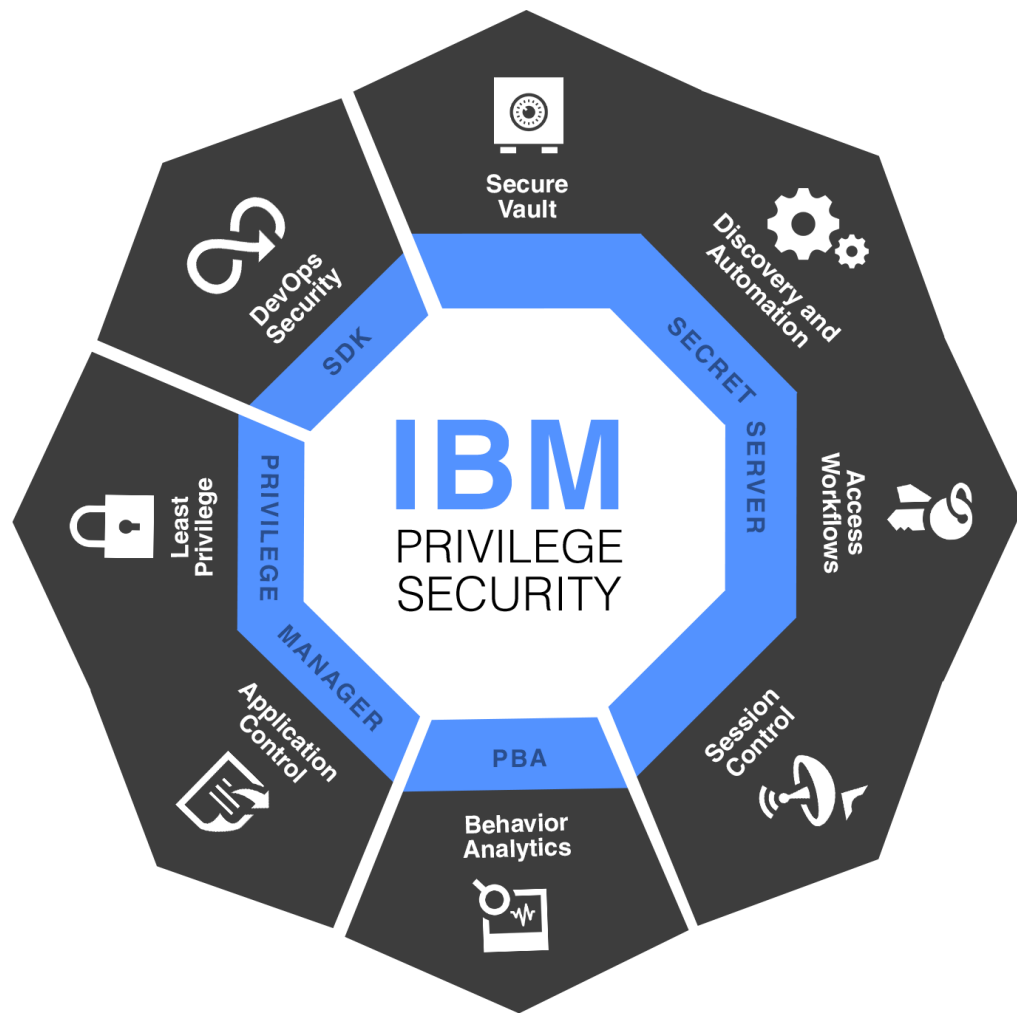
Privilege Manager

소프트웨어 개발 보안

SDK (인하우스
어플리케이션 연동)

내부자 위협 탐지

QRadar SIEM with UBA



Secret Server

권한 있는 계정을 빠르게 검색, 제어, 관리 및 보호합니다.



볼트 설정

보안 암호화된
볼트 권한 사용자,
및 구조 설정

탐지 수행

잠재된 모든 권한
계정을 검색 및
추적

비밀번호 보호

IBM Security
Secret Server 내에
민감한 계정 저장
및 패스워드
사용시/주기적
자동 변경

접근 위임

역할 기반 접근 통제,
요청 기반 접근 통제,
기타 통제 구현

세션 통제

세션 실행
모니터링, 추적,
종료 및 동영상
레코딩

IBM Secret Server /w IBM UBA

계정 사용 현황에 대한 레포트 및 비정상 활용에 대한 통지 지원



권한 계정
통제 수행

Secret Server
구축

BASELINE
설정

계정 사용 현황에
근거한 Baseline
설정 및 UBA
지표 수립

권한 계정
사용현황
모니터링

권한계정 사용
현황을 모두
모니터링하며
UBA 수행

위협 분석 및
통지

비 정상적 / 악성
행위 모니터링 시
보안 위협 내용
통지

세션 격리 및
위협 현황 조치

심각도에 따른
세션 격리 및
보안팀에 따른
세션 차단 및
증빙 검증



"I Couldn't Be Happier"

"The best privileged account security software and the support we need to solve our most pressing problems."

– Liz McQuarrie, Principal Scientist, Director of Security Operations, Adobe

RATED #1 ON CUSTOMER SERVICE

IBM Security Secret Server Customer Reference Sites

NETFLIX



NAVY



HONDA



NETFLIX



Adobe



2020년까지 PAM 시장 확대 요인



클라우드 환경 지원

- 고객 인프라의 클라우드 이전은 클라우드 환경 내의 가상 서버에 대한 접근 관리 영역에 있어 새로운 변화 요구
 - 접근 관리 솔루션의 클라우드 환경에서의 다양한 배치 아키텍처 지원
 - 가상 서버에 대한 접근 관리 지원
 - 클라우드 환경 하에서의 안전한 사용



복잡한 클라이언트 환경

- 윈도우 뿐만이 아니라, 맥 등 사용자 환경의 다각화는 서버 접근 관리 솔루션에 있어서도 도전 과제가 되고 있음.
- 서비스 계정에 대한 예외 처리 및 서비스 계정에 대한 다른 접근 방식 요구



늘어나는 권한 계정

- 서버 특권계정(Root)에서부터 데이터베이스, 네트워크, 어플리케이션, 소셜 계정에 이르기까지 관리해야 하는 특권 계정의 형태와 종류가 지속적으로 증가.
- 차세대 특권 계정 관리 솔루션의 필요성 대두

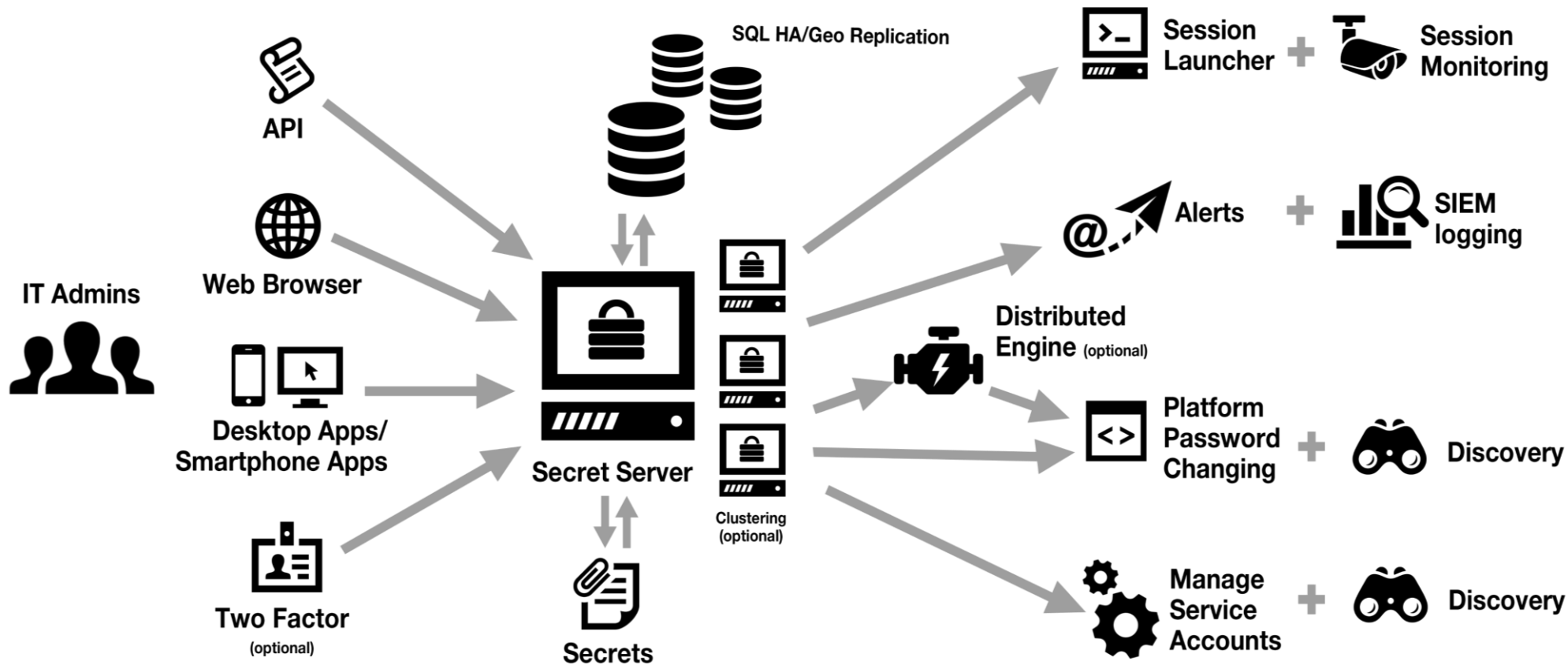


TECHNICAL DETAILS

IBM Secret Server



IBM Secret Server – Logical Architecture



Secret Server Login & Access Control

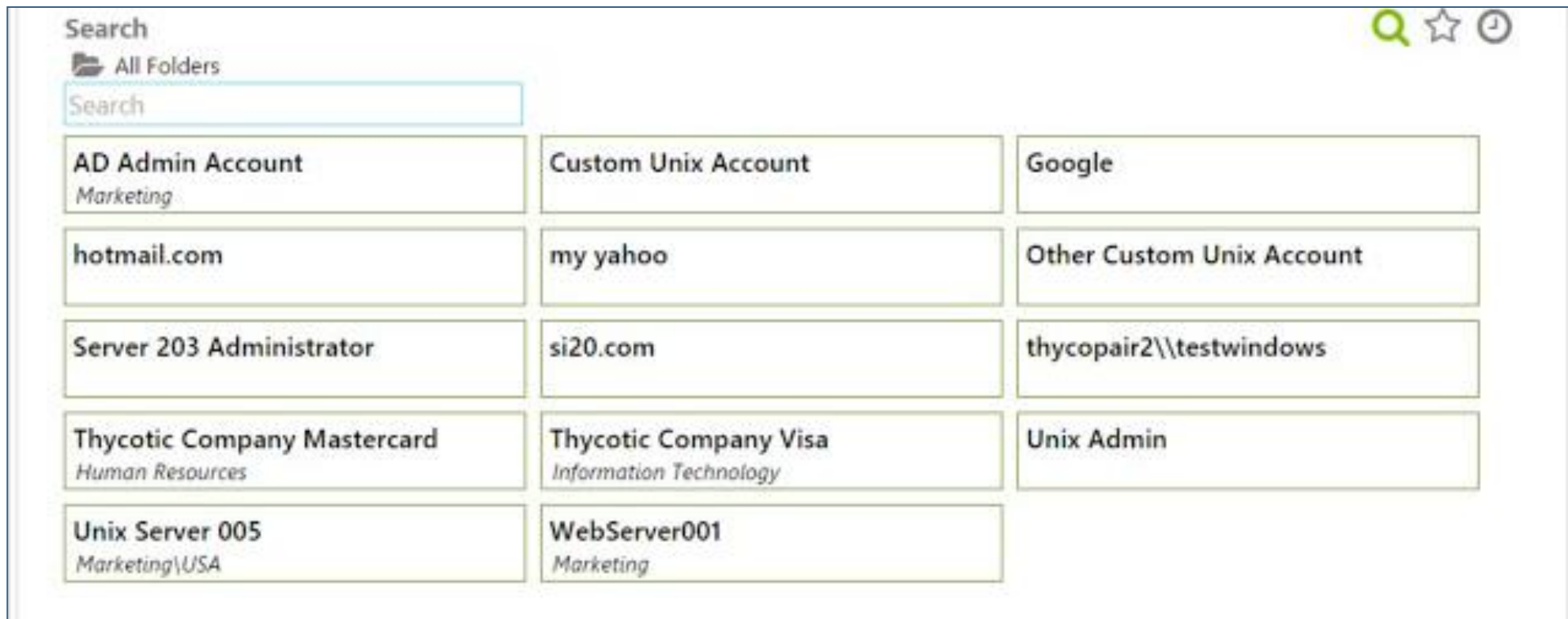
- 통합 관리 콘솔
 - 임직원
 - IT 관리자
- Secret Server 로그인 방법
 - Local account
 - AD Account (via AD Synch)
 - SSO via SAML Integration
- 2 Factor 인증
 - Hard tokens (RADIUS based)
 - Soft Token OTP
 - OATH Support
 - Email OTP
 - Duo Security
- Role Based Access Control

The screenshot displays the IBM Security Secret Server web interface. At the top, there is a navigation bar with a search box labeled 'Search Secrets', a 'Search' button, and links for 'HOME', 'TOOLS', 'ADMIN', and 'REPORTS'. On the right side of the navigation bar, there are icons for notifications, help, and user profile, along with the text 'Advanced | Basic' and a '+ Content' link.

The main content area is divided into several sections:

- Browse**: A sidebar on the left shows a folder tree under '< All Folders >' with 'Personal Folders' and 'Privileged Systems'. Below this is a 'Find Folder' search box and a note '(Drag a folder to create a tab.)'.
- Search in Privileged System**: A search bar with the text 'Advanced'.
- Secret List**: A table with columns 'Secret', 'Folder', and 'Template'. It lists two secrets: 'root' (Privileged Sy... Unix Account...) and 'secretsynch' (Privileged Sy... Active Direct...). Below the table, a detailed view of the 'secretsynch' secret is shown, including fields for 'Secret Name', 'Domain', 'Username', 'Password' (masked with asterisks), and 'Notes'. Action buttons 'View', 'Edit', 'Share', and 'View A' are present.
- Recent Secrets**: A section at the bottom left showing the 'secretsynch' secret.
- Create Secret**: A section on the right with a 'Create New' button and a dropdown menu '< Select >'. Below this are sections for 'Favorite Secrets' and 'Expired Secrets', each with a refresh icon and a trash icon.
- Welcome**: A section on the right with a refresh icon and a trash icon. It contains the text 'Import Secrets' and a paragraph about the 'Secret Server's Import feature' which simplifies integration with legacy systems and allows batch importing of secrets from Excel or CSV/Tab delimited files. It also mentions that multiple types of input data will need to be imported in several batches and that the 'Password Migration Tool' supports easy addition of existing secrets from other third-party password storing applications.

최종 사용자 화면



세션 레코딩 및 감사 방안

Session Playback Search

Search Filters

Search Across

Secret Name

Secret Items

Username

Hostname

Domain

Proxy Session Client Data

RDP Keystroke Data

RDP Application Name

Date

Last 30 Days

Status

All

Launcher Type

All

Users

Search Users

Groups

Search Groups

Everyone

Search for Sessions

Search

10.0.0.243\winuser2 - Accessed By ssadmin Remote Desktop · 4/11/2017 05:46 PM· 0:10:03 win-h0ko2iq58no · ssadmin View Secret	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop · 4/11/2017 05:41 PM· 0:00:59 win-h0ko2iq58no · user282 View Secret	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop · 4/11/2017 05:35 PM· 0:01:44 win-h0ko2iq58no · user282 View Secret	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop · 4/11/2017 05:35 PM· 0:00:11 win-h0ko2iq58no View Secret	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop · 4/11/2017 05:33 PM· 0:00:00 win-h0ko2iq58no View Secret	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop · 4/11/2017 05:19 PM· 0:00:32 win-h0ko2iq58no · user282	

세션 레코딩 및 감사 방안 (계속)

Watch Session Recording

Session Summary

Session Secret: <None>

Machine: Win-1654rotttdte

Launcher User: Administrator

Launcher Used: <None>

Session Start: 3/22/2017 12:27 PM

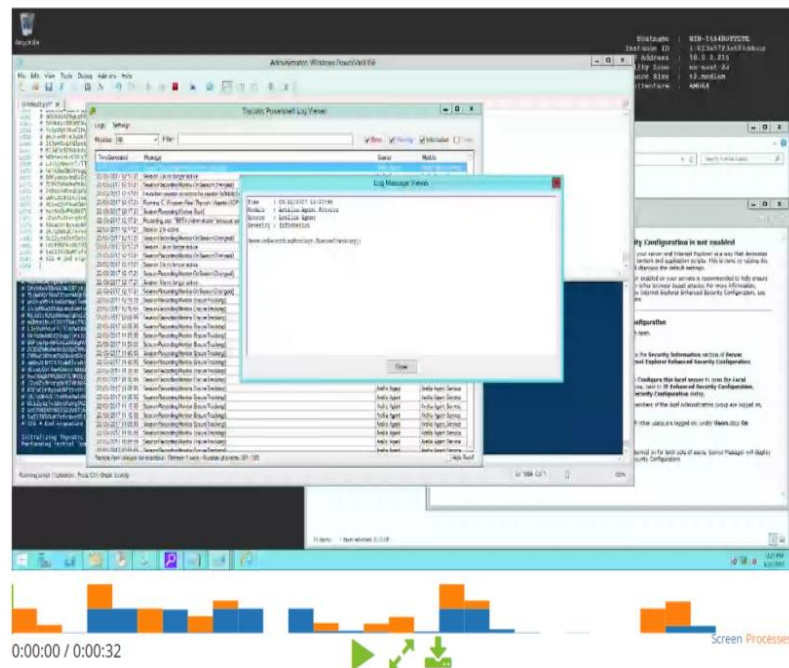
Session End: 3/22/2017 12:28 PM

Search Session Activity

Activity Type: All

Keyword:

Elapsed	Type	Activity	Jump To
00:00:00		powershell_ise	
00:00:00		ieexplore	
00:00:00		mmc	
00:00:00		csrss	
00:00:00		explorer	
00:00:00		Thycotic.SessionRecorder	
00:00:00		notepad	
00:00:00		mmc	
00:00:00		taskhostx	
00:00:00		powershell_ise	
00:00:00		TSTheme	
00:00:00		winlogon	
00:00:00		rdpclip	
00:00:00		notepad	
00:00:00		ieexplore	



다양한 사용자 환경 지원: Windows & MAC

General Personalize Expiration Security Remote Password Changing Dependencies

Secret Name mydomain\administrator
Domain mydomain.local
Username administrator
Password *****
Notes
Status Active
Folder \My Domain
Expiration Expires in 1 days. (Expires every 30 day(s))
Last Heartbeat Success (12/12/2013 01:29 PM)
Favorite? ☐

 **RDP Launcher**  **PuTTY Launcher**

General Settings

Launcher Name SecureCRT
Active Yes
Launcher Image 

Windows Settings

Process Name
[How do I configure process arguments?](#)
Process Arguments
Run Process As Secret Credentials No
Load User Profile No
Use Operating System Shell No

Mac Settings

Process Name /Applications/SecureCRT.app/Contents/MacOS/SecureCRT
[How do I configure process arguments?](#)
Process Arguments /T /SSH2 /PASSWORD \$PASSWORD \$USERNAME@\$MACHINE

[Back](#) [Edit](#) [View Audit](#)



THANK YOU

FOLLOW US ON:

 ibm.com/security

 securityintelligence.com

 ibm.com/security/community

 xforce.ibmcloud.com

 [@ibmsecurity](https://twitter.com/ibmsecurity)

 youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2018. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. 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.