IBM Security

실전! 하이브리드 서버 접근 관리

IBM SECURITY SECRET SERVER

박형근 실장(phk@kr.ibm.com)

2019

IBM

IBM의 멀티 클라우드 보안 전략

box CONCUR Google Apps Office 365 salesforce workday.

IBM Cloud amazon web services™ Microsoft Azure vmware

데이터 보호

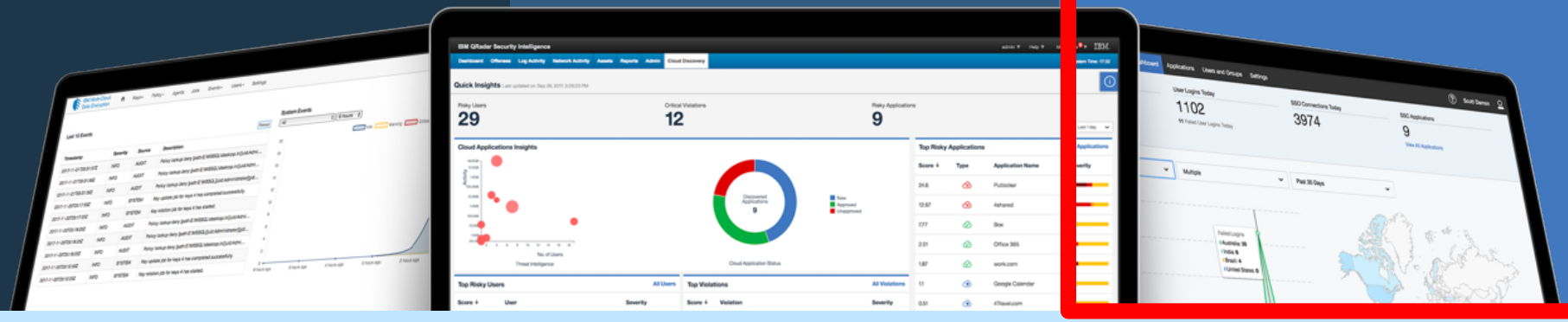
IBM Multi-Cloud Data Encryption
IBM Guardium Data Protection
IBM Guardium Analyzer

가시성 확보

IBM QRadar Security Intelligence Platform

접근 권한 관리

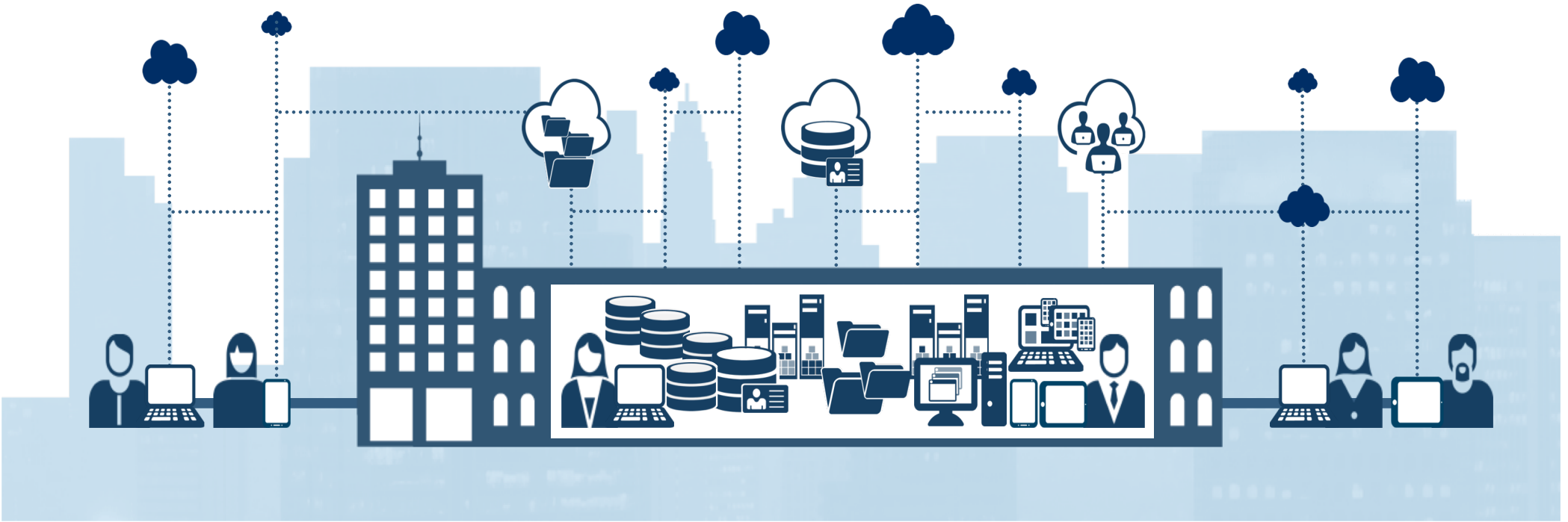
IBM Cloud Identity
IBM Security Identity and Access Assurance
IBM Security Secret Server



각 클라우드 서비스 제공자가 제공하는 내제된 기본 보안 옵션

클라우드 상의 계정 및 접근(권한) 관리가

전통적으로 해 왔던 것과 얼마나 다를까요?



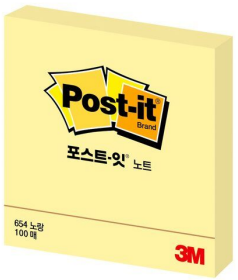
무엇이 문제인가?

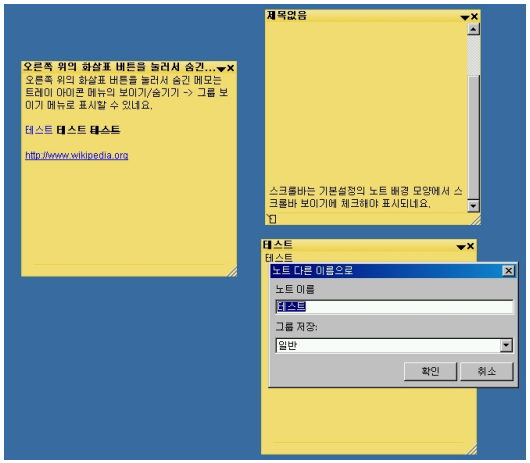
- 어디에 있는지 모르는,
  관리되지 않는 특권 계정 존재
- IT 관리자들 사이에 특권 계정과
  패스워드의 공유 사용.
- 사용자 책임 추구성 및 행위에 대한
  근거 자료 확보 어려움.
- 패스워드 혹은 SSH 키가 변경되지
  않음.
- 멀티 채널 인증이 강제화되지 않음

중요 계정에 대한 패스워드는 어떻게 관리하고 있나요?

54% 기업에서 특권 계정 관리 위해 종이나 엑셀 사용!!!

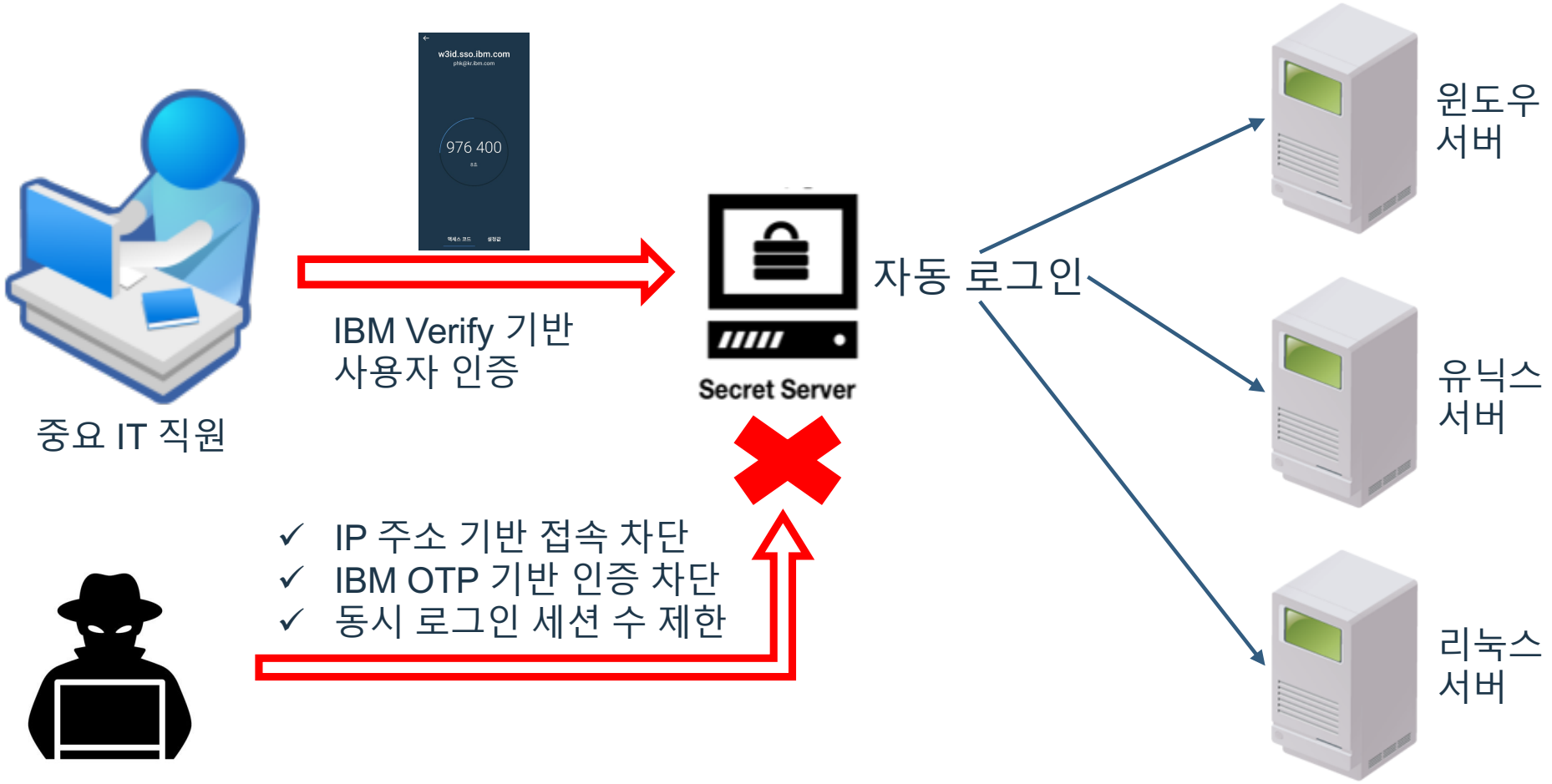
중요 IT 직원





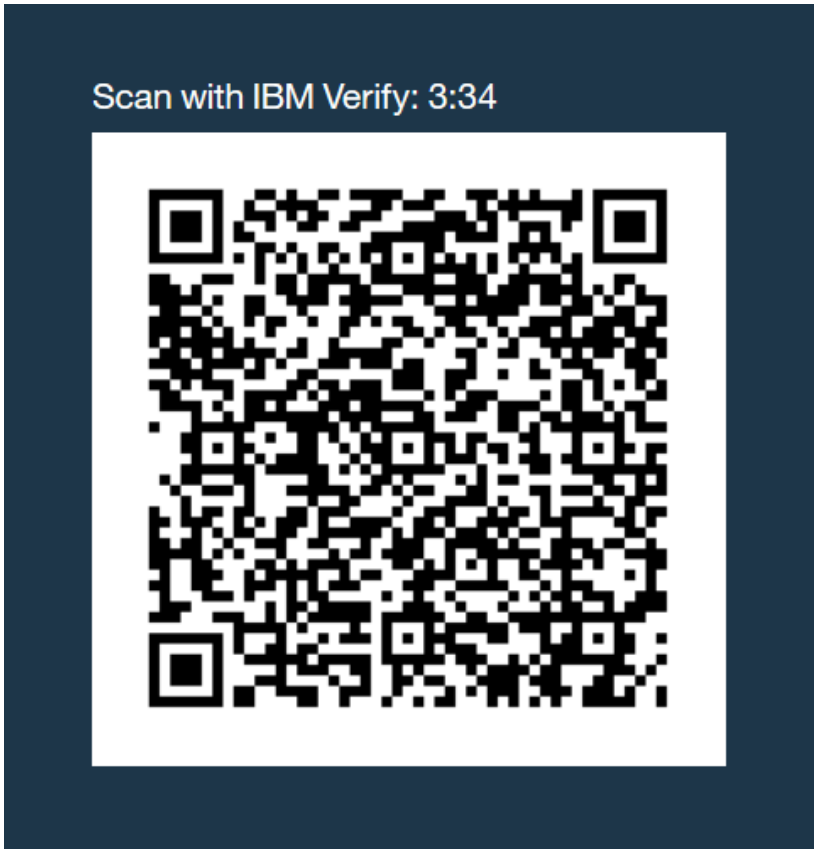
모든 패스워드에 대한 관리는 IBM Security Secret Server로

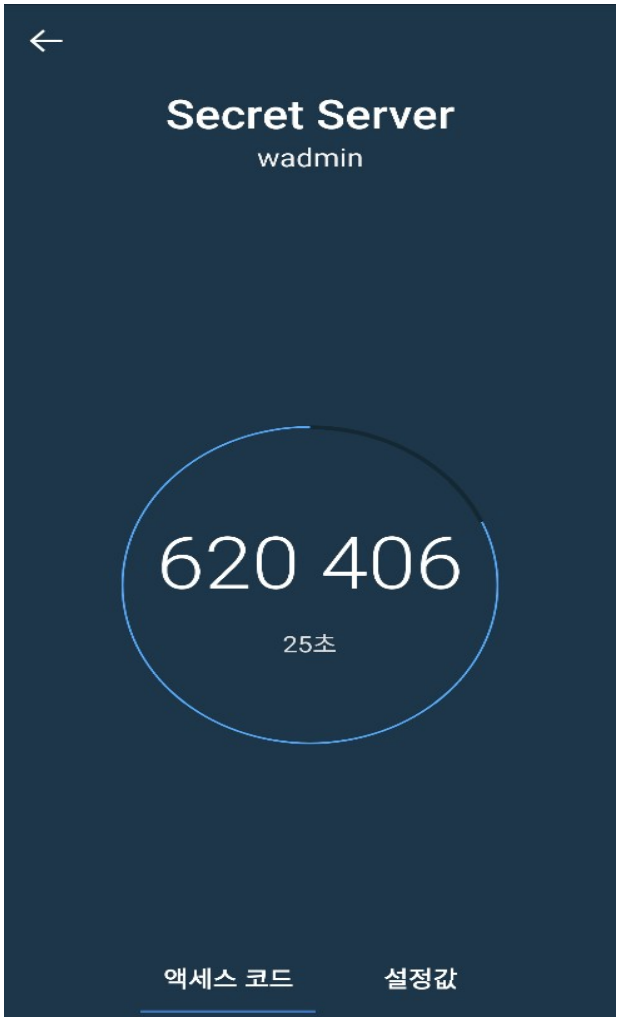
IBM Security Secret Server에 IBM Verify 모바일 OTP 기반으로 로그인해서 권한 있는 시스템에 자유롭게 사용해 주세요. 대상 시스템의 자동 로그인도 지원합니다.



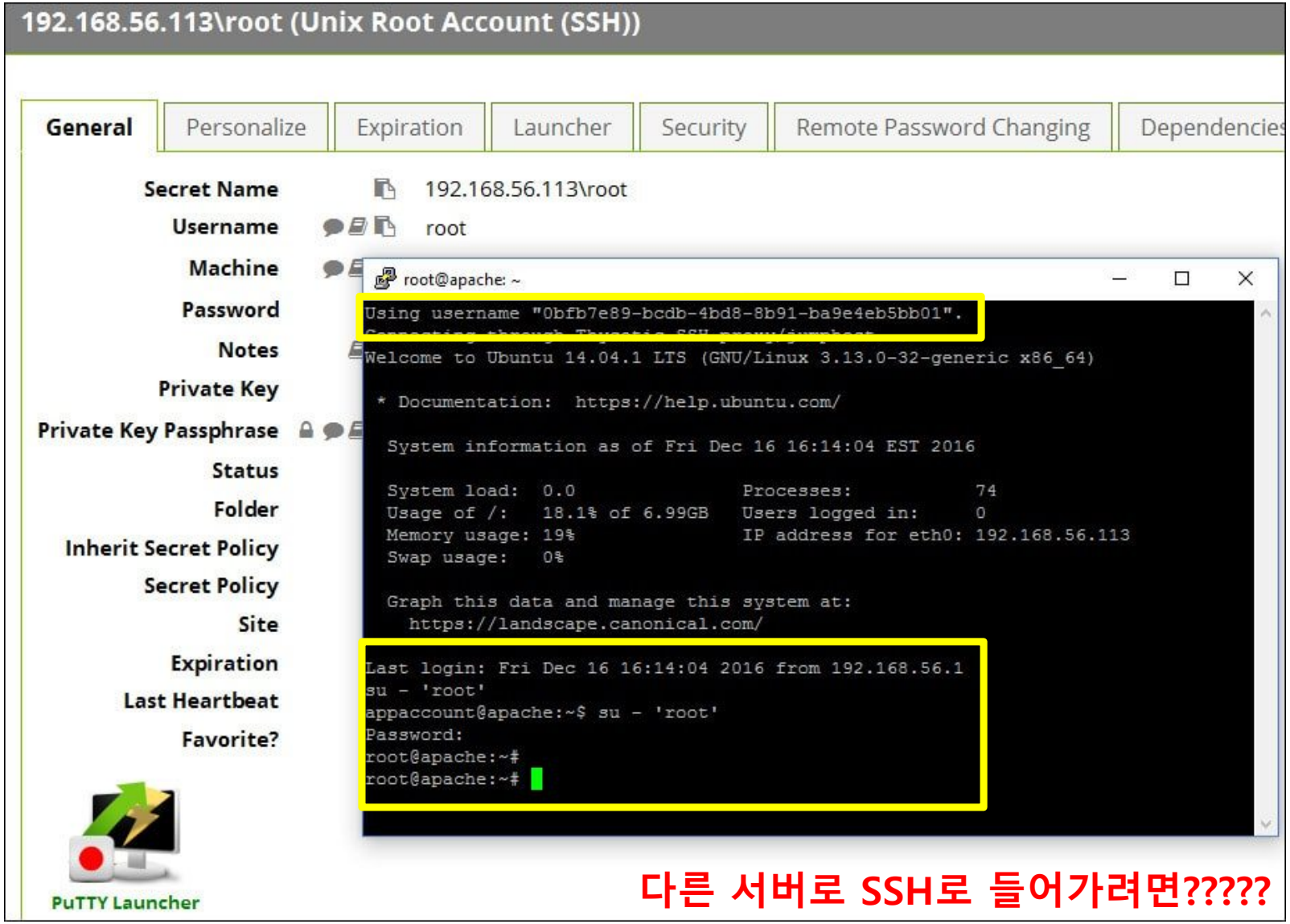
2채널 기반 인증으로 인증 강화!!

서버 접근 관리 시스템의 인증은 보안상 매우 중요하므로, 최소한 2채널(PC + 스마트폰 등) 인증 기반으로 강화해야 합니다.

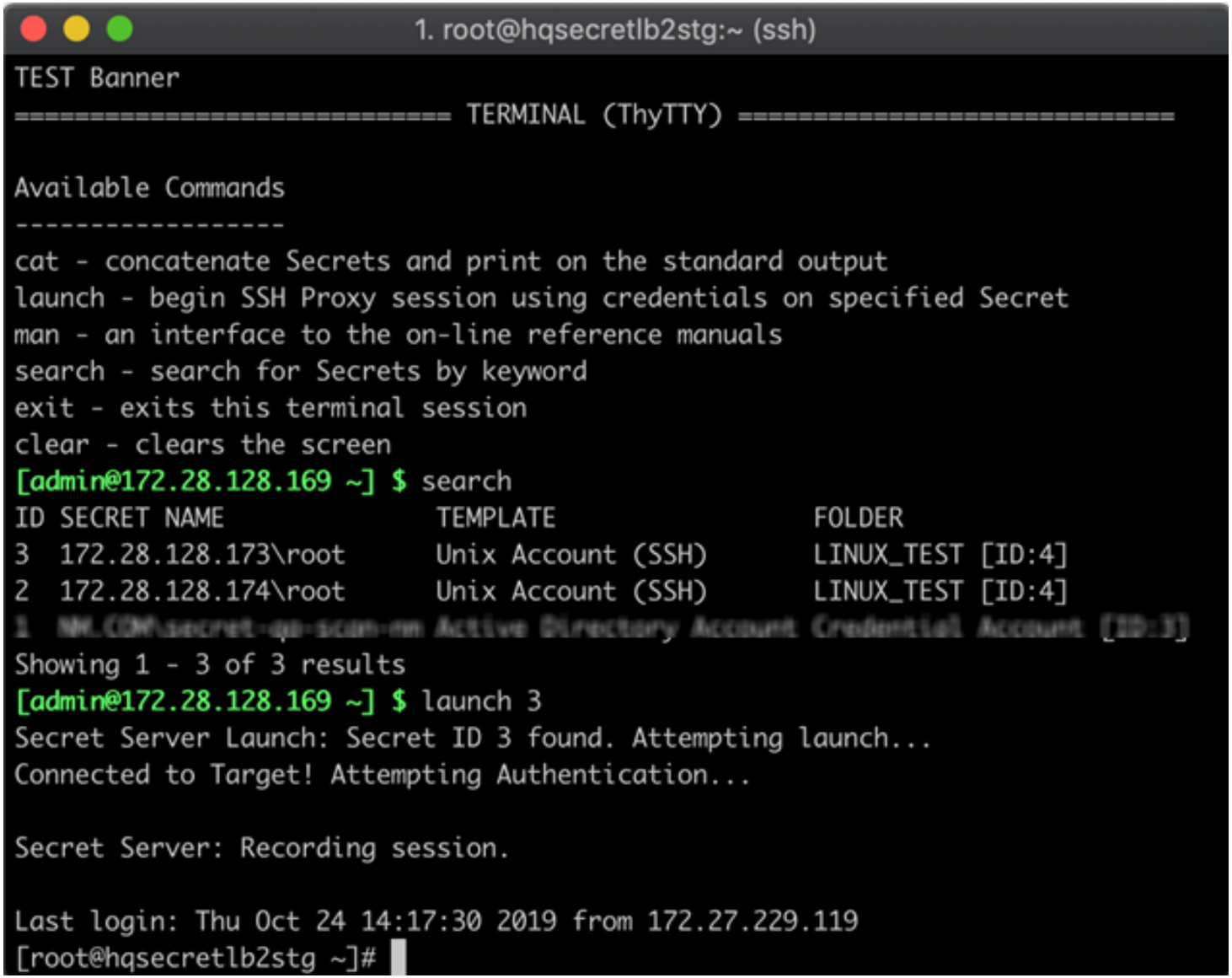




패스워드 공유와 노출에 대한 이슈 해결



SSH Terminal



점점 더 강화되는 패스워드 관련 법 규제 사항

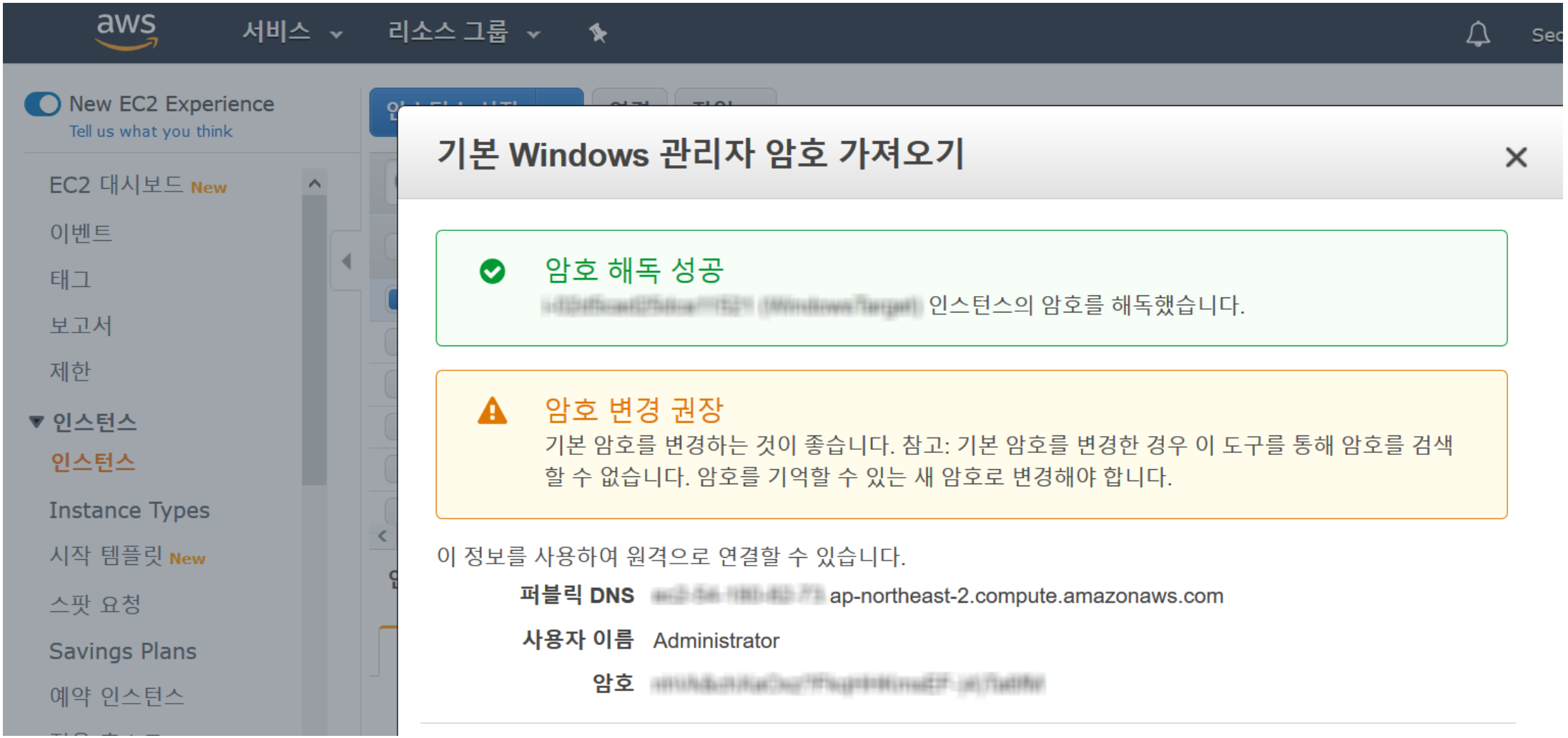
주기적인 패스워드 변경과 복잡한 패스워드 규칙

중요 IT 직원

- ✓ 주기적인 패스워드 변경:
  한달에 한 번, 분기에 한 번
- ✓ 복잡한 패스워드 규칙:
  영숫자특수문자 혼용, 12자리,
  이전 사용 패스워드 불가 등
- ✓ 패스워드 변경에 대한 감사
  데이터?

서버, 데이터베이스 등

기본 암호(Default Password) 사용????



패스워드와 SSH 키에 대한 자동 변경 관리 제공

스케줄과 정책 기반으로 대상 시스템에 대한 패스워드와 SSH키를 주기적으로 변경 관리하며 변경 이력을 제공합니다.

중요 IT 직원

주기적 자동
패스워드 변경

윈도우
서버

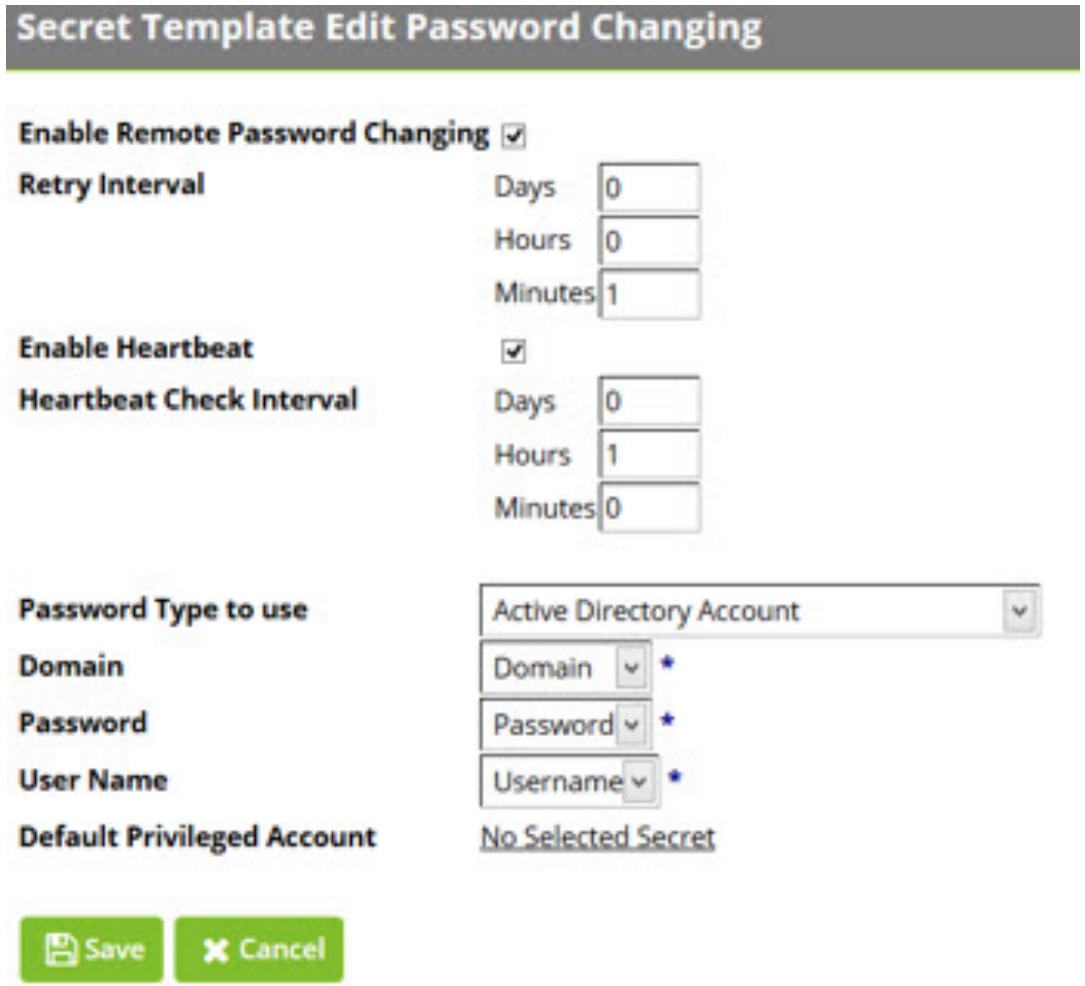
유닉스
서버

리눅스
서버

이제 패스워드 변경 관리로부터 자유로워지세요.
보다 중요한 업무에 집중하시고, 패스워드 변경 이력에 대한 감사 보고서도 바로 제공 가능합니다.

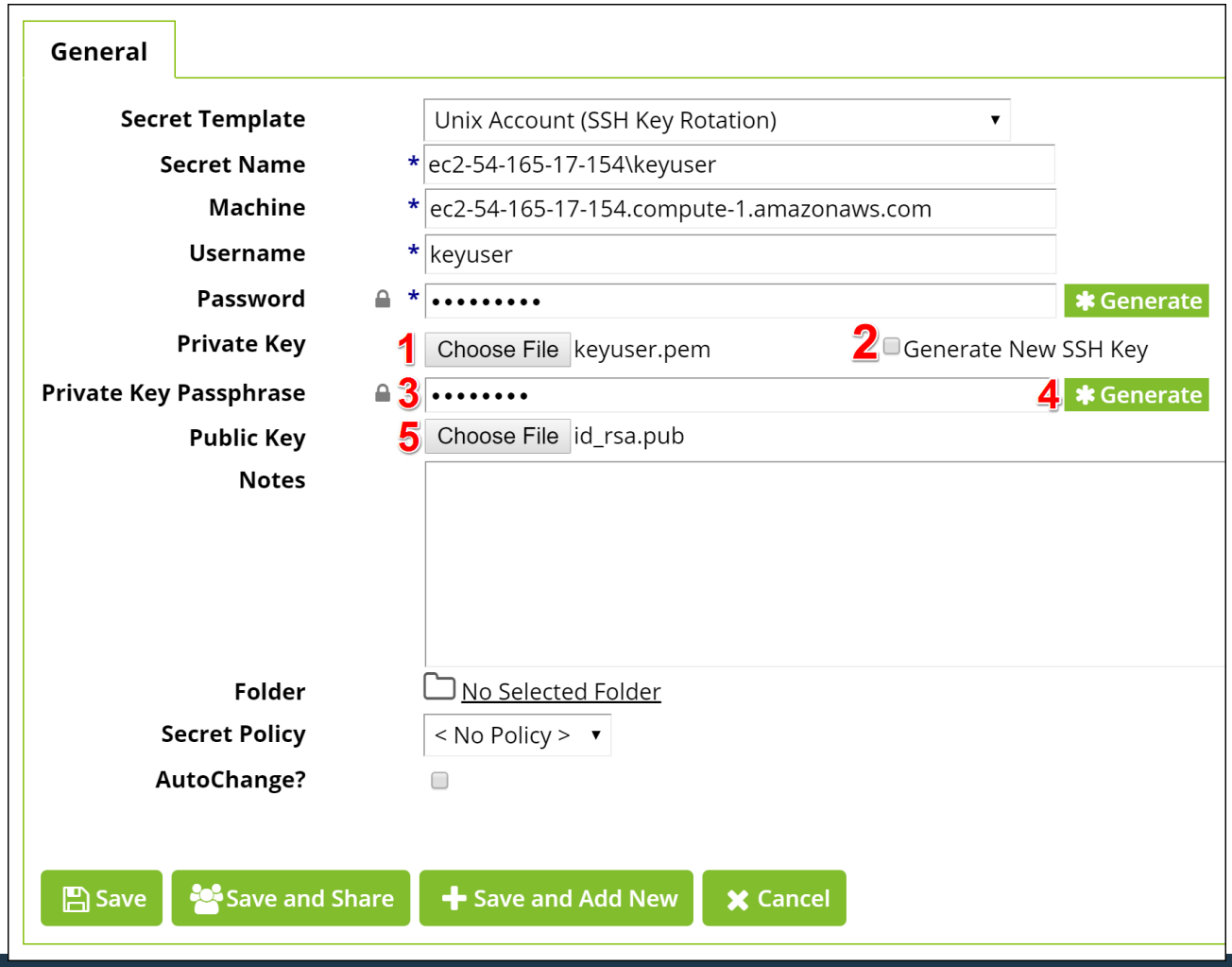
로컬/도메인 계정의 자동화된 패스워드 변경 관리

IBM Security Secret Server 10.x는 로컬/도메인 계정의 자동화된 패스워드 변경 관리를 지원합니다.



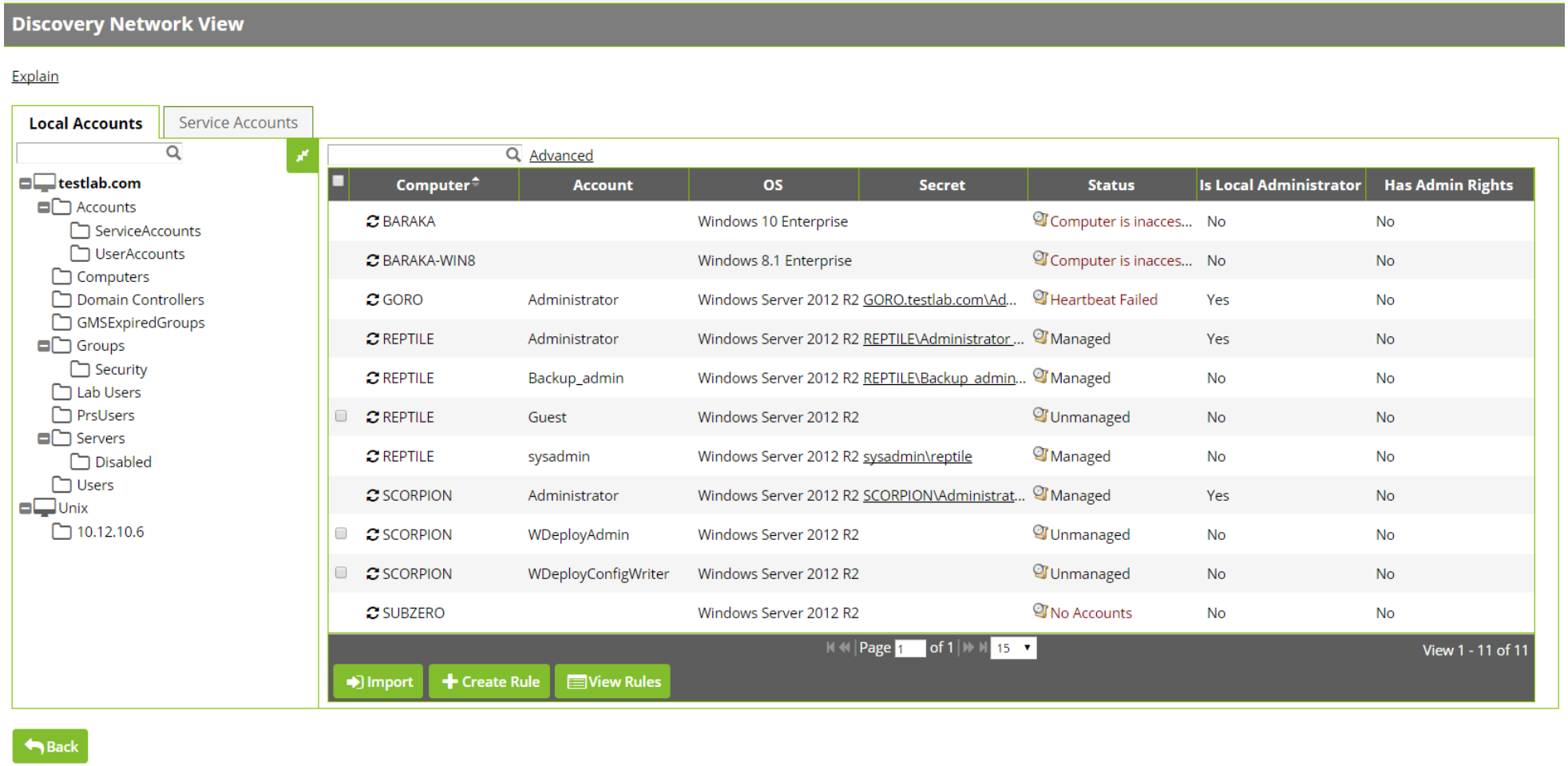
키 기반 인증 방식의 SSH 프로토콜 접근 지원

IBM Security Secret Server 10.x는 SSH의 키 기반 인증 방식을 지원하며 자동화된 SSH 키 Rotation도 지원합니다.



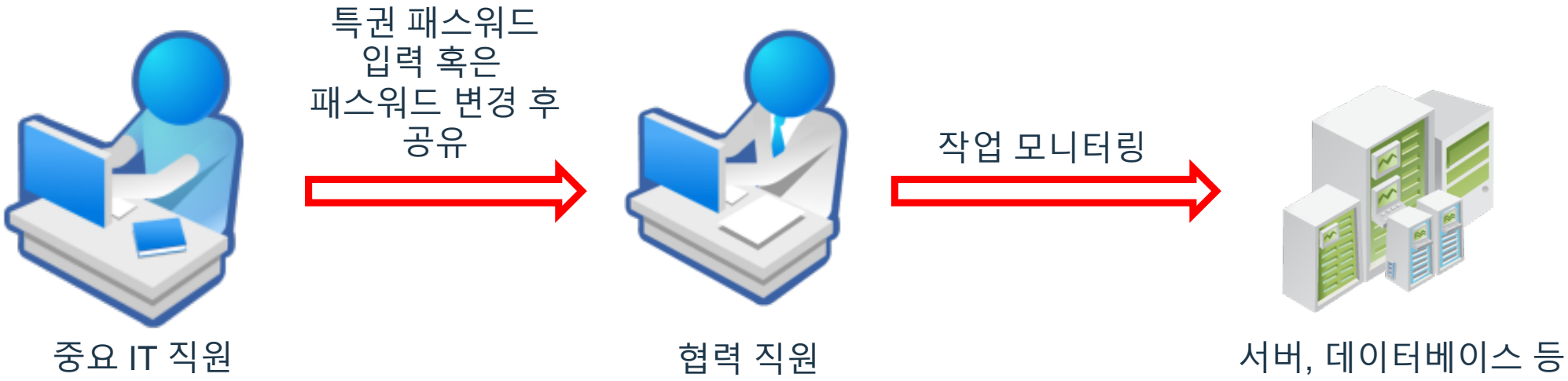
미식별 자산의 자동화된 식별 및 분류 기능

IBM Security Secret Server 10.x는 Active Directory와 연계하거나, 스캐닝 기반으로 미식별된 자산의 자동화된 식별 후, 특권 계정을 탐지하여 자동 등록처리합니다.



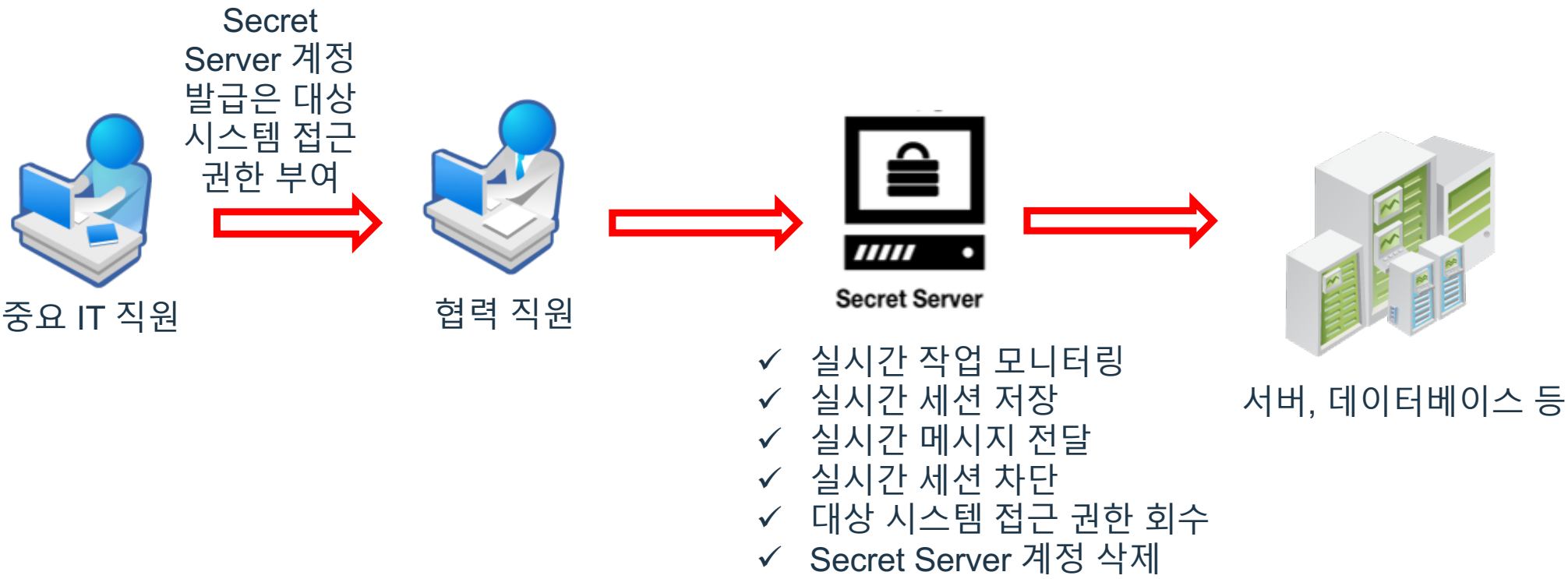
협력직원과의 중요 시스템 작업은 어떻게?

패스워드 입력부터 작업 모니터링까지???



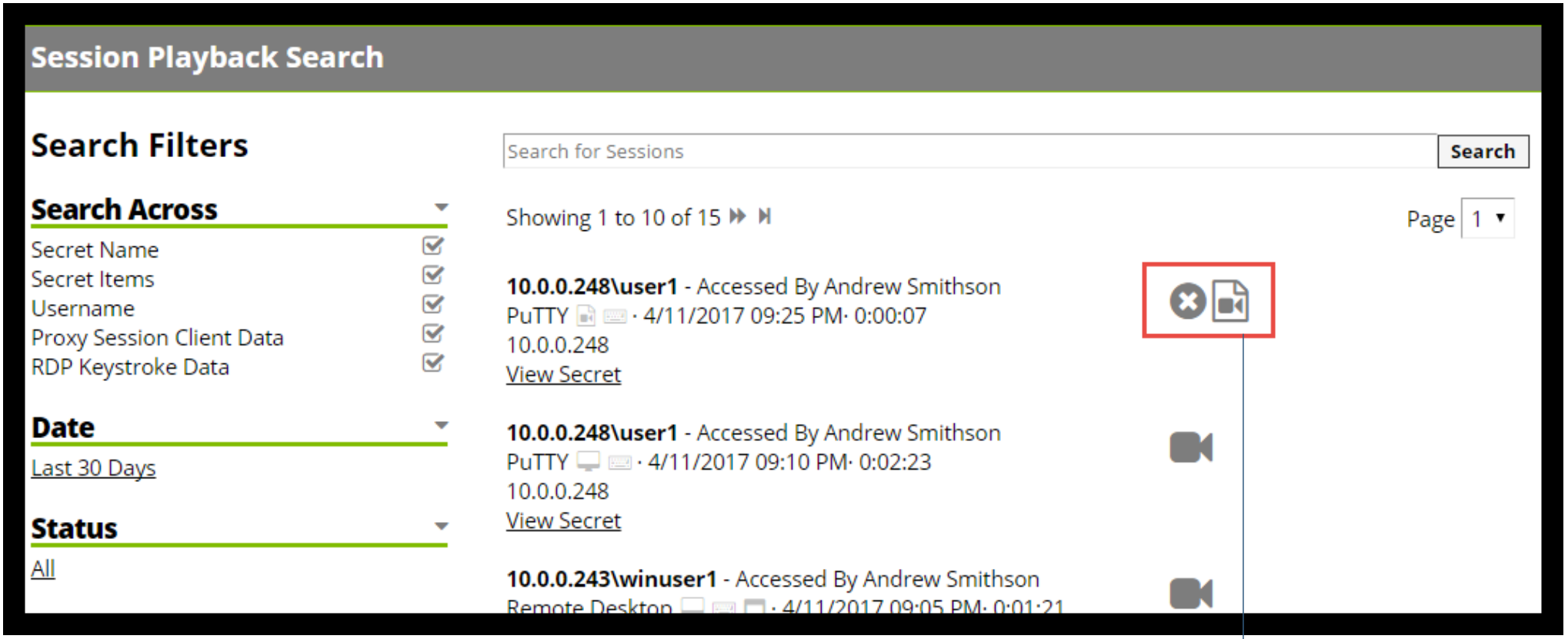
협력업체의 중요 시스템 작업도 원격에서 모니터링하세요!!

임시 계정 발급부터 작업 모니터링과 작업 내용 저장까지. 이 모든 사항을 원격에서 관리할 수 있습니다.



실시간으로 사용자의 원격 접근 세션 차단

IBM Security Secret Server 10.x는 SSH Proxy에 접속한 SSH 혹은 RDP를 사용하고 있는 사용자를 실시간으로 모니터링 및 원격 접근 세션 차단을 지원합니다.



실시간 세션에 대한 표시와 함께 세션 차단 아이콘 제공

세션 레코딩 및 사용자 행위 검색

Watch Session Recording

Session Summary

Session Secret: < None >
Machine: Win-16S4rottdte

Launcher User: Administrator
Launcher Used: < None >

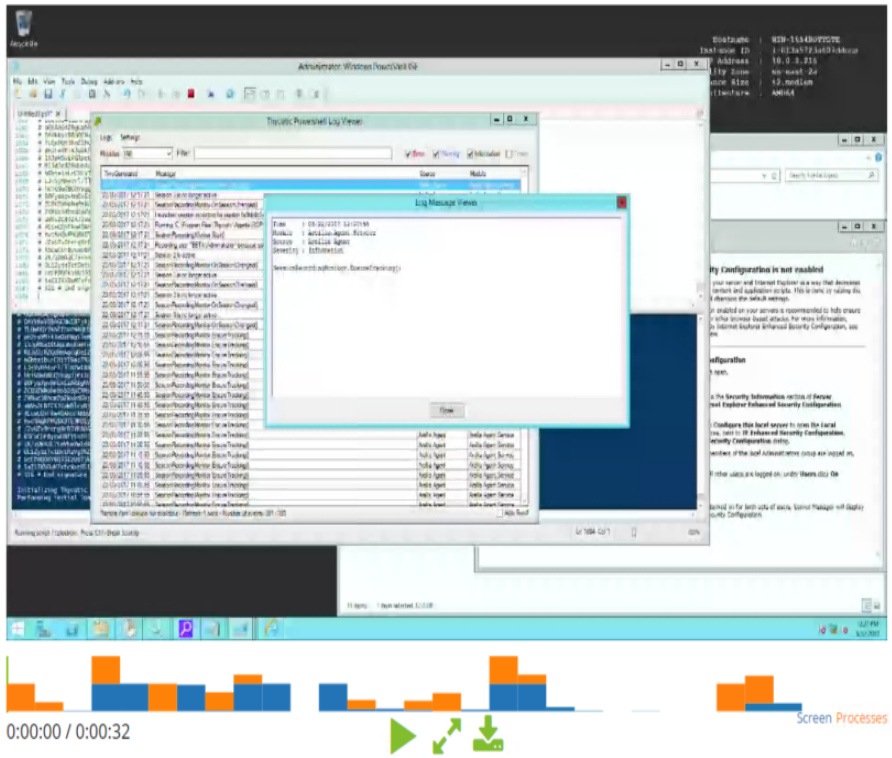
Session Start: 3/22/2017 12:27 PM
Session End: 3/22/2017 12:28 PM

Search Session Activity

Activity Type: All

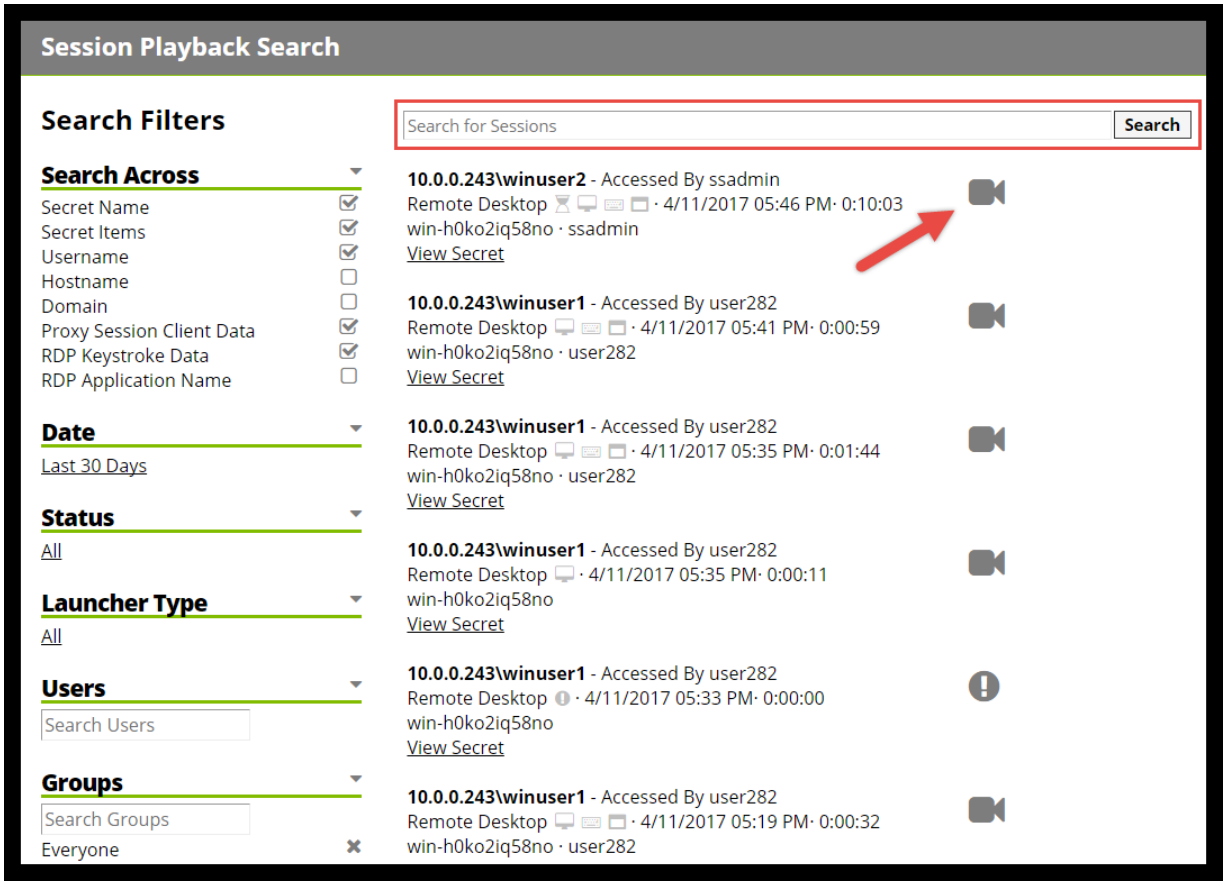
Keyword:

Elapsed	Type	Activity	Jump To
00:00:00		powershell_ise	
00:00:00		iexplore	
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		taskhostex	
00:00:00		powershell_ise	
00:00:00		TSTheme	
00:00:00		winlogon	
00:00:00		rdpclip	
00:00:00		notepad	
00:00:00		iexplore	



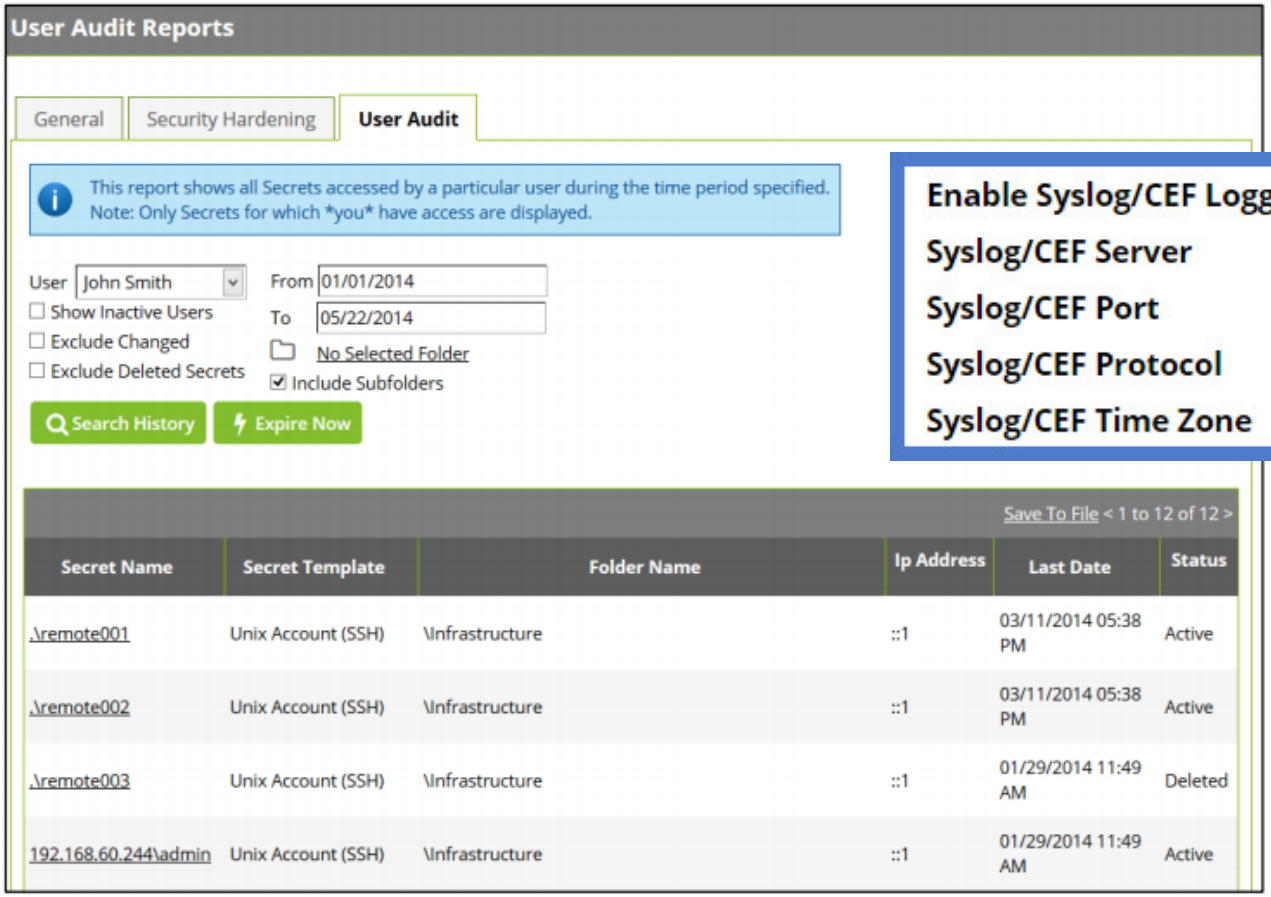
모든 작업 내용 및 결과는 암호화 기록되고, 관리자가 쉽게 검색할 수 있는 형태로 기록

IBM Security Secret Server 10.x는 모든 작업 내용 및 결과는 영상 기록되며, 관리자가 키워드 입력 혹은 필터를 통해 보다 쉽게 검색할 수 있습니다.



감사로그 및 스케줄 리포트 지원, 외부 SIEM/ESM 장비와 연동

IBM Security Secret Server 10.x는 감사로그 및 스케줄 기반 리포트 기능을 지원하며, IBM Security QRadar, Splunk, ArcSight 등과 기본 연동되며, 그외 3rd-party SIEM 및 ESM 장비와의 연동 위해 Syslog/CEF 기반 로그 전송을 지원합니다.

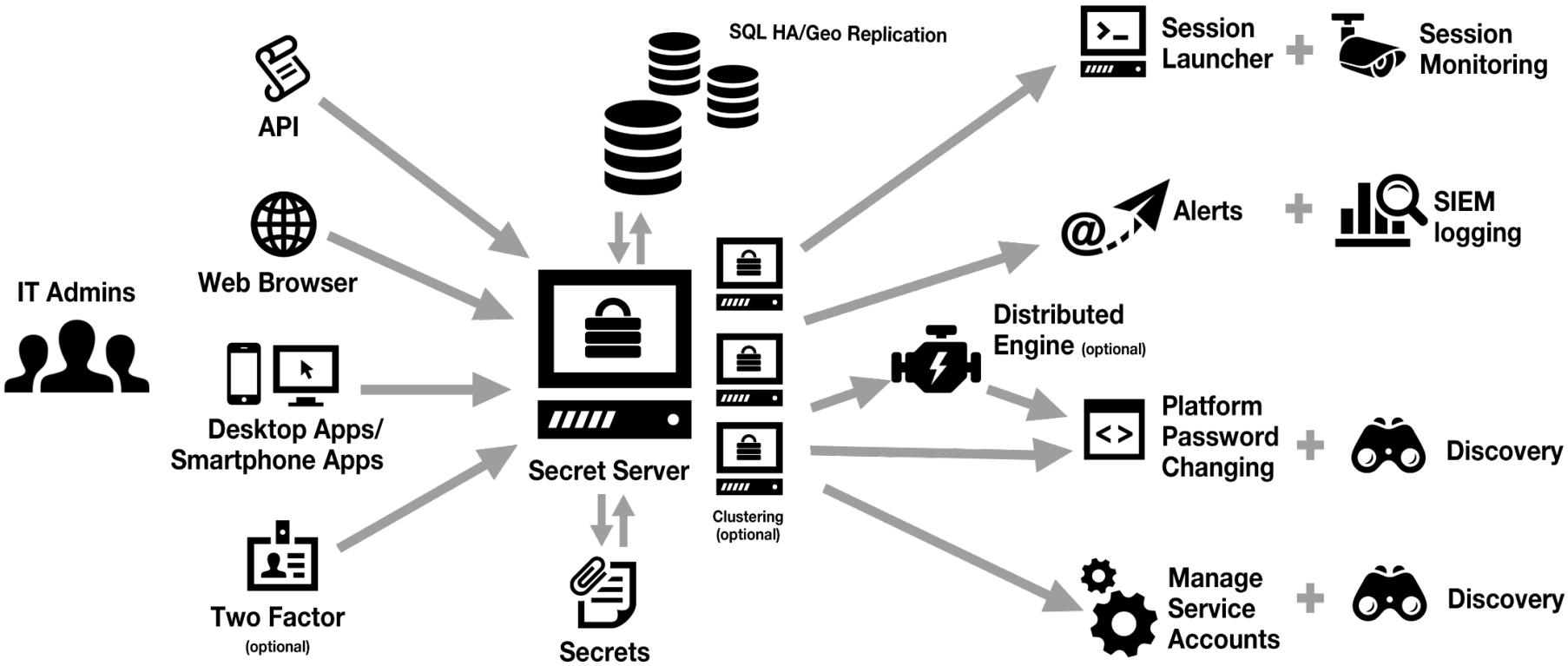


Enable Syslog/CEF Logging	Yes
Syslog/CEF Server	Syslog.Example.com
Syslog/CEF Port	6514
Syslog/CEF Protocol	SECURE TCP
Syslog/CEF Time Zone	Server Time

Syslog/CEF 설정 화면

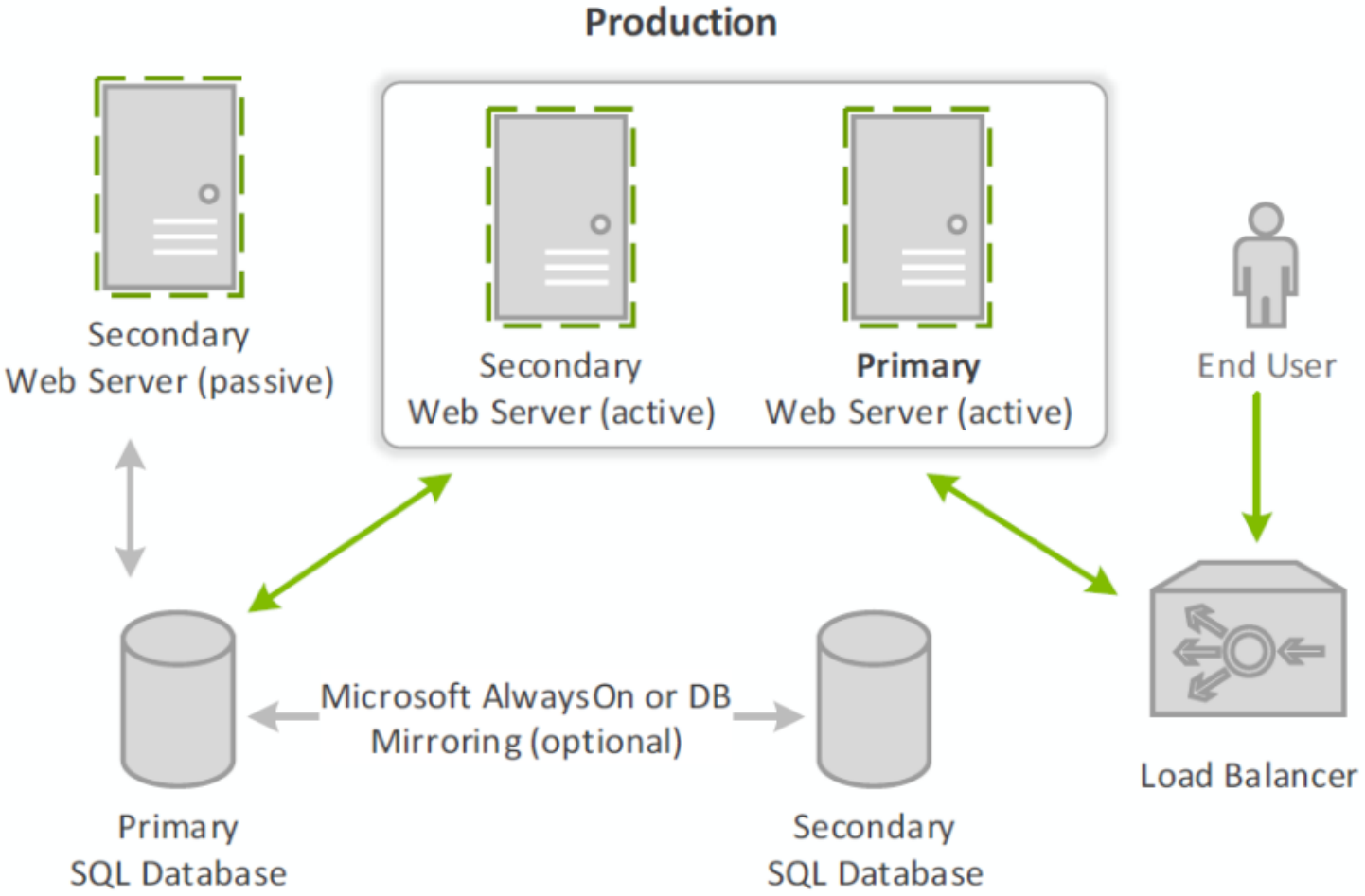
구축 환경은 관리 서버의 On-Premise 구성과 대상 시스템의 Agentless 방식 지원

IBM Security Secret Server 10.x는 Windows Server 2008 R2 SP1 이상, Windows Server 2012 /2019 이상 설치 운영되며, 대상 시스템에는 Agent 없이 운영됩니다.
SSH/RDP Gateway와 사용자 PC 상의 Protocol Handler Launcher 모듈로 전체 기능을 제공합니다.

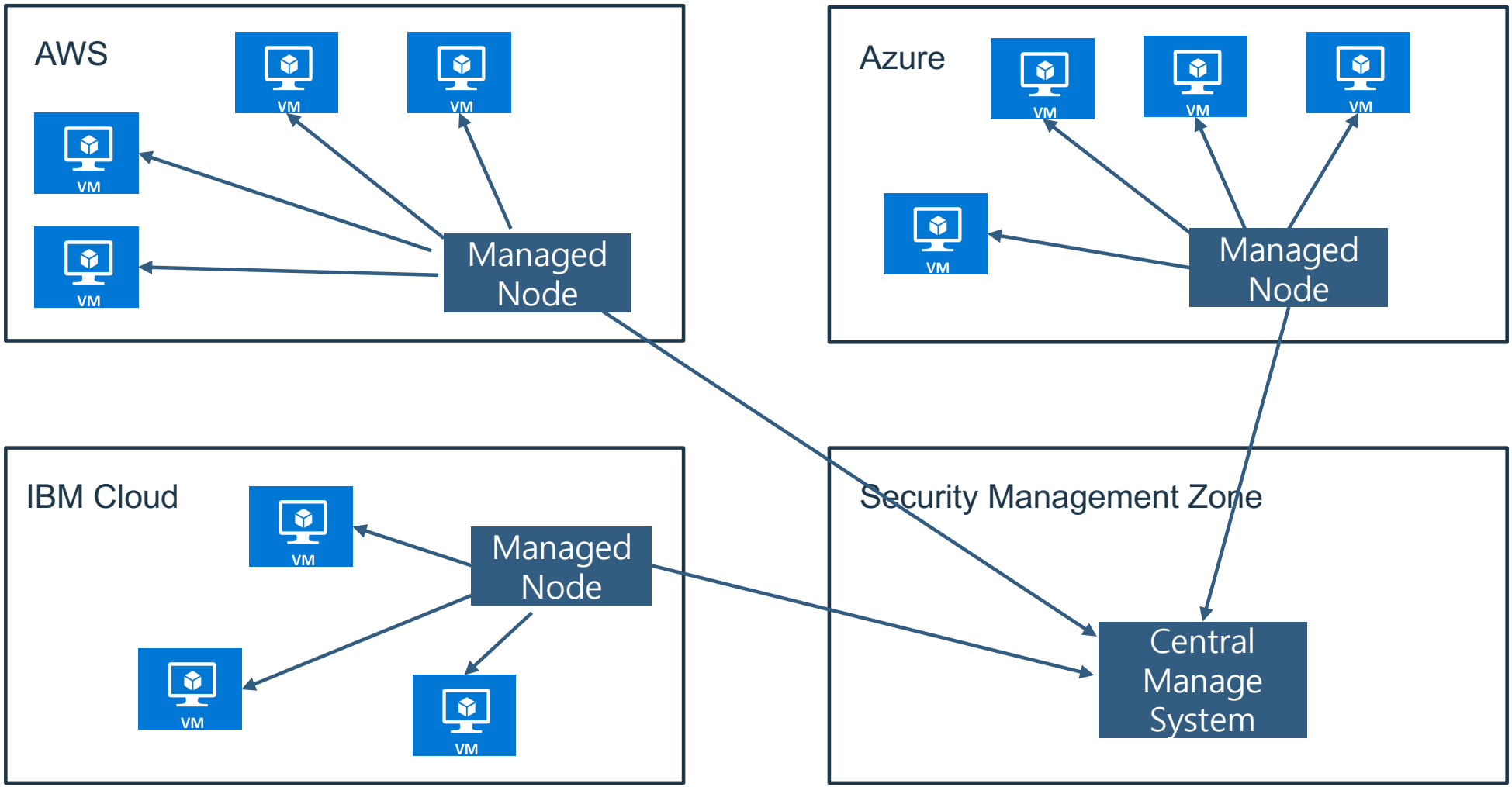


이중화 등 서비스 가용성 확보 위한 기능 제공

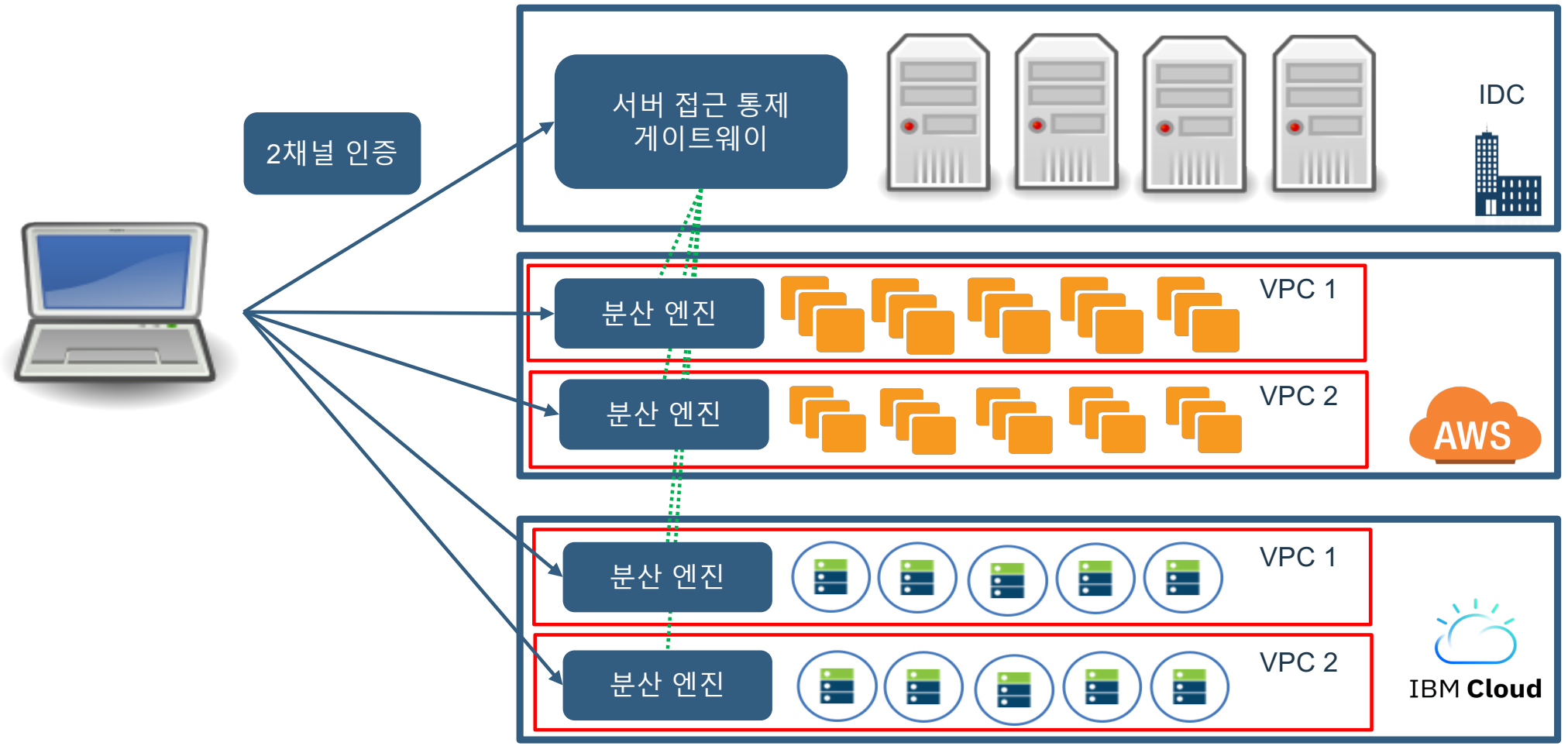
IBM Security Secret Server 10.x는 서비스 가용성 확보를 위한 이중화 및 다중화 구성을 지원합니다.



하이브리드 분산 클라우드 환경 하에서의 보안 관리



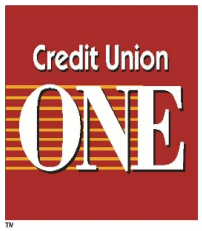
하이브리드 & 멀티 클라우드에 대한 서버 접근 관리
- IBM Security Secret Server

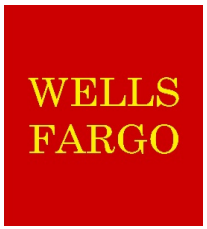


IBM Security Secret Server 고객 레퍼런스

IBM Security Secret Server 공공 고객 레퍼런스

IBM Security Secret Server 금융 고객 레퍼런스





Case Study: Adobe,
특권 계정 보안 제공으로 클라우드 애플리케이션 환경 구축

도전 과제

- Adobe 제품 및 클라우드 서비스는 전 세계 수십억 대의 장치에서 사용.
- Adobe의 빌드 환경은 내부 또는 외부 위협으로부터 환경을 강화하기 위해 구현한 새로운 최첨단 보안 자동화 프로토콜의 대상이었음.
- 이 특정 환경에서 보안 자동화의 우선 순위 중 하나는 사람의 실수와 위험 가능성을 줄이기 위해 가능한 한 인간 요소를 제거하는 것.
- 권한 있는 자격 증명에 대한 접근 관리를 엄격하게 시행하고 사용 중 및 사용 후에 자격 증명을 안전하게 저장하고 관리하는 방법 필요.

IBM Security Secret Server 선택 이유

- ✓ 손쉬운 통합, 배포, 운영 및 유지 관리.
- ✓ 로깅 및 보고 기능, 모든 유형의 자격 증명을 저장하는 기능
- ✓ 사용자 정의가 가능한 친숙한 사용자 인터페이스
- ✓ 낮은 총 소유 비용
- ✓ 복잡한 구성이나 유지 관리 전문 서비스의 필요성 없이 즉각적으로 자격 증명을 안전하게 관리 및 감사

민감한 권한 있는 자격 증명을 보호하고 해당 자격 증명에 대한 권한 있는 사용자 접근을 관리함으로써 제품 및 클라우드 서비스 구축 환경에서 혁신적인 보안 자동화 구현 지원.

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions