

차세대 접근통제 중심의 재택근무 환경 보안 전략

채 흥 소 / 솔루션 컨설턴트

Quest

Where Next Meets Now.

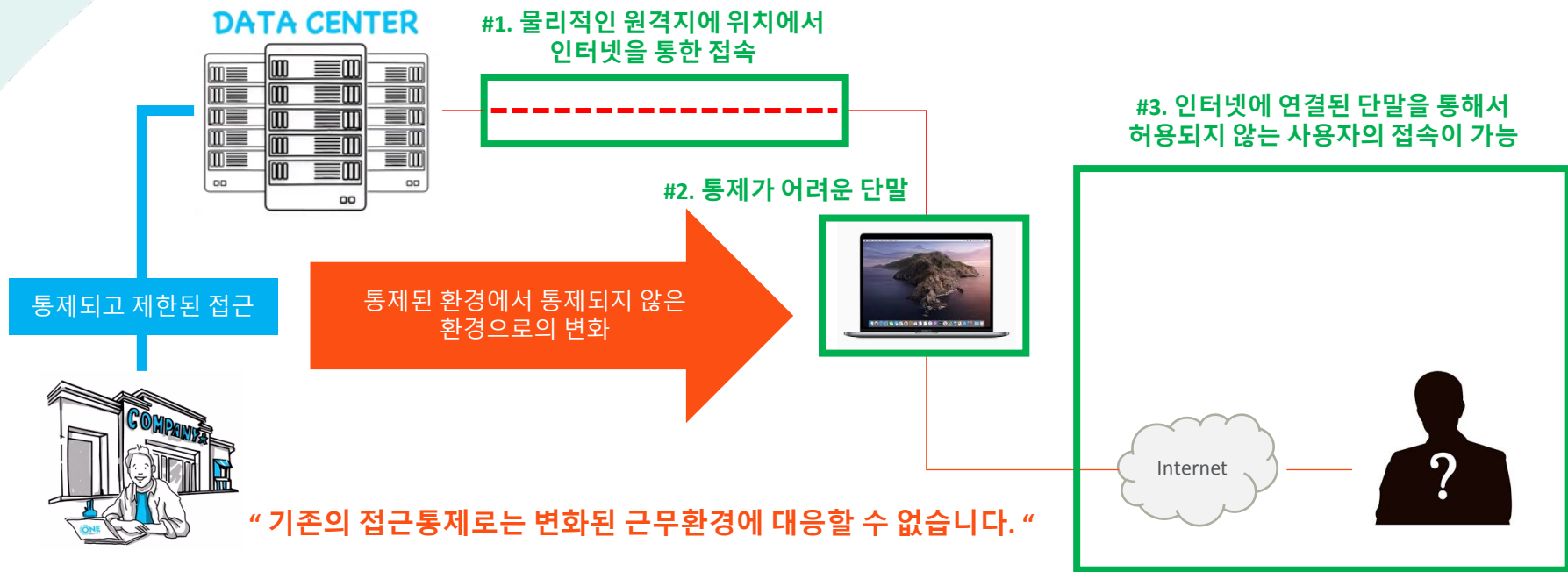
재택근무환경에서의 보안 위협

Quest

Where Next Meets Now.

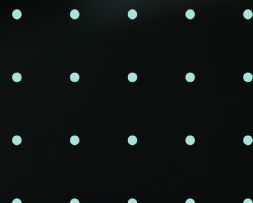
재택근무 환경?

다양한 형태로 통제되고 검증된 사용자로부터의 접속만 가능한 환경에서 허용되지 않은 사용자 접속이 가능해지는 환경으로의 변화



“ 기존의 접근통제로는 변화된 근무환경에 대응할 수 없습니다. ”

기존 접근통제의 한계





1

시스템 접근만을 통제



!=

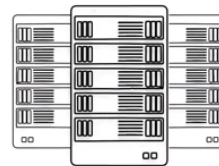


접근통제 대상의 한계



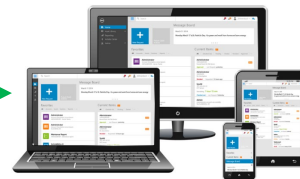
IT운영자, 관리자를 위한 시스템 접근

접근통제 대상



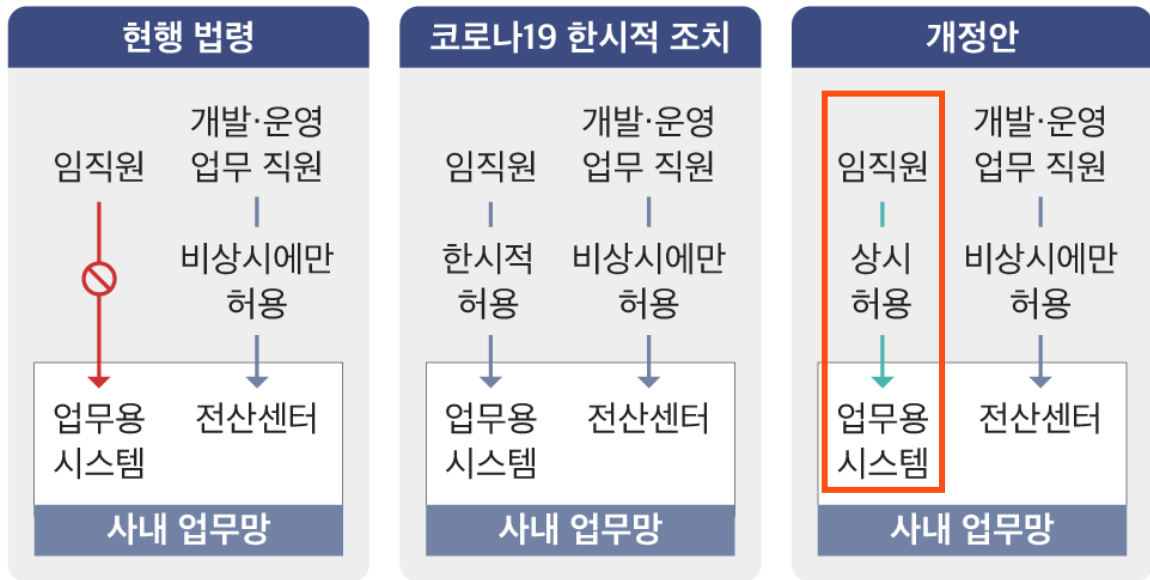
RDP, TELNET, SSH, FTP

임직원을 위한 업무시스템 접근



금융권의 재택근무

재택근무 관련 망분리 제도 개선사항



자료=금융감독원



감사나 통제에 취약

제한된 통제만을 지원

2FA인증만 되면 허용된 모든 시스템에 접근 가능



접근 기록을
남기기 어려움

승인 프로세스의
부재로 담당자
인지가 어려움

요청별로 다른
보안 정책을
적용하기 어려움

단말 해킹에
취약함

기록이나 저장 방식 지원에 제한



스트리밍이 아닌 스냅샷
방식으로 정확한 분석이 어려움



HTTP(s) 프로토콜에 대한
지원이 되지 않음

기록(녹화) / 통제



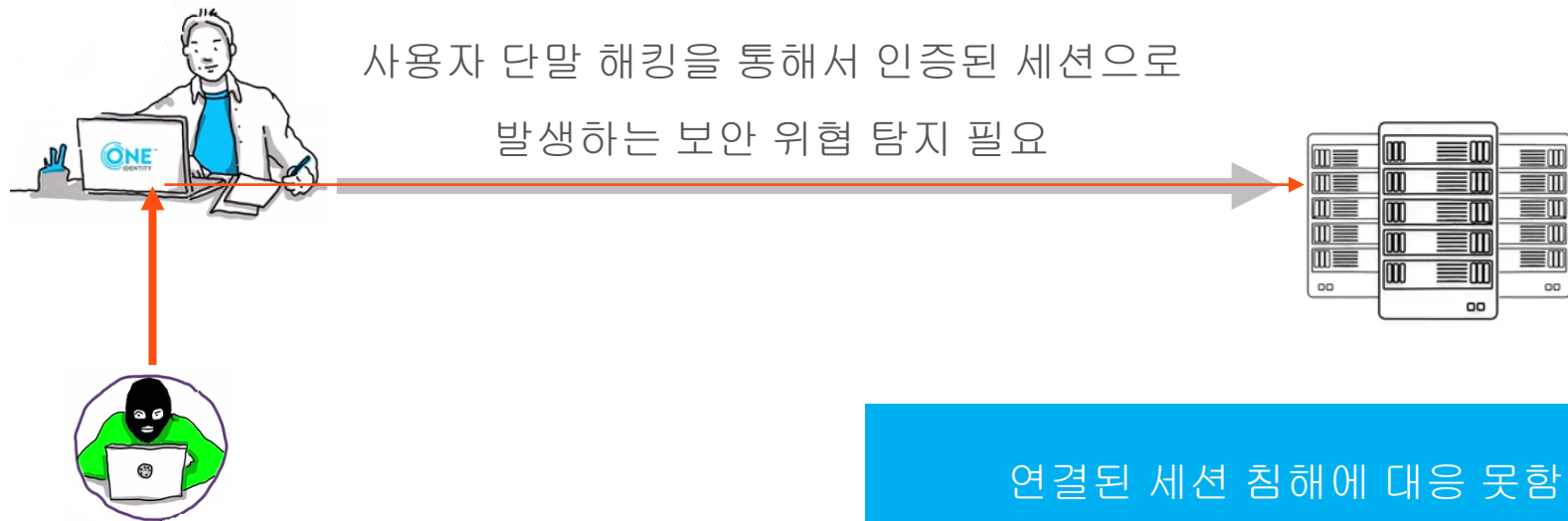
윈도우 GUI 환경에 대한
기록이 제한적임





이상 접근이나 위협에 대한 분석에 약함

보안 위협 대응에 취약

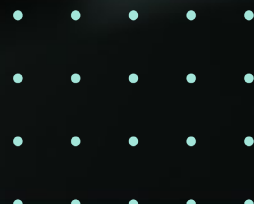


연결된 세션 침해에 대응 못함



새로운 접근통제는?

Quest[®]
Where Next Meets Now.





승인 및 강력한 보안 정책

기반의 계정중심의 접근통제

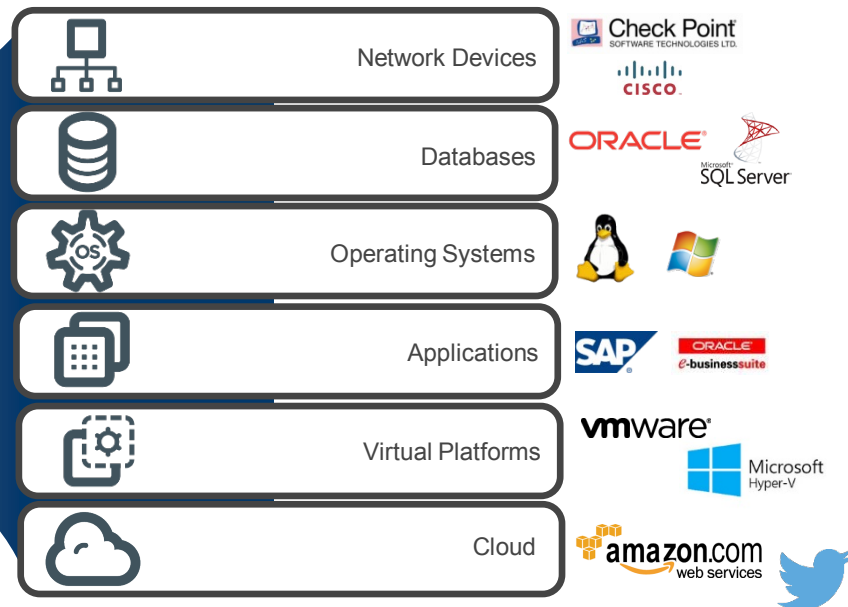
계정중심의 접근통제



Please enter your password to run users-admin

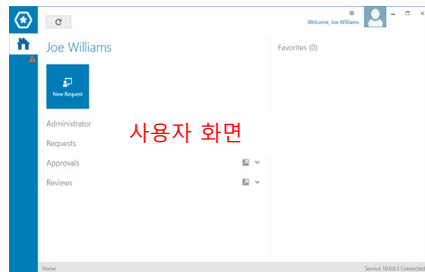
Password:

- 모든 형태의 접근을 통제
- 대부분의 시스템을 지원

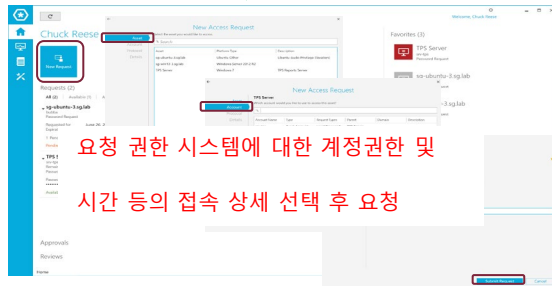


승인 기반의 접속요청 및 자동 접속

사용자별로
접근가능한 시스템 및
계정 정보는 관리자에
의하여 사전에 설정



사용자 직접 접속 요청



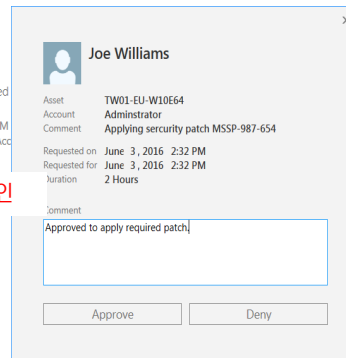
Approver

Approvals (1)
All (1) | Pending (1) | Approved
Joe Williams June 3 2016 2:32 PM
Requested Asset TW01-EU-W10E64, Acc

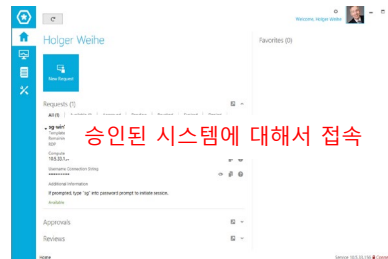
관리자의 승인



Automatic



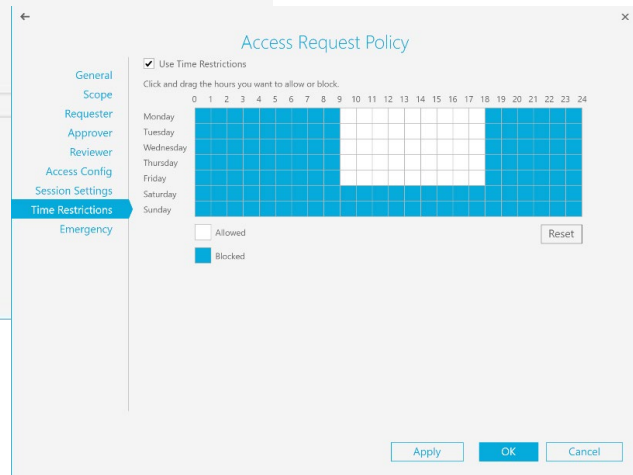
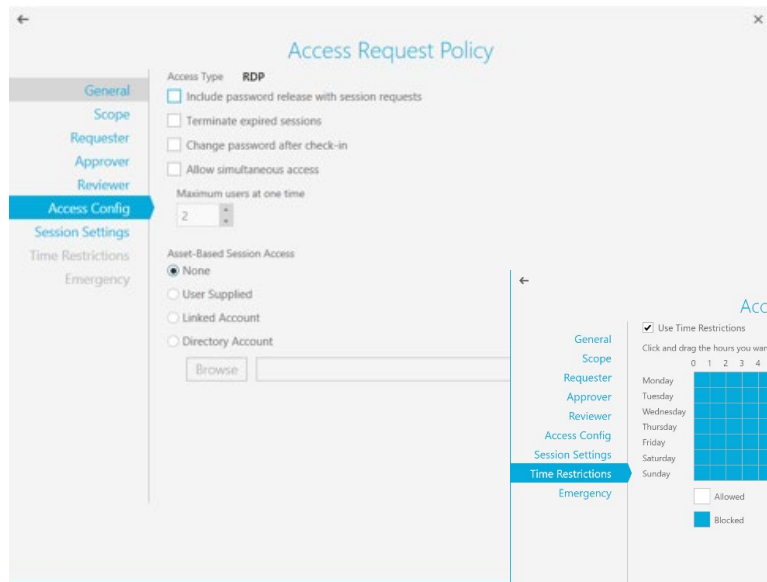
승인



패스워드 입력 없이
자동 접속
(SSH, RDP만 지원)

강력한 보안 정책 및 승인 워크플로우

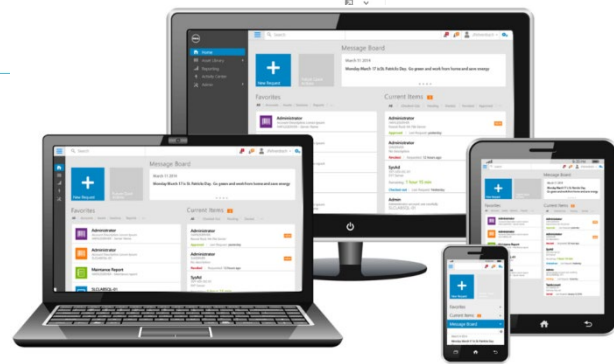
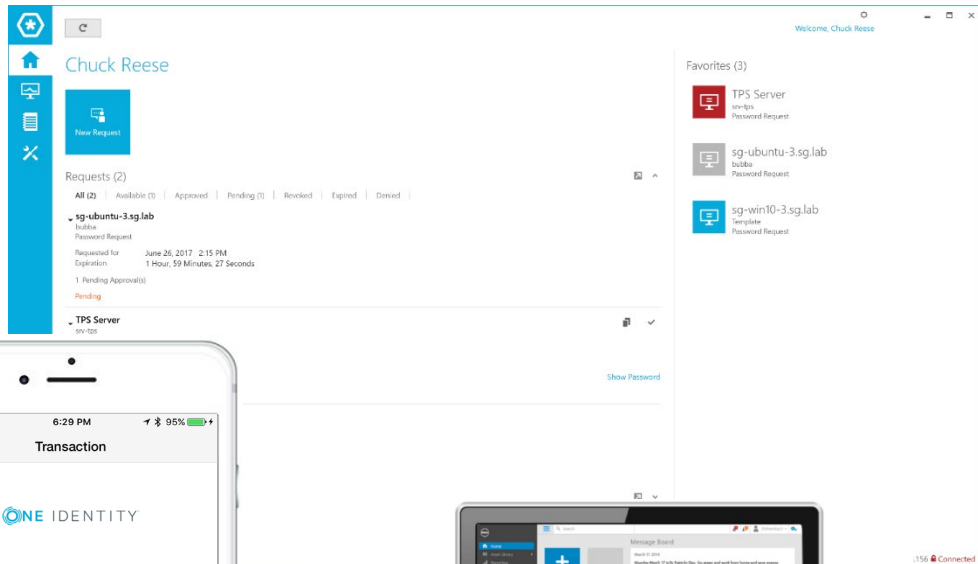
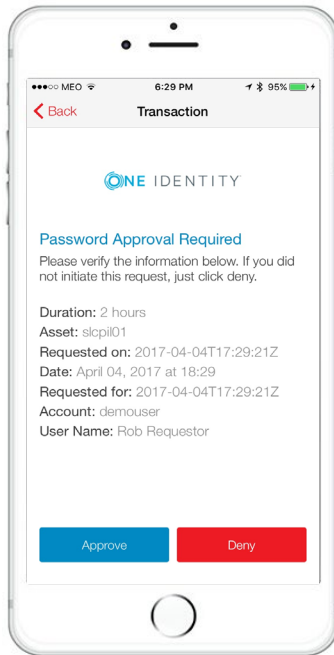
체계적인 승인 워크플로우 기반
강력한 보안 정책



안정적인 Cloud기반의 2FA 서비스 인증 및 승인

Approval Anywhere

Quest



Where Next Meets Now.



2

강력한 감사(기록 및 저장)

모든 접속요청에 대한 감사 기록 제공

The screenshot shows the Quest Active Directory console interface. On the left is a navigation pane with icons for home, activity, and search. The main area displays 'All Activity' for user 'hweihe'. Below this, there are tabs for 'Last 24 Hours', 'Last 7 Days', 'Last 30 Days', 'Last 60 Days', 'Last 90 Days', and 'Custom'. A 'Run' button is present. The main table lists activity events with columns for User, User Name, IP Address, Date, Log, and Event. The 'Columns' panel on the right allows filtering the displayed data.

User	User Name	IP Address	Date	Log	Event
hweihe	hweihe	10.5.37.95	22.06.2017 17:28:39	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 17:52:19	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 17:54:38	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 17:56:24	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 19:07:44	Login	User Authentication Failed
hweihe	hweihe	10.5.37.95	22.06.2017 19:07:48	Login	User Authentication Failed
hweihe	hweihe	10.5.37.95	22.06.2017 19:07:54	Login	User Authentication Failed
hweihe	hweihe	10.5.37.95	22.06.2017 19:08:01	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 19:11:11	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 19:14:46	Login	User Authenticated
hweihe	hweihe	10.5.37.95	22.06.2017 22:07:46	Login	User Authenticated

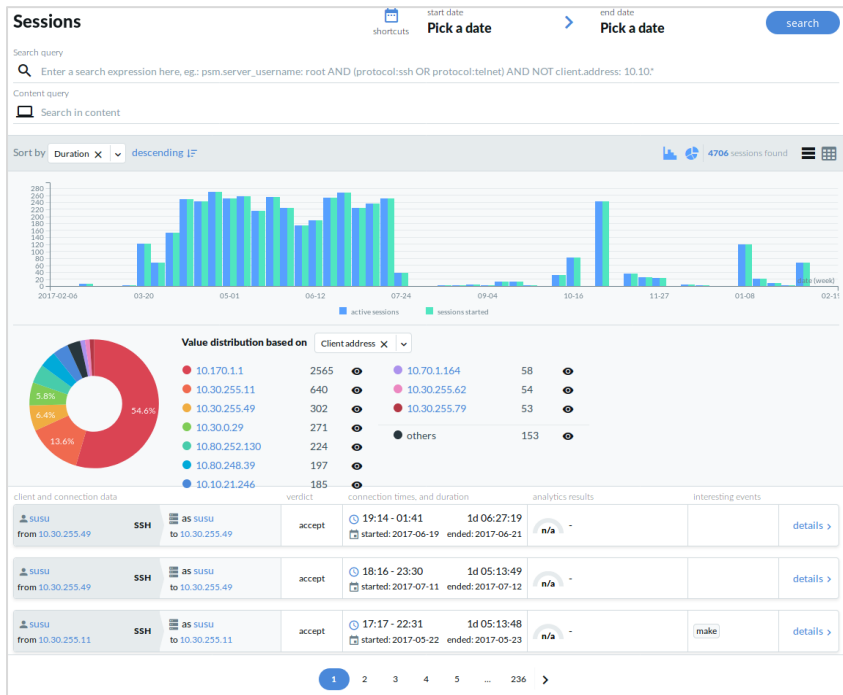
The Activity Center dashboard provides a high-level overview of system activities. It includes a 'Today's Activities' section with metrics for Requested Passwords (10), Automated Password Approvals (0), and Revoked Password Approvals (10). Below this, there are three filters: 'I know who I am looking for', 'I know what I am looking for', and 'I know when it happened'. The main table lists activities with columns for User, User Name, IP Address, Date, Log, and Event.

User	User Name	IP Address	Date	Log	Event
Matillman	15671-a167a-49avea-vae	Admin	slcDex34	Daily Maintenance	Closed July 23, 2014 11:32 AM
Matillman	15671-a167a-49avea-vae	Admin	slcDex34	Daily Maintenance	Checked in July 24, 2014 3:14 PM

This screenshot shows a detailed view of a specific activity event. It includes a table with columns for Time Stamp, Event, Authorizer, and Notes. The event is a 'Daily Maintenance' check-in by 'Matillman' on July 24, 2014 at 3:14 PM. The notes indicate that the system is 'General Maintenance' and the time to complete is '7 Hous 7 minutes'.

Time Stamp	Event	Authorizer	Notes
July 24, 2014 3:14 PM	Checked in		
July 24, 2014 2:32 PM	Viewed		
July 24, 2014 1:13 PM	Approved	Chatt	
July 24, 2014 12:32 AM	Approved	JIBach	
July 24, 2014 8:07 AM	Pending Approval		
July 24, 2014 8:07 AM	Requested		

접속, 명령어 수행 대한 가시성 및 리포트



Privileged Sessions

requester@dc01.oneidentity.demo indexed

Overview Details Events

File Explorer

2020-01-20 14:45:01.617
Windows PowerShell

2020-01-20 14:45:04.298
Administrator: Windows PowerShell

2020-01-20 14:45:04.332
Administrator: Windows PowerShell

2020-01-20 14:45:10.684
13 File Explorer

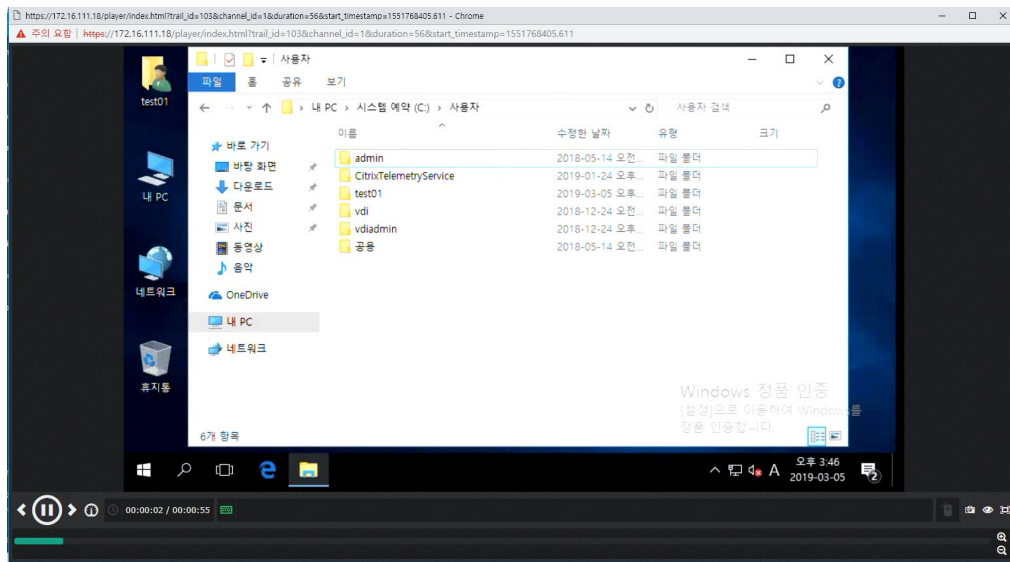
2020-01-20 14:45:10.684
Administrator: Windows PowerShell

2020-01-20 14:45:11.356
File Explorer

Configuration
Search
Reporting
Gateway Authentication
Four-Eyes
Active Connections
Unlock Credential Store
About
admin
Logout (00:19:51)

Europe/Paris GMT+0100
Copyright © One Identity LLC. 2019

HTTP(s), Citrix VDI, RDP,SSH,VNC,TELNET에 대한 스트리밍 녹화



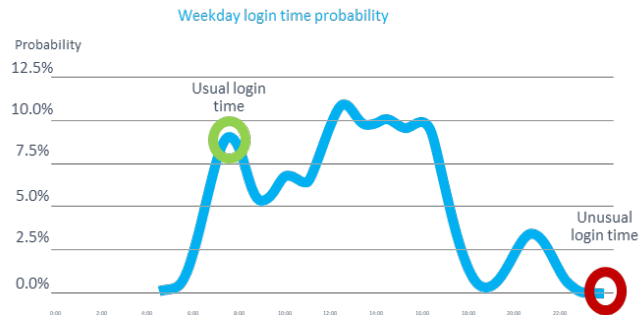
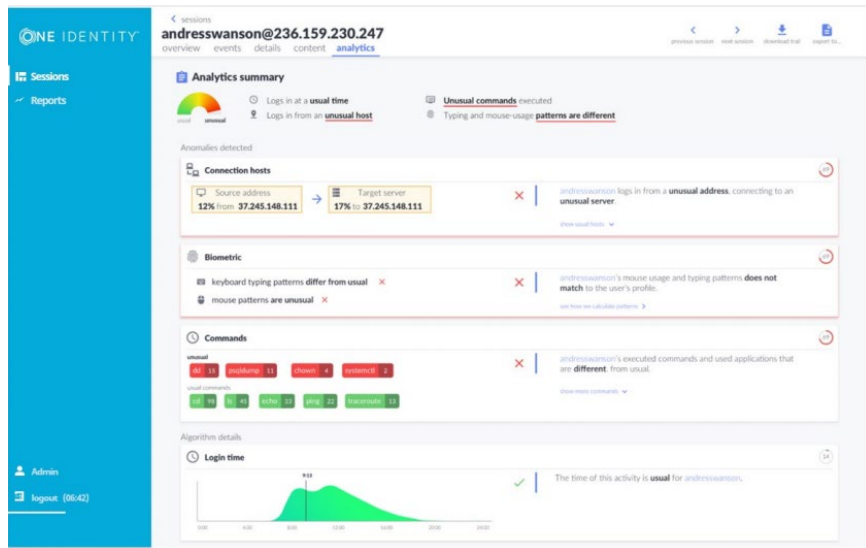
Snap-Shot방식이 아닌 스트리밍
방식으로 작업 유실없이 데이터
저장



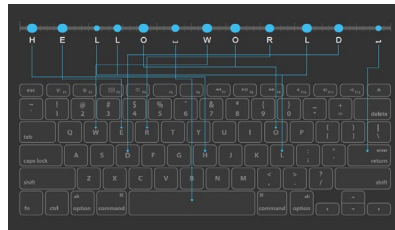
3

행위 기반 분석을 통합 연결된 세션을 통한 보안 위협 탐지

사용자 행위 기반의 머신러닝을 통한 위협 분석



로그인 시간의 이상 분석



키보드 입력의 패턴 분석

마우스 이동의 패턴 분석

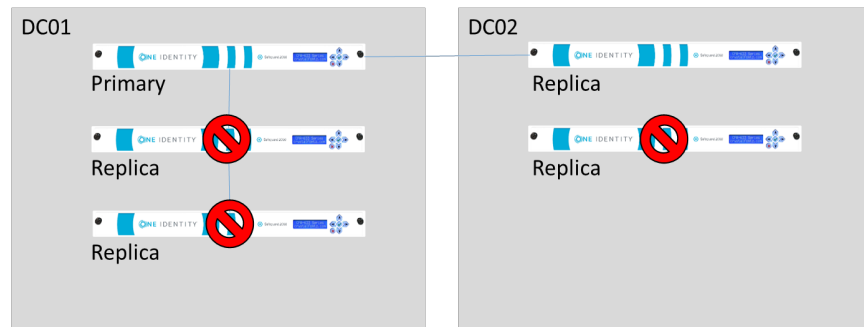
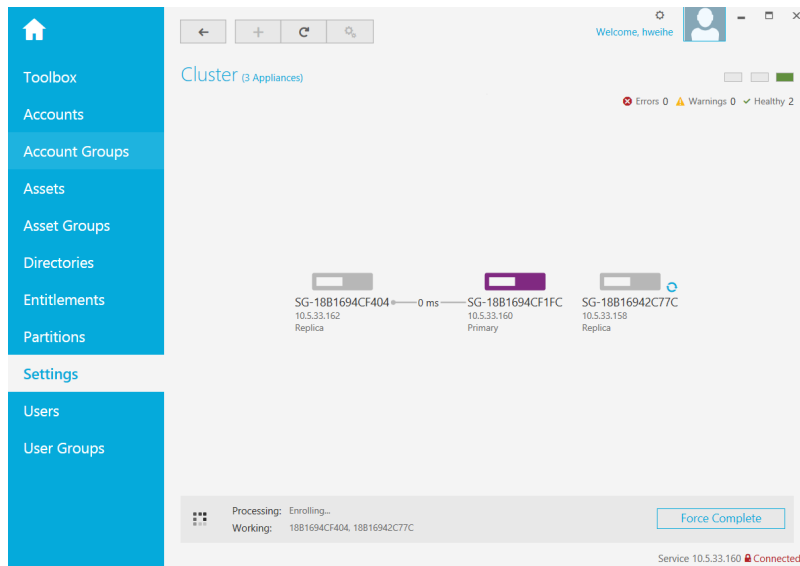


4

HA기반의 클러스터링을 통한

안정적인 서비스 제공

3,5,7중화의 실시간 데이터 동기화 기반 HA



HA기반의 무중단 서비스 제공



감사합니다.