

# 재택근무 컴플라이언스 대응을 위한 단말과 접근통제 보안전략

Hongso Chae / Solution Consultant

Quest

Where Next Meets Now.

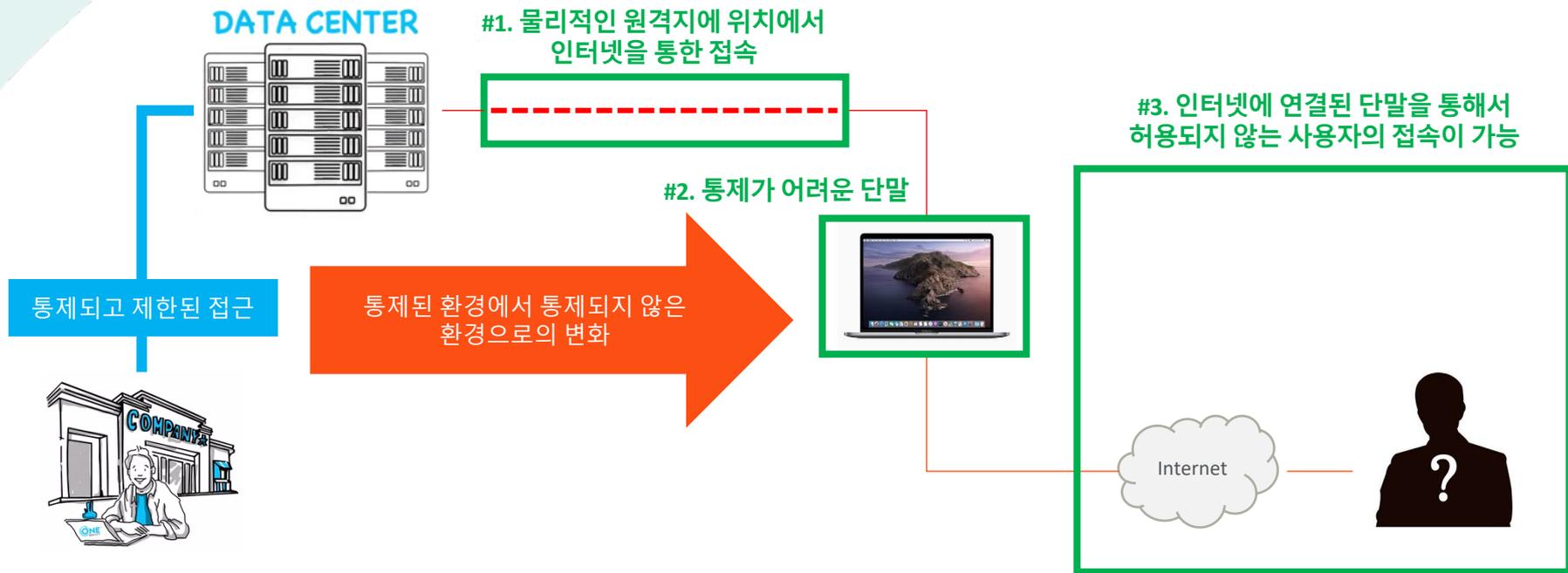
# 재택근무 환경에서의 보안 위협 및 컴플라이언스

Quest

Where Next Meets Now.

# 재택근무 환경?

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



# 재택근무에 따른 주요 보안위협

[ 재택근무에 따른 주요 보안 위협 (출처 : 美 NIST) ]

구 분	주요 보안 위협
외부 단말기의 물리적 통제 미흡	<ul style="list-style-type: none"><li>- 재택근무에 사용되는 외부 단말기의 분실·도난이나 타인의 정보 훔쳐보기 시 단말기 內 데이터가 유·노출</li><li>- 외부 단말기를 통한 허가되지 않은 내부 네트워크 접근</li></ul>
안전하지 않은 네트워크 사용	<ul style="list-style-type: none"><li>- 공용 유무선 네트워크를 통해 내부망 접속 시 도청, 중간자 공격(MITM) 등으로 중요정보가 유출</li></ul>
악성코드 감염에 따른 네트워크 침해	<ul style="list-style-type: none"><li>- 악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능</li></ul>
내부 자원의 원격접근 위협	<ul style="list-style-type: none"><li>- 내부에서만 접근 가능했던 내부 자원에 외부 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안위협</li></ul>

출처 : 금융보안원-금융회사 재택근무 보안안내서

# 전자금융감독규정 시행세칙 개정안

<별표 7> 정보통신망법 제35조 제2항 제1호의2에 따른 정보보호통제

구분	통제 사항		
공통	<ul style="list-style-type: none"> <li>외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료</li> <li>지능형 해킹(APT)차단 대책 수립·적용</li> <li>전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링</li> </ul>		
메일 시스템	<ul style="list-style-type: none"> <li>본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용</li> <li>메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용</li> </ul>		
업무용 단말기	<ul style="list-style-type: none"> <li>사용자의 관리자 권한 제거</li> <li>승인된 프로그램만 설치·실행등록 대책 수립·적용</li> <li>전산자료 저장 시 암호화</li> </ul>		
원격 접속	외부 단말기	공통	<ul style="list-style-type: none"> <li>백신 프로그램 설치, 실시간 업데이트 및 검사 수행</li> <li>안전한 운영체제 사용 및 최신 보안패치 적용</li> <li>로그인 비밀번호 및 화면 보호기 설정</li> <li>화면 및 출력물 등으로 으로 인한 정보유출 방지대책 적용</li> </ul>
		업무용 단말기를 경유하여 내부망에 접속하는 경우 (간접접속)	<ul style="list-style-type: none"> <li>외부 단말기와 업무용 단말기의 파일 송·수신 차단</li> </ul>
	원격 접속	외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)	<ul style="list-style-type: none"> <li>인가되지 않은 S/W 설치 차단</li> <li>보안 설정 임의 변경 차단</li> <li>USB 등 외부 저장장치 읽기/쓰기 차단</li> <li>전산자료 (파일, 문서) 암호화 저장</li> <li>단말기 분실 시 정보 유출 방지 대책적용 (하드디스크 암호화, CMOS비밀번호 적용 등)</li> </ul>
		내부망 접근통제	<ul style="list-style-type: none"> <li>업무상 필수적인 IP, Port에 한하여 연결 허용</li> <li>원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)</li> </ul>
	인증	<ul style="list-style-type: none"> <li>이중 인증 적용(예: ID/PW + OTP)</li> <li>일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단</li> <li>안전한 알고리즘으로 네트워크 구간 암호화</li> </ul>	
	통신 회선	<ul style="list-style-type: none"> <li>내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 원격 접속 단말기는 인터넷 연결 상시 차단)</li> <li>원격 접속 후 일정 유희시간 경과 시 네트워크 연결 차단</li> </ul>	
	기타	<ul style="list-style-type: none"> <li>원격접속자에 대한 보안서약서 징구</li> <li>공공장소에서 원격 접속 금지</li> </ul>	

출처 : 금융감독원

Where Next Meets Now.

# 재택근무 환경의 보안 핵심



재택근무용 단말이  
안전하게 관리



허가된 사람인지  
인증



허용되지 않는 접속과  
작업을 제한 및 감사

안전한 통신(SSL VPN)

위협에 대한 신속한 탐지 및 내부 시스템 보안 강화

# 재택근무 단말의 보안

Quest  
Where Next Meets Now.



# 단말 보안의 핵심



강력한 OS 인증 체계(2FA)

신속하고 정확한 최신 보안  
패치 적용

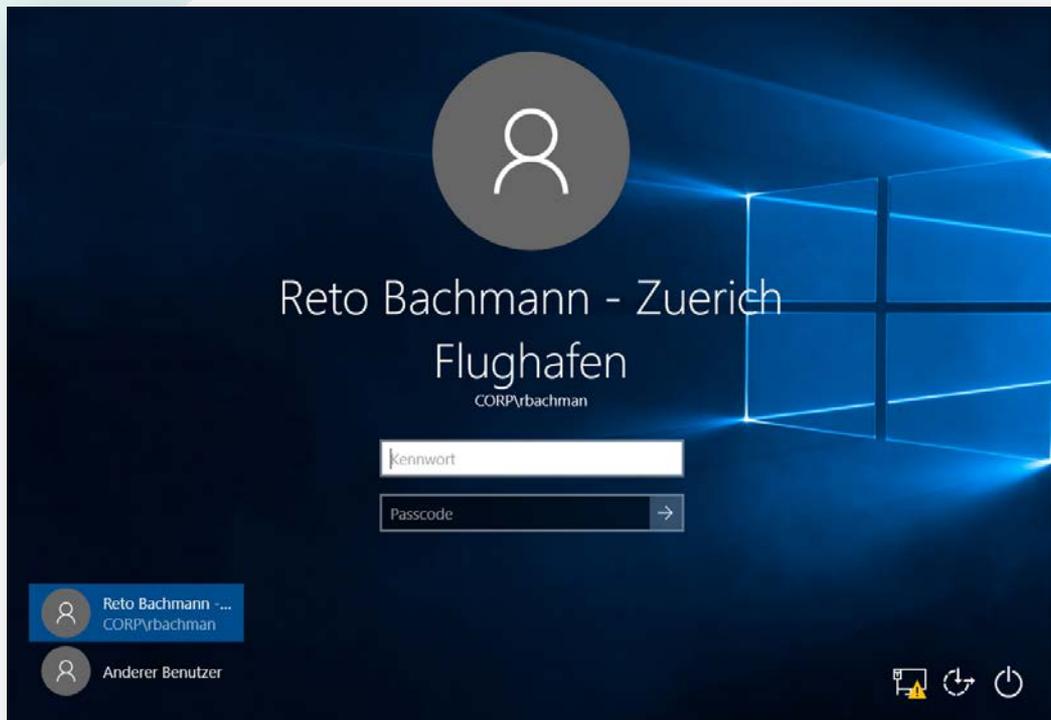
강력한 OS 보안 정책(GPO)



3<sup>rd</sup> Party 보안 제품

윈도우 업그레이드나 패치에 최소의 이슈 발생 환경으로 구성  
즉, 윈도우 기본 보안을 최대한 활용

# #1. OS 2FA 인증



강력한 인증을 통한 보안성 향상

분실 등으로 인한 위험성 최소화

# #2 .자동화된 패치 및 관리

재택근무용 단말에 대한 패치관리 솔루션의 기본 요건

완벽한 자동화

Malware등에 대한  
보안 강화

완벽한 검증 및  
가시성 확보

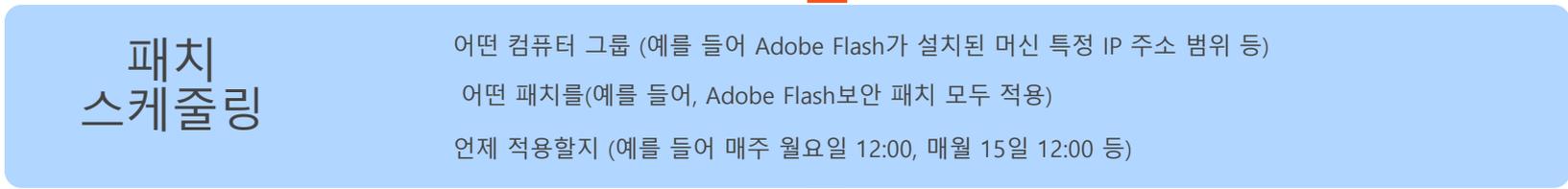
통합 단말 관리

# #2 .자동화된 패치 및 관리 > 완벽한 자동화



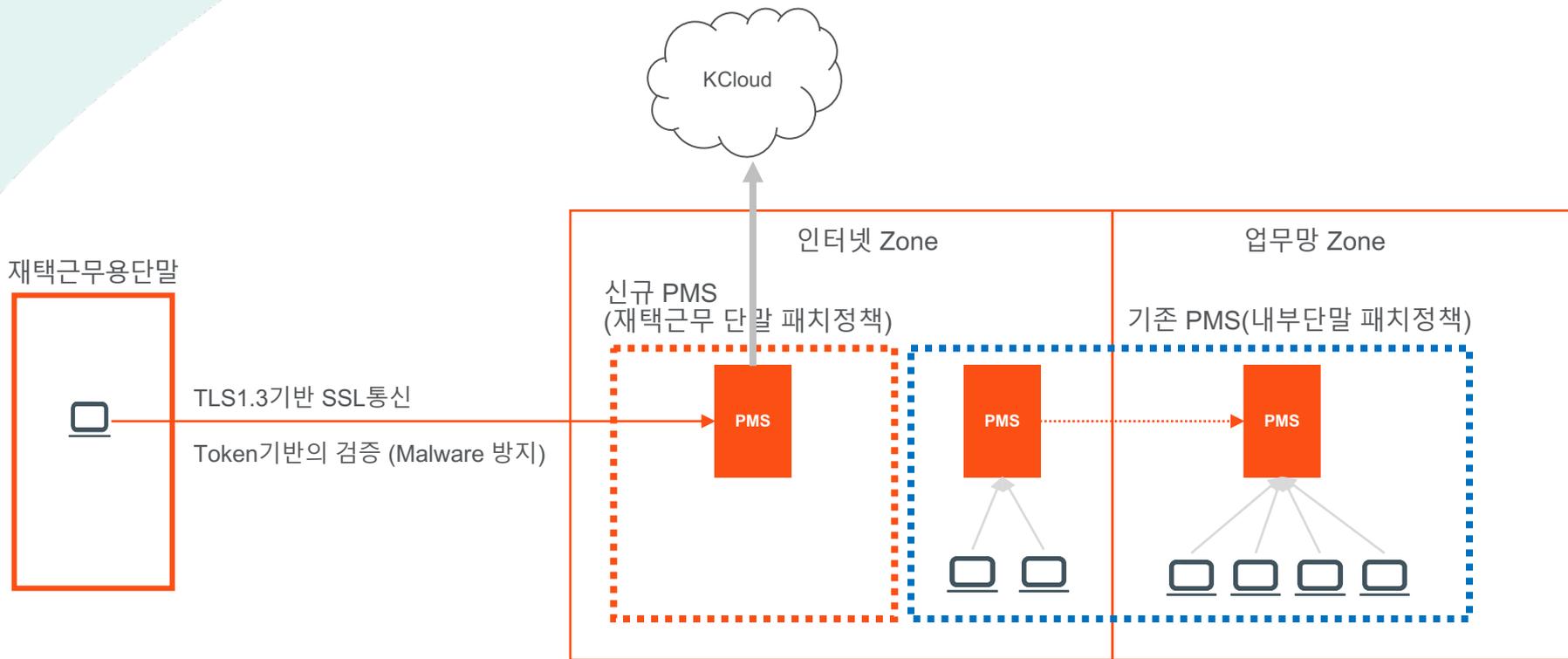
패치 스케줄링

- 어떤 컴퓨터 그룹 (예를 들어 Adobe Flash가 설치된 머신 특정 IP 주소 범위 등)
- 어떤 패치를(예를 들어, Adobe Flash보안 패치 모두 적용)
- 언제 적용할지 (예를 들어 매주 월요일 12:00, 매월 15일 12:00 등)



각 클라이언트의 패치 수준의 차이 각 패치 모듈의 적용 순서 등은 모두 자동 제어

# #2 .자동화된 패치 및 관리 > 강력한 보안



# #2 .자동화된 패치 및 관리 > 통합관리 및 검증

3단계 검증을 통한 완벽한 패치적용 검증 제공

단계1.

대시보드를 통한 검증

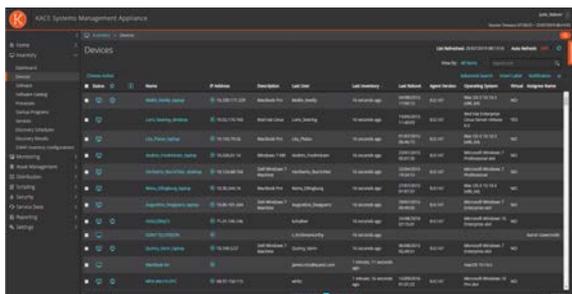
단계2.

인벤토리 정보를 통한  
검증

단계3.

특정 명령어의  
결과값을 통한 검증

자동화되고 사용자 정의 가능한 인벤토리 관리를 통한 통합 단말 관리 및 가시성



# #3 .강력한 OS 보안 정책

## Microsoft의 GPO Baseline

The screenshot shows a Microsoft TechNet blog post. The main heading is "Security baseline (FINAL) for Windows 10 v1809 and Windows Server 2019". Below the heading, there is a sub-heading "Downloaded the content from the Microsoft Security Compliance Toolkit (click Download and select Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip)". The article text describes the download and use of the Security Compliance Toolkit (SCT) to apply security baselines. It includes a list of popular tags such as "SCT", "Security", "Compliance", "Security Baseline", "Baseline", "SAC", "DCM", "SCDM", "System Center", "Powershell", and "Network defense". There is also an "Archives" section with dates from June 2018 to February 2019.

## Windows 10의 보안 서비스



Windows Defender



범용적으로 널리 사용되는 윈도우 보안 가이드와 서비스를 최대한 활용



Where Next Meets Now.

# 재택근무 환경을 위한 새로운 접근통제 전략

Quest  
Where Next Meets Now.





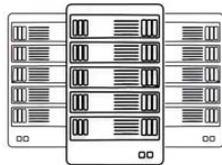
# 기존 접근통제의 한계

# 기존 접근통제 대상의 한계



IT운영자, 관리자를 위한 시스템 접근

접근통제 대상



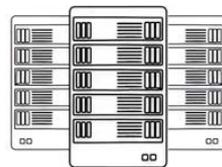
RDP, TELNET, SSH, FTP

임직원을 위한 업무시스템 접근



# 제한된 통제만을 지원

2FA인증만 되면 허용된 모든 시스템에 접근 가능



접근 기록을  
남기기 어려움

승인 프로세스의  
부재로 담당자  
인지가 어려움

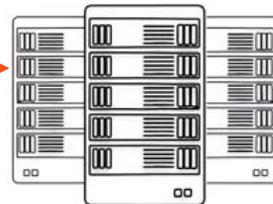
요청별로 다른  
보안 정책을  
적용하기 어려움

단말 해킹에  
취약함

# 보안 위협 대응에 취약



사용자 단말 해킹을 통해서 인증된 세션으로  
발생하는 보안 위협 탐지 필요



연결된 세션 침해에 대응 못함



2

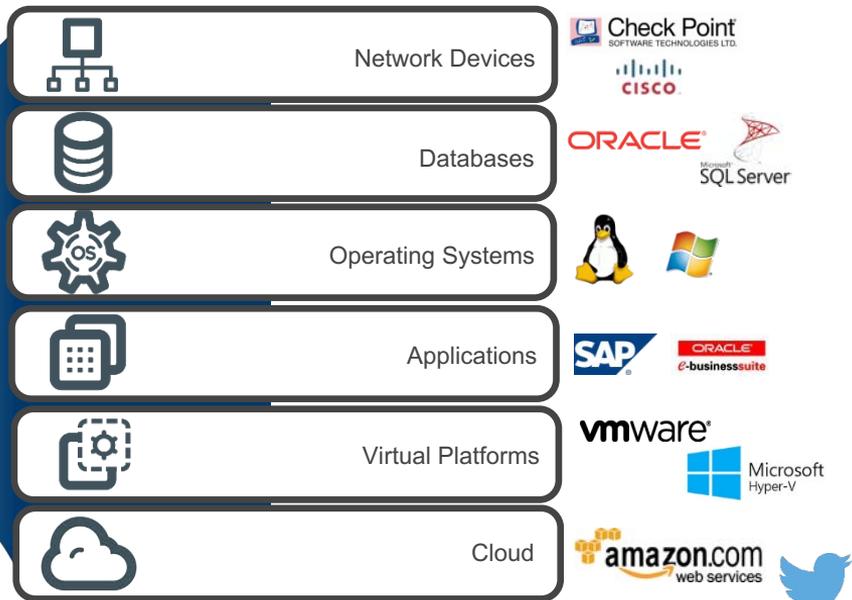
# 새로운 접근통제

# 계정중심의 접근통제

 Please enter your password to run users-admin

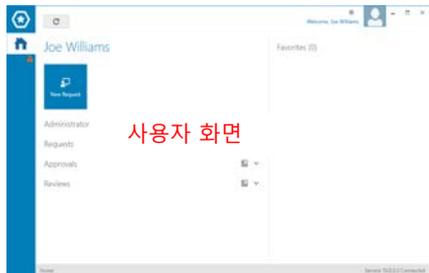
Password:

- 모든 형태의 접근을 통제
- 대부분의 시스템을 지원



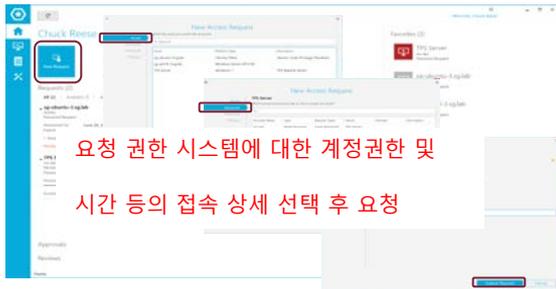
# 승인 기반의 접속요청 및 자동 접속

사용자별로 접근가능한 시스템 및 계정 정보는 관리자에 의하여 사전에 설정



사용자 화면

사용자 직접 접속 요청



요청 권한 시스템에 대한 계정권한 및 시간 등의 접속 상세 선택 후 요청



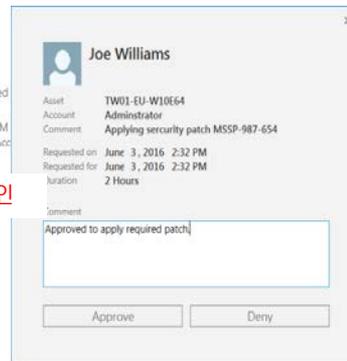
Approver



Automatic



관리자의 승인



승인



승인된 시스템에 대해서 접속

패스워드 입력 없이 자동 접속 (SSH, RDP만 지원)

# 안정적인 Cloud기반의 2FA 서비스 인증 및 승인

Approval Anywhere

Quest

The image illustrates a multi-device authentication system. At the top, a desktop browser window shows a user interface for 'Chuck Reese' with a 'New Request' button and a list of requests. The requests list includes:

- sg-ubuntu-3.sg.lab (Password Request, Pending)
- TPS Server (Password Request, Pending)

The smartphone in the foreground displays a 'Transaction' screen with the following details:

- ONE IDENTITY
- Password Approval Required
- Please verify the information below. If you did not initiate this request, just click deny.
- Duration: 2 hours
- Asset: slcpi01
- Requested on: 2017-04-04T17:29:21Z
- Date: April 04, 2017 at 18:29
- Requested for: 2017-04-04T17:29:21Z
- Account: demouser
- User Name: Rob Requestor
- Buttons: Approve (blue), Deny (red)

Other devices (laptop, tablet, smartphone) in the background show the same interface, demonstrating the 'Approval Anywhere' capability. A blue banner at the bottom left contains the text 'Approval Anywhere'. The Quest logo is in the bottom left corner. The text 'Where Next Meets Now.' is in the bottom right corner.

Where Next Meets Now.



3

# 강력한 감사(기록 및 저장)

# 모든 접속요청에 대한 감사 기록 제공

Activity Center

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

Activity Center

Today's Activities Today Yesterday Date

Requested Passwords 10 Automated Passwords 0 Revoked Passwords 10

I know who I am looking for I know what I am looking for I know when it happened

Requester Name	System	Asset	Reason	Status	Time
Matillman	Admin	skDex34	Daily Maintenance	Closed	July 23, 2014 11:32 AM
Matillman	Admin	skDex34	Daily Maintenance	Checked in	July 24, 2014 3:14 PM

Matillman 15671-a167a-49avea-vae Admin skDex34 Daily Maintenance Closed July 23, 2014 11:32 AM

Matillman 15671-a167a-49avea-vae Admin skDex34 Daily Maintenance Checked in July 24, 2014 3:14 PM

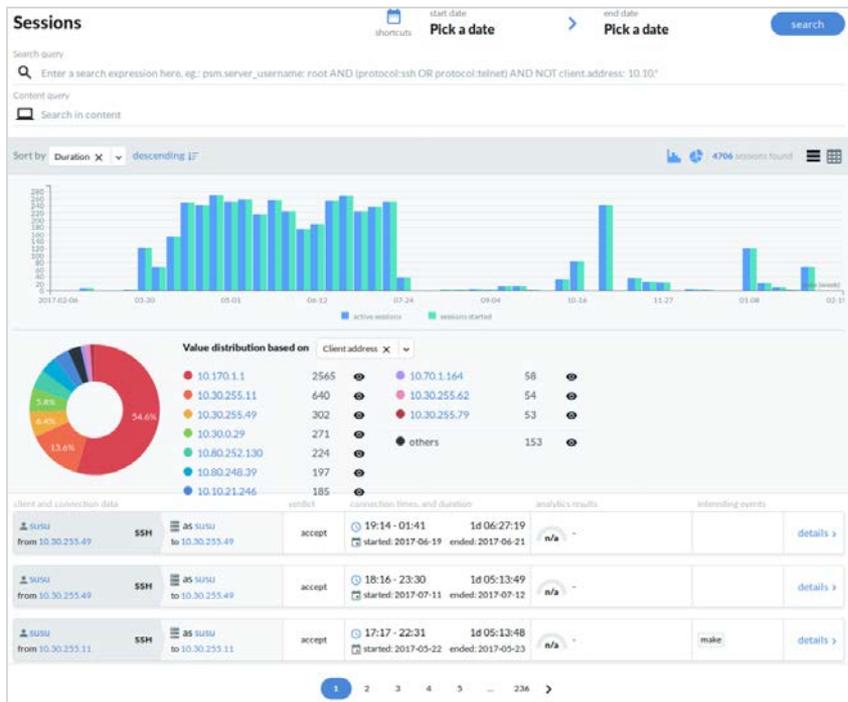
General Policy Asset

Account: Admin System: skDex34 Duration: 4 hours Reason: General Maintenance Unique ID: 15671-a167a-49avea-vae Time to complete: 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		

Matillman 15671-a167a-49avea-vae Service skDex34 Daily Maintenance Checked in July 23, 2014 11:32 AM

# 접속, 명령어 수행 대한 가시성 및 리포트



**Privileged Sessions**

requester@dc01.oneidentity.demo indexed

Overview Details Events Alerts

- 2020-01-20 14:45:01.617 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

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

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

# 효율적인 기록이나 저장 지원



스냅샷이 아닌 스트리밍  
방식으로 정확한 녹화 정보 제공  
(대용량 처리에 대한 안정적인 지원)

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

Quest



HTTP(s) 프로토콜에 대한  
지원  
기록(녹화) / 통제

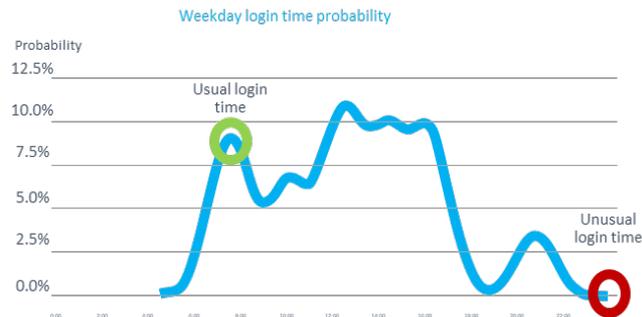
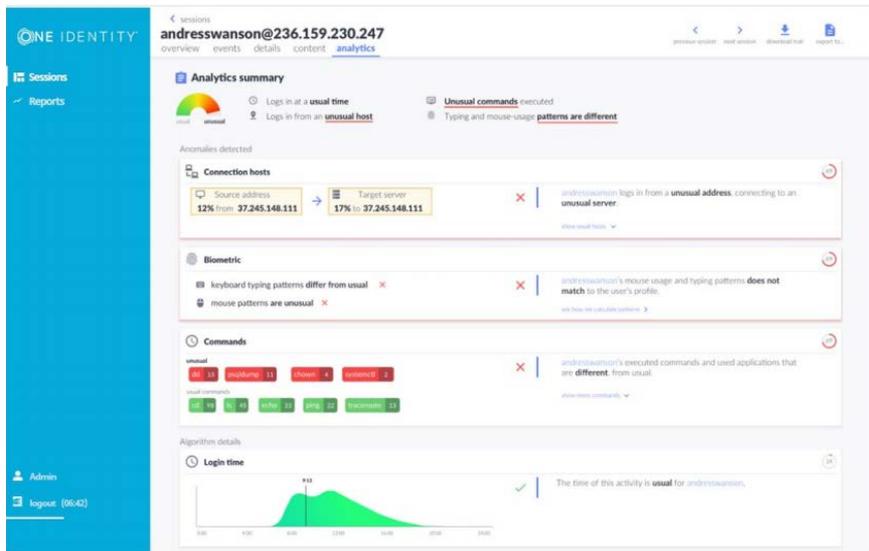


윈도우 GUI환경에 대한  
안정적인 지원

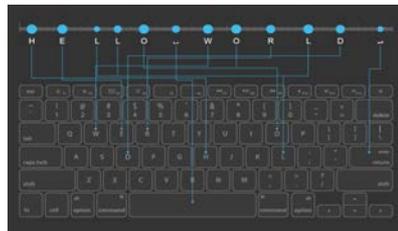


Where Next Meets Now.

# 사용자 행위 기반의 머신 러닝을 통한 위협 분석



로그인 시간의 이상 분석



키보드 입력의 패턴 분석



마우스 이동의 패턴 분석



감사합니다.

Quest  
Where Next Meets Now.