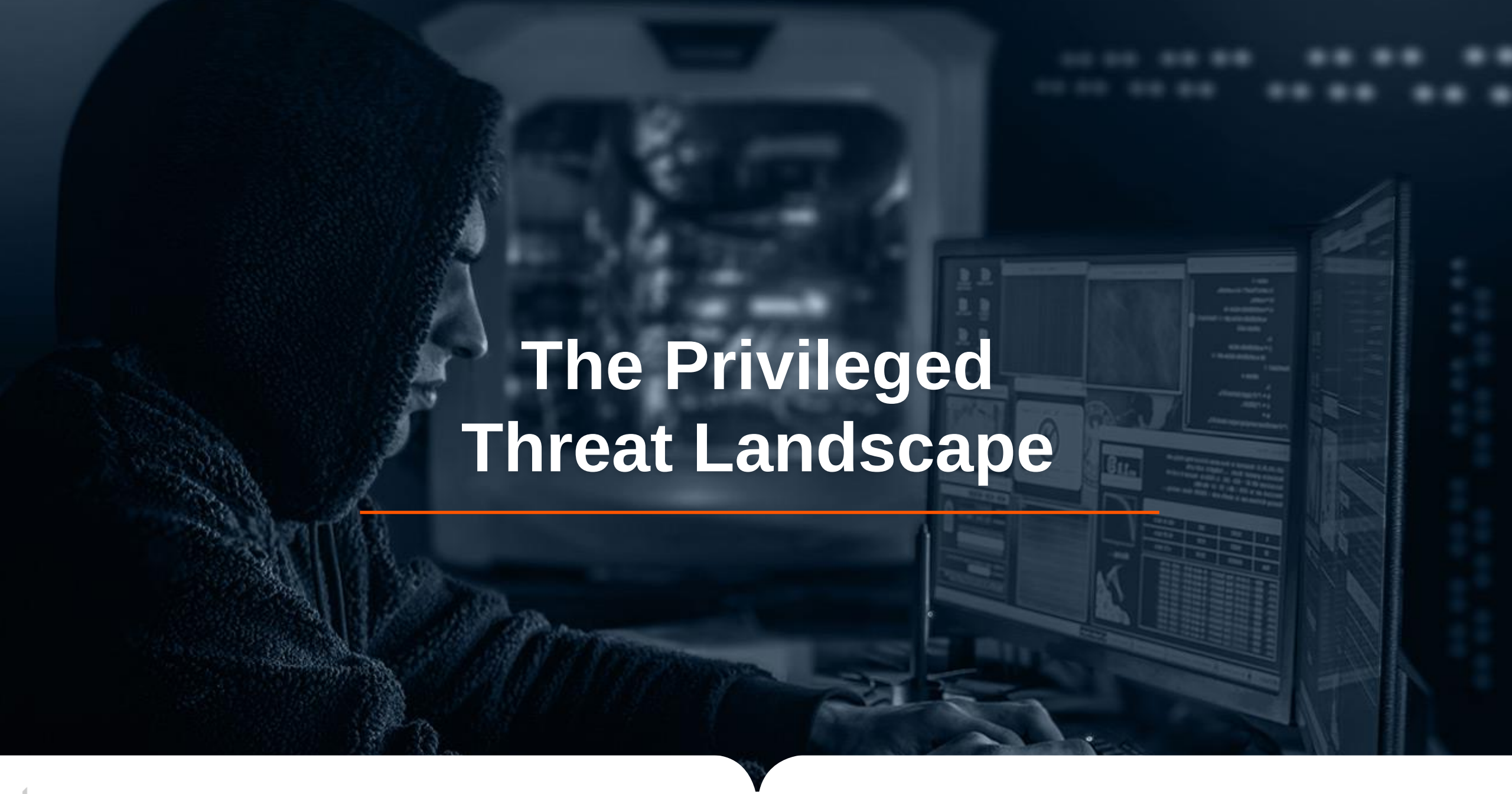
BeyondTrust

# Privileged Attack Vectors

## Building Effective Defense Strategies



# The Privileged Threat Landscape

# 진화중인 사이버 공격 루트

## 20 YEARS AGO

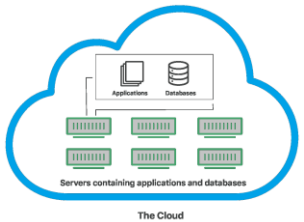
**On-Premise**

- 관리자 계정 공유
- Desktops (Windows, Mac)
- Servers (Unix, Linux, Windows)
- 산업용 제어 시스템
- 보안 인프라
- 네트워크 인프라
- 애플리케이션 및 애플리케이션 서버
- 데이터베이스 및 데이터베이스 서버
- 시스템 자격증명 (AtoA)
- 하이버파바이저 및 가상 머신

## 10 YEARS AGO

**Cloud & Hybrid**

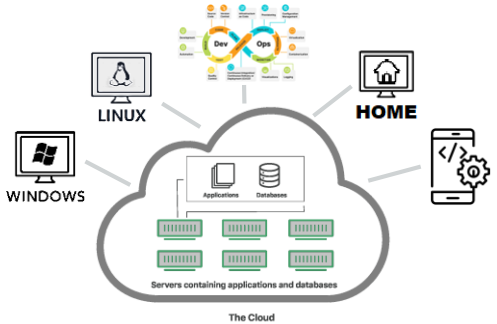
- 클라우드 관리 플랫폼 (AWS, Azure)
- 가상화 환경 (VMWare, MSFT)
- 가상 머신 (Unix, Linux, Windows)
- SaaS Apps (Facebook, LinkedIn, Custom)




## TODAY

**IoT & DevOps**

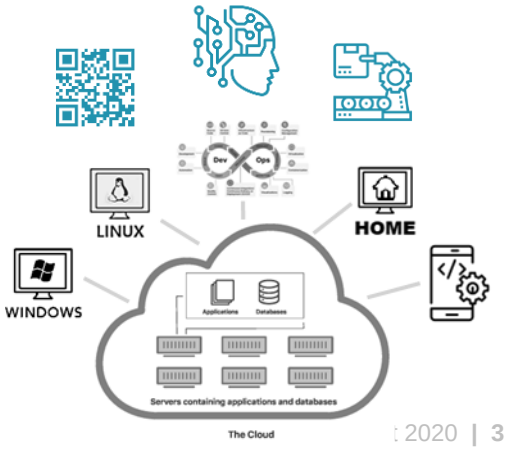
- 로밍 워크스테이션
- BYOD
- 카메라, 센서, 프린터
- DevOps & DevOps Tools
- 동적 가상 환경
- Containers
- 마이크로 서비스




## NEAR FUTURE

**Even More Priv. Accts**

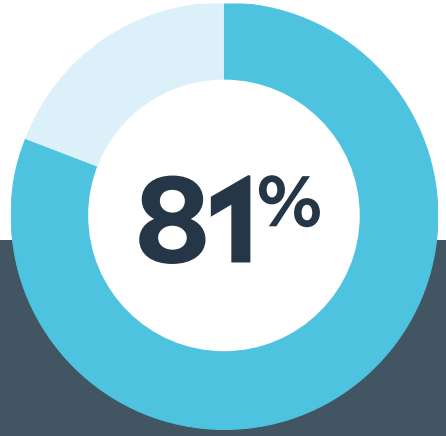
- SaaS Admins
- Cloud Admins
- Application Admins
- 권한 있는 최종 사용자
- Developers
- Machine Password & Keys



# The Impact

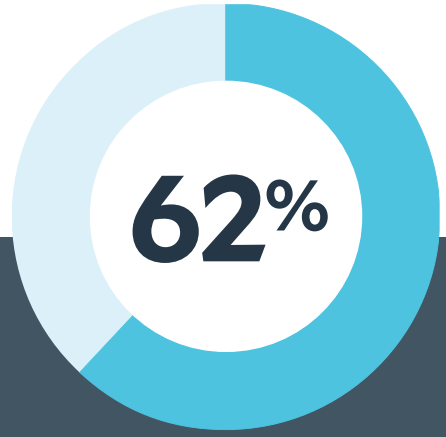
관리되지 않는 권한과 계정은 해커의 침입 경로


**과도한 권리자 권한**과[1] 관련된 취약성




도난 및/또는 **취약한 암호**[2] 인한 위반 수


권한 계정 오남용[3]




권한 있는 액세스 **부적절한 추적시스템**

Source: 1. 2020 Microsoft Vulnerabilities Report, BeyondTrust | 2. 2018 Privileged Access Threat Report, BeyondTrust
3. "The Forrester Wave™: Privileged Identity Management, Q3 2016 | 4. Forrester. "2019 Data Breach Investigations Report" Verizon

# 공격자들은 어떻게 특권을 획득하는가 ?

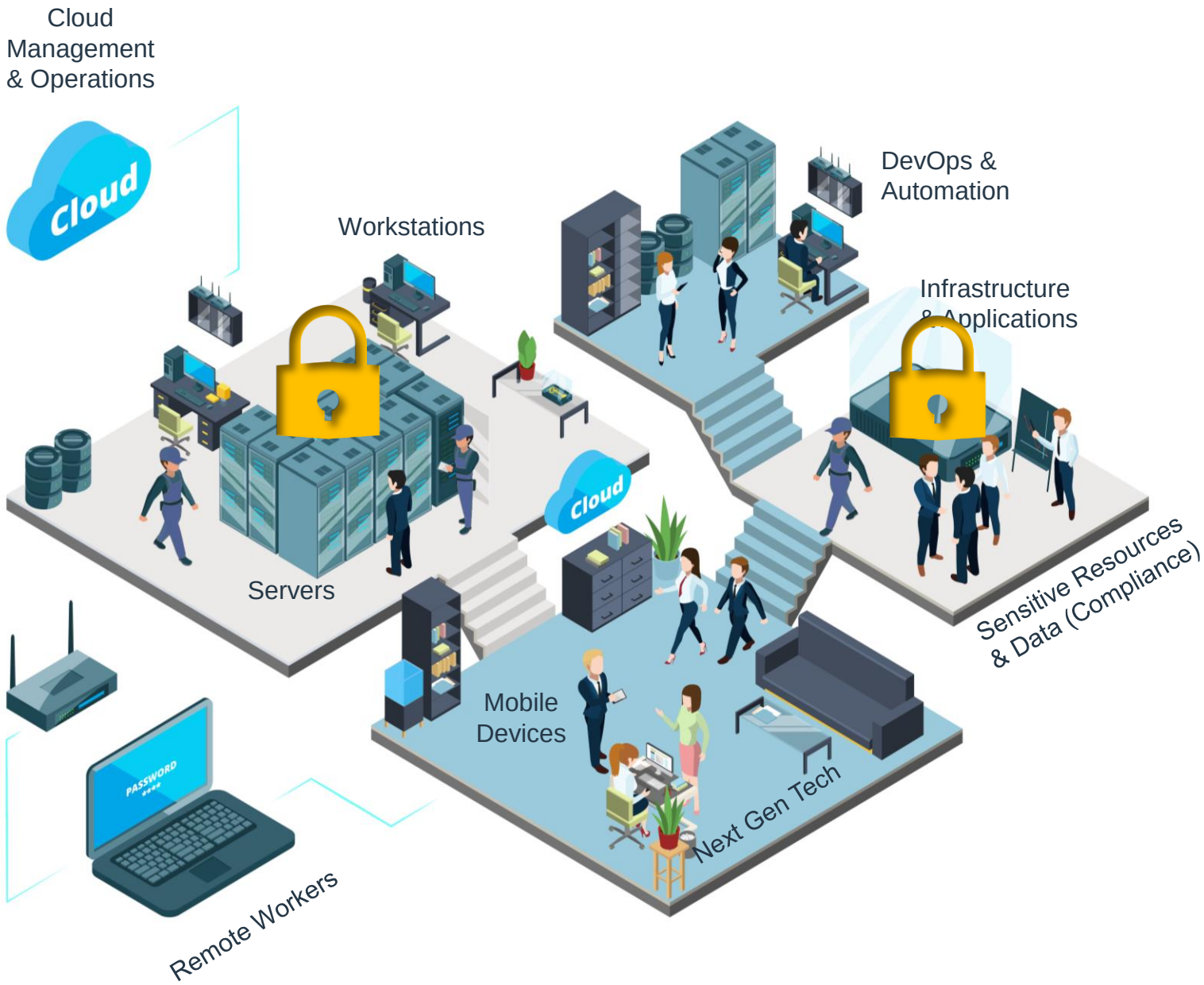
- 추측
- 사전 공격
- Brute Force
- 해시 공유
- 보안 질문
- 암호 재설정
- 암호 살포
- 자격 증명 채우기

- 취약성
- 잘못된 설정/구성
- 위업
- Malware
- Social engineering
- MFA 결함
- SIM-Jacking

- 기본 자격 증명
- 익명
- 예측 가능
- 공유 자격증명
- Temporary
- 재사용
- Shoulder surfing

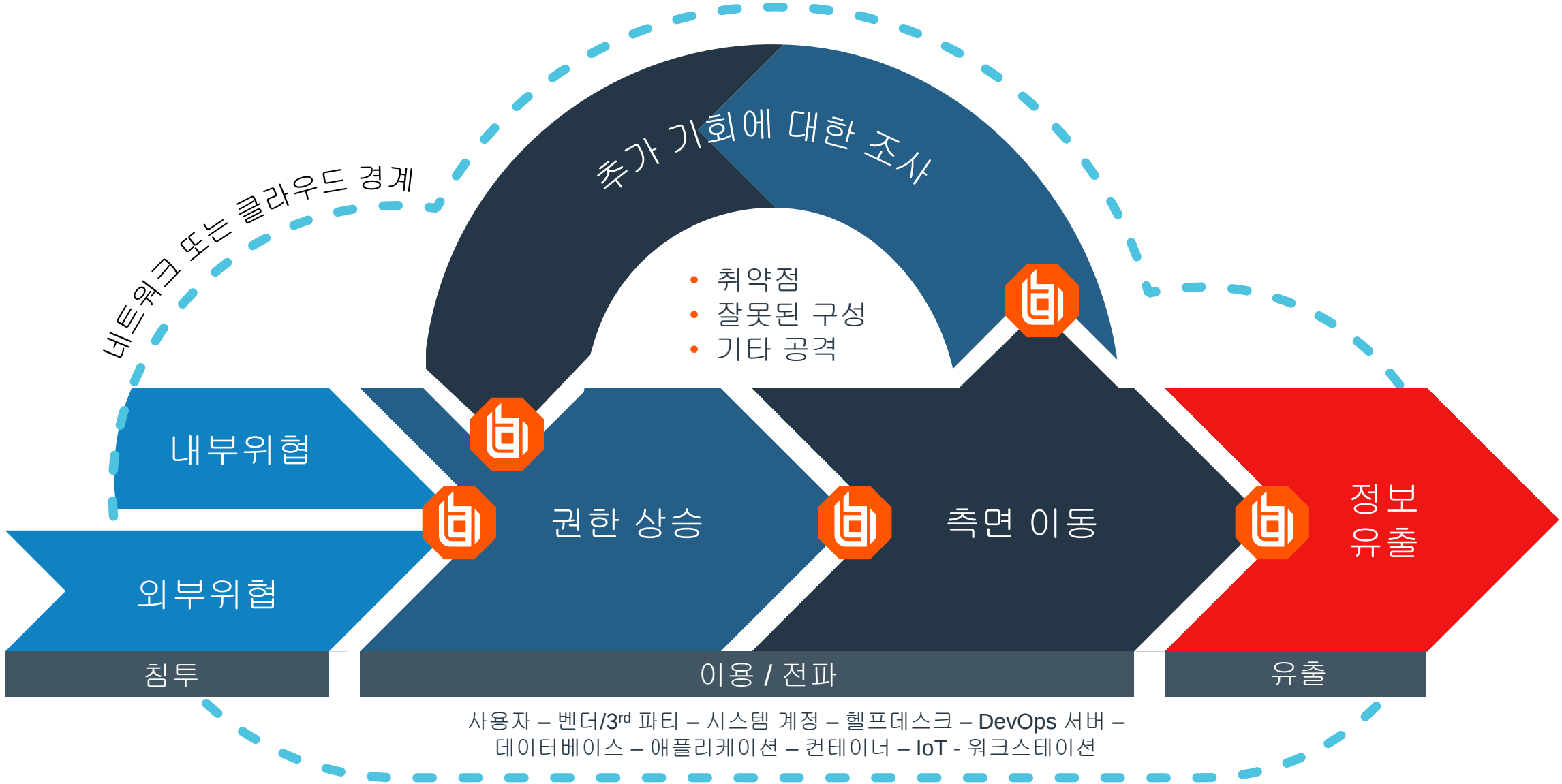
내부 침입자 → 외부 침입자 → HIDDEN THREATS

# 전통적인 암호 관리는 제한적인 공격백터에만 대응 가능



하지만,
최근
공격백터는
과거대비
다양함

# 사이버 공격 체인


네트워크 또는 클라우드 경계
추가 기회에 대한 조사
• 취약점
• 잘못된 구성
• 기타 공격
내부위협
외부위협
권한 상승
측면 이동
정보 유출
침투
이용 / 전파
유출
사용자 – 벤더/3rd 파티 – 시스템 계정 – 헬프데스크 – DevOps 서버 –
데이터베이스 – 애플리케이션 – 컨테이너 – IoT - 워크스테이션

# Top 3
# Privileged Use Cases

# 임직원, 공급업체 & 내부자의 과도한 시스템 및 데이터 액세스

해당 액세스가 모니터링되지 않을 수 있음

**99%**

사용자 장치를 감염시키는 데 필요한 상호 작용이 관찰된 위협

**182**

공급업체의 주간 평균 시스템 로그인 횟수

**583**

기업이 민감한 정보를 공유하는 **3rd Party** 평균

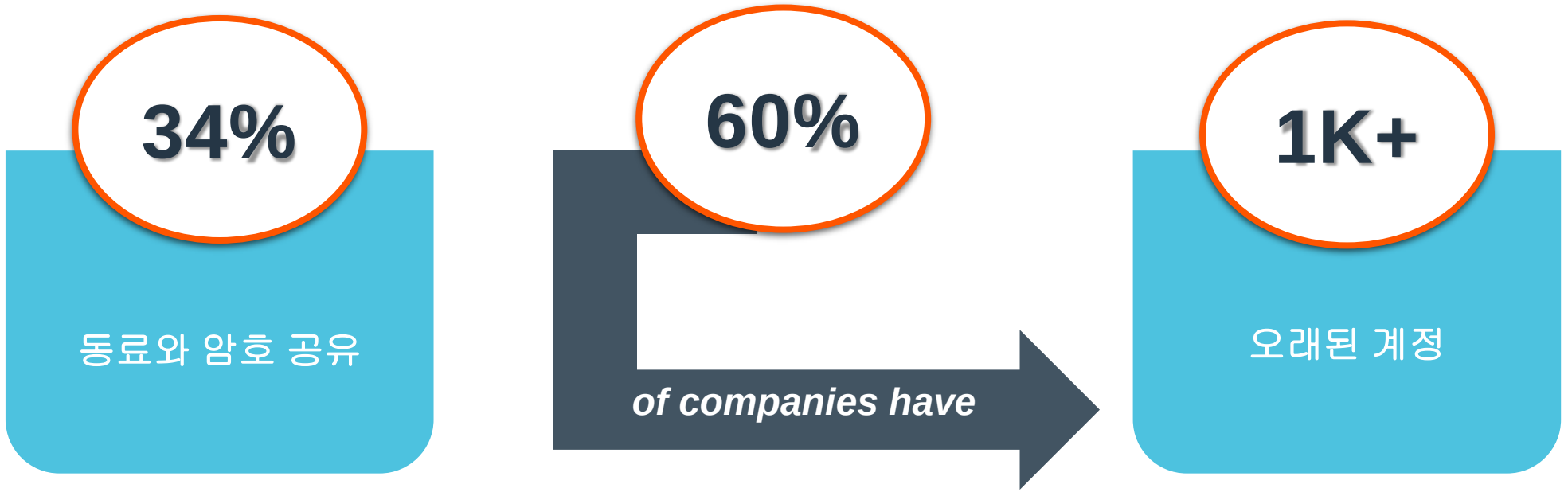
**60%**

작년에 내부자 공격을 경험한 기업

Sources: 2019 Human Factor Report, Proofpoint | BeyondTrust 2019 Privileged Access Threat Report | 2018 Third-Party Data Risk Study, Opus & Ponemon Institute | Nucleus Cyber 2019 Insider Threat Report, conducted with Cybersecurity Insiders

# 자격증명 공유 및 관리부재

비밀번호 사용은 규칙이나 감사, 모니터링 또는 관리되지 않고 있습니다




Sources: SurveyMonkey, 2019 | 2018 Global Data Risk Report, Varonis

# IT 자산들의 네트워크 설정 문제

데스크톱, 노트북, 서버 및 애플리케이션이 중요한 자산 및 데이터에 대한 네트워크 통신 및 개방 경로 제공


## 권한 오용

- 전체 위협 패턴 상위 3개 중 하나
- 몇 개월 이상 발견되지 못한 위반 중 가장 일반적인 패턴

Sources: Global Incidence Response Threat Report, Carbon Black, July 2018 | Verizon 2019 Data Breach Investigations Report

# 10 Steps To Securing Your Privileged Users

# 범용 권한 관리로의 전환

## 어디서나 시작하고 위험을 신속하게 줄입니다


*Top 4 Use Cases

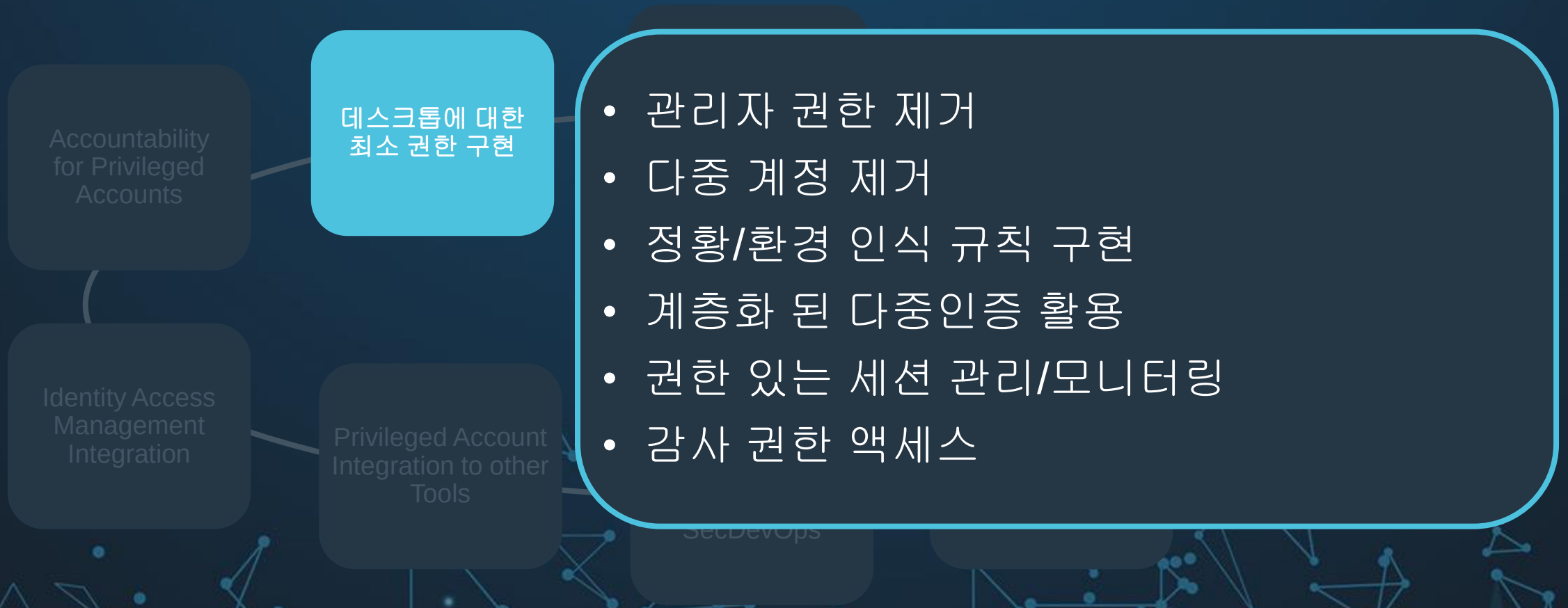
# 권한 있는 계정에 대한 책임

권한 있는 계정에 대한 책임

Identity Access Management Integration

- 권한 있는 계정 자동 검색 및 온보드
- 암호 및 키 로테이션
- 하드코딩된 계정 제거
- 분할 운영 (Segmentation)
- 모든 권한 있는 세션 모니터링/관리
- 권한 있는 사용자 동작 분석

# 데스크톱에 대한 최소 권한 구현



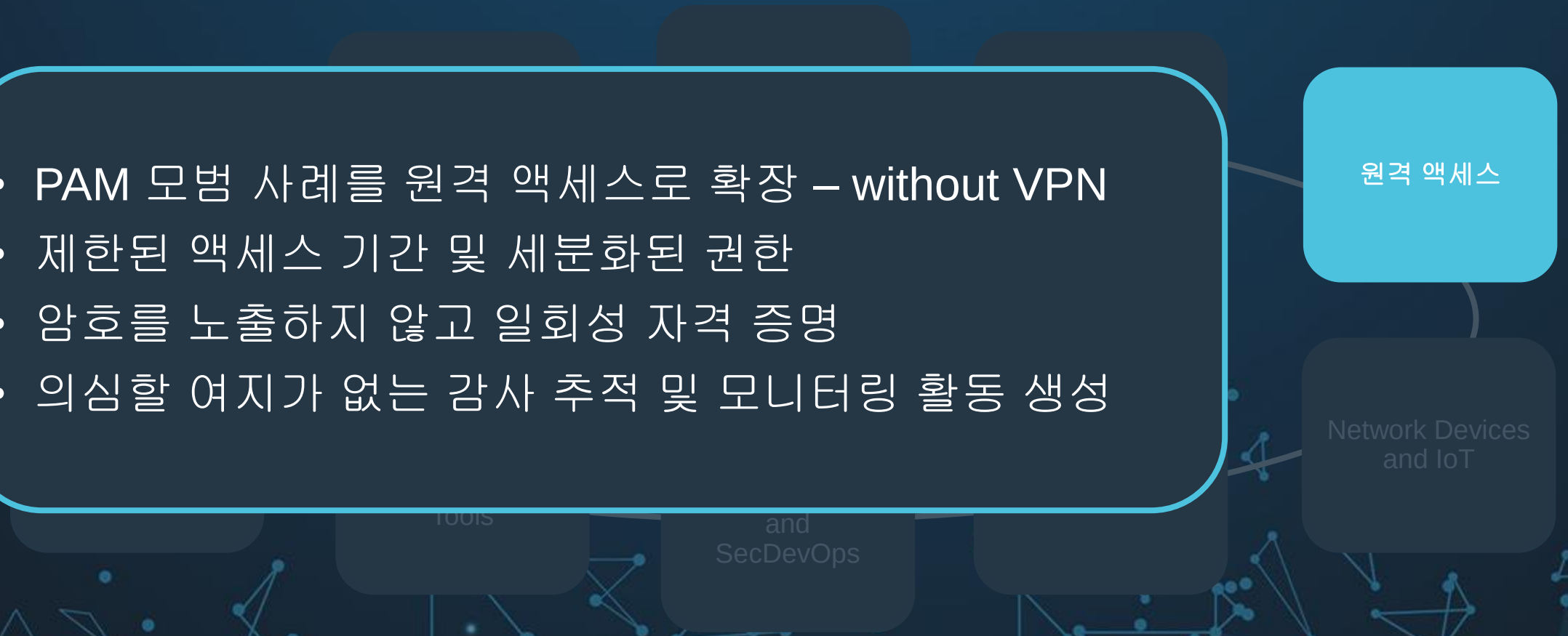

- 관리자 권한 제거
- 다중 계정 제거
- 정황/환경 인식 규칙 구현
- 계층화 된 다중인증 활용
- 권한 있는 세션 관리/모니터링
- 감사 권한 액세스

# 서버에 대한 최소 권한 구현


- 루트 액세스 제거
- 스크립트, 명령 및 쉘을 세부적으로 제어
- 권한 분리 구현
- 상시(Always-On) 액세스 제거
- 파일 무결성 모니터링
- 권한 있는 세션 모니터링
- 모든 권한 있는 액세스 감사

# 원격 액세스

- PAM 모범 사례를 원격 액세스로 확장 – without VPN
- 제한된 액세스 기간 및 세분화된 권한
- 암호를 노출하지 않고 일회성 자격 증명
- 의심할 여지가 없는 감사 추적 및 모니터링 활동 생성

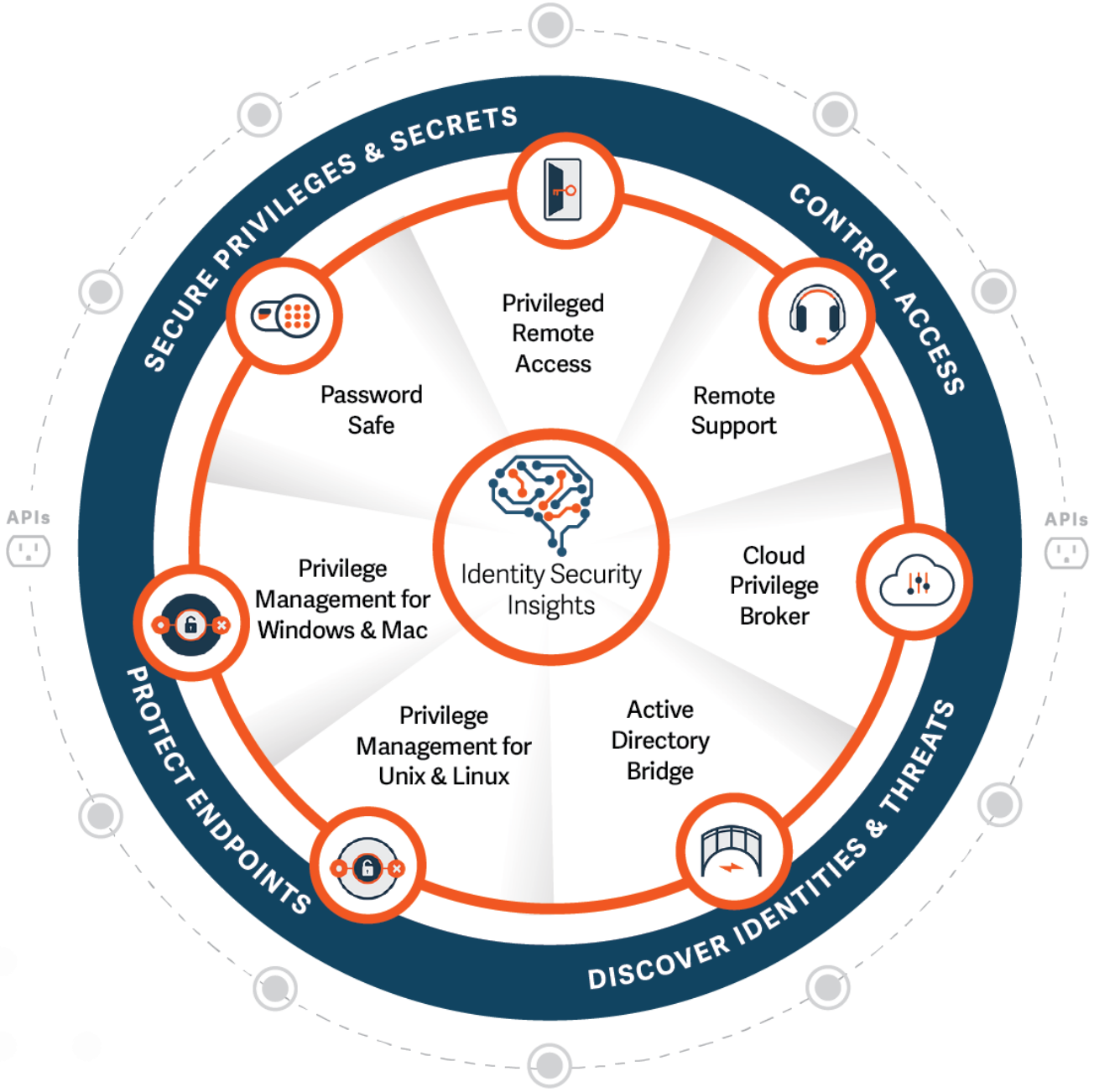


# BeyondTrust

## UNIVERSAL PRIVILEGE MANAGEMENT

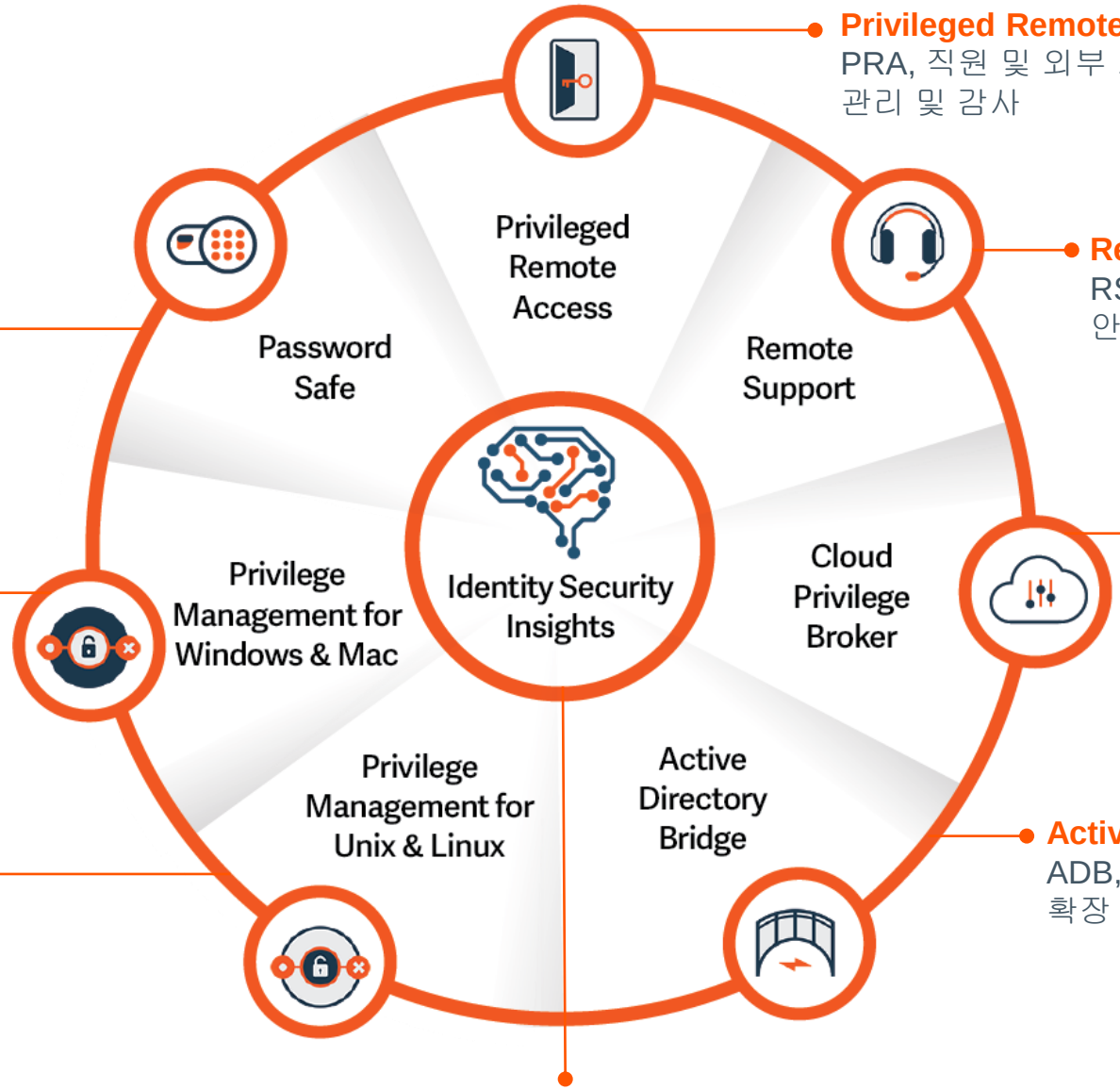
BeyondTrust

# Platform



BeyondTrust

# Platform




**Privileged Remote Access**
PRA, 직원 및 외부 사용자 원격 액세스 관리 및 감사

**Remote Support**
RS, 전 세계 모든 장치 또는 시스템에 안전하게 액세스하여 지원 작업 수행

**Password Safe**
PWS, 권한 있는 자격 증명 및 Secrets에 대한 가시성 확보 및 제어

**Cloud Privilege Broker**
CPB, 클라우드 전반에서 권한 시각화 및 권한 조정 제안

**Privilege Management for Windows & Mac**
PMfWM, 최소 권한 적용 및 애플리케이션 제어

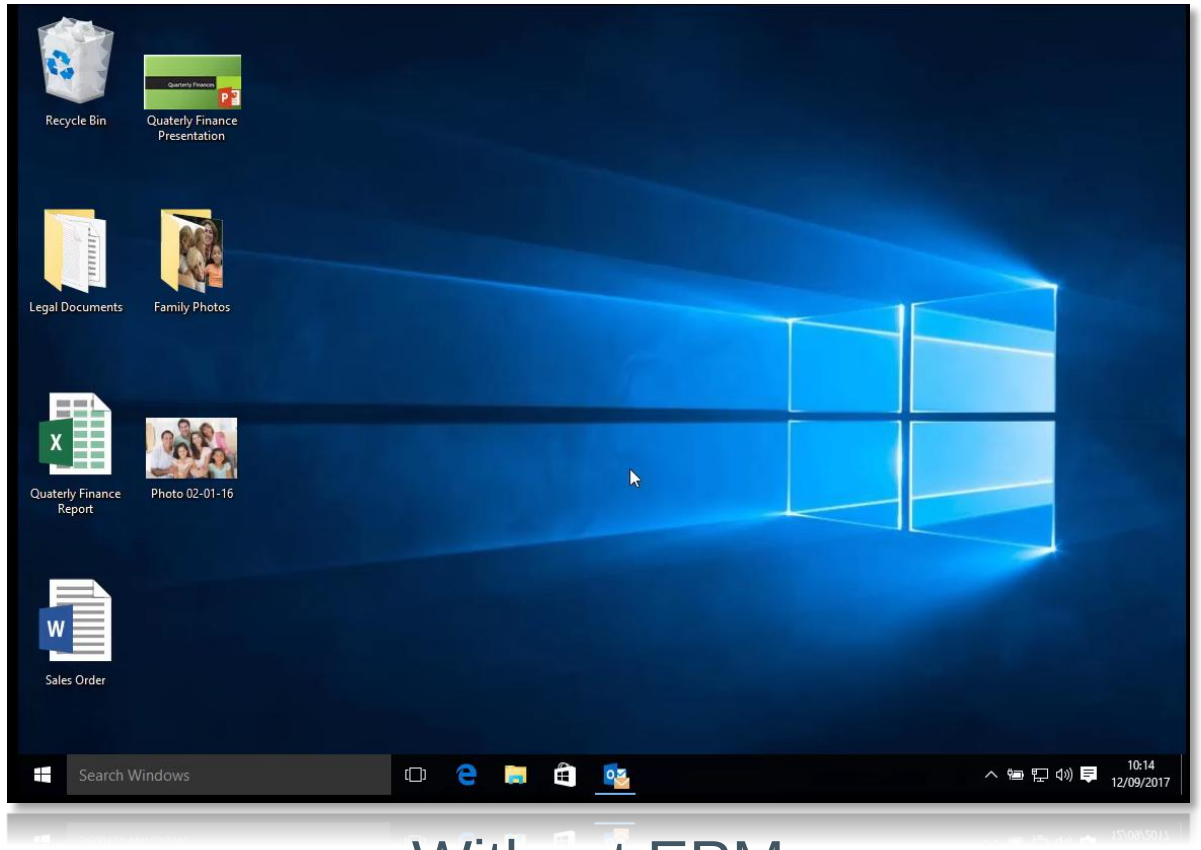
**Active Directory Bridge**
ADB, 유닉스/리눅스 인증 및 그룹 정책 확장 및 관리

**Privilege Management for Unix & Linux**
PMUL, 리눅스 및 유닉스 운영체계 환경에 대한 권한 액세스 보안 구현

**Identity Security Insights**
단일 인터페이스에서 전제 IT 자산에 대한 ID및 액세스에 대한 통합 대시보드

# Trusted Application Protection

실 사례 - Locky Ransomware (.lukitus)


Without EPM



With EPM & TAP

# THANK YOU!

BeyondTrust