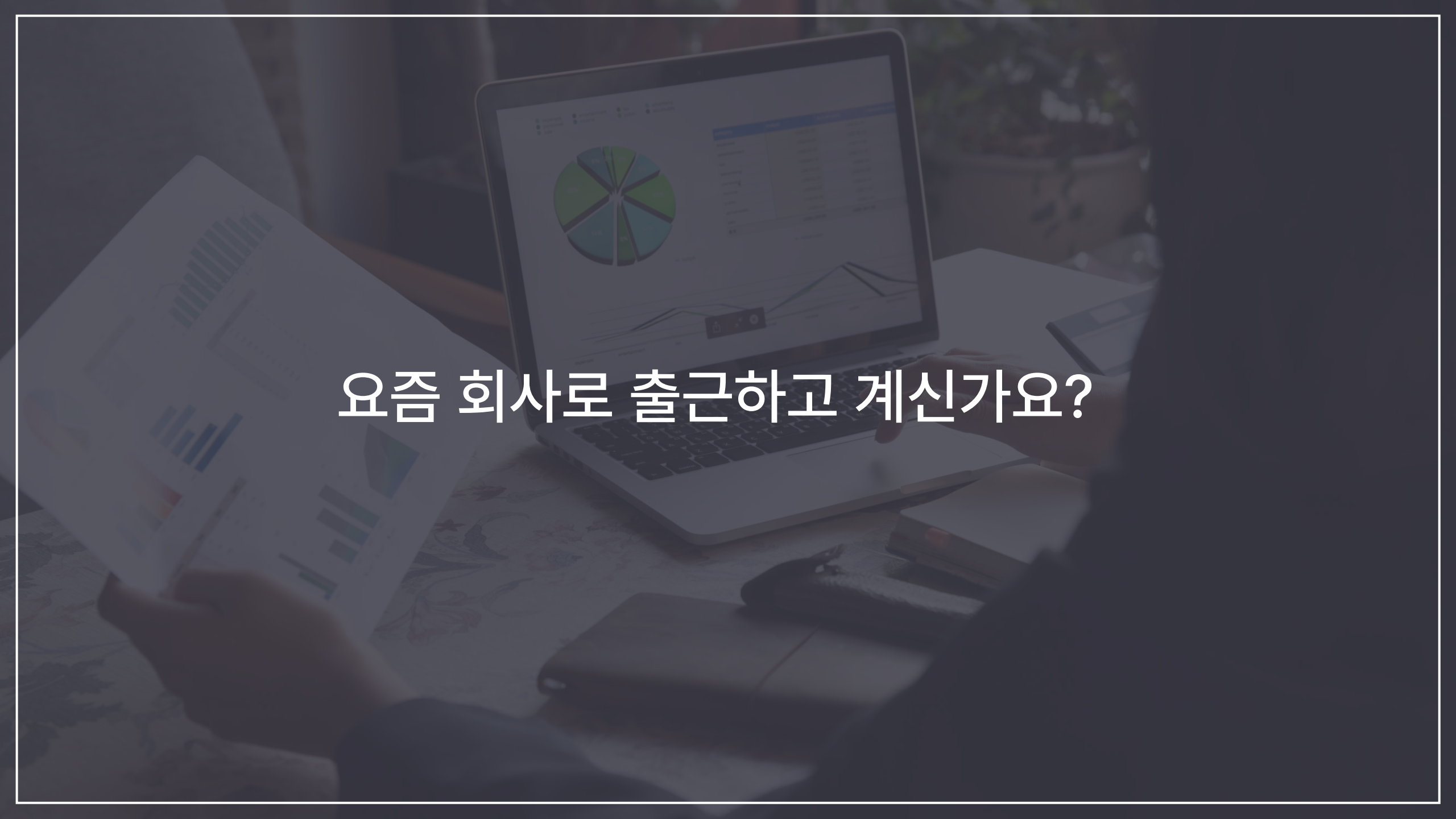
재택근무 보안의 조건

TOCSG
투씨에스지

투씨에스지 사업전략팀
이강일 매니저


요즘 회사로 출근하고 계신가요?

포스트 코로나 시대 하이브리드 근무 환경의 일상화

사무실 근무와 재택근무의 병행

대면 협업과 디지털 협업의 병행

선호하는 재택 근무 일 수 *중복 응답 허용

32% 주5일 사무실 출근

47% 주2일 재택 근무

45% 주3일 재택 근무

40% 주5일 재택 근무

다시 사무실 풀타임으로 돌아가면 이직을 고려하겠다.

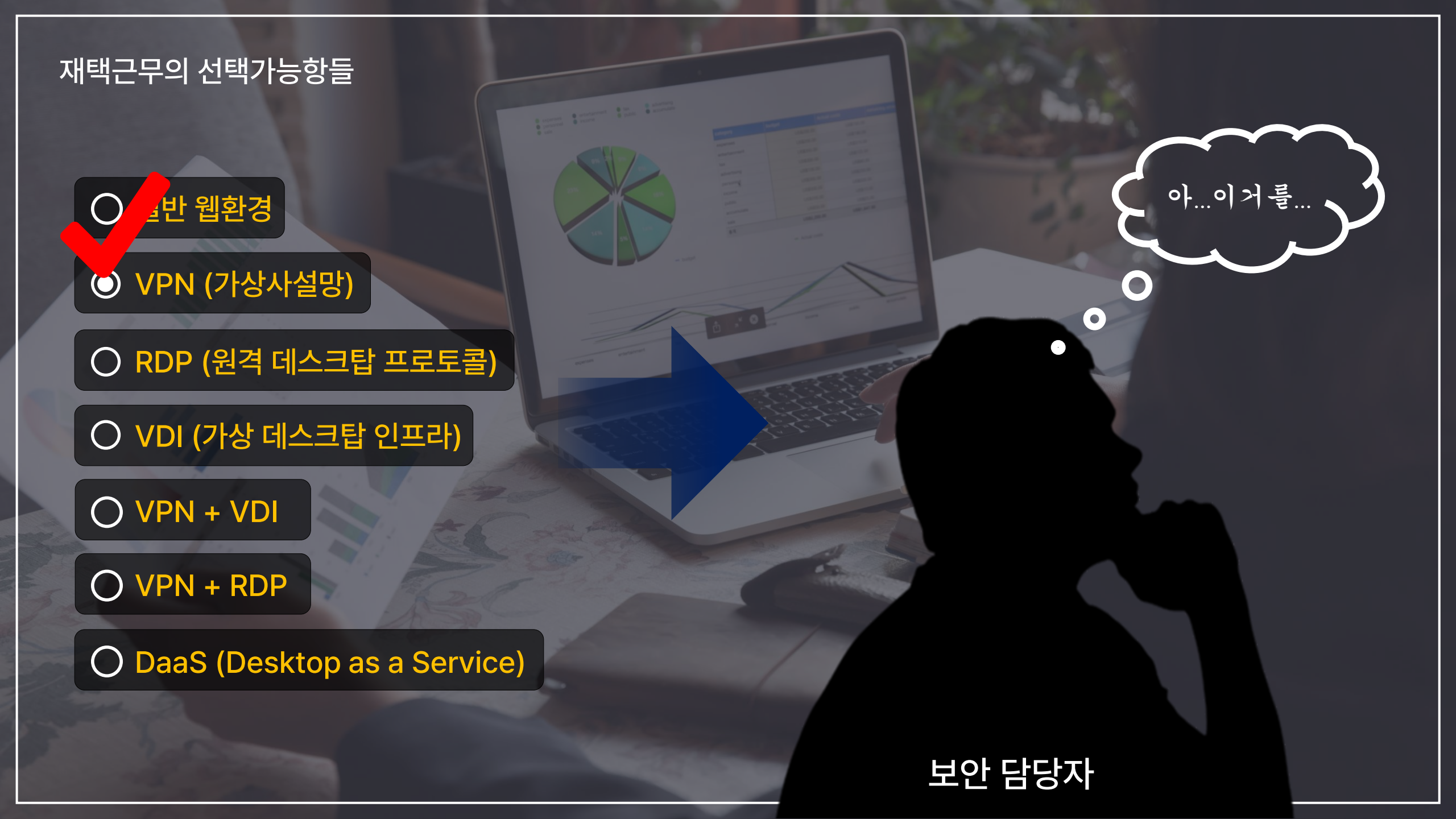
18% 한국

33% 글로벌

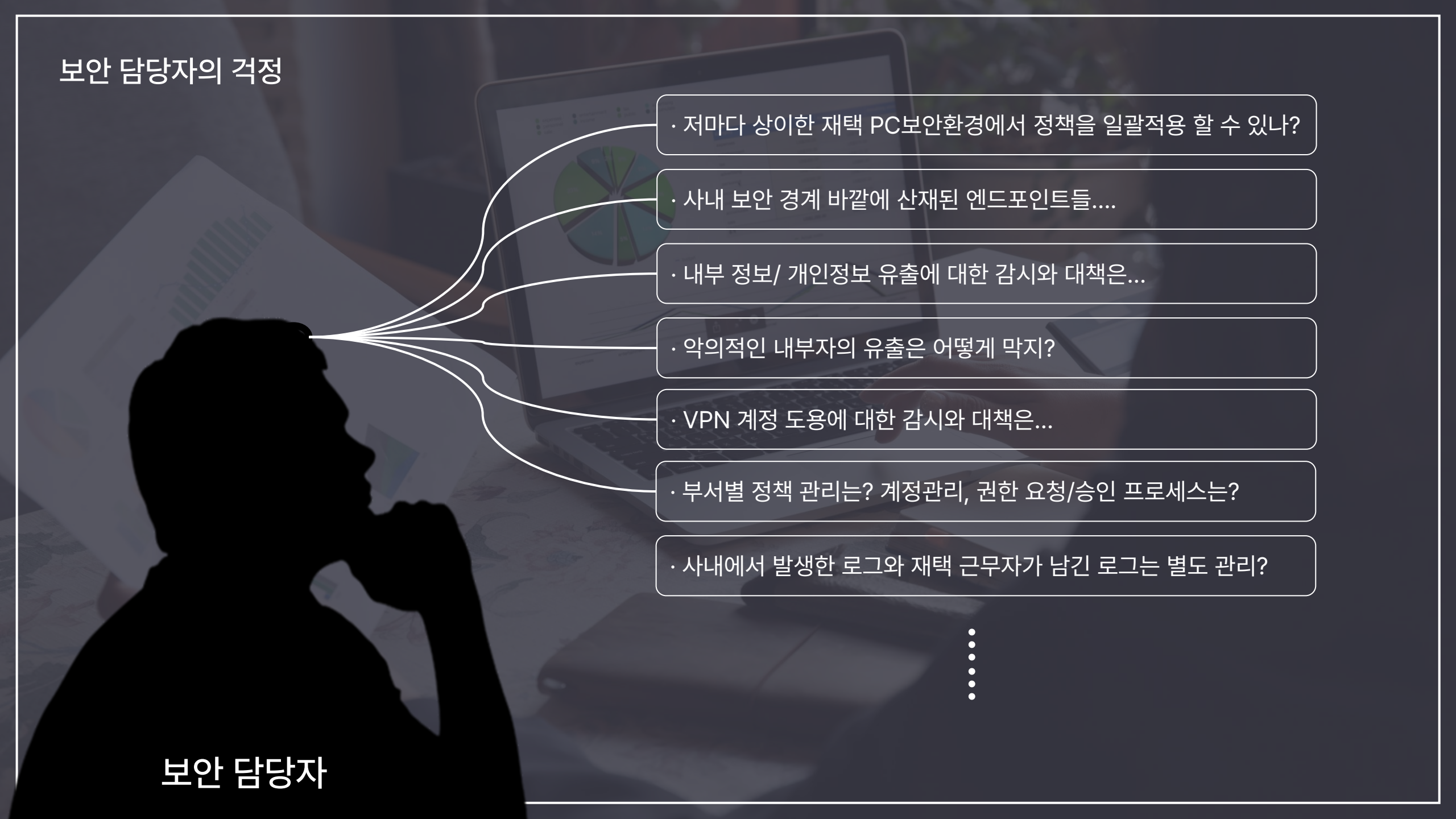
<2022 직원경험 트렌드 보고서, 퀄트릭스 코리아>

재택근무의 선택가능항들

- [ ] 일반 웹환경
- [x] VPN (가상사설망)
- [ ] RDP (원격 데스크탑 프로토콜)
- [ ] VDI (가상 데스크탑 인프라)
- [ ] VPN + VDI
- [ ] VPN + RDP
- [ ] DaaS (Desktop as a Service)



보안 담당자의 걱정



- 저마다 상이한 재택 PC보안환경에서 정책을 일괄적용 할 수 있나?
- 사내 보안 경계 바깥에 산재된 엔드포인트들....
- 내부 정보/ 개인정보 유출에 대한 감시와 대책은...
- 악의적인 내부자의 유출은 어떻게 막지?
- VPN 계정 도용에 대한 감시와 대책은...
- 부서별 정책 관리는? 계정관리, 권한 요청/승인 프로세스는?
- 사내에서 발생한 로그와 재택 근무자가 남긴 로그는 별도 관리?

보안 담당자

재택근무 보안 영역 구분

재택 단말기 보안

단말기 자체의 무결성

통신 구간 보안

구간 위변조, 중간 탈취 행위

네트워크 접근제어

사용자 접근 통제

데이터보안

데이터 외부 유출 방지 / 유출 탐지

보안리스크 탐지

모니터링, 관제, 대응

재택 근무 관리

정책 적용, 권한/승인 , 현황

‘보안 담당자의 걱정’ 세부 목록과 대응방법

재택 단말기 보안

- 최신 백신 설치 확인 / 미적용 차단
- 최신 보안 패치 확인 / 미적용 차단
- 윈도우 로그인 패스워드 설정 확인
- 화면 보호기 활성화 확인
- 개인 방화벽 활성화 확인
- 일정 시간 뒤 강제 잠금 지원
- 취약한 프로그램 차단

백신
최신 보안패치
방화벽 설정

네트워크 + 접근통제

- 사용자 인증
- 단말기 인증
- Host 파일 위변조 차단
- Route Table 변경 차단
- 레지스트리 변경 내역 모니터링
- 화이트 리스트 체크
- 블랙 리스트 차단
- 취약점 PC의 VPN접속 제한
- 취약점 발생시 VPN 실시간 차단

NAC
EDR

데이터 보안

- USB 등 매체제어
- 화면캡쳐 방지
- 개인정보 등 중요 정보에 마스킹처리
- 내부 전산자료 출력 금지
- 이미지 워터마크 / 스크린 워터마크
- 파일 송수신 차단
- 외부 단말기 저장 금지
- 특정 포트 차단
- 파일 내용을 텍스트로 추출하여 관제

DLP
DRM
화면캡쳐 방지 솔루션
USB차단 솔루션
출력물 보안 솔루션

관리 기능

- 인사시스템 연동
- 부서별 정책 적용
- 긴급 사용 승인
- 계정별 권한 관리
- 재택 근무자 보안서약서 청구
- Agent 자동 패치
- 접속이력, 보안이벤트 로그
- 실시간 경고
- 접속현황, 실시간 취약점 현황 제공

통합 관리 콘솔

재택근무가 야기한 새로운 보안 이슈

재택근무 환경에서만 존재하는 근본적 문제 : 경유지의 발생 → 경우의 수 증가

✓ x의 행위가 y에게 영향을 주고 실제 업무행위는 y와 z사이에서 발생한다.

✓ A구간과 B구간에 특화된 제품을 적용한다 하더라도, 이 행위간에 연결점을 찾아야 보안을 확보할 수 있다.

Ex) z로 대용량 DB 요청이 들어왔다. y에 의한 것인가? x에 의한 것인가?

재택근무가 야기한 새로운 보안 이슈

행위간에 연결점을 찾아야 보안을 확보할 수 있다.

- ✓ 사무실에서 B구간에 직접 연결하는 행위와 / A를 통해 B를 연결하는 행위가 구분되어야 한다.
- ✓ A구간을 사용하는 경우에는 기존 사내 보안과 다른 보안정책과 대응방안이 필요하다.
- ✓ 이 흐름 전체가 관리자에게 관제 될 수 있어야 한다. (분절 X, 분산 X)

재택근무가 야기한 새로운 보안 이슈

데이터 보안 범위 확장

- ✓ 재택 근무에서는 x에서 y까지만 접근해도 정보를 유출 시킬 수 있기 때문에,
- ✓ y가 확보한 정보를 관제하는 것과, y의 정보가 x에서 열람, 전달 되는 행위에 대한 관제 소요 추가 발생
- ✓ 때문에, x에서 업무 중 로컬에서 생성되는 정보의 관제, y가 보유한 정보를 관제할 필요.
  → x-y 간 통합된 데이터 보안 정책이 필요

재택근무가 야기한 새로운 보안 이슈

데이터 보안 범위 확장

- 재택 근무에서는 x에서 y까지만 접근해도 정보를 유출 시킬 수 있기 때문에,
- y가 확보한 정보를 관제하는 것과, y의 정보가 x에서 열람, 전달 되는 행위에 대한 관제 소요 추가 발생
- 때문에, x에서 업무 중 로컬에서 생성되는 정보에 대해서 관제해야하며, y가 보유한 정보를 관제할 필요.

Seamless log

끊김 없는, 매끄럽게 연결된

→ 한 번에 한 곳에서 전과정을 확인, 검색, 대응할 수 있는

Seamless log for Security

재택근무자 A씨가 남긴 하루동안의 발자취

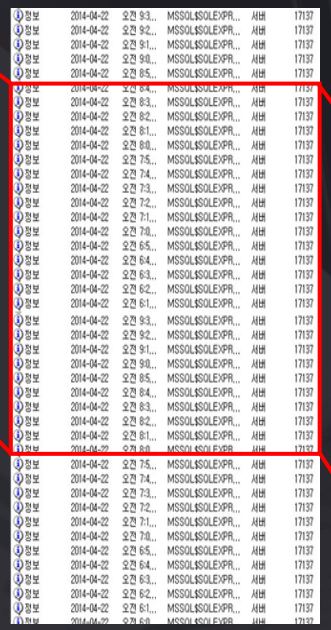
접속 로그

사내망 접속

로그아웃

VPN

시스템 로그



VDI

사용자 행위 로그

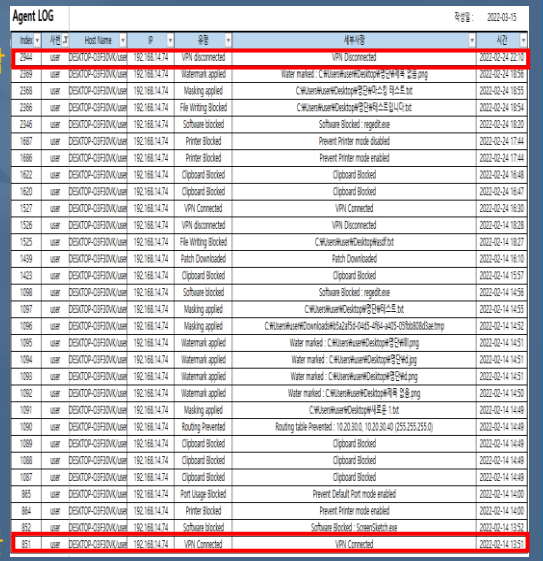
DLP

VS

접속 로그
시스템 로그
사용자 행위로그

근무 시작

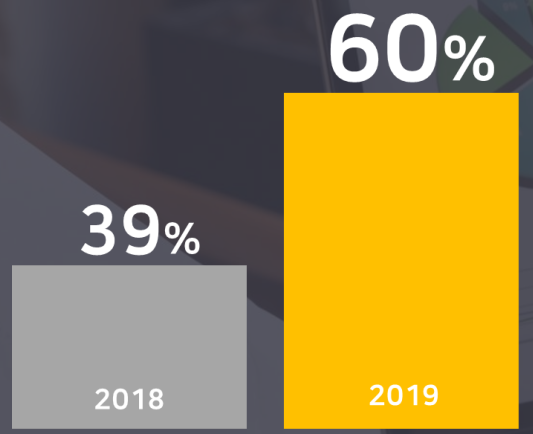
근무 끝



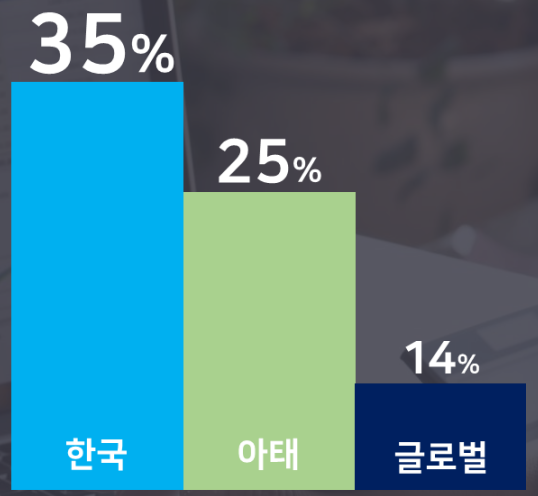
재택근무 통합 보안 솔루션

- 재택근무 시작과 끝의 명확한 구분 → 분석 범위의 특정
- 모든 보안 경고에 대한 원인분석(솔루션간 크로스 분석)을 담당자는 감당할 수 있는가?
- log의 확인, 검색, 대응의 일원화
- 보안 오케스트레이션 이전에 대응의 복잡성 부터 해결

Seamless log for Efficiency



CISO 사이버보안 피로도



일 10만건 이상 경고 수신

56%

10개 이상의 보안 벤더 사용

92%

"멀티 벤더 환경이 힘들다"

40%

보안경고 중 조사되는 비율

<CISCO,2019 아시아태평양 CISO 벤치마크 연구>

Seamless log for integration

통합 = 기능의 통합 + 관리/통제 수단의 통합 + **로그의 일원화**

VPN
DLP
NAC
VDI
DRM
EDR
각종 포인트 솔루션들

이 쏟아내는 로그데이터

- 보안 경고 원인분석 가능?
- 신속 대응 가능?
- 추가 업무량 감당 가능?
- 전담 인력 충원 가능?
- 보안 인프라 운용 하나더?

조건 1. Seamless log

개별 PC의 보안 관리는?
회사꺼 말고 개인 노트북도 가능?
사내망 접근 권한 관리는?
USB/화면캡쳐/프린터까지 통제 가능?
취약점 / 이상징후 발견시 차단가능?
개인정보 비식별처리는?
인사 시스템과 연동은?
정책 자동화 가능?
모니터링 / 리포트 / 감사 가능?
자동 패치 업데이트 가능?
중앙 관리 가능?

필요한 포인트 솔루션 10여개

- DLP (Data Loss Prevention)
- NAC (Network Access Control)
- PC보안 솔루션
- 내 PC 지키미 솔루션
- 화면캡쳐 방지 솔루션
- 화면 워터마크 솔루션
- USB차단 솔루션
- 출력물 보안 솔루션

통합 솔루션

관리소요
구매비용 ↓

조건 2. 행위관리 + 연결 관리

재택근무PC 사용자 행위관리

행위 관리

연결 관리

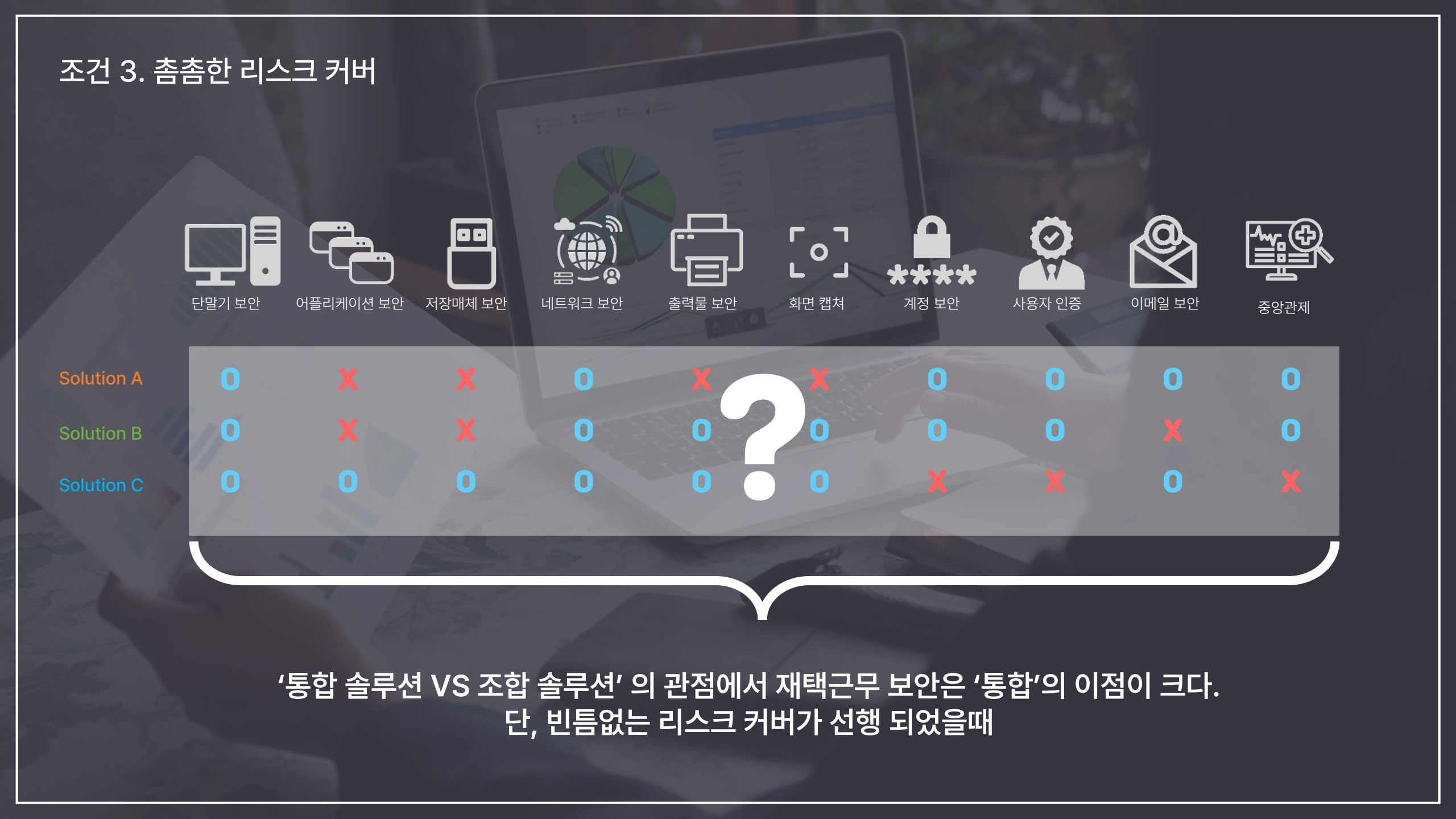
- 원격 접속 제어
- 업무중 외부 인터넷 차단
- 시스템 방화벽 관리
- IP / URL 필터링
- 파일 전송 Port 차단

사내망 연결 관리 및 정보유출 방지

뭘 하는지 + 무슨 일이 일어나는지 모니터링/제어

누가 접속 중인지 / 정상적인 접근인지

조건 3. 촘촘한 리스크 커버



‘통합 솔루션 VS 조합 솔루션’ 의 관점에서 재택근무 보안은 ‘통합’의 이점이 크다.
단, 빈틈없는 리스크 커버가 선행 되었을때

조건 4. 컴플라이언스

컴플라이언스	주요 요구사항
재택근무 시 지켜야할 정보보호 6대 실천 수칙 (과학기술정보통신부, 한국인터넷진흥원)	<보안관리자 실천 수칙> • 원격근무시스템 (VPN) 사용 권장 • 재택근무자 대상 보안지침 마련 및 보안인식 제고 • 개인정보, 기업정보 등 데이터 보안 (랜섬웨어 감염 주의) 등
비대면 업무환경 도입•운영을 위한 보안가이드 (과학기술정보통신부, 한국인터넷진흥원)	<원격근무 환경 도입•운영을 위한 보안> • (단말기 보안) 노트북, 스마트폰, 태블릿 등의 보안 업데이트를 최신 상태로 유지 • (프로그램 보안) 모든 프로그램 보안 업데이트를 최신 상태로 유지 / 백신, DLP 등 단말기 및 데이터 보호 프로그램 사용하기 • (보호대책 수립 등) 접근 허용 범위 기간 설정, 구간 암호화 단말 보안 등
개인정보보호법 (행정안전부 고시,개인정보의 안전성 확보조치 기준)	<제5조 접근통제> 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상시설망 (VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.
전자금융감독규정 (금융감독원, 전자금융감독규정 시행세칙 망분리 대체 정보보호통제)	<원격 접속 : 외부 단말기 공통사항> • 백신 프로그램 설치, 실시간 업데이트 및 검사 수행 • 안전한 운영체제 사용 및 최신 보안패치 적용 • 로그인 비밀번호 및 화면 보호기 설정 • 화면 및 출력물 등으로 인한 정보유출 방지대책 적용

재택근무 보안의 조건

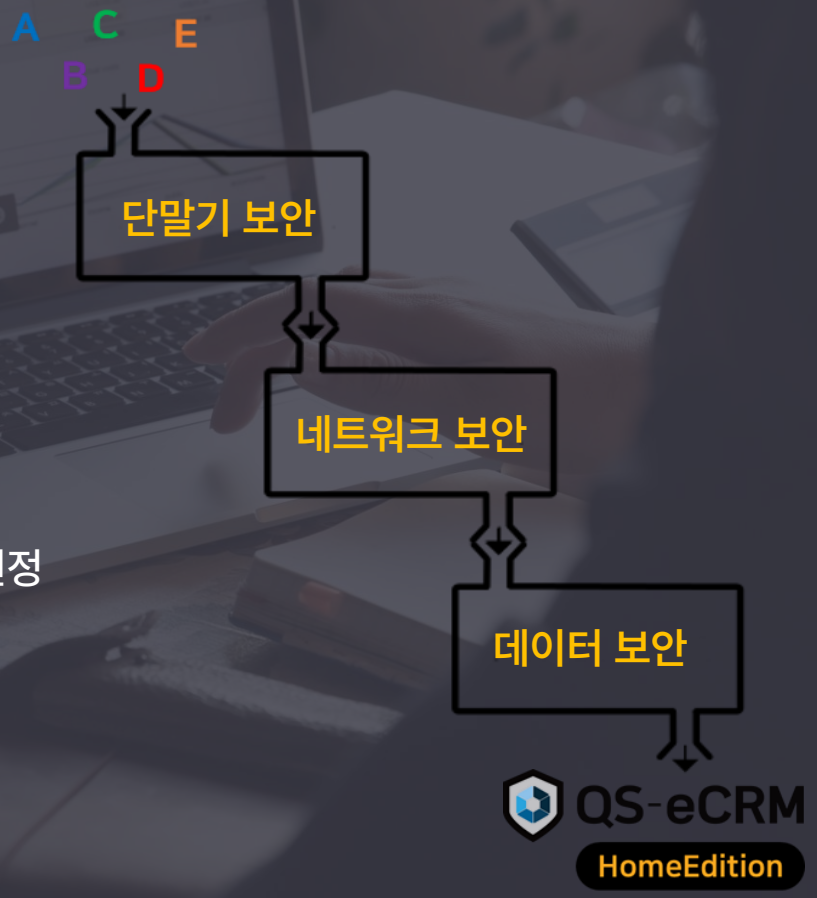
Seamless log

행위관리 + 연결관리

촘촘한 리스크 커버

컴플라이언스 준수

금융권 재택근무 컴플라이언스 기관의 BMT를 유일하게 통과한
재택근무 전용 보안 솔루션



금융결제원
Korea Financial Telecommunications & Clearings Institute

「원격접속 단말기 보안통제 강화 관련 IT자원 도입 사업」 선정