라온시큐업 2021

BEYOND THE DIGITAL WORLD

RAON

기업보안과 임직원 편의성을 한 번에!

IT관리자를 위한 원격근무 가이드

라온시큐어 김형관 팀장

INDEX

01 배경 및 필요성

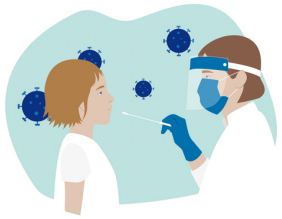
1-1. COVID-19 바이러스 위협
1-2. 원격 · 재택 근무의 확대와 전망
1-3. 원격 · 재택 근무 주요 보안위협

COVID-19 바이러스 위협

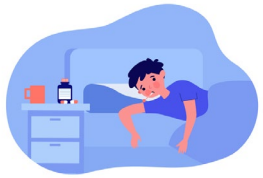
COVID-19 변종 출연과 돌파 감염 등 바이러스로 인한 기업 경영과 근무 환경의 불확실성 지속

코로나 팬데믹

감염

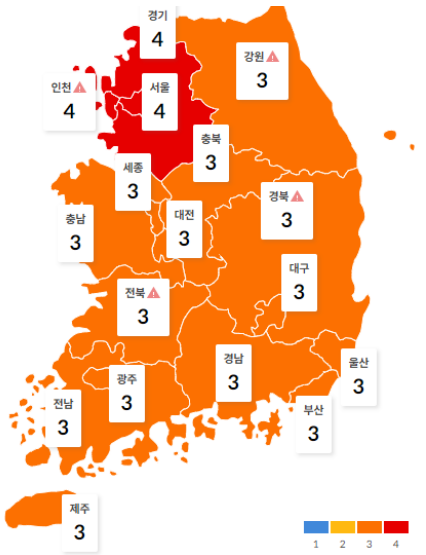


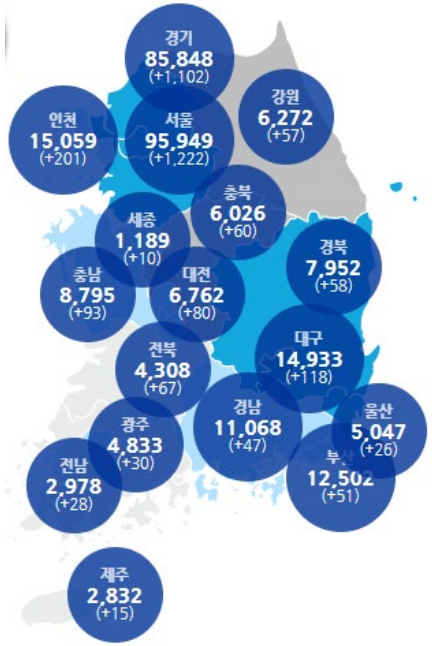
PCR 검사



자가격리

사회적 거리두기





*전국 확진자 현황, 출처 : 보건복지부

원격 · 재택 근무의 확대와 전망

COVID-19 대응 유연근무제 시행과 원격 · 재택 근무를 통한 근로 환경 변화 및 보안강화 필요성 대두

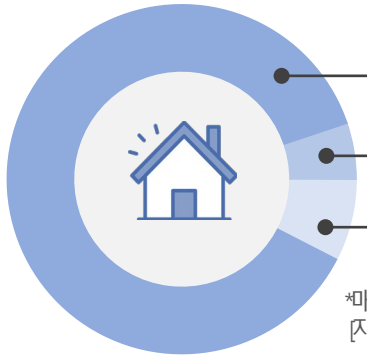
코로나19로 인한 재택근무 경험 비율

경험없음 21.7%

경험있음 78.3%

*직장인 897명 대상 설문조사 [자료=휴넷]

매출 100대 기업 재택근무 시행 현황



재택근무 시행중 88.4 %

곧 시행 예정 2.9 %

미시행 8.7 %

*매출 100대 기업중 응답기업 82개사 분석
[자료=한국경영자총협회(202009)]

코로나19로 인한 사내 보안 강화 필요성

영향없다 32.8%

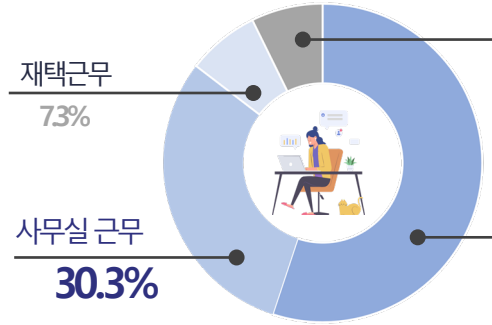
67.2% 보안강화 필요성 커졌다

사내 보안 강화가 필요한 이유 (복수응답)

- 54.9% USB, 외장하드, 장비 등 외부 이용이 불가피해서
- 40.9% 재택 시 회사 내부보다 보안이 취약해서
- 36.6% 직원들의 보안 의식이 낮아서
- 33.5% 안전하지 않은 네트워크 사용 때문에
- 28.7% 개인 기기 사용이 많아서

*기업 244개사 설문조사 [자료=사람인]

코로나19 종식 이후 근무 형태



재택근무 7.3%

잘모르겠다 7.3%

사무실 근무 30.3%

사무실과 재택 근무 병행하는 유연근무 55.1%

*전국18세 이상 성인 1000명 대상 설문조사
[자료=데이터리서치(202106)]

원격 · 재택 근무 주요 보안 위협

원격 · 재택 근무에 따른 사내망 및 업무시스템 접속 시 다양한 보안 취약점으로 인한 보안 위협 발생

원격/재택 근무용 단말기의 관리 및 통제 미흡

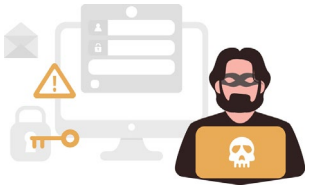
· 원격근무 접속 단말기의 분실, 도난과 화면 훔쳐보기, 캡쳐 등으로 인한 중요 데이터의 노출 및 유출 등 위험 가능

안전하지 않은 네트워크 사용

· 원격근무자가 사용하는 외부 네트워크(인터넷망)는 통제가 어려워 도청이나 중간자 공격(MITM) 등으로 중요 정보 유출 가능
· 잘 못된 네트워크 장비 설정(VPN 등)이나 원격/재택 시 사용하는 네트워크 장비 취약점 존재

바이러스 · 악성코드 감염에 따른 침해

· 각종 바이러스와 악성코드, 공격툴 등에 감염된 원격근무 단말기로 회사 내부망이나 업무 시스템에 접속 시 시스템의 감염 가능
· 원격근무자에 피싱 메일 등을 이용하여 악성코드(Malware) 유포 및 원격 접속 시 사용자 인증 정보 등의 중요 데이터 유출 가능



내부 자원에 대한 원격접근 위협

· 기업 내부에서만 접근 가능했던 내부 정보 및 시스템 자원에 대한 원격 접속이 가능해짐에 따라 비인가 접근 등 불법 접속으로 인한 보안 위협 존재

* [NIST] Guide to Enterprise Telework, Remote Access and BYOD Security 외 참고

02 원격·재택 근무 지침/가이드

2-1. 원격 · 재택 근무 보안 수칙 가이드
2-2. 원격 · 재택 근무 보안 관리 지침사항

원격 · 재택 근무 보안 수칙 가이드

안전한 원격/재택 근무환경 조성을 위한 IT관리자 검토해야 할 기본 보안 수칙 10가지

1. 업무용 시스템 접속시 원격/재택 근무에 대한 의무사항 고지
2. 회사에서 허가 또는 지정 단말기 사용 권장
3. VPN 등 원격 접속 시 ID/PWD 인증 외 다중 인증 필수 적용
4. 여러 계정으로 접속을 금지하고 하나의 계정만으로 접속 관리
5. 관리자인 경우 IP 인증, 비밀번호 복잡도 적용을 통한 접근 허용
6. 기기 보안 상태가 최신 또는 보안설정 완료한 단말기만 접근 허용
7. 원격/재택 접근 단말기의 보안 취약점 지속 관리
8. 계정 통합 관리를 통한 보안 사고 대비 원격 통제 기능 적용
9. 사용자 권한 구분 및 로그 활성화 등 상시 모니터링
10. 악성코드 등의 감염을 대비하여 중요 자료의 백업 필수

원격 · 재택 근무 보안 관리 지침사항

국가정보원

구분	세칙	항목	내용	지원 솔루션
원격업무 통합보안매뉴얼	제2장 원격근무 4. 보안대책	가. 원격근무시스템 자체 구축 시 보안대책	· 원격 근무자 대상 OTP 등 이중 인증 수단을 활용, 인증 보안 강화 및 소관 업무범위에 따른 적절한 접근권한 통제 필수	OnePass TouchEn mOTP
			· 원격근무자용 전용 단말기의 적정 수량 확보 및 보안 관리 방안을 마련 - 원격근무용 단말기에는 VPN 클라이언트, 백신, 화면 캡처 방지 등 필수 SW 설치 및 기타 SW 설치 차단	TouchEn nxWeb TouchEn nxFirewall
	제3장 화상회의 6. 보안대책	나. 보안 인증을 받은 민간 클라우드 서비스 도입 시 보안대책	· 화상회의 사용자 대상 이중 인증 등 안전한 인증방식을 적용한 서비스 선택	OnePass TouchEn mOTP
		다. 화상회의시스템 활용 시 보안대책	· 화상회의 참여자는 화상회의시스템에 접속 시 사용자 식별 · 인증 후 회의에 참여 허용	TouchEn Wiseaccess OnePass / TouchEn mOTP
			· 화상회의실은 용역업체 직원 등 비 인가자 접근을 통제하고 회의 참가자는 스마트폰, 카메라, 휴대용 녹음기 등 불필요 장치 소지 불가	OneGuard
	제4장 온라인 교육 (국가 · 공공기관 직원 대상) 4. 보안대책	가. 자체 구축 시 보안대책	· 학습자 접근권한 통제를 위해 OTP 등 이중 인증 수단을 활용하여 인증보안 강화	OnePass TouchEn mOTP
		나. 보안 인증을 받은 민간 클라우드 서비스 도입 시 보안대책	· 학습자 접근권한 통제를 위해 OTP 등 이중 인증 수단을 활용하여 인증보안 강화	OnePass TouchEn mOTP
		다. 온라인 원격교육시스템 활용 시 보안대책	· 학습자는 교육자료 유출방지를 위해 단말기에 교육용SW · 보안SW 등을 설치 · 운용	TouchEn Anticapture OneGuard / TouchEn nxWeb

원격 · 재택 근무 보안 관리 지침사항

한국인터넷진흥원(KISA)

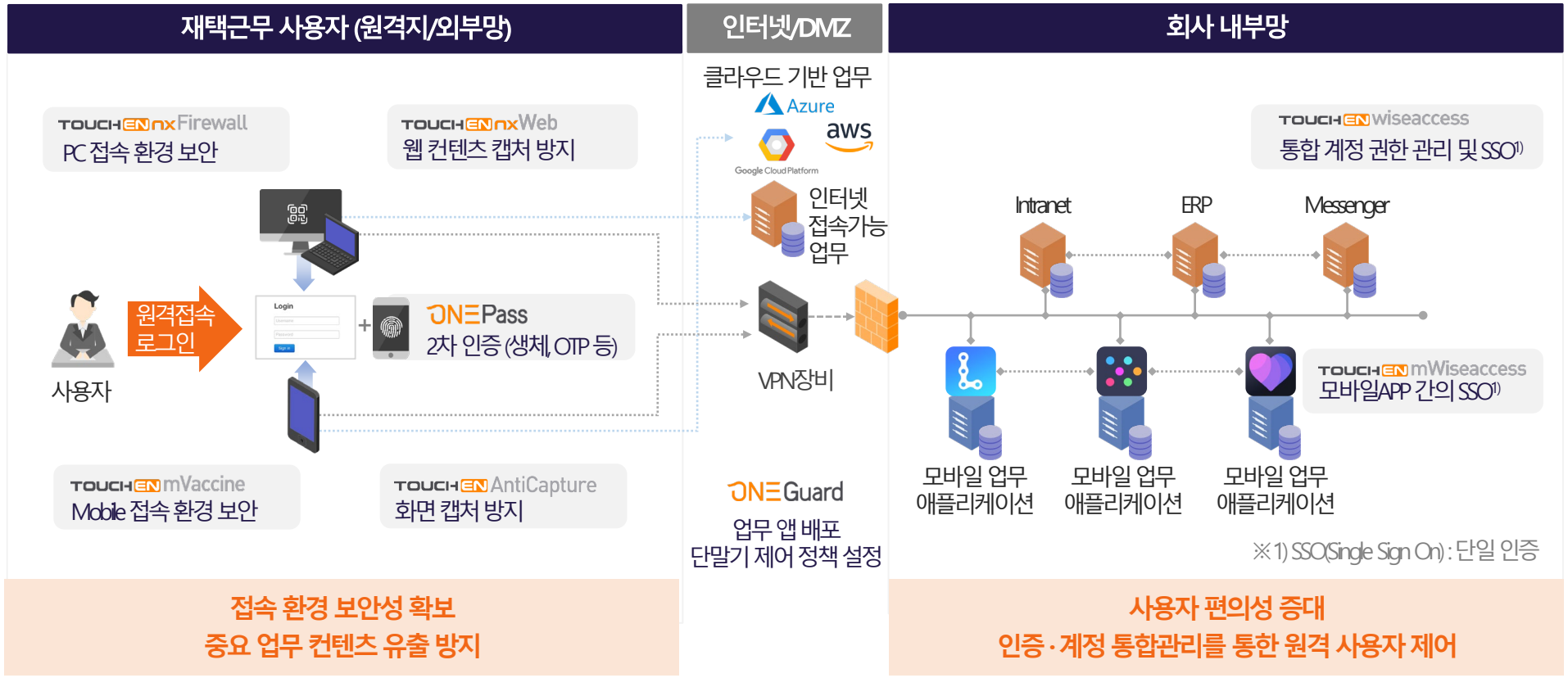
구분	세칙	항목	내용	지원 솔루션
비대면 업무 환경 도입 · 운영을 위한 보안 가이드	4. 비대면 업무환경 보안 강화 방안 2) 원격근무 환경 운영자 / 관리자 보안 수칙	(통합 인증체계 운영) 업무용 전산 환경의 모든 접속은 단일계정으로 통합인증을 수행	· VPN 접속, 업무용 응용 프로그램 로그인 등의 계정을 통합 관리함으로써 사용자 접속 이력 및 행위 추적성 확보 · 계정을 공유할 수 없도록 제한하고 개별 사용자마다 구분된 권한을 부여하여 사용자 별 이력 및 행위 추적성 확보	TouchEn Wiseaccess
		(원격 근무자 인증보안) 원격 근무자가 사내 네트워크에 접속하는 경우 다중 인증 등 강력한 인증 방안 사용	· 원격근무자 접속 인증 시 계정/비밀번호 외에도 추가적으로 OTP, 휴대전화 인증 등의 다중 인증 필수 적용 · 원격 근무자는 다중 접속을 허용하지 않고 하나의 인증 접속 만을 허용	OnePass TouchEn mOTP Key#biz

금융감독원

구분	세칙	항목1	항목2	내용	지원 솔루션
전자금융감독규정 시행 세칙	[별표7] 망분리 대체 정보보호통제 개정(안)	원격접속	원격접속단말기	· 외부단말기에서 내부 망에 직접 접속하는 경우 화면 캡쳐 차단	TouchEn nxWeb
			인증	· 이중 인증 적용 (예 : ID/PW + OTP)	OnePass TouchEn mOTP

03 원격·재택 근무 시나리오

원격 · 재택 근무 사용자 시나리오

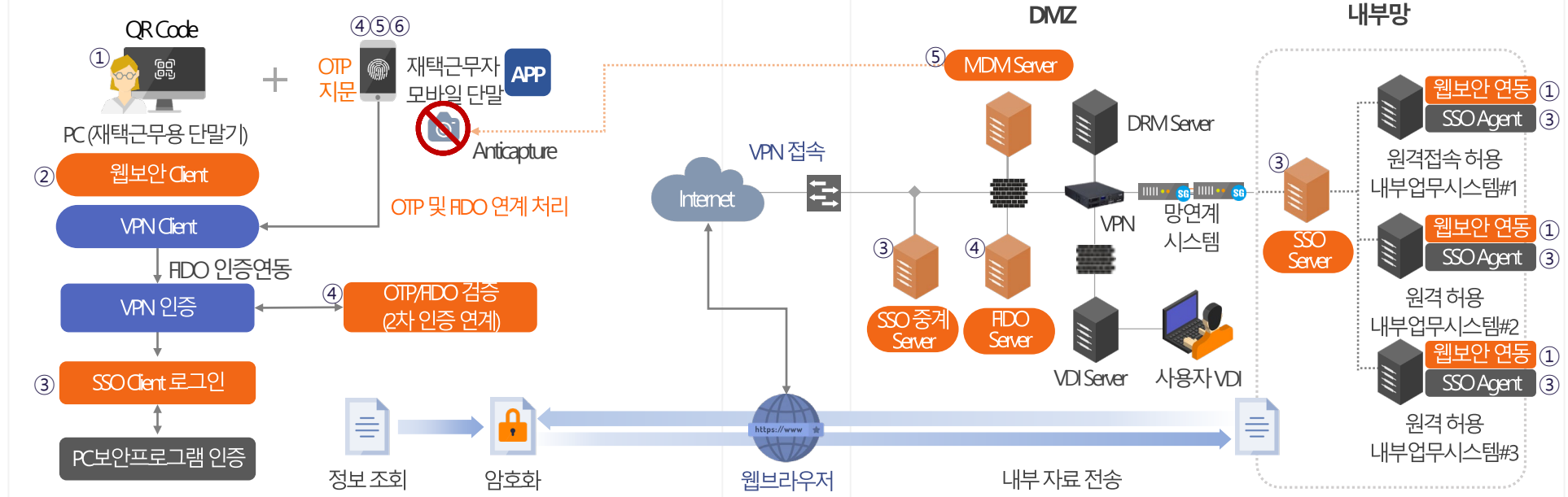


사용자 시나리오

1. 안전한 접속 환경 유지
2. 사용자의 VPN 접속 (인터넷업무/클라우드)
3. 1차 암호 인증
4. 2차 생체 인증
5. 단일 인증으로 여러 업무시스템에 자동 로그인

04 원격·재택 근무 시스템 구성도

원격 · 재택 근무 지원 솔루션 구성(예시)



- 원격사용자 VPN 로그인 시 2차 인증수단으로 OTP / FIDO 지원
- MDM APP 연계를 통한 사용자 모바일단말의 카메라 제어
- VPN 접속 후 보안 프로그램 등 SSO 연동
- 사용자가 내부 업무시스템 접속 시 화면으로 표시되는 정보를 웹보안 Client를 통하여 보호(유출방지)

- VPN 사용자 인증 처리를 SSO/FIDO Server와 연동
- 원격근무 시 사용자가 접속되는 내부업무시스템에 웹보안(nxWeb) 적용
- 사용자 VPN 인증 시 SSO와 연계하여 자동 인증 처리
- 사용자가 원격지에서 내부 업무시스템의 각종 파일 문서는 DRM 솔루션으로 암호화 처리

범례 ①TouchEn nxFirewall ②TouchEn nxWeb ③TouchEn Wiseaccess ④OnePass (mOTP) ⑤OneGuard ⑥TouchEn Anticapture

05 원격·재택 근무 지원 제품 라인업

5-1. 제품소개(1/2)
5-2. 제품소개(2/2)

제품소개(1/2)

PC용

모바일용

ONEPass

FIDO/사설인증 기반 사용자 인증 강화를 위한
FIDO(생체인증) 기반 간편인증 환경 제공

FIDO

- **국제FIDO Alliance 표준 기술 규격**을 준수하여 보안성 강화 및 생체정보 유출 방지
- 다양한 인증수단 제공(지문, 안면, 음성, 핀, 패턴 등)
- FIDO 표준을 지원하는 **다양한 인증 장치와 연동 지원**

OTP

- **2차 인증 보안강화를 위한 mOTP와 통합App 지원**
- 등록 및 인증 과정 간소화로 **사용자 편의성 향상** 지원
- **SAML 2.0 및 JWT** 기반 사용자 인증 연계 지원
- FIDO/PKI 기반 사설인증서 확장을 지원하며, **전자서명 및 무결성 검증을 통한 인증, 부인방지 지원**

PC용

TOUCHEN wiseaccess

재택근무지에서 사용자 로그인/인증에 대하여
통합 SSO 적용을 통한 업무 연계성 강화

SSO

- VPN 인증을 통하여 원격허용 **업무시스템 로그인 대체 및 접근 편의성 제공**
- **다양한 인증체계**(ID/PWD, PKI, OTP, FIDO등)와 연동한 사용자 인증 지원

- SSO 계정 통합관리 및 중복 로그인 차단을 위한 **사용자 인증 세션 관리를 통한 접속 제어 지원**
- 토큰 암호화 및 유효성 검증을 **통한 보안성 강화**
- **C/S 및 웹 환경의 업무시스템을 완벽히 지원**하며, SSO 연동 추가 확장 지원

PC용

TOUCHEN nxWeb

사용자 PC를 통한 업무 환경에 대하여
웹 컨텐츠 유출 방지와 화면 캡쳐 방지 대응 지원

- 멀티 브라우저 지원을 통한 **웹 컨텐츠 유출방지**
- **캡쳐 차단 프로그램에 대한 능동적인 대응** 지원
- Windows PC환경을 완벽히 지원하는 전용Client와 연동 모듈 제공

- 화면 캡쳐 시 사용되는 API 차단으로 웹, CS, PC 전체, 원격제어툴에 의한 캡쳐 방지와 동영상 녹화 방지 제공
- **웹 페이지 저장, 출력, 소스보기, 내보내기 등 방지** 지원

PC용

TOUCHEN nxFirewall

재택근무 환경에서 접속 PC의 안정성 확보를 위하여
트래픽 감시와 바이러스 등의 악성코드 탐지

- **커널 레벨 및 유저 레벨의 모든 트래픽을 감시하여 보다 안전한 사용자 인터넷 접속 환경 제공**
- 보안 등급 설정을 통한 방화벽 설정 기능 제공
- 코드 베이스의 간단한 수정 작업만으로 적용가능
- 다양한 서버 환경과 멀티브라우저를 지원

- **바이러스 탐지 기능과 악성 코드 탐지 기능 제공**
- 네트워크 제어/프로그램 제어/바이러스 탐지 및 기록 기능을 제공
- 사용 중인 네트워크 세션에 대한 연결 상태 조회 및 해제 기능 제공

IT 관리자를 위한 원격근무 가이드

제품소개(2/2)

모바일용

ONEGuard

재택근무 환경에서 모바일을 통한 정보 자산
유출방지를 위한 다양한 보안정책 지원

- **재택근무 시 업무 모드를 통한 카메라 제어와 화면 캡쳐 방지 지원**
- **모바일 APP 제어 및 무결성 검증 지원**
- 모바일 단말기 분실 및 도난 대응

- 원격 단말 제어 지원
  (카메라, Wi-Fi, 마이크,GPS, USB 등)
- **조직/사용자/단말기 통합 관리 및 통계/리포트 지원**
- 모바일 APP의 화이트/블랙리스트 관리 제공

모바일용

TOUCHEN mVaccine

모바일 전용 백신을 통한 안전한 접속 환경을 제공
악성코드, OS 위변조, 원격제어 탐지 지원

- 글로벌 비트디펜더 엔진과 국내 최정상 화이트 해커의 기술력을 통한 mVaccine 엔진의 **듀얼 탐지**
- **중복 탐지 판별 기능**으로 속도 저하 이슈 부재
- 악성코드 탐지 외 **모바일 OS의 위변조 및 부정한 원격 제어 탐지** 등의 기술 제공

- 자동 업데이트를 통한 관리 포인트 감소
- **Web to App/App to App/Library 방식 지원**
- **엔진과 패턴을 분리한 업데이트**로 업데이트 편의성 향상 및 모바일 워크로드 최소화
- 매월 보안 동향 보고서 제공(악성코드 통계 등)

모바일용

TOUCHEN AntiCapture

사용자 모바일 단말기를 통한 업무 환경에 대하여
화면 캡쳐 방지를 통한 보안 컨텐츠 유출 방지

- Android, iOS 환경에서 **모바일 앱의 화면캡쳐방지**를 통한 보안 컨텐츠 유출 방지
- 스마트폰의 캡쳐 단축키, 화면 캡쳐애플리케이션, 외부 기기 연결, Emulator 환경의 화면 캡쳐 방지 지원

- **별도의 추가 앱 설치가 필요 없는 Library 방식**
- 개발자 리소스 투입 최소화로 운영 비용 절감 효과
- 개인 정보 및 단말 정보를 수집하지 않아 개인 정보 유출 및 사생활 침해 우려 원천 차단

모바일용

TOUCHEN mWiseaccess

재택근무지에서 다수 업무 앱의 사용자 인증에 대하여
모바일 앱의 SSO 적용으로 편의성 증대

- 모바일 환경에서 다수의 업무 앱 간의 SSO 인증을 제공하여 스마트폰 사용자의 편의성 향상
- SSO 인증 세션 클러스터링 지원
- 보안 공용 영역 접근을 위한 접근 제어키 사용

- 인증 토큰 재사용 공격에 대응하는 일회용 비밀번호 검증 방식을 적용
- 다중 로그인 정책을 통한 중복 로그인 제어, 장시간 미 사용 시 자동 로그아웃을 지원
- Web to Web / App to App / App to Web지원


라온시큐업 2021
BEYOND THE DIGITAL WORLD
RAON