



Avast 비즈니스 중앙관리

비즈니스 허브





비즈니스

특징

Avast Business Hub는 기업 및 IT 서비스 프로바이더가 네트워크에 구축된 모든 Avast Business 솔루션을 관리할 수 있는 클라우드 기반 통합 보안 플랫폼입니다.

또한 위협 요소, 포괄적인 보고 및 관리 기능을 단일 창에서 실시간으로 파악할 수 있습니다.



직관적인 관리 대시보드

모든 알람을 한 눈에 보고, 문제를 해결하고, 서비스를 추가하고, 신속한 조치를 통해 가동 시간, 안정성 및 보안 향상.



명령

검색, 재시작 등과 같은 여러 장치에 명령을 신속하게 적용. 정책 설정에 따라 자동으로 명령 실행.



실시간 알림

오래된 바이러스 백신 또는 패치 누락을 비롯한 보안 위협 또는 네트워크 문제에 대한 즉각적인 알람 수신.



기기 및 정책 관리

손쉽게 사용자 정의할 수 있는 템플릿을 사용하여 각 장치에 적절한 보호 기능을 제공. 정책 변경 내용은 실시간으로 자동으로 업데이트.



멀티-테넌트 지원

여러 사이트 또는 고객을 손쉽게 관리하고 대규모 팀 전반의 업무 간소화.



보고서

버튼 클릭 한 번으로 읽기 쉬운 상세 활동 보고서를 생성하고 예약.

베스트 클래스의 엔트포인트 보호



최고 평점
제품
2020



최고 제품
2021



올해의 베스트
컴퓨터 보안
소프트웨어
2021



SMB 시장에서의
최고 높은
수준의
안티멀웨어 수상



2019년 뉴스위크
선정 베스트
비즈니스 도구

비즈니스 허브

서비스

비즈니스 허브를 통해 비즈니스 및 IT 서비스
프로바이더는 계층화된 엔드포인트 및
애플리케이션 보안 서비스를 신속하게 구현하고,
지속적인 모니터링을 제공하며, 뛰어난 보호
기능을 제공하는 데 필요한 통찰력을 얻을 수
있습니다.



진보된 클라우드 기반의 보안 – 복잡하지 않은 간편함



고급 보안



복잡성 제거



속도 개선



낮은 TCO



엔드포인트 보안

차세대 안티바이러스

차세대 안티바이러스

특징

안티바이러스는 기업의 사이버 보안 전략에 있어 매우 중요한 부분입니다. 많은 수상 경력으로 빛나는 Avast 비즈니스 차세대 안티바이러스를 통해 기업은 기기, 데이터 및 사용자용 엔드포인트 보호 솔루션을 네트워크 어디에나 구축할 수 있습니다.

여러 사무실/고객의 기기에 바이러스 백신 소프트웨어를 신속하게 설치하고 읽기 쉬운 대시보드에서 중앙 집중식으로 관리하여 모든 기기가 항상 최신 상태이고 멀웨어가 발생하지 않도록 합니다.



예방적 보안

웹, 파일 및 이메일을 모니터링하며 의심스러운 동작에 대한 파일을 분석하는 다계층의 방어 시스템으로 실시간으로 시스템을 감시하고, 위협 요소가 차단되면 이를 알려주는 알림을 받을 수 있습니다.



완벽한 가시성

중앙 집중식 대시보드에서 바이러스 백신 배포, 구성 및 관리하며, 현장 또는 원격에 관계없이 모든 기기를 관리하는 완벽한 가시성 제공합니다.



포괄적인 보고서

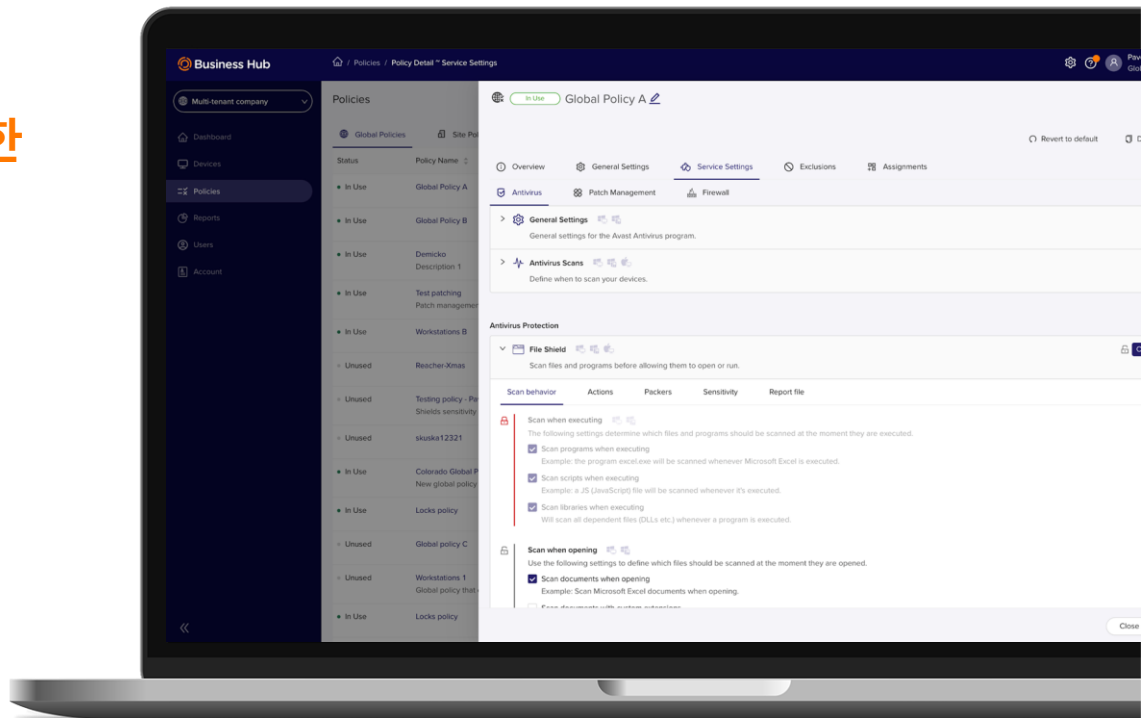
위험 차단, 바이러스 백신이 설치되지 않은 기기 및 바이러스 검사가 오래된 장치를 포함하는 읽기 쉬운 보고서로 심층 분석을 할 수 있으며 이를 통해 보안을 강화할 수 있습니다.

Avast 비즈니스

데이터, 기기, 사람을 위한 완전한 위협 방어

기기 보호 엔진들

- 4개의 실시간 감시 엔진
- 사이버 캡처
- 방화벽
- 스마트검사
- 샌드박스
- Wifi 검사
- 실제 사이트 검사
- 복구 디스크
- 보안 웹브라우저 확장
- 원격접속 방어



비즈니스 프로&프로플러스

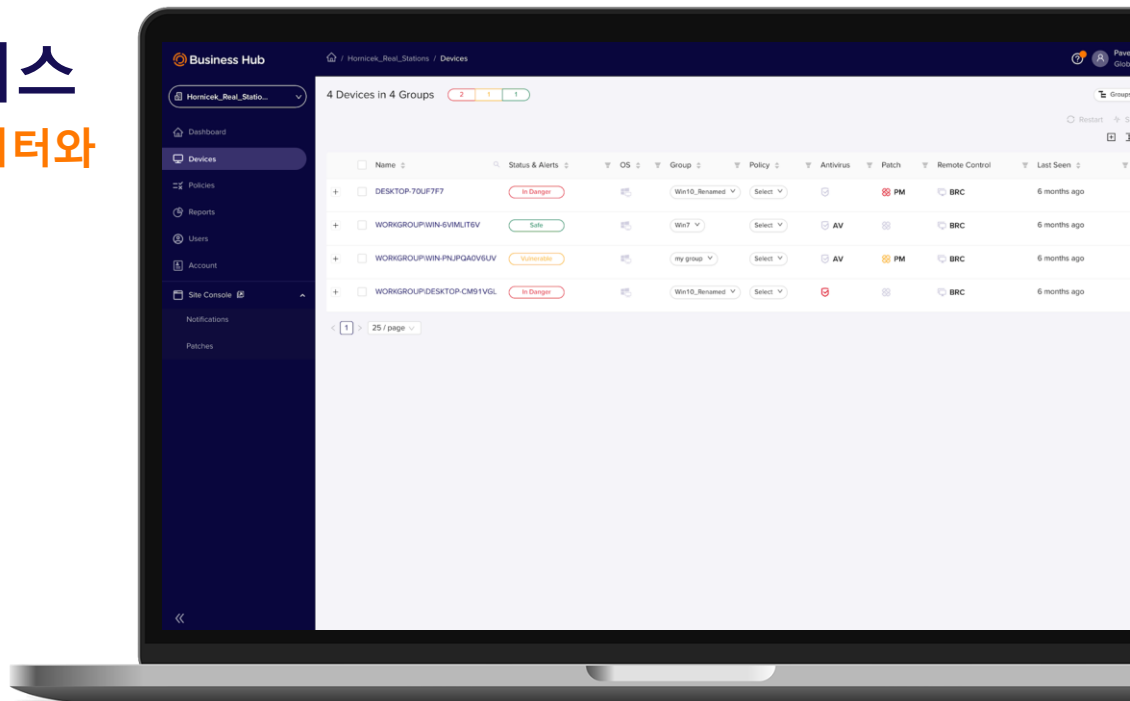
비즈니스 프로 및 프로 플러스는 데이터와 사람을 위한 위협 방어 제공

비즈니스 프로의 데이터 보호

- 데이터 영구삭제
- Exchange 서버 보호
- SharePoint 서버 보호

개인정보 보호를 추가한 비즈니스 프로 플러스

- 비밀번호 보호
- 시큐어라인 VPN
- 브라우저 클린업
- 웹캠 감시



애플리케이션 보안

패치 관리

패치를 해야 하는 일반적인 이유...

57%

데이터 유출의
57%는 패치 관리를
하지 않아서 발생

102 일

주요 소프트웨어 및
어플의 업데이트를
수행하는데 기업에서
평균 102일이 소요¹

86%

취약점의 86%는 3rd
어플로 부터 발생²

¹Ponemon. ²National Vulnerability Database.

....그러나 대부분의 기업은 자신의 시스템에서 패치를 하지 않음

Avast는 5십 만개의
엔드포인트 기기에서 대한
보안 테스트를 수행

29%

이 중 29%만 소프트웨어
업데이트를 하고 있는
것으로 확인

그리고 5십 만 대 기기
중 단,

304

대에서만 100% 업데이트
완료됨



55%

모든 소프트웨어 애플리케이션 중
55%가 패치가 되지 않음



15%

Windows 7 시스템의
15%가 구식 버전



8%

Windows 10 시스템의 8%
가 구식 버전

보안 전문가들이 알려주는 통계적 사실



92%

웹
애플리케이션의
92%가 악용될 수
있는 보안 결함
또는 약점을
가지고 있음



34%

침입 피해자의
34%는 침입
당하기 전에
자신이
취약하다는 것을
알고 있음²

오랫동안 보안 패치가
실행되지 않았기
때문에 기존의 많은
취약점이 여전히 열려
있음.

알려진 상위 10개
취약점이 해킹 공격
성공 사례의 85%를
차지함³



65%

기업의 65%가
패치 우선 순위를
정하기가
어렵다고 답함⁴



82%

82%의 고용주가
사이버 보안 기술이
부족하다고 답했으며
71%는 이러한 인재
격차가 조직에 측정
가능한 직접적인
피해를 입힌다고 생각

^{2,4}Service Now + Ponemon Institute Study. ³Verizon 2016 Data Breach Investigations Report (DBIR).

기업 들이 패치하지 않는 이유?

인식과 행동

SMB 기업은 잠재적인 결과 및 취약점에도 불구하고 Windows 및 타사 소프트웨어 애플리케이션 패치 적용을 꺼려함

데이터 유출의 37%는 취약점에 대한 패치 검사 및 수행하지 않아 발생¹

너무 많은 패치

패치 수가 너무 많아서 따라잡을 수 없습니다.
패치 적용은 시간이 많이 소요되는 수동 프로세스

기업의 65%가 패치 우선 순위를 정하기 어렵다고 답함²

운영 중단

어플 소프트웨어를 패치하면 비즈니스 중단이 발생할 수 있음
최종 사용자가 패치 업데이트를 거부할 수 있음

알려진 상위 10개의 취약점이 성공한 해킹의 85%를 차지³

단순화된 콘솔

전체 회사에서 누락된 패치를 볼 수 있는 간편한 콘솔이 필요
수동 및 자동 패치 모두가 필요

기업의 74%는 인력이 없어 신속하게 패치를 수행할 수 없음⁴

¹ Service Now + Ponemon Institute Study – Today's State of Vulnerability Response. ^{2,4} Service Now + Ponemon Institute Study. ³ Verizon 2016 Data Breach Investigations Report (DBIR).

어플을 업데이트하지 않는 경우의 위험성

- 랜섬웨어 감염
- 데이터 손실 또는 침해
- 데이터 복구와 운영체제 및 어플 재설치에 따른 중대한 시간 손실
- 정부 및 기업이 필요한 규정 준수 위반
- 의심스러운 데이터 무결성
- 신뢰성 및 신용의 추락

THREAT LEVEL TIMELINE



패치 관리

장점

Avast 비즈니스 허브 플랫폼에서 패치관리를 통해 기업은 윈도우 및 타사 소프트웨어 애플리케이션을 모두 최신 상태로 유지, 관리 및 업데이트할 수 있습니다.

중요한 취약점을 파악하고 중앙 대시보드에서 모든 엔드포인트에 패치를 쉽게 구축할 수 있도록 함으로써 패치 적용 여부에 대한 의심을 제거할 수 있습니다.



취약점 방지

윈도우 운영 체제 및 기타 타사 소프트웨어 응용 프로그램을 자동으로 최신 상태로 유지하여 취약점 및 보안 이슈 문제를 방지합니다.



컴플라이언스 확보

회사 및 규정 준수를 위한 보안 패치를 설치했거나 설치하지 못한 오래된 소프트웨어를 식별합니다. 위험 감소로 평판 손상 및 법적 조치를 방지하는 효과가 있습니다.



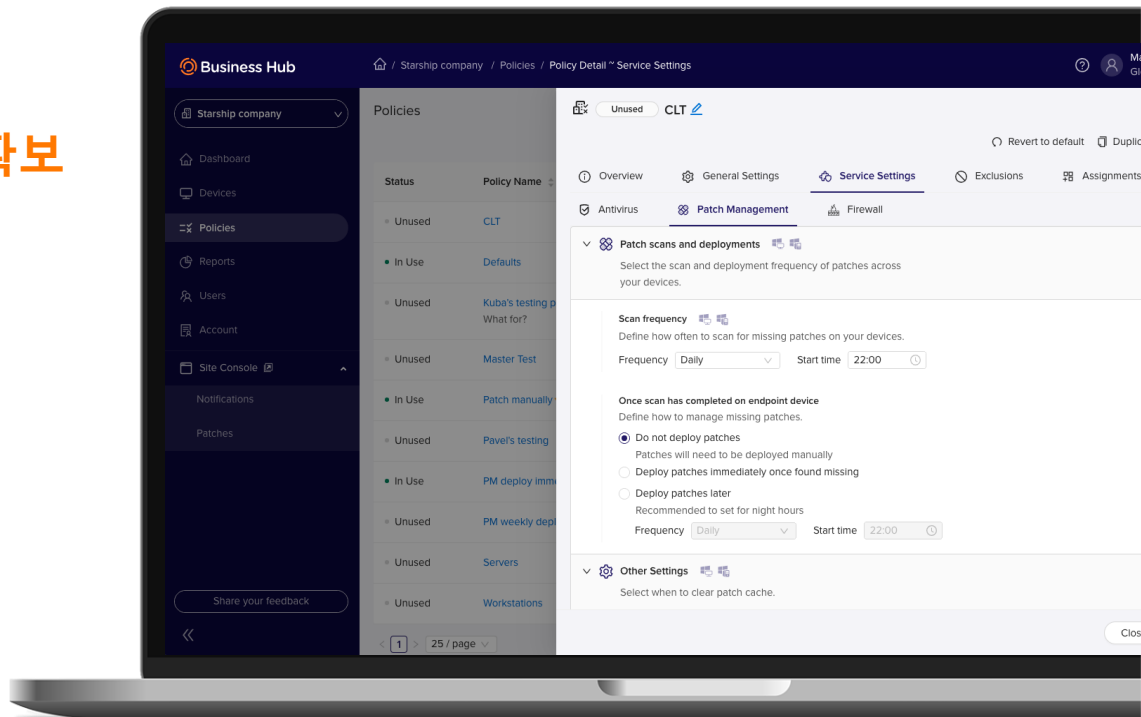
자동으로 패치 적용

한 번 설정하고 잊어버리세요. 수백 개의 패치를 추적할 필요가 없습니다. 콘솔에서 중요 패치를 자동으로 예약하여 기기에 패치를 진행할 수 있습니다.

패치 관리

취약점 방어와 컴플라이언스 확보

- 성능
- 수 천개의 패치 들
- 패치 테스트
- 패치 롤백
- 패치 허용
- 능동적 채택 예약
- 직관적인 대시보드
- 커스터마이징 가능한 패치
- 마스터 에이전트 활용
- 패치 검사 결과



데이터

클라우드 백업

장점

방대한 비즈니스 클라우드 백업 서비스는 구축 및 관리가 간편한 자동 백업 프로세스를 통해 장치를 보호함으로써 데이터를 안전하게 유지하고 비즈니스 연속성을 보장합니다. 장치에서 백업 예약을 신속하게 설정합니다. 하나의 대시보드에서 중앙 집중식으로 관리하여 모든 데이터를 백업하고 사용할 수 있도록 보장합니다. 예상치 못한 상황이 발생할 경우 데이터를 쉽게 복구합니다.



기업 데이터 보호

워크스테이션, 노트북 또는 서버 파일의 전체 백업을 생성하고 한 시간 간격으로 실행되도록 백업을 예약합니다. 각 백업은 데이터에 대한 새로운 변경 사항을 캡처하여 데이터가 기하급수적으로 증가하거나 스토리지에 영향을 주지 않으면서 무제한 파일 버전 관리 및 이전 버전으로 되돌릴 수 있습니다.



빠른 파일 복구

비즈니스 허브 플랫폼 또는 사용자 시스템에서 온디맨드 방식으로 데이터를 복구하고 원래 위치 또는 지정된 새 위치로 복원합니다.



중앙관리&모니터링

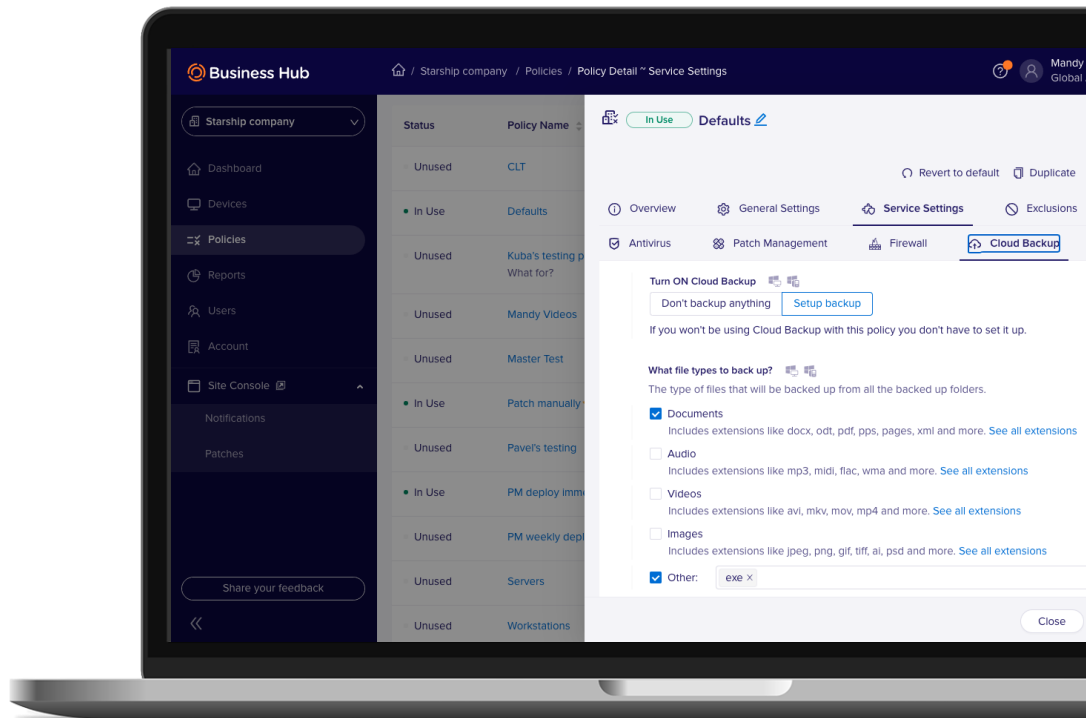
비즈니스 허브 플랫폼 내 또는 최종 사용자의 시스템에서 대시보드를 통해 엔드포인트 장치를 실시간으로 모니터링하여 보다 세밀한 제어를 수행합니다. 실패한 백업, 만료된 백업 및 성공한 백업에 대한 정책을 설정하고 알림을 수신하여 대시보드에서 백업을 쉽게 관리할 수 있습니다.

클라우드 백업

기업 데이터 보호를 위한 자동화된 백업과 복구

특징

- 선택가능한 백업
- 인터넷 속도
- 중단 없는 채택
- 자동 암호화
- 클라우드 스토리지 – 어디서나 접근 가능
- 종합적인 보고서
- 파일 버저닝
- 복구



원격 접속 및 지원

원격 제어

언제든지 어디서나
원격으로 기기에 접속

Avast 비즈니스 원격제어를 통해 IT 관리자는 사용자 시스템에 빠르고 안전하게 연결하여 실시간으로 문제를 해결할 수 있으므로 시간과 비용을 절약할 수 있습니다.



강화된 보안

완벽한 엔드 투 엔드 암호화로
원격 연결을 안전하게 하고
보안이 유지됩니다.



원격 관리

윈도우 및 Mac OS X
시스템에 원격으로
연결하여 새 소프트웨어
설치, 문제 해결, 사용자
전환 등을 수행합니다.



보고서

세션 및 감사 로그 정보를
가져와 어떤 관리자가
어떤 디바이스에
연결되었는지, 날짜, 시간
및 세션 지속 시간을 알 수
있습니다.

원격제어 도입 이유

원격으로 언제 어디서나 기기에 원격 접속



효율성 증대

직원들의 IT자원에
대한 원격 지원을
통해 효율적으로
관리



비용 절감

즉각적인 연결을
통해 시간을
절약하고 현장
방문을 위한 출장
비용을 절감



만족 증대

비용을 절감하면서
탁월한 서비스 제공



중앙 관리

단일 플랫폼에서
모든 Avast
Business 솔루션
관리

특징

원격 관리

윈도우 및 Mac OS X 시스템에 원격으로 연결하여 새 소프트웨어 설치, 문제 해결, 사용자 전환 등을 수행

개선

연결을 위해 .exe 파일을 더 이상 다운로드하지 않아도 되며, 연결 성능 및 사용 편의성 향상

파일 전송

문제해결을 위한 로그 파일을 보내고 소프트웨어 업데이트를 받습니다. 빠르고 효과적으로 문제를 해결

시스템 정보

CPU, IP주소, 메모리, 드라이브 등과 같은 하드웨어 정보 및 소프트웨어 정보 확인

세션 녹화

교육 및 기타 목적으로 세션을 녹화할 수 있음

채팅 및 음성

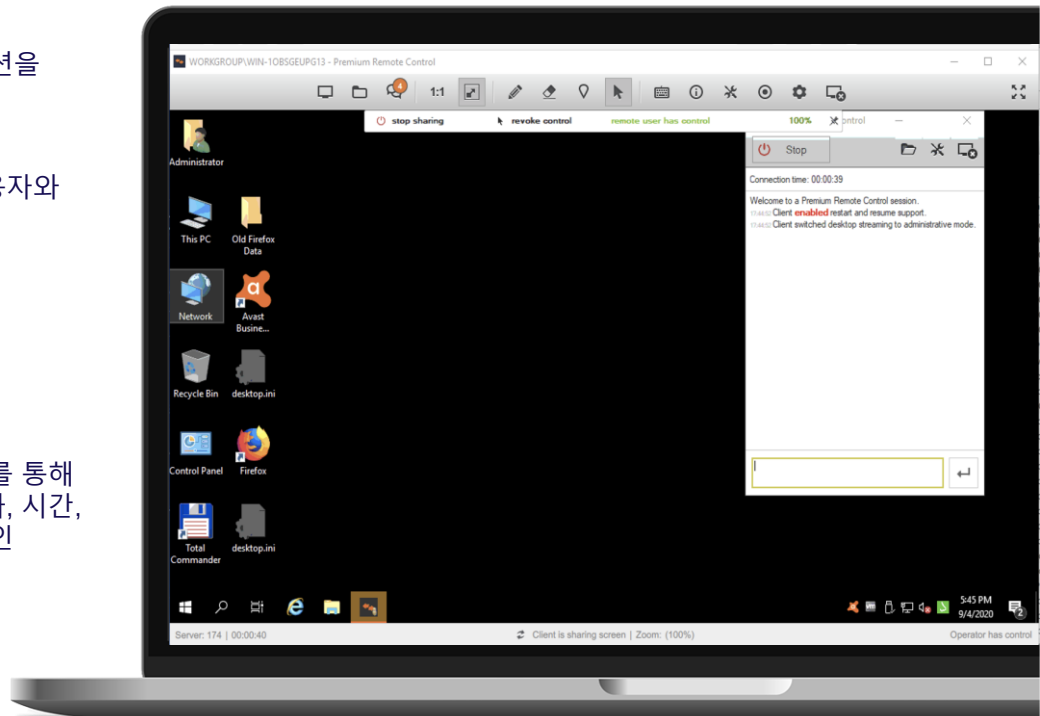
채팅 도구를 탑재하여 사용자와 채팅이나 음성통화가 가능

강력한 보안

암호화 통신을 사용하여 안전하고 보호된 통신으로 보안을 유지

보고서

세션 및 감사 로그 보고서를 통해 연결된 기기의 정보나 날짜, 시간, 세션 정보 등의 정보를 확인



원격접속 베이직 vs 프리미엄

	원격접속 베이직 무료	원격접속 프리미엄 유료 버전 (멀티세션 기준)
월간 접속 세션 수	5	무제한
분 당 세션 기간	5	무제한
동시 세션 수	불가	무제한
관리자 수	무제한	무제한



Soft **Mail**

<https://www.avastkorea.com>

감사합니다