알서포트 제품을 사용해야 하는 22가지 이유

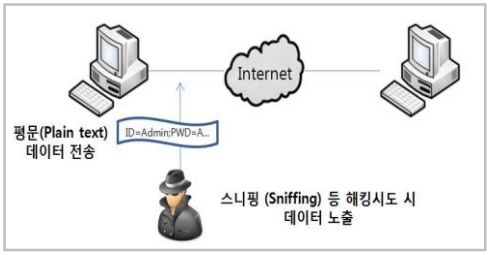
알서포트의 모든 "원격" 제품은 국가보안기술 연구소 (NSRI)의 소프트웨어 업데이트 체계 보안 가이드에 준수 합니다.

고객님이 사용하시는 알서포트의 "원격" 제품은 보안과 고객의 정보를 소중히 생각하며 만들어진 제품 입니다.

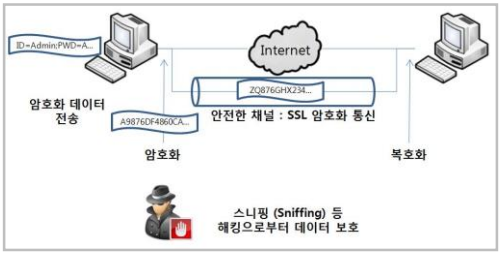
1. 신뢰할 수 있는 암호화 통신 사용

알서포트의 제품은 암호화 통신을 제공함으로 고객의 중요한 개인정보는 암호화 되어 있습니다. 또한 End-To-End에서 256-bit AES 데이터 암호화를 통해 1차 데이터 보안 과정을 거칩니다.
원격 세션 연결 시 1차 128bit SLL (Secure Socket Layer) 암호화 통신 후 256-bit AES 데이터 암호화를 통해 2차 암호화 과정을 거쳐 **안전한 채널을 유지하여 보안에 강력합니다.**

원격 서비스 제공 시 보호되어야 할 데이터는 화면 공유 데이터, 키보드/마우스 컨트롤 데이터, 문자 채팅 (Text Chat) 데이터, 파일 송수신 데이터, 기타 원격 서비스시 사용하는 기능에 의해 생성되는 모든 데이터가 포함 됩니다.



[그림 1. 스니핑을 통한 해킹 시도 시 데이터 노출]



[그림 2 . 스니핑 등 해킹으로부터 데이터 보호]

※ 참고

SSL (Secure Socket Layer)
SSL 은 응용 프로토콜 TCP/IP 사이에 위치하며, 데이터의 암호화, 서버의 인증, 메시지의 무결성을 제공해 준다. 서버에 대한 인증은 반드시 수행되지만 클라이언트에 대한 인증은 선택적으로 수행할 수 있도록 합니다.

SSL은 서버와 클라이언트 양쪽의 TCP/IP 연결을 위하여 핸드쉐이크 (handshake) 프로토콜을 수행합니다. 이 결과로 양쪽은 암호화 통신에 합의하고, 암호화 통신과 인증에 필요한 값들을 준비합니다.

이 단계가 지나면 SSL은 응용 프로토콜에서 생성해 낸 바이트 (Byte) 스트림의 암호화와 복호화 만 수행하게 됩니다. 이는 요청 (Request)과 응답 (Response)에 포함되는 정보들이 **암호화되어 전송된다는 것을 의미합니다.**

AES (Advanced Encryption Standard)
AES (Advanced Encryption Standard)는 2001년 미국 정부에서 채택한 암호화의 형식입니다. AES는 이전의 DES (Data Encryption Standard), 3DES보다 훨씬 안전한 암호화를 제공합니다.

2. 해킹의 위협으로 부터 안전한 엔진 사용

인터넷을 통해 무상으로 제공하는 Open Source (VNC)를 사용한 제품을 이용하면 소스가 공개되어 해킹에 쉽게 노출될 수 있습니다. Open Source (VNC)의 경우 공개된 프로토콜 (RFB)을 사용하고, 특정 포트를 사용함으로 데이터 가로채기, 변조에 취약하고 해킹에 노출되기 쉽습니다.
하지만 알서포트의 제품은 당사 연구소에서 개발한 우수한 엔진으로 알서포트만의 독자 포멧 (엔진소스)를 사용하여 해킹의 위협으로 부터 보다 안전합니다.

3. 서버 이중화로 안정적인 서버 운영

알서포트의 ASP 제품을 사용하는 고객들이 안정적인 서비스를 이용할 수 있도록 서버 구성이 이중화 되어 있습니다. 천재지변으로 데이터센터 (IDC)가 불능 상태가 된다 하여도 다른 데이터센터 (IDC)에도 동일한 시스템 구조로 되어 있어 안정적으로 서비스를가 운영될 수 있도록 만반의 대응체계를 갖추었습니다.

4. ActiveX 설치가 필요 없는 원격 서비스

ActiveX는 인터넷 익스플로러의 기능을 확장하기 위해 MS에서 제공하는 기능 입니다.
ActiveX는 보안성 검증절차가 없어 보안 프로그램에서 조차도 취약점이 발견 됩니다.
보안에 취약한 ActiveX는 해커가 만든 ActiveX를 잘못 내려 받았을 경우 사용자의 PC가 해킹 당할 수 있습니다.
하지만 알서포트의 제품은 일회성 실행파일 형식으로 연결이 가능하여 보안에 더욱 강력합니다.

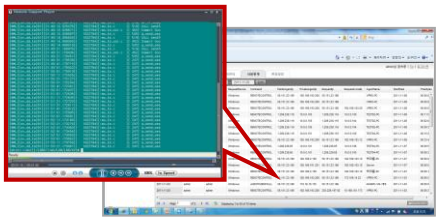
5. 고품질의 원격 서비스 제공

알서포트의 제품은 전세계 11개국에 구축된 중계 서버를 기반으로 세계 어디서나 고품질의 원격 서비스를 제공하고 있습니다. 빠른 속도의 원격 서비스를 제공하기 위해 사용자의 위치에서 가장 근접한 중계 서버를 통해 원격 서비스를 이용하게 됩니다.
뿐만 아니라 당사 연구소에서 개발한 VRVD 엔진을 이용하여 더욱 빠른 속도를 보장 합니다.

6. 원격서비스 중 녹화 기능

SW 녹화 또는 KVM을 통한 HW 녹화

모든 사용 내역이 로그로 저장되어 통계로 표시하고 저장할 수 있습니다.



[그림 3. 관리자 페이지 : 원격제어 중 녹화 리스트]

7. 정부가 권장하는 소프트웨어 업데이트 체계 보안 가이드라인 준수

알서포트의 제품은 국가보안기술 연구소(NSRI) 에서 권고하는 소프트웨어 업데이트 체계 보안 가이드라인을 준수합니다.
알서포트의 제품은 Verisign (서명기관) 에 의한 전자서명 (Digital Sign)을 기반으로 코드 사이닝 (Code Signing)된 실행 파일을 제공하여 안전하게 사용할 수 있습니다.
정부기관이 권장하는 방식을 적용하여 인증된 안전한 모듈을 제공합니다.

8. 새로운 이슈에 대해서 즉각 대응

알서포트의 제품은 새로운 보안 이슈 발생 시 즉각 대응하고 있습니다.
상용화된 **보안 취약점 분석 솔루션을 통해서 분기별 한번씩 보안 점검**을 하고 있으며,
지원되는 운영체제 및 데이터베이스에 대한 보안가이드를 마련하여 체계적으로 관리 되고 있습니다.

9. 정기 점검 리포트 제공

고객사 정기 점검 방문 시 제품별로 시스템, 로그, 솔루션, 통신 으로 구분하여 상세한 점검을 진행합니다. 정기점검을 시행하여 제품의 이상 여부를 확인하고 문제 이슈에 대해서는 해결 후 점검 리포트를 제공합니다.

10. 상담원 PC의 접속 IP 또는 Mac Address 접근통제

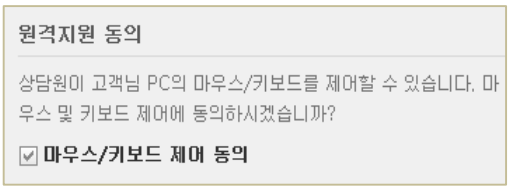
관리자는 허가하는 상담원의 네트워크 또는 장비의 위치를 제한할 수 있습니다. 관리자는 관리자 페이지에서 지정 IP 또는 IP 그룹, Mac Address 를 설정 등록하고, 사용자는 허용되는 위치에서 뷰어 로그인 후 상담을 시작할 수 있습니다.

11. 원격지원 접속 코드 보안

원격지원 인증에 사용되는 접속코드는 랜덤 숫자인 6자리 숫자로 제공됩니다. 생성된 접속코드는 실제 통화(또는 채팅) 중인 상담원과의 원격지원 연결을 위해 1회 생성되고 사용됩니다. 일회성 원격지원을 위해 사용되고, 제 3자의 임의 접근을 차단합니다.

12. 원격지원 시 사용자에게 사전 동의

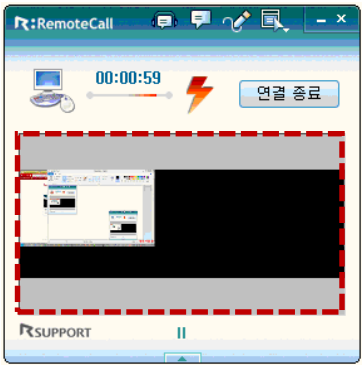
원격지원을 받는 고객은 상담원에게 원격지원을 받기 위해 제어 권한에 대한 사전동의를 받은 후 화면공유 및 지원이 시작됩니다.



[그림 4. 원격지원 동의 메시지창]

13. 고객이 원할 때 원격지원 중지 및 권한 회수

원격지원 중 고객이 원할 때 연결 종료가 가능 합니다.
고객은 언제든지 원격지원 중 연결 종료 버튼을 통해 세션을 종료할 수 있습니다.



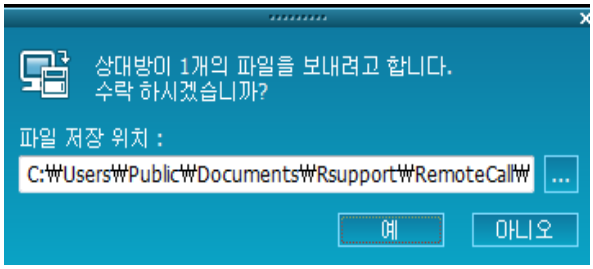
[그림 5. 원격지원 중 연결 종료 메시지창]

고객은 상담원에게 허락한 제어권을 회수할 수 있습니다.
원격지원을 받는 고객은 상담원에게 키보드, 마우스 제어 권한에 대한 사전 승인을 통한 화면 공유 및 지원이 시작됩니다. 원격지원 세션간에 언제든지 상담원에게 허락한 키보드/마우스 제어 권한을 회수할 수 있습니다. 키보드/마우스 제어 중단 기능은 "Ctrl + Alt + Shift" 키로 권한 회수가 가능합니다.

허가된 사용자만 원격지원이 가능합니다.
원격지원 시작 시 고객 PC의 원격지원 모듈이 사전 인증 허가된 사용자로 하여금 원격지원 받을 수 있도록 합니다. 상담원과 1:1 매칭을 통한 원격지원만을 허용합니다. 원격지원 종료 후 고객 PC의 원격지원 모듈은 고객의 요구에 따라 모두 삭제할 수 있습니다. 삭제하지 않은 경우에도 역 제어 방식의 원격지원으로 외부에서 임의 접근이 차단됩니다.

14. 파일 송수신 시 고객 동의

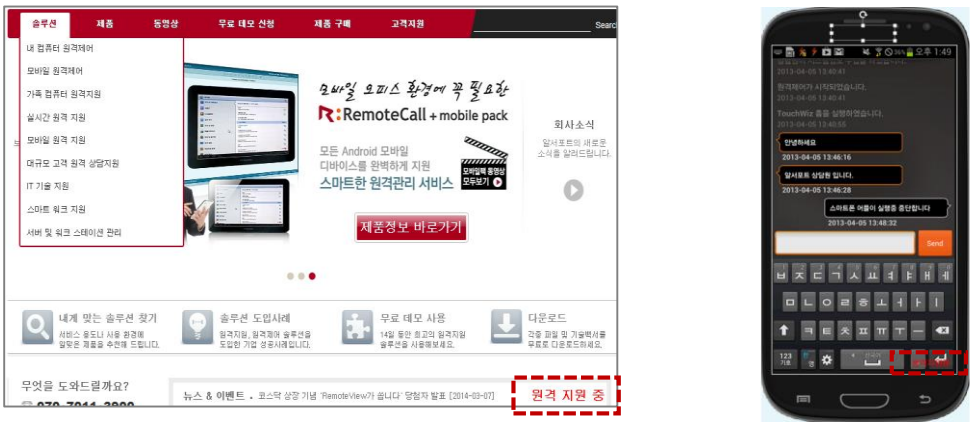
파일 송수신 시 고객의 동의를 받아 파일 송수신을 합니다.
파일 송수신 기능은 고객의 송수신 동의 후 전송이 가능합니다. 고객의 동의 없이 임의 파일에 대해 송수신이 허용되지 않습니다



[그림 6. 원격지원 파일 송수신 고객 동의창]

15. 원격지원 중임을 화면 표시로 제공

원격지원 세션에 대한 공지 : Tray Icon, Taskbar 에 메시지가 표시 됩니다.
고객의 데스크톱과 모바일 모두 화면 오른쪽 하단에 “원격 지원 중”이라는 메시지가 항상 표시됩니다. 고객은 원격지원이 진행 중임을 인식할 수 있습니다.



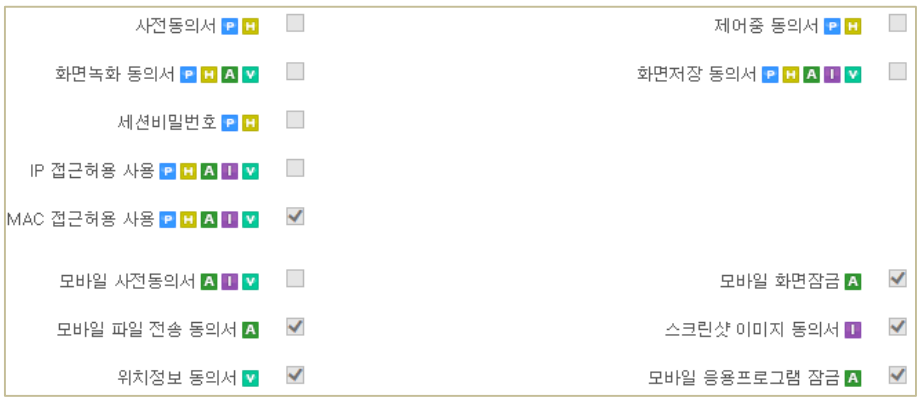
[그림 7. 원격지원 중 알림 메시지]

16. 상담원의 모든 기능에 대한 중앙통제

관리자에 의하여 중앙 통제 가능합니다.
대부분의 주요 기능은 관리자에 의하여 중앙 통제를 할 수 있습니다. 관리자는 상담원의 권한을 등급별로 직접제어 권한 또는 간접제어 권한을 선택적으로 부여할 수 있습니다.

17. 개인정보 보호 옵션 체크로 보안 설정

관리자 페이지에서 상담원 옵션 중 개인정보 보호 옵션 체크로 보안설정이 가능 합니다.
상담원이 직접 보안 관련 하여 사용여부를 체크할 수 있습니다.



[그림 8. 관리자 페이지에서 사용여부 설정화면]

18. 긴급 통제에 의한 1회성 접속

외부 업체 직원을 위한 1회성 제어 권한 부여

- 권한 부여 후 특정 시간 이내 1회만 접속 가능
- 문자, 전화, 이메일 /택 1을 통한 접속번호 제공
- 외부에서 접속 시 로그 저장

사내 관리자 외부 업체 직원

[그림 9. 관리자 페이지 내 1회성 접속 권한 부여]

19. 보안에 더욱 강력한 이중인증

OTP, SMS, E-mail을 이용한 사용자 이중인증으로 더욱 안전 합니다.

원격제어 시 사용자의 2차에 걸친 계정 확인 과정을 통한 중요 기능 접근 시 보안 강화

- ID, PW 인증시 One Time기반의 Key를 생성하여 로그인 시 이중인증
- ID, PW가 노출된 상황에서도 허가되지 않은 사용자의 이용을 차단

[그림 10. OTP, SMS을 이용한 인증 (1회성 접근 코드)]

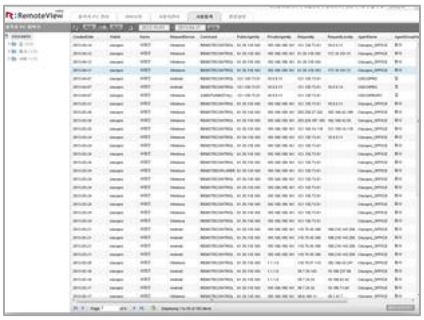
20. 원격제어 시 원격지 화면 잠금 기능

원격제어 시작 시 원격지 화면을 "원격화면 잠금" 기능을 이용하여 모니터를 끄고 켤 수 있습니다.

[그림 11. 원격지 화면 잠금 메시지 / 원격화면 잠금 설정]

21. 사용내역에 대해서 로그 저장 및 통계 제공

관리자 페이지에서 사용내역 통계 확인이 가능합니다. 원격 중 채팅 및 파일 송수신 시 주고 받았던 모든 기록은 로그로 기록되며, 서버로 전송되어 안전하게 관리됩니다. 원격 제어 세션 레코딩은 상담원과 고객 모두 안전한 원격제어를 보장합니다.



[그림 12. 관리자 페이지 사용내역 로그]

22. 응용 프로그램 잠금 기능 설정

관리자 페이지에서 관리자가 응용프로그램 잠금 설정

화면 전체가 아닌 특정 어플리케이션 화면만 상호 공유가 가능합니다.

[그림 13. 관리자 페이지 내 설정화면]

RSUPPORT

For more information about RSUPPORT, please www.rsupport.com

USA :
333 Sylvan Avenue Suite 110,
Englewood Cliffs, NJ 07632, USA
Phone : +1-888-348-6330
Fax : +1-888-348-6340
Tech : support.us@rsupport.com
Sales : sales.us@rsupport.com
Info : info.us@rsupport.com

Japan :
〒105-0001 東京都港区虎の門1-2-20
第3虎の門電気ビル
TEL : +81-3-3539-5761
FAX : +81-3-3539-5762
お問い合わせ : support.jp@rsupport.com
Sales : sales.jp@rsupport.com
Info : info.jp@rsupport.com

China :
北京市朝阳区霄云路38号现代汽车大厦2203室I-101
电话 : +86-10-8256-1810
传真 : +86-10-8256-2978
支持咨询 : support.cn@rsupport.com
业务咨询 : sales.cn@rsupport.com
销售咨询 : info.cn@rsupport.com

Korea :
(138-724) 서울시 송파구 방이동 45번지 한미타워 15층, 16층
전 화 : +82-70-7011-3900
팩 스 : +82-2-479-4429
기술문의 : support.kr@rsupport.com
구매문의 : sales.kr@rsupport.com
기타문의 : info.kr@rsupport.com