AhnLab

Safe Transaction

차세대 해킹 방지 솔루션

표준제안서

More security,
More freedom

AhnLab ENDPOINT SECURITY SOLUTION

AhnLab

Contents

AhnLab
Safe Transaction

AhnLab

01. 제안 배경

- IE, Chrome, Firefox 등 ActiveX , NPAPI 등 서비스 중단 발표로 대체 솔루션 필요 ('15. 9월부터 중단)
- Windows 10 무상 업그레이드로 빠르게 PC 이용 환경 변화 예상 ('15. 8월 이후 예상)
- 웹 표준을 준수하며, 다양한 보안 위협에 체계적으로 대응할 수 있는 솔루션 필요

신규 보안 위협에 대한 대응

- 웹 및 보안제품을 통한 악성코드 배포 사례 급증
- 사용자 정보 탈취 및 변조를 노린 해킹, 파밍 범죄 매년 30% 이상 증가
- 탈취된 정보가 2차, 3차 범죄로 지속적 활용됨

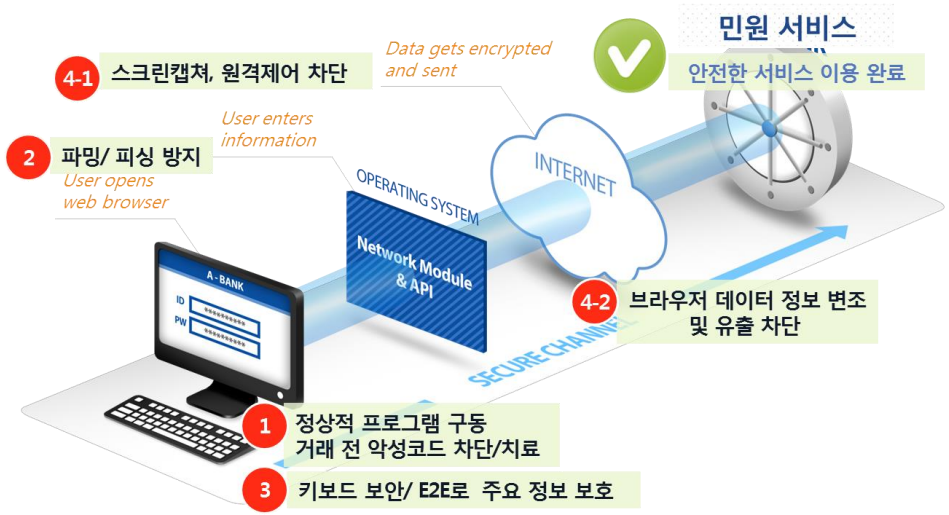
다양한 사용자 환경 지원

- 강력한 보안, 웹 표준을 준수하는 솔루션 필요
- HTML5 사용 확대에 따른 유연한 서비스 제공 요구
- IT 환경변화에 발맞춘 보안 서비스 지원 필요

01. 제안 배경

- Active X 폐지에 따라 홈페이지 보안을 위한 통합 솔루션 도입 필요
- 새로운 보안 위협에 지속적 대응 가능한 보안 강화 대책 마련 필요

홈페이지 보안 강화 대책 필요



홈페이지 보안 개념도

기존 솔루션 대비, 3가지 신규 위협 대응 기능 강화

As-Is
Active X 型 (총 5개 개별 설치)
키보드보안
방화벽
백신
단말 정보 수집
공인인증서

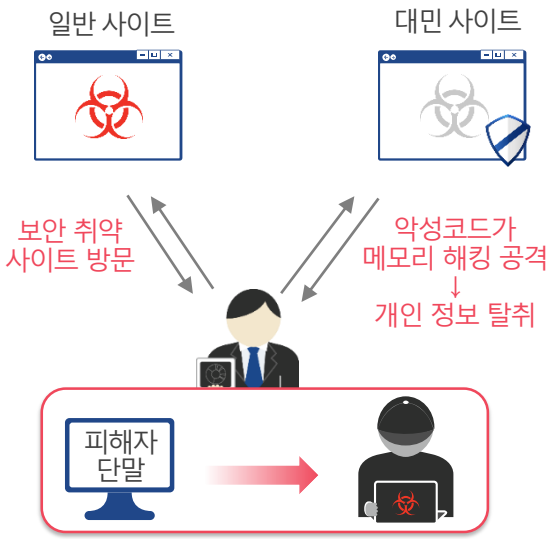
To-be

Safe Transaction (1회 통합 설치)
키보드 보안
방화벽
백신
단말정보 수집
공인인증서
메모리 해킹 방지
안티 피싱
안티 파밍

01. 제안배경 - 보안 위협 트렌드 변화

고전적인 악성코드나 해킹은 주요 취약 요소만을 공격하는 패턴이었으나, '13년도부터 보안솔루션 우회 및 메모리 해킹 등 복합적 기법의 사기 형태가 주요 이슈가 되고 있습니다. 이러한 이슈에 대응하기 위해서는 빠른 모니터링을 통해 위협 요인을 차단하고, 대응하는 것이 중요합니다.

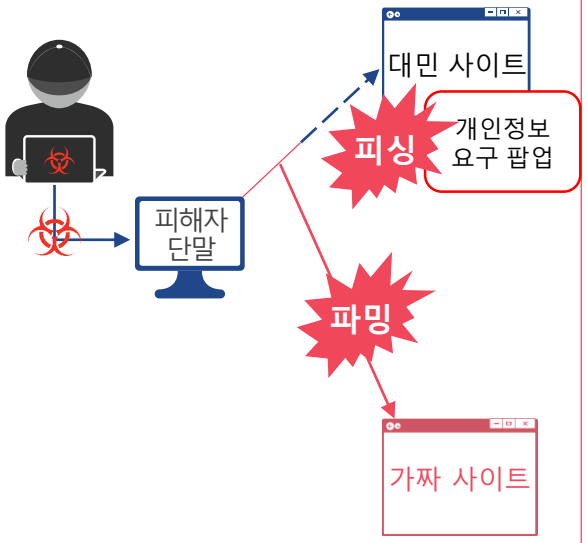
메모리 해킹



- 해커는 피해자 개인정보 탈취 및 조작
- 사회공학적 기법 활용으로 금전 탈취

- 아이디, 패스워드 뿐만 아니라 주소, 생년월일, 직장정보 등 개인정보 유출
- 2차 범죄 재료로 지속적 활용

안티피싱 및 파밍



- 서비스 웹 사이트를 가장한 파밍사이트를 통해 사용자 계정 정보 탈취
- 피싱 사이트로 연결

웹 보안 위협

- ✓ 좀비 PC 사용자 접근으로 인한 웹 사이트 감염
- ✓ 서비스 사이트를 통해 악성코드 무작위 재배포
- ✓ 사이트 신뢰도 하락

- 사용자 단말 내 이상징후 모니터링을 통해 고객사 위협 이슈 사전 차단
- 문제 발생 시, 빠른 원인 파악 및 대응

01. 제안배경 - 홈페이지 보안 강화 대응 방안

고도화된 악성코드, 해킹 기법에 대응 능력을 갖춘 보안 파트너 안랩과 함께 홈페이지 이용 환경을 구축하고, 글로벌 사례를 기준으로 예측할 수 있는 다양한 위협 요인에 대한 대응 체계를 갖춤으로써, 사용자 신뢰를 확보할 수 있습니다.

위협의 다양화

- 키 입력 값 탈취, 변조, 사용자 정보 탈취로 2차 범죄 재료로 활용
- 전문 해커 집단의 보안 솔루션 취약점을 통한 악성코드 배포 및 정보 유출 시도
- MITM(Man In The Middle), MITB (Man In The Browser) 등 메모리 해킹을 통한 금전 사고 급증

사용자 이용 환경 다양화

- Windows, MAC , Linux 등 다양한 OS 환경에서의 보안성 확보
- 멀티 브라우저에 대한 서비스 지원 (IE, Chrome, Firefox, Opera, Safari 등)
- 다양한 보안 제품과 환경에서의 충돌로 서비스 이용성 저해

고도화된 범죄에 능동적 대응

- 보안 업체를 전문적으로 해킹하는 해커 집단들의 등장
- 보안 기법 우회 및 신종 해킹 기법 등에 대한 빠르고 끊임없는 대응이 매우 중요
- 글로벌 주요 보안 업체 등과의 공조를 통해 최신 위협에 대한 정보 확보 및 능동적 대응 중요

신뢰할 수 있는 보안 파트너

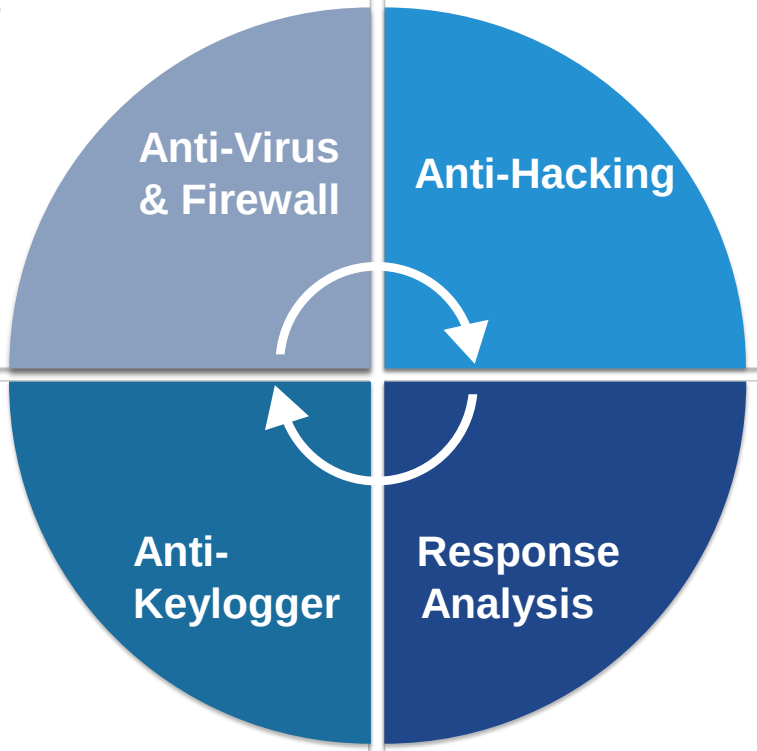
- 국내외 300여 기관 및 쇼핑몰, 은행 웹 사이트 및 일본 금융 보안 서비스 점유 1위
- 보안 위협 대응 능력 만족도 1위 (일본 내 고객만족도 설문조사)
- 글로벌 핫스팟(Hotspot)을 통한 실시간 위협 분석 및 대응 인프라 확보

02. AhnLab Safe Transaction 개요

안랩 세이프 트랜잭션(AhnLab Safe Transaction, ASTx)은 Non-ActiveX 기반의 온라인 트랜잭션을 보호하는 통합 보안 제품으로 웹 서비스 이용 시 발생할 수 있는 다양한 위협과 해킹 요인에 대해 강력한 보안 기능을 제공합니다.

악성코드 탐지 / 네트워크 보호

- 신종 악성코드에 대한 실시간 룰 배포
- 악성코드 확산 대응
- 개인 방화벽
- 악성 패킷 차단 및 위협 대응
- 네트워크 차단 및 사용자 설정 제공
- 취약점 공격 방어



메모리 보호 및 해킹 방지

- 메모리 해킹 방지
- 메모리 접근 및 변조 차단
- 화면 캡처 및 원격 접속을 통한 조작 방지
- 신종 해킹 룰 실시간 배포 및 대응

사용자 정보 보호

- 키보드 보안 (E2E)
- 256bit 암호화 알고리즘 적용
- 커널 레벨 및 애플리케이션 레벨 보호
- 메모리 해킹을 통한 개인정보 유출 및 변조 방지
- 사용자 이용 웹 모니터링 방지

파밍/ 피싱 대응 및 단말 로그 수집

- 피싱, 파밍사이트 경고 및 차단
- 접속 사용자 단말 IP 추적
- 단말 환경 정보 수집
- 보안 위협 정보 수집

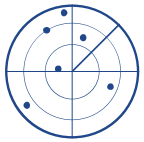
보호 대상에 대한 지속적인 모니터링 및 사용자 정보 변조, 유출 차단
피싱, 파밍에 대한 대응 및 통합 솔루션 기반의 원천적 대응 방안 제공

03. 주요 기능

안랩 세이프 트랜잭션은 Key 입력 값들에 대한 보호부터 개인 정보의 변조와 유출까지, 웹 서비스 이용 시 발생하는 보안 위협을 방어하기 위해 다양한 보안 기능 제공합니다.

온라인 키보드 보안

웹사이트에 접속 할 때 사용하는 ID, PW를 보호하기 위해 커널레벨 및 유저레벨에서 동작하는 다양한 키로거를 원천적으로 방어하며, 256 암호화 알고리즘을 통해 보안성을 강화한 안티키로깅 서비스입니다.



악성코드 탐지 (Process Scanning)

20년간 축적해온 Malware 대응 기술을 집약한 통합검사/ 치료 모듈로 온라인 거래에 적합한 가볍고 빠른 검사 및 진단을 제공합니다. 바이러스,악성코드, 애드웨어, 스파이웨어 등을 모두 동시에 치료하며, 1hourly Update를 통해 신종 악성코드에도 빠르게 대응합니다.

네트워크 보호 (Personal Firewall)

각종 보안 위협으로부터 개인을 보호하기 위한 PC 방화벽으로 네트워크를 통한 침입과 외부의 해킹을 감지하여 각종 개인 암호나 개인정보의 무단 유출 및 데이터 손상의 위협을 사전 차단합니다.

콘텐츠 위변조 방지

PC의 키보드로 사용자가 입력하는 키보드 입력 정보를 가로채어 개인의 중요한 정보를 유출하는 키로거(Keylogger) 및 웹 페이지 조작, 브라우저 DOM 메모리 변조를 통한 콘텐츠 정보 무결성 훼손을 방지 합니다.

메모리 보호 및 해킹 방지 (Anti-Hacking)

미지의 해킹요소에 대한 직접 감지/ 차단/ 복구가 가능한 솔루션으로써 웹상에서 발생하는 거래정보에 대한 변조 / Self Protection 영역에 강점을 가진 안티-해킹 서비스입니다.

04. 제품 특장점 (1/3)

안랩 세이프 트랜잭션은 전세계적으로 사용자의 개인정보 탈취를 목적으로 한 정교하고 고도화된 보안 위협에 대응하여, 4단계 보안위협별 당사 솔루션의 유기적 결합을 통해 효과적인 보안 대책을 제공합니다.

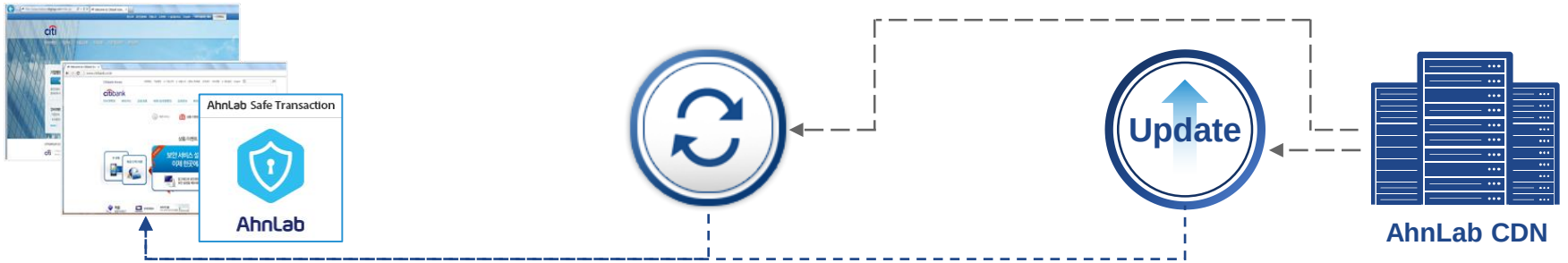
보안 프로그램 무력화	피싱 / 파밍 대응	키 입력값 탈취 변조	해킹 시도 원격 접속
OS 시작 시점부터 구동 안티디버깅 기술로 보안제품무력화 최소화	웹 페이지 경로에 대한 안정성 확보	키보드보안 + E2E 화면 캡처 방지와 브라우저 DOM 보호를 통한 정보 보호	안티해킹, 악성코드 대응 Hourly Update 기반의 민첩한 대응

엔드포인트에서 서버까지 트랜잭션 전 구간의 통합적 보안 기능 제공

※ 사용자 이용 시나리오

웹사이트 접속
보호사이트 Mode 동작

→ **보안 솔루션 다운로드 및 설치 (1회)** → **상시 구동, 자동업데이트, 패치**



04. 제품 특장점 (2/3)

안랩 세이프 트랜잭션은 ActiveX 기반이 아닌 상주형 보안 모듈로 운영체제와 함께 실행되므로 실행 시점 차이로 인한 보안 문제와 ActiveX 이슈를 동시에 해결 할 수 있습니다.

운영체제 시작

사이트 접속

상주형 보안모듈 동작

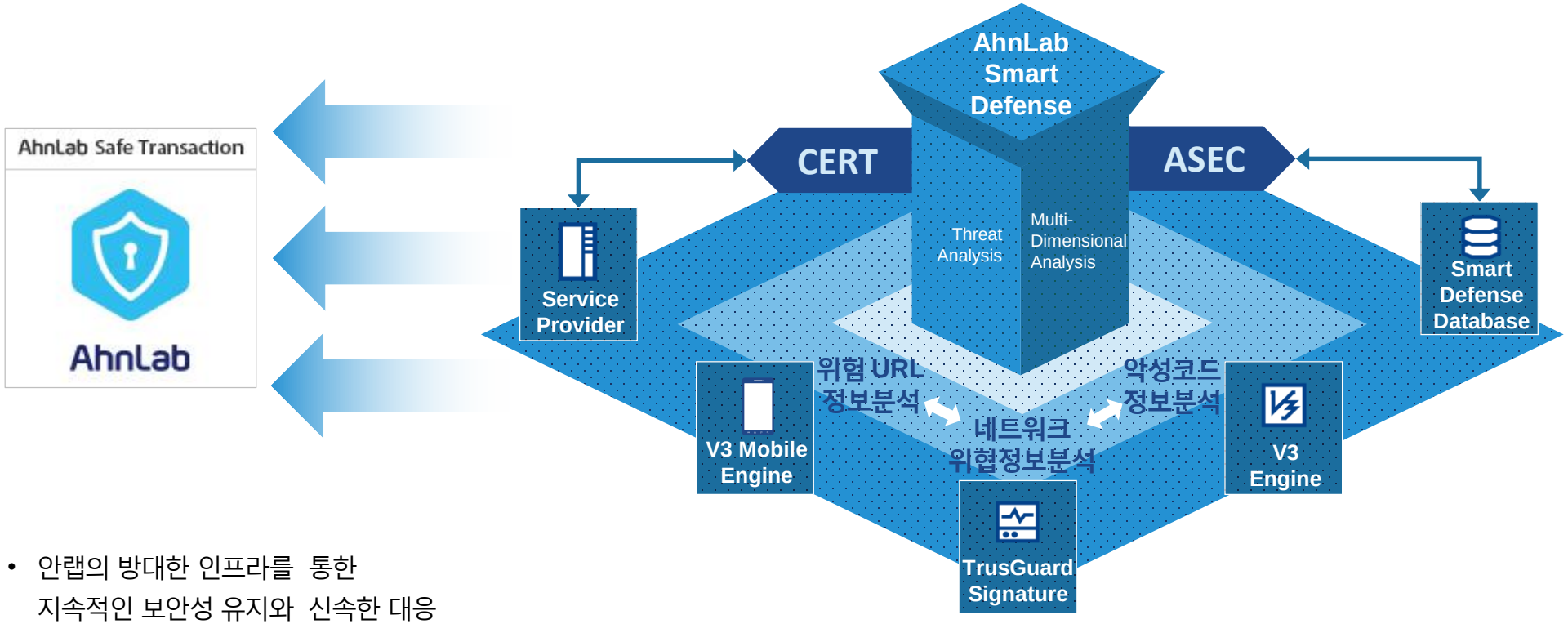
방화벽, 안티해킹, 피싱/ 파밍 대응

웹 서비스 보호 기능 실행

키보드 보안, Process 감시, 웹 콘텐츠 위변조 감시

04. 제품 특장점 (3/3)

안랩 세이프 트랜잭션은 안랩의 통합된 클라우드 분석 인프라 기반의 서비스를 제공함으로써 빠르고 입체적인 조치가 가능합니다. 안랩의 클라우드 분석 시스템은 자사 모든 제품에서 수집되는 다양한 악성코드 및 이상행위에 대해 분석 및 대응하는 안랩만의 독자적인 플랫폼입니다.



- 안랩의 방대한 인프라를 통한 지속적인 보안성 유지와 신속한 대응
- 전 제품과 인프라가 연계되어 있어 매우 민첩하고 빠른 대응이 가능.

05. 경쟁사 비교 자료 (1/2) - 키보드 보안 기능

국내 대다수의 키보드 보안 솔루션은 취약성을 가지고 있으며, 이를 회피하는 악성코드에 그대로 노출되고 있습니다.

주요 기능	설명	AhnLab	경쟁사
설치	Install/Uninstall 제공	○	○
	제품 실행 확인 방법 제공	○	○
	최초 설치 시 웹브라우저 종료 불필요	○	○
자체보호	안티디버깅 / 리버싱	○	X
	메모리보호 암호화	○	X
	Local Memory Protect (LMP) - 후킹 공격 방어	○	X
보안기능 (유저레벨)	SubClassing 방어	○	○
	MessageHooking / API Hooking 방어	○	○
	DOM 접근 입력 정보 탈취 방어	○	○
보안기능 (커널레벨)	[PS2] Port Scanning / IDT Hooking 방어	○	○
	[PS/2] H/W Breakpoint 를 이용한 Debug IDT Hooking 방어	○	○
	[PS/2] Filter 및 Service Callbank Hooking 방어	○	○
	[USB] USB Bus Drivers Hooking / Upper Filter 방어	○	○
	[USB] USB Hub Drivers (or Usbccgp Drivers) Hooking/ Lower Filter 방어	○	○
	[USB] USB Hub Drivers (or Usbccgp Drivers) Upper Filter 방어	○	○
	[USB] HIDUsb Drivers Hooking / Lower Filter / Upper Filter 방어	○	○
	[USB] USB 3.0 Hub Hooking 방어	○	○
	[Bluetooth] HIDBTH upperfilter 방어	○	X
	[Bluetooth] HIDBTH Hooking 방어	○	X
암호화	자체 End to End 암호화 구현	○	○
	256 bit 암호화 알고리즘 적용	○	○
	인증서 탈취, 보안 제품 우회 방어	○	X
	키 입력값 위변조 방지	○	X

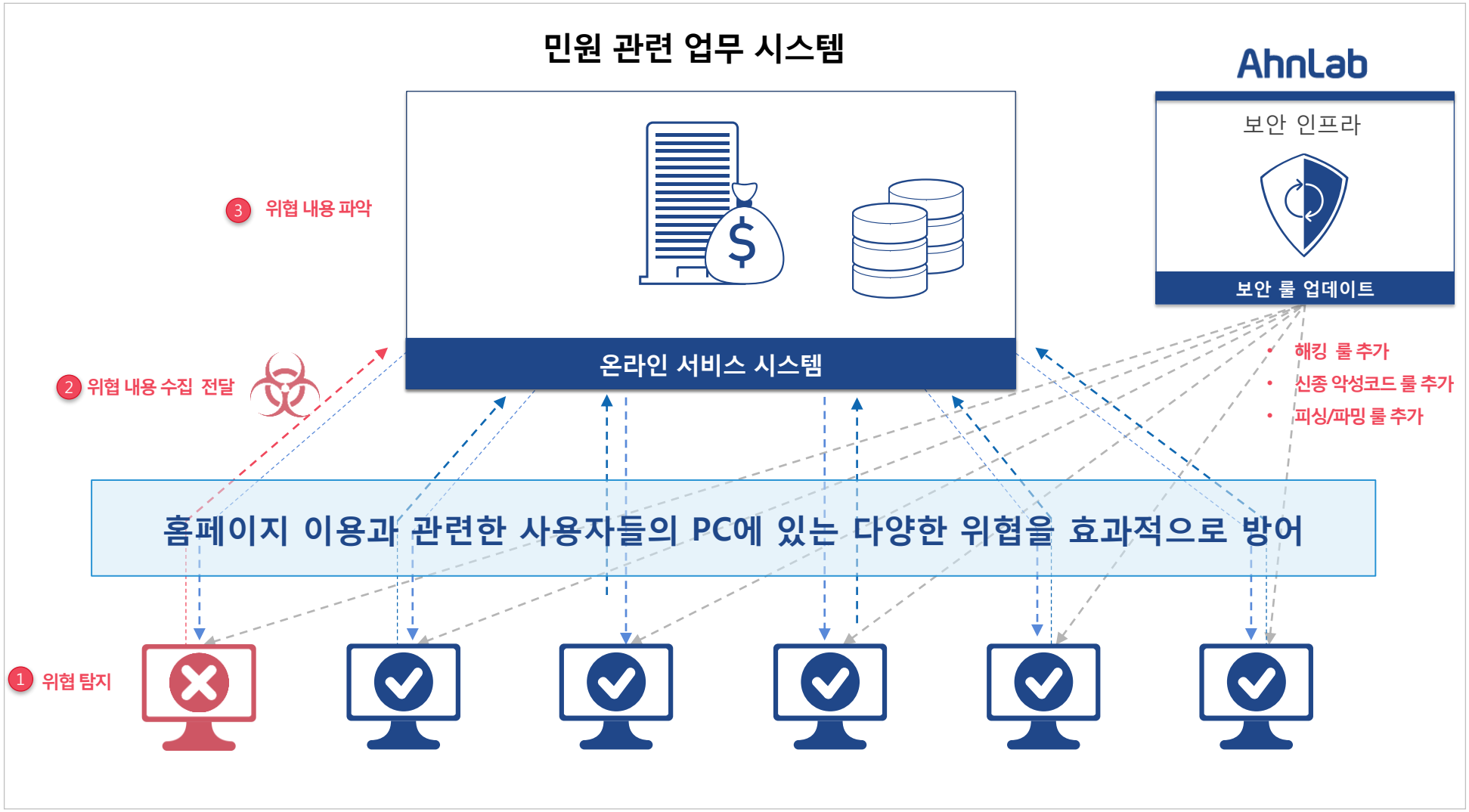
05. 경쟁사 비교 자료 (2/2) - 브라우저 보호 기능

안랩은 기술적으로 가장 난이도 있고, 뛰어난 기술력으로 웹 사이트 보안을 위한 전방위적 솔루션을 제시합니다.

주요 기능	설명	AhnLab	경쟁사
최신 업데이트 지원	최신 제품 셋 유지	O	O
무결성 지원	자체프로그램 변조 방어 및 원복 기능	O	X
보안제품 실행 확인	보안프로그램 실행 유무를 확인하여 강제 해제 시 대응	O	X
로그 기능	보안, 실행 로그 기록 지원	O	X
안티 디버깅/리버싱	자체프로그램 난독화 적용 및 분석 방지 기능	O	O
메모리 접근/조작 방지	외부 접근에 의한 메모리 접근 및 조작 방지 (읽기/쓰기 방지)	O	X
프로세스 접근 차단	외부 프로세스 접근 차단	O	X
웹페이지 변조 차단	외부 접근에 의한 HTML 삽입 차단	O	X
HTTP 요청 변조 차단	HTTP 요청 변조 및 유출 방지	O	X
피싱/파밍 차단	DNS 응답 주소 무결성 검사	O	X
BHO 차단	구동 차단 / 접근 차단(Shield)	O	**X**
화면 캡처 방지	화면 캡처 차단	O	O
원격제어 방지	외부접속(VNS)에 의한 키보드/마우스 제어 방지	O	X

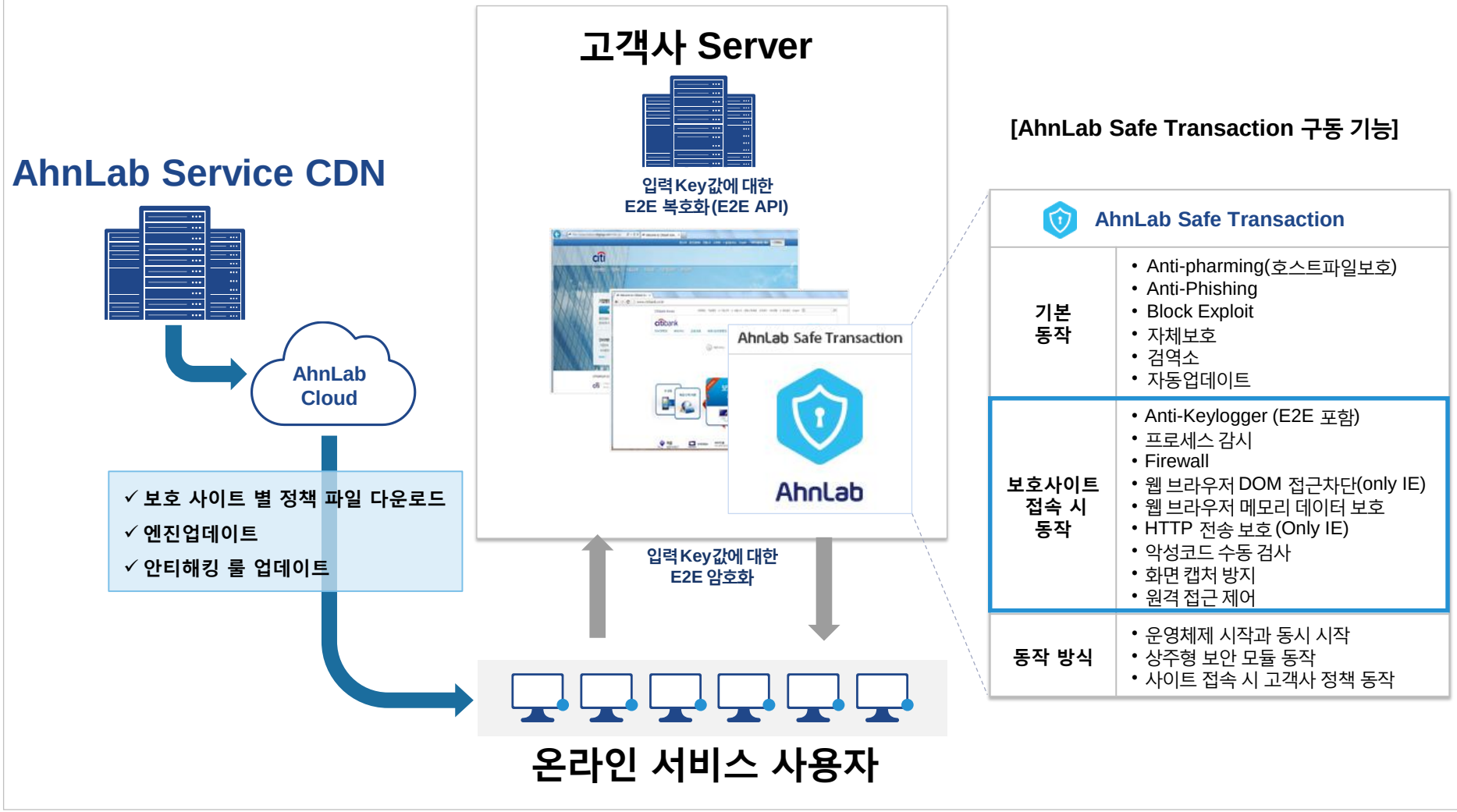
06. 솔루션 구성도

안랩 세이프 트랜잭션은 Non-ActiveX 방식의 통합 보안 솔루션으로 정부의 정책을 준수하면서 사용자가 홈페이지를 안전하게 이용 할 수 있도록 하는 보안 제품입니다.



06. 솔루션 구성도 - 구축 제안 구성 예시

안랩은 시급성이 요구되는 보안 이슈를 고려해 당사 노하우를 기반으로 신뢰성 높은 보안을 제공합니다.

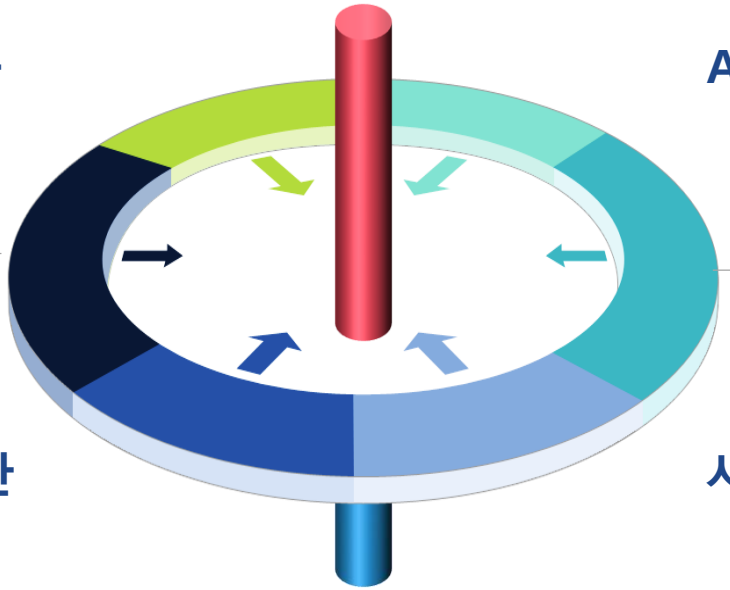


07. 도입 효과

안랩 세이프 트랜잭션은 Non-Active 방식의 통합 보안 솔루션으로서 컴플라이언스를 준수하면서도 안전한 웹 서비스를 제공할 수 있게 해드립니다.

다양한 고객의 환경의 보안 취약점에 대응한, 강력한 최신 해킹 방어와 사전 예방 기능을 통해 고객의 비즈니스 운영 환경을 안전하게 조성 하는데 기여

행정자치부 지침 준수
Non-ActiveX 대응



AhnLab CDN을 통한
배포 및 업데이트

최신 해킹 기법에 대한
빠른 조직적 대응

서버 연동 구축 최소화
보안성은 최대화

Appendix

AhnLab
Safe Transaction

1) ActiveX vs. Non-ActiveX

2) ActiveX 기반 키보드 보안의 취약점 이슈

3) 단일 키보드 보안 솔루션 취약점 개요

4) 기존 개별 보안 솔루션의 취약점 이슈

AhnLab

ActiveX vs. Non-ActiveX

Non-ActiveX 방식으로 온라인 트랜젝션를 보호하기 위해 백신(Anti-Virus) 프로그램처럼 메모리에 상주하여 사용자의 PC를 부팅시점 보호 함
(대상 : 온라인 방화벽, 키보드보안, 온라인 백신 등)

ActiveX

① 웹페이지 접속
② 보안 모듈별 ActiveX 설치/구동
- 사이트별 4~6회 설치필요
③ 보안 모듈별 개별 업데이트
- 년 6~17회 설치필요
④ 웹브라우저 종료 시 보안모듈 종료

※ Windows 10, IE 11버전부터 ActiveX 지원종료 예정

대민 서비스 사이트

Non-ActiveX

① 웹페이지 접속
② 통합보안프로그램 다운로드 후 설치
- 범용 프로그램별 1회 설치
③ 자동 업데이트
- 프로그램별 자동 업데이트
④ PC 부팅 시 부터 종료 시 까지 상시 보호

※ 크롬 NPAPI Plug-in '15년 9월 지원종료 예정

동작방식	내용
ActiveX 및NPAPI 플러그인	웹브라우저 및O/S에 대한 종속성이 존재(제조사 차원에서 지원 종료 예정)
Flash	Flash 사용을 위해ActiveX(또는EXE) 설치가 필요함
JAVA	JAVA 환경 구성을 위해ActiveX(또는EXE) 설치가 필요함
HTML5 (웹 표준)	네트워크 및 커널 레벨 드라이브를 사용하는 보안모듈을 적용하기는 불가능함 PC 자원 접근에 대한 제약사항이 존재함
범용프로그램(EXE)	최초 1회 설치 후 PC 및 전자금융거래 사이트를 보호 가능함

웹 보안 프로그램 동작방식 구분

ActiveX 기반 키보드 보안의 취약점 이슈

ActiveX 기술로 인한 보안 한계가 그 원인

ActiveX 기반의 보안 모듈은 보호 대상 사이트에 접속했을 때, 다운로드 실행 되며,
실행 시점 차이로, ActiveX 보안 모듈 실행을 악성코드가 차단하는 문제 발생

➔ 대부분의 위협은 ActiveX 보안 모듈이 다운로드 되기 이전부터 진행

운영체제 시작

Malicious Code
Zero-Day Attack
Drive-By Attack

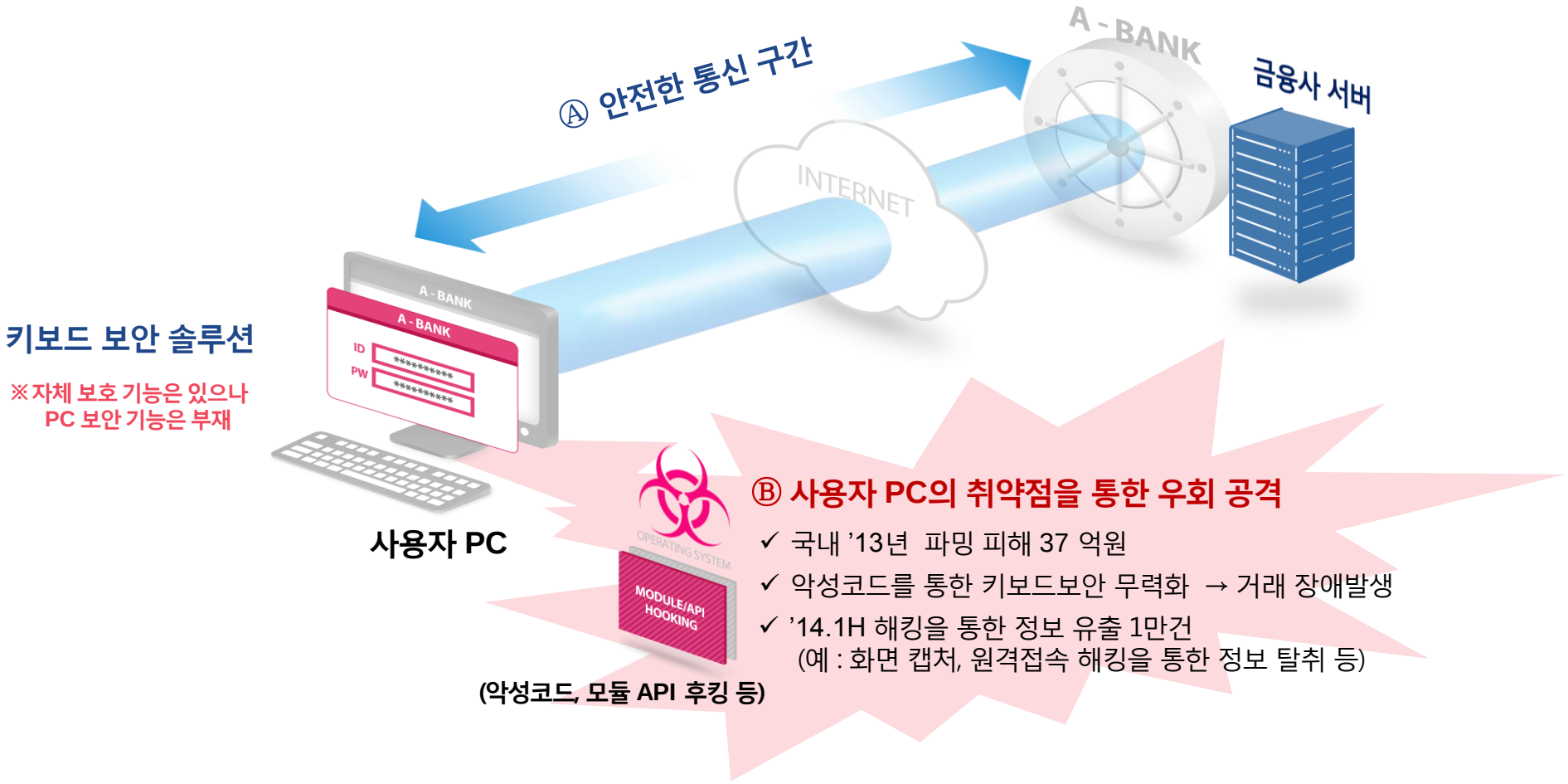
취약 사이트 방문

다양한 취약점 노출

ActiveX 기반
보안모듈 시작

단일 키보드 보안 솔루션 취약점 개요

Ⓐ 키보드 보안 솔루션 정상 동작 時 키 입력 ↔ 카드사 서버 間 통신은 안전한 반면,
Ⓑ 파밍 및 사용자 PC 해킹 등의 우회 공격을 통한 보안 위협에는 취약



기존 개별 보안 솔루션의 취약점 이슈

개별 보안 솔루션 대응의 한계 존재

기존 금융 및 전자결제 보안을 위한 솔루션은 개별 보안 위협에는 대응하나,
개별 솔루션의 기능만으로는 그 취약점을 우회한 해커의 공격 대응 불가
➔ 안티 키로깅, 악성코드, 인증 / 암호화 취약점에 통합 대응 가능한 솔루션 필요

보안위협	기존 솔루션	취약점 (이슈)
악성 코드	[Anti-Malware 솔루션] • 알려진 위협에 대응 가능	• 신·변종 악성코드는 대응 역량에 매우 의존적
키로깅	[Anti-Keylogging 솔루션] • **가상 키보드/마우스 기반 웹 보안 장치** • 웹 기반 보안 취약점 우회 방어	• 기 장악된 PC에서 거래 장애유발을 통한 **콘텐츠 변조, 화면 캡처, 원격 접속**, BHO DOM **취약점은 여전히 잔존함**
통신 및 인증	[암호화 통신 솔루션] • SSL, 키보드 보안 (E2E) , 암호화 구간 Data 신뢰성 제공	• 암호화 전·후 구간에서의 보안 취약성 • 사회공학 해킹 위협
	[인증 솔루션] • PKI, OTP / IC Card • 인증 기반 사용자 신뢰성 확보	• 인증 전 Data 신뢰성 미확보, 인증 우회 가능 • 사용의 불편함

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab
Safe Transaction

AhnLab