# 알약 3.0 제안서


ESTsoft

## 제안내용

1) 제안배경

2) 알약 3.0

3) Reference

4) 회사소개

# 1. 제안배경

End-point 보안의 중요성

End-point 보안의 필수조건

도입효과

# 제안배경 | End-point 보안의 중요성

ESTsoft

## End-point PC는 악성코드의 주요 공격대상

### 인터넷 연결 PC를 목표로 하는 악성코드 급증

- 개인정보 탈취 목적 (주민번호, 계좌번호, 사용자 ID/비밀번호 등)
- PC의 좀비화 목적 (DDoS 공격, 네트워크 침투 등)


### 다양한 경로를 통한 악성코드 확산

- 스마트폰, 태블릿 PC등의 확산 (모바일기기 연결을 통한 악성코드 유입)
- 파일공유, 이동식저장장치(USB) 등을 통한 유입

**USB등을 통한 감염 및 내부자료 유출 방지를 위한 매체제어 기능 필요**

**기업보안의 시작은 End-point 보안!**

**End-point 보안의 기본은 백신!!**

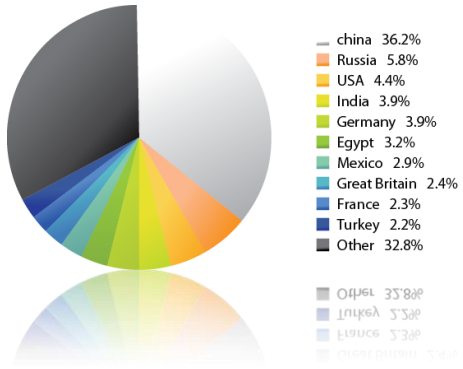
# 제안배경 | End-point 보안의 필수조건

ESTsoft

## 신종 악성코드에 대한 대응과 안정적인 탐지능력

### 악성코드의 97% 이상 해외에서 발생,유입

광범위한 악성코드 정보수집능력과
신종악성코드에 대한 사전 방역능력이 우수한 백신 필요




### 오탐 사고로 인한 업무 중단

- 부팅이나 시스템 불능 사태일 경우 업무 중요 데이터 손실
- 오탐으로 인한 복구 지원 및 비용 발생

오탐지를 최소화 하기 위해 백신 업데이트 제공 시
업데이트 DB에 대한 사전 검증 프로세스 필요

**높은 악성코드 탐지율과 동시에**
**오탐사고의 최소화에 대한 요구**

# 제안배경 | 도입 효과

ESTsoft

인터넷 연결 PC를 목표로 하는 악성코드 급증

다양한 경로를 통한 악성코드 확산

악성코드의 97% 이상 해외에서 발생,유입

오탐 사고로 인한 업무 중단

## 알약의 빈틈없는 사전방역

침투경로 사전차단 매체제어기능,
알려지지 않은 악성코드 탐지 휴리스틱 검사
보안취약점/윈도우업데이트 관리

## 알약의 강력한 백신엔진

특허받은 오탐검증 시스템,
국제인증으로 검증 된 트리플엔진
시스템은 더욱 가볍게 스마트스캔

**알약 하나로 End-point 보안 완전 해결**

# 2. 알약 3.0

**제품라인업**

**알약 3.0의 특장점**

# 알약 제품 라인업

ESTsoft




| 알약 3.0 | 알약 3.0 Server Edition | ASM 3.0 |
|---|---|---|
| 윈도우 워크스테이션용 통합보안제품 | 원도우 서버용 통합보안제품 | 알약 3.0과 알약 3.0 Server Edition을 관리할 수 있는 중앙관리 솔루션 |
| **지원플랫폼** | | |
| Microsoft Windows 2000/XP/ Vista/7/8 (32bit/64bit) | Microsoft Windows Server 2000/ 2003/2008 (32bit/64bit) | MS SQL 사용시 : Microsoft Windows XP SP3/2003 SP2/ 7/VistaSP2 2008 SP2 (32bit/64bit) Cubrid 사용시 : MS Windows XP/Vista/ 7/2003/2008(32bit/64bit) |

# 알약 3.0의 특장점

ESTsoft

알약 3.0은 악성코드가 침투하기 이전에 사전차단하고, 유입된 경우에도 강력한 탐지력으로 악성코드를 퇴치합니다.
또한 알약의 철저한 지원체계는 누구보다 빠르게 악성코드에 대응하고 있습니다.


## 빈틈없는 사전방역!

**악성코드 침투경로 사전차단**

매체제어, 휴리스틱 검사, 자가보호기능 강화, 보안취약점 체크에서 윈도우 보안업데이트
그리고 철저한 업데이트 검증 시스템 까지

## 강력한 백신엔진!

**완벽한 치료와 쾌적한 PC환경**

트리플엔진, 스마트 스캔으로 빠르고 완벽한 탐지, 오탐검증시스템으로 오탐지 피해 차단

## 철저한 지원체계!

**가장 빨리 대응하는 지원 시스템**

악성코드종합처리센터(A-CERT), 원격지원, e-mail상담, 고객핫라인 등 빈틈없는 고객지원

## 빈틈없는 사전방역!

업데이트 검증 시스템

매체제어

휴리스틱검사

자가보호기능 강화

시스템 취약점 점검

윈도우 보안업데이트

ESTsoft

## 알약의 업데이트 검증 시스템

알약의 업데이트 검증 시스템은 무결성 검증 및 전송 데이터 암호화를 통해 업데이트 파일의 위,변조를 방지함으로써 2013년 3월 20일에 있었던 변조된 파일의 배포로 인한 사고와 유사한 형태의 피해를 미연에 방지할 수 있습니다.

### 업데이트 파일의 무결성 검증

고수준 해시(hash) 알고리즘 사용

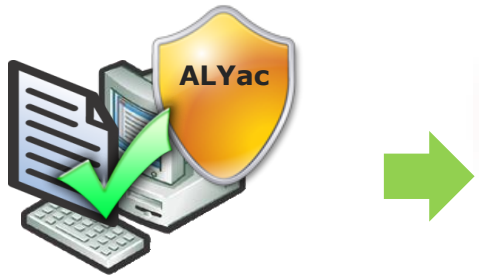
### 전송 데이터 암호화


데이터 난독화 및 SSL 암호화 통신

## 알약의 무결성 검증 방법


1. ASM에서의 무결성 검증

| 무결성 검증 방법 | |
|---|---|
| ASM | 업데이트 파일 셋에 대한<br>**파일별 해쉬 검증** |
| 알약 클라이언트 | 업데이트 파일 셋에 대한<br>**파일별 해쉬 검증과**<br>**실행 파일에 대한 디지털 인증서 검증** |




2. 알약클라이언트 에서의
무결성 검증

3. 무결성 검증에서
이상이 발견될 경우 삭제 처리

# 해쉬 검증과 디지털 서명

### 해쉬검증이란?

해쉬 검증은 데이터를 주고받을 때, 경로의 양쪽 끝에서 데이터의 해쉬값을 구해, 보낸 쪽과 받은 쪽의 값을 비교하여
데이터를 주고받는 도중에 변경이 가해졌는지 여부를 확인할 수 있는 검증 방법

특히 해쉬 검증에 사용되는 해쉬값은 '일방향 해쉬함수'를 통해 계산된 값으로 같은 해쉬값을 가진 다른 데이터를 작성하기가 어려워
통신의 암호화 보조수단이나 사용자 인증, 디지털 서명 등에 널리 활용

### 디지털 인증서 검증

웹상에서 상대편을 믿고 신뢰할 수 있도록 하는 전자 보증서의 일종으로 특정한 인증기관에서 발급하며,
인증서의 소유자 명, 유효기간, 전자서명을 확인 할 수 있는 공개 키, 인증기관의 전자서명 등이 포함

전자서명을 확인 하는데 사용되는 공개키는 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 다르기 때문에 거의 완벽한
데이터 보안이 가능하고 정보유출의 가능성이 적은 암호화 방법

## SSL을 이용한 연결 및 데이터 암호화 전송


**HTTPS 프로토콜을 이용한 서버운영**

### SSL (Secure Sockets Layer) 이란?

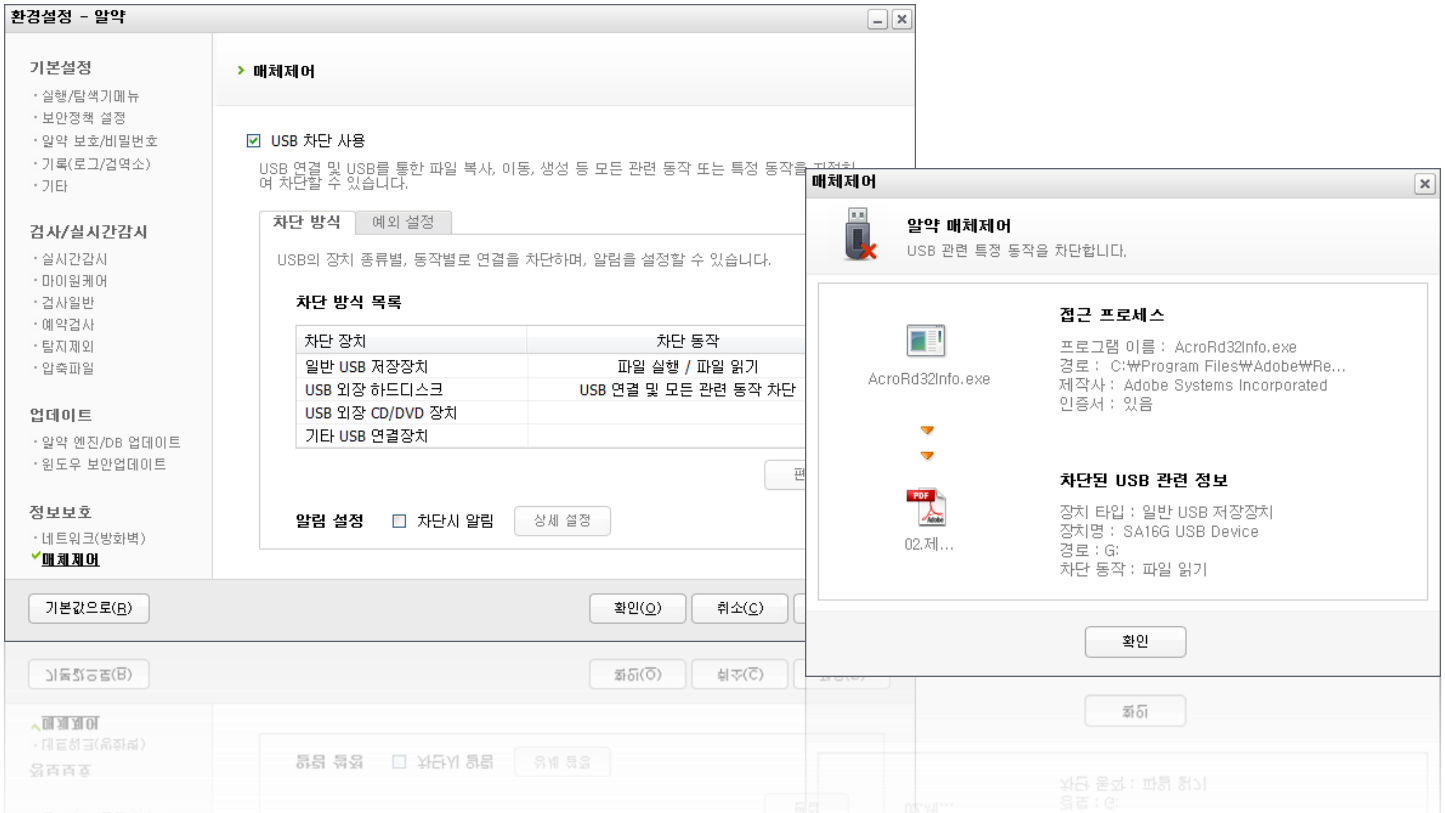
SSL은 사이버 공간에서 전달되는 정보의 안전한 거래를 보장하기 위해 정한 인터넷 통신규약 프로토콜로 서버와 클라이언트의 진위 확인이 가능하도록 해주는 역할을 하며,
웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에도 적용 가능
또한 인증 암호화 기능을 통해 암호화키와 관련된 협상을 할 수 있을 뿐 아니라 상위 응용프로그램이 정보를 서버와 교환하기 전에 서버의 진위 확인이 가능한 장점을 지님

# 빈틈없는 사전방역 | 매체제어

ESTsoft

## 매체제어 기능을 통해 USB 등 다양한 이동식 저장장치를 통한 자료유출/입 차단

• **차단 방식**
- **파일 실행 :** exe와 같이 실행 가능한 파일 실행 차단
- **파일 읽기 :** 각종 오피스 외 미디어 파일들을 열지 못하도록 차단
- **파일 쓰기 :** USB 내에서 파일 복사, 생성 및 수정하는 것을 차단

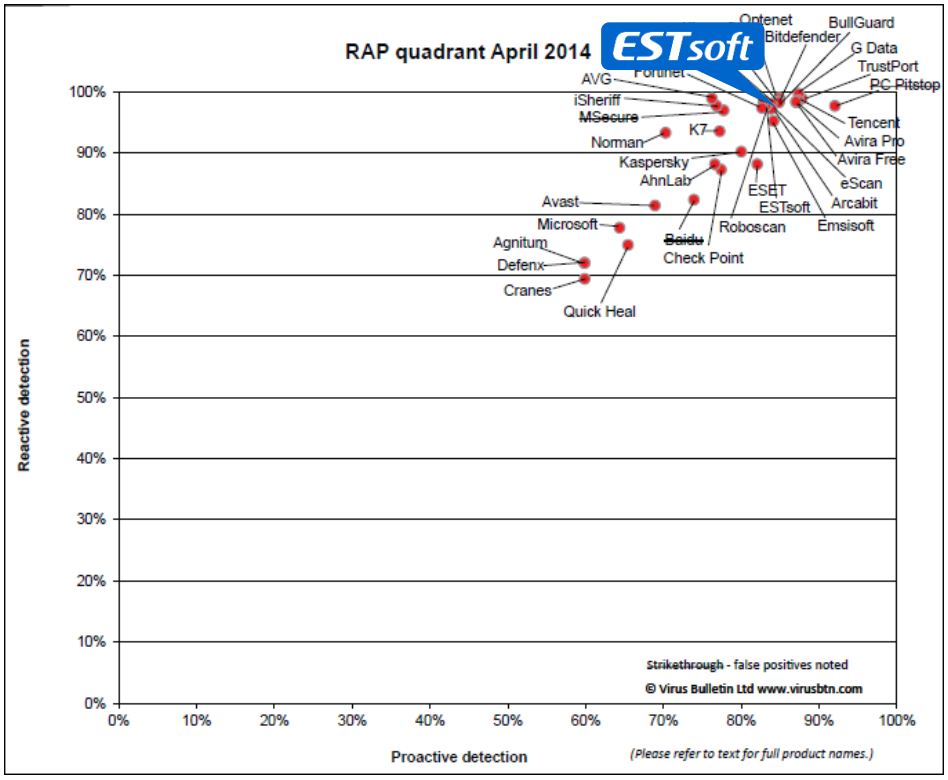


# 빈틈없는 사전방역 | 휴리스틱검사

## 악성코드에 대한 정보가 없어도, 가상PC 환경에서 미리 파일을 실행하여 위험요소 탐지

각종 테스트에서 알약의 휴리스틱검사와 새로운 악성코드 탐지에 대한 우수성 검증

**[VB100% Reactive 및 Proactive 테스트 결과]**




[ RAP 테스트 ]
Reactive detection을 통해 백신 DB의 대응력을 판단하고,
Proactive detection을 통해 사전방역 능력을 판단

새로운 악성코드가 빠르게 발생하고,
모든 악성코드의 진단이 불가능한 현 상황에서
단순한 진단율 테스트보다 중요한 척도가 되는 테스트

| 구분 | **대응능력**<br>Reactive detection | **사전방역**<br>Proactive detection |
|---|---|---|
| **ESTSoft** | **97.75%** | **83.20%** |
| **Average** | 92.18% | 78.92% |

**Reactive detection**
- 새로운 멀웨어와 알려지지 않은 멀웨어에 대한 대처능력

**Proactive detection**
- 휴리스틱, 제네릭 기술을 사용한 사전방역 능력

# 빈틈없는 사전방역 | 자가보호기능 강화

ESTsoft

## 백신을 위협하는 악성코드로부터 알약을 보호하는 강력한 자가보호기능

**[파일 자가보호]**

- **상위폴더 자가보호** : 숨김 파일 및 읽기 전용과 같은 파일 및 폴더 속성 변경에 대해 방어
- **상위의 상위 폴더 자가보호** : 알약이 포함되어 있는 폴더를 외부로 이동하거나 이름 변경 등에 대한 방어

**[프로세스 자가보호]**

### 프로세스 로직 변경으로 알약의 실행을 방해하는 공격에 대한 방어능력 강화

- **Windows 작업관리자** : 작업 관리자에서의 응용프로그램 / 프로세스 종료 방어

| 구 분 | 알약 3.0 | V3 |
|---|---|---|
| 프로세스 끝내기 | O | O |
| 작업 끝내기 | O | X |

- **APT(Advanced Process Termination** : APT 툴에서 제공하는 여러 가지 방법을 이용한 프로세스 킬 모두 방어

* V3 프로세스 – V3Svc.exe, V3Sp.exe

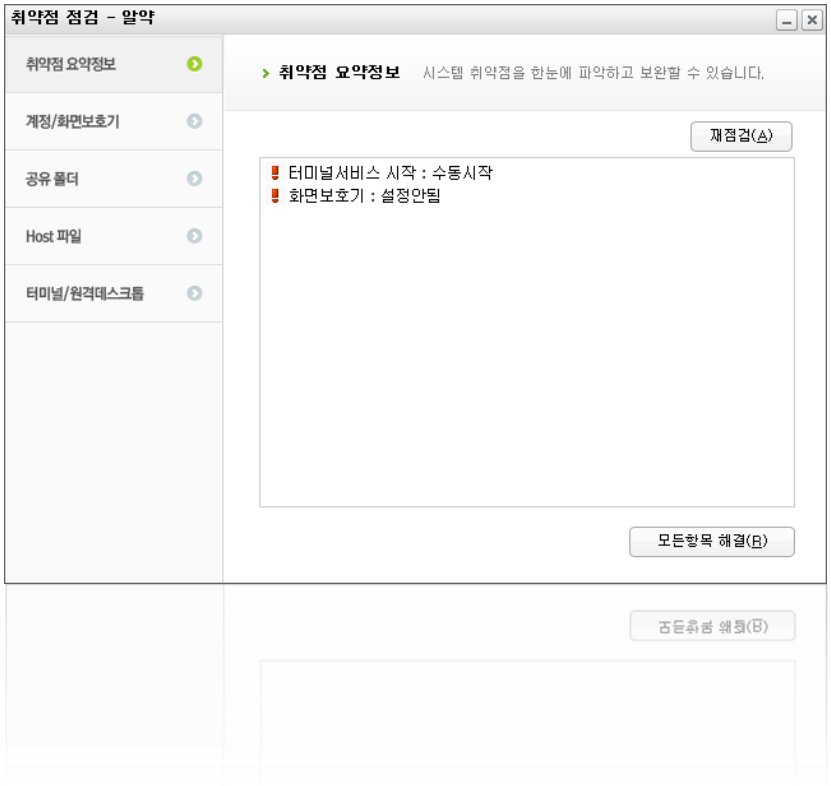
| 구 분 | Kill 1 | Kill 2 | Kill 3 | Kill 4 | Kill 5 | Kill 6 | Kill 7 | Kill 8 | Kill 9 | Kill 10 | Kill 11 | Kill 12 | Suspend 1 | Suspend 2 | Kernel Kill 1 | Kernel Kill 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 알약 3.0 | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O | O |
| V3 | O | X | X | X | O | O | X | O | O | O | O | O | O | O | O | O |

• 프로세스 끝내기 : Windows 작업관리자 – 프로세스 Tab – 프로세스 끝내기 기능
• 작업 끝내기 : Windows 작업관리자 – 응용프로세스 Tab – 작업 끝내기 기능
• APT(Advanced Process Termination) : 프로세스 종료 테스트 툴

## 시스템상 보안 취약점 현황에 대한 관리

위험요소 또는 외부 공격자로부터 시스템이 공격 당할 수 있는 기본적인 보안 취약점 확인 및 보완

- 계정 암호 / Guest 계정 사용 여부
- 화면보호기 사용 유무
- 설정된 공유 폴더 현황
- 악성 Host 파일/ 추가된 Host 점검
- 터미널 서비스/ 원격데스크톱 사용 여부

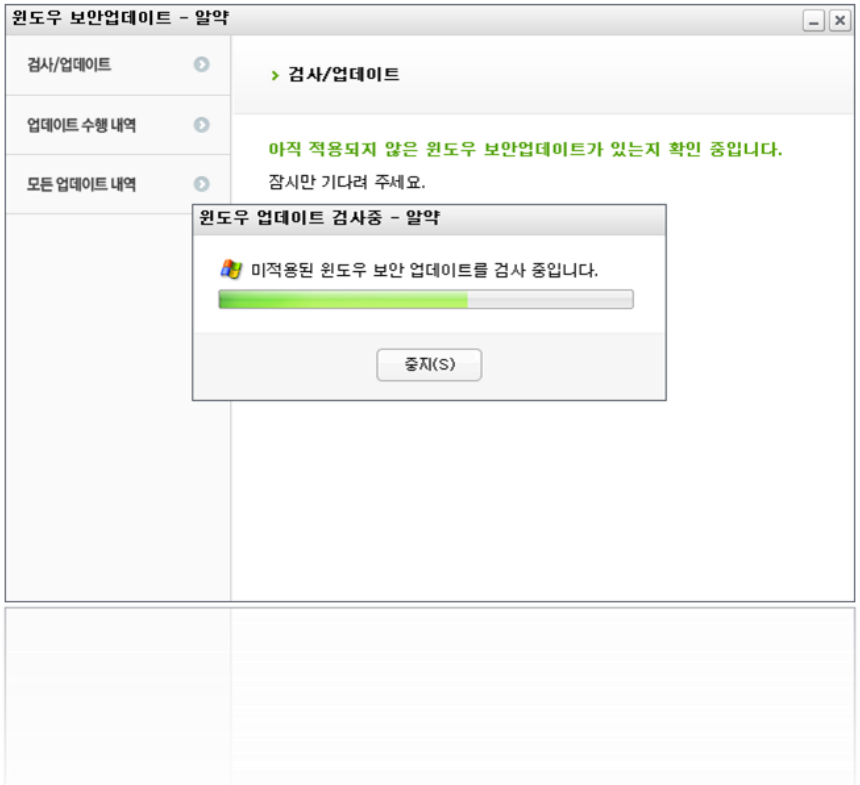


ESTsoft

## 알약에서 윈도우 보안업데이트 점검 및 관리까지

미 적용된 윈도우 보안 패치를 확인하고 업데이트를 진행하여 항상 시스템에 누락 없는 최신 윈도우 보안 패치 유지

- **미적용 윈도우 보안 업데이트 확인 및 업데이트 진행**
- **알약을 통한 업데이트 히스토리 제공**
- **시스템에 설치된 모든 업데이트 내역 확인**



## 강력한 백신엔진!

강력한 Triple 엔진

Smart Scan

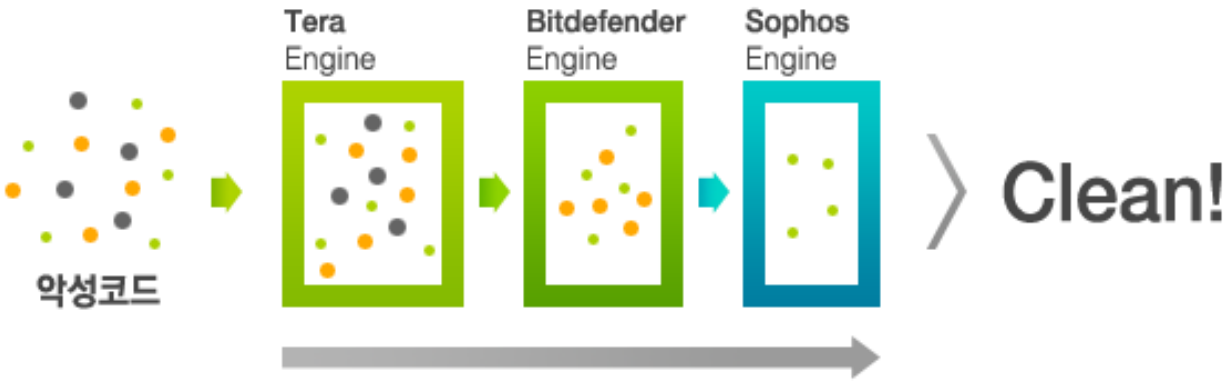
오탐검증 시스템

검증받은 알약엔진

# 강력한 백신엔진 | 강력한 Triple 엔진

ESTsoft

## 국내외 악성코드를 높은 탐지율로 빈틈없이 방어




**테라(Tera) 엔진**

**이스트소프트 알약의 자체 개발 엔진** 으로 7년간의 엔진 개발 노하우와 DB 분석 팀의 패턴 업데이트를 통해 악성코드를 빠르고 정확하게 탐지

**Bitdefender 엔진**

방대한 DB로 전세계 악성코드에 대응하며 알려지지 않은 악성코드를 탐지하는 **사전 방역 능력 우수**

**Sophos 엔진**

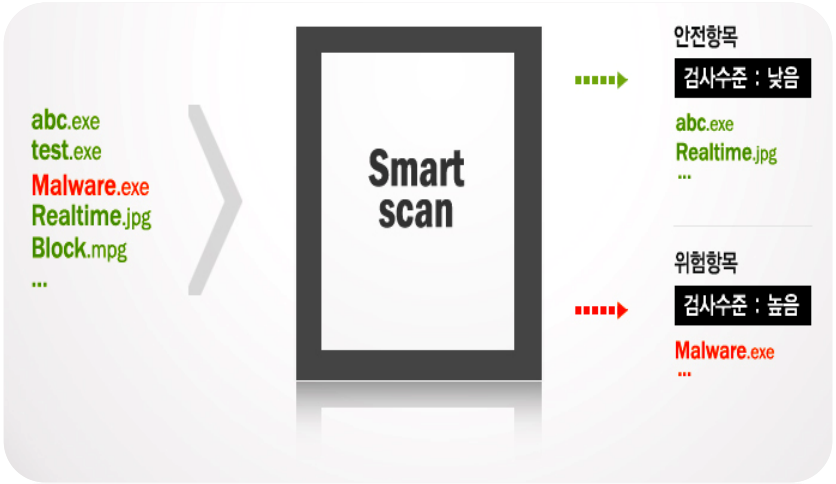
알약 2.0에 새로 추가된 엔진으로 **검사 속도가 아주 빠른 것이 장점이며, 뛰어난 변종 탐지능력 보유**

**전세계 전략적 파트너쉽과 기술 고객사들과의 샘플 공유**
**시간대가 다른 국내외 여러 분석 센터에서 24시간 악성코드 분석 및 업데이트 제공**

# 강력한 백신엔진 | Smart Scan

ESTsoft

## Smart Scan을 통해 검사속도는 높이고 실시간 감시 부하는 낮추고




**높은 탐지율을 유지하면서도 효율적이고 빠른 검사진행**

### Smart Scan 이란?

- Smart Scan은 실시간 감시나 정밀 검사 시 실제 검사가 필요한 파일을 분류하고 관리하는 기술
- 안전함(White List)으로 검증된 파일은 검사에서 제외되어 검사 속도는 빨라지고 실시간 감시 부하는 낮아짐
- 또한 검증된 파일이 변경되거나 새로운 악성코드 DB가 업데이트 되면 추가 검증을 거쳐 지속적으로 관리

# 강력한 백신엔진 | 오탐검증 시스템

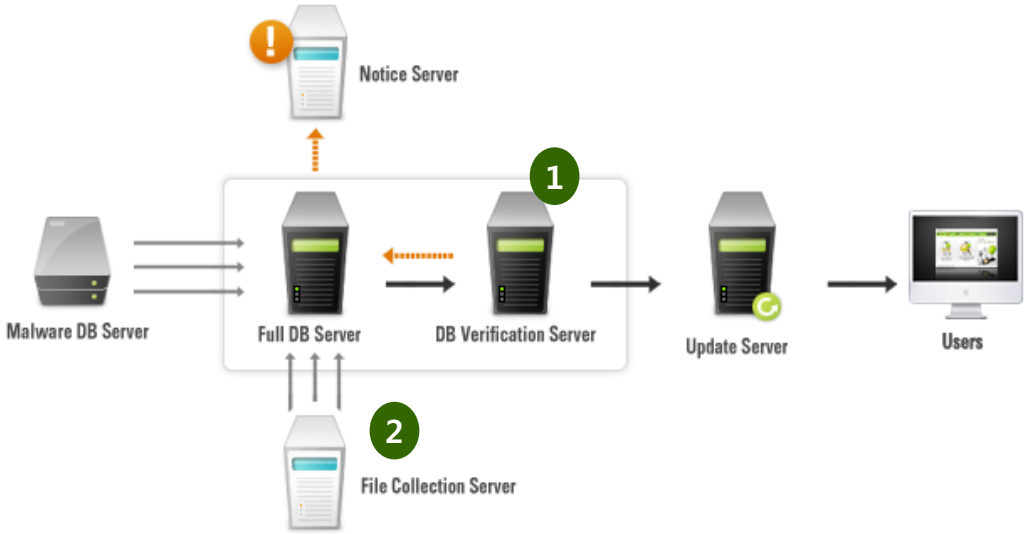
ESTsoft

## 오진으로 인한 피해는 악성코드의 피해 만큼 심각한 문제!

**ESTsoft 특허기술**

- 오탐으로 인한 업무 중단 및 사내 지원 및 문의 증가
- 부팅이나 시스템 불능 사태일 경우 업무 중요 데이터 손실
- 오탐으로 인한 복구 지원 및 비용 발생

오진의 위험을 최소화하기 위해 사용자에게 업데이트 되기 전에 OS 및 주요 보안 프로그램, 주요 범용 프로그램들의 오진 여부를 확인하는 프로세스를 거쳐 업데이트를 진행하는 검증 시스템으로 ESTsoft의 특허기술




### 1. DB 검증

- BlackList와 WhiteList 파일셋을 기반으로 알약의 오진 및 미탐지를 사전에 확인
- 오진 발생 시 SMS와 메일을 발송하며, 추가 검증된 안전한 DB를 사용자에게 제공

### 2. 파일 수집

- 각종 OS상의 다양한 보안, 범용 프로그램 등을 WhiteList로 등록
- 주기적인 모니터링을 통해 관리 하며, 업체간의 협력 프로그램인 'WhiteList 등록 프로그램'을 통해 지속적으로 DB 업데이트

# 강력한 백신엔진 | 검증받은 알약 엔진

ESTsoft

## 엄격한 국제 보안인증 테스트를 통과한 알약

**VB100 인증** Virus Bulletin


전 세계적인 악성코드 목록인 WildList에 대한 **100% 검출 및 False positive**(오탐지) **0%** 조건 충족 시 부여하는 세계 3대 국제보안인증

- 2011.10 : Windows Server 2003
- 2011.12 : Windows 7
- 2012.06 : Windows Server 2008
- 2013.08 : Windows 7
- 2013.10 : Windows Server 2008
- 2013.12 : Windows 8.1
- 2014.04 : Windows 7

**CheckMark 인증** Westcoast labs


Virus Bulletin 100% Award, ICSA와 더불어 **세계 3대 국제보안인증**으로 정보보호 제품의 효율성에 대한 품질을 테스트하여 인증

- 2011.07 : Windows 7
- 2012.08 : Windows 7
- 2013.12 : Windows 7
- 2014.01 : Windows 7
- 2014.03 : Windows 7

## 철저한 지원체계!

긴급대응 시스템

고객지원 서비스

# 철저한 지원체계 | 긴급 대응 시스템

ESTsoft

## 악성코드 종합처리센터 A-CERT (ALYac Computer Emergency Response Team)

알약의 악성코드 종합처리센터 'A-CERT (ALYac Computer Emergency Response Team)'에서
국내외 악성코드 및 보안관련 위험요소에 대한 이슈 발생 시 신속하게 대응방안을 마련하여 외부 위협에 대한 고객의 피해를 최소화

또한 국정원, KISA, 방송통신위원회 등의 유관 기관 뿐만 아니라 국내 주요 ISP 업체들과의 긴밀한 협업을 통해 악성코드에 대한 샘플수집 및
1,300만 명의 사용자로부터 사용상 발생할 수 있는 광범위한 악성코드에 대한 모니터링


**샘플 접수 후 약 2시간 에서 경우에 따라 4시간 이내 대응엔진 및 DB패턴 제작**
**(단, 전용백신을 만들거나 새로 엔진을 개발하는 경우 추가 테스트시간 소요)**

# 철저한 지원체계 | 고객지원 서비스

ESTsoft

## 체계적인 지원 프로세스로 전문 기술 인력의 고객 지원 서비스

### 고객지원 – Part I

- 신고하기/ e-mail 상담 (2시간 이내 회신)
- 전문 기술 인력이 직접 전화 상담
- 핫라인 운영(야간 및 공휴일, 주간)
- PC 원격지원 서비스
- 대규모 사이트 전담 인력 배정 및 정기 방문 점검 서비스 제공

### 고객지원 – Part II

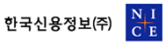
- 제품 교육 서비스 제공(요청 시)
- 악성코드 정보 제공(요청 시, 주 1회)
- 탐지 정보 분석 서비스 제공(요청 시)

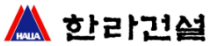

# 3. Reference

# Reference

ESTsoft

## 일반기업






외 5,000여 기업

## 공공기관


외 800여 기관

## 교육기관 및 기타


외 1,500여 기관


# 4. 회사소개

ESTsoft

회사명 : ㈜이스트소프트
대표이사 : 김장중
설립일 : 1993년 10월 2일
상장일 : 2008년 07월 01일(KOSDAQ)
자본금 : 24.7억 (2013년 기준)
매출액 : 365억 (2013년 기준)
임직원수 : 525명 (2014년 기준, 자회사 포함)
홈페이지 : http://www.estsoft.com
소재지 : 서울특별시 서초구 서초동 1464-30

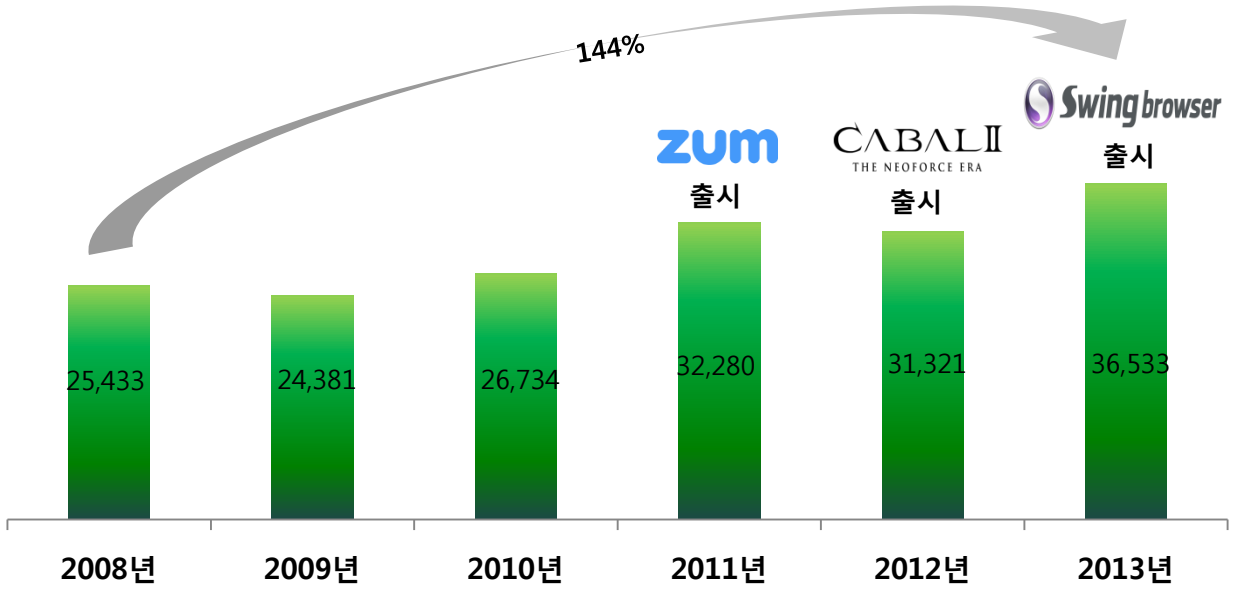



## 연도 별 매출액 및 당기순이익 추이

단위:백만원

| 구분 | 2008년 | 2009년 | 2010년 | 2011년 | 2012년 | 2013년 |
|---|---|---|---|---|---|---|
| 자본금 | 2,475 | 2,475 | 2,475 | 2,475 | 2,475 | 2,475 |
| 매출액 | 25,433 | 24,381 | 29,277 | 32,280 | 31,321 | 36,533 |
| 당기순이익 | 8,208 | 5,848 | 7,738 | 12,457 | (984) | (3,494) |

매출액 성장률 (단위:백만원)



# 회사소개 | 수상내역

ESTsoft

| | |
|---|---|
| **2014** | 제13회 대한민국 SW기업 경쟁력대상 최우수상 수상 (한국소프트웨어산업협회) |
| **2013** | 제12회 대한민국 SW기업 경쟁력대상 기업경영부문 대상수상 (한국소프트웨어산업협회)<br>알약3.0 Server 국제공통평가기준(CC)인증 획득 |
| **2012** | 알약 '2012 대한민국대표브랜드 대상' 수상 (한경닷텀, iMBC, 동아닷컴)<br>인터넷디스크 6i 행정업무용SW 선정<br>제7회 대한민국 인터넷 대상 – 방송통신위원회위원장상 (기술선도부문)<br>알약 2012 히트상품 (디지털타임스) |
| **2011** | '아시아태평양 200대 유망 중소기업' 선정 (美 포브스 誌)<br>알약, '英 체크마크 보안인증', 'VB100보안인증' 획득<br>알약, 알마인드 '2012년 세계에서 주목받을 국산 SW 선정' (한국SW전문기업협회)<br>제 9회 대한민국 SW 기업 경쟁력 대상 최우수상 (한국소프트웨어산업협회)<br>알약 안드로이드 IT 혁신상품대상 (디지털데일리) |

# 회사소개 | 수상내역

ESTsoft

**2010**

비즈하드 3.0 신소프트웨어상품 대상 (지식경제부)
SW글로벌 스타 육성기업 선정 (KOTRA)
알툴즈 통합팩 8.0, 행정업무용 소프트웨어 선정 (한국소프트웨어산업협회)

---

**2009 ~ 2008**

'제 46회 무역의 날 – 500만불 수출의 탑' 수상 (한국무역협회)
제4회 대한민국코스닥대상 '최우수마케팅기업상' 수상(코스닥협회)
'2008 아태지역 고속성장 500대기업' 선정 (딜로이트)
'2008 벤처기업대상' – 대통령 표창 수상 (벤처산업협회)
제7회 대한민국 소프트웨어 기업경쟁력 대상(한국소프트웨어산업협회)
카발온라인, '태국 게임쇼 2008' - 최우수 온라인 게임 등 3개 부문 수상

---

**2007 ~**

알툴즈 통합팩 7.0 행정업무용 소프트웨어 선정(한국소프트웨어산업협회)
카발온라인, 디지털 콘텐츠 대상 수상 – 정보통신부 (2006)
알씨 4.0, '신 소프트웨어 상품 대상' – 정보통신부 (2005)
인터넷디스크, 2004 IT 히트 상품 – 디지털 타임즈 (2004)
알툴즈, 2003년 상반기 IT 히트상품 – 디지털 타임즈 (2003)
유망중소정보통신기업 선정 - 정보통신부 (2002)
디지털이노베이션 대상 – 산업자원부 (2002)

# 회사소개 | Contact Us


알약 홈페이지 http://alyac.altools.co.kr/

ESTsoft 홈페이지 http://www.estsoft.co.kr/

고객센터 1544-9744

구매문의 02-3470-2970


# 감사합니다.