



# Virus Chaser

*Beyond Tradition*

## 통합안티바이러스솔루션

- 차세대 프로액티브 방식의  
BODAR(Behavior Oriented Detection At Run-Time)  
(행위기반 탐지/차단) 엔진 탑재
- 스스로 알아서 신/변종 악성코드의 실행을 사전에 차단
- 보안성(CC인증), 품질성(GS인증), 기술력(특허획득)을  
모두 인정받은 '바이러스체이서 8.0'

스스로 알아서 방어하는!

# 바이러스체이서 8.0

특허를 취득한 '악성 프로세스의 행위를 기반으로 한 악성코드 차단기술'이 적용된 **프로액티브(Proactive)방식의 BODAR (Behavior Oriented Detection At Run-time)** 엔진을 탑재하여 악성 프로세스의 행위를 실시간으로 지켜 “보다”라는 의미로 타사의 패턴 시그니처 기반의 엔진 “보다” 뛰어난 실시간 엔진을 탑재하여 APT(Advanced Persistent Threat) 공격에 “보다” 효과적으로 대응이 가능합니다. CC(Common Criteria)인증으로 보안성을, 특허 획득으로 기술력을, GS인증으로 품질성을 인정받은 ‘바이러스체이서 8.0’이 신/변종 악성코드의 피해로부터 사용자의 컴퓨터를 안전하게 보호할 것입니다.

## 주요기능

### 실시간 감시

악성코드가 수행될 때 자동 치료 또는 사용자가 응답 할 때까지 관련 악성코드가 동작하지 못하도록 잡아두어 어떠한 경우에도 바이러스가 실행되어 컴퓨터에 피해를 입히는 것을 방지할 수 있습니다. (실시간 감지는 1차적으로 행위기반으로 감시하고 2차적으로 패턴 시그니처 기반으로 악성 코드를 비교 합니다.)

### 행위기반 탐지/차단

악성코드 발견 시 패턴 업데이트 후 처리되던 기존 방식이 아닌 별도의 패턴 업데이트 없이 악성코드가 실행 시 행위를 감시하여 악성 행위가 발견되면 실시간으로 차단합니다.

### 간편한 환경설정

기본적인 기능을 모두 포함하면서도 설정이 반드시 필요한 최소한의 주요 기능만을 환경설정 메뉴로 채택하였고, 사용자가 설정하기 어려운 부분은 학습이 가능한 인공지능 기능으로 처리하여 사용이 간편 합니다.

### 패턴 시그니처 기반 탐지

최소의 패턴으로 매우 복잡한 악성코드를 깊고 섬세하게 검출할 수 있습니다.

### 자체보호기능

바이러스체이서와 시스템 파일의 변조를 방지하여 컴퓨터가 안전한 상태로 유지될 수 있도록 합니다.

### 빠른 검사 속도

각 O/S 또는 기업에 알맞은 검사 후 기존 파일을 재 검사 하지 않아도 정상파일로 확인하여 검사 속도를 빠르게 향상 시키며, 스캔 하기 전 불필요한 파일을 삭제 합니다.

### 중앙관리시스템(통합보안관리 솔루션)

바이러스체이서의 중앙 관리뿐만 아니라 PMS(Patch Management System) 으로 확장이 가능한 중앙 관리 도구를 제공 합니다.



**‘바이러스체이서 8.0’**은 급변하는 IT환경에 맞춰 점차 다양하고 지능적으로 변하는 여러 보안 위협에 대비하게 위해 개발된 스스로 알아서 신/변종 악성코드의 실행을 차단하는 신개념 통합안티바이러스 제품입니다.

## 주요특장점

PC에 존재하는 알려진 악성코드를 실시간 탐지하는 것은 물론 알려지지 않은 악성코드를 탐지하기 위하여 행위기반 탐지 및 차단하는 기술을 적용하여 스스로 알아서 신/변종 악성코드의 실행을 차단하는 신개념 통합안티바이러스 제품 입니다.

### **S**TRONG

#### 높은 바이러스 검출율

사전차단 프로액티브엔진과 시그니처 엔진을 통한 높은 바이러스 검출율!

### **S**IMPLE

#### 쉽고 간편한 기능

인공지능적인 처리로 사용자의 개입이 거의 필요 없는 손쉬운 사용!



### **S**MALL

#### 최저 리소스 유지

설치 전 체감속도를 그대로 느낄 수 있도록 최저의 리소스만 사용!

### **S**PEED

#### 더욱 빨라진 검사속도

표준환경에서 최적화 작업을 수행하여 검사 속도 향상!

## 도입효과

### 악성코드 침입에 대한 신속한 대응으로 바이러스 감염피해 최소화

행위기반의 악성코드 탐지기술(BODAR)로 알려지지 않은 새로운 악성코드로의 위협으로부터 컴퓨터를 안전하게 보호

### 신종/변종 악성 프로그램에 대한 실시간 대응 (Zero-day 취약점 보완)으로 2차 피해(DDos) 방지

최근 해킹의 주된 공격 기법인 RAT에 의한 DDos, Zero-day attack, ATP공격 등에 사용되는 신종 악성코드를 실시간으로 탐지하여 동작을 원천적으로 차단

### 중앙 집중적 통합 관리를 통한 엔드포인트 관리 효율성 증가

바이러스 백신(Virus Chaser), 패치관리시스템(Patch Chaser)의 모듈을 통합한 PC통합보안 솔루션 제공

## 권장사항

### | MS-Windows 계열(Windows 32bit, 64bit 모두 지원)

구분	운영체제	CPU	RAM	HDD	Network
최소사양	Windows 2000	Pentium III 400 MHz / AMD64 1.4GHz	512MB 이상	500MB 이상	10/100BaseT
권장사양	Windows XP/ Vista/ 7 / 2003 / 2008	Pentium III 1GHz / AMD64 1.4GHz	1GB 이상	1GB 이상	10/100BaseT

### | LINUX 계열

구분	운영체제	CPU	RAM	HDD	Network
최소사양	RedHat Enterprise Linux 4	Pentium III 400 MHz / AMD64 1.4GHz	512MB 이상	500MB 이상	10/100BaseT
권장사양	RedHat Enterprise Linux 6	Pentium III 1GHz / AMD64 1.4GHz	1GB 이상	1GB 이상	10/100BaseT

### | UNIX 계열

구분	운영체제	CPU	RAM	HDD	Network
최소사양	HP-UX 11.23	Intel Itanium 2	512MB 이상	500MB 이상	10/100BaseT
	HP-UX 11.11	PA-RISC			
권장사양	HP-UX 11.31	Intel Itanium 2(2CPU 이상)	1GB 이상	1GB 이상	10/100BaseT
	HP-UX 11.31	PA-RISC(2CPU 이상)			
최소사양	Solaris 8	Ultra Sparc	512MB 이상	500MB 이상	10/100BaseT
	Solaris 9	Pentium III 400 MHz / AMD64 1.4GHz			
권장사양	Solaris 10	AMD64 1.4GHz	1GB 이상	1GB 이상	10/100BaseT
		Pentium III 400 MHz / AMD64 1.4GHz(2CPU 이상)			
최소사양	AIX 5.1	Power3-II	512MB 이상	500MB 이상	10/100BaseT
권장사양	AIX 6.1	Power3-II (2CPU 이상)	1GB 이상	1GB 이상	10/100BaseT

\* Linux / Unix 계열의 경우 실시간 탐지 등 일부 기능이 제한될 수 있습니다.

## ☎ 고객지원 서비스

최고의 기술력으로 고객만족을 위해 최선을 다하겠습니다.

**고객시스템의 안전을 생각하는 보안서비스 !**

**고객의 열린 소리를 소중히 생각하는 바이러스체이서 입니다.**

고객 지원 센터 연락처 | **070-7308-1004**  
 고객 센터 | <http://www.viruschaser.com>  
 영업 및 구매 문의 | [sales@sgacorp.kr](mailto:sales@sgacorp.kr)  
 기술 문의 | [cs@sgacorp.kr](mailto:cs@sgacorp.kr)  
 바이러스 문의 | [cert@viruschaser.com](mailto:cert@viruschaser.com)



137-896 서울시 서초구 마방로2길 44 (양재동 315-1)  
 Tel\_070-7308-1004 Fax\_02-575-1807  
 URL : <http://www.viruschaser.com>  
 f : <http://www.facebook.com/viruschasercorp>  
 t : @virus\_chaser

