AhnLab

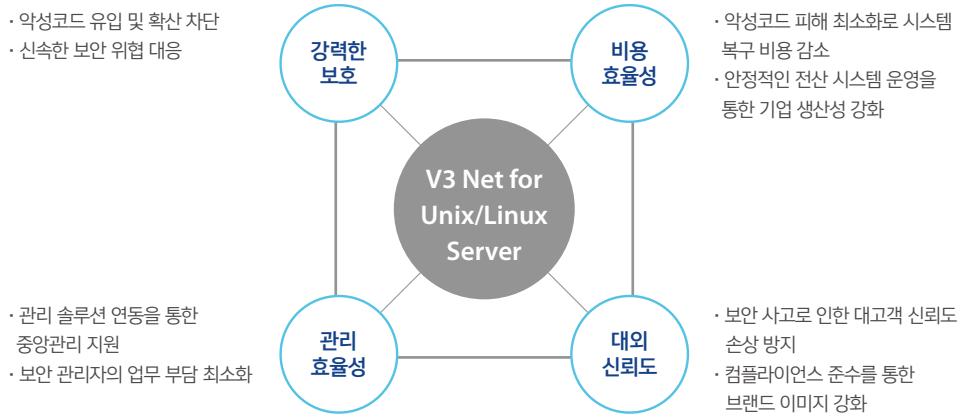
V3 Net for Unix/Linux Server

Unix 및 Linux 서버에 최적화된 보안 솔루션

Unix 및 Linux 서버의 악성코드 감염을 차단해
정보 자산을 보호하는 강력한 서버 전용 보안 솔루션

제품 개요

V3 Net for Unix/Linux Server는 갈수록 고도화되는 악성코드 위협을 원천적으로 차단하고 기업의 중요 정보 자산을 안전하게 보호하기 위한 유닉스(Unix) 및 리눅스(Linux) 서버 전용 보안 솔루션입니다.



왜 서버 보안이 중요할까?

유닉스(Unix) 또는 리눅스(Linux) 기반의 서버는 수많은 클라이언트 PC에 연결되어 다양한 데이터를 저장 및 배포하는 중요한 IT 인프라 구성 요소입니다. 최근 랜섬웨어를 비롯해 유닉스 및 리눅스 기반의 시스템을 겨냥한 악성코드가 크게 증가하면서 비즈니스 중단 등 심각한 피해를 야기하고 있습니다.

오픈소스 OS 노리는 악성코드 급증

· 리눅스 랜섬웨어/트로이목마 등 리눅스 악성코드 급증
· 신/변종 악성코드 유포

서버 노리는 공격 및 피해 증가

· 서버 겨냥한 타깃 공격 증가
· 리눅스 좀비 서버 이용한 DDoS 공격 증가
· 비즈니스 마비

체계적이고 전문적인 관리 시스템 부재

· 관리 시스템/인력 부족
· 서버 위협의 인지 및 대응의 어려움

주요 기능

AhnLab V3 Net for Unix/Linux Server는 20여 년간 축적된 안랩의 악성코드 기술과 대응 노하우를 기반으로 신속하고 정확한 진단 및 치료와 편리한 관리 기능을 제공합니다.

악성코드 대응

악성코드 검사

- Linux 서버 실시간 감시 기능 지원
- 파일 검사
- 다양한 다중 압축 파일 검사 가능
- 수동 검사: 관리자가 지정한 대상에 대해 수동 검사 수행
- 예약 검사: 관리자가 설정한 시간에 예약 검사 수행

엔진 업데이트

- 안랩의 독자적인 자체 엔진 탑재
- 자동 업데이트 / 예약 업데이트

관리 기능

서버 관리

- 포트 설정, 관리 계정 설정
- 안랩의 중앙 관리 솔루션 및 플랫폼 연동을 통한 통합 관리

로그 및 통계 관리

- 웹 기반의 관리 툴 제공
- 검사 로그 및 이벤트 로그 제공
- 설정 기간에 따른 악성코드 통계 제공

환경 설정

- 검사 예외 설정
- 감염되기 쉬운 파일에 대한 검사 설정
- 압축 파일 처리에 대한 설정
- 치료 전 파일을 검역소에 백업 가능

사용 환경

1등급 GOOD Software

구 분	V3 Net for Unix Server	V3 Net for Linux Server
운영체제	• Solaris SPARC 2.6/7/8/9/10 • Solaris 7/8/9/10 (x86) • Solaris x86 5.11 (x64) • AIX 5.2/5.3/6.x/7.2 • HP-UX 11.00/11.11/11.23/11i • HP-UX 11.31 IA (x64)	• Red Hat 9 • Red Hat Enterprise Linux 3.1 ~ 7.4 • Fedora(Core) 1 ~ 24 • CentOS 2.1 ~ 7.5 • Ubuntu 8.1 ~ 16.04 • Oracle Linux 5.1 ~ 7.3 • Debian 9.5 • SUSE Linux Enterprise Server 10 ~ 11 • openSUSE 12.1 ~ 13.2
메모리	512MB 이상	512MB 이상
HDD	500MB 이상	500MB 이상

* 상기 OS 버전의 지원여부는 일반 사항이며, 향후 발표될 모든 OS 버전의 지원을 보장하지 않습니다.
* 하위 버전을 포함한 정확한 지원OS는 별도 문의하시기 바랍니다.
* pSeries와 Itanium은 지원하지 않습니다.

AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901