AhnLab

V3 Net for Unix/Linux Server

Unix 및 Linux 서버에 최적화된 악성코드 방역 솔루션

- 안철수연구소 자체 기술력을 바탕으로 한 악성코드 진단/치료 기능
- 효율적인 수동 및 예약 검사 기능
- 사용자 편의를 극대화한 관리 솔루션 연동 기능
- 사용자의 조작 없이 자동으로 업데이트 해주는 스마트 업데이트

기업 환경에 적합하고 유연한 서버 방역 솔루션

AhnLab V3 Net for Unix/Linux Server

제품 개요

기업은 중요한 자원을 관리하고 공유하기 위해 서버를 사용하고 있습니다. 서버의 보안 취약점을 방치할 경우 악성코드 공격으로부터 서버에 저장되어 있는 중요한 자원의 파괴 및 유출 피해를 입게 됩니다. 또한 서버와 연결되어 있는 많은 클라이언트 PC들이 악성코드에 감염될 수 있습니다.

V3 Net for Unix/Linux Server는 갈수록 심각해지는 바이러스에 의한 피해를 서버 차원에서 원천적으로 차단하는 서버 방역 제품으로 Unix 및 Linux 서버 전용의 악성 코드 방역을 위한 제품입니다.

주요 특징

- Unix 및 Linux 서버에 대한 수동 검사 및 예약 검사를 통해서 바이러스에 감염된 파일이 서버에 존재하지 않도록 바이러스 방역기능을 제공합니다.
- 서버에서 클라이언트로의 바이러스 확산을 막아주며 클라이언트로부터의 바이러스 유입을 차단해 주는 강력한 방역 기능을 제공함으로써 Unix 및 Linux 서버를 효과적으로 방역할 수 있습니다.
- 전사적 악성코드 방역 정책 수립, 적용 및 모니터링을 위한 중앙 관리 솔루션(APC 4.0) 연계 기능을 제공합니다.

서버 방역 제품이 필요한 이유

- 서버는 기업에서 매우 다양한 역할을 담당하며 서버에 저장되는 데이터들은 기업 활동에 매우 중요한 부분을 차지하고 있습니다.
- 최근의 악성코드는 일부 운영체제의 취약점이나 특정한 데이터 유출을 공격 목표로 하고 있습니다.
- 악성코드에 의한 공격으로 서버에 저장되어 있는 중요한 데이터가 파괴되거나 유출될 수 있으며 해당 서버를 이용하는 최종 사용자(End-User)에게 악성코드가 다시 전파되는 등의 보안 위협이 발생할 수 있습니다.
- 중요한 업무용 데이터들이 집중되어 있는 서버는 악성코드의 공격 목표가 되기 쉬우며 다양한 보안 솔루션으로 2중 3중의 보호 장치가 필요합니다.

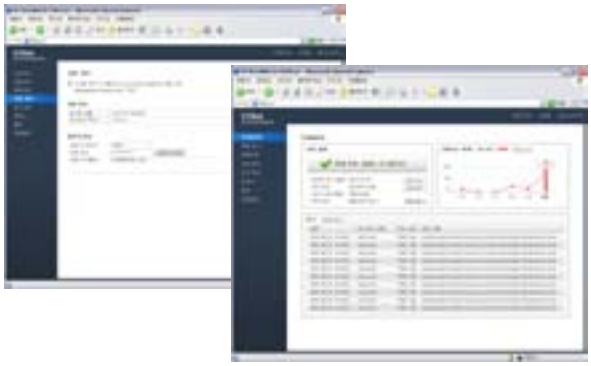
주요 기능

- 정확하고 신속한 바이러스 방역 기능
  - 독보적인 엔진으로 신속하고 정확한 바이러스 진단/치료
  - 다양한 다중 압축 파일 검사/치료 지원
- 효율적인 수동 및 예약 검사 기능
  - 파일 및 메일 박스 대상의 신속한 수동 검사 기능
  - 지정된 시간에 자동 엔진 업데이트를 할 수 있는 예약 기능
- 관리자의 편의를 고려한 효율적인 관리 기능
  - 웹 기반의 편리한 관리 툴 제공
  - 검사 예외 설정 기능으로 효율적인 방역 정책 적용
  - 바이러스 검사/치료에 대한 다양한 통계 리포트 제공
  - 검사 예외 설정 기능으로 효율적인 방역 정책 적용
  - 전사적 악성코드 방역 정책 수립, 적용 및 모니터링을 위한 중앙 관리 솔루션 연계 기능

설치 환경

구분	V3 Net for Unix Server	V3 Net for Linux Server
운영체제	Solaris SPARC 2.6/7/8/9/10 Solaris x86 7/8/9/10 AIX 5.2/5.3/6.x HP-UX 11.00/11.11/11.23/11i	Redhat 7/8/9 Fedora(Core) 1/2/3/4/5/6/7/8/9/10 CentOS 2.x/3.x/4.x/5.x Ubuntu 8.x/9.x/10.x FreeBSD 5.x/6.x/7.x/8.x
Memory	512MB 이상	512MB 이상
HDD	500MB 이상	500MB 이상

주요 화면



Ahn 안철수연구소
주소_150-869 서울시 영등포구 여의도동 12번지 CCMM 빌딩 6층 홈페이지_www.ahnlab.com 대표전화_02-2186-6000
팩스_02-2186-6100 기업 고객 핫라인_02-2186-3082