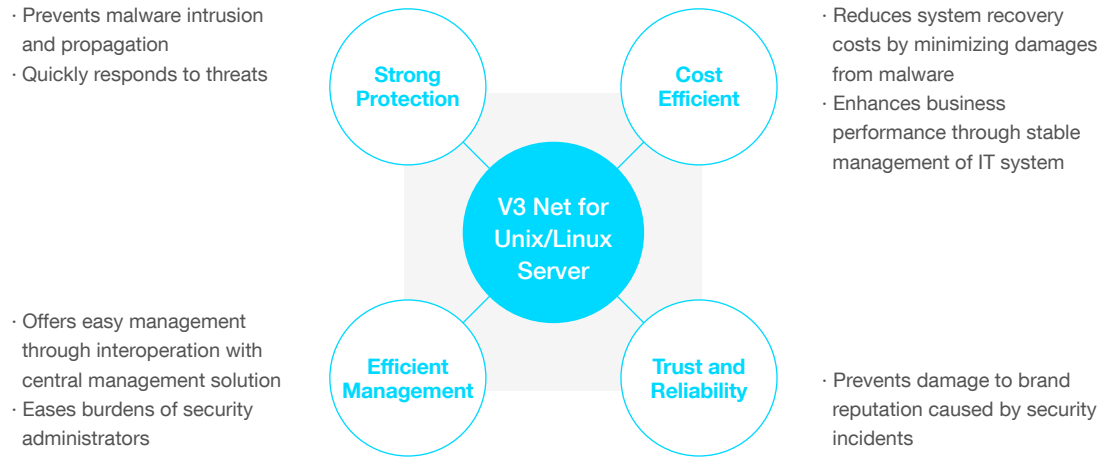
AhnLab

V3 Net for Unix/Linux Server

Optimized for Unix and Linux Server Protection

Robust anti-malware solution for Unix and Linux servers
to protect corporate information assets

AhnLab V3 Net for Unix/Linux Server provides an established anti-malware protection to prevent critical corporate data from being damaged by sophisticated threats.



Importance of Unix/Linux Systems

In numerous companies, a Unix or Linux server, which stores and distributes various data, is considered as a crucial IT infrastructure component connected to many client PCs. The recent increase in malware targeting Unix and Linux systems, including ransomware, is inflicting serious damage, such as business disruptions.

Increase in malware targeting open source OS
- Increase in Linux malware, including Linux ransomware and Linux Trojan
- Increase in new malware and variants

Increase in attacks and damages on servers
- Increase in server-targeted attacks
- Increase in DDoS attacks using Linux zombie servers
- Business disruptions caused by infected servers

Needs for structured and professional management
- Insufficient management resources and low understandings of server threats
- Difficulty in recognizing and responding to the infected servers

Key Features

AhnLab V3 Net for Unix/Linux Server provides fast and accurate malware detection and repair as well as convenient management based on over 20 years of AhnLab's accumulated technology.

Malware Scan	· Provides real-time, manual, and scheduled scan for Linux servers · Scans files including various multi-compressed files · Provides manual scanning on designated directories · Provides scanning at the specified time · Scans Docker container and NFS (Network File System) in real-time · Provides pre-scan of process and memory area · Allows features, such as real-time scan and emergency off, for enhanced server operational availability
Anti-malware Engine	· Employs AhnLab's exclusive anti-malware engine · Provides auto updates and scheduled updates

Server Management	· Manages settings of ports, accounts, and allowed IP addresses · Provides integrated management based on central management solution · Supports policy setting for scheduled scan, scan exception, update period, and update server
Log and Statistics Management	· Provides web-based management tool · Provides scan and event logs · Provides malware statistics for specified period
Policy Settings	· Able to configure scan exceptions · Able to configure scan for specific files · Able to set actions for compressed files · Backups files in quarantine before remediation

System Requirements

System Requirements for Linux and Unix

	Requirements
Memory	512MB or more
HDD	2GB or more

V3 Net for Unix Server

	Version
OS (No Real-time Scanning)	AIX 5.2/ 5.3/ 6.x/ 7.1/ 7.2 HP-UX 11.00/ 11.11/ 11.23/ 11i/ 11.31 IA(x64) Solaris SPARC 2.6/ 7/ 8/ 9/ 10/ 11, Solaris x86 7/ 8/ 9/ 10/ 11

V3 Net for Unix Server

	Version
OS (Real-time Scanning)	Amazon Linux 1~2/ CentOS 5.0~8.4/ CentOS Stream 9/ Debian 9.3~11.4/ Fedora 15~36 openSUSE 12.1~15. 4/ Oracle Linux 5.0~9.0/ ProLinux 7.5~8.5 /Red Hat Enterprise Linux 5.0~9.0 SUSE Linux Enterprise Server 11.1~15.4/ Ubuntu 11.04~22.04/ Rocky Linux 8.5~8.6
OS (No Real-time Scanning)	CentOS 3.1~4.9/ Fedora 1~14/ Red Hat Linux 9 Red Hat Enterprise Linux 3.0~4.9/ SUSE Linux Enterprise Server 10.0~11.0/ Ubuntu 8.04~10.10

* In general, the above OS versions are supported, but proper functioning is not guaranteed on all later operating system versions.
* For HP-UX using Itanium CPU, Aries should be installed.

AhnLab, Inc.
220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea
www.ahnlab.com / global.sales@ahnlab.com

AhnLab