AhnLab

V3 Net for Unix/Linux Server

More security,
More freedom

기업 환경에 적합하고 유연한 서버 방역 솔루션

표준제안서

AhnLab

CONTENTS

AhnLab

01
제안 배경

1. Linux 악성코드의 급격한 증가
2. Linux 서버를 노리는 랜섬웨어 증가
3. 주요 공격 타깃이 된 서버
4. 서버 방역의 중요성
5. 정보처리시스템의 개인정보 안정성 확보 조치 권고

Linux 악성코드의 급격한 증가

2014년 이후 꾸준히 증가하고 있던 Linux/Unix 악성코드가 최근 급격하게 증가하고 있습니다.
특히 지난 2018년 안랩에 보고된 Linux 악성코드는 전년 대비 약 290% 증가하였습니다.

- **최근 시스템의 정보를 탈취하기 위한 공격이 늘어나고 있으며, 금전적인 목적의 공격도 전문화되는 추세**
- 리눅스 악성코드는 크게 취약점을 공격하는 익스플로잇(Exploit), DDoS 공격 유형과 사용자 정보를 탈취하는 백도어 유형이 주를 이루고 있음
- 최근에는 가상화폐 채굴형 악성코드인 코인 마이너(Coin Miner)류가 점차 증가하고 있는 추세

Linux/Unix 악성코드

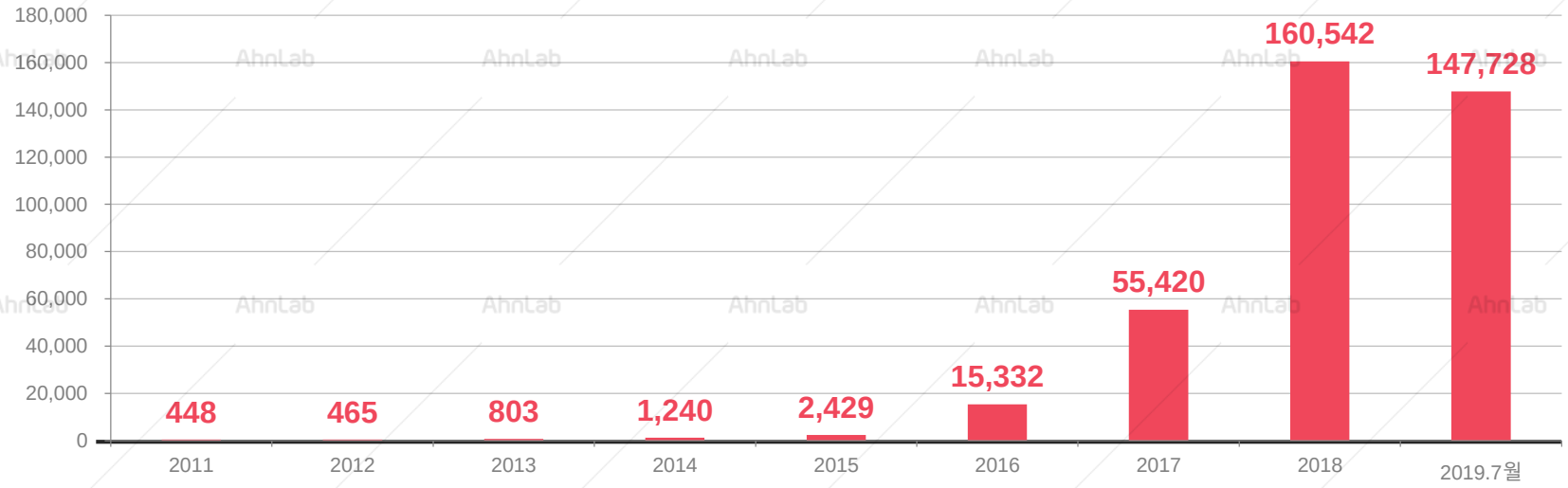
2014년 이후 꾸준한 증가 추세

- ✓ 2016년 전년 대비 약 **631**% 증가
- ✓ 2017년 전년 대비 약 **361**% 증가
- ✓ 2018년 전년 대비 약 **290**% 증가

(2019.7월 기준)

New Malware

(단위 : 건)



2011~2019.07 안랩에 접수된 Linux 악성코드 증가 추이 (*출처: ASEC)

© AhnLab, Inc. All rights reserved.

Linux 서버를 노리는 랜섬웨어 증가

Linux 악성코드 증가와 함께 Linux 서버를 노리는 랜섬웨어도 나타나고 있습니다.
지난 2017년, 국내 호스팅 업체의 Linux 서버 랜섬웨어 감염으로 막대한 피해가 발생한 바 있습니다.

경제신문 디지털타임스 2017.11.30

취약점·해킹 급증…
리눅스 보안 위협 커졌다

데일리시큐 2017.06.15

랜섬웨어 공격자들, 이미 지난해부터
한국 호스팅 업체 공격해 돈 맛 봤다

ZDNet Korea 2017.06.11

웹 호스팅 업체, 랜섬웨어 감염…
일부 사이트 장애

etnews.com 2017.11.06

제2의 인터넷나야나 사태? 코리아IDC
서버 랜섬웨어 걸려

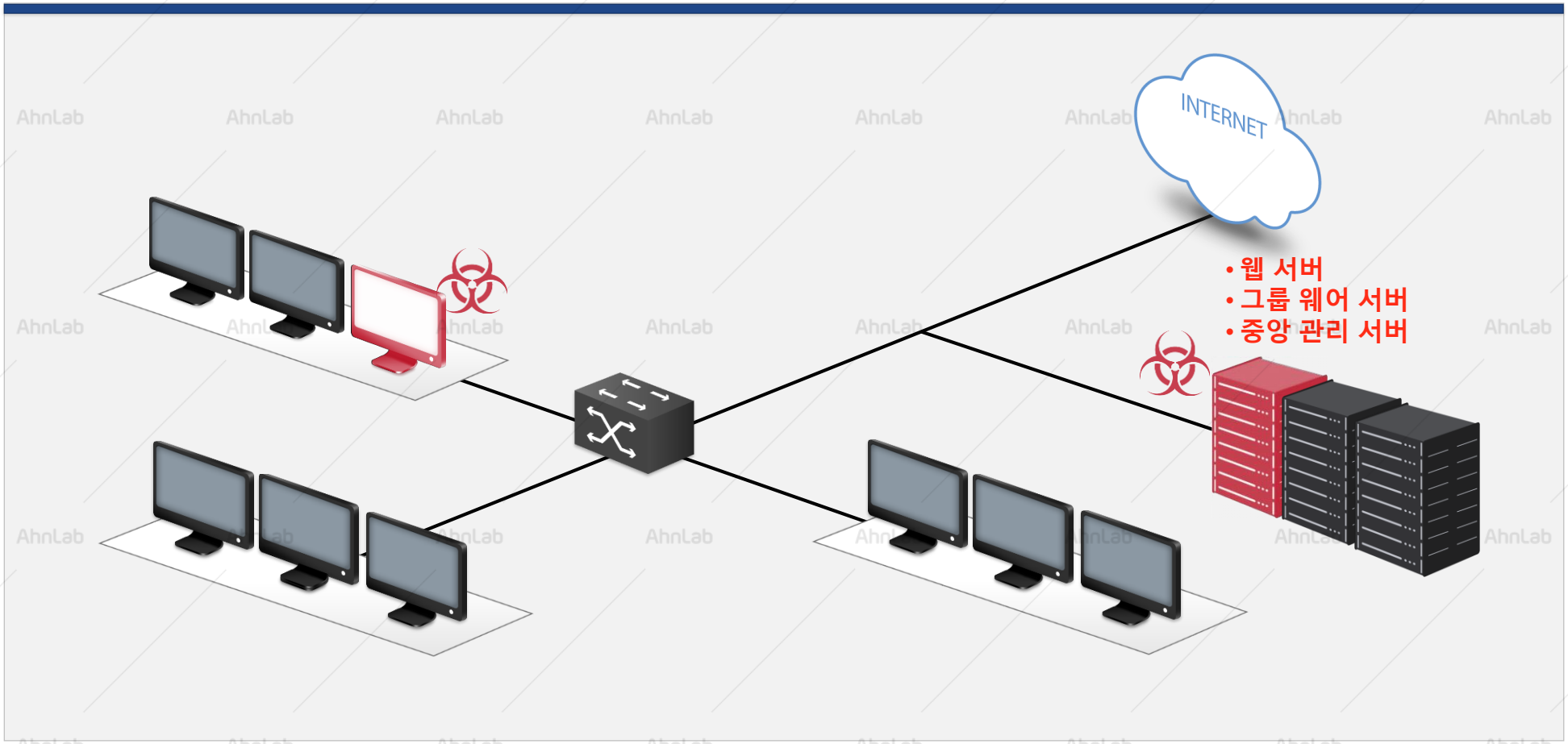
AhnLab © AhnLab, Inc. All rights reserved.

주요 공격 타깃이 된 서버

중요한 업무용 데이터들이 집중되어 있는 서버는 공격자의 주요 타깃임에도 불구하고 보안 대책은 미비한 경우가 많습니다.

- 상대적으로 보안이 취약한 서버에 대한 공격 증가
- DB 서버, 웹 서버 등이 내부망 장악의 경로로 이용

- 2017년 6월 국내 호스팅 업체 리눅스 서버 153대 Erebus 랜섬웨어 감염
- 2017 년 11월 코리아 IDC 서버호스팅 업체 리눅스 서버 감염



© AhnLab, Inc. All rights reserved.

서버 방역의 중요성

기업의 서버가 감염될 경우 전사적인 피해가 야기될 수 있습니다.
서버의 보안 취약점을 방치할 경우 서버에 저장돼 있는 데이터의 파괴와 유출로 연쇄 사이버 위협이 발생할 수 있습니다.

- 네트워크와 연결된 내부망 PC로 급속한 피해 확산, 비즈니스 중단
- 서버 감염으로 인한 정보 유출

서버가 악성코드에 감염되었을 경우의 피해는 클라이언트 PC와 같을 수 없습니다.

서버, 중요 포인트

- 중요한 정보의 관리와 공유를 위해 파일 서버 사용
- 파일 서버는 기업의 정보가 모이고 흩어지는 중요한 포인트에 위치

안전성 중요

- 수많은 PC가 네트워크에 유입/유출되는 상황
- 서버에 접속하는 모든 클라이언트 PC가 안전하다고 판단하기 어려움

기업 생산성에도 직결

- 서버 대책은 기업의 생산성과 직결
- 피해 야기 시 기업의 자산을 효율적으로 보호/서비스 연속성을 보장하기 어려움

© AhnLab, Inc. All rights reserved.

정보처리시스템의 개인정보 안정성 확보 조치 권고

개인정보의 안전성 확보조치 기준(행정자치부고시 제2014-7호)

제8조(악성프로그램 등 방지)

개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

개인정보의 안전성 확보조치 기준 해설서 참고

- ✓ 개인정보처리자는 악성프로그램 등을 통해 개인정보가 위·변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치·운영하여야 한다.
- ✓ 백신 소프트웨어 등의 보안 프로그램은 실시간 검사 등을 위해 항상 실행된 상태를 유지해야 한다.
- ✓ 백신 소프트웨어 등 보안 프로그램은 자동 업데이트 기능을 사용하거나 일 1회 이상 주기적으로 업데이트를 실시하여 최신의 상태로 유지해야 한다.

© AhnLab, Inc. All rights reserved.

02
V3 Net for Unix/Linux

1. V3 Net for Unix/Linux Server 개요
2. 주요 기능
3. 상세 기능
4. 기능 비교
5. 시스템 요구 사항
6. 특장점
7. 도입효과

AhnLab

V3 Net for Unix/Linux Server

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

AhnLab V3 Net for Unix/Linux Server

기업 환경에 적합하고 유연한 서버 방역 솔루션

정확하고 신속한 서버 방역

- 실시간 검사 기능을 통한 모니터링
- 독보적인 엔진으로 신속하고 정확한 바이러스 진단/치료
- 다양한 다중 압축 파일 검사/치료 지원

서버 활용성 극대화를 위한 다양한 기능 제공

- 효율적인 수동 및 예약 검사 기능
- 지정된 시간에 자동 엔진 업데이트를 할 수 있는 예약 기능

관리자 편의를 고려한 효율적인 관리 기능

- EMS(APC) 및 차세대 플랫폼 AhnLab EPP를 통한 통합 관리 지원
- 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 중앙관리 솔루션 연계 기능

© AhnLab, Inc. All rights reserved.

주요 기능

악성코드 대응

악성코드검사	실시간 검사
	파일 검사(모든 파일)
	예약 검사
엔진 업데이트	자동 업데이트
	예약 업데이트
환경설정	모든 파일 검사
	감염되기 쉬운 파일 검사
	압축 파일 검사
	치료 방법 선택
	치료 전 검역소로 보내기

관리자 편의 기능

서버 관리	서버 관리 포트
	호스트 이름
	관리자 정보
로그 관리	검사 로그
	이벤트 로그
검역소	신고하기
	복원하기
통계	월별 통계
	기간별 통계
기타	도움말

AhnLab © AhnLab, Inc. All rights reserved.

상세 기능

서버 보안 (Anti-Malware)	• 실시간 검사(사용 On/Off, 실시간 검사 종료 후 자동 재시작) • 수동(정밀) 검사(검사 대상 설정) • 예약 검사 (예약 검사 목록, 예약검사 추가/수정/삭제, CPU점유율 설정) • DNA 스캔(Scan) 지원 • 압축 파일 검사
업데이트 & 패치	• 최신 업데이트 파일 및 패치 파일 존재 여부 확인 • 스마트 업데이트를 이용한 자동 업데이트 및 패치 제공 • 지정 시간에 수행하는 예약 업데이트(업데이트 주기 설정) • 업데이트 서버 설정(인터넷을 통한 업데이트/사용자 정의 서버를 통한 업데이트/로컬 디렉터리를 통한 업데이트) • 기타 설정(업데이트 시 제품 패치하기/업데이트 정보 보기/무결성 검사하기) • Stable 엔진 지원
서버 관리	• 접속 허용 IP 설정 • 서버 관리 포트 설정(서버 접속 시 사용되는 TCP 포트 설정) : 호스트 이름 설정, 관리자 정보(ID/PW)
검사 환경 설정	• 치료 방법 설정 : 악성코드 감염 파일 치료/그대로 두기 설정, 감염 된 압축 파일 치료/그대로 두기 설정 : 자동 치료 : 치료 또는 삭제 전 감염 된 파일을 검역소로 보내기 • 검사 대상 설정 : 모든 파일 검사, 감염되기 쉬운 파일 검사(실행 파일/매크로 파일/스크립트 파일), 추가 검사 확장자 : 압축 파일 검사
로그 관리/검역소	• 검사/이벤트 로그 • 검역소 목록 확인, 검역소 파일 복원
통계	• 월별/기간별 악성코드 발견 통계
중앙관리	• One Agent 방식의 통합 관리솔루션 연동 • 웹 기반의 관리 툴

© AhnLab, Inc. All rights reserved.

기능 비교

제품명	V3 Net for Unix/Linux Server	E사 for Linux/Unix	H사 Unix/Linux Server	K사 Anti-Virus for Linux Server	S사 Endpoint Protection for Linux
실시간 검사	O	X	X	○	○
수동 검사	O	○	○	○	○
예약 검사	O	○	○	○	○
자동/예약 업데이트	O	○	○	○	○
감염되기 쉬운 파일 검사	O	X	X	○	○
압축파일 검사	O	○	○	○	○
치료 방법 선택	O	○	○	○	○
검사/이벤트 로그	O	○	○	○	○
검역소	O	○	○	○	○
월/기간별 통계	O	○	○	○	○
자체 엔진	O	X	X	○	○
웹 콘솔	O	○	○	○	X
쉘 지원	O	○	○	○	○
일자별(Stable) 엔진 제공	O	X	X	X	X

© AhnLab, Inc. All rights reserved.

시스템 요구 사항

서버 권장 사양(Linux, Unix 공통)

구분	권장 사양
메모리	512MB 이상
HDD	500MB 이상의 여유 공간

V3 Net for Linux Server 지원 운영체제

구분	상세 버전
실시간 검사 지원 운영체제	CentOS 5.0 ~ 8.0 / Debian 9.5 ~ 10.1 / Fedora 15 ~ 29 / openSUSE 12.1 ~ 15.0 Oracle Linux 5.0 ~ 7.6 / ProLinux 7.5 / Red Hat Enterprise Linux 5.0 ~ 8.0 SUSE Linux Enterprise Server 10 ~ 15.1 / Ubuntu 11.04 ~ 19.04
실시간 검사 미지원 운영체제	CentOS 3.1 ~ 4.9 / Fedora 1 ~ 14 / Red Hat Linux 9 Red Hat Enterprise Linux 3.0 ~ 4.9 / Ubuntu 8.04 ~ 10.10

V3 Net for Unix Server 지원 운영체제

구분	상세 버전
운영체제 (실시간 검사 미지원)	AIX 5.2/5.3/6.x/7.2 HP-UX 11.00/11.11/11.23/11i, HP-UX 11.31 IA (x64) Solaris SPARC 2.6/7/8/9/10/11, Solaris x86 7/8/9/10/11

- 상기 OS 버전의 지원여부는 일반사항이며, 향후 발표될 모든 OS 버전의 지원을 보장하지 않습니다.
- pSeries와 Itanium은 지원하지 않습니다.

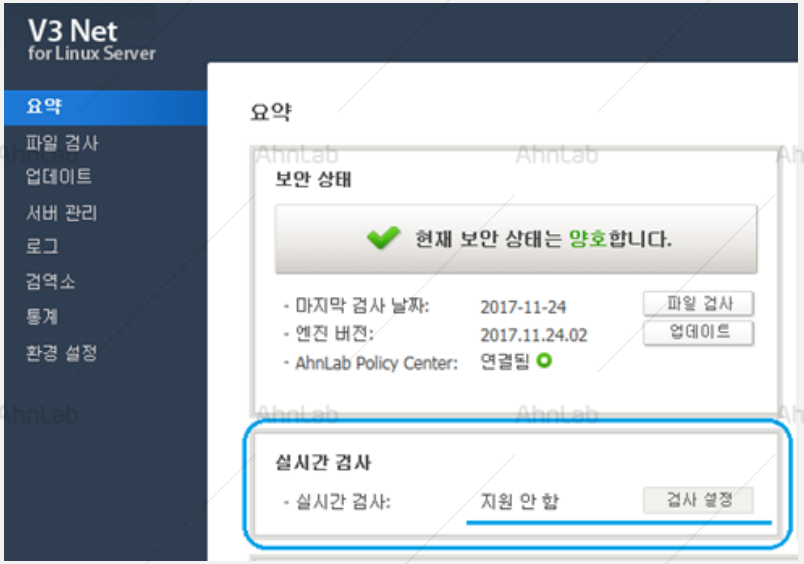
AhnLab © AhnLab, Inc. All rights reserved.

특장점1_실시간 검사 지원여부 확인

V3 Net for Unix/Linux Server 제품 설치 시, 실시간 검사 지원이 가능한 OS 여부와 커널 버전 등을 자동으로 확인하며,
지원 가능 여부에 따라 웹 콘솔에 관련 정보를 표시합니다.

실시간 검사 지원 OS

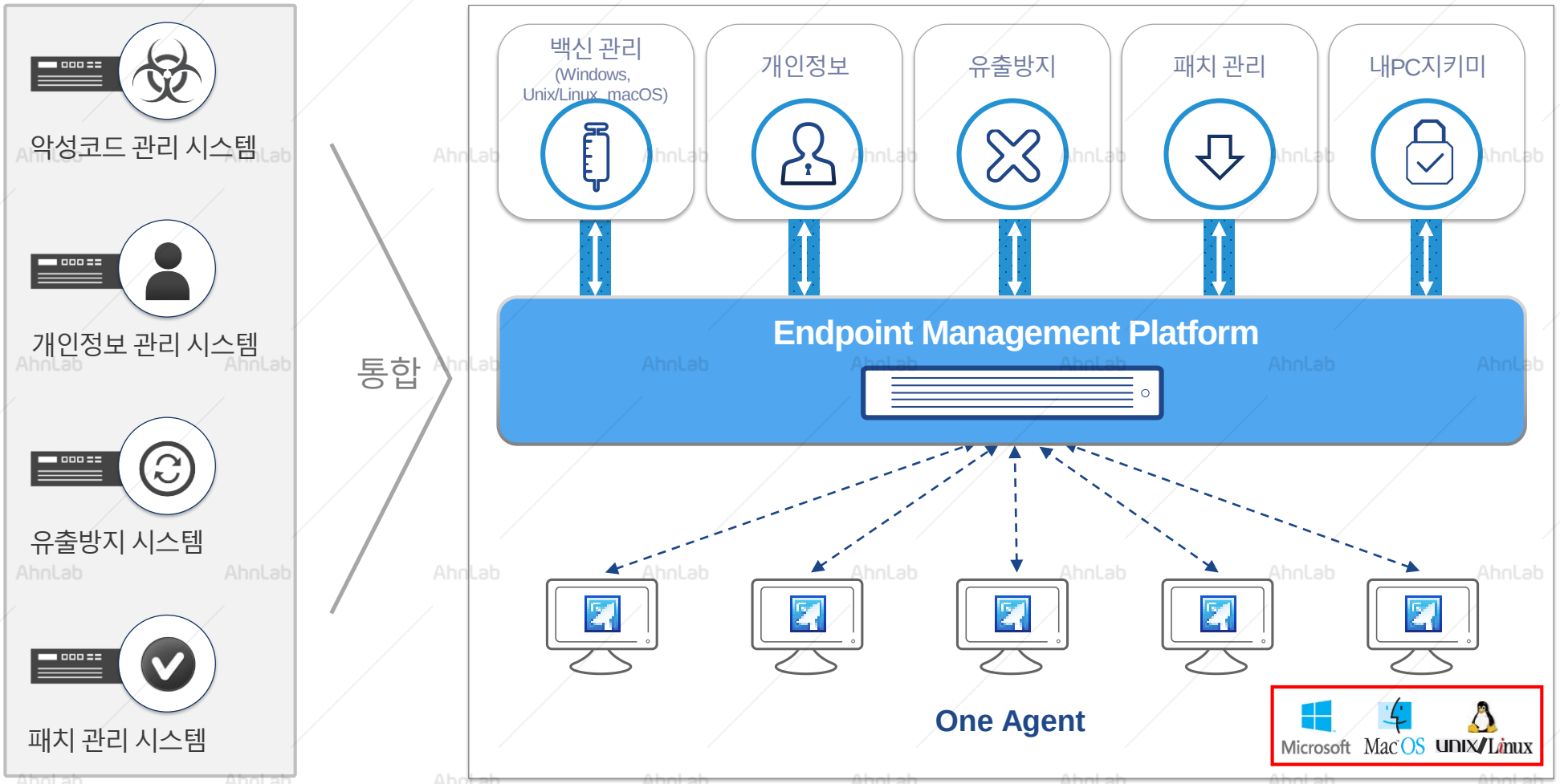
실시간 검사 미지원 OS



© AhnLab, Inc. All rights reserved.

특장점2_ 통합 관리

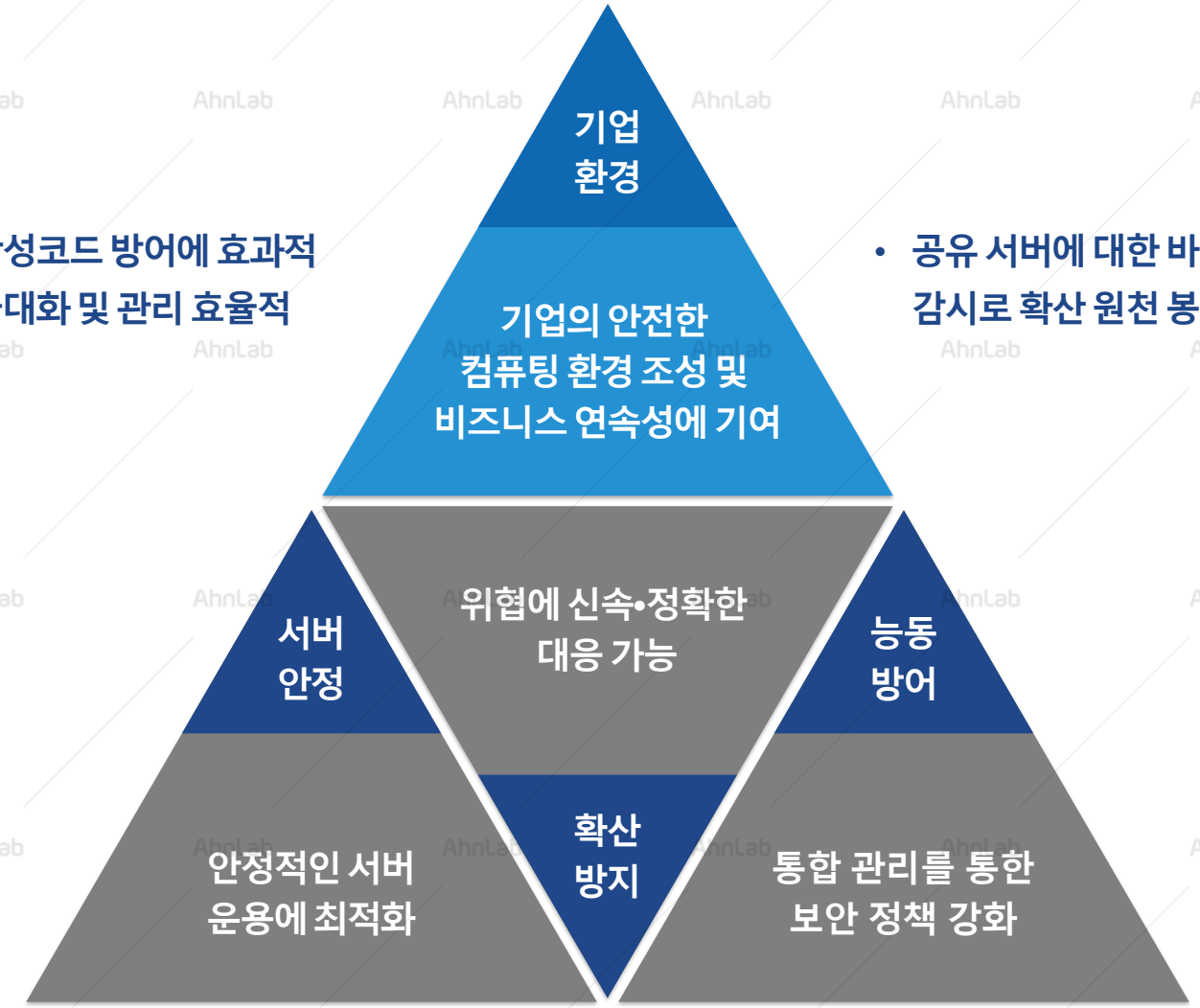
V3 Net for Unix/Linux Server는 중앙관리 솔루션과 연동되어 탁월한 관리 편의성을 제공합니다.
엔드포인트 중앙관리 솔루션 AhnLab EMS 및 AhnLab Policy Center(APC) 와의 연동을 통해 백신관리(V3), 패치관리(AhnLab Patch Management), 개인정보보호(AhnLab Privacy Management)를 하나의 에이전트, 하나의 플랫폼으로 통합 운영 및 관리할 수 있습니다.



© AhnLab, Inc. All rights reserved.

도입효과

- 서버 타깃의 악성코드 방어에 효과적
- 서버 활용성 극대화 및 관리 효율적



- 공유 서버에 대한 바이러스 감염 여부 감시로 확산 원천 봉쇄

- 체계적이고 능동적인 대응 체계 구축

© AhnLab, Inc. All rights reserved.

별첨

1. 왜 서버 보안도 안랩인가?
2. 안랩 전문 고객 지원 프로세스

왜 서버 보안도 안랩인가?

※ 별첨

- **안랩의 차별화된 전문 지원 서비스**
- **24시간, 365일 깨어 있는 ASEC 대응센터**

AhnLab

오랜 기간 쌓아온 악성코드 분석 능력과 대응 경험을 통해
안전한 컴퓨팅 환경 조성과 함께 기업 비즈니스 연속성에 기여합니다.

안랩은 20여 년간 악성코드를 분석하고 연구해온 전문 기업입니다.

안랩은 지난 1988년부터 악성코드와 바이러스 등에 대한 연구를 시작, 25년여 간 노하우를 축적해왔습니다.
국내 최대 규모의 샘플 DB를 보유하고 있으며 독자적인 기술을 마련해놓고 있습니다.

안랩은 다양한 분야의 기업 고객에게 위협 대응 방안을 제공하고 있습니다.

1995년 회사가 설립된 이후 다양한 레퍼런스를 통해 경험을 쌓았습니다.
다양한 기업 환경에서 발생하는 위협을 정확하게 진단해내고 있으며 적절한 대응 방안을 제시하고 있습니다.

안랩은 24시간, 365일 철저한 대응 체계를 가동 중입니다.

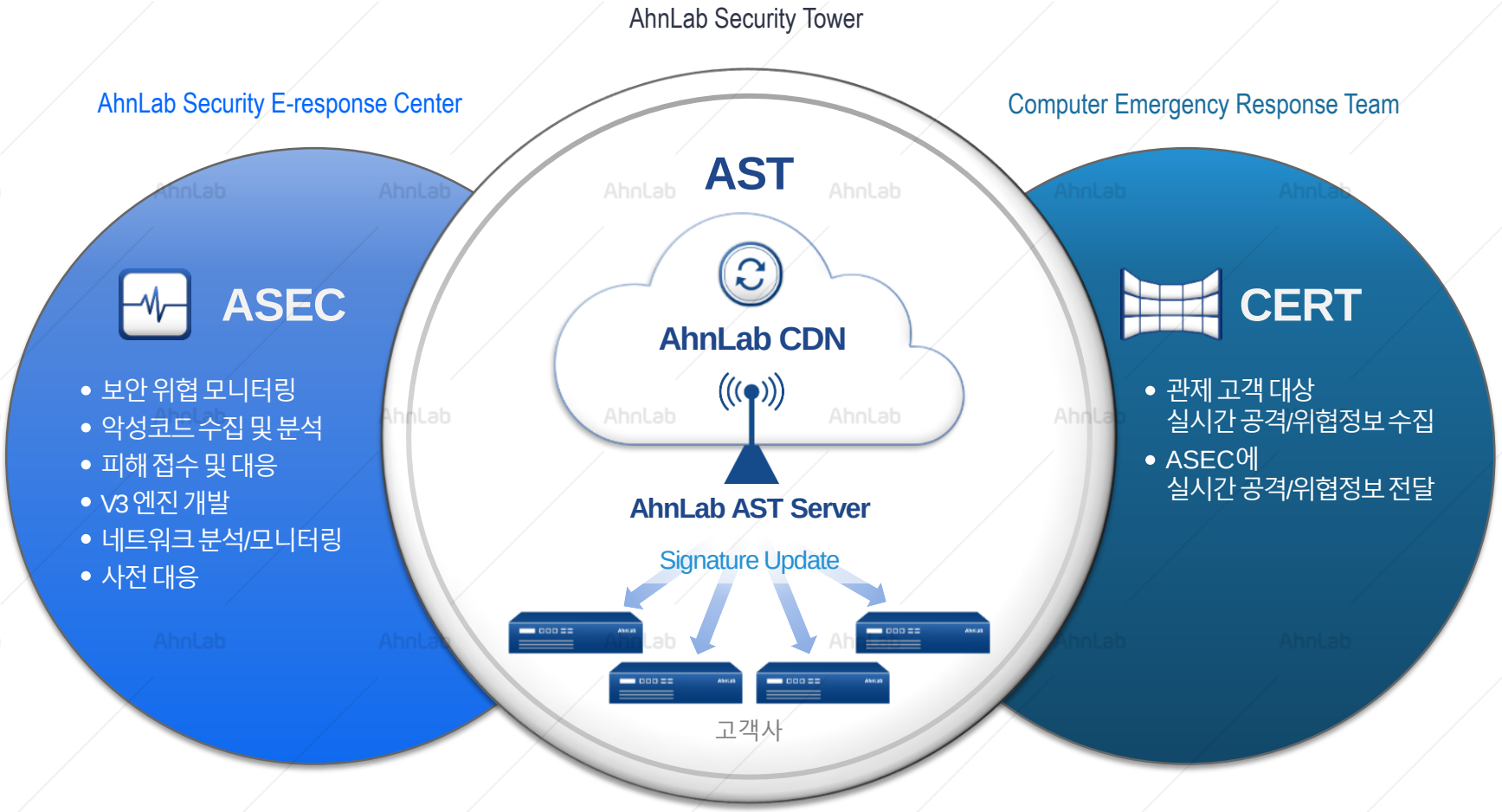
24시간 × 365일 ASEC 대응센터의 전문 인력이 위협을 모니터링하며 대응하고 있습니다.
일일 정기 업데이트 및 긴급 업데이트를 수행함으로써 발 빠르게 악성코드에 대처합니다.

© AhnLab, Inc. All rights reserved.

안랩 전문 고객 지원 프로세스

※ 별첨

보안에 대한 오랜 노하우와 경험을 토대로, 체계적이며 전문적인 지원 서비스 제공을 약속합니다.



© AhnLab, Inc. All rights reserved.

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

© AhnLab, Inc. All rights reserved.

AhnLab
V3 Net for Unix/Linux Server

AhnLab