AhnLab TrusGuard

차세대 네트워크 보안 플랫폼

표준제안서

AhnLab

Contents

AhnLab

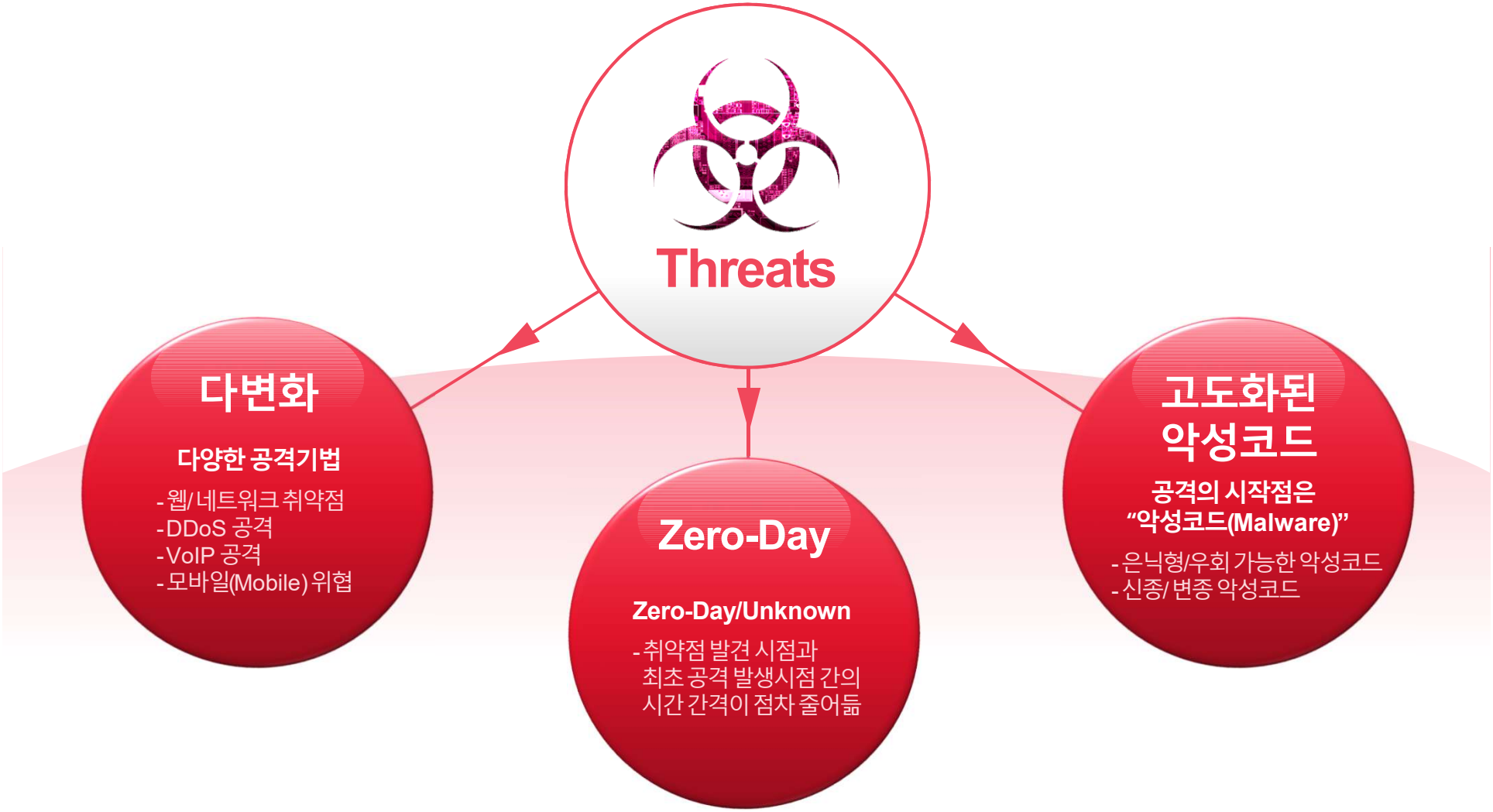
01
배경

최신 보안 위협 동향

AhnLab

보안 위협 동향(1)

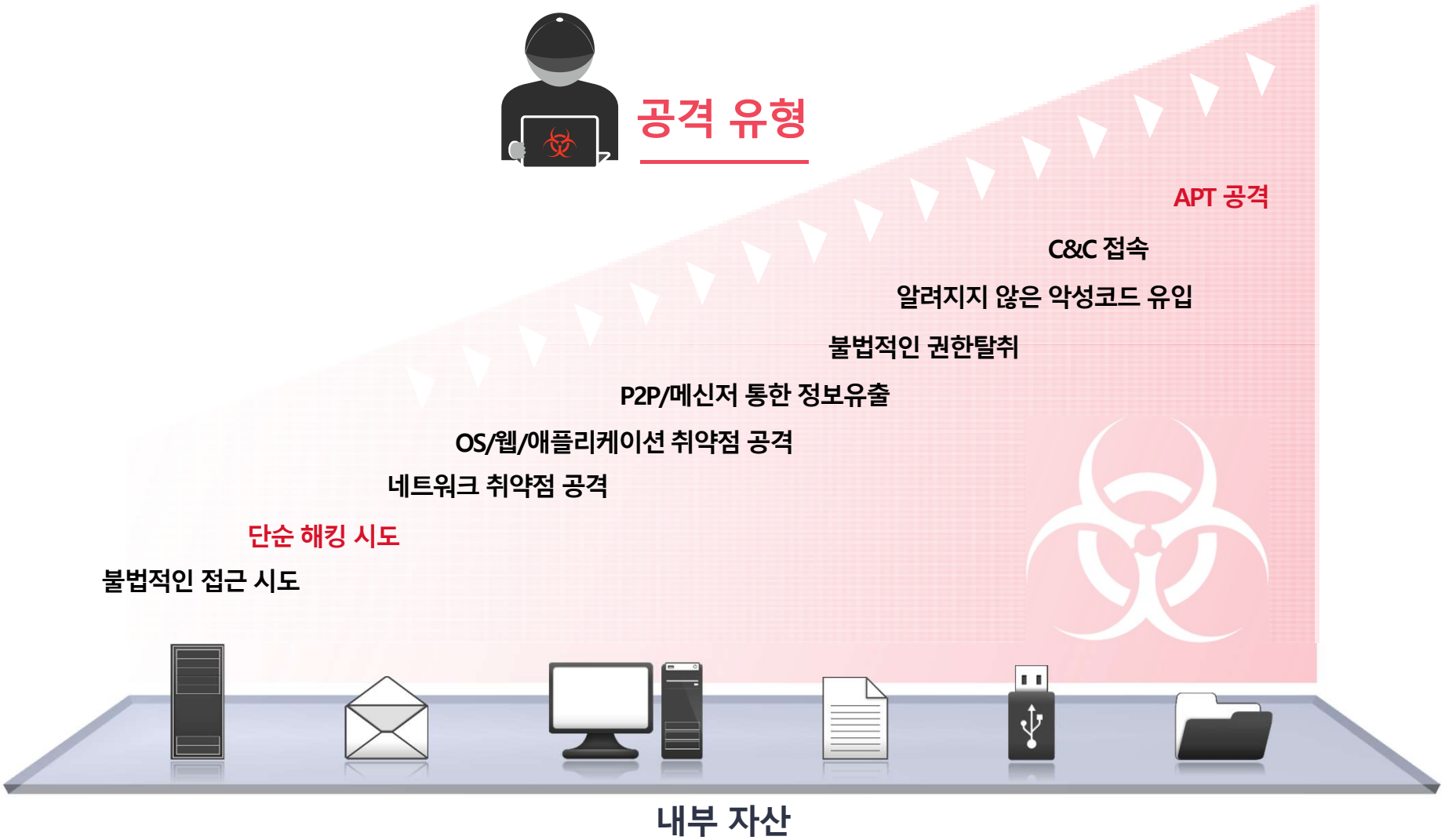
최근 보안 위협의 키워드는 **'다변화', 'Zero-day', '고도화된 악성코드'**입니다.



© AhnLab, Inc. All rights reserved.

보안 위협 동향(2)

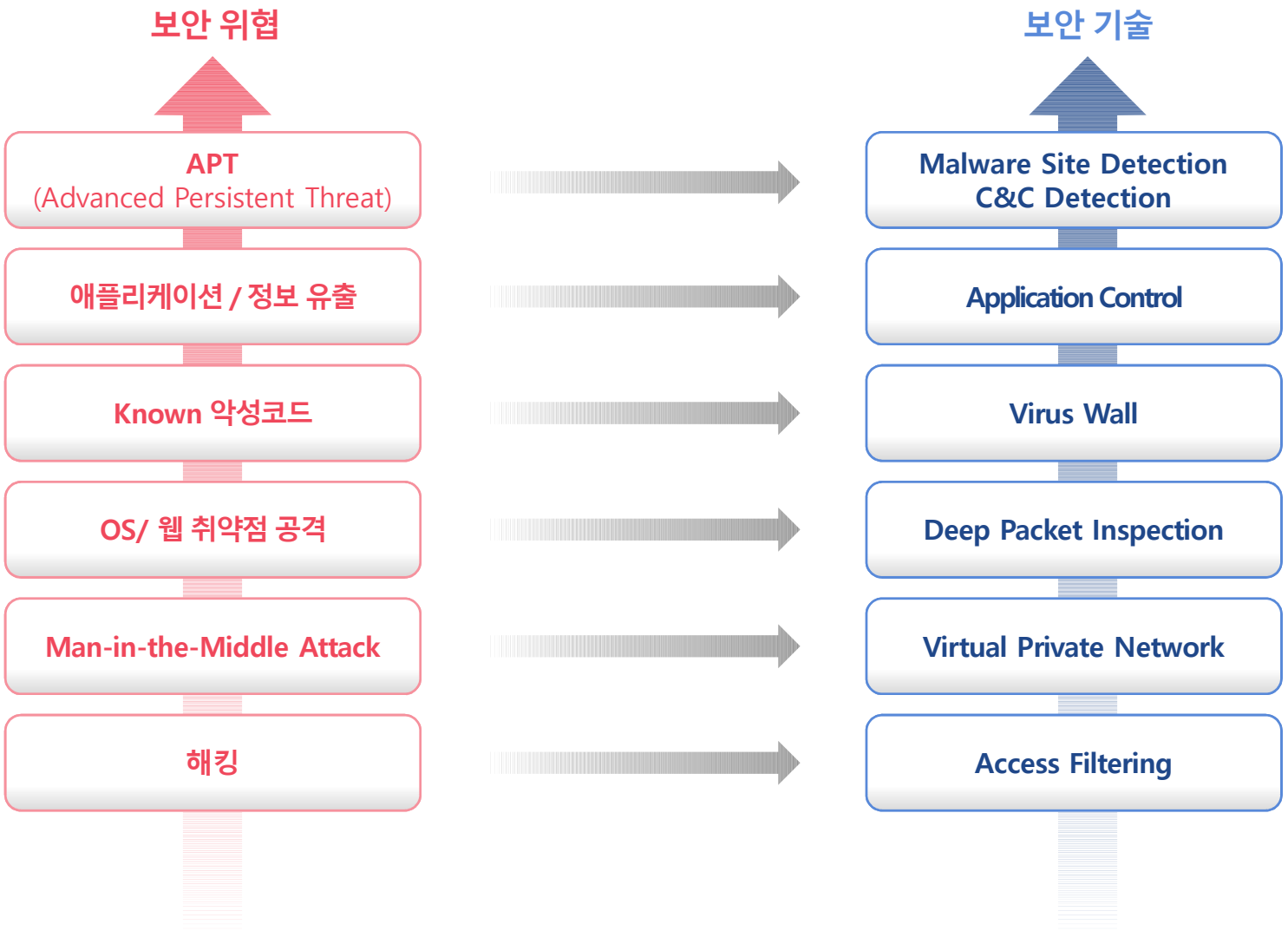
사이버 공격은 단순 해킹부터 타깃화된 APT(Advanced Persistent Threat) 까지 **광범위한 형태로 진행**되고 있습니다.



© AhnLab, Inc. All rights reserved.

보안 기술 동향

보안 위협이 나날이 정교해짐에 따라 이에 대응하기 위한 **보안 기술 또한 고도화**되고 있습니다.



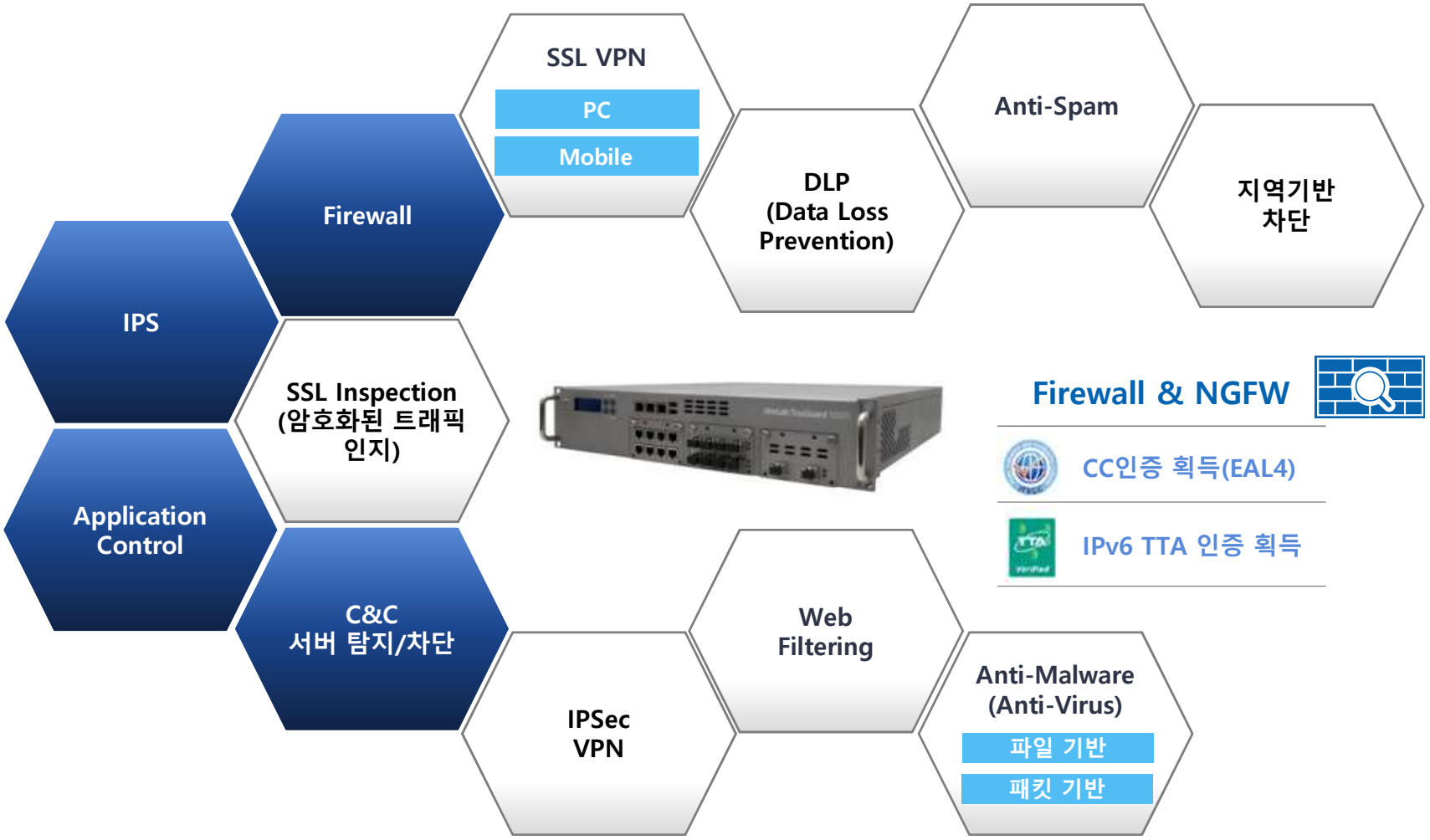
© AhnLab, Inc. All rights reserved.

02
특장점 및 차별점

AhnLab

차세대 방화벽 AhnLab TrusGuard

AhnLab TrusGuard는 '방화벽/ VPN 기반의 고성능 네트워크 보안'과 '강력한 보안 위협 대응 기술력'이 결합된
"차세대 네트워크 통합 보안 시스템" 입니다.

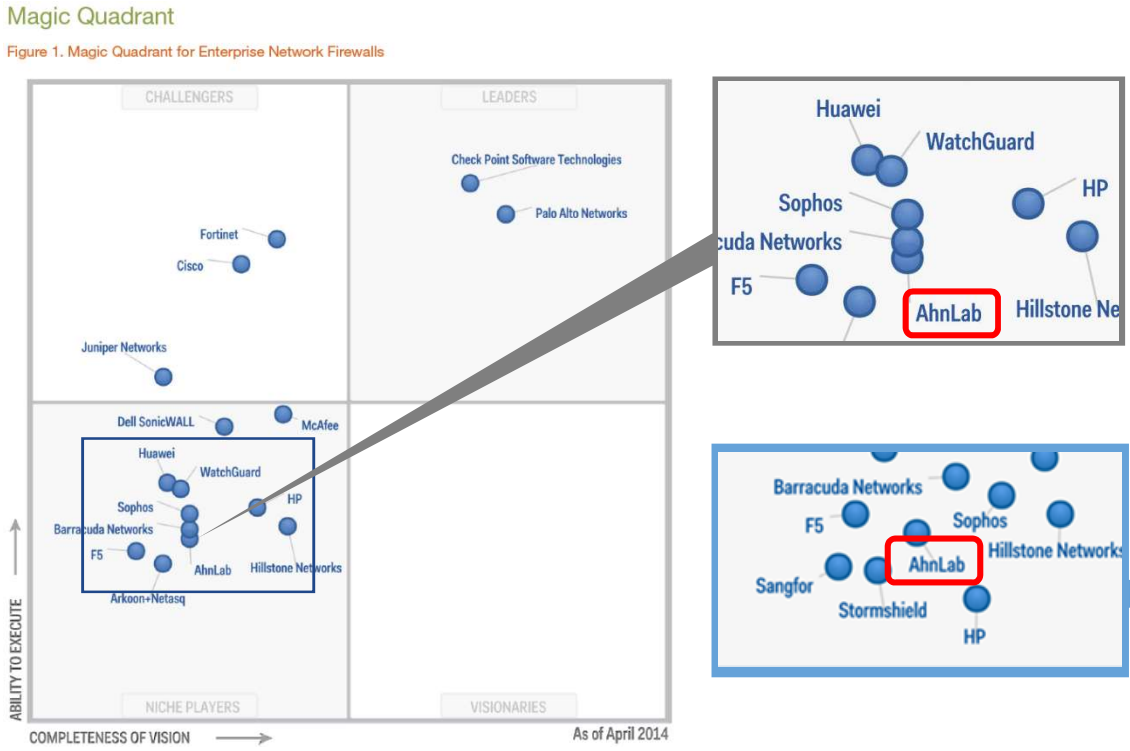


© AhnLab, Inc. All rights reserved.

차세대 방화벽 AhnLab TrusGuard

국내외에서 성능과 기술력을 인정받은 TrusGuard는 가트너(Gartner)가 선정한 '**매직쿼드런트 엔터프라이즈 네트워크 방화벽** 부문'에 등재되었습니다. (2014. 04 / 2015.05)

'14년



'15년

* **매직쿼드런트(Magic Quadrant)**

매직쿼드런트란 글로벌 시장조사 기관인 가트너(Gartner)가 전 세계 IT 기업의 역량과 제품을 기준으로 평가해 시장 부문별로 경쟁력 있는 제품 및 기업을 선정하는 것으로, IT 제품의 기술 및 성능 지표로 인정받고 있습니다.

© AhnLab, Inc. All rights reserved.

차세대 보안 제품 정의

차세대 방화벽 (Next Generation Firewall) 정의 (가트너)

전통적인
방화벽 기능

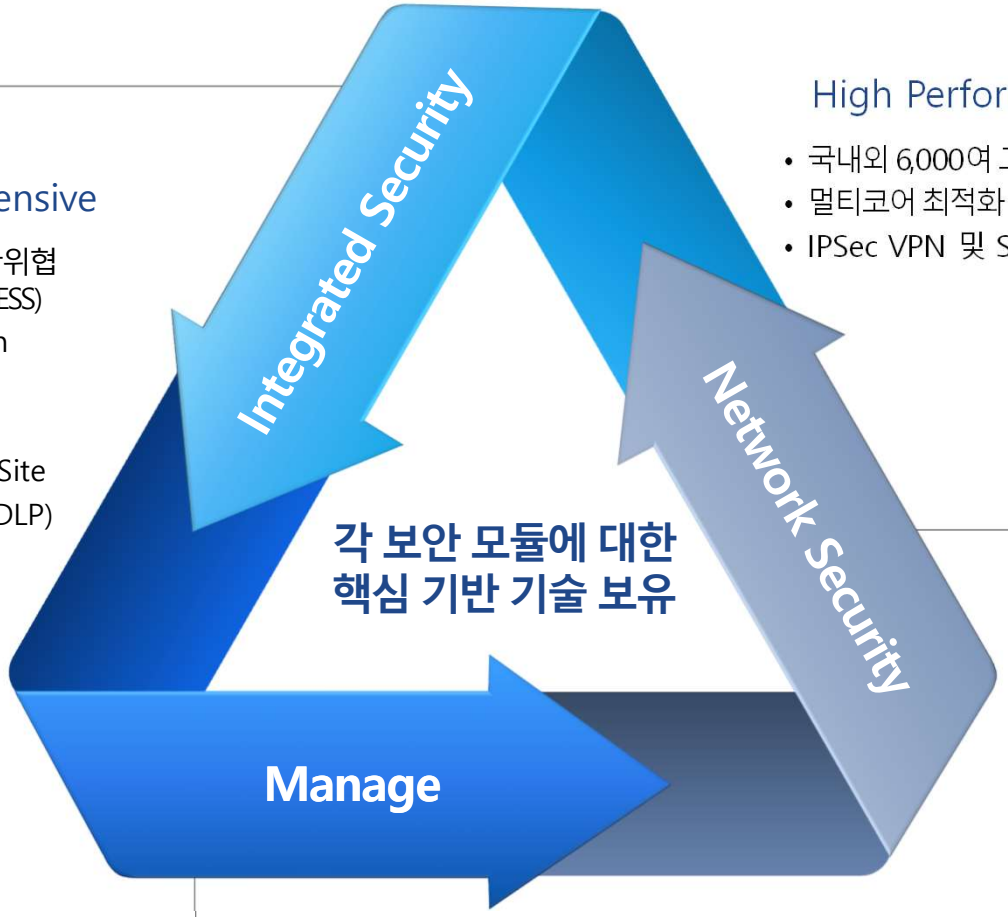
+

- 애플리케이션 인식 및 풀스펙트럼 형태의 가시성
- 네트워크 기반 침입방지시스템(IPS) 기능 통합
- 추가적인 방화벽 기능을 위한 글로벌 위협 정보 반영

© AhnLab, Inc. All rights reserved.

기대 효과

TrusGuard는 고성능•고품질의 **네트워크 보안(Network Security) 기술**과 능동적•종합적인 **통합 보안 기술**의 유기적 결합을 통한 시너지 효과를 제공합니다.



Proactive & Comprehensive

- 국내 최대 클라우드 기반 보안위협 모니터링 및 대응 시스템(ACCESS)
- 강력한 Intrusion Prevention
- Application Control
- C&C 탐지 및 차단
- 자체 DB/ 엔진기반 Anti-MalSite
- 파일제어 및 콘텐츠 제어(DLP)

High Performance & Flexibility

- 국내외 6,000여 고객을 통해 검증된 고품질 • 안정성
- 멀티코어 최적화 설계 및 소프트웨어 가속기술
- IPSec VPN 및 SSL VPN

User Experience

- 사용자 편의성 특화
- 장애/보안 실시간 모니터링
- 전체 관리 장비 통합 모니터링

© AhnLab, Inc. All rights reserved.

특장점(1)_핵심 기반 기술 보유

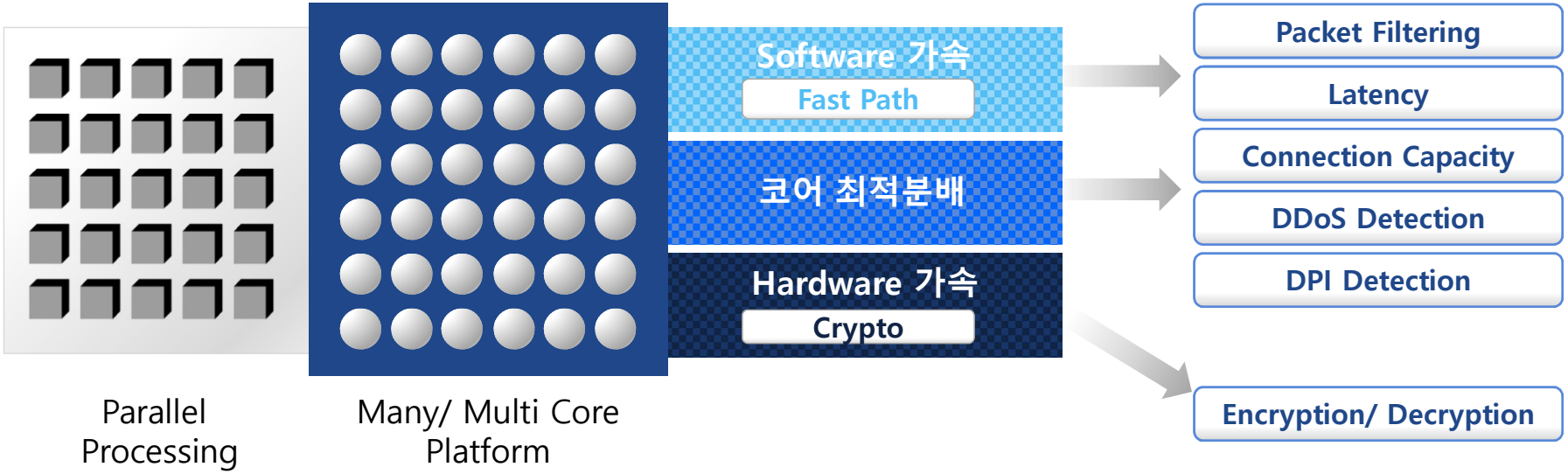
TrusGuard의 각 **보안 모듈**에 대한 **핵심 기반 기술**을 자체 보유하고 있습니다.

방화벽	• 커널/플랫폼 핵심기술 보유 • IPv6 보안 기술 보유
VPN	• VPN 기반기술 보유(IPSec & SSL) • 다양한 응용 기술 보유
Anti-Virus	• 자체 개발 전용엔진 (V3) • 국내 M/S 60% 엔진 • ICSA/ VB 100 등 주요 국제 인증 획득 • 자체 개발 Stream Based Anti-Virus 엔진 보유
Anti-MalSite	• 1000만 대 센서기반 모니터링 체계 • 자체 구축 DB/자체 개발 엔진
Application Control	• 광범위한 국내외 애플리케이션 제어 지원 • 1,300개 이상의 애플리케이션 제어 • 애플리케이션별 도움말 제공
DDoS	• DDoS 공격 방어 엔진 자체 개발 • 국내특허 획득
IPS	• IPS 엔진 핵심기술 보유 • 국내 최대의 보안 위협 분석/대응 조직 • 광범위한 보안 위협 모니터링 인프라
C&C 탐지 / 차단	• C&C Blacklist 기반의 C&C 서버 접속 탐지/ 차단

© AhnLab, Inc. All rights reserved.

특장점(2)_High-Performance

TrusGuard는 **성능 극대화**에 초점을 맞춰 설계된 'Advanced A-TEAM' 아키텍처를 기반으로 **탁월한 성능**을 보장합니다.

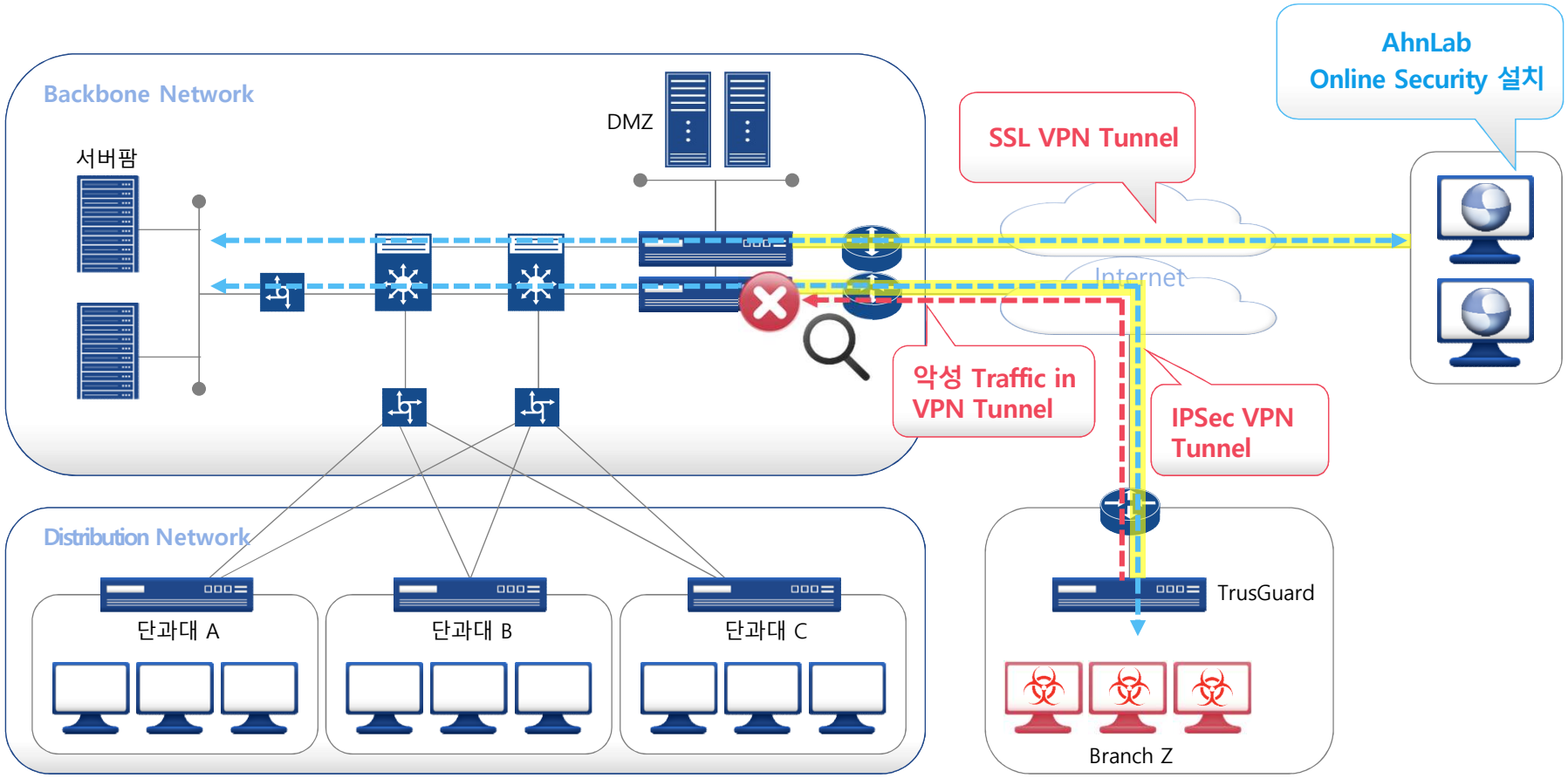


© AhnLab, Inc. All rights reserved.

특장점(3)_Flexible VPN

고객사 환경에 따라 **유연하고 보안성이 강화된 VPN 네트워크** 구성이 가능합니다.

- VPN-IPS 연동을 통한 지사 감염, 악성코드 내부 확산 탐지 및 방어
- IPSec VPN과 SSL VPN을 동시 지원하는 유연한 구조



© AhnLab, Inc. All rights reserved.

특장점(4)_Mobile SSL VPN

Mobile 기기(스마트폰/스마트패드 등)를 통해 고객 내부 인프라에 보안 접속을 위한 SSL VPN 기능을 제공합니다.

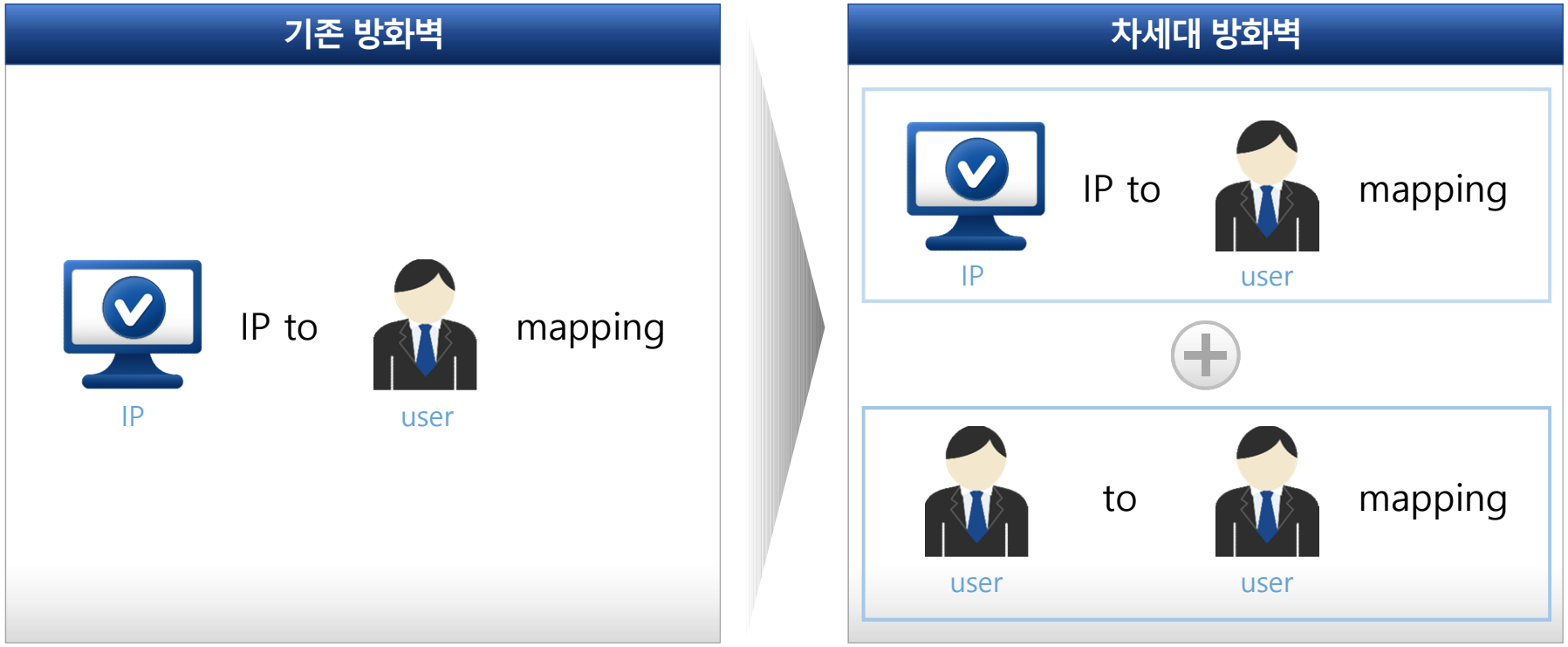
- Mobile 기기를 업무에 활용하는 사이트에 유용한 기능
- 안드로이드 스마트 폰/패드에서 사용 가능한 Mobile SSL VPN 제공

© AhnLab, Inc. All rights reserved.

특장점(5)_사용자(User-ID) 기반 정책 설정 및 관리

IP 주소 기반 뿐만 아니라 **다양한 사용자(User-ID) 기반의 방화벽 정책 설정 및 관리**를 지원합니다.

- 보안 정책 및 보안 현황에 대한 내부 사용자 가시성 확보
- 네트워크 변경 및 이전 용이
- 다양한 인증서버를 통한 USER-ID 실시간 매핑 지원

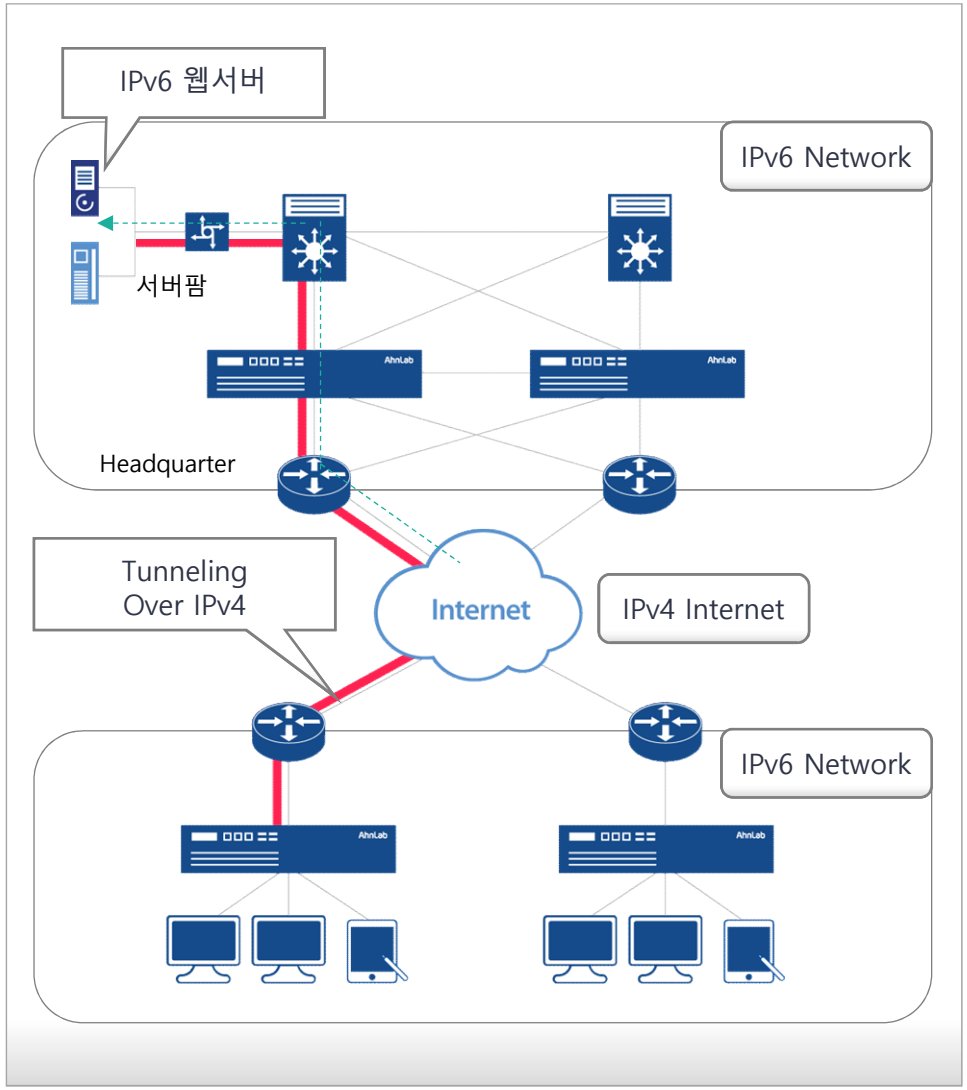


주기적인 매핑(Mapping) 정보 업데이트

© AhnLab, Inc. All rights reserved.

특장점(6)_IPv6

Real Network 환경에서 **IPv4** 및 **IPv6 Dual-stack Security** 환경을 지원합니다.



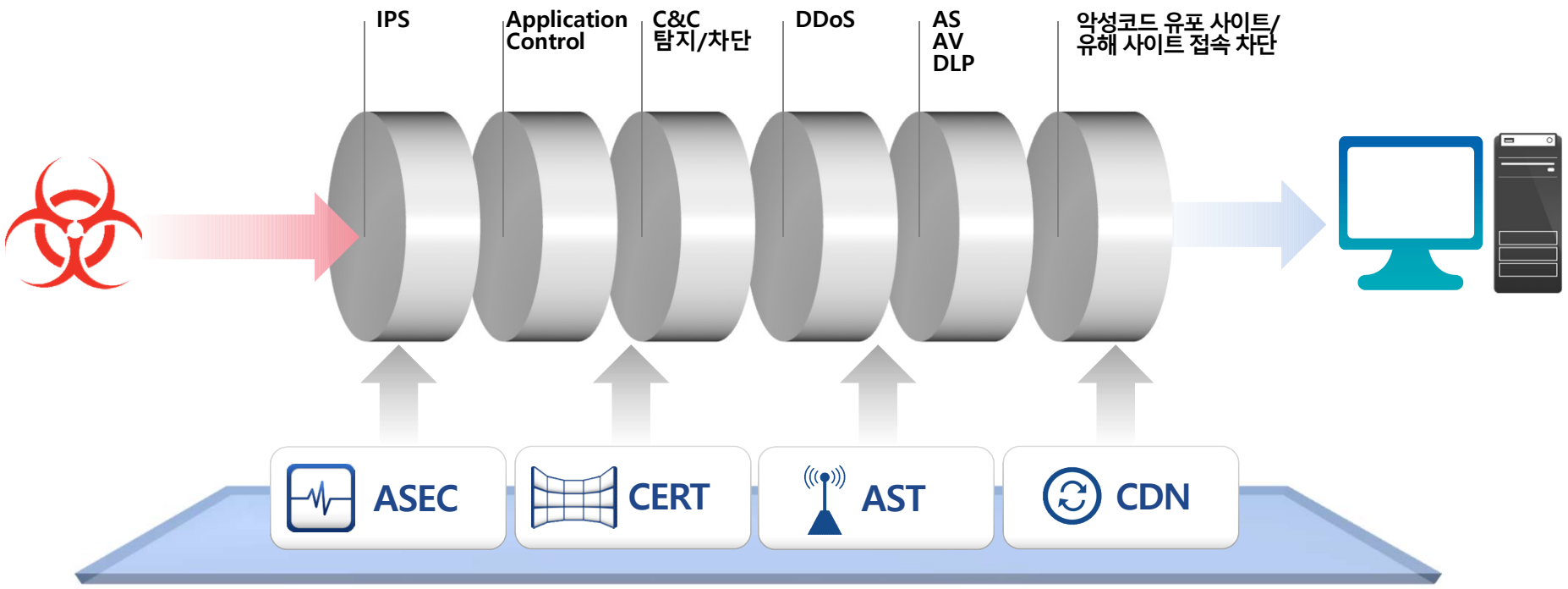
IPv4 & IPv6 Dual-Stack 지원	**IPv6 Routing (Ripv6, OSPFv6)**
Transition 기술 (6to4, NAT-PT)	**DHCPv6, RA**
IPv6 Stateful Inspection	**NAT & Logging**

© AhnLab, Inc. All rights reserved.

특장점(7)_통합 보안 제공

종합적이고 능동적인 방어 시스템을 보유하고 있는 TrusGuard는 다변화된 외부 위협에 대한 통합 보안을 제공합니다.

종합적인 방어 체계
Comprehensive Defense System



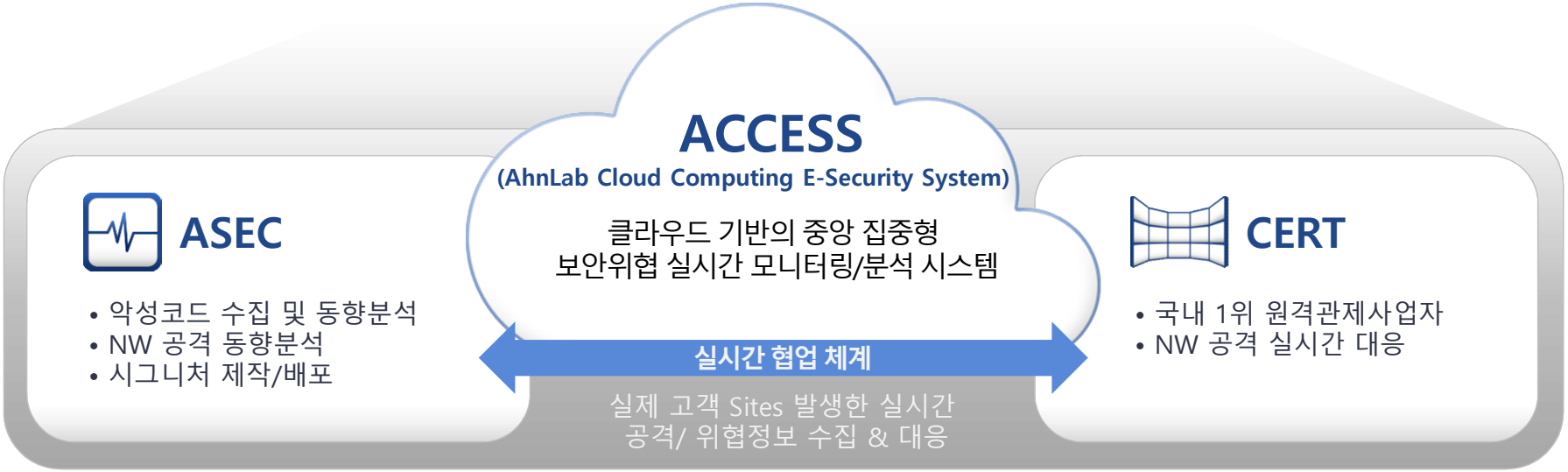
능동적인 방어 체계
Pro-active Defense System

© AhnLab, Inc. All rights reserved.

특장점(7)_통합 보안 제공

통합 보안 리소스(Resource) 및 인프라(Infrastructure)를 기반으로 **차별적인 보안 위협 대응 콘텐츠**를 생성/유지/전달합니다.

Zero-Day Attack Prevention	Outbreak Prevention	최신성 & 정확성
• **취약점 예측 차단** - 예상되는 '취약점 공격' 대응 시그니처 선 배포 • **MicroSoft MAPP Partnership** - 보안패치 정보 사전공유 프로그램	• **악성코드/ 공격의 조기 차단** - 조기확산 방지 시그니처 배포 • **24x7x365 상시근무체계** - 긴급 상황 발생 시, 신속 대응 가능	• **1일 2~3회 시그니처 업데이트** - 시그니처 최신성 유지 • **자체 CERT(보안관제센터)와 협업** - 실제 고객 사에 발생하는 실시간 공격에 대한 탐지 및 즉각 대응 가능



* ASEC : AhnLab Security E-response Center　* ACCESS : AhnLab Cloud Computing E-Security System　* CERT : Computer Emergency Response Team

© AhnLab, Inc. All rights reserved.

특장점(8)_Intrusion Prevention System

정교한 엔진과 **광범위한 시그니처**(Signature)를 기반으로 다양한 공격을 탐지 및 방어합니다.

각종 취약점 공격 방어

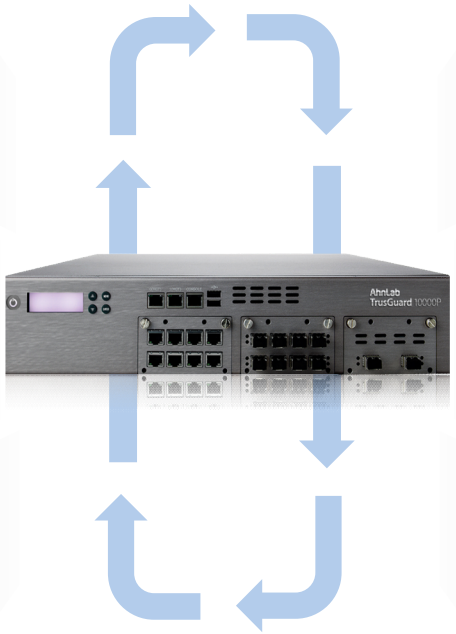
- 웹 취약점 공격 (OWASP)
- 네트워크 취약점 공격
- 애플리케이션 / OS 취약점 공격

다양한 악성코드 공격 방어

- Bot/BotNet / C&C
- 웜, 트로이목마
- Downloader/ Spyware 등

Application Control

- 내부 사용자들의 주요 애플리케이션 접속 / 로그인 등 행위 제어
- 국내 환경에 특화된 애플리케이션 제어 기능 지원



Zero-day 공격방어

- MAPP Partnership (with Microsoft)
- ACCESS 기반의 실시간 보안위협 대응

최신 시그니처 유지

- 일일 정기 업데이트

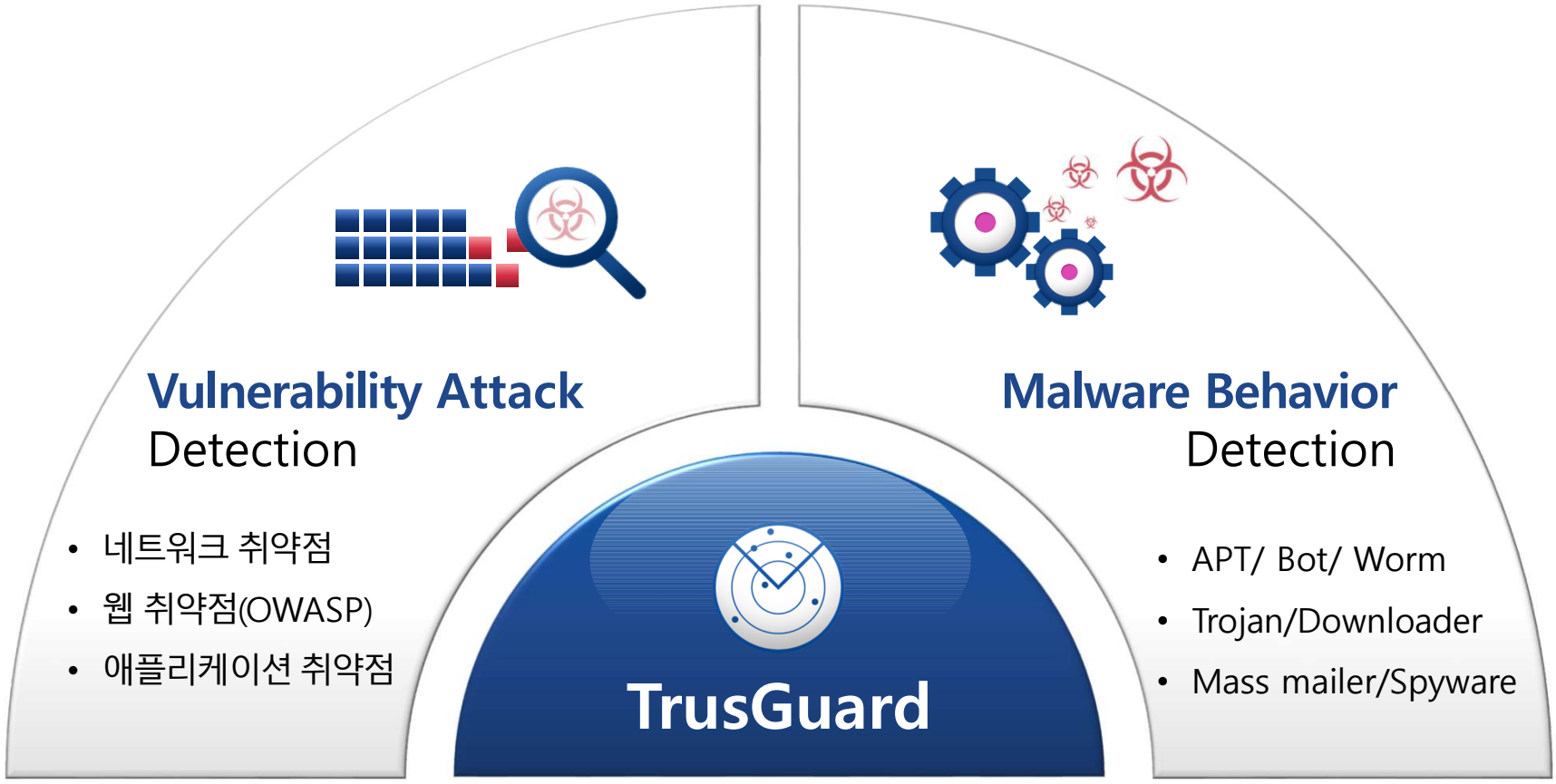
국내 최대의 리소스 보유

- 100여 명의 보안 위협 분석/대응 인력
- 클라우드 기반 보안위협 통합 모니터링/대응 시스템

© AhnLab, Inc. All rights reserved.

특장점(8)_Intrusion Prevention System

각종 취약점 공격, 악성코드 내부 유입 및 행위를 **탐지/제어**합니다.

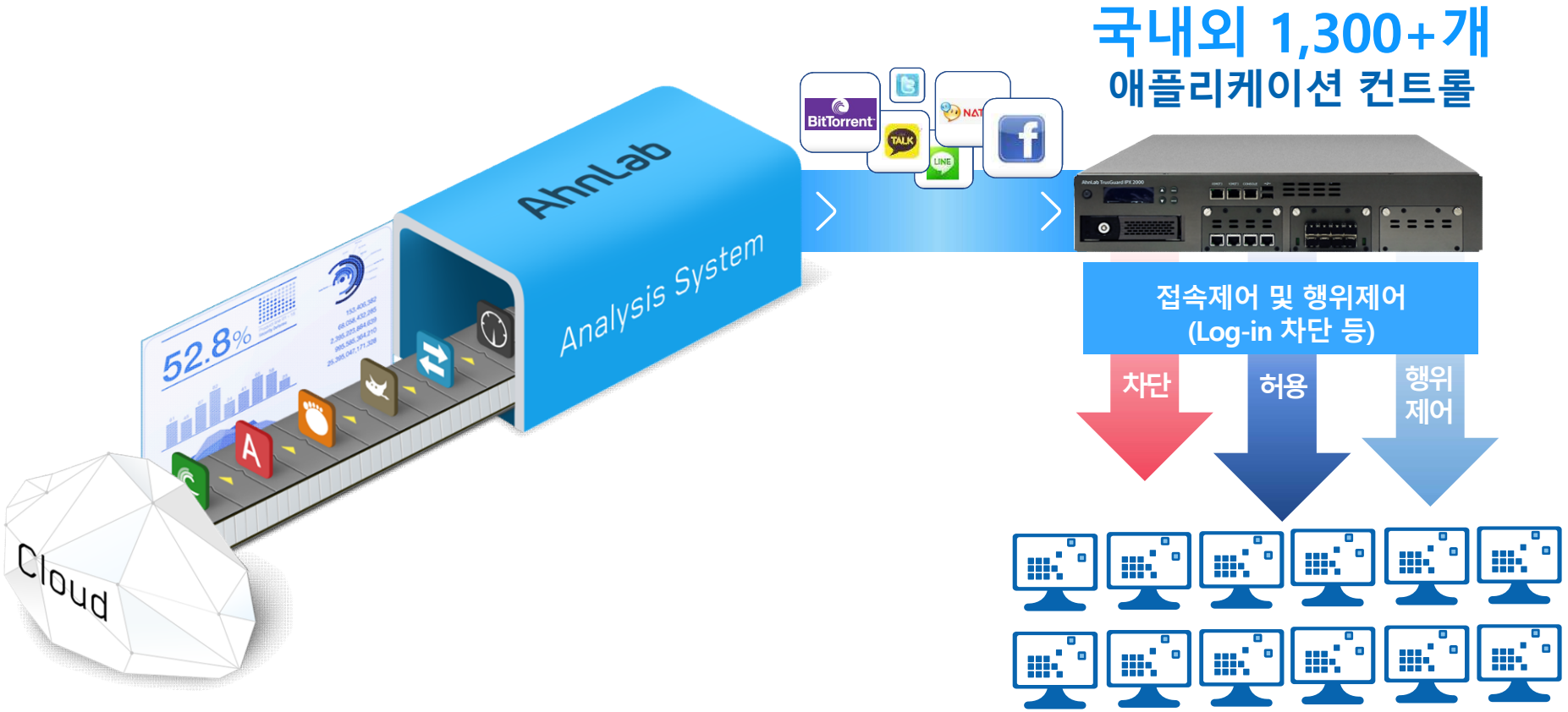


© AhnLab, Inc. All rights reserved.

특장점(9)_Application Control

최근 보안 위협의 주요 수단으로 악용되는 **다양한 유형의 애플리케이션(Application)을 보다 정교하게 제어**합니다.

Application 행위 제어 | **탐지 Application 수 확장** | **Application별 도움말**

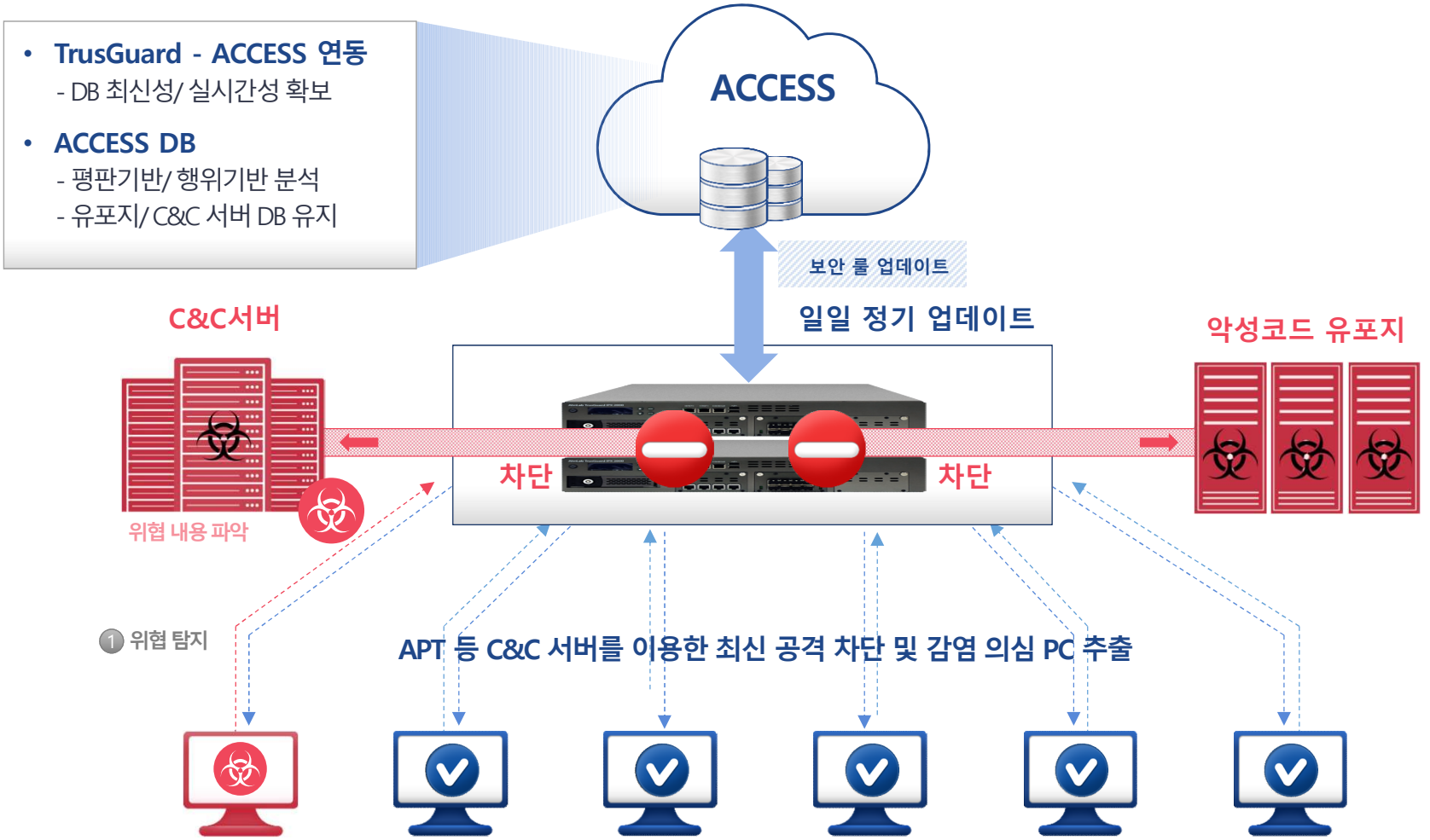


© AhnLab, Inc. All rights reserved.

특장점(10)_C&C 서버 탐지/ 차단

안랩이 자체 보유한 **C&C Blacklist DB**를 기반으로 **C&C 서버 접속 탐지 및 차단** 기능을 제공합니다.

- 클라우드 기반의 안랩 위협분석 시스템(ACCESS)을 통한 C&C 정보 수집 및 분석
- 최근 6개월 이내의 활동 내역이 포함된 높은 신뢰도의 C&C Blacklist DB 기반 + 위험도/ 정확도/ 확산도 기반 탐지 및 차단 설정
- 실시간 업데이트로 DB의 최신성 확보

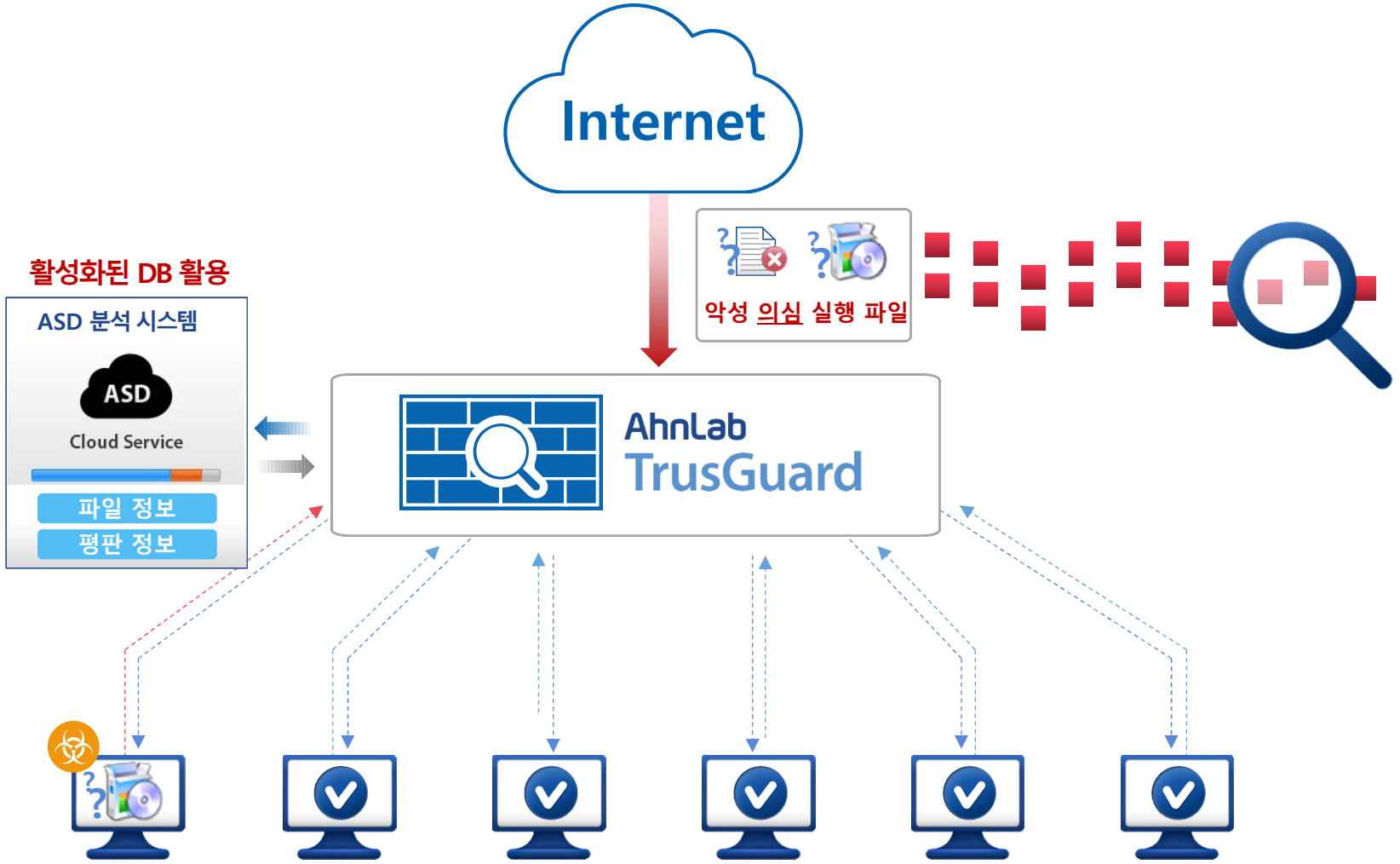


© AhnLab, Inc. All rights reserved.

특장점(11)_위협탐지 필터

내부로 유입되는 **악성의심 실행파일 (Unknown File), 불필요한 프로그램(PUP) 탐지 및 유입 현황 모니터링** 기능을 제공합니다.

- 안랩이 보유한 Cloud 기반의 Security Intelligence인 ASD Database (약 10억 개의 악성/ 정상파일 Database) 연동을 통한 의심 Unknown 파일여부 판단



© AhnLab, Inc. All rights reserved.

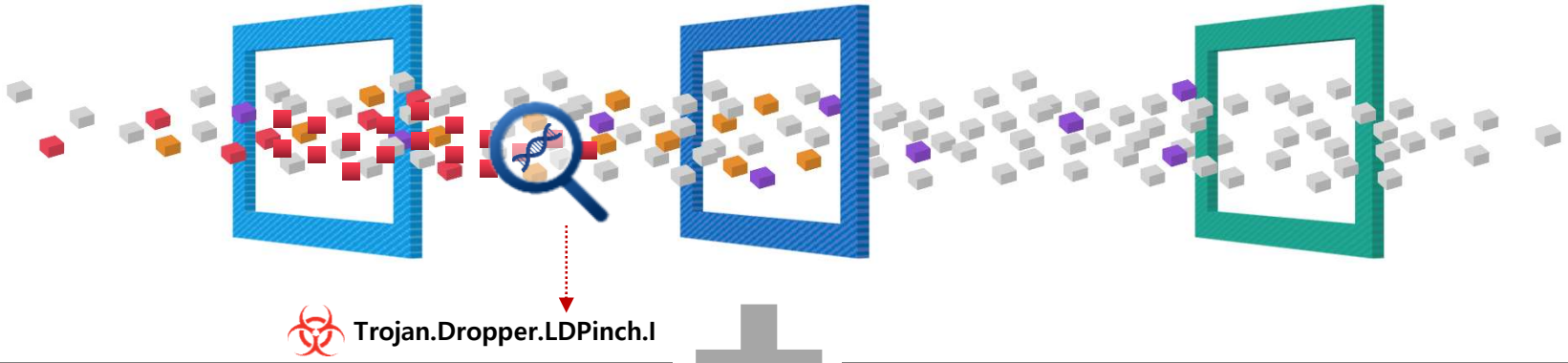
특장점(12)_Stream Based Anti-Virus

안랩이 자체 개발한 **Stream Based AV 엔진은** 보다 **빠른 Virus 탐지 및 차단** 기능을 제공합니다.

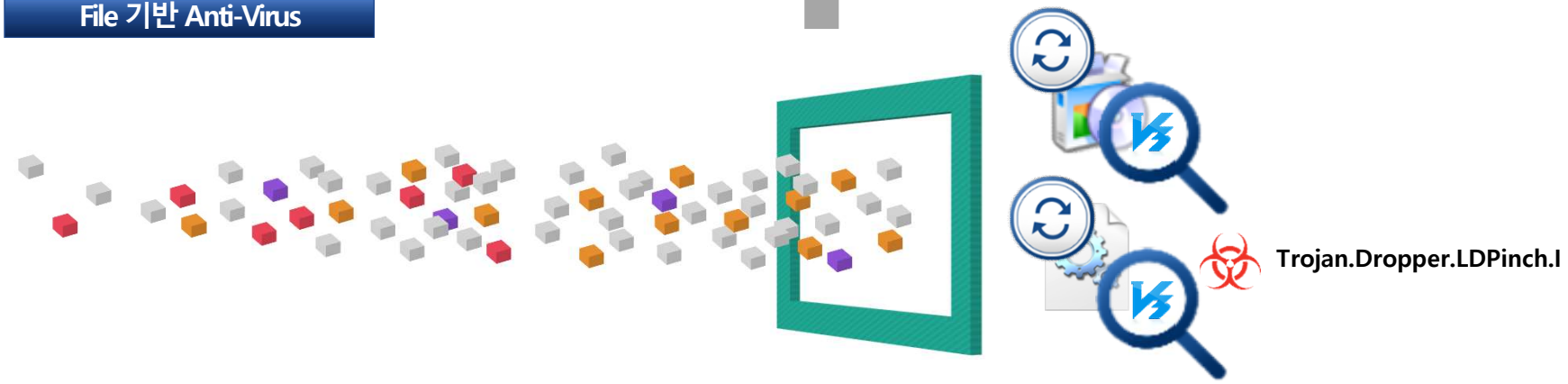
- '패킷 단위의 Anti-Virus 탐지 엔진'을 통해 기존 파일 기반 기법의 성능 한계를 극복한 고속 Virus 탐지/차단 기능 제공
- 안랩 자체 개발 'Stream-based AV 엔진' 탑재로, 수십만 개의 1:N Malware 탐지 시그니처 제공 및 빠른 엔진 업데이트 제공

Stream Based Anti-Virus

안랩 자체 개발 Stream Based AV 엔진 적용



File 기반 Anti-Virus

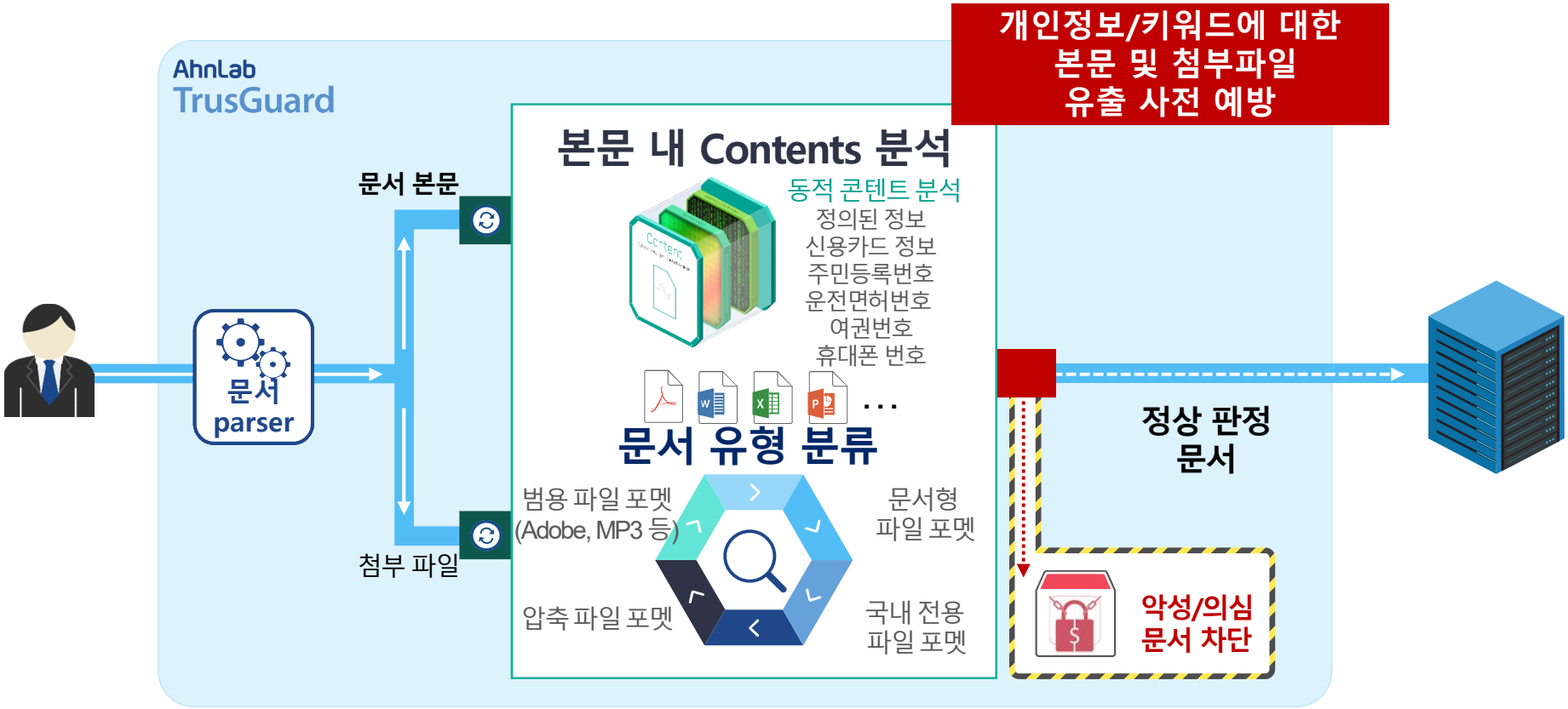


© AhnLab, Inc. All rights reserved.

특장점(13)_Data Leak Prevention (DLP)

데이터 유출 방지(DLP) 엔진을 통해 내부 자산에 대한 유출 방지 / 콘텐츠 가시성 확보 기능을 제공합니다.

- 첨부파일에 대한 유형 분류 , 문서 내 Contents 검사를 통해 내부 자산에 대한 유출 방지 기능 제공

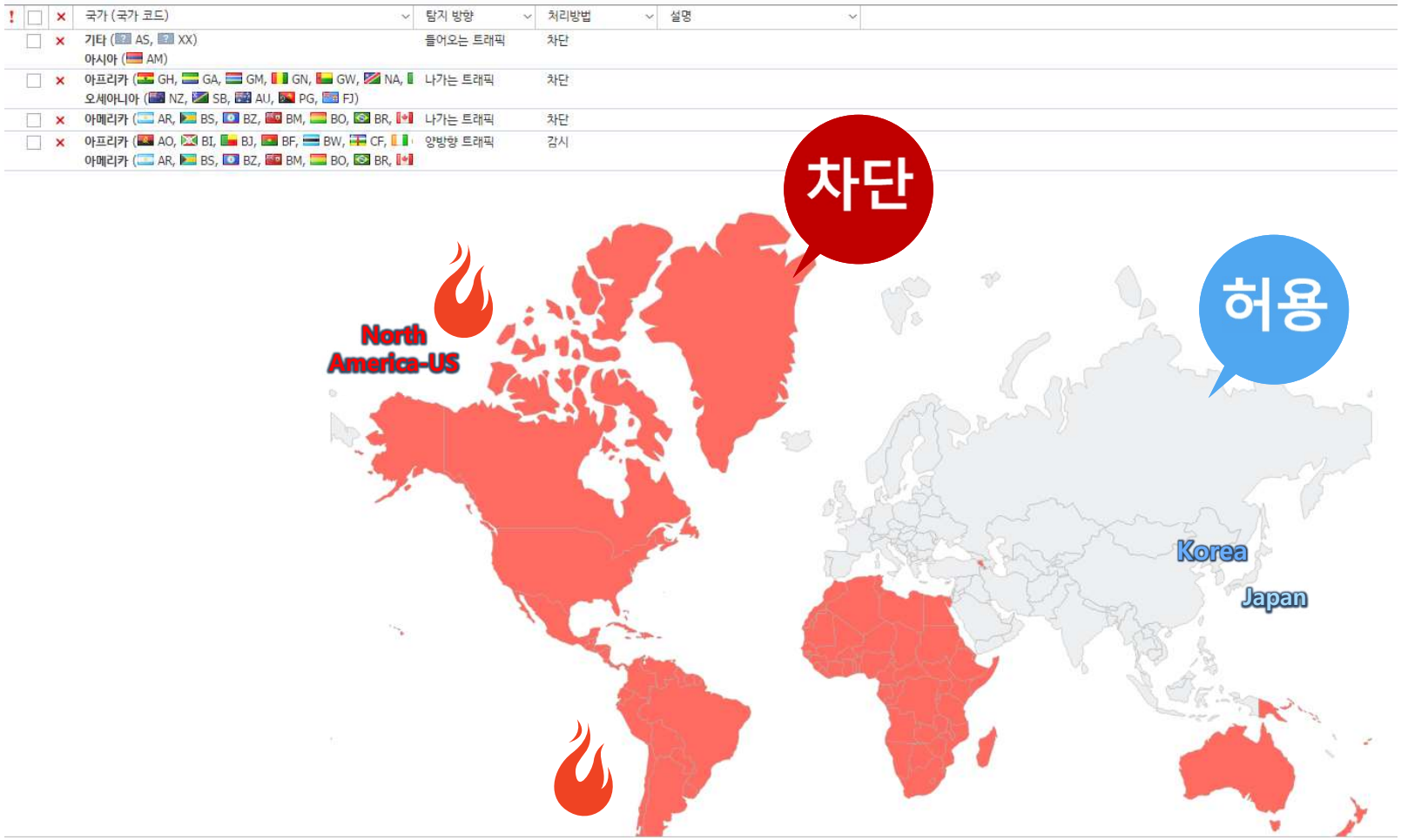


© AhnLab, Inc. All rights reserved.

특장점(14)_지역 기반 차단 설정

지역 기반 차단 정책을 통해 지역별/대륙별 차단 기능을 제공합니다.

- IP Geo-Location / Location-Based Threats

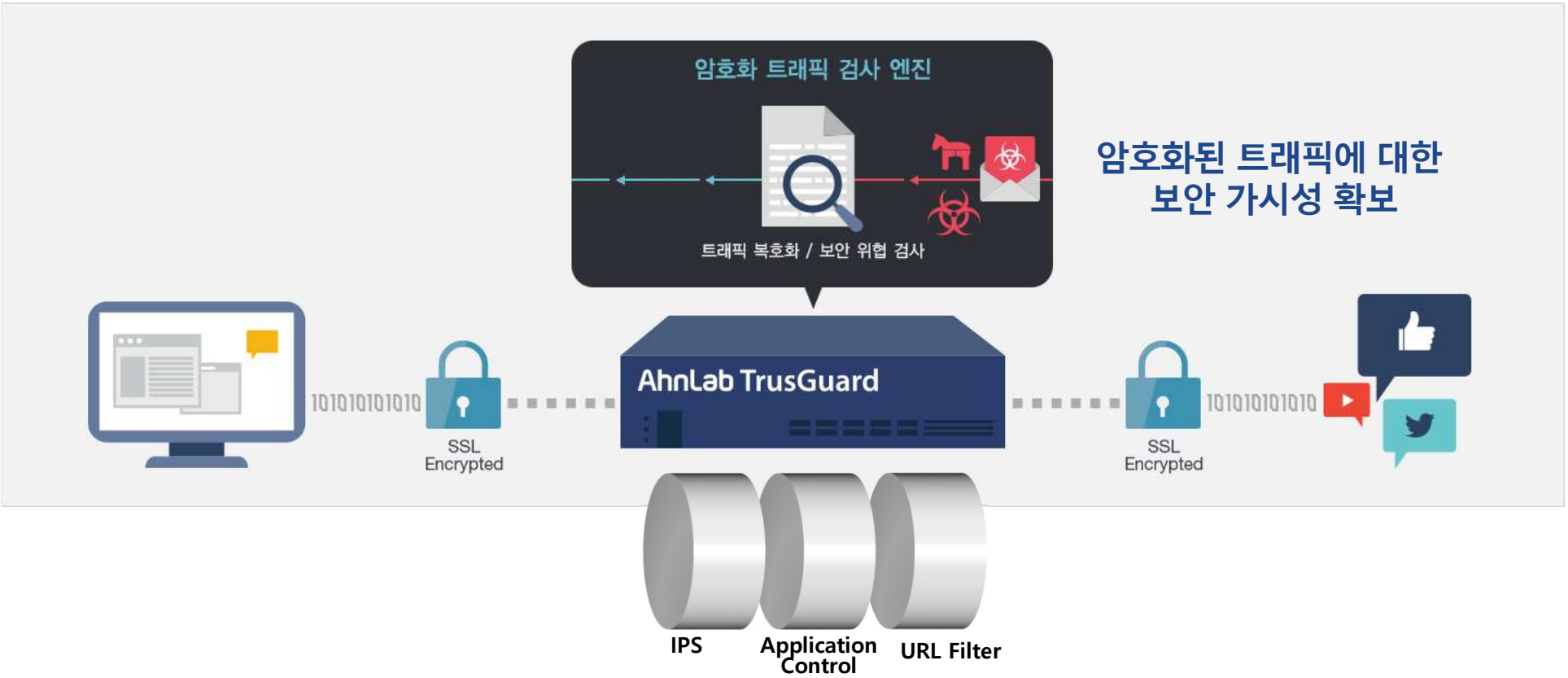


© AhnLab, Inc. All rights reserved.

특장점(15)_SSL Inspection

암호화된 트래픽 가시성 확보를 위해 SSL 트래픽 검사(SSL Inspection) 기능을 제공합니다.

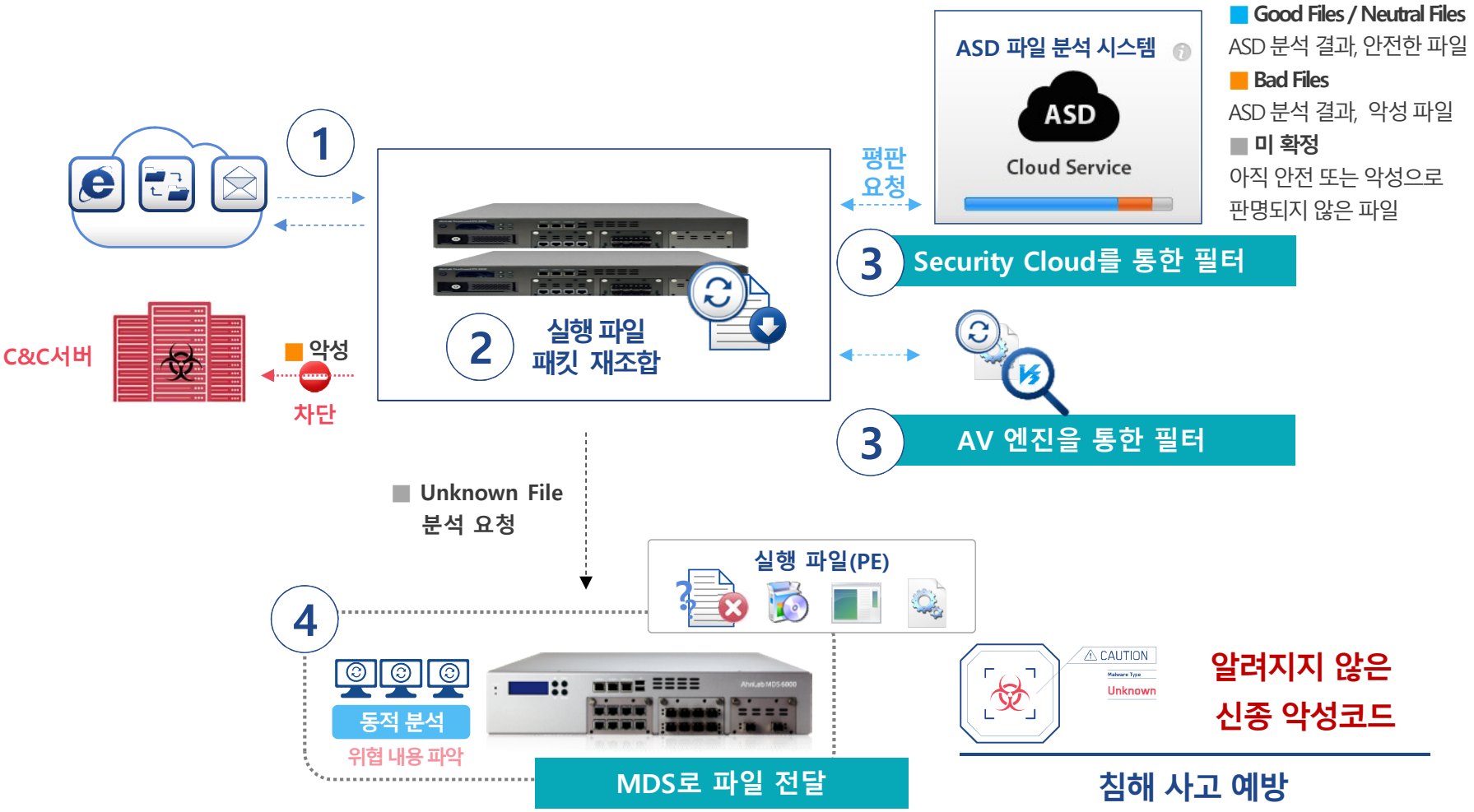
- TrusGuard는 암호화된 보안 위협에 대응하기 위해 SSL 트래픽을 복호화하여 탐지 및 차단하는 기능을 제공합니다.



© AhnLab, Inc. All rights reserved.

특장점(16)_고도화된 위협 대응 - 자사 제품 연동(MDS)

TrusGuard는 자사 APT 보안 솔루션(AhnLab MDS) 연동을 통해 의심파일 동적 분석 기능을 제공합니다.



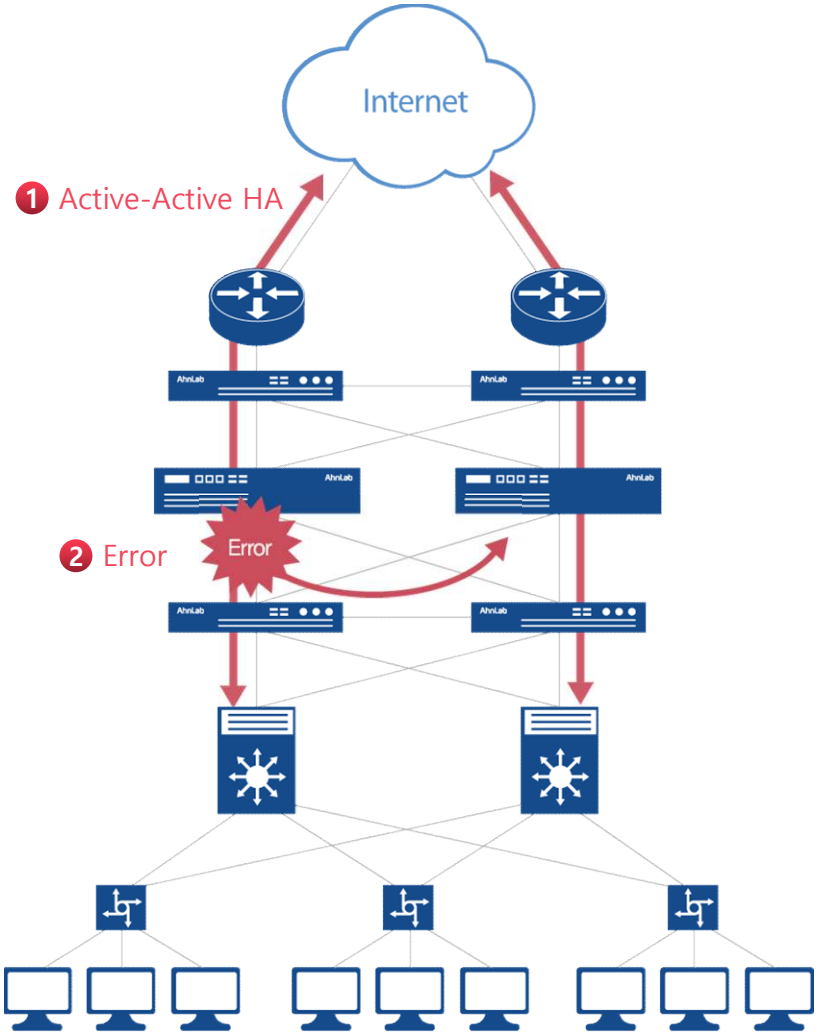
© AhnLab, Inc. All rights reserved.

03
기본 기능

AhnLab

Firewall

TrusGuard는 정교하고 안정적인 **High-Quality Firewall Technology**를 기반으로 탁월한 방화벽 기능을 제공합니다.



Stateful Inspection	• 블랙리스트/화이트리스트 기반 • 다양한 정책 유효성 검증
High Availability	• Fail-Over 기능 (Active-Active, Active-Standby) • 별도의 L4 스위치 없이 백업 가능(Session/ Rule 동기화)
Link Aggregation	• 링크(Link) 간 Active-Active/Active-Standby 지원 • 대용량 Traffic 처리 용이하며, Link 간 Fail-over 기능 제공
QoS	• 정책별/ IP별 / 포트별 QoS 설정(7단계 Leveling) • 최대 대역폭 제한, 최소 대역폭 보장
NAT	• Static (1:1)/ Dynamic NAT (1:N, M:N), Twice NAT • Excluded NAT, NAT Traversal, Load-Sharing NAT
Routing	• Static/ Dynamic Routing (RIP, RIPv2, OSPF, OSPFv3, BGP) • Multicasting 지원 (PIM_SM/ IGMP)/ Source Routing 지원
VoIP 지원	• SIP, H.323 지원 (Dynamic Port 지원)

© AhnLab, Inc. All rights reserved.

IPSec VPN

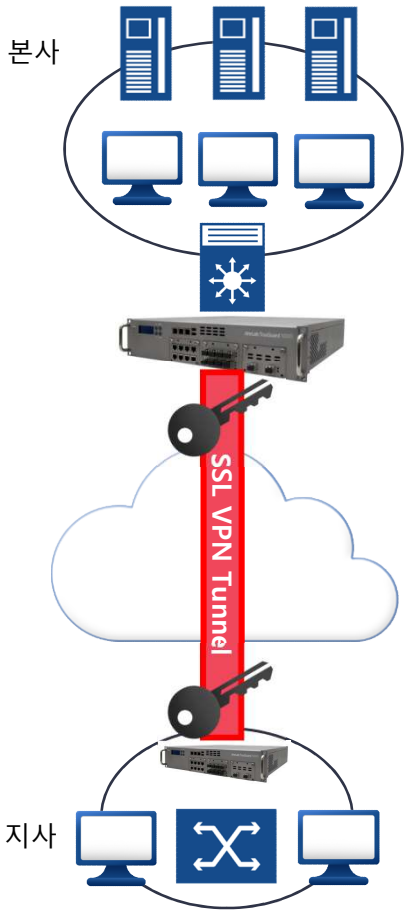
TrusGuard를 통해 본사-지사 간의 보안 위협 대응이 더욱 강화된 VPN 네트워크를 구성할 수 있습니다.

IPSec 표준 지원	• Tunnel mode, ESP, AH, ESP+AH 지원 • 3DES, AES, SEED, ARIA 암호화 알고리즘 지원 • IKEv1, IKEv2, Manual 지원 • Hub&Spoke, Star, Mesh 구조 지원
인증서 기반	• 사설/ 공인인증서 기반 인증지원
Dual Line	• VPN 멀티라인 로드밸런싱 지원 - Per Packet/ Per Session/ 가중치 기반 - Fail-over/ Fail-back 지원 - 출발지/ 목적지별 터널 우선 순위 지정
DPD	• 상대 호스트 상태 감지를 통한 실시간 자동 절체
Firewall/ IPS 연동	• VPN 통신 패킷에 대한 방화벽/ IPS 정책 연동 - VPN 터널을 통한 악성코드 유포 및 확산 방지
Scalability	• L4장비와의 연동지원을 통해 처리능력 확장 가능 • High-Availability 구성 (A-A/ A-S)
기타 기능	• Split Tunnel 기능지원 • Prevent Replay Attack

© AhnLab, Inc. All rights reserved.

SSL VPN

SSL 기반의 유연한 Gateway-to-Client VPN 구성을 지원합니다.



SSL 표준지원	• TLS 지원 • 3DES, AES, SEED, ARIA 암호화 알고리즘 지원
HA 구성	• Active-Standby 지원 (without L4) • Active-Active 지원 (with L4)
사용자 인증방식	• 2-factors 인증 제공 (ID/ PW + 인증서 기반) • 초기 접속 시, 패스워드 강제 변경 기능 • Radius/LDAP/AD/OTP 연동 인증
사용자 접속제어	• 사용자 세션 강제종료 기능 • 사용자 잠금 기능 지원 • 인증실패 횟수 제한 지정 기능
내부서버 접근관리	• 내부 DNS 연동 방식/ WINS 연동 방식 • 사용자별/ 사용자 그룹별 서버 접근 제어
외부접속 보안강화	• 접속 후 PC 캐시(Cache) 정보 삭제 • 접속 PC 해킹 툴 탐지 후 접속(AOS 연동) • 접속 PC의 보안성 강화(AOS 연동) - PC 방화벽 및 Anti-Keylogger 설치를 통해 보안 강화
모니터링	• SSL 터널상태 모니터링 • 실시간 접속 사용자 모니터링

© AhnLab, Inc. All rights reserved.

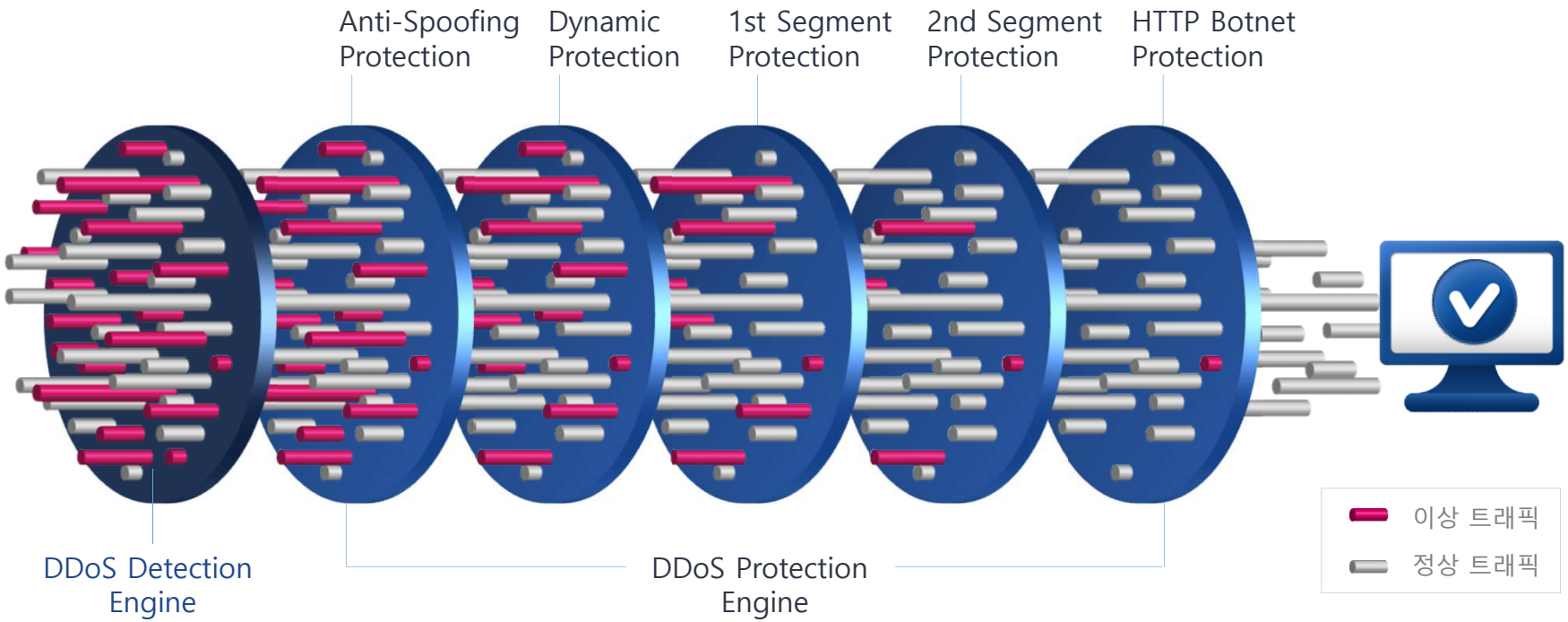
DDoS Mitigation

TrusGuard는 주요 네트워크 공격 유형인 **DDoS 공격에 대한 강력한 방어 능력**을 보유하고 있습니다.

Black-List | Anti Spoofing | Dynamic Protection | Segment Protection | HTTP BotNet | Behavior Signature

정교한 6 단계 방어

국내 특허획득 엔진

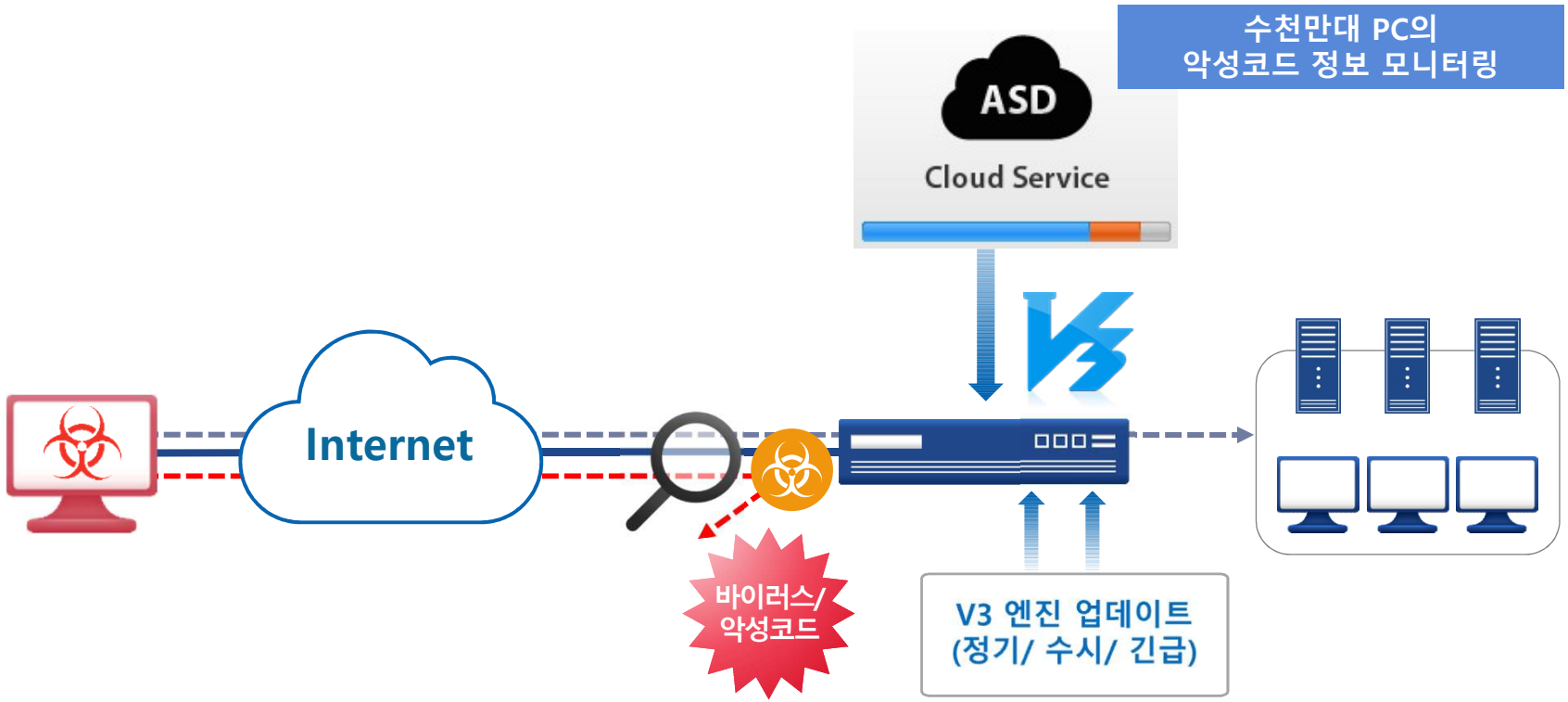


© AhnLab, Inc. All rights reserved.

Anti-Virus

TrusGuard는 전세계적으로 검증받은 V3 엔진을 기반으로 바이러스 필터링 기능을 제공합니다.

- ICSA Labs, AV-Comparatives, AV-Test, VB 100, Check Mark 등 주요 국제 인증을 획득한 글로벌 수준의 Anti-Virus 엔진
- TrusGuard 자체 엔진을 통해 실시간으로 변하는 유해 악성코드 대응에 탁월한 효과

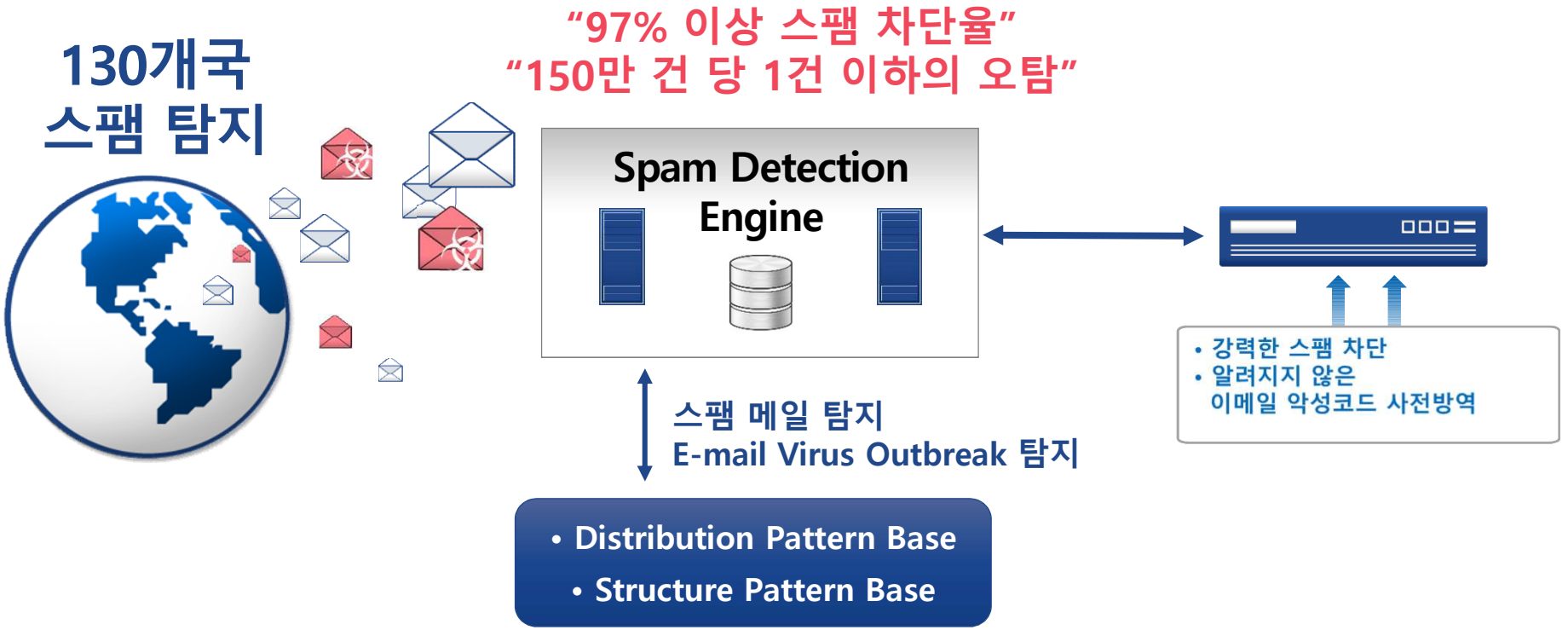


© AhnLab, Inc. All rights reserved.

Anti-Spam

TrusGuard는 스팸 필터링을 위해 국제적으로 공인된 강력한 스팸 엔진을 사용하고 있습니다.

- 97%의 스팸 차단율, 150만 건당 1건 이하의 최소화된 오탐율
- 이메일로 배포되는 알려지지 않은 바이러스에 대한 사전 방역 기능 제공

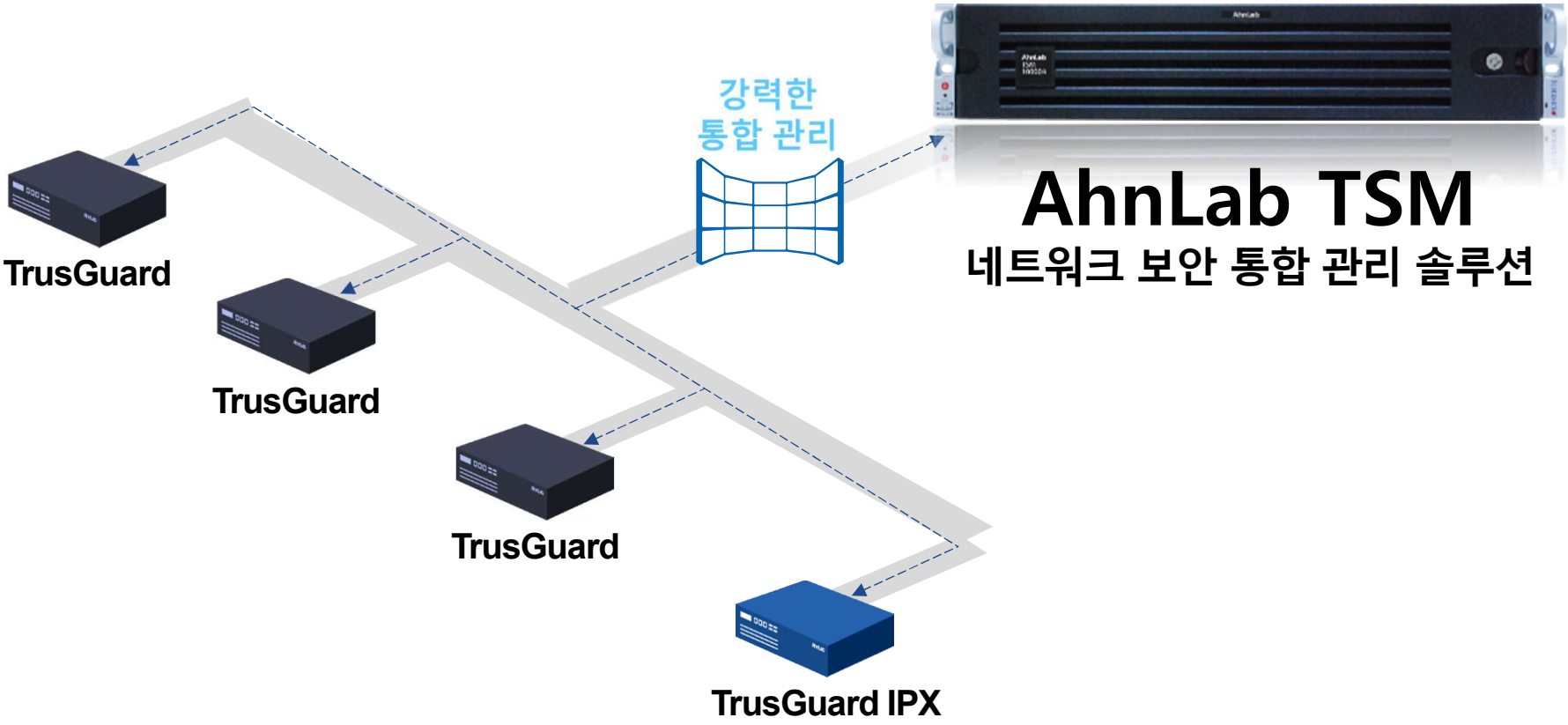


© AhnLab, Inc. All rights reserved.

통합 관리_AhnLab TSM (별도 구매)

AhnLab TSM은 다수의 네트워크 보안 관리 장비를 효율적으로 관리・통제할 수 있도록 간편한 정책 설정 및 통합 모니터링 환경을 제공하는 **차세대 네트워크보안 통합 관리(Total Security Manager) 솔루션**입니다.

- AhnLab TrusGuard 등 안랩의 다양한 차세대 네트워크 보안 솔루션에 대한 효율적인 통합 관리 제공



© AhnLab, Inc. All rights reserved.

통합 관리_AhnLab TSM (별도 구매)

AhnLab TSM은 모듈 기반으로 유연한 정책 설정 및 효과적인 네트워크 통합 관리를 제공합니다.

“통합 정책 설정 / 관리” + “통합 모니터링” + “통합 로그관리”

Policy Manager

- 다수 관리 장비 통합 관리 / 개별 정책 설정 및 관리
- 양방향 정책 설정 및 동기화
- 정책 백업 / 복원, 폐쇄망 엔진 업데이트

Event Monitor

- 다수 관리 장비 통합 모니터링
- 시스템 / 네트워크 / 보안 이벤트 / VPN 모니터링
- 장애 상태 / 장애 징후 / 보안 현황 모니터링

Log Manager

- 다수 관리 장비 통합 로그 수집 및 관리
- 통합 대시보드(Dashboard) / 통합 로그검색
- 통합 보고서

© AhnLab, Inc. All rights reserved.

04
제품 사양

AhnLab

TrusGuard 라인업 및 제품 사양

구분	TG 31A	TG 40A	TG 50A	TG 70A	TG 100A	TG 400A	TG 500A
CPU	1 Core	2 Core	1 Core	2 Core	2 Core	2 Core	4 Core
RAM	1GB	2GB	2GB	2GB	8GB	8GB	8GB
CF	1GB	2GB	2GB	2GB	2GB	4GB	4GB
HDD	-	-	-	-	500GB	1TB	1TB
Interface	10/100/1000 Switch x 4 10/100/1000 Base-T x 2	10/100/1000 Switch x 4 10/100/1000 Base-T x 4	10/100/1000 Base-T x 6	10/100/1000 Base-T x 6	10/100/1000 Base-T x 6	10/100/1000 Base-T x 6 1G Base-X x 4	10/100/1000 Base-T x 6 1G Base-X x 6
방화벽 (Max)	1G	1.5G	1.5G	2G	4G	6G	8G
IPS (Max)	-	-	700M	1G	1.2G	2G	2.5G
VPN Tunnel	1,000	1,000	1,000	2,000	5,000	10,000	12,000
동시세션	200,000	500,000	800,000	1,200,000	1,700,000	2,500,000	3,000,000
Size (WxHxD)	300x44x158	220x44x194.4	440x44x240	440x44x240	438x44x291	437x88x503.6	437x88x503.6
Power	40W Single	40W Single	100W Single	100W Single	250W Single	300W Redundant	300W Redundant

*** TG 31A/40A는 방화벽/ IPSec VPN 기능만 제공**

구분	TG 1000P	TG 5000	TG 10000P	TG 22000_Std.	TG 22000_Accel.
CPU	6 Core	8 Core	12 Core	16 Core	16 Core
RAM	8GB	16GB	16GB	24GB	24GB
CF	4GB	4GB	4GB	4GB	4GB
HDD	2TB	2TB	2TB	2TB	2TB
Interface (기본)	10/100/1000 Base-T x 6 1G Base-X x 8	10/100/1000 Base-T x 10 1G Base X x 4 10G Base-X x 2	10/100/1000 Base-T x 14 1G Base-X x 8 10G Base-X x 2	10/100/1000 Base-T x 10 1G Base X x 4 10G Base-X x 4 (10G * 2 카드 2장)	10/100/1000 Base-T x 10 1G Base X x 4 10G Base-X x 4 (10G * 2 카드 2장)
Interface (옵션)	기존 카드 교체장착 10/100/1000 Base-T x 8 카드	기존 카드 교체장착 (최대 3개 Slot 제공) 1G Base-X x 8 카드 10G Base-X x 2 카드 10G Base-X x 4 카드	기존 카드 교체장착 (최대 3개 Slot 제공) 10G Base-X x 2 카드 10G Base-X x 4 카드	추가 카드장착 (최대 7개 Slot 제공) 1G Base-X x 8 카드 10G Base-X x 2 카드 10G Base-X x 4 카드	추가 카드장착 (최대 7개 Slot 제공) 1G Base-X x 8 카드 10G Base-X x 2 카드
방화벽 (Max)	12G	30G	50G	100G	40G
방화벽 (64byte)	-	-	-	-	40G
Latency	-	-	-	-	3.0us 이하
IPS (Max)	5G	10G	20G	20G	20G
VPN Tunnel	20,000	20,000	40,000	40,000	40,000
동시세션	4,000,000	6,000,000	10,000,000	15,000,000	15,000,000
Size (WxHxD)	450x88x580	438x88x717	450x88x580	438x88x717	438x88x717
Power	500W Redundant	650W Redundant	500W Redundant	650W Redundant	650W Redundant

© AhnLab, Inc. All rights reserved.

TSM 라인업 및 제품 사양

구분	AhnLab TSM 2000	AhnLab TSM 5000 (no RAID)	AhnLab TSM 5000R (RAID)	AhnLab TSM 10000R (RAID)
CPU	2 Core	4 Core	4 Core	4 Core
RAM	8GB	16GB	16GB	32GB
SATA DOM	4GB	4GB	4GB	4GB
인터페이스	10/100/1000 Base-T x 2	10/100/1000 Base-T x 2	10/100/1000 Base-T x 2	10/100/1000 Base-T x 2
RAID	-	-	지원 (0/ 1/ 5/ 10)	지원 (0/ 1/ 5/ 10)
HDD 용량	기본형 500GB 최대 장착 가능 HDD : 2개 탑재 가능 HDD Type (500G/ 1TB/ 2TB)	기본형 1TB (500GB x 2) 최대 장착 가능 HDD : 4개 탑재 가능 HDD Type (500G/ 1TB/ 2TB)	기본형 2TB (500GB x 4) 최대 장착 가능 HDD : 4개 탑재 가능 HDD Type (500G/ 1TB/ 2TB)	기본형 4TB (1TB x 4) 최대 장착 가능 HDD : 12개 탑재 가능 HDD Type (500G/ 1TB/ 2TB)
통합 정책 관리 장비 수	500대	1,500대	1,500대	3,000대
로그 수용 성능	15,000 mps	25,000 mps	25,000 mps	50,000 mps
Size (W×D×H mm)	426 x 574 x 43	437 x 503 x 43	437 x 503 x 43	437 x 648 x 89
Power	260W Single	600W Single	600W Single	1200W Redundant

© AhnLab, Inc. All rights reserved.

별첨

안랩의 차별점

AhnLab

ASEC : 안랩의 악성코드 분석 대응조직

안랩 시큐리티대응센터(AhnLab Security E-response Center, ASEC)는 국내 최고의 악성코드 분석가 및 보안전문가로 구성된 **보안위협 분석 및 대응조직**입니다.

24시간x365일 운영

ASEC은 전세계에서 발생하는
새로운 보안위협에 대해 24시간
모니터링 및 분석 대응하고 있습니다.

네트워크/엔드포인트 통합 시그니처 제공

ASEC은 네트워크와 PC, 서버, 모바일 기기 등
다양한 IT 환경에서 발생하는 보안위협 대응
시그니처를 통합 제공합니다.

정기적인 분석정보 제공

ASEC은 악성코드 및 취약점에 대한
상세분석정보를 제공하고, ASEC 리포트를
통해 보안위협 동향정보를 제공합니다.

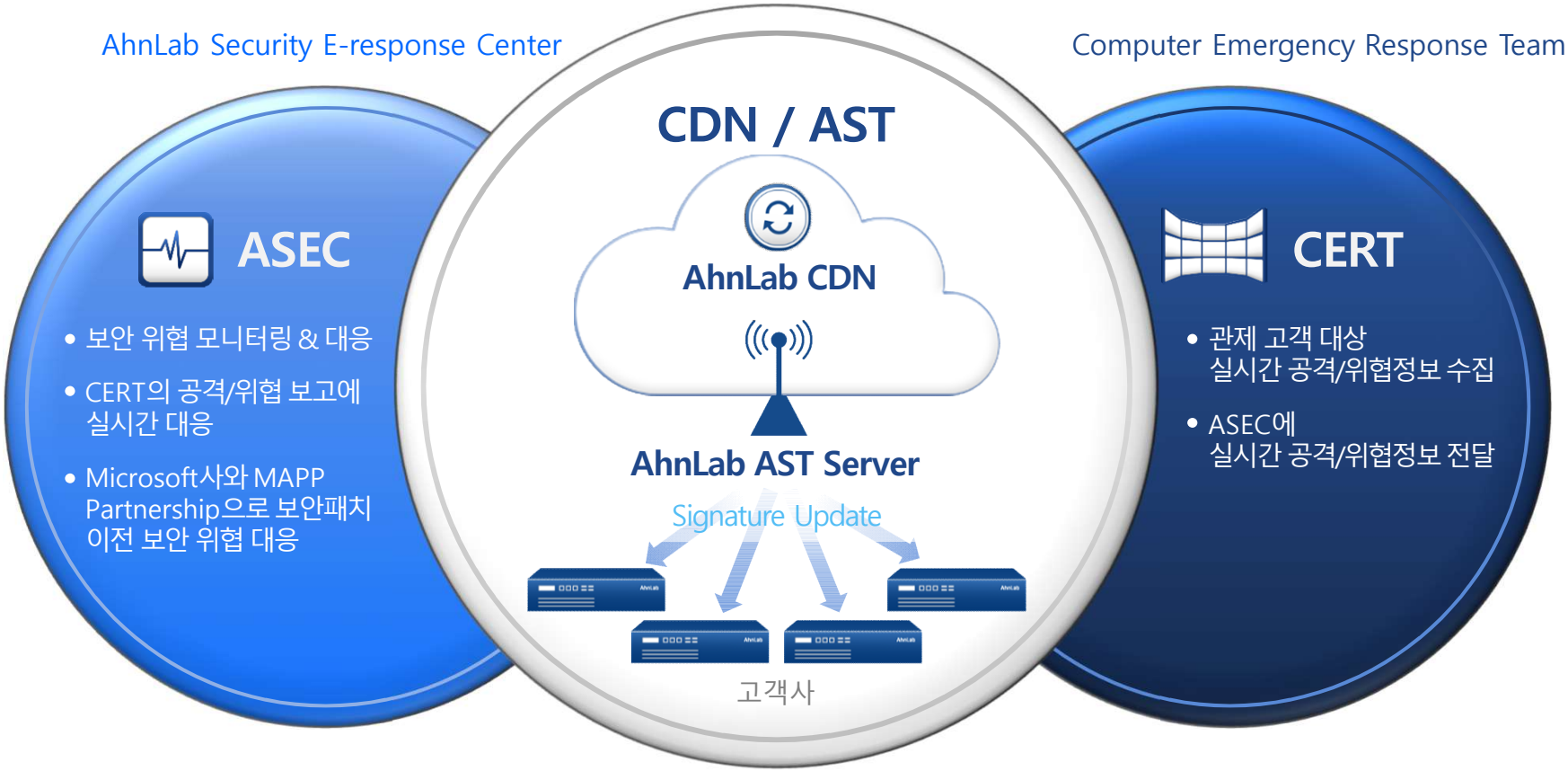
다양한 보안위협 모니터링/ 분석 시스템 활용

- ASEC Intelligence Network™
- BotNet™ : 봇넷정보관리시스템
- WebMon™ : 웹사이트모니터링시스템
- BlueBox™ : 악성코드 패킷 추출 시스템
- 취약점 시그니처 경쟁력 분석 시스템

© AhnLab, Inc. All rights reserved.

국내 유일, ASEC – CERT 동시 보유

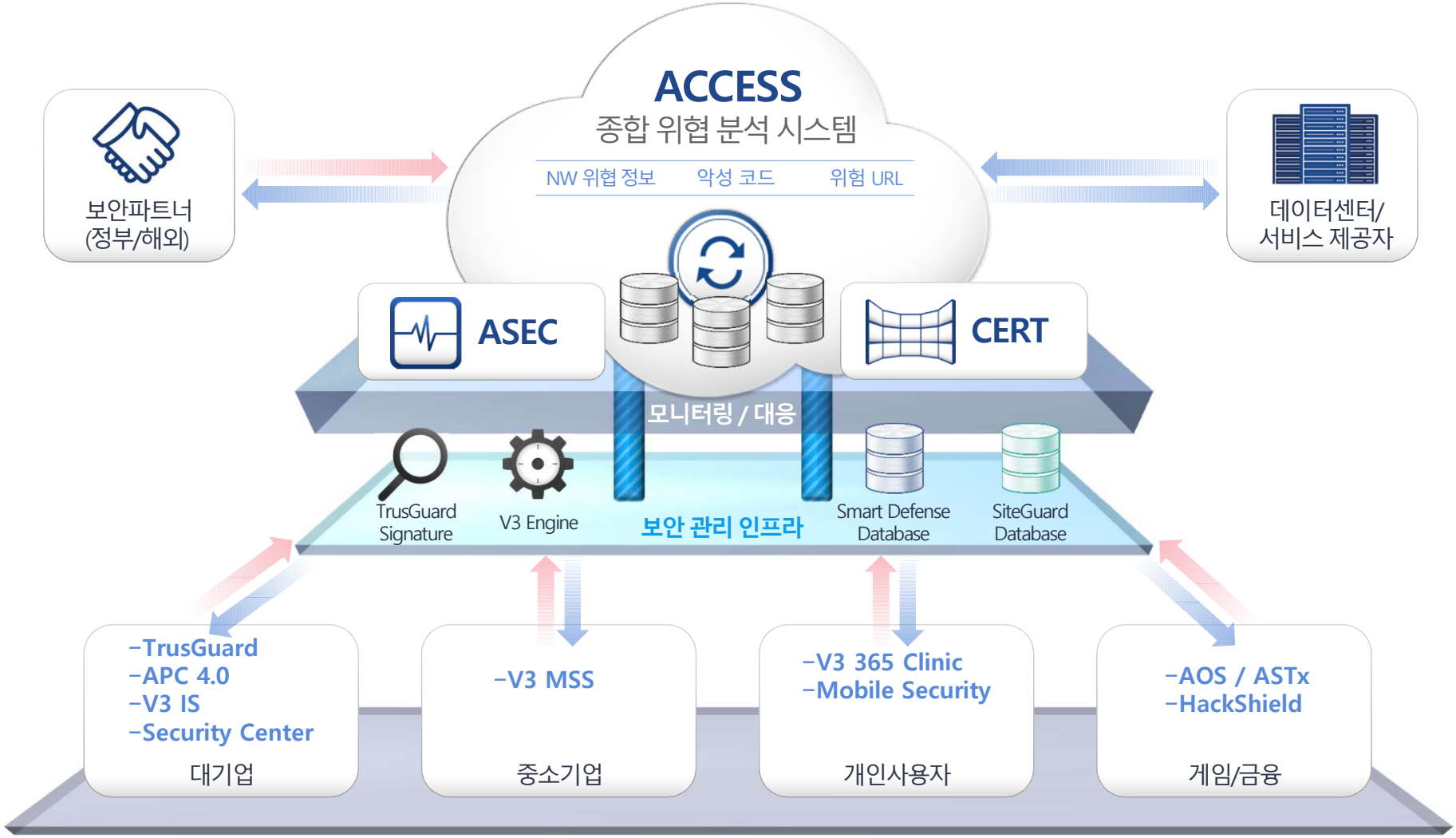
'ASEC-CERT'의 유기적인 연동을 통해 악성코드 및 공격에 대해 효율적인 대응이 가능합니다.



© AhnLab, Inc. All rights reserved.

안랩의 위협 대응 체계 ACCESS

ACCESS(AhnLab Cloud Computing E-Security System)는 실시간으로 급변하는 보안위협에 보다 신속하고 효과적으로 대응하기 위해 안랩이 구축한 **클라우드 컴퓨팅 기반의 종합위협 분석 시스템** 입니다.



© AhnLab, Inc. All rights reserved.

More security, More freedom

AhnLab