보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

실제 사례로 보는 엔드포인트 & 네트워크 보안 플랫폼 통합

AhnLab 2022-05-02

전통적인 개념의 보안에서 엔드포인트는 백신 소프트웨어, 네트워크는 방화벽을 비롯한 하드웨어 장비로 대변되었고 그 영역이 명확히 분리되어 있었다. 하지만, 디지털 전환이 가속화되고 사이버 위협은 고도화되면서 두 영역은 서서히 하나로 합쳐져 통합 보안으로 거듭나고 있다. 어쩌면 '합쳐져야만 했다'라는 표현이 더 적합할 수도 있다. 엔드포인트 – 네트워크 연계 보안 운영 실제 사례를 통해 통합 보안의 필요성을 짚어본다.

지난 월간안 3월호 '보안 복잡성을 해결하는 AhnLab EPP 활용법'과 월간안 4월호 '마이터어택 평가 성적 우수, AhnLab EPP 활용 방안은?'에서는 안랩의 차세대 엔드포인트 보안 플랫폼 AhnLab EPP의 다양한 상황 별 운영 사례들을 살펴봤다.

안랩은 당사가 계속해서 고도화해고 있는 통합 보안 전략을 엔드포인트에 적용하는 것을 넘어 네트워크 영역까지 확장했다. 그 일환으로 AhnLab EPP(이하 EPP)와 차세대 네트워크 방화벽 AhnLab TrusGuard(이하 TrusGuard)를 연동해 '엔드포인트 – 네트워크' 통합 보안 체계를 구축했다.

이번 글에서는 EPP와 TrusGuard 연동을 통한 여러 엔드포인트 – 네트워크 통합 보안 운영 사례들을 살펴볼 예정이다. 본론으로 들어가기에 앞서, 각 솔루션들을 간략히 소개한다.

AhnLab EPP: 안랩 통합 보안 전략의 핵심

AhnLab EPP는 기존 포인트 보안 솔루션 중심의 단순한 보안 관리를 넘어 유기적인 엔드포인트 보안 관리 및 운영을 통해 더 강력하고 효율적인 위협 대응을 역량을 제공한다. 여러 엔드포인트 보안 솔루션들을 단일 에이전트, 단일 관리 콘솔을 기반으로 관리해 복잡다단한 엔드포인트 환경을 효율적으로 보호할 수 있다.

AhnLab EPP는 가장 잘 알려져 있는 안티바이러스 솔루션 'AhnLab V3 Internet Security(V3 IS)'를 포함해 EPP Privacy Management(EPrM), EPP Patch Management(EPM), EPP Security Assessment(ESA)까지 5개의 엔드포인트 보안 솔루션으로 구성되어 있다. 각각의 솔루션이 안티바이러스, 개인정보 보호, 패치 관리, 취약점 점검 & 조치, 위협 탐지 및 대응 등 보안에 필요한 기능들을 수행하고, 이를 단일 에이전트와 단일 콘솔을 기반으로 관리할 수 있어 고객 입장에서 보안성과 효율성을 제고할 수 있다.

Host Name	OS	악성코드 감염건수	악성코드명	파일타입	악성코드 대응	엔진현황	전체 패치율	위협도(상) 패치율	PC점검 현황	개인정보 검출현황
	WINDOWS_7	10	HTML/AmmyyRat.S1	CRDOWNLOAD	치료 완료	최신	100%	0	90	0
	WINDOWS_7	19	PUP/Win32.HFS.R265561	EXE	치료 완료	최신	100%	0	85	167
8NSEQ	WINDOWS_10	11	Win-Trojan/Suspig7.Exp	EXE	치료 완료	최신	96.90%	1	75	2
	WINDOWS_7	6	Win-PUP/Grid.Exp	DLL	치료 완료	최신	99.70%	0	80	3
	WINDOWS_7	3	HTML/AmmyyRat.S2	HTML	치료 완료	최신	99.60%	0	100	0
P7DUR	WINDOWS_10	7	Unwanted/Win32.KeyGen.R270083	EXE	치료 완료	최신	97.20%	0	95	3
160HT	WINDOWS_10	3	PUP/Win32.vGrid.R253661	EXE	치료 완료	최신	100%	0	100	0
V3A0F	WINDOWS_10	2	HackTool/Win64.Injector.C3167416	EXE	치료 완료	최신	93.80%	0	75	0
	WINDOWS_7	1	HTML/AmmyyRat.S3	HTM	치료 완료	최신	100%	0	100	0
HKPTCV	WINDOWS_10	2	Adware/Win32.Anyad.C878385	EXE	치료 완료	최신	96.90%	1	80	0
57VP2	WINDOWS_10	1	JS/BlueCrab.S4	JS	치료 완료	최신	93.80%	0	85	4
	WINDOWS_10	7	Backdoor/Win32.Bifrose	EXE	치료 완료	최신	97.40%	0	55	0
84PKA	WINDOWS_10	1	HackTool/Win32.KMSAuto.C3288293	DAT	치료 완료	최신	100%	0	90	2
T52UG	WINDOWS_10	10	Win32/Hac	XXX	치료 보가	최신	100%	0	60	2
N4LEU	WINDOWS_10	2	HackTool/Win32.Injector.C3166449	EXE	치료 완료	최신	100%	0	100	0
	WINDOWS_7	1	PUP/Win32.DealPly.C2387741	EXE	치료 완료	최신	99.70%	0	95	0
HBH0Q	WINDOWS_10	1	Malware/MDP.AutoRun.M24	EXE	프로세스 종료	최신	97%	0	0	5
DMAE6	WINDOWS_10	1	PUP/Win32.Generic.R261350	EXE	치료 완료	최신	96.90%	0	80	0
	WINDOWS_7	1	Win-PUP/Grid.Exp	EXE	치료 완료	낮음	100%	0	100	0
	WINDOWS_7	2	Trojan/Win32.WannaCryptor.R200572	EXE	치료 완료	낮음	72.30%	18		
57VP2	WINDOWS_10	2	Unwanted/Win32.KMSActivator.R207904	EXE	치료 완료	낮음	83.30%	3	90	0

[그림 1] AhnLab EPP를 통한 보안 관리

AhnLab EPP를 통해 다수의 엔드포인트 보안 솔루션 간 규칙 및 대응 조치를 유기적으로 연계해 설정함으로써 보안 위협에 더욱 강력한 대응이 가능해진다. 보안 담당자의 필요에 따라 다양한 보안 정책을 적용할 수 있어 고객 주도적이며 능동적인 보안 운영이 가능하다.

AhnLab TrusGuard: 진화를 거듭하는 차세대 네트워크 방화벽

지난 2021년 하반기, 안랩은 차세대 방화벽 기능을 고도화한 AhnLab TrusGuard 3.0 버전을 선보였다. 자사 엔드포인트 보안 솔루션들과의 연동 강화로 보안성과 편의성을 높였고 ▲멀티팩터 인증 기능 강화 ▲SSL VPN 기능 고도화 ▲알려지지 않은 애플리케이션(Unknown Application) 인지 기능 제공 ▲디바이스 상태 정보 기반 제어 기능 제공 등 비대면 환경에서 보안성을 강화한 것이 주요 특징이다.

TrusGuard는 철저한 시장 검증을 통해 기술력, 성능 및 안정성을 인정받아 왔으며, IPS(Intrusion Prevention System), 애플리케이션 제어, VPN, C&C 탐지 및 차단, 안티바이러스, 안티스팸, DLP(Data Loss Prevention) 등 다양한 기능을 지원한다. 또, 로우엔드 모델부터 데이터센터급 모델까지 다양한 제품 라인업을 갖추고 있어 기업이 네트워크 환경에 맞춰 효율적으로 적용할 수 있다.

다음은 TrusGuard의 주요 기능 중 본 문서에서 소개할 운영 사례와 관련된 주요 기능들을 정리한 것이다.

1. 애플리케이션 제어

TrusGuard는 차세대 보안 기술인 애플리케이션 제어(Application Control) 기능을 탑재해 P2P, 웹하드, 메신저, SNS 등 수 천 개의 글로벌 및 국내 애플리케이션에 대해 실시간 분석 및 차단•허용•행위 제어가 가능하다. 특히 국내 환경에 특화된 주요 애플리케이션에 대한 독보적인 대응 능력을 제공한다. 또한, 식별이 불가능한 알려지지 않은(Unknown) 애플리케이션 인지를 통해 허용된 애플리케이션에 대한 통신만 가능하게 하여 보안성을 강화한다.

2. 사용자 & 디바이스 기반 제어

TrusGuard는 IP 주소를 기반으로 사용자를 식별하는 방식과 함께 사용자 ID 기반의 사용자 구분 및 행위 제어 기능을 제공해 효율적인 내부 보안 관리와 신속한 보안 위협 대응이 가능하도록 한다. 또한, 디바이스 상태 정보를 인지하여 OS 버전, 보안 패치 여부, 필수 SW 설치 유무, 취약점 점검 결과 등에 따라 네트워크 접근을 제어할 수 있다.

3. SSL VPN 기능 고도화

AhnLab ESA 보안 점검 점수를 기반으로 TrusGuard의 SSL VPN 로그인을 제어하고 신뢰할 수 없는 디바이스의 업무 환경 접근을 원천적으로 차단한다. 따라서 기업들은 뉴노멀로 자리 잡은 비대면 재택근무 환경에서 중요 자산을 효과적으로 보호할 수 있다.

EPP & TrusGuard 연동 사례 1: 디바이스 기반 제어

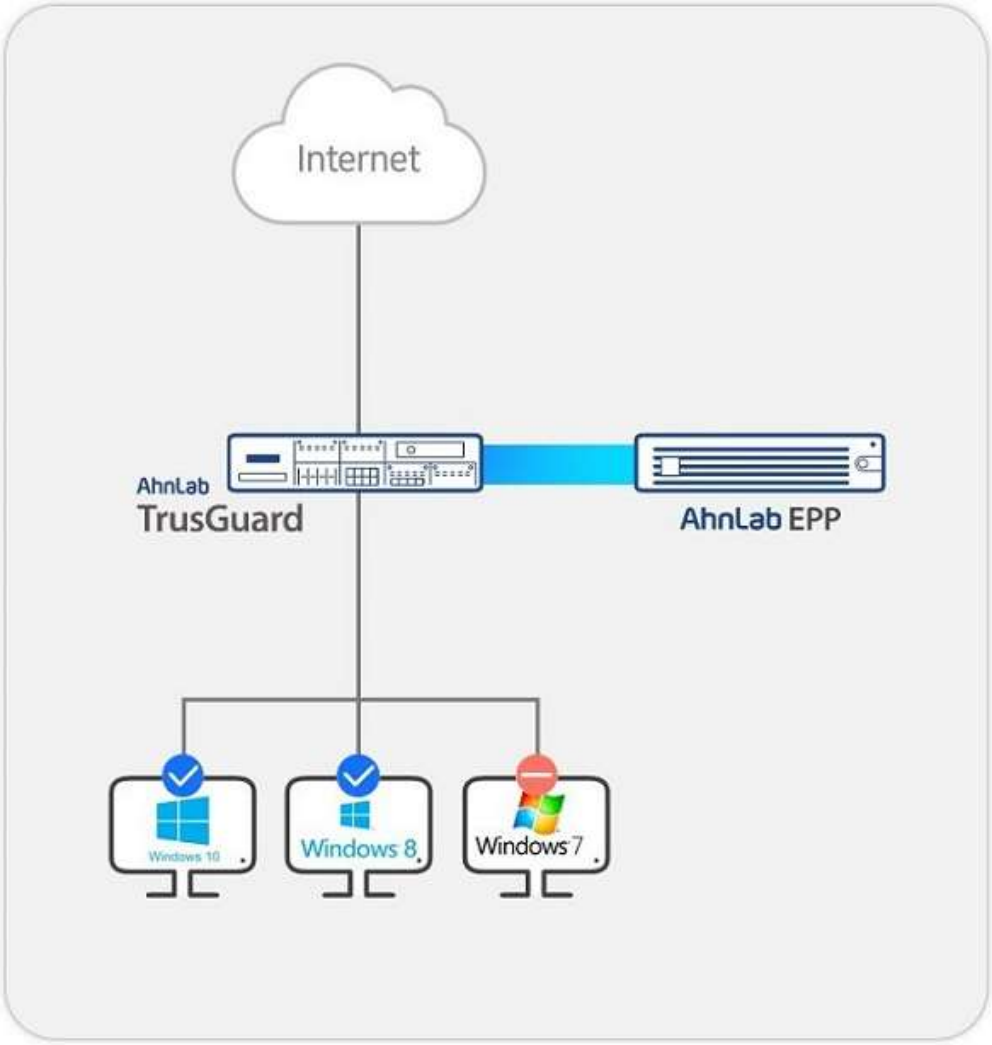
디바이스 기반 제어 연동 사례의 핵심은 EPP 서버에서 에이전트가 설치된 사내망 PC를 관리하고, TrusGuard가 EPP 서버로부터 PC들에 대한 다양한 정보 수집하여 관리자가 설정한 디바이스 제어 기준에 따라 트래픽 허용/차단 등 다양한 방화벽 기능을 적용하는 것이다. 이 때, TrusGuard의 에이전트는 별도로 설치할 필요가 없어(Agentless) 사용자 입장에서 보다 효율적으로 엔드포인트 - 네트워크 연계 보안을 운영할 수 있다.

EPP와 TrusGuard의 디바이스 기반 제어 운영 사례는 크게 ▲OS 버전 기준 제어 ▲보안 점검 점수 기준 제어 ▲V3 설치 여부 기준 제어가 있다.

1. OS 버전 기준 제어

기업에서 아직까지 Windows 7을 사용하는 단말이 있다고 가정해보자. Windows 7은 마이크로소프트(Microsoft)에서 지원을 종료한 버전으로 보안 이슈가 발생했을 때 패치가 어렵다. 그간 Windows 10으로의 이전이 상당 부분 진행되었지만, 부득이한 사정으로 혹은 파악이 되지 않은 채로 Windows 7을 계속 사용하는 경우가 있다.

먼저, EPP에서 Windows 7을 사용 중인 단말을 확인하면 TrusGuard와의 연동을 통해 Windows 7을 사용하는 PC에 대하여 내부 네트워크 접근은 허용하되 인터넷 접속을 차단하고 안티스팸 기능을 적용한다. 그리고, Windows 10 미만 버전을 사용하는 PC는 유해사이트와 C&C 연결을 차단할 수 있다. 만약 Windows 8이나 8.1을 사용하는 PC가 있다면 SSL Proxy(프록시)와 DLP 기능을 적용하는 것도 가능하다.



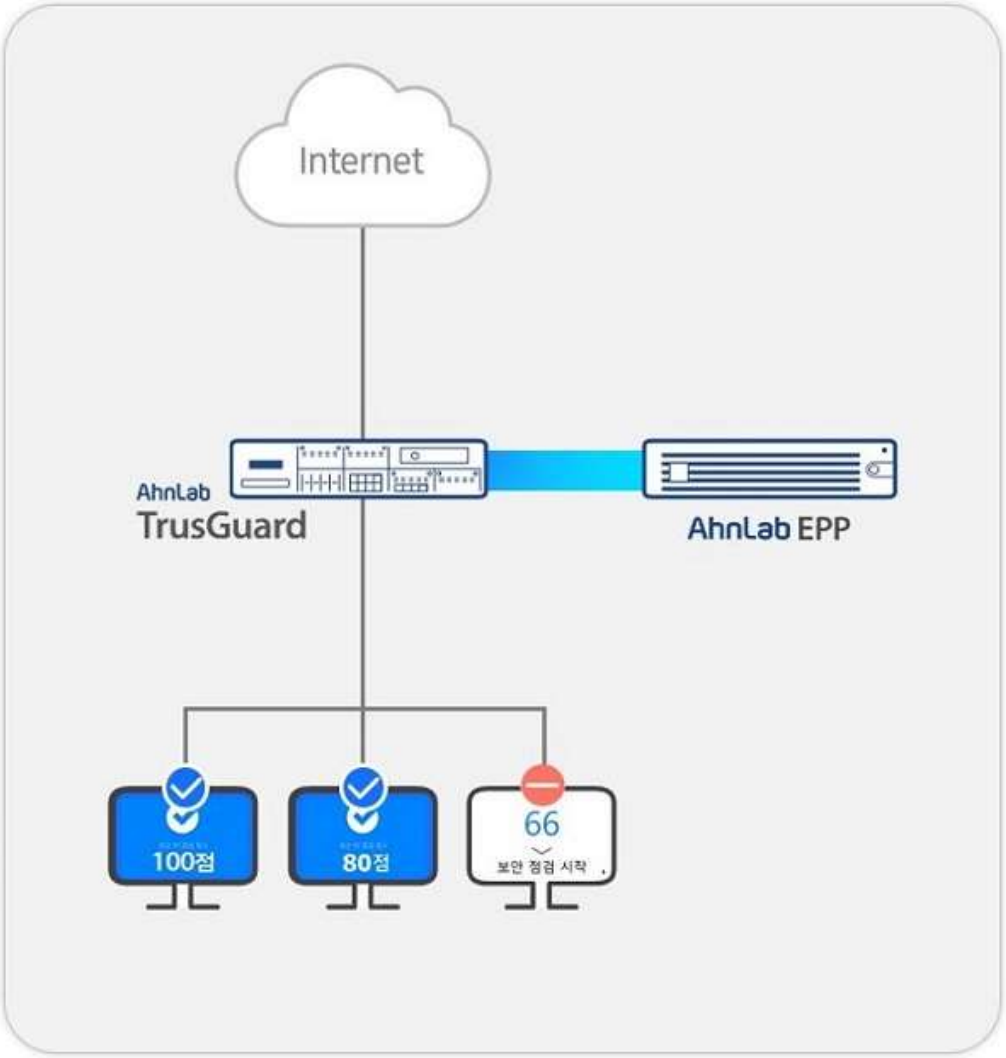
[그림 2] OS 버전 기준 제어

이 밖에, Windows 7을 사용하는 PC는 카카오톡의 메신저 기능만 허용하고 파일 업/다운로드는 차단하거나, Windows 10 미만 버전에 대해 원격 접속을 방지하고 Windows 8 PC의 경우 대역폭을 1Mbps, 세션 수를 1만개로 제한하는 것도 가능하다. 이처럼, 엔드포인트에서 확인된 OS 관련 보안 정보를 TrusGuard의 애플리케이션 및 디바이스 제어 기능과 연동하여 탁월한 보안 효과를 누릴 수 있다.

B. 보안 점검 점수 기준 제어

EPP의 구성 솔루션 중에는 취약 PC 점검 및 조치를 수행하는 'AhnLab ESA (이하 ESA)'가 있다. ESA를 활용하면 엔드포인트 단에서 보안 점검 결과와 점수 현황을 파악할 수 있게 된다. 이를 '보안 지수화'라고도 한다. 엔드포인트의 보안 지수를 TrusGuard와 연계하고 점수가 특정 수준 이하라면 네트워크 단에서 TrusGuard를 통해 여러 활동들을 제한하여 엔드포인트를 안전하게 보호하는 것이 보안 점검 점수 기준 제어의 핵심이다.

이를 테면, ESA 점검 결과 보안 점수가 100점인 PC는 모든 네트워크에 접근을 허용한다. 다만, 보안 점수가 80점 이하인 PC는 주요 퍼블릭 클라우드(AWS, Azure, GCP)로의 접근을 제한하고, 70점 미만인 경우에는 AhnLab MDS 연동 기능 활성화하여 악성 파일 유입과 악성 추정 URL 접속을 차단하는 정책을 적용할 수 있다.



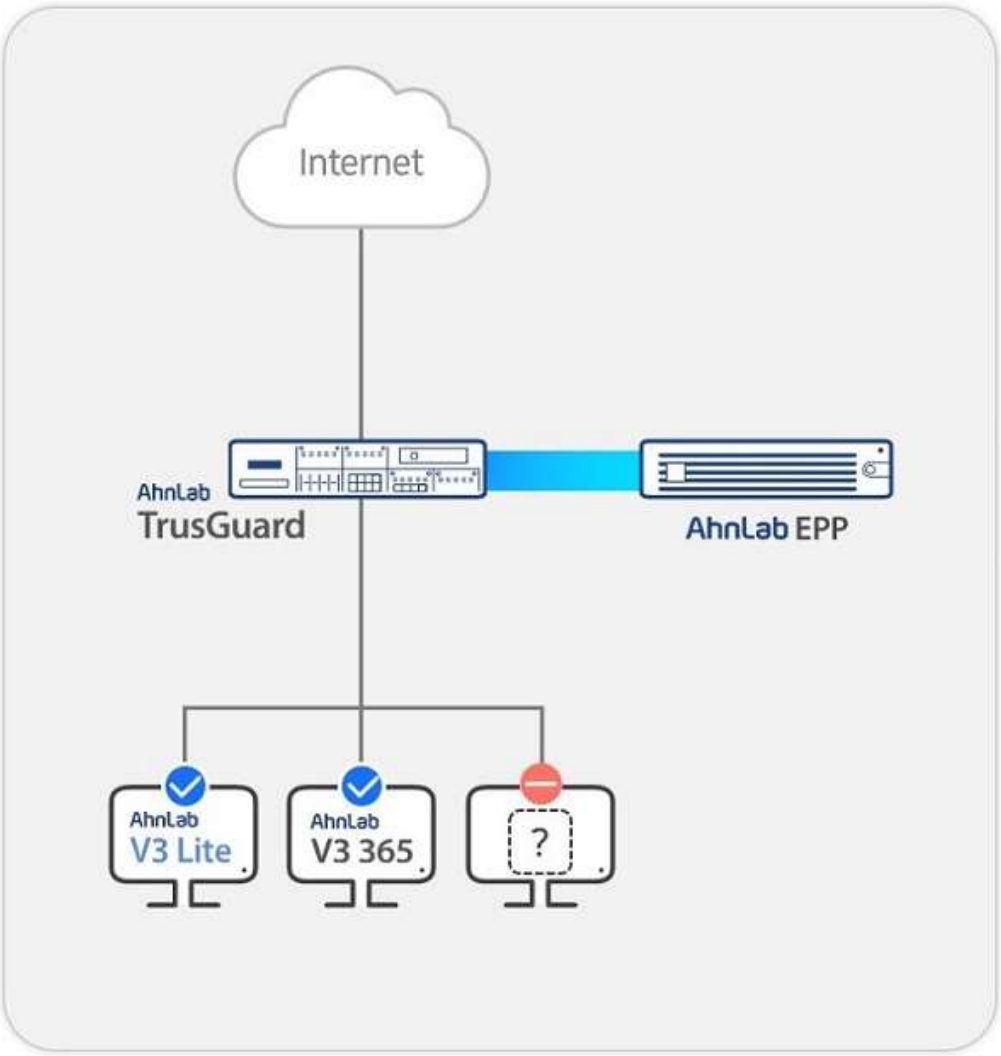
[그림 3] 보안 점검 점수 기준 제어

조금 더 낮은 점수를 보면 60점 미만 PC는 업무 시간 이외에는 사내 결제 시스템 외 모든 네트워크 접근 차단하고, 50점 이하인 경우 대역폭을 10Kbps로 제한하는 등 보안 점수를 기준으로 유효한 연계 정책을 적용해 보안을 강화할 수 있다.

C. V3 설치 여부 기준 제어

V3 설치 여부를 기준으로 단말을 제어하는 것은 본 운영 사례의 가장 기본이라 할 수 있다. 기업에서 보안 담당자가 관리하는 임직원의 PC가 다수가 아니라면 수동으로도 관리가 가능하다. 하지만, 그 수가 천 단위 혹은 만 단위가 되면 기본적인 백신 프로그램이 설치되지 않은 PC들이 종종 발견된다.

EPP는 정책 적용을 통해 V3 설치를 강제할 수 있다. 하지만, 해당 정책이 적용되어 있지 않은 경우에 여러가지 이유로 백신이 설치되지 않은 PC가 존재한다. 이 때 V3 설치 여부를 파악하고 설치되어 있지 않은 단말에 대해서는 TrusGuard와 연동해 네트워크 차단 혹은 부분적 허용 등을 적용할 수 있다.

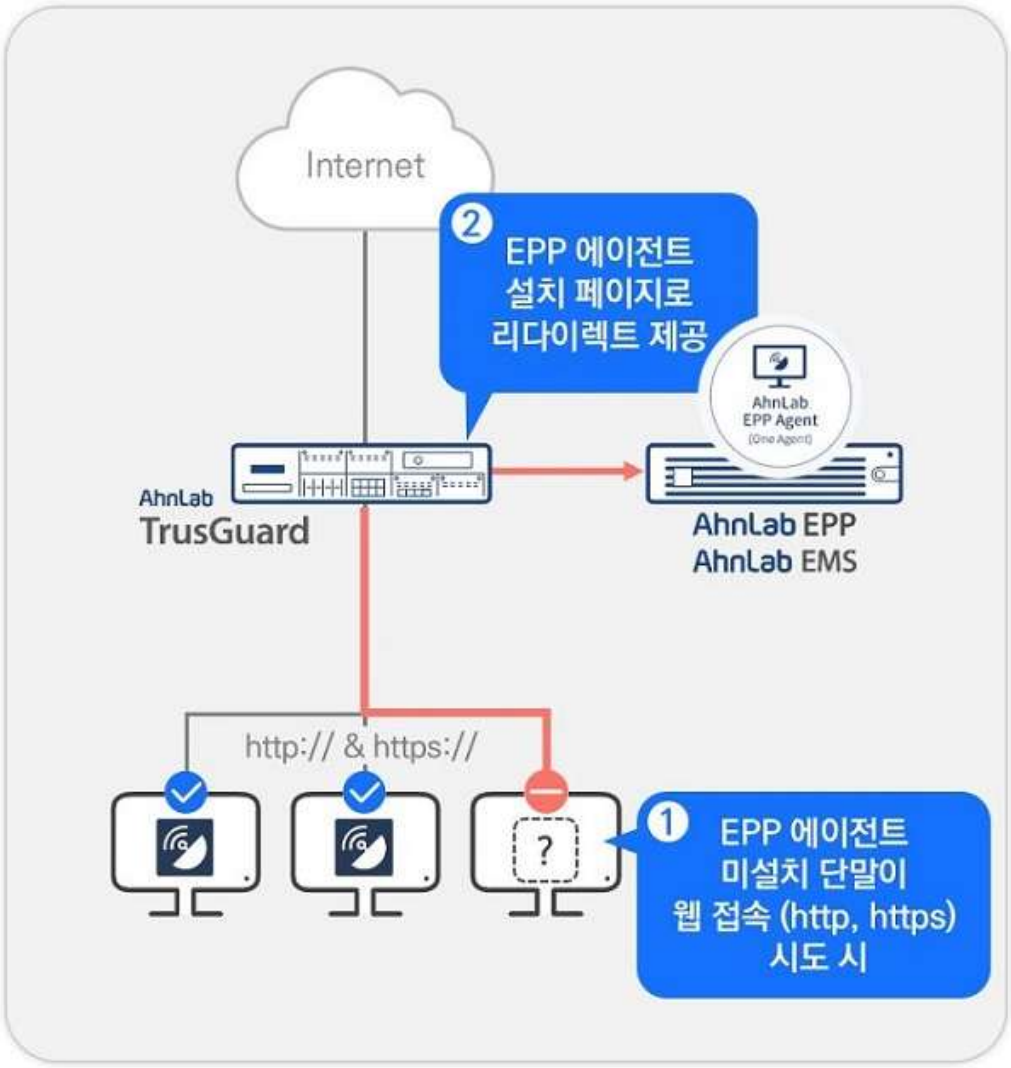


[그림 4] V3 설치 여부 기준 제어

세부적인 적용 방안은 위 두 가지 사례와 유사하다. V3 설치 PC에 대해서만 특정 외부 사이트로의 접근을 허용할 수 있고, 메신저 서비스의 경우에도 V3 미설치 PC는 접근을 차단하고 설치 PC는 카카오톡 파일 업/다운로드를 허용할 수 있다. 또, V3 미설치 PC는 침입방지시스템(IPS), 웹필터, 안티스팸, 유해사이트 차단 등 보안 위협 대응 기능을 모두 적용하는 등 V3 설치 여부에 따라 다양한 정책 적용이 가능하다.

EPP & TrusGuard 연동사례 2: EPP 에이전트 리다이렉트

EPP 에이전트 리다이렉트 기능은 EPP 에이전트가 설치되지 않은 PC가 인터넷 통신을 할 경우, 에이전트 설치를 유도하여 보안성을 확보할 수 있도록 한다. 동작 원리를 살펴보면, EPP 에이전트 미설치 PC가 인터넷 통신을 시도하면 TrusGuard에서 해당 트래픽을 EPP 서버로 리다이렉트하고, EPP 서버에서 에이전트 설치 유도 페이지를 안내한다. 이후, EPP 에이전트가 설치된 PC만 네트워크를 사용하도록 할 수 있다.



[그림 5] EPP 에이전트 리다이렉트

사용자 입장에서 보면, EPP 신규 도입을 계획하거나 사용 중인 상황에서 HTTPS 웹 접속에 대해서도 EPP 에이전트 리다이렉트 기능을 원하는 경우 효과적이다. TrusGuard는 HTTP와 HTTPS 모두에 대해 해당 기능을 제공하기 때문이다. 또, 네트워크가 NAT(Network Address Translation) 환경이라 EPP 에이전트 리다이렉트가 불가능한 경우에도, TrusGuard를 NAT 장비로 사용하면 문제가 해결된다.

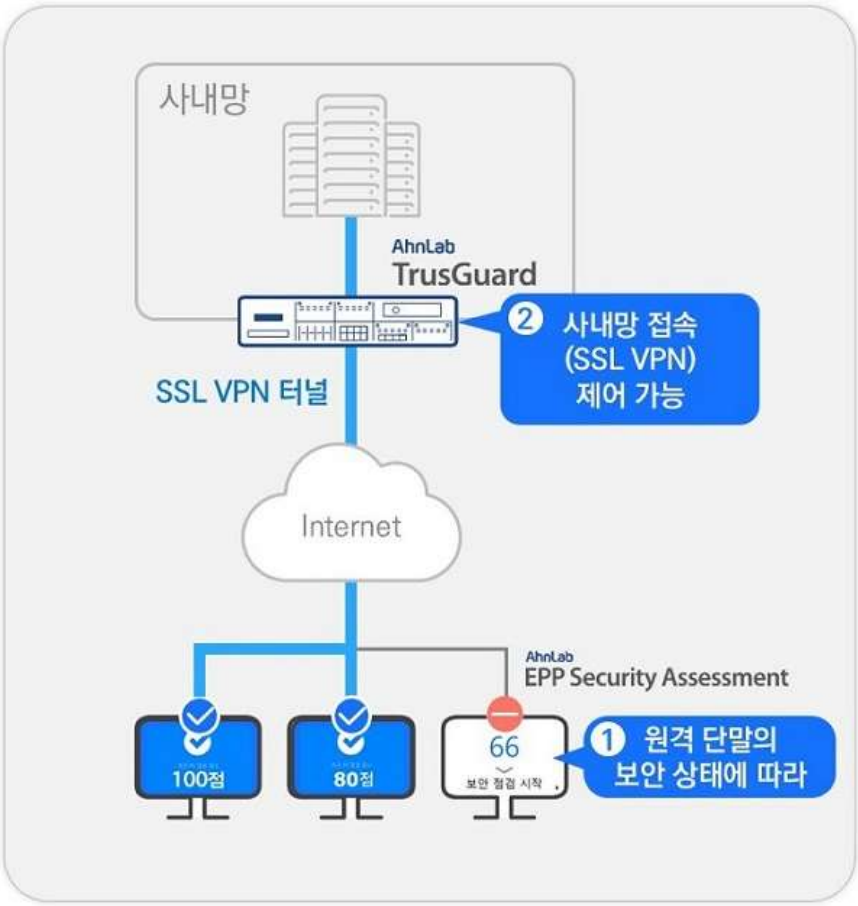
또한, 해당 기능은 TrusGuard의 모든 라인업에서 제공하므로, 오직 리다이렉트 기능만 필요하고 고가의 방화벽 추가 도입이 어려운 사용자도 최하위 모델인 TrusGuard 40B로 비용 부담을 최소화할 수 있다는 장점이 있다.

EPP & TrusGuard 연동사례 3: SSL VPN – ESA 연동

코로나19 팬데믹 이후 두드러진 변화 중 하나가 바로 재택 근무의 활성화다. 다만, 외부에서 내부 시스템으로 접속하는 재택 근무의 특성에 부합하는 보안 체계 수립이 필요해졌고 이는 많은 조직들이 지속적으로 고민하고 있는 부분이기도 하다.

재택 근무 시에는 안전한 사내망 접속을 위해 기본적으로 SSL VPN이 적용된다. SSL VPN은 외부 단말이 사내망에 있는 업무 시스템에 접속할 때 2-Factor 인증을 거쳐 암호화 통신을 하게 되어 있다. 다만, SSL VPN 자체에만 보안을 의존해서는 안된다. SSL VPN을 활용하더라도 외부 단말이 악성코드에 감염되거나 해커에 의해 장악되어 있다면 큰 의미가 없다. 따라서, 내부 시스템에 접근하는 원격 단말 자체의 보안을 점검하는 것이 굉장히 중요하다.

안랩은 EPP 구성 솔루션인 ESA와 TrusGuard의 SSL VPN을 연동하여 안전한 단말에 대해서만 원격 접속을 허용할 수 있도록 한다. 동작 원리를 간단히 살펴보면, TrusGuard의 SSL VPN 클라이언트가 단말의 보안 점검 점수를 확인하여, 관리자가 설정한 점수를 충족할 경우에만 SSL VPN 로그인이 가능하도록 제어한다. 이를테면, 보안 점검 점수 90점을 넘는 경우에만 접속이 가능하도록 하는 정책을 적용하는 것이다. 또, ESA 점검 점수를 분 단위로 판단하여 실시간성까지 보장한다.



[그림 6] SSL VPN – ESA 연동

사용자 입장에서는 '안전한 단말과 암호화 통신'을 통해 안정적으로 업무를 수행할 수 있게 된다. 특히, 금융권의 경우에는 '전자금융감독규정 시행세칙'에 따라 원격접속 시 보안조치 사전 검사가 의무화되어 있으며, 이 때 안랩의 솔루션을 활용하면 규제를 효과적으로 준수하는 동시에 안전한 보안 환경을 조성할 수 있다.

비단 금융권 뿐만 아니라 다른 업종 역시 마찬가지로, 재택 근무자의 사내망 접속 단말 대부분이 개인용 PC이며 이에 대한 보안 적용과 관리가 불가능할 때, 혹은 다른 여러 원격 근무 상황에서 최소한의 단말 보안에 대한 점검 후 사내망 접속을 허용하고자 하는 경우 효과를 볼 수 있다.

결론

최근, 특히 코로나19 팬데믹 이후 보안 지형은 ▲위협 고도화 ▲보안 복잡성 심화 두 가지로 요약할 수 있다. 풀어보면, 공격 방식이 고도화되는 가운데 기업들은 많은 솔루션들을 도입하고 또 많은 것들을 분석해야 하는 보안 복잡성을 마주하고 있다는 뜻이다.

이 두 가지 도전과제를 효과적으로 해결할 수 있는 전략이 바로 통합 보안이다. 이번 글에서 살펴본 엔드포인트 – 네트워크 보안 운영 사례와 같이 조직들이 통합 보안 전략을 올바르게 적용한다면 보다 강력하면서도 효율적인 보안 체계를 구축해 안정적인 비즈니스 환경을 조성할 수 있다.

이는 안랩이 가장 심혈을 기울이고 있는 부분이기도 하다. 안랩은 엔드포인트, 네트워크 뿐만 아니라 클라우드 그리고 전체적인 보안 운영까지 각 영역에서의 보안 역량들을 연계해 시너지를 내고 관리 편의성을 높이는 '연계형 통합 보안 플랫폼(Unified Security Platform)'을 구현하기 위해 계속해서 진일보하고 있다.

포스트 팬데믹 보안 전략을 고심하고 있는 많은 기업들이 올바른 통합 보안 체계를 구축하여 장기적인 비즈니스 경쟁력을 제고해 나가길 바란다.

AhnLab 콘텐츠기획팀 신재만 대리