TREND MICRO 트렌드마이크로

트렌드마이크로

티핑포인트® 위협 방어 시스템

실행력 있는 보안 인텔리전스를 통한 포괄적인 네트워크 보안

위협 환경은 정교함과 기술적 측면에서 끊임없이 발전을 거듭하고 있습니다. 따라서 이러한 동적인 위협 환경에 적응하라면 효과적이고 유연한 보안 시스템이 필요합니다(네트워크의 요구에 맞게 보안을 사용자 지정할 수 있는 시스템). 네트워크 보안 플랫폼은 현재와 미래의 지능형 네트워크 보안 기능의 기반이 되므로 신중하게 결정해야 합니다. 변화하는 위협 환경 속에서 네트워크 보안의 중요성이 계속 높아짐에 따라 보안 구현도 점차 힘든 과제가 되어가고 있습니다.

트렌드마이크로 티핑포인트 위협 방어 시스템(TPS)는 고도의 정확성으로 취약점을 보호하고 익스플로잇을 차단하며 알려진 공격 및 제로데이 공격을 방어하는 포괄적인 위협 방어 기능을 제공하는 강력한 네트워크 보안 플랫폼입니다. 뛰어난 유연성 및 우수한 성능과 함께 지능형 위협, 멀웨어 및 피싱 등의 다양한 위협 벡터들에 대한 가장 폭넓은 커버리지를 제공합니다. TPS는 심층 패킷 검사, 위협 레퓨테이션 및 지능형 멀웨어 분석과 같은 여러 기술들을 결합하여 네트워크에 공격이 발생할 때마다 이를 탐지하여 방어합니다. TPS를 통해 기업들은 사전 대응식 보안을 구축하여 포괄적으로 상황을 인식하고 네트워크 트래픽을 심층 분석할 수 있습니다. 이러한 완전한 상황 인식 기능이 디지털 백신 랩(DVLabs)의 위협 인텔리전스와 결합되어 현대의 동적이며 끊임없이 발전하는 기업 네트워크의 요구 사항을 수용할 수 있는 민첩성과 가시성을 제공합니다.

주요 이점

알려진 멀웨어 및 알려지지 않은 멀웨어 무력화: 알려진 멀웨어 및 알려지지 않은 멀웨어들의 공격 시도를 탐지하여 능동적으로 차단합니다.

뛰어난 가시성: 암호화된 트래픽을 포함한 모든 유형의 트래픽을 모니터링하여 공격을 탐지하여 저지합니다.

네트워크 안정성: 공격 하에서도 고성능을 발휘하도록 설계된 기능들이 탑재된 특수 제작된 하드웨어에 배포됩니다.

업계 선두의 위협 인텔리전스: 귀사의 자산을 표적으로 하는 최신 위협에 대응하기 위해 업계 선두의 연구팀과 협력합니다.

포괄적인 보안 솔루션: 네트워크 보안, 지능형 위협 및 사용자 보호 기능이 포함된 단일 업체 솔루션

주요 특징

On-box SSL
암호화된 트래픽으로 인해 생기는 보안 사각지대가 줄어듭니다.

머신 러닝이 실시간으로 익스플로잇 킷 차단
머신 러닝 기법으로 개발된 통계 모델을 통해 익스플로잇 킷을 실시간으로 탐지하여 처리합니다.

기업 취약점 치료(eVR)
고객들이 여러 취약점 관리 및 사고 대응 업체로부터 정보를 수집하고 CVE(Common Vulnerabilities and Exposures)를 티핑포인트 디지털 백신 필터에 매핑시켜 즉각적인 조치를 취할 수 있습니다.

고가용성
TPS는 다양한 손상 보호(fault tolerant) 기능을 갖추고 있기 때문에 핫 스왑 전원 공급, 빌트인 검사 우회 및 제로 출력 고가용성(ZPHA)을 포함한 인라인 배포에 이상적입니다.

통합 보호
TPS 패밀리는 티핑포인트 지능형 위협 방어(TippingPoint Advanced Threat Protection)와 통합되며 NSS 랩이 추천하는 가장 효과적인 위협 탐지 시스템으로 선정되었으며 표적 공격과 지능형 위협을 탐지하여 차단합니다.

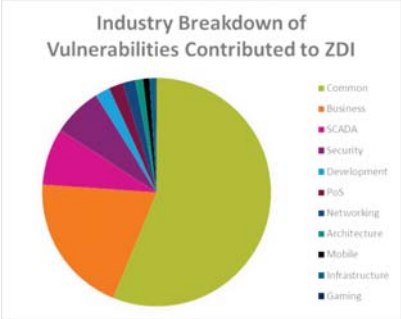
민첩성과 유연성
티핑포인트 TPS는 하드웨어이건 혹은 가상화 환경이건, 네트워크가 어디로 이동을 하건 상관없이 상시 네트워크를 보호하도록 설계되었습니다.

운영 편의성
티핑포인트 보안 관리 시스템은 정책 및 기기 관리를 한 곳에서 관리할 수 있습니다.

가상 패칭
알려진 위협들을 차단하는 강력하고 확장이 가능한 전방 방어 메커니즘으로 취약점 기반 필터를 이용하여 특정 취약점에 대한 모든 공격을 효과적으로 방어합니다.

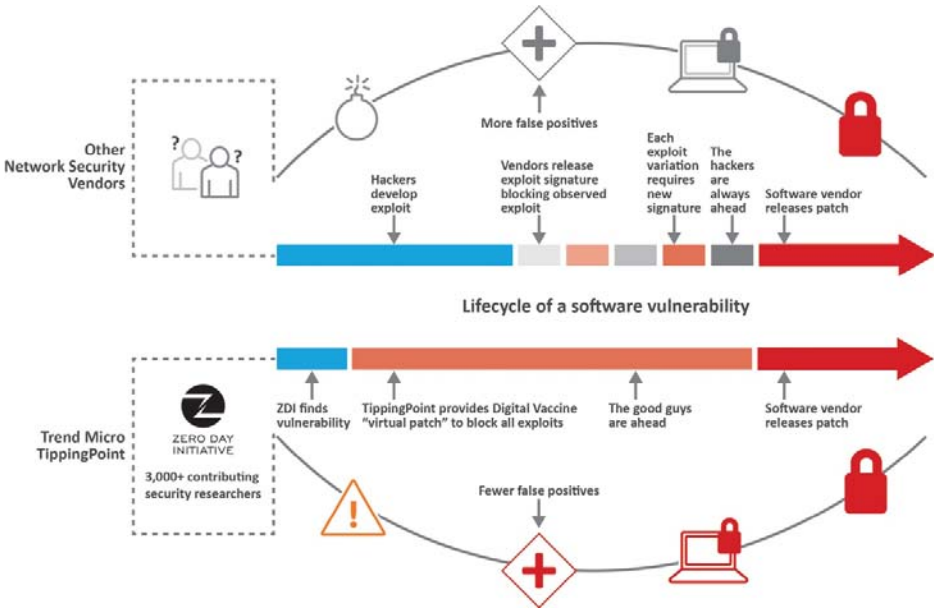
보안 효과

보안 팀의 가장 중요한 해결 과제 중 하나는 네트워크 무결성을 손상시키지 않으면서 위협 상황을 사전에 관리하는 것입니다. 끊임없이 진화하는 위협 환경에 뒤쳐지지 않기 위해 네트워크 보안 플랫폼은 제로데이 위협에 대처할 수 있는 사전 대응식 위협 프레임워크를 구현해야 합니다. TPS는 이러한 번거로운 프로세스를 사용이 편리한 정책 프레임워크와 권장 설정이 결합된 사전 대응식 위협 인텔리전스를 이용한 프로세스로 전환시킵니다. 그리고 자동 업데이트 기능을 통해 최소한의 수작업으로 즉각적이며 지속적인 위협 보호를 구현할 수 있습니다.



보안 효과를 측정할 수 있는 또 다른 측면은 대응 시간입니다. 이 수치는 새로운 위협들을 얼마나 신속하게 탐지할 수 있는지 그리고 이러한 위협들로부터 조직을 보호하기 위해 어떤 조치를 취할 수 있는 지를 반영합니다. 이 부문에서 티핑포인트의 디지털 백신(DVLabs) 팀과 제로데이 이니셔티브(ZDI)가 매우 중요한 역할을 합니다. 이들은 기존 및 새로운 위협들을 파악하고 예측하며 해결하기 위한 선행 조사에 주력합니다.
DVLabs의 내부 조사와 ZDI를 통해 티핑포인트는 고객들에게 지속적으로 업데이트된 보안 커버리지를 제공하며 필터를 통해 제로데이 취약점과 알려진 취약점을 파악합니다. 또한 익스플로잇을 수 개월 먼저 파악하여 보안 팀들에게 중요한 보안 정보를 제공합니다.

소프트웨어 취약점 라이프사이클



티핑포인트 ZDI는 2014년에 가장 많은 취약점을 탐지하였습니다(317건)

- Frost & Sullivan 2014 Public Vulnerability Research Market

ZDI 는 2015년 653건의 취약점을 탐지하였습니다

운영 편의성

다양한 보안 업체들과 SIEM, IDS, IPS, 방화벽 및 기타 어플라이언스의 도구들이 끊임없이 늘어나고 있습니다. 따라서 보안팀들은 네트워크 보안 제품들을 효과적으로 관리해야 하는 문제에 직면하게 되었습니다. 조직의 방어선 내, 코어 또는 데이터 센터와 하이브리드 네트워크(물리적 및 가상 어플라이언스)의 데이터 자산과 네트워크를 보호하려면 여러 경계를 초월하여 확장되는 관리 프레임워크가 필요합니다. 티핑포인트 보안 관리 시스템(SMS) 어플라이언스는 대규모로 배포된 제품들에 대한 통합된 관리 인터페이스와 광범위한 가시성 그리고 보안 정책 제어 기능을 제공합니다.

티핑포인트 보안 관리 시스템 대시보드

이 외에도 강력한 관리 기능과 유연한 물리적/가상 배포 옵션을 제공합니다. 트렌드마이크로 티핑포인트 보안 관리 시스템(SMS)은 트래픽 통계, 필터링된 공격, 네트워크 호스트 및 서비스에 대한 동향 보고서, 상관관계 분석 및 실시간 그래프, 티핑포인트 차세대 침입 방치 시스템(IPS)와 위협 방어 시스템(TPS)의 인벤터리 및 상태가 포함된 종합적인 분석이 가능합니다. 티핑포인트 SMS는 확장이 가능한 정책 기반의 운영 모델을 제공하고 배포된 수많은 IPS 및 TPS 제품들을 간편하게 관리할 수 있습니다.

사각 지대 관리: 암호화된 트래픽

SSL 암호화는 인터넷 보안을 보장하는 핵심 기술입니다. 이메일, 전자상거래, 음성통신(voice-over-IP), 온라인 뱅킹, 원격 진료 및 수 많은 서비스들이 SSL로 보호되고 있습니다. 정교한 표적 공격들도 점차 암호화를 이용하여 침입 방지 시스템의 탐지를 회피하고 있으며 이로 인해 기업들은 부담스러운 해결 과제에 직면하게 되었습니다. 실제로 일반 조직 내 모든 인터넷 트래픽의 25 – 35% 이상이 SSL 트래픽이며 매년 20% 가량 증가할 것으로 예상됩니다. 이로 인해 조직들의 보안 태세에 엄청난 공백이 생기게 됩니다. 티핑포인트 TPS는 동일한 관리 및 그래픽 인터페이스를 통해 네트워크 성능을 방해하지 않으면서 암호화된 SSL 트래픽을 검사하여 SSL 사각 지대를 제거합니다. 이로써 솔루션 관리가 간편해지고 IT 부서의 설정 및 관리 업무 부담이 최소화됩니다. 정책 기반의 제어 기능은 검사를 위해 해독하거나 해독하지 말아야 할 SSL 암호화 플로를 결정합니다. 이로써 개인 키 저장소와 SSL 인증서 관리가 통합되어 SSL 관리와 비용이 절감될 수 있습니다.

주요 이점

- On-box SSL은 전용 SSL 어플라이언스가 필요치 않습니다(관리해야 할 어플라이언스 감소)
- SSL은 고성능을 지원합니다
- 2K 키 지원

기능	2200T 1Gbps	2200T 2Gbps
IPS + SSL 처리량	500 Mbps + 500 Mbps	1.5 Gbps + 500 Mbps
동시 세션	40,000	40,000
초당 새로운 연결	1,200	1,200
보안 컨텍스트	40,000	40,000
SSL 키	2,048 bits	

유연하고 민첩하며 탄력적으로 확장되는 네트워크 보안

물리적 네트워크에서 가상 네트워크 세그먼트로 수요가 변화함에 따라 유연하고 강력한 보호 기능을 제공하는 물리적 및 가상 보안 시스템이 필요합니다. 티핑포인트 가상 위협 방어 시스템(vTPS)은 가상 폼 팩터 형태로 IPS 보호를 제공하므로 물리적, 가상 및 복합형 네트워크 환경을 유연하게 보호할 수 있습니다. TPS와 vTPS는 동일한 관리 시스템을 사용하기 때문에 혼합 환경을 관리하기가 훨씬 용이하며 포괄적인 보호를 위해 물리적/가상 환경 간에 정책과 설정을 공유합니다.

가상 위협 방어 시스템 성능 테스트는 CPU 아키텍처와 기타 요인들에 따라 다를 수 있습니다.	
기능	**티핑포인트** vTPS Standard Virtual Appliance TPNM0034
가상 플랫폼 지원	VMWare ESXi 5.5, 6.0
	NSX는 투명한 검사 및 실행이 필요치 않습니다
	KVM - Redhat Enterprise Linux 6, 7
네트워크 드라이버	VMWare - VMXNet3
	KVM - virtIO
논리적 코어 수	3 또는 4
필요 메모리	8 GB
필요 디스크 공간	16GB
가상 어플라이언스 사양	
성능	500Mbps검사 라이선스 포함
IPS 동시 연결	1,000,000
초당 새로운 연결	최대 120K VMware 최대 60K KVM
네트워크 세그먼트 수	1
가상 세그먼트 수	무제한
관리 포트	있음

TPS 기술 사양

기능	440T	2200T
IPS 검사 처리량	500 Mbps + 500 Mbps	1.5 Gbps + 500 Mbps
SSL 검사	불가능	가능
대기 시간	<100 마이크로 초	<100 마이크로 초
보안 컨텍스트	750,000	2,500,000
동시 세션	1,000,000	2,500,000
초당 새로운 연결	50,000	170,000
폼 팩터	1U	2U
무게	15.28 lbs. (6.93Kg)	26.26 lbs. (11.91Kg)
크기 (Wxdxh)	16.78 in.(W) x 17.3 in.(D) x 1.72 in.(H) 42.62 cm x 45.00 cm x 4.40cm	16.77 in. (W) x 18.70 in.(D) x 3.46 in.(H) 42.60 cm x 47.50 cm x 8.80 cm
관리 포트	1개의 대역 외 10/100/1000 RJ-45, 보안 관리 시스템, LSM HTTPS 웹 인터페이스, 명령줄, 티핑포인트 MIB을 통해 관리할 수 있는 1개의 RJ-45 시리얼 콘솔	
네트워크 연결성	8개의 10/100/1000 RJ-45 포트 1개의 10/100/1000 RJ-45 고가용성 포트	통합 우회를 지원하는 8개의 10/100/1000 RJ-45 포트 8 x 1G SFP 4 x 10G SFP+ 1개의 10/100/1000 RJ-45 고가용성 포트 SFP/SFP+를 위한 외부 ZPHA 지원
On-box 저장소	8 Gb 솔리드 스테이트 교체 가능한 CFast 플래시 드라이브	
전압	100-240 VAC, 50-60 Hz	
전류(max. fused power)	4-2 A	12-6 A
최대 소비 전력	250W(853 BTU/hour)	493W(1,682 BTU/hour)
전원 공급	싱글 픽스드(Single fixed)	듀얼 리던던트 핫 스왑
작동 시 온도	32°F to 104°F(0°C to 40°C)	
작동 시 상대 습도	5% to 95% 비응축식	
비 작동 시 저장소 온도	-4°F to 158°F(-20°C to 70°C)	
비 작동 시 저장소 상대 습도	5% to 95% 비응축식	
고도	최대 10,000 feet (3,048m)	
안전도	UL 60950-1, IEC 60950-1 EN 60950-1,CSA 22.2 60950-1 RoHS 규정 준수	
EMC	Class A, FCC, VCCI, KC EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2 EN61000-3-3, CE Marking	