CHECK POINT
SANDBLAST 어플라이언스

CHECK POINT

SANDBLAST 어플라이언스

알려지지 않은 새로운 위협의 차단

제품 특장점

- 문서 또는 실행 파일에서 새롭고 알려지지 않은 공격 방지
- 해커의 탐지 회피 시도를 사실상 무력화
- 기존 보안 인프라를 활용하여 비용 감소
- 관리, 모니터링, 보고서 통합으로 최고 수준의 보호 기능 제공
- 신규 공격 정보를 ThreatCloud™를 통해 자동 공유하여 보안 강화

제품 기능

- Adobe PDF, Microsoft Office, Java, 플래시, 실행 파일, 압축 파일 등 40 가지 이상의 파일 형식에서 신규 맬웨어 식별
- 다중 Windows OS 환경 대상 공격의 방어
- 1 개월에 10 만개부터 2 백만개까지 파일 검사를 수행할 수 있는 다양한 종류의 어플라이언스 제공
- 위협 추출(Threat Extraction) 기능을 통해 공격 가능 콘텐츠를 제거한 깨끗한 파일을 지연 없이 제공
- 독특한 CPU 수준의 기술을 통해 배포되거나 탐지를 회피하기 전에 맬웨어를 식별

현황

사이버 위협은 갈수록 교묘해지고 있으며, 많은 소프트웨어 취약점을 이용한 표적 공격이 다운로드 된 파일 또는 이메일 첨부 파일을 통해 발생하고 있습니다.

이러한 위협은 거의 매일 새로운 공격 형태 또는 기존 공격의 변형 형태로 나타나고, 이 같은 신규 및 변형 공격에는 아직 시그니쳐가 존재하지 않기 때문에 전통적인 보안 솔루션으로는 탐지가 불가능합니다. 이제 신규 및 변형 공격의 탐지를 위해 이미 알려진 위협 시그니쳐에 의존하지 않는 새로운 솔루션이 필요합니다.

솔루션

Check Point SandBlast 제로-데이 보호(Zero-Day Protection) 기능은 탐지 회피 맬웨어를 찾아내어 치명적인 위협으로부터 포괄적인 보호 기능을 제공하면서도 사용자에게 안전한 콘텐츠를 신속하게 제공합니다. 솔루션의 핵심은 2 개의 독특한 기능인 위협 에뮬레이션(Threat Emulation)과 위협 추출(Threat Extraction) 기능으로, 다음의 위협 방어 기능을 수행합니다.

Check Point SandBlast 솔루션의 일부분인 위협 에뮬레이션(Threat Emulation) 엔진은 해커가 맬웨어에 샌드박스를 우회하는 회피기술을 적용했다 하더라도 수행 단계에서 맬웨어를 찾아냅니다. 파일을 신속하게 격리하고 조사한 후, 가상 샌드박스에서 실행하는 방식으로 악의적인 코드를 네트워크 침투 전에 탐지합니다. 이 혁신적인 솔루션은 CPU 수준의 명령어 조사와 OS 수준의 샌드박스 조사를 결합하여, 치명적인 취약점 공격과 제로-데이(Zero-Day) 공격, 표적 공격을 방지합니다.

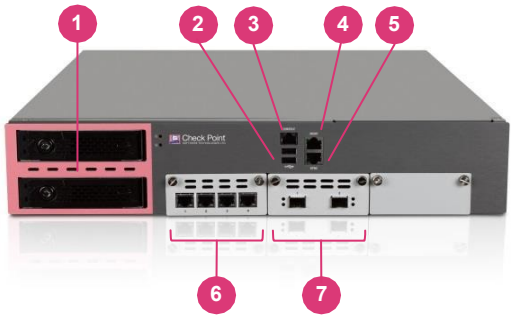
또한, SandBlast 위협 추출(Threat Extraction) 기능은 잠재적 위협이 내재된 콘텐츠의 안전 버전을 사용자에게 즉시 제공합니다. 파일에서 활성 콘텐츠와 다양한 유형의 내장 오브젝트를 포함한 모든 공격 가능 콘텐츠를 끄집어낸 후 파일을 재구성함으로써 잠재적 위협을 제거합니다. 의심스러운 원본 버전에 대한 접근은 SandBlast 제로-데이 보호(Zero-Day Protection) 기능에 의해 완전히 분석될 때까지 차단됩니다. 사용자는 콘텐츠에 즉시 접근할 수 있고, 가장 진보된 맬웨어 또는 제로-데이(Zero-Day) 위협으로부터 안전하게 보호받고 있다는 확신을 가질 수 있습니다.

SANDBLAST 어플라이언스

다양한 종류의 SandBlast 어플라이언스가 제공됩니다. 이 제품들은 규제 또는 내부 사정으로 클라우드 기반의 SandBlast 위협 에뮬레이션(Threat Emulation) 서비스를 이용할 수 없는 고객에게 적합합니다.

TE1000X SandBlast 어플라이언스 예시

1. 2 x 2 TB 하드디스크
2. 2 x USB 포트
3. 콘솔 포트
4. 10/100/1000Base-T 관리 포트
5. 10/100/1000Base-T Sync 포트
6. 4 x 10/100/1000Base-T 포트
7. 2 x 10GBase-F SFP+ 포트



배포 옵션

두 가지 배포 옵션으로 위협 에뮬에이션을 수행할 수 있습니다.

1. 프라이빗 클라우드: Check Point 보안 게이트웨이가 파일을 SandBlast 어플라이언스로 전송하여 에뮬레이션을 수행합니다.
2. 인라인: 독립 실행형 옵션으로, SandBlast 어플라이언스가 인라인 혹은 SPAN 포트에 설치되어 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 소프트웨어 블레이드 역할을 수행함으로써 네트워크 통신을 보호합니다.

포괄적 위협 방지

SandBlast 어플라이언스는 안티 바이러스 및 안티-봇, 샌드박스를 이용한 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction) 기술을 이용하여 알려졌거나 아직 알려지지 않은 위협 모두를 방지합니다.

SANDBLAST 제로-데이(ZERO-DAY) 위협 방어

SandBlast 위협 에뮬레이션(Threat Emulation) 기술은 가장 빠르고 정밀한 샌드박스 엔진을 이용하여 파일을 사전에 차단함으로써, 공격자가 네트워크에 침입하기 전에 조직을 공격으로부터 보호합니다.

알려진 위협 탐지

안티바이러스 소프트웨어 블레이드는 ThreatCloud™로부터 전송 받은 실시간 바이러스 시그니쳐를 사용하여 게이트웨이에서 맬웨어를 탐지함으로써, 사용자에게 영향을 미치기 전에 맬웨어를 차단합니다.
안티-봇 소프트웨어 블레이드는 봇이 감염된 머신을 탐지하고, 봇의 명령 및 제어 통신을 차단함으로써 피해를 방지합니다.

탐지 회피의 감지

전통적인 샌드박스 솔루션은 OS 수준에서 맬웨어를 탐지하는데, 이는 해커가 작성한 코드가 이미 실행되어 공격이 시작된 이후에 수행됩니다. 따라서 맬웨어는 탐지를 회피할 수 있습니다.

SandBlast 위협 에뮬레이션(Threat Emulation) 기능은 CPU 수준에서 명령어 흐름을 주시하여, 공격 코드가 OS 보안 제어를 우회하는 것을 방지하고 실제 실행되기 전에 공격을 효과적으로 차단하는 독특한 CPU 수준의 탐지 엔진을 사용합니다.

능동적 방어와 안전한 콘텐츠의 신속한 전달

위협을 방지함에 있어 속도와 범위, 정확도 중 어느 하나도 포기할 필요가 없습니다. 타 솔루션과 달리 Check Point 제로-데이 보호(Zero-Day Protection) 기능은 비즈니스 흐름을 전혀 방해하지 않는 방지 모드로 설치 가능합니다.

SandBlast 위협 추출(Threat Extraction) 기능은 파일에서 활성 콘텐츠와 내장 오브젝트를 포함한 모든 공격 가능 콘텐츠를 삭제하고, 잠재적인 위협을 제거한 후 재구성한 안전한 콘텐츠를 사용자에게 즉시 제공하므로, 비즈니스 흐름에 전혀 영향이 없습니다.

위협 추출(Threat Extraction) 기능 구성 방식은 두 가지가 있습니다. 사용자에게 재구성된 문서를 빠르게 제공하는 방식, 또는 SandBlast 위협 에뮬레이션(Threat Emulation)의 응답을 받은 후 문서의 재구성 여부를 결정하는 방식 중 하나를 사용합니다.

암호화된 통신 검사

SSL 또는 TLS 통신을 통해 전송되는 파일은 대다수의 업계 표준 솔루션을 우회하는 공격 요소 중 하나입니다. Check Point Threat Prevention 은 이러한 암호화된 SSL 또는 TLS 터널로부터도 파일을 추출하여 실행함으로써 숨겨진 위협을 탐지해 냅니다.

위협 에뮬레이션(THREAT EMULATION) 상세 보고서

모든 파일의 에뮬레이션 후 상세 보고서가 생성됩니다. 보고서는 이해하기 쉽도록 단순하게 구성되어 있고, 파일의 실행으로 발생한 악의적인 시도를 조사하는데 필요한 상세 정보를 포함하고 있습니다. 보고서에는 파일이 실행되는 시뮬레이션 환경의 실제 스크린샷이 포함되어 있습니다.

THREATCLOUD 에코시스템

위협 에뮬레이션(Threat Emulation)에서 새로운 위협이 발견되면 신규 시그니쳐가 생성되어 Check Point ThreatCloud 로 전송되고, 이 시그니쳐는 다른 게이트웨이에 연결된 Check Point 에 배포됩니다. 위협 에뮬레이션(Threat Emulation) 기능은 새로 식별된 알려지지 않은 위협을 알려진 시그니쳐로 변환함으로써, 위협이 광범위하게 유포되는 것을 방지합니다. 이러한 끊임 없는 협력 시스템을 통해 ThreatCloud 에코시스템은 최신 정보를 가진 가장 진보된 위협 정보 네트워크로서의 입지를 확고히 구축할 수 있습니다.

기술 규격

	TE100X	TE250X	TE1000X	TE2000X / TE2000X HPP
				
성능				
권장 파일 수 (개월 당)	10 만개	25 만개	100 만개	150 만개 / 200 만개
권장 사용자 수	1 천명까지	3 천명까지	1 만명까지	2 만명까지
처리량	150 Mbps	700 Mbps	2 Gbps	4 Gbps
가상 머신 수	4	8	28	40 / 56
하드웨어				
스토리지	1 TB HDD		이중화되고 핫스왑 가능한 2 TB HDD, RAID1	
LOM	포함되지 않음			
슬라이드 레일 (22-32 인치)	포함			
네트워크				
10/100/1000Base-T RJ45	5	9	6	6
10GBase-F SFP+	-	-	2	4
확장 슬롯	사용하지 않음			
크기 및 무게				
케이스	1U	1U	2U	2U
미터 (너비 X 깊이 X 높이)	435 x 448 x 44 mm	438 x 621 x 44 mm	438 x 561 x 88 mm	
인치 (너비 X 깊이 X 높이)	17.13 x 17.64 x 1.63 인치	17.25 x 24.45 x 1.73 인치	17.24 x 22.1 x 3.46 인치	
무게	7.7 kg (16.9 파운드)	9.8 kg (21.6 파운드)	17.05 kg (37.6 파운드)	
환경				
운영	32º ~ 104ºF / 0º ~ 40ºC, (20~90%, 비응축식)			
보관	-14° ~ 158°F / -10° ~ 70°C, (20%~90% 비응축식)			
전원				
이중화, 핫스왓 가능	-	선택 사항	포함	
AC 전압:	100-240V			
진동수	47-63 Hz			
단일 전원 공급 장치 용량	250W	400W	400W	400W
최대 전력 소비량	50.4W	104W	225.6W	
최대 발열량	172.2 BTU/h	355.7 BTU/h	771.5 BTU/h	
인증				
보안	CB, UL, Multiple Listing, LVD, TUV			
배출	FCC, CE, VCCI, RCM			
환경	RoHS			

어플라이언스 패키지

기본 구성 [1]	
TE100X SandBlast 어플라이언스와 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 1 년 서비스 (4 개 가상 머신의 Microsoft Windows 및 Office 라이선스 포함)	CPAP-TE100X-4VM
TE250X SandBlast 어플라이언스와 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 1 년 서비스 (8 개 가상 머신의 Microsoft Windows 및 Office 라이선스 포함)	CPAP-TE250X-8VM
TE1000X SandBlast 어플라이언스와 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 1 년 서비스 (28 개 가상 머신의 Microsoft Windows 및 Office 라이선스 포함)	CPAP-TE1000X-28VM
TE2000X SandBlast 어플라이언스와 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 1 년 서비스 (40 개 가상 머신의 Microsoft Windows 및 Office 라이선스 포함)	CPAP-TE2000X-40VM
TE2000X HPP SandBlast 어플라이언스와 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 1 년 서비스 (56 개 가상 머신의 Microsoft Windows 및 Office 라이선스 포함)	CPAP-TE2000X-56VM-HPP
소프트웨어 블레이드 패키지 [1]	
TE100X 어플라이언스를 위한 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 연간 서비스	CPSB-TE-100-1Y
TE250X 어플라이언스를 위한 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 연간 서비스	CPSB-TE-250-1Y
TE1000X 어플라이언스를 위한 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 연간 서비스	CPSB-TE-1000-1Y
TE2000X 및 TE2000X HPP 어플라이언스를 위한 위협 에뮬레이션(Threat Emulation), 위협 추출(Threat Extraction), 안티 바이러스 및 안티-봇 연간 서비스	CPSB-TE-2000-1Y

[1] 2-3 년 서비스 상품도 있음 (온라인 제품 카탈로그 참고)

부품

인터페이스 카드 및 트랜시버	
10G 광 포트용 SFP+ 트랜시버 모듈 - LR (10GBase-LR)	CPAC-TR-10LR
10G 광 포트용 SFP+ 트랜시버 모듈 - SR (10GBase-LR)	CPAC-TR-10SR
예비 부품 및 기타	
TE250X 용 AC 전원 공급 장치	CPAC-PSU-TE250X
TE1000X 및 TE2000X 어플라이언스용 부품 교체 키트 (하드디스크 1 개와 전원 공급 장치 1 개 포함)	CPAC-SPARES-TE1000X/2000X

연락처

본사 | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | 전화: 972-3-753-4555 | 팩스: 972-3-624-1100 | 이메일: info@checkpoint.com

한국지사 | 서울특별시 영등포구 국회대로 62 길 21 동성빌딩 7 층 | 전화: 02-786-3303 | 팩스 02-761-9391 | krissl@checkpoint.com