Check Point
보안 웹 게이트웨이 어플라이언스

보안 웹 게이트웨이는 웹 맬웨어에 대한 실시간 다계층 보호, 가장 많은 어플리케이션을 제공하며, 세밀한 어플리케이션 제어, 집중적이고 직관적인 관리, 그리고 최종 사용자 교육을 통해 안전한 Web 2.0 사용을 지원하는 올인원 솔루션입니다.

Check Point는 20년 동안 최고의 보안 서비스를 제공하는 회사로서 끊임없이 변화하는 위협 환경으로부터 고객을 보호해왔습니다. 보안 웹 게이트웨이와 관련하여 Check Point는 조직에 가장 중대한 위협인 웹 맬웨어를 막기 위해 필요한 보호 기능을 제공하기 위해서 보안 전문성과 업계 최고의 완전한 보안 혁신 포트폴리오를 활용합니다.

이제 웹 액세스는 어느 곳에나 있으며 업무 현장의 가장 기본적인 "표준"으로 여겨집니다. 웹은 또한 기업 공격을 위한 지배적인 루트가 되었습니다. 공격자는 기업 사용자를 맬웨어에 감염된 웹사이트로 유도하는데, 최근의 Check Point 조사에 따르면 74%의 조직에서 호스트가 1시간 30분마다 악의적인 웹사이트에 액세스하고 있는 것으로 확인되었으며 이러한 위험은 직원이 고위험 어플리케이션을 사용할 때 더욱 심각해집니다. Check Point 조사에 따르면, 91%의 조직에서 사용자가 잠재적 보안 위험이 있는 어플리케이션에 액세스하고 있었습니다. 공격자의 공격이 더욱 정교해지면서 웹 맬웨어를 막아내는 데 보안 웹 게이트웨이의 역할이 매우 중요해졌습니다. 효과적인 보안 웹 게이트웨이는 가장 정교한 형태의 맬웨어를 막아내고 공격을 방지하기 위해 다계층 보안을 제공할 수 있어야 합니다.

개요

보안 웹 게이트웨이는 웹 맬웨어에 대한 실시간 다계층 보호, 가장 많은 어플리케이션을 제공하며, 세밀한 어플리케이션 제어, 집중적이고 직관적인 관리, 그리고 최종 사용자 교육을 통해 안전한 Web 2.0 사용을 지원하는 올인원 솔루션입니다. 이 솔루션은 다음과 같은 가장 강력한 웹 보안 기능을 결합하여 구축된 것입니다.

핵심 특징

- 안티바이러스, URL 필터링, 어플리케이션 제어, 사용자 인식, IPS 및 안티봇 블레이드를 통한 분석과 보고를 통합한 전용 어플라이언스
- 클라우드 기반 카테고리제이션의 실시간 URL 업데이트
- 6900개 이상의 웹, 24만 개의 위젯, 130개의 카테고리를 포함한 최대의 앱 라이브러리
- 웹의 모든 측면에 대한 통일된 보안
- 정책과 보고에서 사용자와 사용자 그룹 세밀도
- ThreatCloud™ 글로벌 보안 인텔리전스를 통해 맬웨어를 차단하기 위한 다계층 보안
- 세밀한 보고서와 포렌식 도구를 사용한 직관적인 이벤트 분석

핵심 특장점

- 다계층 보안을 통한 맬웨어 감염 및 감염 후 손상 예방
- 맬웨어 감염 웹사이트와 위험도가 높은 어플리케이션에 대한 액세스 제어
- 브라우저 및 어플리케이션 취약성 공격 방지
- 통일된 집중식 관리의 운영 활동 강화
- 통일된 제어, 강화 및 보고를 통해 웹 기반 활동을 보호하는 유일한 솔루션의 특장점

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

- 정교한 맬웨어를 식별하고 차단하기 위한 안티바이러스
- 맬웨어를 식별하기 위한 ThreatCloud의 글로벌 보안 인텔리전스
- 수백만 개의 맬웨어 및 피싱 웹사이트에 대한 액세스를 제어하기 위한 URL 필터링
- 위험한 앱이나 특정 기능의 사용을 막기 위한 세밀한 어플리케이션 제어
- 웹 중심 사이버 공격에 맞서 싸우기 위한 IPS와 안티봇
- 모든 웹 사용자와 활동에 대한 360도 가시성을 위한 SmartEvent
- 모든 웹, 어플리케이션, 사용자 및 머신을 커버하는 통일된 정책

Check Point의 보안 웹 게이트웨이 솔루션에는 지사와 소기업, 중기업, 대기업 및 초대형 기업에 적합한 다양한 모델과 함께 제공되는 독립형 전용 어플라이언스와 모든 보안 게이트웨이에서 사용할 수 있는 안전한 웹 소프트웨어 패키지를 포함하고 있는 유연한 설치 옵션이 있습니다.

보안 웹 게이트웨이 특징

안티바이러스

사이버 범죄에 맞서기 위한 최초의 협업 네트워크인 ThreatCloud의 실시간 바이러스 시그니처와 변칙 기반 보호 기능을 이용해서 악성 파일이 사용자에게 영향을 주기 전에 게이트웨이에서 파일 유입을 막습니다. 끊임없이 업데이트되면서 지속적인 맬웨어 인텔리전스를 제공하는 전 세계적인 센서 네트워크를 통해 9백만 개 이상의 시그니처와 90만 개 이상의 악성 웹사이트를 식별합니다.

ThreadCloud

보안 웹 게이트웨이에 제공되는 실시간 보호 정보. 전 세계적 네트워크의 위협 센서를 사용해서 동적으로 업데이트되는 이 솔루션은 사이버 범죄와 효과적으로 싸울 수 있는 최초의 실시간 협업 네트워크입니다.

URL 필터링

사용자의 생산성과 보안 정책을 지원하기 위해 새로운 웹사이트를 끊임없이 업데이트하는 클라우드 기반 기술을 통해 카테고리별, 사용자별, 그룹별 및 머신별로 수백만 개의 웹 사이트에 대한 액세스를 제어합니다. 전체 웹사이트 또는 사이트 내 페이지에 대한 액세스를 차단하고, 시간 할당 또는 대역폭 제한을 통해 강제합니다. 허용되는 웹사이트 및 허용되지 않는 웹사이트 URL 목록을 관리하여 보안 정책을 세밀하게 조정합니다.

어플리케이션 제어

업계 최대의 어플리케이션 보호 범위로 6900개 이상의 어플리케이션과 24만 개 이상의 소셜 네트워크 위젯에 대한 액세스를 제어합니다. 또한 인스턴트 메시징, 소셜 네트워킹, 비디오 스트리밍, VoIP, 게임 등과 같은 웹 어플리케이션과 위젯의 사용을 식별하거나 차단 또는 제한하기 위해 사용자 또는 그룹을 토대로 한 세밀한 보안 정책을 수립하고 보안을 확보하면서 비즈니스를 지원합니다.

IPS(옵션)

NSS Labs 조사에서 상위권에 포진한 IPS Software Blade는 완전하고 사전에 예방할 수 있다. Microsoft와 Adobe의 위협 보호에서 3년 연속 1위를 차지하였고, IPS Software Blade는 시의적절하고 효과적인 방식으로 브라우저와 어플리케이션 취약성 공격을 방어하여 네트워크를 안전하게 지켜줍니다.

안티봇(옵션)

Secure Web Gateway의 기능을 더욱 확장한 개념으로, 안티봇은 감염된 호스트를 식별하고 봇에 의한 손상을 방지하기 위함입니다. 감염된 호스트를 탐지하고, 봇 발생을 정확히 식별하고, 감염된 호스트와 원격 작업자 사이의 봇 통신을 차단하고, ThreatCloud 지식 베이스로부터 가장 최근의 봇 정보를 수신합니다.

사용자 인식

세밀한 가시성과 정책 시행을 위해 사용자, 그룹, 또는 머신별로 회사 리소스와 인터넷에 대한 액세스를 제어합니다. 직원과 게스트 또는 외부업체를 쉽게 구별하고 액세스를 제한하여 원치 않는 데이터 손실이나 데이터센터, 네트워크 및 어플리케이션에 대한 위협을 예방합니다. 인가된 사용자의 원격 작업은 허용하면서 기업 리소스에 대한 무단 액세스를 예방합니다.

통일된 보안 정책

기존의 인터넷 보안은 웹 보안의 각 요소에 대한 확실한 정책이 필요합니다. Check Point의 웹 보안 게이트웨이 어플라이언스는 모든 웹사이트, 웹 어플리케이션, 사용자 및 머신에 대한 통일된 제어를 제공하는 유일한 솔루션이며 인터넷 보안의 복잡성을 크게 줄이고 조직이 보다 쉽고 경제적인 방식으로 기업 보안 정책을 구현하고 시행할 수 있도록 지원합니다.

Source	Applications/Sites	Action
Any	Spyware / Malicio... P2P File Sharing	Block
Engineers	Media Streams	Allow Download_10Mbps

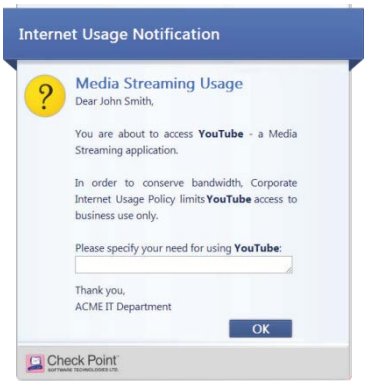
©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

통합 보안 관리

통일된 보안 관리는 증가하는 위협, 디바이스와 사용자를 관리하는 엄청난 작업을 단순화합니다. Check Point의 포괄적인 집중식 보안 관리 시스템은 SmartDashboard에서 모든 Check Point 게이트웨이와 소프트웨어 블레이드를 제어하며 직관적인 GUI는 IT 관리자가 일체의 광범위한 보안 관리 기능을 쉽게 관리하도록 지원합니다.

Check Point UserCheck

IT 직원이 관여할 필요 없이 사용자에게 현재의 온라인 활동에 대해 재고해볼 수 있는 기회와 조언을 제공하는 실시간 팝업 에이전트를 통해 기업 정책과 인터넷 안전에 대한 관심을 유도하고 교육합니다. 의사결정 과정에 사용자를 참여시키면 보안 위협에 대한 인식을 높일 수 있고 기업의 인터넷 사용과 관련된 보안 위협을 완화하는 데 도움이 됩니다.



SSL 암호화 트래픽 검사

게이트웨이를 통과하는 SSL 암호화 트래픽을 스캔하고 보안을 확인합니다. 트래픽이 통과할 때 게이트웨이는 보내는 사람의 공개 키로 트래픽 암호를 해독하고 검사 및 보호한 다음 재암호화하여 새롭게 암호화된 콘텐츠를 수신자에게 전송합니다. 사용자 프라이버시를 보호하고 기업 정책을 준수하기 위해 SSL 검사 예외 대상을 세심하게 정의합니다. 게이트웨이를 통과하는 암호화 콘텐츠 중 일부는 검사해서는 안 되기 때문에 관리자 정책 정의를 통해 예외처리할 수 있습니다.

SmartEvent

중대한 보안 이벤트를 신속하게 표시해주고, 통일된 보안 이벤트 관리를 통해 즉흥적인 보호 기능을 추가합니다. SmartEvent는 Check Point 제품과 제3자 장치의 모든 활동을 서로 관련시키고 보안 상태의 상세한 스냅샷에 대한 동향, 통계 및 맵을 포함한 보안 일정표를 제공합니다. 오프라인 보고와 다수의 사전 정의된 보안 이벤트, 그리고 이벤트 마법사를 활용하여 자체 이벤트를 맞춤 구성합니다. 가장 많이 사용된 어플리케이션과 가장 많이 액세스된 사이트, 상세한 사용자 웹 활동 등에 대해 오프라인 보고서(PDF, HTML 또는 excel 형식) 일정을 계획하고 이메일로 발송합니다.

여러 설치 옵션

Check Point 보안 웹 게이트웨이(Secure Web Gateway)는 인라인 설치 옵션뿐만 아니라 프록시 역할을 할 게이트웨이 설정 옵션을 포함한 다수의 비즈니스 요구 사항 및 규모를 지원하기 위해 유연한 배포 옵션을 제공합니다.

필요할 때 기능 추가

Check Point 보안 웹 게이트웨이(Secure Web Gateway)는 보안 필요가 증가하는 경우 추가적인 소프트웨어 기능을 더할 수 있으며 안티봇과 IPS 같은 소프트웨어 블레이드를 원활하게 추가 할 수 있습니다.

check point 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 국회대로62길 21 동성빌딩 7층 | 전화: 02-786-3303 | 팩스 02-761-9391 | krissl@checkpoint.com

©2015 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content