IBM Security Network Protection

차세대 네트워크 보호를 위한

보안성, 가시성 및 통합성의 통합

주요 내용

- IBM® X-Force를 기반으로 제로데이 위협에 대한 우수한 보호 기능과 보안 인텔리전스 제공
- 암호화된 트래픽을 포함하여, 네트워크 활동에 대한 핵심적인 통찰력 및 가시성을 제공
- IBM QRadar® Security Intelligence Platform과 통합 가능
- 사용자별 및 그룹별로 웹 애플리케이션 및 기타 애플리케이션에 대한 세밀한 통제 가능
- 통합을 통한 비용 절감, 복잡성 및 대역폭 소비 감소

IBM Security Network Protection는 위협에 대한 보호, 가시성 및 통제성의 차별화된 결합을 통해 비즈니스의 핵심 네트워크 인프라를 보호하도록 설계되었습니다. IBM은 네트워크 보안 전문가에게 네트워크에 대한 완벽한 보안성, 가시성 및 통제성을 제공하는 차세대 솔루션을 제공하여 기존 침입 방지 시스템의 기능을 확장하고 있습니다. IBM Security Network Protection을 이용하면 개별 솔루션들을 하나의 확장 가능한 네트워크 보안 플랫폼으로 통합하여 비용을 절감하고, 복잡성을 줄일 수 있습니다. 그리고 높은 대역폭을 차지하지만 중요하지 않은 활동을 통제 및 제거하여 인프라 내에서 추가적으로 비용을 절약할 수 있습니다.

오늘날의 보안 위협을 해결하기 위해서는 매우 정교한 보안 조치가 요구되며, 관리 복잡성을 줄이고 비용을 억제하는 것 또한 가장 시급한 사안입니다. IBM Security Network Protection은 이 모든 과제를 달성할 수 있는 통합 솔루션입니다. 여러 가지 고급 기능이 결합되어 있는 이 솔루션을 이용하면 위협을 방지하고, 네트워크 활동에 대한 핵심적인 통찰력을 제공하고, 세밀한 애플리케이션 통제를 실현하여 통합되고 간소화된 새로운 수준의 보안을 구축할 수 있습니다.

진화하고 있는 위협으로부터의 보호

보안 위협은 지속적으로 진화하고 있습니다. 최첨단 웹 애플리케이션의 급속한 증가 및 파일 공유의 증가로 인해, 과거에는 위협적이지 않던 활동도 이제는 공격자의 표적이 될 잠재적인 취약점이 되고 있습니다.

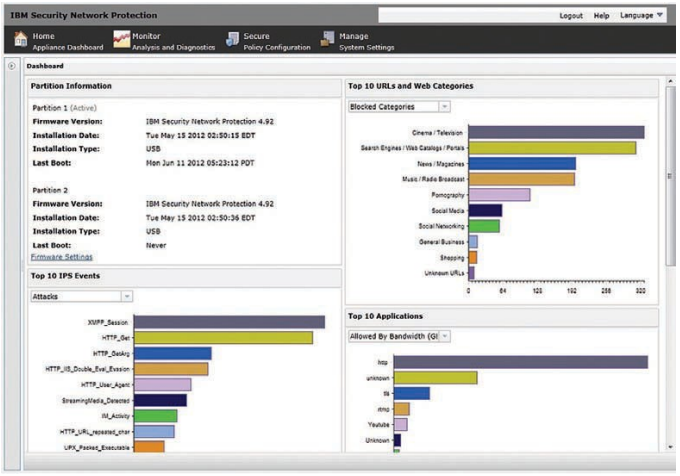
악성코드 제거 소프트웨어 및 방화벽과 같은 기존의 보안 수단은 이제 쉽게 우회할 수 있게 되었습니다. 위협에 사전에 대처하는 우수한 보호 기능은 생산성, 데이터 보안 및 규정 준수를 보장하는 중요한 수단입니다. IBM Security Network Protection은 새롭게 발생하는 위협에 대하여 웹 애플리케이션 보호 기능, 내장 쉘 코드 위협 발견 기능 및 기타 다수의 고급 기능을 통한 종합적인 보안을 제공합니다.

조직은 위협에 대한 예방적 보호 기능을 제공하는 IBM Security Network Protection을 이용할 수 있습니다. IBM X-Force의 연구 개발 팀이 설계한 IBM Protocol Analysis Module은 지속적인 컨텐츠 업데이트를 제공하여 보안 전문가가 새로운 위협에 미리 대처할 수 있도록 하는 핵심 요소입니다. Protocol Analysis Module에는 클라이언트 측과 웹 애플리케이션, 고급 네트워크 및 데이터를 포함한 여러 핵심 영역에 대한 보안이 포함되어 있습니다.

이러한 보안 업데이트에 대한 컨텐츠는 세계에서 가장 종합적인 위협 데이터베이스를 유지관리하고 있는 곳 중 하나인 X-Force 연구 개발 팀에서 제공합니다. X-Force 팀은 Global Threat Operations Center에서 전 세계의 인터넷 위협 수준을 추적하여 위협 데이터베이스를 컴파일하며, 이 데이터베이스는 위협에 대한 최신 보호 기능을 통해 IBM Security 솔루션을 업데이트합니다. Protocol Analysis Module은 X-Force 데이터베이스와 결합되어 제로데이 악용에 대한 높은 수준의 보호 기능을 제공하며, 악성코드, 봇넷, P2P(Peer-to-Peer) 활동 등의 광범위한 보안 위험을 정확하게 식별하는 기능을 제공합니다.

핵심적인 통찰력 및 가시성

IBM Security Network Protection은 여러 핵심 보안 기능을 결합하여 기본적인 위협 보호 기능 이상의 기능을 수행할 수 있으며, 어떠한 애플리케이션이 이용되고 있는지, 어떠한 웹사이트를 방문하고 있는지, 그리고 누가 이러한 웹사이트를 방문하고 있는지 등의 네트워크 활동에 대한 핵심적인 통찰력 및 가시성을 제공합니다.



IBM Security Network Protection 대시보드는 더 높은 수준의 보안을 위해 네트워크 활동에 대한 핵심적인 통찰력과 가시성을 제공합니다.

보안을 유지하려면 네트워크 내에서 정확히 어떠한 일이 일어나고 있는지 파악해야 하며, 애플리케이션, 인스턴스 메시지, 동영상 및 오디오 스트림, 그리고 파일 공유를 모두 식별하고 모니터링해야 합니다. 이러한 활동은 공격에 대한 기회를 제공할 수 있으며, 이로 인해 데이터 손실이 발생되거나, 사내 정책 위반과 규정 준수 관련 문제가 야기될 수 있습니다. 비즈니스 핵심 활동 이외의 활동은 많은 양의 대역폭과 자원을 소비할 수 있으며 조직을 위험에 처하게 할 수도 있습니다. IBM Security Network Protection은 대역폭 사용 현황에 대한 가시성을 제공하여 비즈니스 핵심 활동 이외의 활동을 식별함으로써 이러한 유형의 활동에 대한 통찰력을 제공할 수 있습니다.

네트워크 활동에 대한 세밀한 통제

높은 수준의 위협 보호 기능과 강화된 네트워크 가시성이 내장된 IBM Security Network Protection에는 세밀한 통제 기능이 포함되어 있으며, 사용자는 이를 통해 네트워크에 대한 새로운 통찰력을 확보하고 조치를 취할 수 있습니다. 이 기능은 잠재적인 공격 및 위협에 대한 노출을 줄이도록 설계되었으며, 소셜 미디어 사이트와 같은 일반적인 공격 제공 방법에 대한 세밀한 통제 기능을 제공하여 사용자를 대상으로 하는 스피어 피싱이나 다른 고도의 위협이 발생하는 것을 방지합니다. 세밀한 통제 정책을 생성하는 기능을 이용하면 전체적인 위험을 줄일 수 있으며, 비즈니스 이외의 목적으로 이용하는 네트워크와 관련된 대역폭 비용을 줄일 수도 있습니다.

광범위한 애플리케이션 보호를 제공하기 위해, IBM Security Network Protection은 2,000개 이상의 애플리케이션 및 개별적인 행동에 대한 지원을 제공하며, 200억 개 이상의 URL이 포함된 데이터베이스를 이용합니다. 최고 수준의 정확성을 보장하기 위해, IBM의 웹 크롤링 기술은 URL이 변경될 때마다 지속적으로 URL을 재분류합니다. 이러한 기능은 IBM Security Network Protection 어플라이언스가 지속적으로 업데이트되어 정책 사용의 효과를 최대화하고 최신 인터넷 위협에 대해 보호되도록 보장합니다.

빈틈 없이 완벽한 배치와 통합

IBM Security Network Protection은 QRadar Security Intelligence Platform과 같은 다른 보안 기술과 통합되어 광범위한 환경에 완벽하게 배치될 수 있습니다. 이러한 제품군은 상호 교환 가능한 네트워크 인터페이스 모듈(NIM)을 통해 다양하고 광범위한 네트워킹 표준과 구성의 변경을 지원합니다. 또한, 하드웨어 변경 없이도 성능을 업그레이드할 수 있는 유연한 성능 라이센스 방식을 제공합니다. 조직은 사전에 구성되는 X-Force의 기본 정책과 지속적인 보안 업데이트를 통해 보안 보호 기능을 바로 이용할 수 있습니다. IBM Security Network Protection 어플라이언스는 신속하게 설치 가능하며, IBM Security SiteProtector™ System을 이용하는 여러 지점에 걸쳐 중앙 집중식으로 관리할 수 있습니다.

IBM Security Network Protection XGS 5100 어플라이언스는 두 개의 네트워크 인터페이스 모듈로 구성할 수 있습니다.

IBM Security Network Protection 어플라이언스는 QRadar Security Intelligence Platform과의 차별화된 통합을 통해 IPFIX(Internet Protocol Flow Information Export) 데이터를 전송하여 더욱 정교한 분석 및 상관관계 파악을 위한 데이터 피드를 지속적으로 제공합니다.

IBM을 선택해야 하는 이유

네트워크 보안에 대해 똑똑한 접근법을 이용하는 IBM은 위협에 대한 보호, 가시성 및 통제성을 위한 종합적인 솔루션을 제공하고 있습니다. IBM Security Network Protection은 진화하는 보안 위협에 대한 완벽한 보호를 위해 차세대 침입 방지 시스템 기능을 제공합니다. IBM Security Network Protection을 이용하면 관리자는 네트워크에 대한 더 높은 통제성을 갖게 되며, 최적의 보안성과 향상된 대역폭 효율을 얻으면서 비용을 절감할 수 있습니다. IBM X-Force의 위협 데이터와 방대한 URL 데이터베이스를 활용하는 이 솔루션을 이용하면 새로운 위협에 대해 사전에 대처하는 최신 보안 기능을 활용할 수 있습니다. 여러 핵심 보안 기능이 하나의 오퍼링에 통합되어 있는 IBM Security Network Protection은 여러 조직이 직면한 과제에 대해 종합적이고 비용 효과적인 해답을 제공합니다.

IBM Security Network Protection XGS 5100 개요	
성능 특성 *	
처리량	최대 5Gbps
처리량(SSL 이용 시)	최대 2.5Gbps
평균 레이턴시	150µs 미만
초당 연결	50,000개
동시 세션(최대 속도)	2,000,000개
물리적 특성	
폼 팩터	1U
높이	44.2mm/1.75in.
넓이	430mm/16.9in.
깊이	500mm/19.7in.
중량	10kg/22lb
관리 인터페이스	1GbE 2개, RJ-45(IPv6 지원)
고정 모니터링 인터페이스	1GbE 4개, RJ-45(통합 바이패스)
인라인 보호 세그먼트	최대 10개
최대 모니터링 인터페이스 (10GbE)	최대 4개
최대 모니터링 인터페이스(1GbE)	최대 20개
지원되는 물리적 매체 유형	구리선 직접 연결, RJ-45, 광섬유(SX/L X), 10G 광섬유(SR/LR), SFP, SFP+
네트워크 인터페이스 모듈(NIM) 개수	최대 2개

IBM Security Network Protection XGS 5100 개요	
네트워크 인터페이스 모듈(NIM)	1GbE 고정 TX(통합 바이패스) 8개 1GbE 고정 SX(통합 바이패스) 4개 1GbE 고정 L X(통합 바이패스) 4개 10GbE 고정 SR(통합 바이패스) 2개 10GbE 고정 LR(통합 바이패스) 2개 1GbE SFP 4개 10GbE SFP+ 2개
고가용성 지원	액티브/액티브 및 액티브/패시브 환경 지원
이중 전원 공급 장치	예
스토리지 유형/MTBF 등급	SSD(Solid-State Drive)/2백50만 시간
전기 및 환경 관련 수치	
교류 입력 정격	100V~127V @ 5.6A/200V~240V @ 2.8A
전원 공급장치 정격/ 평균 전력 소비량	460W/194W
작동 온도/상대 습도	0°C~40°C(32°F~104°F)/5%~85% @ 40°C(104°F)
안전 인증/선언	UL 60950-1, CAN/CSA C22.2 no. 60950-1, EN 60950-1(CE Mark), IEC 60950-1, GB4943, GOST, UL-AR
전자파 적합성 인증/선언	FCC Class A, Industry Canada Class A, AS/NZS CISPR 22 Class A, EN 55022 Class A(CE Mark), EN 61000-3-2(CE Mark), EN 61000-3-3(CE Mark), EN 55024(CE Mark), VCCI Class A, KCC Class A, GOST Class A, GB9254 Class A, GB17625.1
환경 관련 선언	유해물질 제한지침(RoHS)

* IBM Security Network Protection에 대해 인용된 성능 데이터는 일반적인 라이브 트래픽을 반영하도록 의도된 TCP/UDP 혼합 트래픽을 이용한 테스트를 근거로 합니다. 프로토콜 구성 및 평균 패킷 크기와 같은 환경적 요인은 각 네트워크마다 다르며, 측정된 성능 결과도 이에 따라 달라집니다. IBM Security Network Protection의 처리량은 압축되지 않은 혼합 프로토콜 트래픽을 IBM Security Network Protection 어플라이언스를 통해 전송한 후 패킷 손실이 없었을 때의 처리량을 측정하여 구한 값입니다. 벤치마크 테스트 시, “Trust X-Force” 정책을 이용하는 기본 인라인 모드 및 드롭 미분석 모드의 채워진 10G 네트워크 인터페이스 모듈 2개를 이용해 XGS 시리즈 어플라이언스가 배치되었습니다. Spirent Avalanche 및 Spirent TestCenter 테스트 장비의 펌웨어 버전은 v4.03(또는 이후 버전)입니다. 트래픽의 혼합률은 HTTP=69%, HTTPS=20%, SMTP=5%, FTP=5%, DNS=1%이며, 여기서 HTTP/HTTPS 트래픽은 44kb의 객체 크기를 이용하며 표준 HTTP/S 1.1 GET 요청을 포함하고 있는 압축되지 않은 트래픽입니다. SMTP 단순 연결은 객체를 전송하지 않고, 15,000바이트의 FTP GET 요청은 2ms 버스트 상태로 전송되며, DNS 표준 A 기록 룩업이 이용되었습니다. SSL 검사 속도는 SSL 복호화 정책을 활성화한 상태에서 측정하였습니다.

추가 정보

IBM Security Network Protection에 대해 자세히 알아보려면 IBM 영업 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 다음 웹 사이트를 방문하십시오.
ibm.com/security

우수 보안 관리제도에 대한 설명: IT 시스템 보안은 귀사 내/외부로부터의 부적절한 접근을 방지, 감지, 대응함으로써 시스템과 정보를 보호하는 일을 포함합니다. 부적절한 접근은 정보의 변경, 파괴 또는 유용을 초래하거나, 타 시스템에 대한 공격을 포함한 귀사 시스템에 대한 피해나 오용을 초래할 수 있습니다. 어떠한 IT 시스템이나 제품도 완벽하게 안전할 수 없으며, 단 하나의 제품이나 보안 조치만으로는 부적절한 접근을 완벽하게 방지하는 데 효과적이지 않을 수 있습니다. IBM 시스템과 제품은 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템과 제품이 임의의 당사자의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지는 않습니다.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2013

WGD03017-USEN-01