IBM Security Server Protection

윈도우즈 서버를 위한 똑똑한 보안 솔루션

주요 특징

- **다양한 공격 유형으로부터 시스템을 보호**
- **데이터 보안과 규제 준수를 위한 강력한 모니터링 기능**
- **다계층 감시 기능으로 보다 완벽한 보호가 가능**
- **중앙 관리 방식으로 관리 비용을 절감**

보다 진보적인 윈도우즈 서버 보안 솔루션

방화벽과 안티바이러스 소프트웨어를 이미 보유하고 있지만 많은 기업들은 여전히 보안 관리 업무에 어려움을 느끼고 있습니다. 조사에 따르면 보안 사고 발생시 평균 피해액은 70억원에 달한다고 합니다. 계속해서 발견되는 보안 취약점으로 운영체제와 애플리케이션 패치가 계속해서 발표되고 있으며, 해커들은 계속해서 웹 애플리케이션을 통해 중요한 정보를 노리고 있습니다. 의도적이던 우발적이든 간에 회사 및 조직 내부 인력의 보안 침해 역시 계속해서 증가하고 있습니다.

최근 많은 기업 및 정부 기관 등에서 도입 비용상의 이유로 네할렘 EX 기반의 하이엔드급 윈도우즈 서버를 주요 업무 서버로 도입하고 있습니다. 하지만 윈도우즈 운영 체제는 가장 많은 취약점을 발표하고 있으며 가장 많은 악성 코드를 지닌 운영체제로 운영시 보안 관련 비용이 가장 크게 소요되는 플랫폼이기도 합니다. 일반적으로 윈도우즈 서버 보안을 위해서 패치를 적용한다거나 안티 바이러스를 설치하고 있지만, 현재의 보안툴은 아래와 같은 한계가 있습니다.

안티 바이러스 소프트웨어의 한계: 악성 코드 샘플이 확보되지 않은 새로운 공격에 대해서는 안티 바이러스가 서버를 보호할 수 없기 때문에 새로운 샘플이 발표될 때까지 서버는 사실상 무방비 상태에 있게 됩니다.
보안 패치 적용 시간상의 한계: 보안 패치가 발표된다고 곧바로 서버에 설치를 할 수는 없습니다. 운영 서버와 동일한 테스트 시스템에 테스트를 한다거나 주말의 유지 보수 시간까지 기다려야 하는 등, 패치가 적용될 때까지 서버는 사실상 무방비 상태에 있게 됩니다.

새롭게 발표된 IBM 시큐리티 서버 프로텍션 소프트웨어는 Hyper-V, vmware, zen 등의 다양한 가상화 환경을 포함하는 윈도우즈 서버를 위한 보다 강력한 보안 솔루션을 제공합니다.

IBM Security Server Protection은
다양한 가상화 환경을 보호할 수 있습니다.

- VMware ESX
- 윈도우즈 서버 2008 Hyper-V
- IBM Logical Partitions
- IBM Workload partitions
- HP vPars, nPars
- Solaris Container

버추얼 패치 관리 | 위협 발견 및 보호 | 컨텐트 분석 | 웹 보호 | 네트워크 정책 준수

IBM Security Server Protection의 다양한 기능

IBM Security Server Protection은 아래와 같은 다양한 기능을 제공하는 제품입니다.

방화벽 : 승인되지 않은 포트와 IP 주소로의 접속을 차단해 외부로부터의 공격으로부터 서버를 보호합니다.

취약점 기반 가상 패치 시스템(VPS Virtual Patch System) : 허용된 서비스를 통해 침투해 오는 다양한 위협을 X-Force에서 제공하는 VPS 엔진으로 선제적으로 방어할 수 있습니다.

버퍼 오버플로우 방어 : 메모리 버퍼상의 취약점을 공격하는 악성 코드를 인식해 방어할 수 있습니다.

다양한 감시 기능 : OS 감사 모니터링, 레지스트리 모니터링, 파일 무결성 모니터링 등의 다양한 모니터링 기능을 제공합니다.

웹 애플리케이션 보호 : 암호화되어 전송되는 데이터를 검사함으로써 아파치, IIS 웹서버에서 운영되는 웹 애플리케이션을 보호할 수 있습니다.

애플리케이션과 커뮤니케이션 조정 : 애플리케이션 화이트 리스트, 블랙 리스트를 통해 호스트 네트워크에 승인되지 않은 애플리케이션을 보호할 수 있습니다.

광범위한 플랫폼 지원 : vmware 등의 가상화 플랫폼을 포함하는 윈도우즈 운영 체제의 보안 문제를 해결할 수 있습니다.

시스템 통합 및 규정 준수 : 다양한 법규, 산업별 규약을 준수하는데 필요한 데이터 기밀성을 보장하고 보안 통제 역량을 강화할 수 있습니다.

IBM Security Server Protection만의 특별한 기술들

IBM 보안 프레임워크 기반의 토탈 보안 솔루션

보안에 대한 청사진을 제공하는 IBM 보안 프레임워크를 기반으로 다양한 제품들간의 통합성과 연계성을 높이실 수 있습니다. 또한 보안 성숙도에 따라 단계별 로드맵에 기반한 도입 계획을 수립하실 수 있습니다.

세계 최고 수준의 X-Force 연구개발팀

세계 최대 규모의 취약점 분석 전문 연구 기관인 X-Force에는 약 150명의 보안 전문가 및 해커들이 다양한 취약점을 발견하고 있으며, 이러한 기술과 정보들이 IBM 제품에 반영되고 있습니다.

가상 패치 기술

끊임없이 발표되는 패치에 대한 대안으로 제시된 가상 패치 기술은 취약성 자체에 초점을 맞추어 미리 패턴을 작성하고 업데이트할 수 있습니다. 이 기술을 통해 취약점을 발견하고 패치 설치 기간 동안 시스템을 효과적으로 방어할 수 있습니다. 또한 취약점을 악용하는 악성 코드가 발표 되기도 전에 악성 코드에 대한 대응 방안을 제시할 수 있을 정도로 선제적인 보호 기능을 제공합니다.

보다 자세한 정보를 필요로 하십니까?
지금 한국IBM의 보안 영업 전문가들을 만나보십시오.

보다 자세한 내용은 아래 웹 사이트에서 보실 수 있습니다.
kr.ibm.com/security

IBM Security Solutions, IBM Korea

(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩 마케팅총괄본부

TEL : (02) 3781-7800
www.ibm.com/security

재활용 하십시오.

TIS 14011-USEN-00

Tivoli software