IBM **Power Systems**

POWER9를 통한 보안을 위한 다층적인 접근 방법

IT 인프라에 대한
완벽 보안 및 최적화

자세한 정보는 IBM Business Partner®에 문의하십시오.

[비즈니스 파트너 이름]
[비즈니스 파트너 전화번호/이메일]
[비즈니스 파트너 웹사이트]

정교한 사이버 공격의 시대의 엔터프라이즈 IT

잘 알려진 매우 충격적인 데이터 유출로 인해, 오늘날 많은 경영진의 관심의 최전선에는 보안이 자리하게 되었습니다. 그 결과 조직 전반에 걸쳐 보안 예산이 증가했습니다. 하지만 적어도 부분적으로는 증가된 소비 및 기술 변화로 인해 IT 보안을 위협하는 새로운 복잡성과 위험이 발생했습니다. 보안 전문가를 대상으로 한 2019 Forrester 설문 조사에 따르면 “1/4에 못 미치는 응답자만 보안 직원 생산성 향상, 데이터 해석 및 효율성 향상을 위한 고급 위협 인텔리전스 기능 개발 지원에 대한 회사의 보안 포트폴리오에 완전히 만족하고 있습니다.” [1]

보안 전문가의 가장 큰 우려는 공격의 수와 정교함이 증가하고 있는 것으로 오늘날 비즈니스의 여러 측면은 그 어느 때보다도 더 이런 공격에 노출되고 있습니다. 하드웨어 및 펌웨어 수준의 취약점은 그렇게 멀지 않은 과거에만 하더라도 그리 큰 관심의 대상이 아니었습니다. 하지만 이제 이런 취약점은 중요한 관심 대상이 되었습니다.

IT 아키텍처가 발전하면 한편으로 위협이 계속 늘어날 것입니다. 여러 가지 면에서, 오늘날 비즈니스에서 극복해야 하는 사이버 보안 문제는 다음과 같은 두 가지 경험적 사실로 분류될 수 있습니다. IT 스택이 확장되고 있으며 그 직접적인 결과로 해커는 보다 다양한 공격을 해옵니다.

현재의 위협 환경의 현실

오늘날 조직은 보안 시스템에 의존하여 지적 재산권, 민감한 기업 정보, 민감한 개인 정보와 개인 정보 보호에 대한 위협을 방지합니다. IT 보안에 대한 조직의 전략적 접근 방법은 필수적인 것입니다.

보통의 경우에는 비즈니스, 규정 준수 또는 경제성 등에 중심을 둔 접근 방법을 통해 IT 보안에 전략적으로 접근할 수 있습니다. 이런 접근 방법도 가치는 지니고 있지만 IT 시스템 위협 증가에 대비해서 비즈니스 프로세스를 적절하게 보호하지는 못합니다. 이런 접근 방법은 주요 복합 분야적 측면도 간과할 수 있습니다.

이상적인 조치의 과정은 보안과 관계된 중요한 영역의 위험을 식별하기 위한 계획 및 평가가 포함됩니다. IBM® Power® Systems 및 POWER9™ 프로세서는 조직 안전 및 규정 준수 보장을 위해 보안 전략에 대한 전체적이고 다층적인 접근 방법을 제공합니다. 이런 다층적인 접근 방법에는 다음이 포함됩니다.

- 하드웨어
- 펌웨어
- 하이퍼바이저
- 운영 체제
- PowerSC

전체적 보안 접근 방법을 채택하면 현재의 보안 환경에 영향을 미치는 4가지 현실 요구를 충족시킬 수 있습니다.

해커들이 점점 더 정교해지고 있습니다. 조직이 기존 온프레미스 데이터 센터의 한계를 더 많이 벗어날수록 사이버 공격자는 기존 틀을 깨는 생각을 더 많이 해야 합니다. 해커들의 해킹 방법은 더 이상 네트워크 수준에 그치지 않고 다양한 공격을 하게 되고 더 확률 높은 공격이 가능해집니다.

모바일 및 엣지 기기에 대해서 더 많은 비즈니스가 진행되고 있습니다. 서버, 하이브리드 클라우드 환경 및 수많은 모바일 및 엣지 기기 등 이제 거의 모든 곳에서 직원이 조직 내의 데이터를 저장하고 액세스할 수 있습니다. 서버와 기기를 넘나드는 이런 엄청난 상호간 교차 액세스는 계속되고 있는 디지털 변환의 부산물이지만 악용이 가능한 완전히 새로운 공격의 경로가 만들어 집니다.

엄격한 규제는 위험 프로파일에 영향을 미칩니다. 규제 관련 규정 준수를 보장하기 위해 마련된 프로세스는 의도하지 않은 위험 노출로 이어질 수도 있습니다. 또한 EU의 GDPR은 최근 증가하는 추세의 한 가지 전개 양상일 뿐입니다. 관리 주체는 귀하의 조직에서 데이터를 사용하는 방법에 대해 훨씬 더 많은 주의를 기울이고 있습니다. 또한 관리 주체는 일상적인 비즈니스 운영에 복잡한 계층을 추가시킵니다.

직원들은 잠재적인 취약점입니다. 어떤 보안 통제를 적용하든 취약점을 얼마나 잘 처리하든 귀사의 직원들은 늘 어느 정도의 위험을 초래할 것입니다. 의도하지 않은 실수나 영리한 악의적인 공격으로 인해, 엔드 포인트 보안과 규정 준수를 위한 노력이 무산될 수 있습니다. 한편, 많은 조직은 유능한 보안 직원을 찾고 고용하기 위해 노력하고 있으며 반복되는 기술 부족에 시달리고 있습니다.

IT 아키텍처가 진화하고 끊임없이 변화하는 기술, 업무 문화 및 규정 준수에 적응함에 따라 오늘날 사이버 위협의 규모, 다양성 및 속도가 증가할 것입니다. 즉, 보안 전략도 네트워크 수준을 넘어서서 진화해야 합니다.

보안에 대한 전체적이고 다층적인 접근 방법이 필요합니다

다양한 타사 공급 업체 보안 솔루션 구현을 통해서도 모든 수준의 스택에 보안을 구축할 수 있습니다. 하지만 이런 접근 방법은 이미 존재하는 복잡성을 복합화하고 네트워크에는 훨씬 더 많은 취약점과 노출 지점을 들여옵니다. 가장 좋은 방법은 조직의 모든 데이터와 시스템을 보호하면서 복잡성을 최소화하는 다층적이고 전체적인 접근 방법을 채택하는 것입니다.

이를 염두에 두고 IBM은 비즈니스 중심 보안에 대한 전체적인 접근 방법을 사용할 때, 모든 IT 보안 측면을 올바르게 처리할 수 있도록 IBM Security® Framework를 개발했습니다.

IBM Security Framework는 다음에 중점을 둡니다.

1. **인프라**—사용자, 컨텐트 및 애플리케이션에 대한 통찰력을 통해 정교한 공격으로부터 보호합니다.
2. **고급 보안 및 위협 연구**—취약점 및 공격 방법에 대한 지식을 얻고 보호 기술을 통해 그에 대한 해석을 적용합니다.
3. **사람**—포괄적인 아이덴티티 인텔리전스로 보안 도메인에서 엔터프라이즈 아이덴티티를 관리하고 확장합니다.
4. **데이터**—조직에서 가장 신뢰할 수 있는 자산에 대한 개인 정보 보호 및 무결성을 확보합니다.
5. **애플리케이션**—더 안전한 애플리케이션 개발하는 데 따르는 비용을 줄입니다.
6. **보안 인텔리전스 및 분석**—추가 컨텍스트, 자동화 및 통합으로 보안을 최적화합니다.

IBM Security Framework 및 IBM Security Blueprint를 사용한 정보 및 드릴 다운 학습에 대해 더 자세히알아 보십시오.

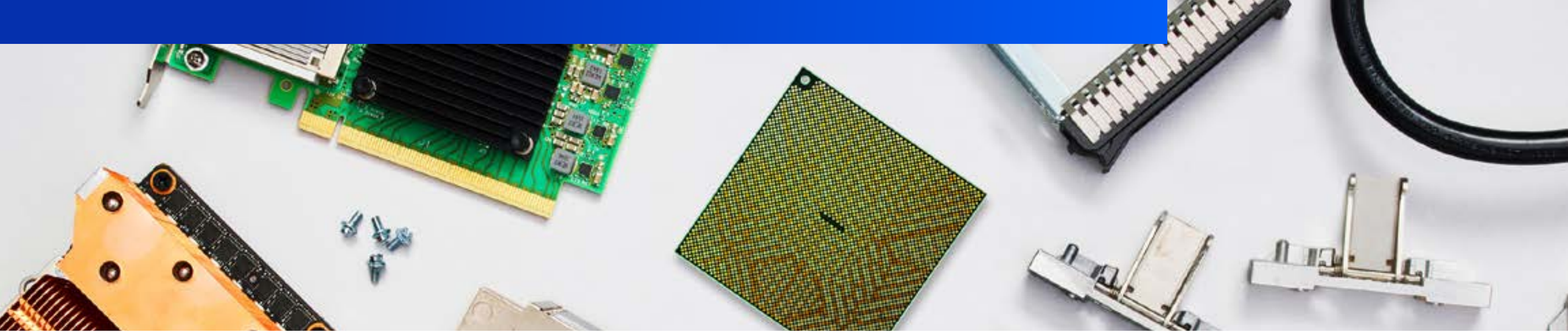
IBM Power Systems 및 POWER9가 스택을 보호하는 방법

IBM Power Systems를 사용하면 프로세서 및 펌웨어에서 OS 및 하이퍼바이저, 앱 및 네트워크 리소스, 보안 시스템 관리에 이르기까지 전체 스택에 긴밀하게 통합되는 포괄적인 엔드 투 엔드 보안을 얻을 수 있습니다.

하드웨어, 펌웨어 및 하이퍼바이저

24 암호화 엔진

POWER9 프로세서는 POWER8® 이전 버전보다 2배 많은 암호화 엔진을 보유합니다. 스택의 모든 계층에서 2배 속도 또는 그보다 더 빠른 속도로 정지 중이거나 동작 중인 데이터를 암호화할 수 있습니다.



온칩 액셀러레이터

POWER9에는 자랑할 만한 온칩 액셀러레이터가 있어, 소프트웨어보다 훨씬 빠르게 GZIP 파일을 압축 및 압축 해제합니다. 전체 VM이 빠르게 압축 및 암호화되고 네트워크를 통해 안전하게 이동됩니다.

POWER9의 보안 부팅

보안 부팅은 디지털 서명을 통해 모든 펌웨어 구성 요소를 확인하고 검증하여 시스템 무결성을 보호합니다. IBM이 배포한 모든 펌웨어는 디지털적으로 서명되어 검증이 가능합니다. 고유한 펌웨어 설치와 펌웨어 확인에 필요한 공개 키 계층 교체도 가능합니다.

트러스트 부트 및 Trusted Platform Module(TPM)

POWER9 프로세서는 서버의 모든 펌웨어 구성 요소를 검사하고 원격으로 검증(인증)할 수 있습니다. 신뢰할 수 있는 부팅 기능은 소프트웨어 스택을 측정하기 위해 RoT(신뢰 루트) 역할을 하는 TPM을사용합니다. 확인에 대해서는 TPM 자체에서 서명이 되기 때문에 펌웨어가 어떤 식으로도 변경이 되지 않았다는 것을 알 수가 있습니다.

IBM PowerVM® 엔터프라이즈 하이퍼바이저

IBM PowerVM® 은주요 경쟁 업체와 비교해 탁월한 보안 실적을 보유하고 있으므로 가상 머신(VM) 및 클라우드 환경을 믿고 보호할 수 있습니다.

운영 체제

IBM Power Systems는 IBM AIX®, IBM i 및 Linux®와알아보십시오. 기능은 OS에 따라 다르지만 기능 예는 다음과 같습니다.

- 보안을 위태롭게 하지 않으면서도 루트 사용자를 위해서 일반적으로 예약된 관리 기능을 할당하는 기능
- 개별 키 저장소를 통해 파일 수준 데이터를 암호화하는 기능
- 사용자가 액세스할 수 있는 개체에 대한 제어와 함께, 사용자가 사용할 수 있는 명령과 기능에 대해 더 강력하게 제어하는 기능
- 시스템 값 및 사용자와 개체에 대한 개체 감사 값을 사용하여 보안 감사 일지에 개체에 대한 액세스를 기록하는 기능
- 전체 드라이브에 암호화를 수행해 먼저 개체를 암호화한 다음 암호화된 형식으로 작성하는 기능
- 요청하는 사용자를 위해 파일을 실행하거나 열기 전에 모든 파일을 측정하고 확인하는 기능

워크로드, VM 및 컨테이너

워크로드는 더 이상 온프레미스 데이터 센터로 제한되지 않고 지속적으로 가상화 및 클라우드 환경으로 이동하고 있습니다. 이는 많은 조직이 하이브리드 인프라에 새로운 애플리케이션 및 기존 애플리케이션을 배포하는 데 컨테이너를 채택하고 있음을 의미합니다. 더 역동적인 환경과 워크로드에는 다목적 보안 기능이 필요합니다.

Live Partition Mobility(LPM)

IBM Power Systems를 사용하면 데이터를 안전하게 보호할 수 있습니다. LPM은 한 시스템에서 다른 시스템으로 마이그레이션해야 할 때 암호화를 통해 VM을 보호합니다. 온프레미스 데이터 센터 및/또는 하이브리드 클라우드 환경을 가상화한 경우에는 이 기능이 대단히 중요합니다.

Protected Execution Facility

Protected Execution Facility는 IBM Power Systems가 이러한 수준의 스택을 보호하는 방법의 한 예입니다. 이 기능은 보안 메모리에서 VM을 암호화하고 실행하는 POWER9의 기능으로 손상된 하이퍼바이저는 액세스를 할 수가 없습니다. 또 클라우드 환경에서 VM에 액세스할 수 있는 악의적인 내부자 또는 관리자는 보안 메모리에서 실행되는 워크로드에 액세스할 수 없습니다. 암호 해독 프로세스는 확인된 시스템에서만 이루어집니다.

IBM Power Systems의 통합 보안 제품

IBM PowerSC 는클라우드 및 가상 환경에서의 엔터프라이즈 보안 및 규정 준수를 위한 통합 포트폴리오 제품입니다. 이는 가장 낮은 레벨에서 상주하는 IBM Power Systems의 보안 기능을 관리하기 위한 웹 기반 UI를 제공하면서 스택 위에 상주합니다.

IBM PowerSC를 통한 시간, 비용 및 위험 감소

IBM PowerSC는 단순화 및 자동화 기능을 통해 규정 준수 및 감사 프로세스를 간소화해 시간과 비용이 감소되도록 합니다. 또 스택 전체의 가시성을 높여 보안 위험도 감소시킵니다.

IBM PowerSC Standard Edition의 기능

규정 준수 자동화

IBM PowerSC는 수많은 산업 표준을 지원하는 사전 구축된 프로파일이 함께 제공됩니다. XML을 건드릴 필요 없이 이러한 프로파일을 사용자 정의하고 엔터프라이즈 규칙과 병합할 수 있습니다.

실시간 규정 준수

보안에 중요한 파일에 대한 실행 또는 상호 작용이 있을 때는 이를 탐지하고 경고합니다.

Trusted Network Connect(TNC)

VM이 규정된 패치 수준에 있지 않을 때 경고합니다. 또한 수정 사항을 사용할 수 있게 되면 알려줍니다.

트러스트 부트

서버에서 실행 중인 모든 펌웨어 구성 요소를 검사하고 원격으로 확인할 수 있습니다.

트러스트 방화벽

AIX, IBM i 및 Linux 운영 체제 간의 내부 네트워크 트래픽을 보호하고 라우팅합니다.

트러스트 로깅

백업, 보관 및 관리가 쉬운 중앙 집중식 감사 로그를 만듭니다.

사전 구성된 보고 및 대화식 타임라인

IBM PowerSC Standard Edition은 5개의 사전 구성된 보고서로 감사를 지원합니다. IBM PowerSC Standard Edition에는 VM 수명 및 이벤트를 볼 수 있는 대화식 타임라인도 있습니다.

IBM PowerSC의 많은 기능에 대해 자세히 알고 싶으시면 다음 IBM Redbook, “클라우드 및 가상화 환경에서 IBM PowerSC의 보안 및 규정 준수 관리 단순화” 를 참조하십시오.

보안에 대한 가장 강력한 접근 방법은 최적화된 접근 방법

해커의 능력이 더욱 더 정교해지고 기술의 발전으로 인해서 오늘날의 비즈니스에 새로운 취약점이 생겨나면서, 이제는 조직의 복잡성을 가중시키는 않는 다층적이고 전체적인 보안 솔루션을 통합하는 것이 중요합니다. IBM Power Systems는 단일 공급 업체의 긴밀하게 통합된 심층 솔루션으로 모든 수준의 스택을 보호합니다. 여러 공급 업체가 제공한 여러 구성 요소에 의존한 보안 전략은 결국 여러모로 비용만 더 든다고 입증될 복잡성만 초래합니다.

단일 공급 업체의 보안 기능은 보안 전략이 단순화되면서 강화되게 되는 자연스러운 이점을 제공합니다. 30년의 보안 리더십을 바탕으로 IBM Power Systems는 IBM 내외부의 다른 조직과 광범위한 파트너십을 맺어 보안 전문성을 심화시키고 확대시킵니다. 이러한 파트너십을 통해 IBM Power Systems는 더 큰 규모의 보안 전문가 커뮤니티를 활용하여 문제를 신속하게 식별하고 자신 있게 해결할 수 있습니다. POWER9 서버는 IBM Security 및 IBM Research™ 사업부의지원으로 PowerSC 포트폴리오와 함께 내부자 공격을 포함한 여러 가지 위협을 모두 막아냅니다.

전체적이고 다층적인 접근 방법으로 전체 스택에서 보안을 간소화해서 귀하의 비즈니스를 안전하게 유지해 보십시오.

POWER9 서버의 인프라 보호 방법에 대한 자세한 내용은
IBM 담당자 또는 **IBM** 비즈니스 파트너에게 문의하십시오.

1. “2019 사이버 보안의 복잡성에 대한 보고서: 복잡성을 줄여 보안 성과를 향상하는 방법” Forrester Research, Inc., 2019년 5월

IBM Systems, 11501 Burnet Road, Austin, Texas 78758

33028633KRKO-00