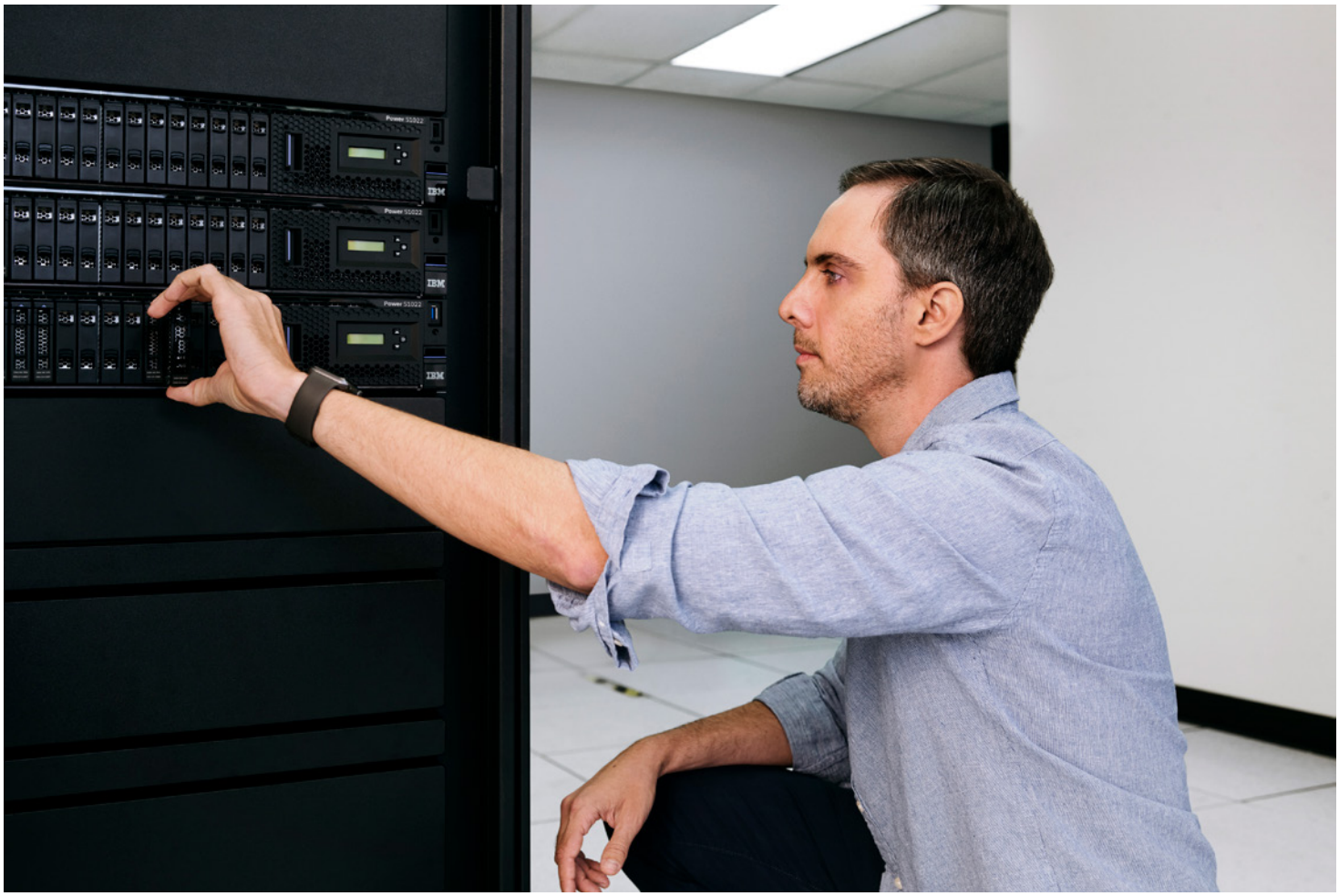
IBM Power를 통한 다층적 보안 접근 방식

제로 트러스트 접근 방식을 위한 필수 인프라



목차

03
오늘날의 IT 환경

04
거시적 접근 방식

06
제로 트러스트 전략

07
IBM Power 살펴보기

10
IBM PowerSC 2.0 기술

12
완벽한 통합

정교한 사이버 공격 시대의 엔터프라이즈 IT

오늘날의 IT 환경

코로나19 팬데믹이 시작된 이래 파괴적인 데이터 유출이 엄청난 수로 기록되었습니다. 데이터 유출에 따른 평균 피해 비용은 현재 424만 달러로, 지난해 386만 달러보다 10%나 증가했습니다. 이는 지난 7년 동안 업계가 목격한 것 중 가장 큰 증가치로, 이로 인해 보안 문제가 최우선 관심사로 떠오르고 있습니다. 보안 전략을 개선하는 일, 그리고 모든 것이 상시 가동되는 세상에서 기업에 신속하고 안전한 기동성을 지원하는 일이 오늘날 수많은 경영진의 주요 고민거리로 자리잡게 되면서, 결과적으로 보안 예산이 증가하고 있습니다. 하지만, 증가한 지출과 기술 변화는 새로운 복잡성과 위험을 유발하여 IT 보안을 계속 위협하고 있습니다. 보안 전문가의 가장 큰 관심사 중 하나는 정교한 공격 벡터가 증가하고 있다는 점입니다. 이는 그 어느 때보다 오늘날 기업의 많은 측면을 노출시킵니다.

하드웨어 및 펌웨어 수준의 취약성은 가까운 과거만 해도 그리 큰 우려 사항이 아니었을 수 있지만, 오늘날과 같은 위협 환경에서는 그러한 취약성이 일차적 표적이 됩니다.

여러 면에서, 오늘날 기업이 극복해야 할 사이버 보안 문제는 아래의 두 가지 경험적 사실로 요약할 수 있습니다.

- IT 스택이 확장되고 있으며 해커들이 영역을 넓히고 있습니다.
- 조직은 미래의 위협에 한 발 앞서 대비하여 최고 수준의 보안으로 하이브리드 클라우드 인프라를 보호해야 합니다.

424만 달러

데이터 유출에 따른 평균 비용은 현재 **424만 달러로, 지난해 기록된 386만 달러보다 10%** 증가했습니다.

오늘날 위협 환경의 현실

거시적 접근 방식

기업은 지적 재산과 민감한 기업 정보, 고객 정보, 워크로드 정보에 대한 현재와 미래의 위협을 방지하기 위해 보안 시스템에 의존하고 있습니다.

데이터 유출과 사이버 공격을 방지하기 위해서는 전문가가 IT 보안에 전략적으로 접근하는 것이 관건입니다. 보안 취약성은 가동 휴지시간으로 이어질 수 있을 뿐만 아니라 어느 조직에나 추가 비용을 초래합니다. 랜섬웨어 공격은 공격당 평균 462만 달러의 손실을 입히는 최대 위협입니다[1]. IBM® Power® 플랫폼은 무결성을 바탕으로 엔드포인트 탐지 및 대응(EDR), 지속적인 다단계 인증(MFA)과 같은 제로 트러스트 개념을 구현하여 랜섬웨어의 위험을 줄입니다.

비즈니스 중심, 규정 준수 중심 또는 재무 중심 접근 방식을 채택하는 것만으로는 증가하는 IT 시스템 위험으로부터 비즈니스 프로세스를 적절하게 보호할 수 없습니다. 단독 접근 방식을 채택하면 효율적인 통합 보안 전략이 다루는 주요 교차 분야를 놓칠 수 있습니다. 이상적인 대처 방식에는 보안과 관련된 주요 영역에서 위험을 식별해내는 계획과 평가가 포함됩니다. IBM Power 기술과 IBM® Power10 프로세서 기반 시스템은 조직의 보안과 규정 준수를 보장하는 보안 전략을 세우기 위해 거시적이고 다층적인 제로 트러스트 접근 방식을 제공합니다. 이러한 다층적인 접근 방식에는 다음 사항이 포함됩니다.

- 하드웨어
- 운영 체제
- 펌웨어
- IBM® PowerSC 2.0 기술
- 하이퍼바이저

거시적인 보안 접근 방식을 채택하면 조직은 보안 환경에 영향을 미치는 위협의 요구 사항을 충족할 수 있습니다.

점점 더 정교해지는 해커

조직이 기존 사내 구축형 데이터 센터의 제약에서 벗어나 하이브리드 클라우드 또는 멀티 클라우드 환경으로 전환할수록, 사이버 공격자는 기존의 틀을 더 많이 깨야 합니다. 최소한의 권한만을 구현하고 경계 기반 제어를 강화하면 증가하는 위협을 관리하는 데 도움이 됩니다. 과거의 방법은 더 이상 네트워크 수준에 포함되지 않으므로 공격의 범위가 넓어지고 공격 능력도 강화되고 있습니다.

데이터 액세스 증가에 따른 보안 필수

이제 직원은 서버, 하이브리드 클라우드 환경, 수많은 모바일 및 에지 기기 등 어디에서나 조직의 데이터를 저장하고 액세스할 수 있습니다. 이처럼 서버와 기기 간에 뗄래야 뗄 수 없는 교차는 지속적인 디지털 전환과 현대화의 부산물입니다. 따라서 악용되기 쉬운 공격 벡터를 수도 없이 만들어내는 결과를 초래합니다.

위험 프로파일에 영향을 미치는 엄격한 규제

규정 준수를 보장하기 위해 시행 중인 프로세스 또한 의도하지 않은 위험 노출을 야기할 수 있습니다. EU 개인정보보호 규정(GDPR)은 요즘 증가하고 있는 추세 중 하나에 불과합니다. 규제 기관은 조직이 데이터를 사용하는 방식에 훨씬 세심한 주의를 기울이고 있지만, 이는 또한 평상시의 기업 운영에 복잡성을 가중합니다.

직원으로 인해 필연적으로 발생하는 취약성

직원이 개입된 인증 정보 유출은 지난해 발생한 전체 데이터 유출 사건 중 20%에 해당합니다[1]. 로그인 정보 외에도 피싱 사기와 이메일 정보 유출은 직원 본인도 모르는 사이에 회사 정보를 위험에 빠뜨리는 또 다른 원인이 됩니다. 어떤 보안 통제를 적용하든, 취약성을 얼마나 잘 처리하든 직원은 항상 어느 정도의 위험을 초래하기 마련입니다. 사이버 범죄 시대에는 일반적인 보안 위협에 대해 직원을 교육하고 보고 시스템을 마련하는 것이 필수입니다. 엔드포인트를 보호하고 규정을 준수하는 데 들인 노력이 직원의 실수나 지능형 악성 공격으로 인해 무의미해질 수 있습니다.

한편, 많은 조직에서 유능한 사이버 보안 직원을 채용하고 근속을 유지하는 데 어려움을 겪고 있으며 늘 기술 부족에 시달리고 있습니다. 이러한 기술 부족을 해결하기 위해 조직은 운영, 규정 준수, 패치 적용, 모니터링 작업을 자동화하는 단순화된 보안 관리를 구현할 수 있습니다. 별도의 리소스 없이도 추가 엔드포인트 탐지를 통해 보호하도록 설계된 엔드투엔드 보안의 이점을 누릴 수 있습니다.

오늘날 사이버 위협 환경의 규모와 다양성, 속도는 IT 아키텍처가 계속해서 진화하면서 기술, 업무 문화, 규정 준수의 변화 추세에 적응해 감에 따라 더욱 증가하게 될 것입니다. 따라서 보안 전략도 네트워크 수준 이상으로 발전해야 합니다.

제로 트러스트 전략은 필수

거시적 접근 방식

제로 트러스트 개념을 구현하면 흔히 복잡한 IT 환경에서 조직이 보안을 해결하는 데 효과적일 수 있습니다. IT 전문가는 하이브리드 클라우드 및 멀티클라우드 환경에서 가시성과 제어를 확보하는 데 어려움을 겪고 있습니다. 제로 트러스트는 성능이나 사용자 경험에 지장을 주지 않으면서도 액세스 제어권을 제한하는 보다 포괄적인 전략으로 위험을 관리합니다. 아울러 다양한 타사 공급업체 보안 솔루션을 구현하여 스택의 모든 단계에 보안을 강화할 수 있습니다. 하지만 이러한 접근 방식은 이미 존재하는 복잡성을 악화하고 네트워크에 훨씬 더 많은 취약성과 노출 지점을 야기합니다. 최선의 방법은 다층적인 제로 트러스트 접근 방식을 취하는 것으로, 이는 조직의 모든 데이터와 시스템을 보호하는 동시에 복잡성을 최소화해줍니다. IBM® Information Security Framework는 이 점을 염두에 두고 있으며, 비즈니스 중심 보안에 거시적인 접근 방식을 사용할 때 IT 보안의 모든 측면을 적절하게 처리하도록 보장합니다.

IBM Information Security Framework는 다음 사항을 중점적으로 다룹니다.

1. 인프라 - 사용자, 콘텐츠, 애플리케이션에 대한 인사이트를 통해 정교한 공격으로부터 보호합니다.
2. 고급 보안 및 위협 연구 - 취약성과 공격 방법에 대한 전문 지식을 확보하고, 보호 기술을 통해 해당 인사이트를 적용합니다.
3. 인력 - 포괄적인 ID 인텔리전스를 통해 보안 도메인 전반에 걸쳐 기업의 ID를 관리하고 확장합니다.
4. 데이터 - 조직에서 가장 신뢰하는 자산의 개인 정보 및 무결성을 보호합니다.
5. 애플리케이션 - 보안 애플리케이션 개발 비용을 더욱 절감합니다.
6. 보안 인텔리전스 및 분석 - 추가 컨텍스트와 자동화, 통합 기능으로 보안을 최적화합니다.
7. 제로 트러스트 철학 - 조직을 보호하는 동시에 올바른 사용자를 올바른 데이터에 연결합니다.

IBM Security Framework (PDF, 25.2MB)와 그 활용 방법에 대해 자세히 알아보세요.

IBM Power 기술이 스택을 보호하는 방식

IBM Power 살펴보기

IBM Power 기술을 사용하면 프로세서, 펌웨어, OS, 하이퍼바이저, 애플리케이션, 네트워크 리소스, 보안 시스템 관리를 망라한 전체 스택에 걸쳐 통합되고 포괄적인 엔드투엔드 보안을 통해 사이버 복원력을 높이고 위험을 관리할 수 있습니다.

하드웨어, 펌웨어, 하이퍼바이저

온칩 액셀러레이터
IBM Power10 프로세서 칩은 사이드 채널 완화 성능을 개선하도록 설계되었으며 서비스 프로세서로부터 향상된 CPU 격리를 갖추고 있습니다. 이 7nm 프로세서는 최대 3배 용량을 제공하도록 설계되어 성능을 향상합니다[2].

엔드투엔드 암호화
IBM Power 솔루션의 투명한 메모리 암호화는 기업이 현재 직면한 까다로운 보안 기준을 충족하도록 설계되어 엔드투엔드 보안 기능을 제공합니다. 아울러 암호화 가속, 양자 안전 암호화, 완전한 동형 암호화를 지원하여 향후 위협을 보호하도록 설계되었습니다. 최신 IBM Power 시스템 모델의 가속 암호화는 IBM Power E980 기술보다 코어당 2.5배 더 빠른 고급암호화표준(AES) 암호화 성능을 제공합니다[3]. 조직은 이를 사용하여 추가 관리 설정 없이도 투명한 메모리 암호화의 이점을 누릴 수 있습니다.

EDR 소프트웨어
외부 위협의 증가로 인해 고객 정보와 디지털 자산 보호에 있어 엔드포인트 보안이 매우 중요해졌습니다. 엔드포인트에서 잠재적인 위협을 탐지하면 비즈니스 연속성을 해치지 않고도 신속하게 조치를 취하고 보안 사고를 해결할 수 있습니다. 통합 접근 방식은 복잡성을 제거하고 치명적인 공격으로부터 조직을 보호해 줍니다.

2.5배

최신 IBM Power 시스템 모델의 가속화된 암호화는 IBM Power E980 기술보다 **코어당 2.5배 더 빠른 고급 암호화 표준(AES) 암호화 성능**을 제공합니다[3].

다단계 인증, 최소 권한 등의 원칙을 활성화하면 모든 API, 엔드포인트,데이터, 하이브리드 클라우드 리소스를 안전하게 지키는 추가 보호 기능이 제공됩니다.

제로 트러스트 원칙
조직은 증가하는 위협을 관리하는 데 도움이 되는 제로 트러스트 원칙을 채택하고 있습니다. 다단계 인증, 최소 권한을 비롯한 원칙을 활성화하면 모든 API, 엔드포인트, 데이터, 하이브리드 클라우드 리소스를 안전하게 지키는 추가 보호 기능이 제공됩니다.

IBM 제로 트러스트 프레임워크는 이러한 개념을 현실화합니다.

- **인사이트 확보** – 사용자, 데이터. 리소스를 파악하여 완전한 보호를 보장하는 데 필요한 보안 정책을 세웁니다.
- **보호** – 컨텍스트를 빠르고 일관되게 검증하고 정책을 시행하여 조직을 보호합니다.
- **탐지 및 대응** – 비즈니스 운영에 미치는 영향을 최소화하고 보안 위반을 해결합니다.
- **분석 및 개선** – 정책과 관행을 조정하여 정보에 입각한 결정을 내림으로써 보안 태세를 지속적으로 개선합니다.

기업은 제로 트러스트 원칙을 구현하여 안전하게 혁신하고 확장할 수 있습니다.

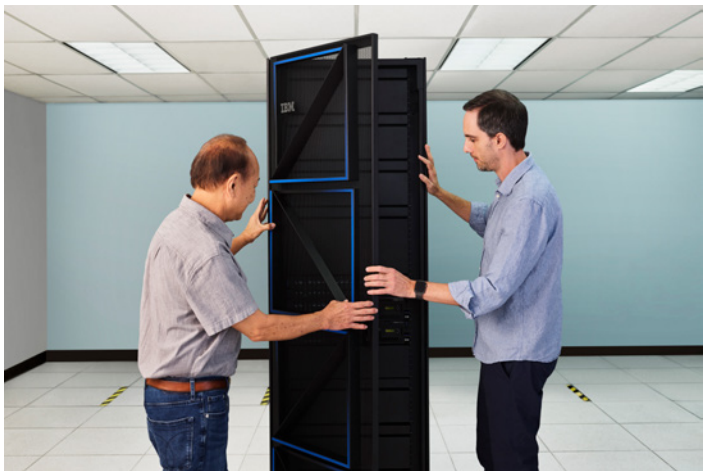
IBM Power10 솔루션의 보안 부팅
보안 부팅은 디지털 서명을 통해 펌웨어의 모든 구성 요소를 확인하고 검증하여 시스템의 무결성을 보호하도록 설계되었습니다. IBM에서 출시한 모든 펌웨어는 부팅 프로세스의 일부로 디지털 서명되고 검증됩니다. 모든 IBM Power 시스템은 서버에 로드된 모든 펌웨어 구성 요소의 측정값을 누적하여 검사와 원격 검증을 가능하게 하는 신뢰할 수 있는 플랫폼 모듈과 함께 제공됩니다.

IBM PowerVM 엔터프라이즈 하이퍼바이저
IBM PowerVM® 엔터프라이즈 하이퍼바이저는 주요 경쟁업체와 비교해 뛰어난 보안 성능을 갖춰 가상 머신(VM) 및 클라우드 환경을 확실하게 보호합니다.

운영 체제

IBM Power 시스템은 IBM® AIX®, IBM i, Linux®를 비롯해 광범위한 운영 체제에 최고의 보안 기능을 제공합니다. IBM Power용 엔드포인트 탐지 및 대응(EDR) 기술은 VM 워크로드에 추가 보안을 제공하여 네트워크 내 모든 엔드포인트에서 완벽한 보호 효과를 보장합니다. 보안을 위해 암호화를 이용하는 시스템의 경우 AIX와 리눅스 운영 체제가 모든 사용자에 대해 추가 인증 절차를 요구하는 IBM PowerSC 다단계 인증(MFA)를 활용하여 비밀번호 크래킹 맬웨어로부터 보호합니다. 기능은 운영 체제에 따라 달라지지만, 다음과 같은 예시를 참고할 수 있습니다.

- 보안을 타협하지 않으면서도 일반적으로 루트 사용자를 위해 예약된 관리 기능 할당
- 개별 키 저장소를 통해 파일 수준 데이터 암호화
- 사용자가 액세스할 수 있는 개체에 대한 제어력과 함께, 사용자가 사용할 수 있는 명령과 기능에 대한 제어 능력 향상
- 사용자 및 개체에 대한 시스템 값과 개체 감사 값을 사용하여 보안 감사 저널에 개체에 대한 액세스 기록
- 개체를 먼저 암호화하고 암호화된 형식으로 작성하여 전체 드라이브에 암호화 수행
- 요청한 사용자를 위해 열기 전에 모든 파일을 측정하고 확인



워크로드, VM, 컨테이너

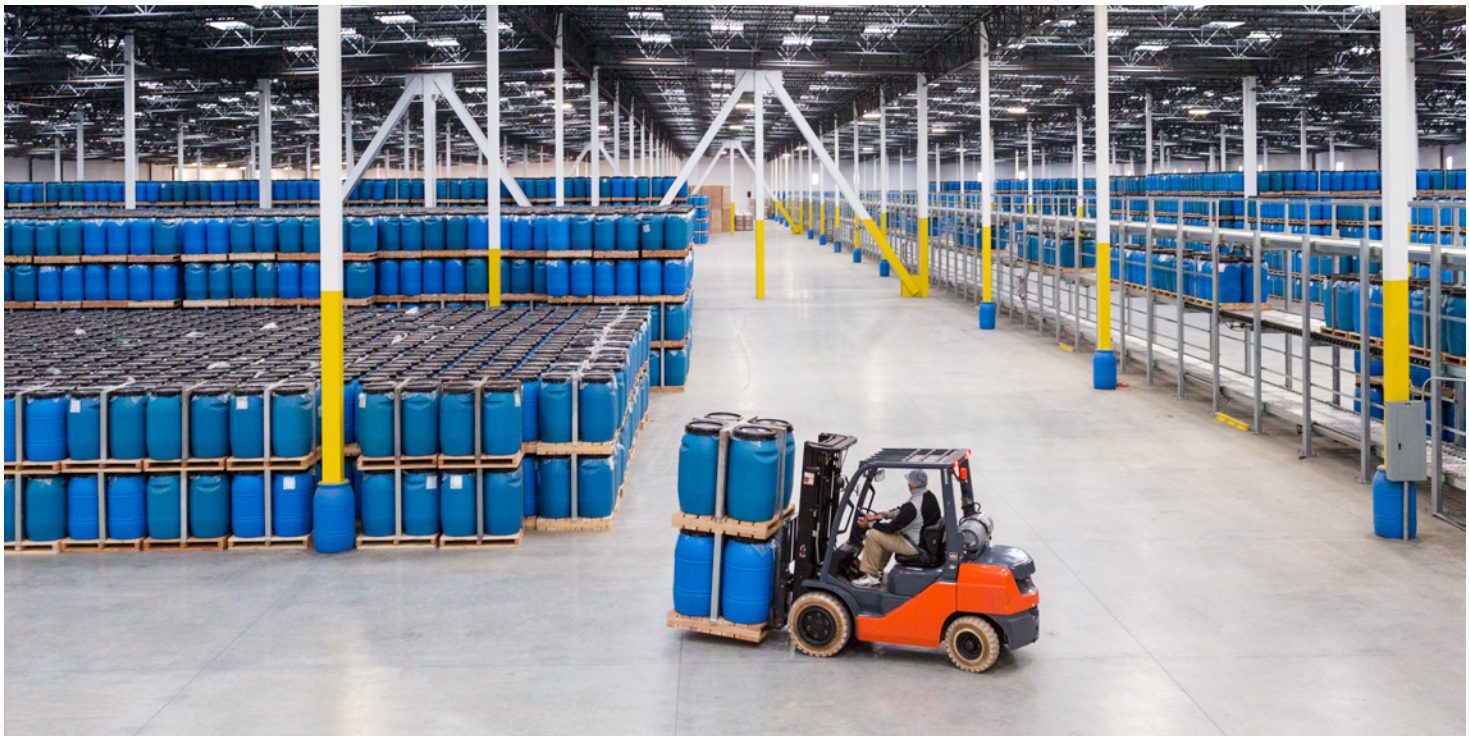
워크로드는 더 이상 사내 구축형 데이터 센터로 제한되지 않고, 가상화된 하이브리드 클라우드 및 멀티클라우드 환경으로 끊임없이 이동하고 있습니다. 한 예로, 대다수 조직은 컨테이너를 채택하여 하이브리드 인프라 전반에 걸쳐 신규 애플리케이션과 기존 애플리케이션을 배포하고 있습니다.

이처럼 점점 더 동적으로 변화하는 환경과 워크로드에는 동일한 수준으로 활용도 높은 보안 기능이 필요합니다. IBM Power 솔루션은 암호화 알고리즘 가속화, 보안 키 스토리지, 포스트 양자 암호화, 완전 동형 암호화(FHE) 알고리즘을 위한 CPU 지원을 통해 워크로드의 개인 정보를 보존함으로써 보안 요건을 충족합니다.

IBM은 컨테이너형 배포에 따른 고유한 보안 요구 사항을 해결하기 위해 IBM Power 기술 및 Red Hat® OpenShift® 컨테이너 플랫폼으로 구축하여 수명 주기 내내 컨테이너를 더 안전하게 보호하는 Aqua Security와 같은 독립 소프트웨어 공급업체(ISV)와도 파트너십을 맺었습니다.

IBM Power 서버는 엔드투엔드 메모리 암호화와 가속화된 암호화 성능을 통해 사내 구축형에서 클라우드에 이르기까지 데이터를 보호하도록 설계되었습니다. VM, 컨테이너, 서버리스 기능을 비롯한 클라우드 네이티브 워크로드에 포함된 정책은 애플리케이션 현대화를 위한 보안 및 규정 준수 요구 사항을 통합할 때 Red Hat OpenShift와 IBM Power 고객을 지원하도록 구축되었습니다.

라이브 파티션 모빌리티 (LPM)
IBM Power 기술을 사용하면 전송 중인 데이터를 보호할 수 있습니다. LPM은 시스템 간에 마이그레이션해야 할 때 암호화를 통해 VM을 보호합니다. 사내 구축형 데이터 센터, 하이브리드 클라우드 환경 또는 그 모두에서 가상화했다면 이는 매우 중요한 기능입니다.



IBM Power 솔루션에 통합된 보안 제품

IBM PowerSC 2.0 기술

IBM® PowerSC 2.0 기술은 클라우드와 가상 환경에서 기업용 보안 및 규정 준수를 위한 통합 포트폴리오 제품입니다. 스택의 최상위에 자리함과 동시에 최하위 레벨업 솔루션에 상주하는 IBM Power 기술의 보안 기능을 관리하는 웹 기반 UI를 제공합니다.

IBM PowerSC 2.0 기술은 단순화와 자동화 기능을 통해 규정 준수 모니터링과 시행 작업을 간소화하여 시간, 비용, 위험을 모두 줄여줍니다. 아울러 감사 프로세스를 지원하고 고객이 보다 효율적으로 규정 준수 인증을 획득하게 해줍니다. 스택 전반에 가시성을 높여 보안 위험을 줄이기도 합니다.

IBM PowerSC 2.0 Standard Edition의 기능

다단계 인증(MFA) 기술
이제 MFA 기술이 IBM PowerSC 2.0 솔루션에 통합되었습니다. 이는 '절대 신뢰하지 말고, 항상 검증하라'는 제로 트러스트 원칙에 따라 MFA 메커니즘의 배포를 간소화합니다. 이 접근 방식은 사용자가 RSA SecurID 기반 인증 및 공통 액세스 카드(CAC), 개인 신분 확인(PIV) 카드를 비롯한 인증서 옵션을 사용해 로그인할 수 있는 대안 방식을 지원합니다. IBM PowerSC MFA는 사용자에게 추가 인증 요소를 요구하여 시스템의 보안 수준을 강화합니다.

IBM PowerSC 2.0 기술로 시간, 경비, 위험을 절감

EDR 기능
IBM PowerSC 2.0 솔루션은 침입 탐지와 방지, 로그 검사와 분석, 이상 탐지와 사고 대응을 비롯해 엔드포인트 보안을 관리하기 위한 최신 업계 표준 기능을 제공하는 Linux용 EDR을 IBM Power 워크로드에 도입합니다.

규정 준수 자동화
IBM Power 제품군에는 수많은 업계 표준을 지원하는 프로필이 사전 탑재되어 있습니다. 확장 가능한 마크업 언어(XML)를 건드릴 필요 없이 이러한 프로필을 사용자 정의하고, 기업의 규칙과 통합할 수 있습니다.

실시간 규정 준수
누군가 중요한 보안 파일을 열거나 이와 상호 작용할 때 탐지하고 경고합니다.

신뢰할 수 있는 네트워크 연결
VM이 지정된 패치 수준에 있지 않을 때 경고를 보내고, 수정 사항을 사용할 수 있게 되면 알려줍니다.

신뢰할 수 있는 부팅
AIX 논리 파티션에서 실행 중인 모든 소프트웨어 구성 요소의 무결성을 검사하고 원격으로 확인합니다.

신뢰할 수 있는 방화벽
AIX, IBM i, Linux 운영 체제 간 내부 네트워크 트래픽을 보호하고 라우팅합니다.

신뢰할 수 있는 로깅
손쉽게 백업, 보관, 관리 작업할 수 있는 중앙 집중식 감사 로그를 생성합니다.

사전 구성된 보고 및 대화형 타임라인
IBM PowerSC Standard Edition은 사전 구성된 다섯 개의 보고서로 감사 작업을 지원합니다. 또한 VM의 수명과 이벤트를 볼 수 있는 대화형 타임라인도 갖추고 있습니다.

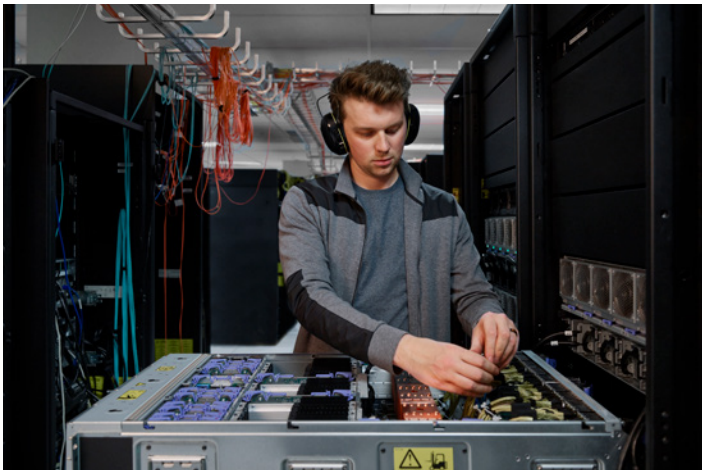
클라우드 및 가상화 환경 내 IBM PowerSC를 통해 IT 보안과 규정 준수 관리를 간소화하는 방법을 알아보세요.

가장 강력한 보안 접근 방식은 완벽하게 통합된 접근 방식

완벽한 통합

사이버 범죄자의 공격 방법이 계속 발전하고 있고, 기술 발전으로 오늘날 기업이 새로운 취약성에 노출됨에 따라 조직에 복잡성을 가중시키지 않는 다층적인 제로 트러스트 보안 솔루션을 통합하는 것이 중요해졌습니다. IBM Power 솔루션은 단일 공급업체의 긴밀하게 통합된 심층 솔루션을 통해 에지, 클라우드, 코어까지 모든 수준의 스택을 보호합니다. 여러 공급업체와 작업하면 결국 여러 모로 비용이 많이 들 수 있는 복잡성이 발생합니다. IBM Power 기술은 성능에 차질을 주지 않으면서 프로세서 수준에서 엔드투엔드투 암호화를 지원합니다. 인프라를 하나로 통합하면 스택의 모든 계층에 초점을 맞출 수 있습니다.

단일 공급업체를 이용하면 보안 전략을 단순화하고 강화하는 자연스러운 이점을 얻을 수 있습니다. IBM Power 기술은 30년 전통의 보안 리더십을 바탕으로 IBM 내부 및 외부 조직과의 폭넓은 파트너십을 통해 보안 전문성을 더욱 심화하고 확장해 나갑니다. IBM Power 기술은 이러한 파트너십을 통해 훨씬 더 큰 보안 전문가 커뮤니티를 활용할 수 있을 뿐만 아니라 문제를 신속하게 파악하고 확실하게 해결합니다. Power10 서버는 PowerSC 2.0 제품군은 물론 IBM Security®, IBM Research® 사업부의 지원을 받아 내부자 공격을 비롯한 여러 위협을 위에서 아래로 무력화합니다.



IBM Power 솔루션의 잠재력에 대해 자세히 알아보려면 상담을 예약하세요.

문의하기 →

참고
1. 2021 데이터 유출 비용 보고서, IBM Security, 2021년 7월 (PDF, 3.6MB)
2. 3배 성능은 2×30-코어 모듈의 POWER10 듀얼 소켓 서버 제품과 2×12-코어 모듈의 POWER9 듀얼 소켓 서버 제품의 엔터프라이즈 및 부동소수점 환경에 대한 사전 실리콘 엔지니어링 분석을 기반으로 하며, 두 모듈 모두 동일한 에너지 레벨을 가지고 있습니다.
2 10-20배 AI 추론 개선은 2×30-코어 모듈의 POWER10 이중 소켓 서버와 2×12-코어 모듈의 POWER9 이중 소켓 간의 다양한 워크로드(Linpack. Resnet-50 FP32, Resnet-50 BFloat16, Resnet-50 INT8)에 대한 사전 실리콘 엔지니어링 분석을 기반으로 합니다.
3. GCM 및 XTS 모드의 AES-256은 RHEL Linux 8.4 및 OpenSSL 1.1.1g 라이브러리에서 얻은 예비 측정값에 따라 IBM Power10 E1080(15코어 모듈)과 IBM POWER9 E980 (12코어 모듈) 비교 시 코어당 약 2.5배 더 빠르게 실행됩니다.

(07326) 서울특별시 영등포구 국제금융로 10
서울국제금융센터(3IFC)

미국에서 제작됨
2022년 6월