SAP용 SailPoint Identity Security

전 세계 대부분의 기업은 SAP의 전사적 자원 관리(ERP) 도구 및 시스템을 활용하여 서로 다른 비즈니스 프로세스를 통합합니다. 이러한 엔터프라이즈 SAP 환경은 모듈, 애플리케이션 서버, 레거시 인터페이스, 사용자 설정, 다양한 구조로 구성된 고도로 복잡한 시스템입니다.

이처럼 방대한 환경을 파악하고, 특히 각종 SAP 시스템 및 애플리케이션에 대한 사용자 액세스를 간편하게 관리하고 제어할 수 있는 능력은 조직의 보안 태세와 전반적 생산성 및 원활한 운영의 성패를 결정하는 요소입니다. 더욱이 SAP 비즈니스의 중대한 변화와 전반적인 구조적 복잡성으로 인해 안전하고 포괄적인 액세스 솔루션의 필요성이 부각되고 있습니다.

- 첫째, SAP의 **클라우드 중심 전략** 및 온프레미스 SAP ECC(SAP Enterprise Central Component)에서 클라우드 기반 S/4HANA으로의 전환은 기존의 온프레미스 솔루션이 아니라 클라우드 기반 플랫폼을 사용해서 SAP 제품과 서비스를 개발, 제공, 개선하는 데 초점을 맞추고 있습니다.
- 둘째, SAP 환경은 온프레미스, 클라우드, 하이브리드 및 맞춤형 애플리케이션과 솔루션 수십 개에 이르며 비SAP 애플리케이션 등과 함께 SAP 환경 내부와 외부 모두에서 **복잡한 데이터 플로**를 형성합니다.
- 중앙 집중화된 정책이 마련되지 않은 상태에서의 **미승인 SAP 시스템 및 애플리케이션 액세스**는 조직에 큰 부담이 될 수 있습니다. 또한 S/4HANA로의 전환을 추진하고 더 많은 클라우드 기반 솔루션을 도입하는 조직에게는 액세스를 보호하고 전환과 관련된 위험을 완화할 솔루션이 필요합니다.

- 마지막으로 기업은 액세스를 관리해야 하며 **SAP 애플리케이션 뿐만 아니라 모든 전사적 애플리케이션에 대한 종단 간 보안 조치**를 확립해야 합니다. SAP IdM(SAP Identity Management)과 같은 SAP 레거시 아이덴티티 보안 시스템의 수명이 다하고 있는 만큼, 기업들은 비즈니스를 보호하고 클라우드 전환을 지원하며 엄격한 규정, 컴플라이언스, 정책 요건을 충족하는 대안적 아이덴티티 보안 솔루션을 찾고 있습니다.

SAP 환경에서의 아이덴티티 보안 과제

SAP 고객 및 관리자는 복잡한 SAP 환경의 전반적 거버넌스와 컴플라이언스에 영향을 미칠 수 있는 다음과 같은 주요 아이덴티티 보안 문제들에 직면하고 있습니다.

- **중앙 집중식 보안 정책**을 이해하고 수립해야 합니다.
- SAP 온프레미스, 클라우드, 하이브리드 모듈과 애플리케이션에서 **액세스 권한 및 제어 관리**의 복잡성을 직면하고 있습니다. 사용자 권한을 소홀하게 관리할 경우 무단 액세스로 이어져 심각한 보안 위험이 초래될 수 있습니다.
- 대부분 여러 SAP 애플리케이션에 대한 **프로비저닝이 주로 수작업**으로 진행되어 자동화와 효율성 개선이 필요합니다.
- 입사, 직무 이동, 퇴사 등의 잦은 조직 변동 속에서도 **정확한 사용자 기록을 유지**해야 합니다. 라이프사이클 관리를 자동화하지 않으면 사용자 권한을 신속하게 업데이트하는 데 상당한 노동력이 소모되며 그 과정에서 오류가 발생할 가능성도 높아집니다.
- **업무 분리(SoD) 충돌 및 액세스 인증의 모니터링과 시행**을 비롯한 거버넌스, 위험 및 컴플라이언스(GRC) 요건 등과 같은 충돌을 해소하지 않을 경우 사내 부정 행위 및 컴플라이언스 위반이 발생할 수 있습니다.
- **SAP 시스템을 기존 아이덴티티 거버넌스 프레임워크와 통합**할 때는 원활한 상호 운영성 및 종합적 감독 능력을 확보하기 위해 전문적 지식과 상당한 리소스가 요구되는 경우가 많습니다.
- 레거시 아이덴티티 보안 관리자와 SAP 관리자 간의 **협업이 필요**합니다. 두 관리자는 아이덴티티 보안 및 제로 트러스트 이니셔티브와 관련하여 협력하면서 비즈니스 전반의 액세스를 적절히 관리해야 합니다.

SAP용 SailPoint Identity Security: 디지털 전환을 위한 솔루션

SailPoint 엔터프라이즈 아이덴티티 보안을 통해 기업은 사용자 및 핵심 애플리케이션과 리소스에 대한 액세스를 관리, 통제, 중앙 집중화할 수 있습니다. 이를 통해 조직은 액세스를 중앙 집중식으로 관리 및 제어하고, 일관된 정책을 적용하며, 위협을 감지하고, 위험을 파악할 수 있습니다.

SAP용 SailPoint Identity Security는 SailPoint Identity Security Cloud와 IdentityIQ 모두를 아우르는 유연한 솔루션으로 구성되어 있습니다. 조직은 이를 활용하여 온프레미스, 클라우드, 하이브리드 환경에서 SAP에 대한 액세스를 보호하고 그에 대한 감사를 수행할 수 있으며, SAP 애플리케이션, 인프라, 서비스 전반의 액세스 경로에 대한 세부 정보를 수집하고 SoD 및 GRC 요건을 충족할 수 있습니다.

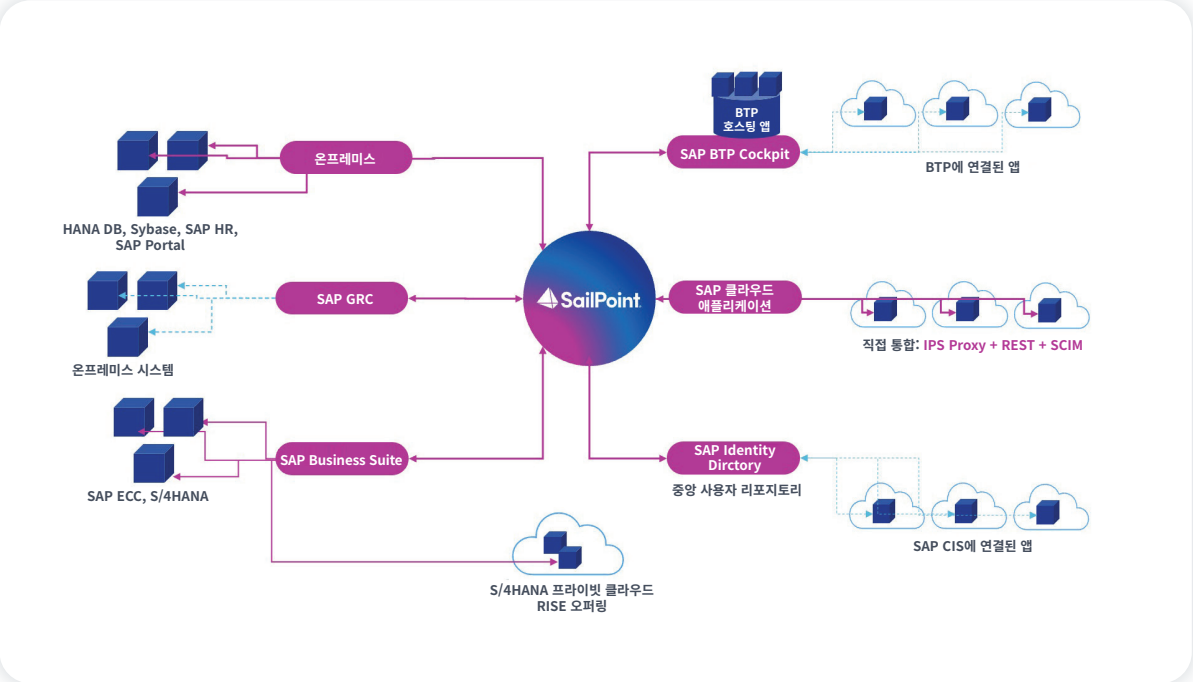


그림 1: SAP용 SailPoint Identity Security

이러한 솔루션은 다음과 같은 방식으로 기업이 복잡한 SAP 환경에 대하여 실질적 거버넌스를 구축하고 보안 및 디지털 전환 과제를 해결할 수 있게 도와줍니다.

- **새로운 SAP 클라우드 인프라 서비스를 포괄적으로 지원하여 신속한 도입 촉진:** SAP의 레퍼런스 아키텍처에 따라 SAP BTP(SAP Business Technology Platform) 및 SAP IAS(Identity Directory/ Identity Authentication Service) 등 SAP의 새로운 클라우드 인프라 통합이 포함되어 SAP CIS(Cloud Identity Services)를 통해 40개 이상의 SAP 애플리케이션에 대한 중앙 집중식 사용자 관리와 프로비저닝을 지원합니다.
- **SAP 클라우드 업무 영역 애플리케이션 및 서비스에 대한 액세스를 관리하고 보호하는 기능:** SAP의 IPS(SAP Identity Provisioning Services)를 사용해 SuccessFactors, SAP HR, Concur, Ariba, Fieldglass 등과 같은 가장 중요한 SAP 클라우드 업무 영역 애플리케이션과 통합함으로써 비즈니스 요구 사항에 따라 조정 가능한 신속하고 확장성 있는 통합을 구현할 수 있습니다.
- **클라우드로 전환하는 고객에게 일관된 아이덴티티 보안을 제공할 수 있는 통합 기능:** 온프레미스 SAP Business Suite 애플리케이션과 S/4HANA 클라우드에 대한 포괄적인 아이덴티티 보안을 제공하며, SAP RISE로 전환하는 SAP ECC 애플리케이션을 지원하고 SAP GRC 및 SAP IAG(SAP Identity Access Governance)와 통합하여 SoD 검사를 수행합니다.
- **SAP 온프레미스 및 하이브리드 환경을 위한 보안 지원:** SAP ECC, S/4HANA, SAP GRC와 같은 SAP 온프레미스 애플리케이션에 대한 심층적 거버넌스 기능을 제공하여 위험 분석, 프로비저닝, 액세스 인증을 뒷받침하며, 하이브리드 SAP 환경 전반에 대한 SoD 점검을 통해 기업이 중앙 집중식 보안을 확립하고 액세스에 대하여 전방위적 투명성을 확보할 수 있도록 지원합니다.
- **SoD 요구 사항을 충족하는 솔루션 제공:** 기업이 여러 애플리케이션에서 중앙 집중식 보안 정책을 구현하고, 위험 요소, 정책 위반, 액세스 인증을 점검할 수 있도록 다양한 옵션을 제공합니다. 여기에는 SailPoint ARM(Access Risk Management), SAP GRC 통합, 하이브리드 에코시스템에서 온프레미스 및 클라우드 SAP 애플리케이션의 프로비저닝과 SoD 분석을 위해 SAP GRC와 SAP IAG를 사용하는 조직을 위한 SAP GRC-IAG(Identity Access Governance) 브리지 통합이 포함됩니다.

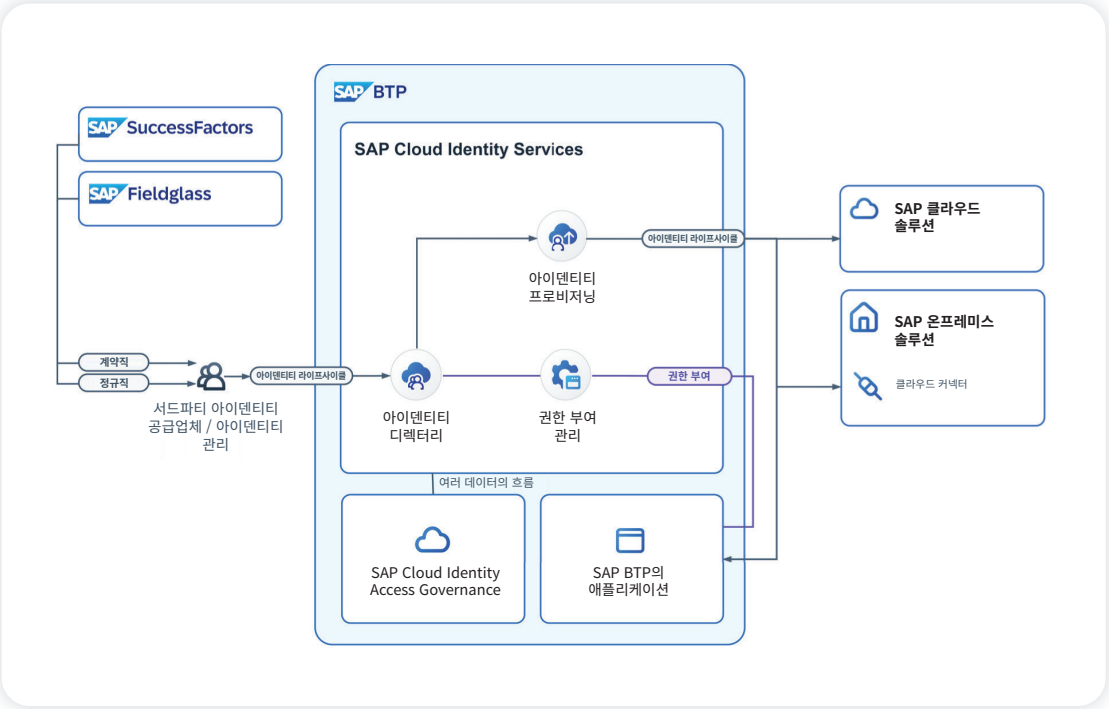
SAP용 SailPoint Identity Security 솔루션은 디지털 전환의 어느 단계에서도 SAP 클라우드, 온프레미스, 하이브리드 애플리케이션 및 서비스에 대한 액세스를 확인하고 제어하고 관리할 수 있도록 지원하며, 기업의 필요에 따라 SoD와 액세스 인증 기능을 구현할 수 있게 합니다.

클라우드 도입 여정: SAP와 연계된 전환 솔루션

SailPoint는 1,100개 이상의 엔터프라이즈 애플리케이션과 20,000개의 맞춤형 애플리케이션을 지원합니다. 고객은 SaliPoint의 기술력을 활용하여 단일 아이덴티티 플랫폼을 바탕으로 SAP 고객이 일상적으로 사용하는 주요 비즈니스 애플리케이션의 핵심적 아이덴티티 보안 기능을 확장, 연결, 통합할 수 있으며 이를 통해 아이덴티티 보안의 가치 실현 시간을 단축할 수 있습니다.

SailPoint와 SAP의 전략적 기술 협력이 이를 입증하는 대표적 사례입니다. SAP를 위한 당사의 포괄적 아이덴티티 보안 솔루션은 업계의 모범 사례 및 SAP 기술 요건에 모두 부합하므로 조직은 이를 바탕으로 주요 액세스를 보호하고 안전하게 클라우드로 전환할 수 있습니다.

SailPoint의 SAP 애플리케이션용 아이덴티티 보안 접근 방식은 SAP의 전략적 비전, 레퍼런스 아키텍처, 제품 구성, 통합 환경, 방법론, 로드맵과 일치합니다. 예를 들어 SailPoint 애플리케이션 통합은 SAP의 IPS(Identity Provisioning Service) API를 활용함으로써 고객이 가장 널리 사용되는 SAP 클라우드 애플리케이션으로 신속하게 아이덴티티 보안을 확장할 수 있도록 지원합니다.



출처: SAP CIO Guide: Identity Lifecycle in SAP Landscapes, 30페이지

이러한 핵심 아이덴티티 보안 기능으로는 액세스 요청, 액세스 승인, 라이프사이클 관리, 내부 인증, 주요 SAP 애플리케이션에 대한 심층적인 거버넌스를 뒷받침하는 인사이트 등이 있습니다. 또한 필요한 경우 고객의 구체적 요구 사항에 따라 해당 프레임워크를 확장하여 심층적 컨텍스트와 거버넌스를 제공하고 REST, SCIM, SOAP 및 기타 표준 연결성 옵션들을 통해서 확장성을 지원할 수도 있습니다.

더 나아가 SAP의 BTP(Business Technology Platform)와의 통합, 관련 SAP CIS(Cloud Identity Services), SAP의 RISE 관리형 서비스와의 상호 운용성을 통해서 SAP 시스템에 추가되는 SailPoint의 엔터프라이즈 아이덴티티 보안 기능을 바탕으로 기업은 SAP 애플리케이션 및 서비스 전반에서 원활한 사용자 액세스 관리 환경을 구축하면서도 액세스 보안을 확립할 수 있습니다.

SailPoint는 SAP GRC 및 SAP GRC/IAG Bridge와의 심층적인 통합도 지원합니다. 두 가지 통합 모듈은 모두 프로비저닝 요청에 대한 위험 분석 기능을 제공할 뿐만 아니라 논리적 액세스 및 SoD 충돌에 대한 IT 거버넌스 제어 수단을 제공합니다.

마지막으로 조직은 SailPoint Identity Security Cloud와 IdentityIQ 모두에서 사용할 수 있는 수천 개의 기존 연결성 솔루션을 추가로 활용하여 핵심적인 비SAP 애플리케이션(Salesforce, Workday, Microsoft Entra 등)에 대한 액세스를 제어함으로써 아이덴티티 보안의 범위를 전사적 차원으로 확장할 수 있습니다.

SailPoint는 SAP 시스템과 애플리케이션에 대하여 대규모 연결성과 기능적 확장성을 확보하는 데 전략적으로 집중함으로써 기업이 경쟁력과 보안을 유지하고, 디지털 전환 목표를 달성하며, 새로운 엔터프라이즈 시스템의 신속한 도입을 촉진하는 데 필요한 컴플라이언스, 보안 및 아이덴티티 관리 요구 사항을 강화합니다.

SailPoint

SailPoint 소개
SailPoint는 오늘날의 기업이 아이덴티티의 관점에서 애플리케이션과 데이터에 대한 액세스 권한을 대규모로 원활하고 신속하게 관리하고 안전하게 보호할 수 있도록 지원합니다. 당사는 업계 선두 주자로서 기업 보안의 기반이 되는 아이덴티티 보안을 끊임없이 혁신하고 있습니다. SailPoint가 제공하는 확장성을 갖춘 통합 지능형 플랫폼은 생산성과 효율성을 증대하면서도 오늘날의 변화를 거듭하는 아이덴티티 중심의 사이버 위협에 맞설 수 있게 합니다. SailPoint는 세계에서 가장 복잡하고도 정교한 여러 기업들이 비즈니스 혁신을 촉진하는 안전한 기술 생태계를 갖출 수 있게 돕고 있습니다.