



제로 트러스트 보안 구현 가이드

아무것도 믿지 마세요. 모든 것을 철저하게 인증하고 권한을 부여하세요.

기존의 온프레미스 데이터 센터와 환경에서 동적인 클라우드 인프라로의 전환은 매우 복잡하며, 기업 보안에 새로운 과제를 안겨 주고 있습니다. 관리해야 할 시스템이 늘어나고, 모니터링해야 할 엔드포인트는 많아졌으며, 연결할 네트워크와 액세스 권한이 필요한 인원도 더 많아지고 있습니다. 보안 침해의 발생 가능성이 크게 높아졌으며, 적절한 보안 태세를 갖추지 않는다면 보안 침해는 시간 문제일 뿐입니다.

기존 데이터 센터를 보호하기 위해서는 네트워크와 방화벽, HSM, SIEM, 그리고 기타 물리적 액세스 제한 조치를 통해 IP 기반의 경계를 관리하고 보안을 유지해야 했습니다. 하지만 기업들이 클라우드로 전환함에 따라, 이러한 기존 솔루션들만으로는 더 이상 충분하지 않습니다. 대규모 환경에서 액세스와 IP를 관리하는 방식은 불안정하고 복잡해지고 있습니다.

클라우드에서 인프라를 보호하려면 [Security Lifecycle Management\(SLM\)](#)에 대한 플랫폼 기반의 접근 방식이 필요합니다.

기업이 클라우드로 전환함에 따라, IP 기반 경계와 액세스는 임시 IP 주소와 민첩한 인력 구조로 대체되면서, 조직은 며칠이 아닌 몇 분 안에 공유 리소스에 액세스해야 합니다. 클라우드와 온프레미스 데이터 센터 전반에 걸쳐 인프라, 데이터, 액세스 권한을 보호하는 일은 점점 더 어려워지고 있으며, 이를 위해 막대한 운영 비용과 고도의 전문 지식이 요구됩니다. 이러한 변화는 기존과는 다른 신뢰 모델을 요구합니다. 즉, 아무것도 신뢰하지 않고 모든 것을 철저히 검증한 뒤 인증하고 권한을 부여하는 모델입니다.

매우 역동적으로 변화하는 분산형 클라우드 환경에서, 조직은 클라우드 보안을 위한 '제로 트러스트' 접근 방식을 논의하고 있습니다. 그렇다면 '제로 트러스트'란 실제로 무엇을 의미하며, 이를 성공적으로 도입하려면 무엇이 필요할까요?

멀티 클라우드 제로 트러스트 보안의 과제



IP 기반의 액세스 관리

인프라와 데이터, 그리고 액세스를 보호하기 위한 기존의 솔루션들은 IP 주소를 기반으로 보안을 유지하는 방식에 뿌리를 두고 있습니다. 데이터베이스와 통신하는 애플리케이션, 호스트 및 서비스에 액세스하는 사용자, 그리고 클라우드 간의 서버 통신 등, 기존에는 모두 IP 주소를 기반으로 액세스를 허용하거나 제한하여 보호해 왔습니다. 기업들이 클라우드로 전환함에 따라, 이와 동일한 인프라와 데이터에 대한 액세스를 관리하는 일은 훨씬 더 어려워지고 운영상의 복잡성 또한 심화됩니다. 이는 IP 주소가 이전보다 훨씬 유동적이며 수시로 변하기 때문입니다.



머신 연결 보안

머신 간 액세스는 클라우드 우선 조직의 핵심 요소입니다. 전통적인 티켓 시스템에 의존하는 기존의 ITIL 기반 방식은 처리 속도가 느리고 번거로울 뿐만 아니라, 오늘날의 역동적인 클라우드 환경이 요구하는 엄격한 보안 수준을 충족하기에는 유연성이 부족합니다.



수요에 따른 확장

수동 프로세스 기반의 기존 액세스 및 신원 관리 방식은 속도가 느리고 비효율적이며, 보안 효과 또한 떨어집니다. 토큰, 키 카드, 비밀번호와 같은 보안 조치들은 IT 부서의 직접적인 개입을 필요로 합니다. 특히 수백, 수천 명의 개인 사용자와 머신을 대상으로 할 경우, 이러한 방식은 막대한 리소스와 시간을 소모합니다.

멀티 클라우드 제로 트러스트 보안을 구현하는 ID 기반 제어

포괄적인 SLM이란 보안 정보와 인증서를 보호하고, 디지털 자산을 점검하여 보안되지 않은 자격 증명을 찾아내며, 오직 권한을 부여받은 머신과 서비스, 사용자만을 연결하는 것을 의미합니다. 제로 트러스트의 4가지 핵심 요소는 이러한 SLM 구성 요소의 대부분을 아우르고 있습니다.

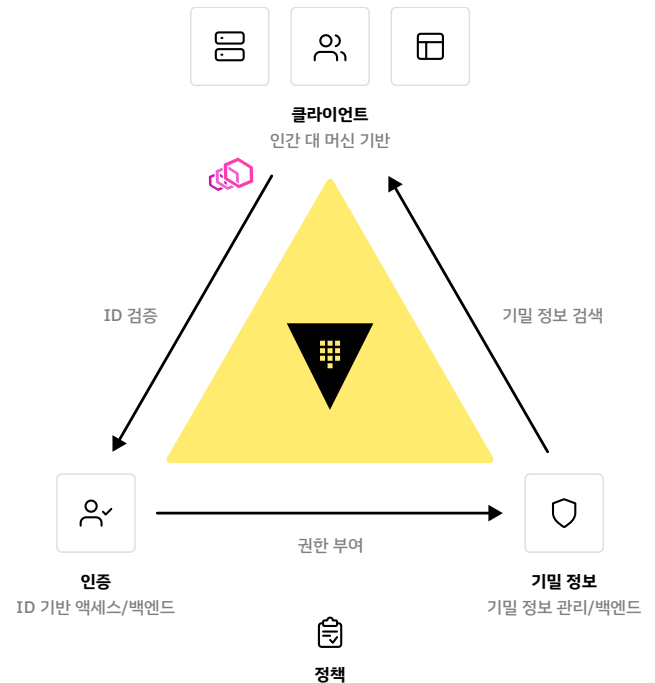
제로 트러스트의 4가지 핵심 요소

- 머신 인증 및 권한 부여
- 머신 간 액세스
- 사람 인증 및 권한 부여
- 사람과 머신 간의 액세스

이 네 가지 핵심 요소를 관통하는 일관된 요구 사항은 바로 신원 기반 제어입니다. HashiCorp의 SLM 모델은 신원 기반의 액세스 및 보안 원칙을 근간으로 합니다. 어떤 머신이나 사용자가 작업을 수행하기 위해서는, 반드시 자신이 누구인지 또는 무엇인지 인증해야 합니다. 그다음, 해당 신원에 부여된 권한에 따라 수행할 수 있는 작업이 결정됩니다. HashiCorp의 제품군이 제로 트러스트의 핵심 요소를 지원하고, 이를 통해 제로 트러스트 보안을 실질적으로 구현하는 방법은 다음과 같습니다.

머신 인증 및 권한 부여

[Hashicorp Vault](#)는 많은 기업이 하이브리드 및 멀티 클라우드 환경 전반에서 토큰, 비밀번호, 인증서, 암호화 키와 같은 동적 보안 정보를 중앙 집중식으로 저장, 액세스 및 배포하는 데 사용하는 핵심 신원 브로커입니다. 번거로운 ITIL 기반 시스템과 달리, HashiCorp 솔루션은 동적인 방식으로 수명이 짧은 자격 증명을 발급하여 시스템과 애플리케이션 간에 키, 자격 증명, 인증서 등을 빠르고 안전하게 교환할 수 있도록 지원합니다.



머신 간 액세스

HashiCorp Consul은 마이크로서비스 규모의 애플리케이션 간 암호화 및 인증을 강제함으로써 네트워크상의 머신 간 액세스 보안을 확보하고, 오직 권한을 부여받은 머신들끼리만 통신하도록 보장합니다. 또한 Consul은 신원 기반 방식을 채택하여 트래픽 규칙을 코드화하고 적용합니다. 조직은 Consul을 통해 서비스를 발견하고, 네트워크 구성을 자동화하며, Consul 서비스 메시를 사용하여 모든 클라우드 또는 런타임에서 보안 연결을 활성화할 수 있습니다.

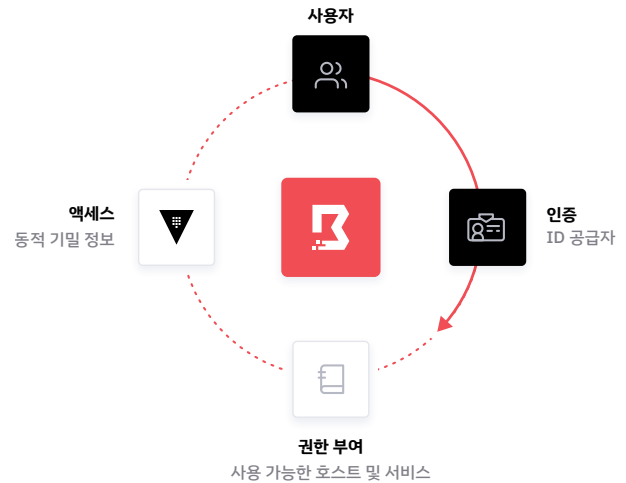
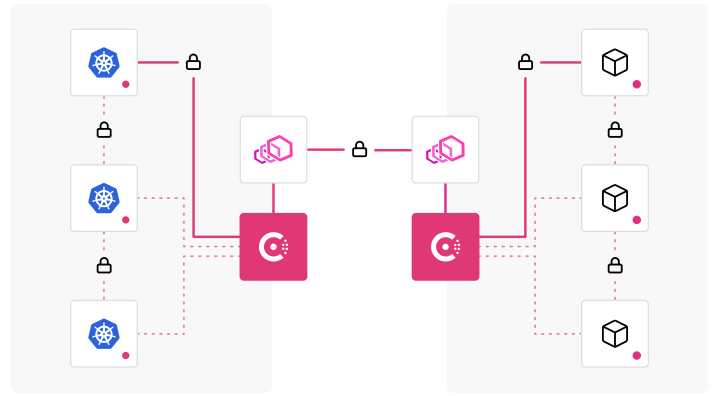
사람 신원 인증

기업은 연동된 기록 시스템을 구축하기 위해 다양한 신원 플랫폼(IdP)을 활용합니다. 여기에는 Active Directory, LDAP, Okta, Ping 등이 포함될 수 있습니다. 이러한 신뢰할 수 있는 신원 제공업체를 활용하면 신원 기반의 액세스 및 보안 원칙을 지원할 수 있습니다. HashiCorp 제품은 업계 선도하는 주요 신원 제공업체들과 긴밀하게 통합되어 있습니다.

사람과 머신 간의 액세스

사용자 액세스를 보호하기 위한 기존의 솔루션에는 VPN이나 베스천 호스트(Bastion Host)와 같은 네트워크 장비가 포함됩니다. 이러한 방식은 사용자에게 네트워크상의 모든 리소스에 대한 액세스 권한을 제공하며, 네트워크 방화벽과 같은 추가 장비를 도입하지 않고서는 최소 권한 원칙을 강제하지 않습니다. 또한 이러한 방식은 자격 증명 관리에도 도움이 되지 않습니다. 이로 인해 사용자나 관리자, 혹은 별도의 툴이 SSH 키, 인증서, 사용자 이름 및 비밀번호와 같은 자격 증명을 직접 관리하고 배포해야만 합니다. 이러한 낙후된 인프라 리소스 접속 방식은 심각한 보안 위험을 초래할 뿐만 아니라, 운영상의 엄청난 수고를 야기합니다.

기업은 흔히 **자격 증명이 무분별하게 확산되는 문제**에 직면하며, 번거로운 절차를 피하기 위해 사용자에게 네트워크 전체에 대한 액세스 권한을 부여하곤 합니다. HashiCorp Boundary는 최종 사용자 액세스를 간소화하고 최소 권한 원칙을 강제하여 보안을 강화하는 현대적인 PAM 방식입니다. Boundary는 네트워크를 외부에 노출하거나 사용자가 직접 자격 증명을 관리할 필요 없이, 스마트한 추상화, 자동화 및 보안 계층을 제공합니다. 특히 Boundary는 Vault와 통합되어 세밀한 단회성 인증 토큰으로 애플리케이션과 핵심 시스템에 대한 액세스를 보호하므로, 수동으로 자격 증명을 생성하고 관리할 필요가 전혀 없습니다.



멀티 클라우드 보안의 비즈니스 영향력

신원 기반의 보안 및 액세스에 대한 HashiCorp의 접근 방식은, 기업이 멀티 클라우드 세계로 전환하는 과정에서 인프라와 애플리케이션, 데이터를 안전하게 마이그레이션하고 보호할 수 있는 견고한 토대를 제공합니다.



클라우드 도입 가속화

클릭 한 번으로 완료되는 배포와 이미 내장된 모범 사례를 통해 클라우드 도입을 가속화하세요.



생산성 향상

현대적인 중앙 집중형 보안 플랫폼을 통해 생산성을 높이고 비용을 절감하세요.



멀티 클라우드 유연성

모든 클라우드 제공업체에 적용되는 단일 워크플로를 통해 멀티 클라우드의 유연성을 지원합니다.

[무료 맞춤형 데모](#)를 예약해 제로 트러스트 환경에서 멀티 클라우드 보안을 강화하는 방법을 자세히 알아보세요.

© Copyright IBM Corporation 2025

미국에서 제작
2025년 8월

IBM, IBM 로고, HashiCorp, Vault, Consul 및 Boundary는 미국 및/또는 기타 국가에서 International Business Machines Corporation의 상표 또는 등록 상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 다른 회사의 상표일 수 있습니다. 현재 IBM 상표 목록은 [ibm.com/kr-ko/trademark](https://www.ibm.com/kr-ko/trademark)에서 확인할 수 있습니다.

이 문서는 최초 발행일을 기준으로 최신 상태로 업데이트된 문서로, 내용은 언제든지 IBM에 의해 변경될 수 있습니다. IBM이 현재 영업 중인 모든 국가에서 모든 제품이 제공되는 것은 아닙니다.

본 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증이나 비침해성에 대한 보증 또는 조건을 포함해 그 어떠한 명시적 또는 묵시적 보증 없이 '있는 그대로' 제공됩니다.

IBM 제품은 제품을 제공 당시의 계약 조건에 따라 보증됩니다.

