

COHESITY

ID

확인 계층이

바로 사이버 공격의 핵심입니다



보안 및 IT 리더들이 ID 인프라가 복구
가능하다는 점을 **증명**해야 하는 이유

서론

엔터프라이즈 ID는 삶을 더 단순하게 만들어 줄 것으로 기대되었습니다. 조직들은 1960년대 후반과 1970년대 초반에 처음으로 디지털 액세스를 중앙 집중화하여, 누가 들어오고 무엇을 다룰 수 있는지 결정할 수 있는 단일 창구를 마련했습니다. 이후 LDAP와 Active Directory 같은 플랫폼은 이러한 개념을 전체 네트워크를 위한 단일 진실 공급원으로 발전시켰습니다. 이는 훌륭하게 작동했습니다.

그것이 바로 문제입니다.

이제 그 단일 진실 공급원은 가장 쉬운 단일 침투 경로가 되었습니다. 공격자들은 더 이상 무단 침입하지 않습니다. 그들은 탈취한 자격 증명과 합법적인 액세스 권한으로 로그인한 뒤, 가장 중요한 시스템으로 곧장 이동합니다. 아무런 문제도 발생하지 않습니다. 경보도 울리지 않습니다. 그들은 직원들이 매일 아침 사용하는 것과 같은 문을 사용하며, 이는 대부분의 보안 프로그램이 해결하도록 설계된 문제와는 근본적으로 다릅니다.

수년 동안 방어 체계는 침입자를 막기 위한 장벽, 즉 경계를 중심으로 구축되었습니다. 장벽은 여전히 존재하지만, 공격자들은 더 이상 그것을 넘지 않습니다. **ID 인프라를 손상시키는 것이 더 쉽고 조용하며 확실하기 때문에, ID가 네트워크 경계를 대신하여 주요 전장으로 자리 잡았습니다.** 대부분의 보안 스택은 이 전장에서 싸우도록 구축되지 않았습니다.

수치가 이를 명확히 보여줍니다. 2024년 공격의 79%는 맬웨어가 없었습니다. 즉, 탐지할 바이러스 없이 소셜 엔지니어링, 탈취된 자격 증명, 신뢰할 수 있는 원격 도구만이 탐지를 피해 갔습니다. 2025년에는 공격자들이 유효한 자격 증명, 신뢰할 수 있는 인증의 흐름, 승인된 SaaS 통합에 더욱 의존하여 도메인 간에 들키지 않고 이동함에 따라 이 수치는 82%로 증가했습니다(CrowdStrike 글로벌 위협 보고서). 추세선은 정확히 한 방향을 가리키고 있습니다.

이곳이 바로 제대로 된 보안 프로그램이라면 이제 시작해야 할 불편한 지점입니다. 모든 것에 대한 액세스를 제어하기 위해 구축한 시스템이 조용히 모든 것에 접근하는 가장 쉬운 방법이 되었습니다. 그렇다고 당황할 필요는 없습니다. 그 무엇보다 먼저 ID를 보호하고, 이를 복구할 수 있음을 증명해야 하는 이유입니다.

엔터프라이즈 ID가 공격받는 이유

단 하나의 자격 증명이 손상되면 그 뒤에 있는 모든 것에 접근할 수 있기 때문에, 공격자에게 ID는 기업 내에서 가장 가치가 높고 노력이 적게 드는 표적입니다. ID는 단순한 또 다른 공격 벡터가 아닙니다. 그것은 현대의 공격자가 적극적으로 노리는 단 하나의 벡터입니다.

하지만 여기에 문제가 있습니다. 스택의 거의 어떤 것도 이를 막도록 설계되지 않았다는 것입니다. EDR, 방화벽, 네트워크 세분화는 모두 무단 침입자를 잡도록 설계되었으며, 유효한 자격 증명으로 로그인한 사람을 의심하도록 설계되지 않았습니다. 방어 체계의 관점에서 공격자는 직원과 완전히 똑같아 보입니다.

그리고 사각지대는 갈수록 커집니다. 대부분의 Active Directory 환경은 수십 년이 되었습니다. 수년간의 임시방편, 잊혀진 계정, 아무도 보지 않는 백그라운드에서 조용히 쌓인 잘못된 구성들이 누적되어 왔습니다. 이러한 누적물은 단순한 기술 부채가 아닙니다. 그것은 열려 있는 창문이며, 그것이 바로 공격자들이 가장 먼저 찾는 것입니다.

하이브리드 ID는 상황을 더욱 악화시킵니다. 현재 대부분의 조직은 온프레미스 Active Directory와 Entra ID, Okta 같은 클라우드 ID 공급자를 혼합하여 운영하고 있으며, 이들 간의 모든 연결은 공격 표면을 넓힙니다. 더욱 최악인 것은 Entra ID나 Okta의 취약점이 종종 Active Directory로 바로 이어진다는 점입니다. Active Directory는 대개 다른 모든 것이 신뢰하는 단일 진실 공급원이기 때문입니다. 기반에 금이 가면 전체 구조가 흔들립니다.

ACTIVE DIRECTORY는 엔터프라이즈 ID의 핵심입니다

Active Directory는 25년 이상 엔터프라이즈 ID를 운영해 왔으며, 전 세계 조직의 90%에서 여전히 사용되고 있습니다. 대부분의 클라우드 ID 공급자는 이와 페더레이션되거나 동기화됩니다. 즉, 새로운 플랫폼을 채택하더라도 Active Directory는 여전히 이 모든 것을 지탱하는 기반이라는 의미입니다.

사실:

- 공격자는 사람이 직접 조작하는 침입의 78% 이상에서 도메인 컨트롤러를 뚫습니다.
- 그중 35%의 경우, 도메인 컨트롤러는 랜섬웨어가 전체 환경으로 확산되는 기점이 됩니다.

공격이 발생할 때, Active Directory는 종종 복구를 가로막는 유일한 장애물이 됩니다. 이것이 의미하는 바를 생각해 보십시오. 자체 백업 솔루션에 로그인할 수 없다면 그 어떤 복구도 시작할 수 없습니다. 공격자들은 이를 완벽하게 이해하고 있으며, 이것이 바로 백업 시스템과 Active Directory를 동시에 공격하는 횡수가 점점 늘어나는 이유입니다. 두 가지를 모두 빼앗기면 더 이상 운수 나쁜 날로 끝나지 않습니다. 인질극 상황에 처하게 됩니다.

그리고 시간은 무자비합니다. 전체 Active Directory 포리스트 복구에는 며칠 또는 몇 주가 걸릴 수 있으며, 가동 중지 시간은 조직에 시간당 최대 730,000 달러의 비용을 초래할 수 있습니다([Forrester, Quest Recovery Manager for Active Directory Disaster Recovery Edition의 Total Economic Impact™](#)).

전통적인 백업 도구는 여기에서 도움이 되지 않습니다. 개별 도메인 컨트롤러와 파일을 복사할 수는 있지만, 전체 Active Directory 포리스트를 재구축하는 데 필요한 정밀하고 순서가 지정된 단계를 체계적으로 조율할 수는 없습니다. 조각들을 백업했다고 해서 그것들을 다시 조립할 수 있다는 의미는 아닙니다.

지원 데이터

32%

2025년 상반기, ID 기반
공격의 급격한 증가.
공격의 97%가 패스워드
스프레이 또는 무차별
대입 공격

(Microsoft 디지털 방어 보고서 2025)

22%

탈취된 자격 증명과 관련이
있는 전체 데이터 침해.
기본 웹 애플리케이션에
대한 공격의 88%가
구체적으로 탈취된 자격
증명과 관련

(Verizon 2025 데이터 침해 조사 보고서)

35%

유효한 계정의 악용으로
인해 발생한 클라우드
사고

(CrowdStrike 2025 글로벌 위협 보고서)

ID는 현재와 미래의 MVC 및 신뢰의 기반입니다

최소 기능 기업(MVC)은 조직이 생존하고 필수 운영을 유지하는 데 필요한 가장 작고 린(lean)한 형태를 말합니다. 조직이 사이버 사고를 당했을 때, 백업이 손상되어 복구에 실패하는 것은 아닙니다. 종종 모든 것을 한 번에 복구하려고 하거나 잘못된 순서로 복구하려고 하기 때문에 실패합니다.

대부분의 조직이 놓치는 계층은 신뢰와 제어를 중심으로 하며, ID는 이 두 가지가 교차하는 지점에 정확히 위치합니다. 이것은 기업의 만능 열쇠입니다. 신뢰할 수 있는 ID를 확립할 수 없다면, 다른 어떤 것도 안전하게 복원할 수 없습니다.

ID 및 액세스 관리(IAM)는 세 가지 핵심 기능을 담당합니다.

- **ID 수명 주기 관리:** 온보딩, 역할 업데이트, 프로비저닝 해제를 자동화하여 직원이 입사하고, 역할을 변경하고, 퇴사할 때 액세스가 정확하게 유지되도록 합니다.
- **인증:** 일반적으로 다중 요소 인증(MFA) 및 싱글 사인온(SSO)을 통해 누군가가 본인이 주장하는 당사자가 맞는지 확인합니다.
- **권한 부여:** 인증된 각 사용자에게 업무에 필요한 특정 액세스 권한을 부여하는 동시에 다른 모든 것은 제한합니다.

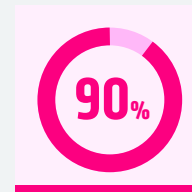
이 세 가지 기능을 결합하면 Active Directory, Entra ID, Okta는 단순한 배관 역할을 넘어 비즈니스의 운영 백본이 됩니다. 이들은 모든 직원,

모든 애플리케이션, 모든 트랜잭션을 인증합니다. 이는 단순하고도 불편한 진실로 이어집니다. ID 인프라가 중단되면 비즈니스도 함께 중단된다는 것입니다.

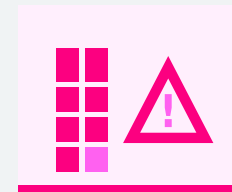
그리고 이 운영 백본은 앞으로 훨씬 더 많이 노출될 것입니다. 조직들이 AI 및 에이전트 워크플로우의 도입을 서두르고 있는 가운데, 이러한 에이전트는 안전하게 작동하기 위해 ID 인프라에 의존하며 그 변화는 이미 데이터에서 나타나고 있습니다. 조직의 93%가 패스워드 재설정 및 VPN 액세스와 같은 민감한 보안 작업에 AI 에이전트를 이미 사용 중이거나 사용할 계획입니다(Semperis, 2026년 5월).

주목해야 할 부분은 다음과 같습니다. 이러한 에이전트는 종종 자신에게 작업을 수행하고 민감한 데이터에 액세스하도록 지시하는 직원의 ID를 빌립니다. 이들 각각은 새로운 열쇠 세트입니다. ID를 확보, 보호, 복구하는 일의 중요성이 그 어느 때보다 커졌습니다.

지원 데이터



전 세계 **기업의 90%** 이상이 **Active Directory**와 **Entra ID**를 사용합니다(Semperis).



사이버 공격 **10건 중 9건에 Active Directory**가 연관되어 있습니다. 구축이 잘못되어서가 아니라 어디에나 존재하기 때문입니다([Cohesity CERT](#)).

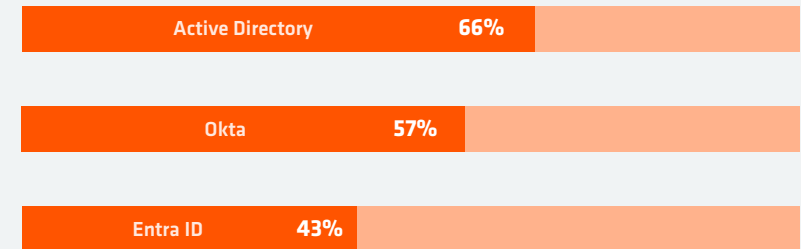
ID, 비즈니스 연속성 및 사이버 레질리언스의 교차점

전통적인 비즈니스 연속성 계획은 ID를 전기처럼 취급합니다. 즉, 스위치를 켜면 인프라가 켜져 있을 것이라고 가정합니다. 조직이 무너지는 지점이 바로 이 가정입니다. 이제 ID는 더 이상 당연한 가정이 아닙니다. ID 자체에 대한 복구 계획이 필요합니다.

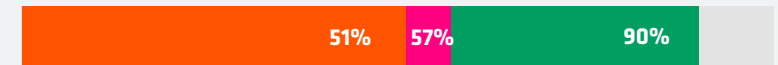
사이버 레질리언스는 그 가정을 완전히 뒤집습니다. 주변의 모든 것이 손상되었을 때에도 ID를 가장 먼저 공격받을 대상이자 가장 먼저 (독립적이고, 테스트되고, 격리되고, 신뢰할 수 있는 상태로) 복원할 수 있어야 하는 요소로 취급합니다. “작동할 것이라 가정한다”와 “작동함을 증명했다” 사이의 격차가 바로 조직이 공격 후 수일 또는 수주를 허비하게 만드는 지점입니다. 파일을 무사히 복원할 수는 있습니다. 하지만 단 한 사람만으로 로그인하여 이를 사용할 수 없습니다.

보안, IT 및 임원진 리더를 위한 시사점은 명확합니다. 사전 예방적 ID 보안 및 ID 복구가 독립적인 분야로 계획, 테스트 및 리소스화될 때에만 비즈니스 연속성 및 사이버 레질리언스가 성공할 수 있습니다. 다른 모든 것을 복원하는 동안 이러한 작업이 자동으로 이루어질 것이라고 절대 가정하지 마십시오.

지원 데이터



재해 복구 계획에 **Active Directory**가 포함된 조직은 66%, **Entra ID**는 43%, **Okta**는 57%에 불과하여, 많은 연속성 계획이 ID 계층 자체에 사각지대를 남겨두고 있습니다 (Semperis, 2025년 11월).



조직의 90%가 ID 취약성을 검사하지만, 교정 절차를 갖춘 조직은 51%에 불과하며 ID 복구를 자동화한 조직은 57%에 불과합니다 (Semperis, 2025년 11월).

조치를 취하지 않을 때의 비용

기다림의 대가에 대해 이야기해 보겠습니다. 기다림 역시 하나의 결정이며, 선택지 중 가장 비싼 결정이기 때문입니다. 단지 재정적인 측면뿐만 아니라 운영 및 평판 측면에서도 마찬가지입니다.

이 비용은 단일 청구서가 아닙니다. 세 가지 비용으로 구성되며, 이는 복합적으로 작용합니다.

- 침해 청구서: 사고 대응, 규제 벌금 및 법적 책임 노출
- 가동 중지 시간 청구서: 생산성 손실, 수익 차단, ID 계층이 노출된 상태에서 발생하는 반복적인 공격
- 신뢰 청구서: 사이버 보험료 상승, 임원 책임 및 거래 위험

그리고 기다린다고 해서 미터기가 멈추는 것은 아닙니다. ID 공격 표면은 기업 내에서 가장 표적이 되는 영역 중 하나이며, 전통적인 방어 수단으로는 따라잡을 수 없는 곳이므로 조치를 취하지 않을 때의 비용은 정체되어 있지 않습니다. 해결하지 않고 방치하는 분기마다 그 비용은 상승합니다. 지연은 조심스러움이 아닙니다. 그것은 원하지도 않은 부채에 붙는 복리 이자입니다.

지원 데이터



조직은 3년에 걸쳐 **120만 달러**의 비용이 드는 성공적인 ID 공격, **109,000달러**의 비용이 드는 하이브리드 ID에 대한 수동 모니터링, 그리고 수동 Active Directory 복구에 따른 생산성 손실 및 가동 중지 시간으로 인해 **390만 달러**의 비용에 직면할 수 있습니다. (Forrester 총 경제적 영향(Total Economic Impact) 연구).



데이터 유출의 전 세계 평균 비용은 **444만 달러**이지만, 자격 증명 기반 침해의 비용은 약 **467만 달러**이며, 식별하고 억제하는 데 약 292일이 걸려 공격 벡터 중 가장 느립니다 (IBM 데이터 침해 비용 2025).



랜섬웨어 경제학이 변화하고 있지만, 고통 없이 이루어지는 것은 아닙니다. 평균 랜섬웨어 지불액은 **11만 5천 달러**로 떨어졌고 피해자의 **64%**가 지불을 거부했습니다. 이는 더 많은 조직이 랜섬웨어 지불 대신 복구에 대한 운영 비용을 감당하고 있음을 의미하며, ID 복구 속도에 더 큰 압박을 가하고 있습니다 (Verizon DBIR 2025).



8개의 주요 사이버 보험사 중 8곳 모두 이제 사이버 정책을 인수할 때 ID 관련 보안 및 레질리언스를 요구하고 검증하며, 강력한 ID 강화를 입증하는 것은 더 낮은 보험료 및 더 넓은 보장 범위와 직결됩니다 (Cohesity, "사이버 보험에서 ID 레질리언스는 필수적입니다").

이것들은 무관한 데이터 포인트가 아닙니다. 이들은 명세서화된 침해 청구서와 가동 중지 시간 청구서이며, 보험사가 보험료를 ID 보안 태세에 직접 연결함에 따라 신뢰 청구서가 그 뒤를 바짝 쫓고 있습니다. ID 문제가 해결되지 않은 상태로 오래 지속될수록, 이들 각각의 비용은 더 비싸집니다. 어떤 상황이든 상관없이 이 비용을 지불하게 될 것입니다. 유일한 질문은 지금 원하는 조건에 따라 조금만 지불할 것인지, 아니면 나중에 공격자의 조건에 따라 전부 지불할 것인지입니다.

결론

이제 ID 기반 침해는 거의 모든 주요 데이터 유출 사고에서 나타나며, 그 패턴은 결코 변하지 않습니다. 공격자들은 무단 침입하지 않습니다. 그들은 유효한 자격 증명과 신뢰할 수 있는 ID 흐름으로 로그인하고 이들을 잡을 수 있도록 구축되지 않은 환경을 들키지 않고 넘나듭니다. 그런 다음 데이터를 훔치고 시스템을 장악하며 랜섬웨어를 배포합니다.

이 중 어느 것도 불가피한 것은 아닙니다.

수 시간 내에 복구하는 조직과 ID 서비스에 대한 신뢰를 재구축하는데 수 주를 소비하는 조직의 차이는 운과도 상관없고 비용을 얼마나 지출했는지와도 상관없습니다. 이것은 단 하나의 결정으로 귀결됩니다. 전체 공격 수명 주기에 걸쳐 ID 레질리언스를 그 자체의 규율로 필요하기 전에 구축했는지 여부입니다.

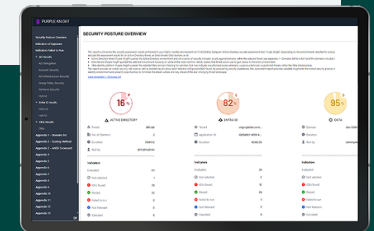
따라서 ID 레질리언스를 현재의 위상에 맞게 취급하십시오. 선택 사항이 아니라 기업 보안의 핵심 요구 사항입니다. ID는 최전선의 문이자 기반이며 복구 병목 현상이기도 합니다. 포인트 도구의 미봉책은 항상 부족할 것입니다. 결정적인 순간에 ID가 존재할 것이라고 단순히 가정하는 연속성 계획도 마찬가지일 것입니다. 실제 공격 상황에서 살아남는 유일한 전략은 필요하기 전에 미리 테스트하고 입증한 전략뿐입니다.

좋은 소식은 여러분이 이 상황을 앞서나갈 수 있다는 것입니다. 가장 중요한 ID 시스템의 사이버 레질리언스를 가속화할 수 있습니다.

그리고 저희가 도와드릴 수 있습니다.

Cohesity가 ID 레질리언스를 구축하고 강화하는데 어떻게 도움이 되는지 **자세히 알아보세요**

Active Directory, Entra ID 및 Okta 전반의 취약성과 격차를 식별하기 위해 **무료 ID 보안 평가를 받아보십시오**



COHESITY

© 2026 Cohesity, Inc. All rights reserved. Cohesity, Cohesity 로고, SnapTree, SpanFS, DataPlatform, DataProtect, Helios 및 기타 Cohesity 마크는 미국 및/또는 해외에 있는 Cohesity Inc.의 상표 또는 등록 상표입니다. 기타 회사 및 제품명은 관련된 회사 및 상품과 관련된 각 회사의 상표일 수 있습니다. 이 자료는 (a) Cohesity 및 당사의 사업과 제품에 관한 정보를 제공하기 위한 것이고, (b) 작성 당시 진실하고 정확한 것으로 판단하였으나 통보 없이 변경될 수 있으며, (c) '있는 그대로' 제공한 것입니다. Cohesity는 모든 종류의 명시적 또는 묵시적 조건, 진술, 보증을 부인합니다.

6100036-001 KO 8-2026