COHESITY

ID 레질리언스 솔루션 평가를 위한 경영진 가이드

다음은 접근을 통제하고, 중요한 데이터를 보호하며, 파괴적인 사이버 공격으로부터 신속하게 복구하기 위해 알아야 할 모든 것입니다.

ID 및 접근 관리 시스템은 악의적인 공격자의 주요 표적입니다.

이유가 무엇일까요?

사이버 공격의 10건 중 9건은 ID 및 접근 관리(IAM) 시스템과 관련되어 있습니다. 이는 모든 조직 인프라에서 가장 많이 공격받는 부분입니다.

ID 시스템은 침해 시 공격자에게 조직 내 사실상 모든 리소스에 접근할 수 있는 권한을 주기 때문에 매우 중요한 공격 표적입니다. 이러한 이유 때문에 ID 레질리언스가 포괄적인 사이버 레질리언스 전략의 핵심입니다. 최소한의 구성으로 운영 가능한 기업을 신속하게 복원하기 위해서는, 많은 중요 시스템과 비즈니스 프로세스가 ID 서비스에 의존하기 때문에 이를 제일 먼저 신뢰할 수 있는 상태로 복구해야 합니다.

대부분의 조직에서 기본 IAM이자 다른 ID 공급자를 위한 신뢰할 수 있는 정보 소스는 온프레미스 Microsoft Active Directory(AD)입니다. 특히 여러 포리스트를 포함하고 있는 복잡한 환경에서 AD의 사이버 복구는 전문 지식이 요구되는 까다로운 프로세스이며, "또 다른 평범한 작업"이 아닙니다. AD 외에도, Entra ID와 Okta를 혼합하여 사용하고 있을 가능성이 높습니다.

사이버 공격에 대한 방어를 강화하고자 할 경우, 모든 핵심 ID 서비스에 전반에 걸쳐 종합적인 ID 레질리언스 전략을 확보해야 합니다.

ID 레질리언스는 비즈니스가 다음과 같이 할 수 있도록 지원합니다.

- **ID 위협 탐지 및 해결:** 진행 중인 ID 기반 공격을 탐지하고, ID 위협 탐지 및 대응(ITDR)을 이용해 사람의 개입을 기다릴 수 없는 위험한 변경 사항을 자동으로 원상 복구합니다.
- **ID 서비스를 안전하게 복구하고 신뢰 회복:** 지속적인 재감염으로 이어지는 공격자나 백도어를 다시 되살리지 않고 ID 서비스를 복구합니다.
- **중단 시간 줄이기:** ID는 접근 및 인증의 열쇠입니다. ID가 손상되면 비즈니스가 중단됩니다. ID 공격으로부터 비즈니스 운영을 안전하고 원활하게 복구하여 중단 시간을 최소화합니다.

어떤 조직도 사이버 공격으로부터 100% 안전할 수는 없습니다. 따라서 침해 사고로부터 복구할 수 있는 능력, 즉 레질리언스에 투자해야 합니다. 귀사는 ID 기반 공격을 지속적으로 탐지하고 복구하며, 어떠한 상황에서도 AD, Entra ID, Okta를 안전하고 빠르게 복구할 수 있는 검증된 복구 전략을 구현함으로써 ID 레질리언스를 개선하고 확장해야 합니다. 본 가이드는 솔루션을 평가하고, 적절한 질문을 던지고, 현재의 위협으로부터 ID 인프라를 보호하기 위한 확신 있는 투자를 실행하는 데 도움을 드립니다.

“어떤 조직도 사이버 공격으로부터 100% 안전할 수는 없습니다. 따라서 침해 사고로부터 복구할 수 있는 능력, 즉 레질리언스에 투자해야 합니다.”

ID 레질리언스 솔루션에서 고려할 사항

옵션을 평가할 때, ID를 단순히 필요할 때 백업하고 복구하는 또 다른 작업으로 생각하기 쉽습니다. 이것은 매우 위험한 낡은 사고방식입니다. ID 및 액세스 시스템까지 사이버 레질리언스를 확장하는 최신 접근 방식은 공격 라이프사이클의 모든 단계에서 선제적인 지능형 보안과 안전한 복구를 함께 제공합니다. 진정한 엔터프라이즈급 ID 레질리언스 솔루션과 다른 솔루션을 구분하는 요소는 다음과 같습니다.

고급 ITDR: ID 레질리언스는 침해 이전부터 시작됩니다. AD와 같은 IAM 시스템은 시스템에 대한 열쇠를 제공하기 때문에 공격자가 가장 먼저 표적으로 삼는 시스템입니다. 단순히 백업만으로는 충분하지 않습니다. 솔루션은 ITDR(Identity Threat Detection and Response) 기능을 통해 ID 환경의 보안 태세를 지속적으로 모니터링할 수 있어야 합니다. 이를 통해 취약점을 탐지하고 ID 인프라를 보강하며 개선 조치를 자동화할 수 있습니다. 사람의 개입을 기다릴 수 없는 악의적인 변경 사항에 대한 자동 롤백 및 복구는 공격 성공 기회를 줄일 수 있습니다. 이러한 지속적인 위협 탐지 및 복구와 사전 보강을 통해 공격자가 ID 시스템을 악용하기 전에 차단할 수 있습니다.

공격에 견딜 수 있는 보호 능력: 침해가 발생할 경우, 안전한 백업 데이터를 통해 ID 인프라를 복구할 수 있도록 보장하는 것이 중요합니다. 공격자들은 백업이 최후의 방어선이라는 것을 알고 있기 때문에, 적극적으로 이중 협박을 사용하거나 백업을 암호화, 수정 또는 삭제하려고 시도하며, 사용자는 무방비 상태에서 엄청난 몸값을 지불해야 합니다. 따라서 ID 레질리언스 솔루션은 설계 단계부터 불변성을 보장해야 합니다. 공격자가 도메인 관리자 자격증명을 획득하더라도 AD 백업을 변조할 수 없도록 해야 합니다. 웜 저장소, 쿼럼 기반 승인 및 암호화 검증은 레질리언스 있는 백업을 위한 핵심적인 기능입니다. 네트워크 내부에 이미 공격자가 침입했을 때 보호 계층이 제대로 작동하지 못한다면 진정한 보호가 아닙니다.

빠르고 악성코드 없는 복구력: ID가 침해되면 모든 비즈니스 기능이 중단됩니다. 복구 속도뿐 아니라 복구의 무결성도 중요합니다. 신뢰할 수 있는 위험 검증 없이 단순히 ID를 복원하는 것은 악성 코드나 백도어를 다시 되살려 반복 감염과 악순환으로 이어질 수 있습니다. 효과적인 솔루션은 AD, Entra ID 및 Okta를 자동적으로 체계적이며 신속하게 복구할 수 있는 기능을 결합해야 합니다. 특히 AD의 경우, 손상된 자격증명과 악성 코드가 다시 복구되지 않도록 복구를 OS와 분리해야 합니다. 이를 통해 신뢰할 수 있는 복구로 지속적인 감염을 예방하여 복구 프로세스 중 가동 중단 시간을 줄일 수 있습니다.

세분화된 복구 옵션: 모든 ID 사고가 전체 복원을 필요로 하는 것은 아닙니다. 세분화된 복구는 객체 수준, 속성 수준 및 포리스트 수준 복구를 위한 옵션을 제공하여 시간을 절약하고 중단을 최소화합니다. 포리스트 및 세분화된 복구 도구를 모두 갖추고 있으면 단순한 헬프데스크 지원 요청과 대규모 사이버 공격 모두에 적절한 솔루션을 제공할 수 있습니다.

하이브리드 ID 전반의 보호: ID는 더 이상 온프레미스 AD에만 국한되지 않습니다. Entra ID와 Okta는 특히 클라우드 앱 액세스를 위한 엔터프라이즈 ID 아키텍처의 핵심적인 부분으로 빠르게 자리 잡고 있습니다. AD, Entra ID 및 Okta를 모두 보호하면서 하이브리드 ID 환경 전반에서 원활하게 작동하는 미래 지향적인 레질리언스 솔루션이 필요합니다. 많은 조직에서 Entra ID와 Okta는 AD와 동기화되어 있어서, Entra ID와 Okta를 성공적이고 안전하게 복원하려면 먼저 AD를 보호하고 복구할 수 있는 기능이 필요합니다. Entra ID와 Okta는 AD와는 별개의 애플리케이션이며, 온프레미스에서 클라우드로 단방향으로 동기화됩니다. 온프레미스 보호가 없으면 솔루션의 절반만 보유한 것이 됩니다. ID 레질리언스 솔루션은 클라우드 ID 연속성을 보장하기 위해 Entra ID와 Okta를 안전하게 복구할 수 있도록 보호 및 복구 기능을 포함하고 있어야 합니다.

침해 후 포렌식으로 신뢰성을 검증하고 향후 공격 방지: 인사이트 없는 복구는 반복적인 사고에 취약하게 됩니다. 최신 솔루션에는 팀이 복구가 안전한지 검증할 수 있는 포렌식 기능이 내장되어 있어야 합니다. 이는 사고 후 조사에 도움이 될 뿐만 아니라 예방 조치에 중요한 정보를 제공하므로, 엔터프라이즈가 방어력을 강화하고 규정 준수 또는 규제 보고 요건을 충족하는 데 도움을 드립니다. 복구 후 철저한 실사를 하지 않으면 후속 공격을 당할 위험이 있습니다. 포렌식이 사후 고려 사항이 되어서는 안 됩니다. 이는 ID 레질리언스의 필수적인 부분입니다.

인터넷 접속 없이 복구 가능: 대규모 정전이나 사이버 공격 발생 시 안정적이거나 안전한 인터넷 접속이 보장된다고 가정할 수 없습니다. ID 레질리언스 솔루션은 어떤 상황에서도 시스템을 안전하게 복원하고 온라인 상태로 되돌릴 수 있도록 인터넷 연결 없이도 중요한 ID 시스템을 성공적으로 복구할 수 있습니다.

연중무휴 24시간 사고 대응 지원: ID는 특히 복구 측면에서 독특하고 복잡한 작업입니다. 핵심 ID 인프라의 사이버 복구를 위해서는 솔루션 공급업체가 ID 보호, 보안 및 복구에 대한 검증된 전문성을 갖추고 고객에게 필요한 지침을 제공할 수 있는지 확인하는 것이 중요합니다. 모든 복구 상황은 다를 수 있으며, 숙련된 전문가의 적절한 대응 지원과 포렌식은 조직이 가장 치명적인 ID 공격이나 장애로부터 신속하고 확실하게 복구할 수 있도록 보장하기 위해 핵심적인 부분이 됩니다.

공급업체에 물어볼 중요 질문

1. 공격자에 의한 AD, Entra ID 또는 Okta 백업의 변조나 삭제를 어떻게 방지합니까?
2. 하루 안에 전체 ID 인프라를 완벽하게 복구할 수 있다는 사실을 시연할 수 있습니까?
3. 복구된 AD, Entra ID 또는 Okta에 악성 코드, 백도어가 없거나 손상된 자격증명이 복구되지 않았음을 어떻게 확인합니까?
4. 인터넷 접속 없이도 동일한 환경과 UI로 ID를 복구할 수 있습니까?
5. 하이브리드 ID 환경(온프레미스 AD + Entra ID + Okta)을 지원합니까?
6. 귀사의 솔루션은 자동화된 방식으로 AD에 대한 전체 포리스트 복구를 실행하고 Microsoft Recovery Runbook을 준수할 수 있습니까?
7. 귀사의 솔루션은 ID에 특정된 위협을 추적해 침해가 발생하기 전에 악성 공격자를 탐지하고 제거합니까?

주의해야 할 경고 신호

- ! 복구 중에 OS와 분리할 수 없습니다. OS와 사용자 ID 데이터를 함께 복구하면 악성 코드 및 백도어가 다시 복구될 수 있습니다.
- ! 물리적 소스/가상 소스를 복구 대상으로 삼을 수 없습니다. 정확한 패치 레벨이 요구되면 가동 중단 시간이 길어질 수 있습니다.
- ! 24/7 사고 대응 지원을 위한 ID 포렌식 및 사고 대응(IFIR) 전문가가 없습니다.
- ! ID 보안 기능이 없습니다. 레질리언스란 영향 발생 전 위험 감소 및 침해 방지를 위한 위협 완화를 포함합니다.
- ! Microsoft 기본 도구에만 의존하는 솔루션. 이러한 방법은 수동이고 느리며, 가장 필요할 때 신뢰성이 떨어집니다.
- ! 백업은 운영 환경에 저장됩니다. 공격자는 백업을 삭제하여 복구할 데이터를 하나도 남기지 않을 수 있습니다.
- ! 여러 도메인 컨트롤러(DC)의 병렬 복구를 위한 조정이나 자동화 기능이 없습니다. 이 기능이 없으면 관리자는 스트레스가 높고 혼란스러운 환경에서 길고 복잡한 수작업을 진행해야 합니다.
- ! 이 솔루션은 안전하고 안정적인 인터넷 연결에 의존합니다. 인터넷 연결이 사이버 공격이나 복구 중에 항상 유지될 것이라고 가정하거나 이에 의존할 수 없습니다.
- ! 복구 테스트 기능이 없습니다. 연습해 볼 수 없으면 신뢰할 수 없습니다.

공급업체 평가 체크리스트

공급업체와 협의 시 이 점수표를 사용하십시오.

요구 사항	공급업체 1	공급업체 2	공급업체 3	참고
여러 DC를 병렬로 복구(AD용)				
모든 물리적/가상 소스 복구 대상 지정				
변조 불가능하고 격리된 AD 백업				
객체부터 포리스트 수준까지 복구 세분화				
자동화된 포리스트 복구 워크플로우				
공격 경로를 식별하고 차단하기 위한 사전 예방적 강화				
백업에서 악성 코드/손상 탐지				
변조 방지 다중 소스 변경 추적 및 롤백				
주요 표적이 되는 서비스 계정의 인벤토리 및 모니터링				
하이브리드 AD(온프레미스 + Entra ID) 지원				
인터넷 접속 없이 복구할 수 있는 능력				
침해 사고 후 포렌식				
확장성(다중 포리스트/글로벌)				
24/7 전문가 ID 사고 대응 지원				

결론

ID 기반 침해는 거의 모든 주요 침해의 핵심적인 부분입니다. 그렇기 때문에 핵심 ID 시스템에 관한 사이버 레질리언스를 강화하는 것은 더 이상 선택이 아니라 기업 보안의 기본입니다.

검증된 ID 레질리언스 솔루션은 단순한 백업 그 이상입니다. ID 침해에 대한 방어를 보강하고, ID 공격 및 위협으로부터 보호하며, 신속하고 신뢰할 수 있는 복구를 제공하고, 악성코드 없는 안전한 복원을 위해 백도어를 차단하는 데 도움이 됩니다. ID 레질리언스에 대해 자세히 알아보고 가장 중요한 ID 서비스를 보호하는 데 어떻게 도움이 될 수 있는지 알아보려면 지금 바로 Cohesity 담당자에게 연락하십시오.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500064-004-KO 7-2026