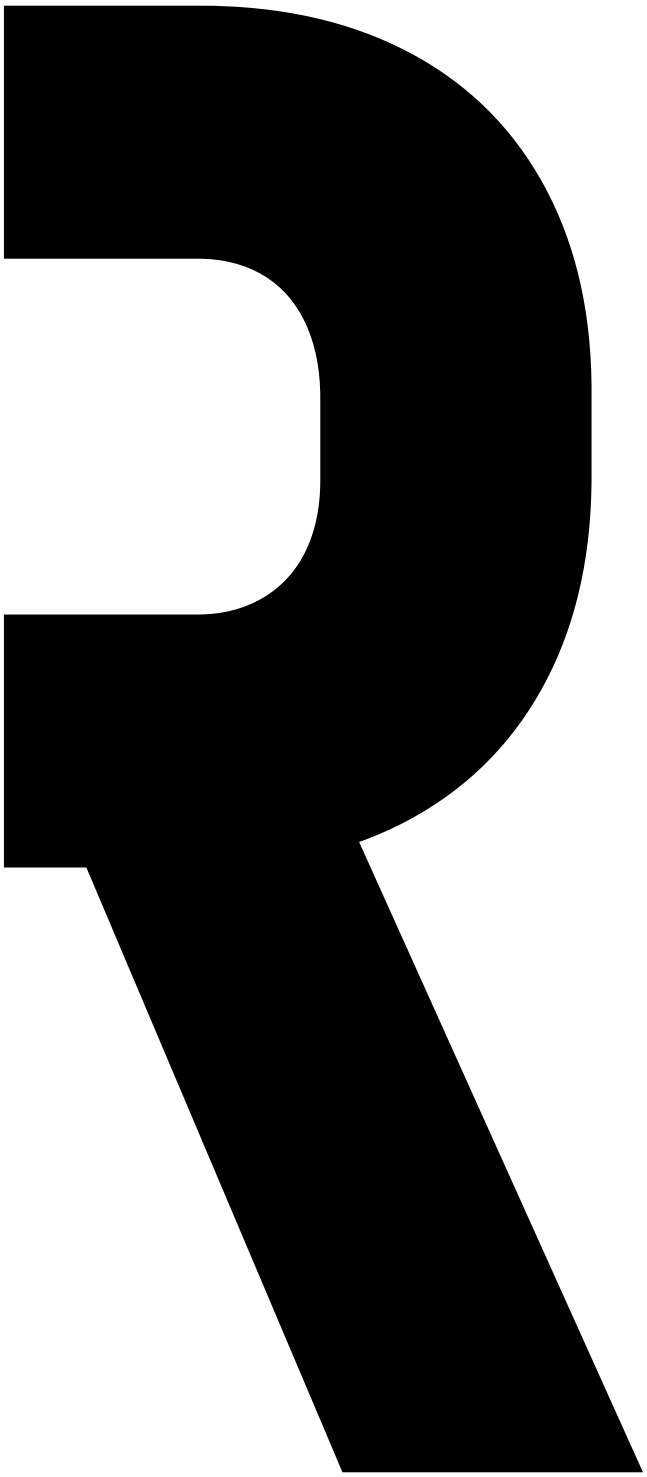
에어코드

AirRBI

웹격리 시스템 AirRBI

제로트러스트를 기반으로 위협으로부터 모두 차단합니다.



목차

N2SF와 RBI 3

1. 웹 환경의 발전과 제로 트러스트 3

2. N2SF와 RBI 3

AirRBI: 대한민국을 대표하는 RBI 3

1. 15년간 축적된 노하우를 바탕으로 한 독자 기술로 개발 3

2. 경제적으로 구축/운영 가능한 설계 4

3. 확장된 보안 4

4. 최고의 사용성: 사용자 불만 최소화 5

5. 관리 편의성 5

AirRBI 활용안 6

1. 안전한 웹 사용을 위한 논리적/물리적 망분리를 제공 6

2. 제로데이 위협을 포함한 웹을 통한 위협 원천 차단 6

3. 원격 사용자를 위한 보안/내부 웹 시스템 보호 7

4. 첨부 파일에 의한 위협 원천 차단 7

5. 웹/생성형 AI 사용 중 발생 가능한 정보 유출 방지 8

6. 보안망에 위치한 시스템 개발 및 유지보수를 위한 환경 제공 8

N2SF와 RBI

N2SF(National Network Security Framework, 국가 망 보안체계)는 기존 망 분리 중심의 보안 정책 한계를 극복하기 위해 국정원이 제시한 제로 트러스트 기반 국가 보안 프레임워크이다.

---

1. 웹 환경의 발전과 제로 트러스트

웹은 단순 정보 제공 수단에서 클라우드, 모바일, 원격 협업, AI 서비스까지 포함하는 핵심 업무 플랫폼으로 발전하였다.

내부망과 외부망을 분리하는 경계형 보안 모델을 중심으로 운영되던 보안 개념은 클라우드, 민관 협업, 원격근무 확산으로 내부와 외부의 경계가 급격히 약화되며 구조적 한계가 드러났다.

제로 트러스트는 네트워크 위치에 관계없이 모든 접근을 항상 검증하는 보안 개념으로, 사용자, 단말, 접속 환경, 행위 등을 종합적으로 판단해 접근을 허용하는 새로운 보안 개념으로 전통적인 경계망 중심의 보안의 한계를 극복하고자 등장하였다.

2. N2SF와 RBI

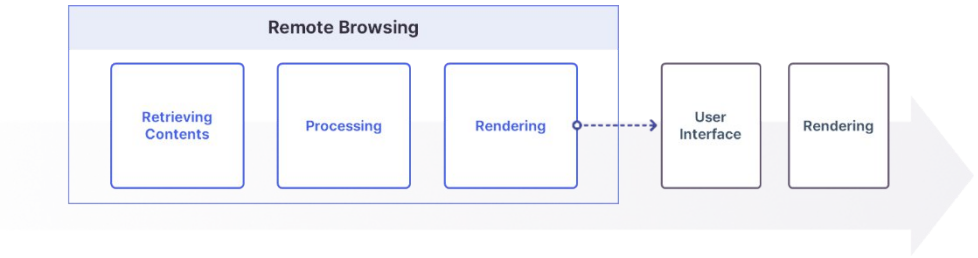
정보 통신 환경 변화로 인해 공공 영역도 제로 트러스트 개념을 받아들여, 보안성과 업무 효율성을 동시에 만족시키고자 N²SF라는 새로운 보안 체계를 도입하였다.

인증 및 수상

- GS 1등급 인증 한국정보통신기술협회 2022
- 신SW장관상 수상 과학기술정보통신부 2024
- 신속확인서 취득 한국인터넷진흥원 2025
- 조달청 디지털 서비스몰 등록

N²SF에서는 인터넷 사용을 위해 단말 인증과 보안 통제가 반드시 필요하며, 이를 실현하는 대표적 기술로 RBI(Remote Browser Isolation)를 권고한다. 따라서 RBI는 선택이 아닌, 웹 이용을 위한 필수 구성 요소다.

RBI는 웹 브라우저를 사용자 단말이 아닌 외부 격리 서버에서 실행하고, 사용자에게는 렌더링된 화면 정보만 전달한다. 이 방식으로 웹 사이트 내 위협 요소는 RBI 서버 내부에서만 실행되며, 사용자 PC의 운영체제·메모리·파일 시스템 접근은 원천 차단된다. 이를 통해 단말과 사용자를 안전하게 보호된다.



국가망보안체계 보안가이드라인
정보서비스모델해설서
모델4. 업무단말의 인터넷 활용
(P19~20)

대한민국을 대표하는 RBI

은 기업들이 RBI를 시장에 소개하고 있지만, 보안과 업무 효율 두 가지 요구를 만족시킬 수 있는 대안은 에어코드의 AirRBI이다.

1. 15년간 축적된 노하우를 바탕으로 한 독자 기술로 개발

AirRBI는 **15년 이상의 웹 격리 코어 기술 경험을 기반으로 개발된 자체 기술 솔루션**으로, 고객 환경에 최적화된 다양한 커스터마이징이 가능하며, 시장의 요구를 지속적으로 반영하는 주기적인 업그레이드와 신속한 기술 지원을 통해 장기적으로 안정적인 보안 운영 환경을 제공한다.

AirRBI는 Aircode가 독자 기술로 개발한 원격 브라우저 격리 솔루션으로, 외산 엔진이나 단순 오픈소스 조합이 아닌 자체 설계·구현을 통해 보안성, 성능, 확장성에서 높은 신뢰성을 확보했다.

자체 기술을 확보하고 있다는 것은 고객의 다양한 환경과 요구에 빠르게 대응할 수 있는 기반을 확보하고 있다는 의미로, 고객의 인프라 환경과 운영 정책에 따라 **On-Premise, Private SaaS, Public SaaS 등 다양한 설치 방식**을 유연하게 지원하여, 공공기관, 금융권, 기업 내부망 등 서로 다른 보안 환경에서도 최적의 형태로 구축·운영이 가능하다.

또한 다양한 인증 및 정책 설정, 로그 수집 기술 표준과 연동을 제공하여 고객 환경에 맞춘 폭넓은 커스터마이징(Customizing)을 지원한다. 이를 통해 기존 보안 인프라 및 인증 체계와 자연스럽게 연계되며, 조직별 보안 정책을 세밀하게 반영한 맞춤형 운영이 가능하다.

아울러 시장 요구와 보안 위협 환경의 변화에 신속하게 대응하기 위해 주기적인 업그레이드(Upgrade)를 통해 성능 개선, 보안 강화, 기능 확장을 지속적으로 수행하고 있으며. 장애나 정책 변경, 환경 변화에 대해서도 **빠른 유지보수 체계**를 통해 안정적인 서비스 운영이 가능하도록 기술적 대응력을 갖추고 있다.

2. 경제적으로 구축/운영 가능한 설계

다중 사용자가 컴퓨팅 자원을 공유하는 RBI 시스템에서는 최소한의 자원으로 다수의 사용자 요청을 처리하고, 단말로 전달되는 트래픽을 줄이는 것이 기업과 기관의 투자·운영 비용 관리에 있어 핵심 과제이다. AirRBI는 다양한 기술을 통해 동영상 중심의 RBI 대비 최대 70% 이상 자원 사용량과 트래픽 발생을 절감한다.

먼저, 단말 및 브라우저의 활성 상태에 따라 원격 브라우저의 동작을 동적으로 제어함으로써 불필요한 서버 자원 사용을 최소화한다. 사용자가 비활성 상태이거나 브라우저가 백그라운드에 있을 경우, 원격 브라우저의 CPU와 메모리 사용을 제한하거나 일시 정지하여 자원 낭비를 억제하고, 동일한 인프라에서도 더 많은 사용자 세션을 안정적으로 수용할 수 있도록 한다.

브라우저 이벤트 관리와 변경 영역 추출 알고리즘을 기반으로, 화면 전체를 상시 전송하지 않고 실제 변화가 발생한 영역만 선택적으로 전송함으로써 네트워크 트래픽을 근본적으로 절감한다. 축적된 변경 영역 추출 노하우를 적용해 최소한의 화면 정보만 전송하면서도 사용자 체감 반응성은 최적의 수준으로 유지한다.

아울러 웹 콘텐츠 특성에 따라 최적의 방식을 적용하는 하이브리드 스트리밍을 통해 하드웨어 리소스와 네트워크 사용량을 동시에 최소화한다. 정적인 화면에는 저부하 스트리밍을, 실시간 반응이 중요한 화면에는 비디오 스트리밍을 적용하여 불필요한 연산과 트래픽을 줄이고, 시스템 성능과 경제성을 함께 향상시킨다.

3. 확장된 보안

HTML과 스크립트 중심으로 구성된 웹 페이지는 RBI 자체만으로 충분한 보안 기능을 수행하지만 웹 페이지에 첨부된 다양한 파일에 대한 보안은 별도의 수단이 필요하다. 이를 위해 AirRBI는 최고 수준의 CDR(Contents Disarm and Reconstruction)을 내장하고 있으며, 바이러스 검출 시스템과 연동을 제공한다.

AirRBI CDR 기술은 비실행형 파일을 포함한 다양한 문서에 대해 먼저 **콘텐츠 타입을 식별하고** 문서 내에 존재할 수 있는 숨겨진 코드, 외부 참조 링크, 삽입 객체 등 **잠재적인 위협 요소의 포함 여부를 정밀하게 분석**하여, **문서 내 유해 요소를 선택적으로 제거**한다. 이를 통해 문서 실행을 통한 악성코드 감염, 내부 시스템 침투, 정보 유출 등의 보안 위협을 원천적으로 차단한다.

마지막 단계에서는 **무해화가 완료된 안전한 정보만을 기반으로 원본 문서와 동일한 레이아웃과 형태를 유지한 상태로 문서를 재구성**한다. 문서 서식, 표, 이미지, 본문 구성 등 시각적·논리적 구조는 그대로 유지하면서, 실행 가능한 위험 요소만 제거된 상태로 재조합되기 때문에 사용자는 원본과 동일한 콘텐츠를 안전하게 열람할 수 있다.

본 기술은 한글(HWP), Word, PowerPoint, Excel, PDF는 물론 BMP, PNG, JPEG 등 이미지 파일을 포함한 **비실행형 파일 약 30여 종 이상의 다양한 포맷을 폭넓게 지원**하여, 최종 사용자에게는 **원본과 동일한 품질의 안전한 문서가 제공되며**, 동시에 조직 전체의 보안 수준을 근본적으로 향상시키는 효과를 제공한다.

4. 최고의 사용성: 사용자 불만 최소화

AirRBI는 글로벌 표준인 Chromium 엔진을 기반으로 구현되어, 일반 사용자가 일상적으로 사용하는 웹 브라우저와 기능, 화면 구성, 동작 방식, 호환성 측면에서 사실상 동일한 사용 경험을 제공한다. 사용자는 별도의 조작 방식이나 추가 학습 없이도 기존에 사용하던 일반 웹 브라우저와 전혀 차이 없는 자연스러운 사용성을 그대로 유지할 수 있다.

또한 그 처리 속도에 있어서도, **단말에서 직접 브라우저를 사용하는 것과 거의 차이가 없는 평균 100ms 이하의 지연 시간**을 구현하여, 사용자가 체감하는 반응 속도는 일반 브라우저 사용과 큰 차이가 없다. 화면이 갱신되는 영역만을 정밀하게 추적하여 전송하는 최적화 기술을 적용함으로써, 불필요하게 큰 이미지나 전체 화면을 반복 전송하는 방식에서 발생하는 지연 요소를 근본적으로 제거하였다. 또한 하나의 웹 페이지 내에서도 콘텐츠의 특성에 따라 가장 적합한 전송 방식을 선택적으로 적용하는 **하이브리드 스트리밍 구조**를 채택하여, 반응성이 중요한 영역은 즉각적으로 처리하고, 변화가 적은 영역은 저부하 방식으로 전송함으로써 전체적인 응답 지연을 최소화한다.

결과적으로 본 기술은 원격 환경이라는 물리적 제약에도 불구하고, 일반 로컬 브라우저 수준에 근접한 즉각적인 반응성을 제공함으로써, 사용자가 지연을 거의 인식하지 못하는 고속 웹 사용 환경을 구현한다.

---

5. 관리 편의성

RBI 사용에 필요한 정책 설정을 정책 템플릿을 기반으로 한다. **정책 템플릿 기반의 유연한 제어 구조**를 통해, 조직이 요구하는 다양한 보안 정책을 안정적이고 일관되게 적용할 수 있는 최적의 통합 관리 환경을 제공한다.

정책은 **템플릿 정책 → 사이트 정책 → 사용자 정책**의 계층 구조로 관리되며, 상위 정책의 기본 규칙을 유지하면서도 하위 단위에서 필요한 예외 설정이나 세부 조정이 가능하도록 설계되어 있다. 이를 통해 조직 전체의 보안 기준은 유지하면서도, 부서별·업무별·사용자별 특성에 맞는 맞춤형 보안 정책을 유연하게 적용할 수 있다.

또한 통합 관리자 화면을 통해 전체 사용자 현황, 접속 현황, 정책 적용 상태, 보안 이벤트 등을 한눈에 파악할 수 있으며, 정책 변경 사항 역시 실시간으로 반영되어 운영 관리의 신속성과 안정성을 동시에 확보할 수 있다. 이러한 구조는 단순한 설정 관리가 아닌, **조직의 다양한 보안 요구사항을 체계적으로 관리·통제할 수 있는 정책 중심 보안 운영 체계**를 구현하는 기반이 된다.

또한 사용자 관리 및 인증에 있어서, MS Active Directory를 비롯한 다양한 **IAM(Identity and Access Management) 시스템과의 연동**을 통해 사용자 및 권한을 통합적으로 관리할 수 있는 체계적인 인증·권한 관리 환경을 제공한다. O-Auth 2.0, SAML, Kerberos, OIDC 등 주요 표준 인증 프로토콜을 폭넓게 지원하며, Microsoft AD, Okta와 같은 외부 인증 시스템과도 유연하게 연동되어 조직의 기존 인증 인프라를 그대로 활용할 수 있다.

사용자별 권한 및 역할(Role) 기반의 접근 제어를 지원하여, 일반 사용자와 관리자 권한을 명확히 분리하고 업무 역할에 따른 세분화된 접근 통제가 가능하다. 이를 통해 관리자 권한 오남용을 방지하고, 조직 내 보안 정책을 일관되게 적용할 수 있는 역할 기반 권한 관리 체계(RBAC)를 안정적으로 운영할 수 있다.

사용자 및 관리자 로그인 시에는 TOTP(Time Based One Time Password) 기반의 멀티 팩터 인증(MFA)을 적용하여 계정 탈취 및 비인가 접근에 대한 보안성을 한층 강화한다. Google Authenticator, Microsoft Authenticator 등 상용 인증 앱과 연동되는 2단계 인증 방식은 비밀번호 기반 인증의 한계를 보완하고, 내부 계정 및 관리자 계정에 대한 공격 시도를 효과적으로 차단한다.

AirRBI 활용안

AiRBI는 기본적으로 안전한 웹 브라우징을 위한 수단이지만, 다양한 요구에 대응할 수 있는 보안 수단이다.

1. 안전한 웹 사용을 위한 논리적/물리적 망분리를 제공

AirRBI는 기존 물리적 망분리 환경의 구조를 유지한 상태에서 웹 활용을 가능하게 하는 가장 현실적인 대안 기술이다. 업무망에 위치한 단말은 외부 인터넷과 TCP/IP 수준에서 직접 연결되지 않는다. 따라서 기존 망분리의 보안 원칙은 그대로 유지되며, 응용 계층에서만 통제된 웹 접근이 허용되는 구조가 완성된다.

이를 통해 기존 망분리 환경에서도 다음과 같은 웹 활용이 가능해진다.

- 외부 포털·정보 검색
- 정부 24, 금융·행정 대민 웹 서비스
- 클라우드 기반 협업 시스템
- 외부 SaaS 기반 업무 도구

2. 제로데이 위협을 포함한 웹을 통한 위협 원천 차단

제로데이(Zero-day) 위협은 보안 패치와 탐지 시그니처가 존재하지 않아 기존 백신, EDR, IPS, WAF 등 탐지 기반 보안 솔루션으로는 사전 차단이 구조적으로 어려운 한계를 가진다. 이러한 환경에서 AirRBI는 위협을 “탐지”하는 방식이 아닌, 실행 환경 자체를 격리하는 방식으로 제로데이 공격을 근본적으로 무력화한다.

제로데이 공격이 웹 콘텐츠에 포함되어 있어도 해당 코드는 RBI 서버 내부에서만 실행되며, 사용자 단말의 OS, 메모리, 파일 시스템에는 접근할 수 없다. 또한 RBI 세션은 사용 종료와 동시에 폐기되므로, 공격 코드가 내부에 잔존하거나 확산될 가능성도 구조적으로 제거된다.

즉, AirRBI는 탐지 실패를 전제로 하더라도 안전한 구조를 제공함으로써, 제로데이 및 신종 웹 공격에 대해 가장 효과적인 사전 격리 기반 방어 체계를 구성할 수 있다. 설령 RBI 서버 세션 내에서 제로데이 공격이 발생하더라도, 해당 세션은 종료와 동시에 폐기되므로 내부 업무 환경으로의 확산 가능성은 원천적으로 차단된다.

주요 고객

카카오페이증권(25.12)
네오트랜스(25.12)
세종네트웍스(25.11)
세종디엑스(25.11)
파수(23.11)
KT(21.9)

3. 원격 사용자를 위한 보안/내부 웹 시스템 보호

기업 내부에 구축된 웹 서비스에 외부 사용자가 접근할 때 사용하는 VPN 방식은 원격 사용자의 단말을 내부 네트워크에 논리적으로 편입시키는 구조로, 단말 보안 수준에 따라 악성코드 감염, 계정 탈취, 내부망 확산 등 침해 사고로 직결될 수 있는 구조적 위험을 내포하고 있다.

반면 AirRBI는 외부 사용자가 사내 웹 서비스에 직접 접속하지 않고, RBI 서버가 내부 웹 서비스에 대신 접속한 뒤 그 실행 화면만을 외부 사용자에게 전달하는 **중계·격리 구조로 동작**한다. 외부 사용자의 단말은 내부 웹 시스템과 직접적인 네트워크 세션을 형성하지 않으며, 모든 웹 실행은 RBI 서버 내부에서만 처리, 단말의 보안 상태와 무관하게 내부 시스템을 안전하게 보호할 수 있는 구조적 격리 효과를 제공하는 것이다.

정리하면 VPN이 네트워크 터널링 기반의 내부망 확장 기술이라면, AirRBI는 응용 계층(Application Layer) 기반의 실행 분리 및 화면 중계 기술로 볼 수 있다. VPN은 내부망과 동일한 수준의 네트워크 접근 권한을 부여하는 반면, AirRBI는 사전에 정의된 웹 서비스만 제한적으로 접근하도록 통제할 수 있어 최소 권한 기반 접근제어와 제로 트러스트 보안 모델에 더욱 부합하는 구조를 제공한다. VPN과 병행 운영할 경우 다중 방어 기반의 최고 수준 원격 접속 보안 체계를 구현할 수 있다.

구분	VPN	AirRBI
접근 방식	내부망 직접 접속	서버 중계 기반 간접 접속

외부 단말 보안 의존도	높음	낮음
내부망 확산 위험	존재	구조적으로 차단
제로데이 대응	취약	사전 격리로 무력화
접근 통제	네트워크 단위	웹·업무 단위 세밀한 통제
정보 유출 통제	제한적	다운로드·복사·캡처 통제 가능

4. 첨부 파일에 의한 위협 원천 차단

AirRBI는 웹을 통해 유입되는 첨부 파일에 포함된 위협 요소를 원천적으로 제거하고, 사용자가 안전하게 문서를 활용할 수 있는 보안 환경을 제공한다.

웹 환경에서 첨부 파일에 대해서는 **원격 파일 미리보기 기능**을 제공하여, 사용자가 파일을 직접 다운로드하지 않고도 내용을 안전하게 확인할 수 있다. MS 오피스 문서(Word, Excel, PowerPoint), HWP, PDF 등 주요 업무용 문서를 폭넓게 지원하며, 주요 업무 문서는 원격 브라우징 환경에서 직접 미리보기 형태로 안전하게 열람할 수 있다.

또한 사용자는 격리된 웹 기반 문서 작업 환경에서 직접 문서를 편집하고 협업할 수 있으며, Microsoft 365, Google Docs 등 **주요 클라우드 기반 문서 서비스도 함께 지원**하여 외부 웹 문서 작업 시에도 단말 감염 위험 없이 안전한 업무 수행이 가능하다.

다운로드가 필요한 파일에 대해서는 **CDR(Contents Disarm & Reconstruction)** 기술을 적용하여 모든 비실행형 파일에 포함된 액티브 콘텐츠를 잠재적 위협 요소로 간주하고, 위험 가능 요소를 완전히 제거한 후 안전한 원본 형식의 파일로 재구성한다. 이를 통해 매크로, 스크립트, 외부 참조 코드 등 문서 기반 위협을 근본적으로 제거한다.

다운로드 정책 역시 실행 파일과 비실행 파일을 구분한 정적·동적 정책 제어 및 무해화 정책 적용이 가능하며, 사용자, 사이트, 그룹 단위로 세분화된 다운로드 권한을 설정할 수 있다. 이를 통해 조직의 보안 정책에 따른 정교한 파일 반입 통제가 가능하다. 정책적으로 허용된 파일의 다운로드 시에 다양한 바이러스 검사 솔루션과 연동을 제공하여 안전하지 않은 파일 다운로드를 차단한다.

5. 웹/생성형 AI 사용 중 발생 가능한 정보 유출 방지

AirRBI은 **정규식 기반**으로 민감정보를 탐지하는 기능을 내재하고 있다. 사용자가 프롬프트 내에 입력한 정보에 대해 민감 정보 포함 여부를 판단하며, 12가지 이상의 패턴에 대한 검사 기능을 제공한다.

또한 AirRBI는 AI 기반 자연어 처리(NLP) 기술을 활용한 DLP(Data Loss Prevention) 연동을 통해, 외부 웹 접속 과정에서 발생하는 모든 사용자 입력 데이터를 실시간으로 분석하고, 정보 전달 여부를 지능적으로 통제한다. 사용자가 웹 입력창에 입력하는 텍스트는 물론, 업로드를 시도하는 파일 내용까지 모두 검사 대상에 포함되며, 이 과정에서 개인정보를 포함한 법적 보호 대상 민감 정보와 고객이 보유한 영업비밀 정보를 기준으로 정밀한 보안 검사가 수행된다.

이를 통해 **생성형 AI 및 웹 서비스 이용 과정에서 발생할 수 있는 정보 유출을 근본적으로 차단**하며, 사용자는 정보 유출에 대한 우려 없이 생성형 AI 서비스를 안전하게 활용할 수 있는 보안 환경을 제공받게 된다. AirRBI를 통해 생성형 AI 활용 확대에 따른 보안 리스크를 효과적으로 해소하고, 조직의 핵심 정보 자산을 안전하게 보호할 수 있다.

6. 보안망에 위치한 시스템 개발 및 유지보수를 위한 환경 제공

AirRBI는 엄격한 보안 통제 환경에서도 외부 접근에 따른 리스크 없이 안전하게 개발 및 유지보수를 수행할 수 있는 유연한 원격 접근 환경을 제공하며, 보안성과 업무 효율성을 동시에 만족하는 차세대 보안 개발·운영 인프라로 활용될 수 있다.

AirRBI는 보호가 필요한 시스템이 위치한 네트워크와 가까운 위치에 직접 설치·운영할 수 있으며, 이를 통해 네트워크 구조와 보안 정책에 최적화된 형태로 유연하게 구축이 가능하다.

또한 **Sub Path 및 API 단위의 세분화된 정책 설정 기능**을 제공하여, 사용자별로 접근 가능한 시스템, 자원, API 범위를 정밀하게 통제할 수 있다. 이를 통해 개발자, 운영자, 외주 인력 등 역할에 따라 서로 다른 접근 권한을 부여하고, 불필요한 시스템 노출을 최소화함으로써 보안성과 운영 효율성을 동시에 확보할 수 있다.

아울러 **원격 브라우저 기반의 로그 수집 기능**을 통해, 개발 및 운영 과정에서 발생하는 다양한 예외 상황과 오류 이력을 브라우저 수준에서 직접 확보할 수 있다. 이를 통해 폐쇄망 환경에서도 장애 분석, 이슈 대응, 감사 및 추적이 가능하며, 문제 발생 시 신속한 원인 분석과 대응이 가능하다.

AirRBI는 에어코드가 독자적으로 개발 발전시킨 원격 브라우저 기술로,
글로벌과 국가 기준이 요구하는 보안 기준을 충족하며
고객의 요구하는 다양한 요구에 유연하고 능동적으로 대응하는 원격 브라우저 격리 시스템이다.

제품 문의

홈페이지:
www.airrbi.com

기술문의: 김광태
ktkim@aircode.com,
010-6397-2623

사업문의: 김윤상yskim
@aircode.com,
010-6681-8930