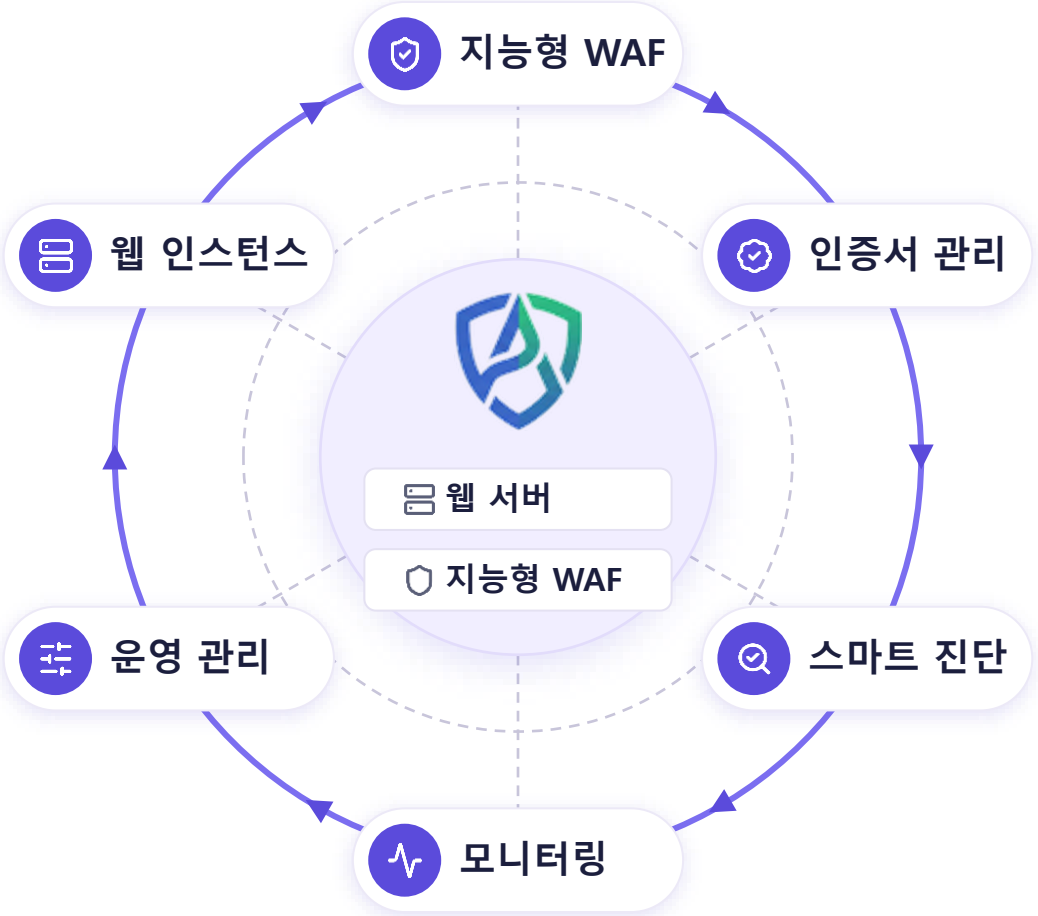
AtiCore

지능형 WAF를 내장한 스마트 보안 웹 서버

웹 서버 · WAF · 인증서 관리· 진단을 한 곳에서

웹 서버에 WAF를 내장하고, 웹 인스턴스의 설정·제어·상태·보안·진단·변경·감사·복구를 중앙에서 관리 합니다.



제품 소개 자료

㈜솔인시스템 · www.solinsystem.co.kr/product/aticore

목차

AtiCore 소개 자료

AtiCore - 스마트 보안 웹 서버



01 제품 소개 및 필요성

- AtiCore 제품 소개
- 웹 서버 보안·운영의 어려움과 해결 방식
- 제품 비교, 구성과 아키텍처

02 주요 기능 소개

- 기능 한눈에 보기
- 인증서 관리
- 지능형 WAF.
- 보안 이벤트 및 접근 제어
- 스마트 진단 과 성능 튜닝
- 통합 관제 및 분석

03 제품 구성 및 도입 효과

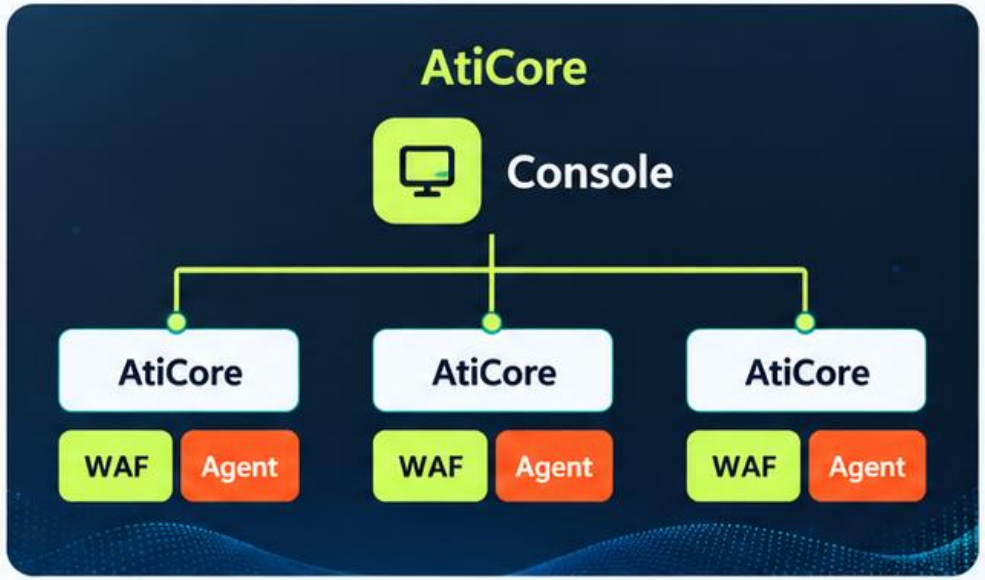
- 기본 구성과 옵션 팩
- 웹 서버 기능 비교
- 도입 효과
- 도입 사례

지능형 WAF가 내장된 웹 서버와 통합 운영 Console

1-1. AtiCore란?

AtiCore는 지능형 WAF가 내장된 웹 서버를 하나의 Console에서 운영하는 스마트 보안 웹 서버입니다.

웹 인스턴스를 만들고 복제하며 설정을 운영 서버에 반영합니다. 트래픽을 학습한 WAF로 공격 요청을 가려 차단하고, 인증서는 만료 전에 자동으로 갱신하며, 스마트 진단으로 성능과 보안 취약점을 찾아 개선 결과까지 확인합니다.



지능형 WAF

트래픽을 학습해 공격 요청을 가려 차단

인증서 자동 갱신

만료 전 자동 발급·갱신, 무중단 재적용

스마트 진단 및 가이드

주요 설정 검증을 통해 성능과 보안을 근거와 함께 진단하고, 개선 방향을 가이드

통합 Console

웹 인스턴스 운영을 콘솔 하나로 관리

서버마다 따로 운영하는 보안·인증서 → 보안과 운영을 하나의 Console로 → AtiCore

AtiCore는 웹 서버·보안·운영을 하나의 환경으로 통합합니다.

1-2. 웹 서버 보안·운영의 주요 문제점

서버마다 다른 웹 서버 기준 01

실행 파일·모듈·설정이 서버마다 달라 운영 기준이 제각각입니다

웹 보안의 일상 운영 어려움 02

차단이 업무에 영향을 줄까 걱정되고 오탐 예외 관리가 번거롭습니다

하드웨어 WAF 도입 부담 및 다중 보안 방어 체계 필요 03

기존 보안 장비를 통과한 웹 공격에 대해서도 웹서버 단계에서 추가적인 보안 검증과 차단이 필요하며, 이를 통해 단일 보안 체계의 한계를 보완하고 다중 방어 체계를 강화할 필요가 있습니다.

설정 취약점 점검 부담 04

점검에 별도 비용과 인력이 필요하고 개선 결과를 확인하기 어렵습니다

인증서 만료 관리 부담 05

인증서 만료를 추적하고 여러 서버의 인증서를 직접 교체해야 합니다

변경·복구 근거 분산 06

로고·성능·인증서·변경 기록이 흩어져 복구 판단이 어렵습니다

핵심 메시지: 웹 서버·보안·운영을 하나의 기준으로 묶어야 합니다.

1-3. AtiCore를 통한 운영 과제 해결

웹 서버 보안·운영 과제를 **AtiCore**로 하나의 흐름에서 해결합니다

웹 서버 보안·운영 과제	WAF 내장 통합 운영	AtiCore 적용 방식
1 서버마다 다른 웹 서버 기준	›	같은 기준의 웹 인스턴스 운영
2 웹 보안의 일상 운영 어려움	›	트래픽 학습 WAF·오탐 예외 체안
3 하드웨어 WAF 도입 부담 및 다중 방어 체계 필요	›	소프트웨어 WAF를 웹 서버에 내장
4 설정 취약점(성능, 보안) 점검 부담	›	소마트 진단·조치 후 재점검
5 인정서 만료 관리 부담	›	자동 갱신·일괄 교체·응답 확인
6 변경·복구 근거 분산	›	변경 이력·설정 복구·연계 조사

- 웹 보안 일상화
- 인증서 자동화
- 근거 기반 변경
- 운영 가시성 확보

AtiCore는 웹 보안과 운영 과제를 하나의 환경에서 해결합니다.

1-4. 구성과 아키텍처

Console과 Agent로 운영하고, **요청은 WAF 검사를 거쳐** 고객 영역으로 전달됩니다



AtiCore는 중앙 Console에서 다수 웹 서버를 통합 관리·제어합니다.

2-1. 주요 기능 한눈에 보기

웹 서버 운영부터 보안·진단·관제까지 **하나의 Console**에서 수행합니다

기본

웹 인스턴스 관리

생성·복제, 설정 편집, 제어·동기화

8p

인증서 관리 자동화

만료 확인·교체와 자동 발급·갱신

9p, 10p

지능형 WAF·접근 제어

트래픽 학습 탐지·차단, IP·대역·국가 정책

11p

스마트 진단 및 가이드

설정·보안·SSL/TLS 진단과 성능 튜닝

12p

통합 관제·분석

대시보드·메트릭·로그·토폴로지

기본

사용자 체감 분석(RUM)

체감 속도·오류·세션 분석

기본

운영 관리

작업·알람·알림 채널·시스템 설정

기본

권한·보안·감사

권한·MFA·감사 로그·Agent 승인

AtiCore는 웹 서버 운영·보안·진단·관제를 하나의 Console에서 수행합니다.

2-2. SSL 인증서 관리 자동화

인증서 만료 확인부터 **자동 갱신, 응답 확인까지** 연결합니다

01 만료 현황

기본

- 상황판에서 만료가 가까운 인증서와 조치할 일 확인
- 현황 맵으로 인스턴스와 인증서 연결 상태 확인
- 일정에서 만료·갱신 일정 확인



02 검증과 교체

기본

- 인증서 상세 확인·검증
- 검증한 인증서로 단건·일괄 교체
- 직접 받은 인증서도 키 일치·유효기간 확인



03 인증서 자동 발급·갱신 (옵션)

ACME 팩

- 만료 전 자동 발급·갱신·적용
- 와일드카드 인증서는 DNS 검증으로 발급
- 발급기관(ACME)·DNS 서비스 연결
- 부하분산기·프록시·클라우드에 동일 적용, 실제 응답 확인



AtiCore는 인증서 만료 대응을 확인 가능한 절차로 연결합니다.

※ 자동 발급에는 발급기관 연결과 도메인 검증 준비가 필요합니다.

2-3. 지능형 WAF (Web Application Firewall)

트래픽을 학습해 공격 요청을 가려 차단합니다

1

트래픽 기반 보호

- 경로별 정상 요청을 학습해 허용 범위 설정
- 차단 없이 먼저 시험한 뒤 적용

2

점수 합산 탐지

- 여러 탐지 규칙의 점수를 합산
- 기준을 넘는 요청만 차단, 보호 강도로 조정

3

오탐 예외 제안

- 반복된 정상 요청의 탐지 근거로 예외 제안
- 운영자가 확인한 뒤 반영

4

규칙·보호 설정

- 탐지 규칙의 의미와 적용 여부 관리
- 운영 모드·보호 강도·검사·저장 범위 설정

적용 원칙 | WAF 학습 규칙은 먼저 차단 없이 시험하고, 운영자가 승인한 뒤에만 적용합니다.

AtiCore는 | 업무 영향을 줄이면서 공격 요청을 차단하는 WAF 운영을 지원합니다.

2-4. 실시간 의심 이벤트 감지와 차단

보안 이벤트를 **조사하고 판정**한 뒤 예외까지 반영합니다

1 **요청 현황**

의심 이벤트가 많은 대상과 시간대 확인

2 **이벤트 탐색**

요청 하나의 처리 결과와 탐지 근거 확인

3 **탐지 검토**

정상·공격·추가 확인으로 판정하고 후속 조치 결정

4 **예외 관리**

정상 요청에 필요한 검사 제외를 검토·반영

5 **업무 확인**

반영 후 업무에 영향이 없는지 확인

접근 제어

웹 인스턴스별 IP·대역·국가 접근 정책을 만들어 운영 서버에 반영합니다. Console 로그인 권한과는 별개입니다.

WAF 보고서

기간별 보안 결과를 저장해 비교하고 공유합니다.

AtiCore는 보안 이벤트 조사부터 예외 반영까지 하나의 흐름으로 운영합니다.

2-5. 스마트 진단 항목과 성능 튜닝

진단 영역을 **항목별로 점검**하고 성능 설정 값을 제안합니다



보안 취약점 설정 진단 6개 영역

- 접근 통제
- 불필요한 기능 제한
- 정보 노출 차단
- 전송 보안·보안 헤더
- 권한과 경로
- 요청 크기·시간 제한

성능·안정성 설정 진단 3개 영역

- 성능
- 안정성
- 기본 설정

SSL/TLS 진단 5개 영역

- 프로토콜
- 암호화 방식
- 인증서
- 보안 헤더
- 세션·고급 설정

스마트 성능 튜닝

1. 메트릭과 로그를 분석
2. 최적의 성능 설정 값 제안
3. 편집본에 반영한 뒤 검토·배포

APM을 연결하면 WAS 지표와 요청 프로파일도 추가로 확인 가능합니다(조견부).

성능 튜닝 권장값은 자동 적용되지 않고, 검토 후 배포합니다.

2-6. 통합 관제와 분석

여러 서버의 상태·메트릭·로그를 **한 콘솔에서 연결해 분석**합니다.

모니터링

기본

- 커스텀 대시보드로 여러 웹 서버의 주요 지표를 위젯으로 확인
- 인스턴스별 자원·요청·응답 상태 확인



로그 & 메트릭

기본

- 서버 자원과 웹 서버 성능 지표를 기간별로 조회
- 접속·오류 로그 실시간 확인
- 여러 서버의 로그를 한 번에 검색
- 과거 로그를 조건별로 조회



웹 토폴로지 팩 (옵션)

웹 토폴로지 팩

- 웹 서버에서 WAS-DB로 이어지는 경로와 부하를 지도로 확인
- 느린 요청과 처리 중인 요청 추적



상태, 메트릭, 로그를 같은 대상과 시간 기준으로 연결해 조사합니다.

3-1. 제품 구성: 기본 구성과 옵션 팩

기본 구성에 **필요한 기능을 옵션 팩으로 확장**합니다

기본 구성

- 웹 인스턴스 생성·복제·제어·설정 동기화
- 인증서 현황·검증·교체
- 지능형 WAF와 접근 제어
- 대시보드·메트릭·로그 조회
- 스마트 설정·보안 진단 및 가이드
- 작업·알람·알림 채널
- 권한·감사·시스템 관리



옵션 팩

인증서 자동화 ACME 팩	인증서 자동 발급·갱신·적용, 발급 기관·DNS 연결
웹 토폴로지 팩	WEB/WAS·DB로 이어지는 경로와 부하 전체 확인
RUM	프론트엔드 오류 모니터링 사용자 체감 속도·오류·세션 분석

구성·라이선스·계약 방식은 도입 문의를 통해 안내합니다.

3-2. 웹 서버 기능 비교(1) – 관리, 설정, 제어

비교 항목 (기능)	AtiCore	타 상용 A 웹서버	타 상용 B 웹서버
Web GUI 기반 중앙 집중식 인스턴스 관리	● 다수 인스턴스 통합 관리 (상태, 설정, 배포, 모니터링)	△ 관리 콘솔 제공 (기본 관리 기능)	✕ 기본 제공 없음 (별도 솔루션 필요)
설정 및 인프라 취약점 스마트 자동 진단	● 설정/NVD 연계 취약점 자동 진단 및 개선 가이드	✕ 기본 제공 없음 (수동 점검 필요)	✕ 기본 제공 없음 (수동 점검 필요)
SSL 인증서 만료 모니터링 및 자동 교체	● 통합 인증서 관리 및 자동 갱신, 알림 설정	△ 인증서 관리 기능(관리 콘솔) (자동 갱신·교체 미지원)	✕ 기본 제공 없음 (스크립트 수동 작업)
GUI 연동형 WAF 보안 정책 통합 제어	● ModSecurity 기반 WAF 정책 통합 관리(GUI), 실시간 공격 탐지 차단	△ ModSecurity 제공 (GUI 통합 정책 제어 제한)	△ ModSecurity 제공 (GUI 통합 정책 제어 제한)
다수 노드 설정 일괄 배포 및 동기화	● 그룹 관리 기반 일괄 배포·동기화	△ 설정 동기화·스크립트 활용 (다중 노드 일괄 운영 제한)	△ Ansible 등 외부 도구 활용 (별도 자동화 구성 필요)
설정 버전 형상 관리 및 즉시 롤백 기능	● 설정 변경 이력 관리 및 원클릭 롤백	✕ 구성 변경 가능 (버전 관리·자동 롤백 미확인)	✕ 기본 제공 없음 (수동 백업 및 복원)
GUI 상에서 설정 문법 실시간 유효성 검증	● 설정 파일 실시간 검증 및 오류 가이드	△ httpd -t 명령 기반 검증 (GUI 실시간 검증 미지원)	△ configtest 제공 (스크립트 수동 실행)
무중단(Graceful) 인스턴스 재시작 원격 제어	● Graceful 재시작 원격 제어 (다수 인스턴스 동시 제어)	● 관리 콘솔·WLST 지원 (Soft Restart 가능)	● Graceful 명령 기본 제공 (apachectl -k graceful)
에이전트 기반 자동화 신규 노드 프로비저닝	● 에이전트 기반 자동 설치·동록 및 설정 반영	✕ 인스턴스 생성·스크립트 가능 (에이전트 자동 동록 미확인)	△ Ansible 인증 컬렉션 제공 (에이전트 자동 동록 미지원)
RBAC 권한 분리 및 수행 내역 감사 로그	● 사용자·역할 기반 권한 관리, 모든 작업 이력 감사	△ 역할 기반 권한 기본 제공 (세부 감사는 별도 설정 필요)	✕ 기본 제공 없음 (별도 솔루션 필요)

● **지원** (기본 제공 또는 통합 기능으로 제공) | △ **부분 지원** (일부 기능 또는 추가 구성·도구 필요) | ✕ **미지원** (해당 기능 기본 제공되지 않음)

3-3. 웹 서버 기능 비교(2) – 보안, 인증서 , 모니터링, 성능

비교 항목 (기능)	AtiCore	타 상용 A 웹서버	타 상용 B 웹서버
실시간 트래픽 및 시스템 리소스 통합 대시보드	● 통합 대시보드 제공	△ 기본 모니터링/상태 확인 (관리 콘솔, 실시간 지표 위주)	△ 기본 상태 페이지 제공 (통합 대시보드 없음)
다중 서버 로그 중앙 수집 및 실시간 스트리밍	● 다중 서버 로그 통합 수집	✕ 기본 제공 없음 (실시간 수집·스트리밍 미지원)	✕ 기본 제공 없음
로그 데이터 고속 통합 검색 및 필터링	● 통합 검색/필터링 제공	△ 로그 뷰어 기본 검색 제공 (도메인 내 한정)	✕ 기본 제공 없음
ACME 연동 SSL 인증서 자동 갱신	● 자동 갱신 및 적용	✕ 기본 제공 없음 (수동 갱신/적용)	✕ 기본 제공 없음 (수동 갱신/적용)
주/월간 운영·보안 통계 리포트 자동 생성	● 자동 리포트 생성	✕ 기본 제공 없음	✕ 기본 제공 없음
사용자 정의 이벤트 알람	● 이벤트/임계치 알람	✕ 기본 제공 없음 (별도 관리 제품 필요)	✕ 기본 제공 없음
HTTP/2 기본 활성화 (수동 튜닝 불필요)	● 기본 활성화	✕ 기본 제공 없음 (HTTP/2 모듈 미포함)	△ 지원 가능 (모듈 로드·수동 설정 필요)
Brotli 압축 기본 내장 지원	● 기본 지원	✕ 기본 제공 없음	△ Brotli 모듈 포함 (수동 설정 필요)

AtiCore는 모니터링, 보안, 인증서 자동화, 성능 최적화 기능을 단일 콘솔에서 통합 제공 합니다.

3-4. 도입 효과

서버마다 달랐던 웹 서버 운영을 **하나의 기준과 보안 체계**로 바꿉니다

01

웹 서버 운영 기준 통일

서버마다 달랐던 실행 파일·모듈·설정을
같은 기준의 운영으로 정리

02

일상 운영에 정착한 웹 보안

요청 차단, 업무 영향, 오탐 예외 관리를
하나의 흐름으로 운영

03

근거 기반 변경

로그·성능·인증서·변경 기록을 연결해
복구 판단 지원

04

범용 백엔드 호환

Java 모든 WAS와 Node.js 서비스를 한 웹 서버에 연결하고,
온프레미스부터 클라우드까지 같은 방식으로 설치·운영

05

비용·인력 부담 완화

하드웨어 WAF 없이 소프트웨어 WAF로 웹 보안을 확보하고,
추가 비용·인력 없이 설정/보안 취약점을 점검·개선
최고 가성비의 합리적인 도입 비용

핵심 메시지: 웹 서버는 하나의 기준으로, 보안과 운영은 한곳에서.

3-5. 도입 사례: G사 고향사랑기부제

G사는 소프트웨어 WAF와 소마트 진단으로 웹 보안을 확보했습니다

> “스마트 진단으로 웹 서버의 보안 취약점을 신속하게 개선하고, 결과까지 검증할 수 있었습니다”

01 도입 배경

- 사이트 오픈을 앞두고 하드웨어 WAF의 도입 비용과 운영 자원 부담이 컸음
- 설정 취약점 점검에 별도 비용과 인력이 필요

02 적용 방식

- 하드웨어 WAF 대신 AtiCore의 소프트웨어 WAF 도입
- 스마트 진단으로 점검 → 조치 → 재점검
- 웹 기반 콘솔·사전 점검·토폴로지 활용

03 도입 효과

- 추가 비용·인력 없이 설정 취약점을 점검·개선하고 재점검으로 검증
- 사전 점검으로 잘못된 설정 변경 방지
- 콘솔·토폴로지로 서비스와 인프라 확인

AtiCore는 비용과 인력 부담을 줄이면서 웹 보안과 설정 개선을 함께 지원합니다.

AtiCore

Thank you.

- AtiCore 스마트 보안 웹 서버
- AtiCore Web Manager 스마트 웹 운영 매니저
- ARIA Tomcat 통합 운영관리 플랫폼

서울시 구로구 디지털로 31길 41, 이앤씨벤처드림타워 6차 1302호

전화 02-6749-6250 | 팩스 02-6749-6265

sales@solinsystem.co.kr

www.solinsystem.co.kr/product/aticore

㈜솔인시스템 | www.solinsystem.co.kr