SecuLogic

Web Traffic Security Solution

지능적 사이버 공격 걱정 끝!

SecuLogic

논리적 보안

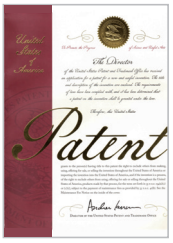
물리적 보안의 한계를 해결합니다.

특허 기술 **5건**을 기반으로 탄생

- 웹 애플리케이션 서버로부터 수집된 트랜잭션 정보를 이용한 보안장치
- 웹 서버로부터 수집된 트랜잭션 정보를 이용한 보안장치
- 웹 애플리케이션 서버로부터 수집된 트랜잭션 정보 및 고유 세션 ID를 통한 사용자 식별을 이용한 보안장치
- 웹 애플리케이션 서버를 통한 사용자 식별 기반의 데이터베이스 보안장치
- (미국 특허) 웹 애플리케이션 서버 또는 웹 서버로 부터 수집된 트랜잭션 정보를 이용한 보안장치







SecuLogic

제품특징

주요기능

SecuLogic은 다양한 사이버 공격에 대비하여 **정확하게 탐지하고 자동차단**함으로써 고객의 소중한 정보를 지켜줍니다.
이제는 논리적 보안으로 당신의 시스템을 안전하게 보호하세요.

정확한 사용자 식별	- 사용자 IP, 사용자 ID, Application Session ID - User Session ID(변하지 않는 세션 ID)
정확한 탐지 정책 제공	- HTTP Header 기반 탐지, 사용자 행위 기반 탐지 - 사용자별 통계 기반 탐지, DB Access 기반 탐지
Lightweight 트랜잭션 정보 전수수집	- WAS 메모리 내에서 이미 복호화 되어있는 트랜잭션 정보 전수 수집 - DML 데이터 수집(SQL Select, Update, Insert, Delete) - HTTP Request Header값 모두 수집(HTTP Header, Query String, Cookie)
Lightweight 탐지 제공	- Light Weight HTTP Header 기반으로 탐지 항목만 정확히 식별 - SecuLogic 서버에서 식별, 시스템에 부하 없음
다양한 차단 방법 제공	- HTTP Header 기반 차단, 사용자 IP 기반 차단 - Application Session ID 차단, User Session ID 차단
자동 차단 실현	- 정확한 탐지로 인한 차단 자동화, 차단 시간 설정을 통한 자동 차단 (차단 기준별로 차단 시간 설정, 분단위 및 영구 차단 가능)
서비스 관점의 정책관리	- 서비스/도메인 기준 정책 적용, 클라우드 시스템에 효과적 - 대규모 데이터 센터에 최적
빅데이터 분석	- 탐지 및 차단 이력 관리, 도메인/서비스별 추이 분석, 트랜잭션 분포도 분석 - Elasticsearch Kibana 활용, 사용자 행위 추적 분석

특장점

기대효과

SecuLogic은 웹트래픽 가시성 확보, 정확한 사용자 식별, 탐지 및 차단 자동화, 다양한 탐지 정책을 제공합니다.
그에 따른 **다양한 기대효과**를 경험하세요.

웹트래픽 가시성 확보

비 암호화 구간에서 웹트래픽 정보 수집
웹트래픽 정보 100% 전수 수집
웹서비스에 영향 없이 수집
빅데이터 저장 및 분석

정확한 사용자 식별

정확한 사용자 식별이 가능해짐
다양한 사용자 식별 방법
(IP, AP세션,사용자 세션,사용자 ID)

탐지 및 차단 자동화

명확한 탐지에 의한 100% 자동 차단 실현
차단을 위한 별도의 수작업 분석 불필요
탐지 및 차단 현황 이력 관리 자동화

다양한 탐지 정책

시그니처 기반 탐지
사용자별 통계 기반 탐지
사용자별 행위 기반 탐지
데이터 액세스 기반 탐지
사용자의 비정상 행위 탐지

SecuLogic

기능 비교표

구분	세부기능	SIEM	NG WAF	SecuLogic	비 고
제품 정의	정의	빅데이터 기반 보안관제 시스템	차세대 웹방화벽	소프트웨어 웹방화벽 + 빅데이터 기반 웹트래픽 보안	
데이터 수집	데이터 수집 방식	로그	네트워크 패킷	WAS 메모리	
	데이터 수집 종류	로그 및 이벤트 정보	웹트래픽	웹트래픽	
	데이터 구분	비정형 데이터	정형 데이터	정형 데이터	
	암호화 데이터(SSL)수집	SSL 가시성 솔루션과 연동 필요	복호화후 수집	비암호화 구간에서 수집	
	데이터 수집 부하	거의 없음	많음	거의 없음	
	사용자 식별	식별 불가	식별 불가	식별 가능	식별 불가 : IP로만 식별
탐지	탐지시 부하	거의 없음	많음	거의 없음	
	IP 변조 공격탐지	불가	불가	가능	
	사용자 ID 변조공격탐지	불가	불가	가능	
	통계 기반 탐지	일부 가능	불가	가능	
	사용자별 통계기반 탐지	불가	불가	가능	
	사용자 행위기반 탐지	불가	불가	가능	
	과다 호출 사용자 탐지	불가	불가	가능	
	웹트래픽 DDoS 공격 탐지	불가	불가	가능	
	DB Access 기반 탐지	불가	불가	가능	
	APT 공격 탐지	일부 가능	불가	가능	일부 가능 : 타제품 연동시
	세션 및 계정 탈취 탐지	일부 가능	불가	가능	일부 가능 : 타제품 연동시
	웹셸 탐지	일부 가능	가능	가능	일부 가능 : 타제품 연동시
	매크로 호출 탐지	일부 가능	불가	가능	일부 가능 : 타제품 연동시
차단	탐지시 자동 차단	일부 가능	가능	가능	
	세션 ID 기반 차단	불가	불가	가능	
	사용자 ID 기반 차단	불가	불가	가능	
	DB Access 기반 차단	불가	불가	가능	
트랜잭션 분석	장기간 트랜잭션 분석	가능	불가	가능	
	사용자 식별 기반 분석	불가	불가	가능	

elevisor

T. 042-485-8582 | F. 042-485-8583 | H. www.seculogic.co.kr
대전광역시 서구 둔산대로 117번길 66, 318호 (만년동 골드타워)