

# AISWG Application Insight Secure Web Gateway

완전한 웹 프로토콜 분석을 통해 비즈니스 요구사항에 필요한 비 업무 사이트 및 네트워크 어플리케이션을 통제하고 다양한 웹 기반 위협으로부터 내부 사용자를 보호합니다. SSL/TLS 통신에 대한 암호화를 대행 함으로써 네트워크 보안 시스템들의 암호화 트래픽 처리에 따른 부하를 감소 시키고 가시성을 제공하여 보안 사각지대를 방지하는 보안소프트웨어 입니다.

## Why Need Web Gateway?

### 비즈니스 효율성 이슈

- ▶ 비 업무 사이트 접속에 따른 생산성 저하
- ▶ 내부 사용자에 대한 인터넷 환경 제어 및 가시성 확보 필요
- ▶ 내부 사용자에 의한 주요/기밀 정보 유출
- ▶ 비 인가 경로 생성으로 인한 보안 사각지대 발생
- ▶ IT 컴플라이언스에 대응하는 정보보호시스템 구축



SSL/TLS Visibility



Real-time URL Filtering



Application Filtering

### 암호화 트래픽과 보안 위협

- ▶ HTTPS, SMTPS, POP3S, FTPS 등 SSL/TLS의 일반화로 암호화 트래픽 급증  
- 매년 20% 수준의 암호화 트래픽 증가 추세
- ▶ 암호화 트래픽 속에 숨겨진 보안 위협 증가  
- APT 공격의 80%는 암호화 트래픽을 활용
- ▶ 암호화 트래픽 탐지가 불가하거나 지속적으로 증가하는 트래픽으로 인해 보안 솔루션들의 부하 발생  
- HTTP/2 및 TLS 1.3 사용률 증가



Anti-malware



WEB DLP



Bandwidth Optimization

## Key Benefits of AISWG

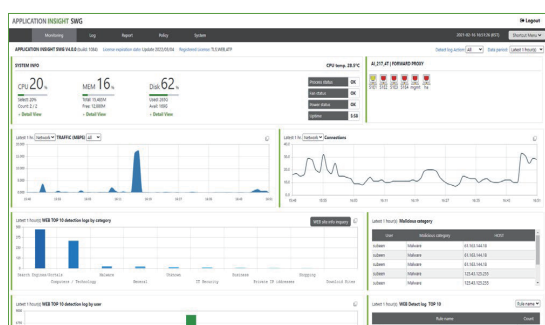
### 안전한 웹 환경 구축

- ▶ 요청 트래픽 분석을 통해 비 업무 또는 악성 URL 접근 차단  
- 사전 정의된 약 70여개의 카테고리를 이용하여 간편한 정책 수립
- ▶ 응답 트래픽 본문 분석을 수행하여 악성코드 유입 차단
- ▶ AV, 정적/동적, 자동화 리버스엔지니어링 등을 통한 악성파일 분석 및 차단
- ▶ 웹 메일 로깅 및 기능별 통제
- ▶ 보안 솔루션을 우회 하기 위한 프록시 및 VPN 트래픽 차단
- ▶ SNS, Messenger, Game, Office365, Google APP 등 1,100개 이상의 네트워크 어플리케이션 식별 및 필터링
- ▶ 키워드, 정규표현식, 첨부파일 제한 등 WEB DLP
- ▶ Youtube 콘텐츠 카테고리별 필터링
- ▶ 웹 서비스 품질향상을 위한 웹 캐시 및 QoS

### 암호화 트래픽에 대한 완전한 가시성 확보

- ▶ 기존 네트워크에 영향 없는 Full Transparent Proxy 모드 제공  
- 보안 시스템 연동 구간 장애 발생시 자동 바이패스 수행 및 서비스 가용성 확보
- ▶ SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3 지원 및 암호화 트래픽 자동 식별  
- RSA, DH, DHE 등 다양한 암호화 알고리즘 지원
- ▶ ALPN(Application-Layer Protocol Negotiation) 지원
- ▶ NAT(Network Address Translation) 네트워크 구성 지원
- ▶ 비동기 트래픽 네트워크 구성 지원
- ▶ 인증서 배포 및 관리  
- 인증서 설치 클라이언트 식별 및 설치페이지 리 다이렉트  
- NAC 연동을 통한 인증서 설치 현황 자동 관리
- ▶ PKP(Public Key Pinning) 리스트 온라인 업데이트

## AISWG Administration GUI



### 01. 시스템 모니터링

실시간 시스템 상태 및 탐지, 트래픽 현황 모니터링

### 02. 로그분석

> 다양한 검색 조건을 통한 상세 로그 조회  
> 사용자별 웹 접속 이력 로깅

### 03. 정책설정

사용자 및 그룹 별 세분화 된 정책 설정

### 04. 통계 및 보고

트래픽 및 IP, URL, 사용자, 카테고리 등 다양한 기준점으로 통계 보고서 생성

# Key Features of AISWG

## 1) 네트워크 구성모드

- > In-line: Full Transparent Proxy
- > Out-of-path: Forward proxy

## 2) 네트워크 호환성 최적화

- > Full Transparent Proxy 방식으로 기존 네트워크 구성 변경 불필요
- > TCP 세션과 관련된 모든 형상을 유지하여 다양한 이기종 보안 솔루션과의 유기적인 연동

## 3) Threat intelligence 플랫폼

- > 실시간 위협 및 카테고리 정보 업데이트
- > Machine learning 기반 URL, File 분석

## 4) 표준 SSL/TLS 트래픽 처리

- > SSL3.0, TLS1.0, TLS1.1, TLS1.2, TLS1.3

## 5) 다양한 알고리즘 지원

- > RSA, DHE, EDH, Camellia
- > AES, DES, SEED, 3DES, RC4
- > MD5, SHA-1, SHA-2

## 6) Full HTTP/2 지원

- > 완전한 HTTP/2 연결 및 구문 분석
- > HTTP/1.1과 동일한 보안 기능 제공

## 7) Full Access logging

- > 모든 클라이언트에 대한 웹 접속 이력 로깅

## 8) 카테고리 필터

- > 주식, 쇼핑, 게임, SNS 등 70개 이상의 사전 정의 카테고리를 이용해 간편한 웹 사이트 통제

## 9) Web DLP

- > Deep packet inspection 기반 데이터 유출 방지
- > 키워드, 정규표현식, 파일 확장자/사이즈 등 다양한 조건으로 규칙 생성

## 10) Web Mail 제어

- > 웹 메일 원문 로깅 (첨부 파일 포함)
- > 웹 메일 서비스 기능별 제어
  - 본문: 읽기, 쓰기, 특정 키워드 제한 등
  - 첨부 파일: 확장자 및 사이즈 제한 등

## 11) ATP 대응

- > 악성 URL 접근 차단
- > C&C 서버 및 봇넷 트래픽 차단
- > 첨부 파일 분석 및 파일 내 악성 URL 차단
- > 응답 페이로드 분석으로 악성 코드 유입 차단
- > (옵션) 웹 트래픽 내 실시간 파일 추출 및 정적/동적 분석 수행

## 12) 웹 가속

- > 웹 캐싱 기능을 통한 트래픽 절감 및 서비스 응답 속도 향상

## 13) 네트워크 어플리케이션 필터링

- > 메신저, VPN, 원격접속, 증편 등 약 1,700개 네트워크 어플리케이션 식별 및 필터링

## 14) PKP 리스트 관리

- > 정기적 PKP 목록 업데이트를 통한 서비스 가용성 확보

# AICC for Threat Intelligence



# 조달등록 가격정보

(VAT 포함)

모델명	물품식별번호	조달가격
보안소프트웨어, 모니터랩, APPLICATION INSIGHT SWG V2.0, 1~400User	22982631	22,300,000원
보안소프트웨어, 모니터랩, APPLICATION INSIGHT SWG V2.0, 401~600User	22982632	32,900,000원

### 제조사



(주)모니터랩  
 서울시 구로구 디지털로 31길 20, 407  
 TEL : 070-4633-7280  
 EMAIL : sales@monitorapp.com

### 조달 등록 업체



(주)비전테크  
 부산시 해운대구 센텀중앙로97 센텀스카이비즈 A동 2509호  
 TEL : 051-892-3723 FAX : 051-955-3723

### 조달 총판 업체



(주)아이터윈  
 부산: 부산시 서구 보수대로 111, 동아빌딩 2F TEL : 051-245-5321  
 서울: 서울시 서초구 반포대로 24길 15, 중앙빌딩 1층 TEL : 0 2-574-5321  
 대전: 대전시 서구 대덕대로 319, 우림빌유 213호 TEL : 042-483-5321