APPLICATION INSIGHT SWG

We Secure & Accelerate e-Business

MONITORAPP

What is APPLICATION INSIGHT SWG?

APPLICATION INSIGHT SWG(Secure Web Gateway)는 완전한 웹 프로토콜(HTTP/HTTPS) 분석을 통해 비즈니스 요구사항에 필요한 비 업무 사이트 제어와 진화하는 다양한 웹 공격 위협으로부터 기업 내부 사용자의 안전한 웹 환경을 보장하는 전용 어플라이언스 기반의 보안 웹 게이트 웨이 제품 입니다.

APPLICATION INSIGHT SWG는 다양한 형태로 사용자의 웹 접속을 제어하며 최신의 웹 위협을 차단합니다.

- 자사 Threat Intelligence를 통한 카테고리 및 악성 URL 실시간 업데이트
  - 시그니처에 의존하지 않는 행위기반 수집 시스템을 통해 다양한 Unknown 공격에 대한 선제적 방어
  - 57개의 일반 카테고리와 9개의 악성 카테고리 제공
- 우회 접속 및 Network Application(P2P, 메신저 등) 제어
- 네트워크 기반 DLP 제공으로 주요 자산 및 정보 유출 방지
- 사용자 인증을 통한 NAT/DHCP 환경 지원

APPLICATION INSIGHT SWG는 성능이 우수합니다.

- Transparent Application Proxy (특허번호 제 10-0898371호)
  - 고성능 패킷 처리 및 부하분산 알고리즘을 통한 대용량 트래픽 처리 성능 극대화
  - Full Transparent Proxy 타입으로 네트워크 구성 변경 없음
- Fail-open 및 Fail-over 기능을 통한 무중단 서비스 제공
- DPI(Deep Packet Inspection)를 통한 요청 및 응답 웹 트래픽에 대한 완전한 제어
- 자체 SSL 암복호화 기술을 통한 HTTPS 트래픽 분석

Why APPLICATION INSIGHT SWG?

WEB을 통한 보안 위협 요소 증가

- 최근 보안 사고의 80% 이상이 WEB 에서 발생
  - SSL 트래픽 속에 숨겨진 보안 위협
  - 기업이나 국가를 상대로 한 APT 공격 증가
  - 온라인 광고 배너 클릭만으로 악성코드 감염
  - 대부분의 기업은 알려진 악의적인 파일 또는 웹 서비스를 제공하는 도메인 접속
- 비 업무 사이트 접속 등을 통한 업무 효율성 및 생산성 저하
- P2P, SNS 등 위협 대상 다각화

APPLICATION INSIGHT SWG 도입 효과

- IT Compliance에 대응할 수 있는 정보보호시스템 구축
- 악성 사이트 접속 이나 C&C 서버 통신에 대한 선제적 대응으로 다양한 위협으로부터 내부 사용자 보호
- 네트워크 DLP를 통해 내부 사용자로부터의 중요 정보 및 기밀 유출 차단
- 내부 사용자의 인터넷 및 Network Application 통제를 통한 내부 트래픽 관리, 비즈니스 효용성 증대
- 별도의 SSL 가시성 솔루션과의 연동 없이 자체 SSL 트래픽 처리 기능을 통한 예산 절감

APPLICATION INSIGHT SWG Function

Internet Threats Control

- 요청 트래픽 분석을 통한 악성 URL 및 비 업무 사이트 차단
  - URL Filtering Categories 지원 : 약 1억 개 이상 URL DB
- 응답 트래픽 분석을 통한 악성코드 유입 차단
- Command and Control Center 및 Botnet 통신 차단
- 상용 웹 메일 서비스 기능별 통제
- 비 표준 웹 트래픽 및 Non HTTP 트래픽 제어
- P2P, 메신저, 웹 하드 등 Network 어플리케이션 제어
- Proxy 및 우회 접속 프로그램 차단
- 키워드, 정규식 등을 통해 첨부파일을 포함한 Network DLP 수행

Equipment Management

- Transparent Gateway로 One-Step 설치 및 기존 네트워크 영향 없음
- HA Configuration Mode: Active-Standby, Active-Active
- 사용자 인증 기능을 통한 NAT / DHCP 환경 지원
- 각 조직(또는 고객사)별 논리적으로 완전하게 분리된 다중 사용자 그룹관리 기능
- SSL 트래픽 처리를 위한 인증서 자동 설치 유도 기능
  - SSL 통신 불가 웹 사이트 자동 학습 및 대응 기능
- Real time Dashboard를 통한 종합 정보 제공
- 탐지로그, SSL 연결 로그, 감사 로그 등 다양한 로그 제공

APPLICATION INSIGHT SWG Physical Deployment

In-Line Mode (Full Transparent Proxy)

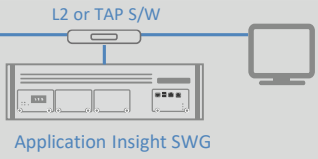
- 네트워크 경로상에 Bridge 형태로 In-Line 구성
- Transparent Proxy Mode 로 동작
- 시스템 이상 시 Bypass 지원
- Multi-Segment 지원

Out-of-path Mode (Forward Proxy)

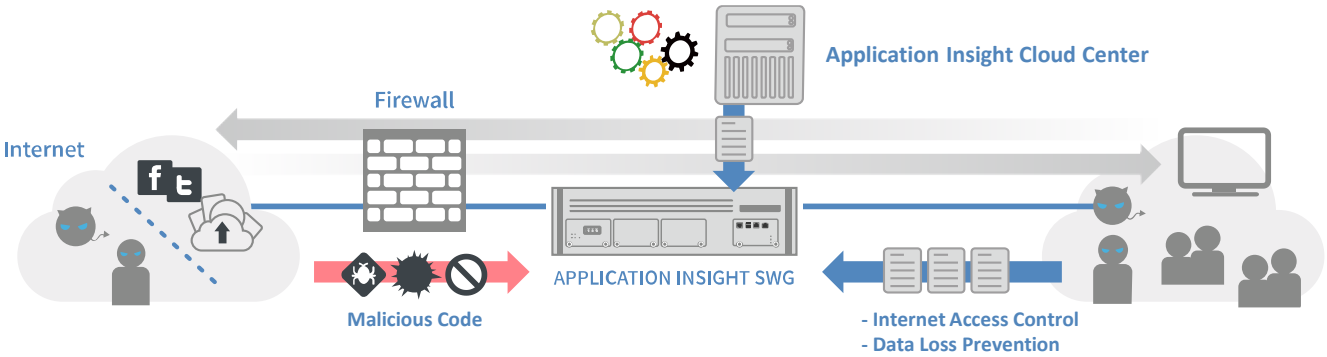
- 분산 클라이언트들에 대한 광범위 보호 구성
- PAC 및 브라우저 설정 (WEB 프로토콜 전용)
- 시스템 이상 시 Bypass 지원

Out-of-path Mode (Mirroring)

- TAP 또는 L2 Switch의 Mirror 기능을 이용한 구성
- 기존 네트워크에 미치는 영향도 없음
- 복사 된 트래픽 기반 Inspection 수행



AICLOUD Center For Threat Intelligence



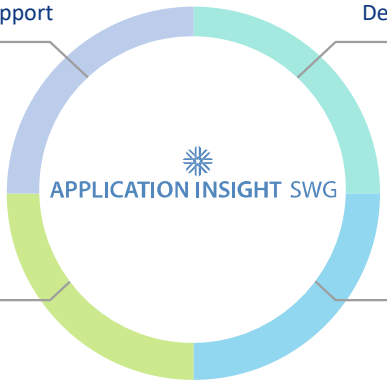
APPLICATION INSIGHT SWG Special Technology

Various Network Deployment Support

- In-line Mode
  - Full transparent Proxy
- Out-of-path Mode
  - Forward Proxy, Mirroring
- Multi-Segment, Bonding

Deep Packet Inspection

- 사용자 별 웹 서비스 제어
- 비 업무 및 악성 사이트 접속 차단
- 응답 트래픽에 포함된 악성코드 검출
- Network Data Loss Prevention



Proxy Gateway

- Transparent Application Proxy
  (특허번호 제 10-0898371호)
- 자체 SSL 트래픽 암복호화

Threat Intelligence

- 다양한 카테고리 및 DB : 1억개 이상 URL
- 클라우드 센터를 통한 실시간 업데이트
- 악성 URL 탐지에 대한 상세 근거

APPLICATION INSIGHT SWG Graphic User Interface

모니터링 및 시스템 현황
- 시스템 상태 및 트래픽 추이 실시간 확인
- 사용자 별 웹 서비스 이용 현황 실시간 모니터링

로그분석
- 정책에 위반된 로그에 대해 다양한 검색 조건을 통한 조회 및 관리

정책 설정
- 사용자 중심의 프로파일 타입 정책설정
- 예외 URL, 유해사이트 필터, 카테고리 필터, 웹 필터

통계 및 보고 기능
- IP, URL, 사용자, 카테고리 등 다양한 공격 탐지 정보 및 트래픽 현황에 대한 리포트

APPLICATION INSIGHT SWG Feature

Physical Configuration Mode
- In-Line Mode : Transparent Proxy
- Out-of-path Mode : Forward Proxy

  Mirroring
- Multi-Segment, Bonding

APPLICATION INSIGHT Cloud Center
- 자사 Threat Intelligence AICC와의 연동을 통해 실시간 위협 정보 업데이트

사용자 인증
- 자체 사용자 인증 기능을 통해 NAT/DHCP 환경에서도 완벽한 사용자별 정책 수립

멀티 사용자 그룹 관리
- 각 조직(또는 고객사)별 논리적으로 완전하게 분리 되어 조직간 독립적인 정책 수립 용이

SSL 트래픽 암복호화
- 별도의 SSL 가시성 솔루션 연동 없이, 자체 SSL 암복호화 기능을 사용하여 SSL 트래픽 속에 숨겨진 보안 위협 제거

네트워크 DLP
- 키워드, 정규표현식을 통해 사내 중요 정보 입력
- 본문, 첨부파일 필터링 등을 통한 내부 직원의 정보유출 방지

C&C 서버, Botnet 통신 제어
- 내부사용자의 C&C 서버 또는 Botnet 과의 통신 차단 (Reverse 세션 포함)

악성코드 유입 탐지
- 웹 응답 트래픽을 분석하여 Drive By Download, Malicious Script, Exploit Kit 등 탐지

카테고리 필터
- 57개의 카테고리(증권, 쇼핑, 포털 등)를 통한 사용자별 접속 가능한 웹 사이트 제어

악성 사이트 접속 제어
- 익명 서비스, 악용된 사이트, 피싱/사기 사이트, 악성 소프트웨어 등에 접근 하는 트래픽 차단

우회 접속 제어
- 보안 우회 목적으로 Anonymizing VPN Services, Tor Exit Nodes 등의 프로그램을 통한 접속 트래픽 제어

Network Application 제어
- 웹 트래픽 외에 P2P, 메신저, 웹 하드 클라우드 등과 같은 어플리케이션 제어

상용 웹 메일 서비스 제어
- 상용 웹 메일 서비스에 대한 상세 기능 (읽기, 쓰기, 첨부파일 사이즈/확장자, 특정 키워드 등) 별 제어

APPLICATION INSIGHT ATP Model & Specification

* Optional Interface

AISWG-200_Y17	AISWG-500_Y17	AISWG-1000_Y17	AISWG-2000_Y17	AISWG-4000_Y17
				
• UTP 1G x 6 * UTP 1G x 4 x 1 or Fiber 1G x 4 x 1 * SSL accelerator card	• Redundant Power Supply • UTP 1G x 6 * UTP 1G x 4 x 2 or Fiber 1G x 4 x 2 * SSL accelerator card	• Redundant Power Supply • UTP 1G x 2 and UTP 1G x 4 x 1 or Fiber 1G x 4 x 1 or 10G x 2 x 1 * UTP 1G x 4 x 1 or Fiber 1G x 4 x 3 or 10G x 2 x 3 * SSL accelerator card	• Redundant Power Supply • UTP 1G x 2 and UTP 1G x 4 or Fiber 1G x 4 or Fiber 10G x 2 * UTP 1G x4 x 7 or Fiber 1G x 4 x 7 or 10G x 2 x 7 * SSL accelerator card	• Redundant Power Supply • UTP 1G x 2 and UTP 1G x 4 or Fiber 1G x 4 or Fiber 10G x 2 * UTP 1G x4 x 7 or Fiber 1G x 4 x 7 or 10G x 2 x 7 * SSL accelerator card

MONITORAPP

306, 38-9, Digital-ro-31-gil,
Guro-Gu, Seoul, Korea, 08376
T. 02.749.0799 F. 02.749.0798
E. sales@monitorapp.com
www.monitorapp.com