웹 보안 게이트웨이 – ProxySG

웹을 통한 위협 차단을 위해 포괄적이고 세밀한 정책 적용이 가능한 웹 보안 전용 솔루션

- 웹 보안 게이트웨이 ProxySG는 웹 보안 정책을 제공하는 서비스로서 인터넷 트래픽의 90%를 차지하는 웹 트래픽에 대한 완벽한 보안 정책을 수립할 수 있도록 지원하는 웹 전용 게이트웨이 솔루션입니다. 항상 열려있는 80, 443 포트를 통해 끊임없는 위협이 도사리고 있으므로 복잡한 웹 프로토콜을 정확하게 파악하고 대응할 수 있는 전용 웹 보안 솔루션이 반드시 필요합니다.

비즈니스 요구사항

- 웹 트래픽에 대한 완벽한 통제
- https 암호화 트래픽에 대한 안정적인 제어
- Out-of-path Proxy 구성을 통한 상세한 웹 보안 정책 적용
- 웹 필터 DB(Intelligence Service)를 통한 전반적인 보안 정책 수립

시만텍 솔루션

- 업계 최초 10년 연속 가트너 리더그룹에 포함된 검증된 웹 보안 솔루션
- 다년간 축적되고 최적화된 업계 최고의 웹 필터 DB 보유
- TLS 1.3 및 HTTP/2 등 최신 트랜드의 수준 높은 프로토콜 지원
- AD 등과 같은 다양한 인증 솔루션 연동 지원
- 네트워크 DLP, AV엔진, 샌드박스와의 연동을 통한 파일에 대한 제어 기능 제공

도입 기대 효과

- 웹을 통해 유입되는 악성 트래픽에 대한 원천 차단 정책 지원
- 의심스러운 파일, 트래픽에 대한 사전 차단으로 기타 보안 장비 리소스 절약
- 샌드박스와 연동을 통해 알려지지 않은 악성코드에 대한 실시간 차단 정책 지원

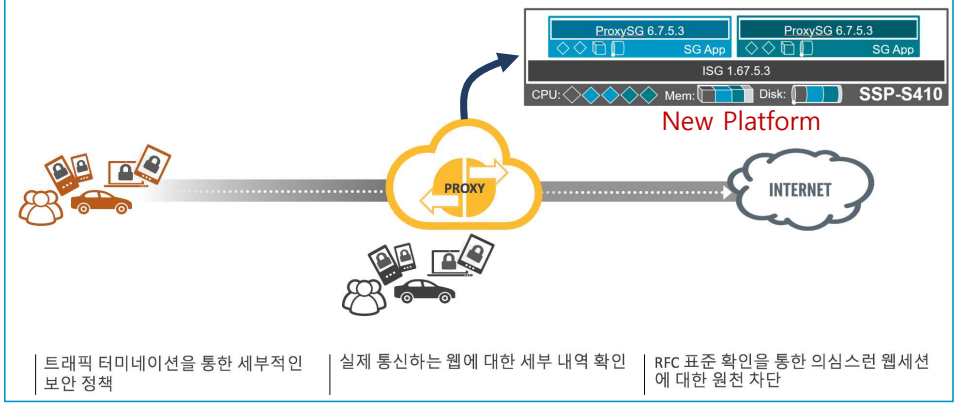
Host OS 기반의 High Performance 전용 플랫폼

- Hypervisor와 같이 Host OS 기반의 플랫폼 : SSP-410
- 요구 성능에 따라 하드웨어 리소스를 구매하여 성능 확장이 용이
- 네트워크 AV(CAS), 샌드박스(MA) 등과 통합 구축 운영 가능

시만텍 솔루션의 차별화 요소

- 클라우드 앱 DB를 포함한 업계 최고의 웹 DB 보유
- 웹을 통해 접속하는 악성 웹 사이트 및 유입되는 악성 트래픽에 대한 사전 차단 및 실시간 탐지/차단
- 신규나 의심되는 웹 사이트에 대한 접속 사전 차단
- 웹 트래픽에 대한 전수검사 기능 지원 (헤더, 바디, 데이터..등)
- 운영중인 보안 솔루션과 다양한 연동 기능 (DLP, CAS/AV, 샌드박싱, 복호화 트래픽 전송, SIEM..등)

솔루션 아키텍처



BROADCOM SOFTWARE

컨텐츠 분석 솔루션 – CAS (Content Analysis System)

웹을 통해 유입되는 파일의 다단계 검사를 위한 파일 검사 솔루션

- 기업의 인터넷 트래픽의 80~90% 차지하는 웹 또는 이메일 트래픽을 통해 유입되는 다양한 악성코드, 바이러스, 랜섬웨어 같은 지능형 위협들이 기존 운영중인 보안 장비를 우회해서 침투하고 있습니다. 알려진 위협을 차단하고 아직 알려지지 않는 위협을 분석할 수 있는 다단계 심층적 방어 기능을 통해 완벽한 보안 정책을 수립할 수 있도록 지원하는 웹 전용 콘텐츠 분석 솔루션입니다. 항상 열려있는 80, 443 포트를 통해 끊임없는 유입되는 위협을 효율적으로 탐지 차단을 위해서 완벽한 통합 방어 능력을 가진 콘텐츠 분석 전용 솔루션이 반드시 필요합니다.

비즈니스 요구사항

- 다단계 심층 방어 기능을 통해 기존 AV 제품의 한계 극복
- 웹/메일을 통해 유입되는 알려진 악성코드나 바이러스 완벽한 탐지/차단
- 랜섬웨어 같은 지능형 위협이나 공격을 탐지 및 차단

시만텍 솔루션

- 업계 유일한 듀얼 AV 엔진을 탑재한 웹 전용 인라인 악성코드 탐지 및 차단 솔루션
- 다단계 심층적 방어 기능 탑재하여 악성코드 차단 범위 및 정확도 향상(파일 평판 DB, 정적코드 분석 등)
- 실시간 글로벌 인텔리전스 네트워크와 새로운 결과 공유 통해 효과적인 제로데이 공격 방지
- 50억 개의 파일 평판 DB를 통한 AV 엔진 효율성 증대
- 매 5분 마다 악성코드 시그니쳐 DB 업데이트
- ICAP 연동을 통한 다양한 보안 장비와의 연동 기능 제공

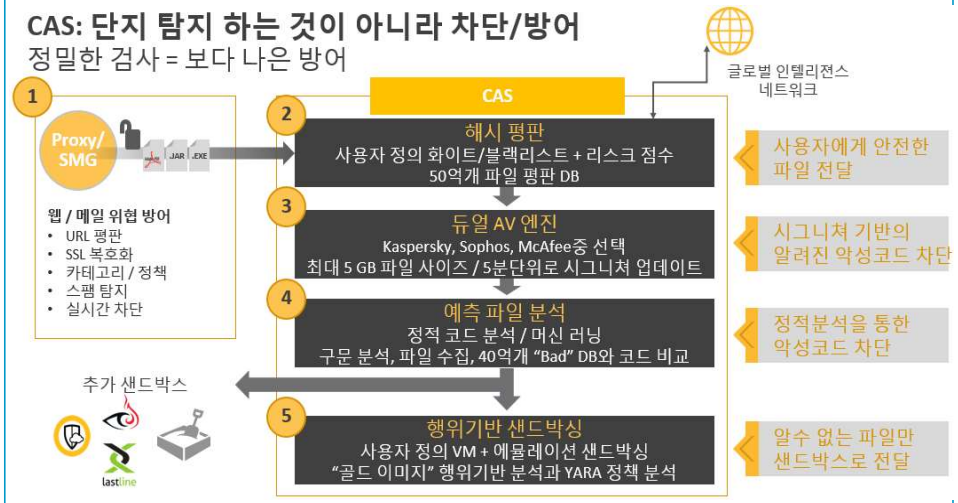
도입 기대 효과

- 웹을 통해 유입되는 악성코드나 바이러스 원천 차단 정책 지원
- 다단계 심층적 방어 기능을 통해 랜섬웨어 같은 지능형 위협 탐지 및 차단
- 샌드박스와 인라인 연동을 통해 알려지지 않은 악성코드에 대한 실시간 차단 정책 지원

시만텍 솔루션의 차별화 요소

- 업계 유일한 다단계 심층 방어 기능을 통해 알려진 또는 알려지지 않은 악성코드 탐지 및 차단 (해시 평판 DB, 듀얼 AV엔진, 정적 파일 분석 등)
- 알려진 악성코드 사전 필터링 기능을 통해 샌드박싱 최적화 기능 제공

솔루션 아키텍처



BROADCOM SOFTWARE

동적 파일 검사 – MA (Malware Analysis)

정적검사에 의해 탐지되지 않은 의심스러운 파일들의 동적검사 수행을 위한 솔루션

- Symantec Malware Analysis는 다양한 방식의 강력한 커스터마이징 기능을 제공하고, Hybrid SandBox로 우회기법을 탐지하며, 악성 여부에 대한 명확한 스코어링을 통하여 알려지지 않은 위협을 차단하는 행동기반탐지 솔루션 입니다. 1일 최대 50,000개의 샘플을 처리할 수 있는 높은 성능을 보유하고 있으며, Symantec CAS 시스템의 연동 기능을 통해 알려지지 않은 위협에 대응할 수 있도록 효과적인 운영 방안을 제시합니다.

비즈니스 요구사항

- 알려지지 않은 공격의 효과적인 탐지
- 행동기반 탐지의 범용성 (DRM 문서파일의 탐지 외)
- 통제를 위한 명확한 분석 결과 제공
- 기존 고객사가 유지하고 있는 다양한 보안솔루션과 유연한 연동 기법 제공

시만텍 솔루션

- Symantec Malware Analysis 솔루션은 샌드박스 기술을 통한 알려지지 않은 공격의 효과적인 탐지 기술 제공
- 강력한 커스터마이징 기능을 통해서 DRM, 한국에서만 사용하는 특정 어플리케이션 등에 대한 광범위한 탐지기술 제공
- 행동기반탐지 결과의 스코어링을 통한 명확한 분석 리포트 제공
- Emulate 기반과 Virtualized의 두가지 다른 기술의 하이브리드 샌드박스 제공
- 행동기반탐지간 생성된 모든 파일들의 추출 가능

도입 기대 효과

- 1일 10,000개 에서 50,000개 까지의 처리성능을 보장
- Sandbox 환경의 커스터마이징 뿐 아니라 탐지 패턴에 대한 커스터마이징 기능을 통하여 탐지 결과 내역 최적화 기능 제공
- Symantec의 다양한 솔루션(ASG, CAS, SA, SMG, APT)의 직접적인 연동을 통하여 솔루션의 고가용성 및 효율적인 운영

시만텍 솔루션의 차별화 요소

- 강력한 처리 성능
- 샌드박스 및 탐지패턴의 커스터마이징
- 윈도우즈, 안드로이드, IOS 등 다양한 샌드박스 환경 제공
- 강력한 Remote API 기능 제공

솔루션 아키텍처

BROADCOM SOFTWARE

웹 위협 격리 솔루션 – Web Isolation

웹 접속을 단순 차단/허용하는 것이 아니라 웹 페이지의 소스를 격리하여 가장 완벽한 웹 보안 제공

- Symantec Web Isolation은 사용자가 요청하는 웹 페이지를 스트리밍 형태로 제공하여 실제 위협이 닿을 수 없는 완벽한 웹 격리 솔루션 입니다. 모든 웹 페이지 및 파일들이 스트리밍 및 뷰어 형태로 제공되어 실제 사용자 PC에 어떠한 위협 요소도 실행 및 저장되지 않는 가장 완벽한 보안 기능을 수행합니다. 100% 모든 웹 구성요소에 대한 완벽한 스트리밍 기술력을 제공하며 가장 빠른 속도의 스트리밍 격리 서비스를 제공합니다.

비즈니스 요구사항

- 기존의 화이트리스트, 블랙리스트 정책에서 구분되지 못하는 사이트들에 대한 보안성 여부 판단 필요
- 드라이브바이다운로드, 스크립트를 통한 악성코드유입과 같은 지능적인 웹 공격에 대한 방어
- 보안장비에서 예외처리한 사이트에서 발생할 수 있는 악성 행위 시도 여부 방어
- 기존 웹 필터에서 카테고리 등록되지 않은 신규 사이트 등에 대한 방어

시만텍 솔루션

- 웹사이트를 차단하는 것이 아니라 스트리밍 형태로 제공하여 사이트는 차단되지 않고 서비스를 이용할 수 있지만 어떠한 종류의 파일도 다운되지 않는 방식의 웹 격리 솔루션
- 별도의 에이전트 없이 브라우저만으로 구현 가능 국내외 거의 모든 사이트 지원
- 키보드 타이핑, 마우스 등 실제 웹페이지에서 행하는 모든 기능에 대한 지원 가능
- 파일다운로드 시에 별도 뷰어 형태로 스트리밍 페이지 제공

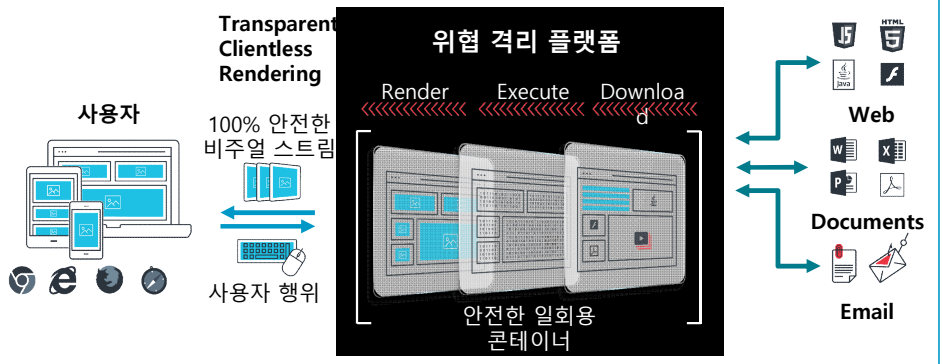
도입 기대 효과

- 화이트리스트, 블랙리스트 기반 차단정책시 반드시 존재하는 그레이 영역에 대한 완벽한 보호 (그레이 영역이란 허용, 차단에 대한 기준이 모호한 영역의 웹사이트 ex : DynamicDNS, file sharing, un-catagries 등)
- 모든 트래픽을 격리하여 서비스할 경우 웹을 통해 유입될 수 있는 우회 공격에 대한 가장 확실한 보안 시스템 구축 가능

시만텍 솔루션의 차별화 요소

- 100% 모든 웹구성요소에 대한 스트리밍 기술 제공 (경쟁사의 경우 CSS, font와 같은 정보를 스트리밍 에 포함시키지 않고 그대로 사용자에게 보냄)
- 기존 프록시 제품과 완벽한 연동 및 클라우드 서비스 구축 가능
- 시만텍 파일 분석 및 차단 솔루션 (Content Analysis)의 연동을 통한 단계별 보안체계 및 완벽한 격리 플랫폼 구축

솔루션 아키텍처



BROADCOM SOFTWARE

클라우드 웹 보안 솔루션 – WSS (Web Security Service)

재택근무자의 웹 보안 정책 적용을 위한 클라우드 기반의 웹 보안 게이트웨이 서비스

- WSS(web security service)는 클라우드 기반의 토탈 보안 솔루션으로서 원격 사용자를 포함한 내부 사용자가 외부망으로 통신할 때 SASE 개념의 통합보안 서비스를 제공하고, 데이터 접근에 대한 Zero Trust구현을 위한 다양한 보안기술을 제공합니다. WSS 서비스는 전세계의 GCP(Google Cloud Service)를 IaaS로 사용하고 있으며 대한민국의 Seoul 리전에서 직접 서비스를 제공 합니다.

비즈니스 요구사항

- 원격 사용자를 포함하여 외부에서 스마트폰을 포함한 다양한 단말기를 지원하며, 고객 니즈에 따라 VPN, Agent, Proxy등 다양한 접속 방법을 제공
- 이동 사용자에 대한 웹 보안 정책 적용 필요
- 지사 등 소규모 오피스에 대한 보안 정책 적용 및 동기화 요구
- 디바이스에 대한 관리 및 운영 어려움

시만텍 솔루션

- 다양한 구성 방식 지원(Proxy, WSS Client, Mobile, Firewall VPN/IPsec 등)
- AD 인증, O365 연동, SAML IDP, Captive Portal 등을 통한 다양한 인증 및 사용자 기반의 정책방안 제공
- 시만텍 인텔리전스 및 어플리케이션 인지 기능 통한 효율적인 차단기능 및 정책의 고도화
- AV, 샌드박스, 웹 격리, 방화벽(Fortinet), 네트워크 DLP, CASB 등의 토털 솔루션 제공
- 온프라미스와 클라우드를 동시에 운영 가능(One Management), 능동적인 리포팅 제공

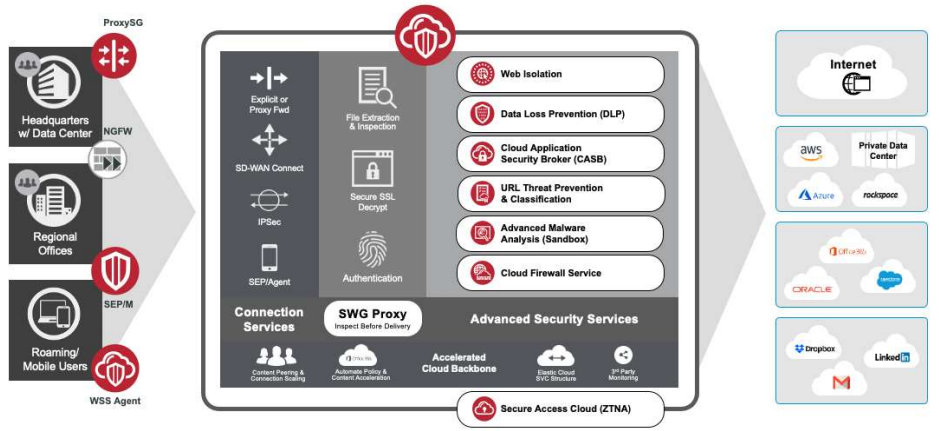
도입 기대 효과

- 어느 장소, 어느 디바이스에도 동일한 보안 정책 적용을 통한 웹 보안 향상
- ProxySG와 정책 동기화를 통하여 하이브리드 구성
- 유저당 번들 형태의 도입을 통하여 초기 투자 및 TCO 절감 효과

시만텍 솔루션의 차별화 요소

- 전세계 GCP 리전의 사용을 통한 가용성 및 안정성 확보
- 시만텍의 기술이 압축 되어있는 클라우드 기반의 SASE
- 엔드포인트 솔루션이 WSS Agent에 통합되어 네트워크와 엔드포인트 보안을 동시에 수행

솔루션 아키텍처



BROADCOM SOFTWARE

시만텍 인텔리전스 – IS (Intelligence Services)

URL Categorization 및 최신 위협 차단을 위한 가장 방대하고 광범위한 보안 인텔리전스 제공

- Symantec IS (Intelligence Services)는 시만텍 글로벌 리서치 기관인 STAR와 더불어 Global Intelligence Network(GIN)을 활용한 인텔리전스 서비스 입니다.

비즈니스 요구사항

- 글로벌 보안 위협 인텔리전스의 필요성
- 솔루션 자체의 평판서비스가 아닌 API등으로 자사 시스템과 연동 필요
- 로컬의 국지적인 DB가 아닌 글로벌 DB의 필요성

시만텍 솔루션

- 전세계에서 올라오는 실시간 평판정보를 실시간으로 업데이트
- URL, URL Category, File 평판, Application에 대한 IS 제공
- API 서비스 제공
- 175M+ Endpoint, 80M+ SWG, 160M+ Email, 15,000+고객사에서 업데이트
- 하루에 수십 억개의 위협을 차단
- 하루에 수백만개의 새로운 URL을 등록 및 업데이트
- 35,000개 이상의 Cloud 어플리케이션 ID

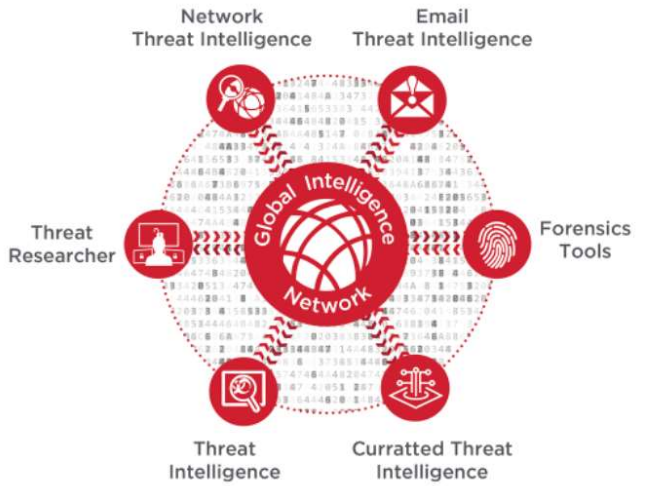
도입 기대 효과

- 모든 시만텍 솔루션의 평판 정보는 공통 플랫폼으로 GIN(시만텍 인텔리전스)을 사용
- API를 활용하면 내부 ESM등의 분석시스템과의 연동 등 다양한 응용이 가능

시만텍 솔루션의 차별화 요소

- 엔드포인트, 네트워크, 이메일 위협을 동시에 수집
- WSS, SEP, DLP, CASB, Email.Cloud, SWG, ASG, Isolation등 평판서비스가 필요한 모든 시만텍 솔루션에 적용

솔루션 아키텍처



BROADCOM SOFTWARE