Symantec Solution Portfolio

DS data
Digital Security

BROADCOM
SOFTWARE

BROADCOM SOFTWARE

Contents

✓ On-premise
✓ Part of SES

1. 엔드포인트 보안 – SEP (Symantec Endpoint Protection)

세계 최대의 평판 DB와 행위기반 탐지기술을 통해 내부로 유입되는 신종 및 변종 악성코드 탐지

- Symantec Endpoint Protection은 시만텍의 핵심기술인 평판기술과 행위기반 탐지기술을 바탕으로 사용자 PC 및 서버에 유입되는 신종 및 변종 악성코드에 대해 혁신적인 차단율을 제공합니다. 단순 안티바이러스 기술을 통해 대응할 수 없는 표적공격 및 지능형 지속가능 위협공격(APT)에 대해 효과적이고 강력한 대응기술을 제공하며, 또한 확장된 보안통제 기능들을 단일 에이전트로 구현하였습니다.

비즈니스 요구사항

- 최근 위협 동향에 따른 다양한 리눅스 플랫폼의 실시간 감시 기능 필요
- 랜섬웨어의 행동 특성에 따른 단계적 방어(Kill Chain) 수단 필요
- 저장매체에 대한 통제 필요
- 엔드포인트의 무결성(내부 보안정책 준수)에 대한 보장 어려움
- 단일 에이전트를 통한 포괄적인 통합보안 필요

시만텍 솔루션

- Symantec Endpoint Protection은 전세계에서 수집된 악성코드 정보를 바탕으로 빅데이터 기반의 인텔리전스 기술인 평판기술과, 악성코드 행위분석을 통해 구현한 행위기반 차단기술로 패턴에 없는 신종/변종 악성코드를 진단 및 차단
- 안티바이러스: 세계 최고의 악성코드 진단기술, 높은 탐지율과 시스템 안정성
- 침입 탐지: 글로벌 벤더와 사전 공유된 취약점 대응 패턴 보유
- 매체 통제: USB, 외장하드, 스마트폰 등 디바이스에 대한 통제
- 애플리케이션 통제: 프로세스,레지스트리 통제를 통한 애플리케이션 제어
- 호스트무결성: PC보안설정 및 S/W설치 등 내부 보안정책 강제화 통제
- 랜섬웨어 차단 위한 새로운 엔진 : 첨단 머신 러닝, 애뮬레이터, 취약점 차단 기술

도입 기대 효과

- 최신 보안 위협으로부터 안정적인 비즈니스 연속성 보장
- 기업 보안 경쟁력 증대 및 관리 리소스 감소
- 사내 보안정책 강제화를 통한 회사 보안레벨 증대

시만텍 솔루션의 차별화 요소

- 안티바이러스 그 이상의 포괄적인 통합보안 제공
- 업계 최고의 탐지율, 안정성
- 신종/변종 위협에 빠르게 대처할 수 있는 글로벌 인프라
  - Symantec Global Intelligence Network

솔루션 아키텍처

BROADCOM SOFTWARE

✓ Part of SES-C

2. 지능형 위협 대응 – EDR (ATP 및 통합 대응)

모든 경로를 통해 유입되는 외부 공격을 기록하여 보다 적극적인 탐지 및 대응을 위한 솔루션

- Symantec ATP는 엔드포인트/이메일/네트워크 영역에서 알려지지 않은 위협을 발견/조사/대응하기 위한 통합 솔루션으로 위협을 가시적으로 표현하고 위협의 내용에 따라 우선순위를 배정하여 대응하는 유일한 솔루션입니다. 추가 에이전트 없이 SEP와 연계하여 모든 엔드포인트의 이벤트 및 행위를 추적 / 조치 합니다.

비즈니스 요구사항

- 엔드포인트 상에서 알려지지 않은 위협을 탐지 및 조치가 필요함
- 위협의 지속적인 유입이 있으나 유입 경로 방어 및 대응이 효과적으로 되지 않음
- 웹 또는 이메일을 통해 감염될 수 있는 악성코드에 대해 자동탐지 및 차단 필요
- 의심스러운 파일 및 악성 실행파일에 대한 위협 파악 및 차단

시만텍 솔루션

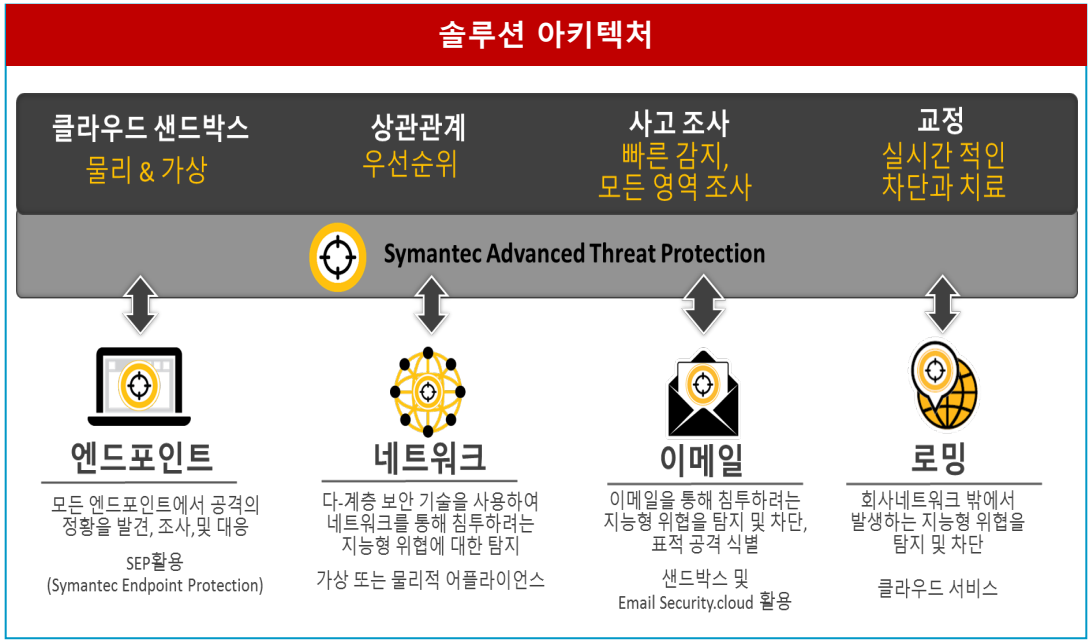
- SEP와 통합된 EDR솔루션으로 성능 저하 없이 엔드포인트 상의 위협 제거
- 인시던트 관리: 공격을 가시적으로 표현하여 공격을 직관적으로 이해 및 즉시 조치
- 우선순위 제공: 조치가 필요한 중요 인시던트를 먼저 표시하여 관리자가 피해를 최소화 하여 빠른 시간에 조치가 가능하게 함
- 통합 ATP 솔루션
  - ATP Endpoint(EDR): SEP클라이언트를 이용하여 엔드포인트 내의 의심스러운 악성코드를 판별, IOC 검색 , 조치 지원 (EDR기술)
  - ATP Email: Email Security.cloud 연동 모듈로 메일로 유입되는 표적공격 및 지능형 위협을 탐지하고 차단, URL분석 및 URL링크를 클릭시에 보호하는 기능을 제공

도입 기대 효과

- 엔드포인트에서 알려지지 않은 위협의 탐지 및 검색 / 차단
- 알려지지 않은 위협의 유입경로 별 효과적인 차단 및 대응
- 탐지 및 대응에 필요한 시간의 감소로 빠른 위협 대응

시만텍 솔루션의 차별화 요소

- 엔드포인트 상의 알려지지 않은 위협의 빠른 제거 / EDR기능을 위해 별도 에이전트 필요 없음
- 위협의 내용별 조치 우선순위 제공으로 효과적인 대응가능
- 표적 공격의 유무 보고 / 시각적인 위협 상태 보고



BROADCOM SOFTWARE

3. 기업의 주요 자산 유출 방지 – DLP (Data Loss Prevention)

기업 내부와 클라우드 상에 존재하는 주요 정보 자산의 외부 유출을 막기 위한 정보유출방지 솔루션

- Symantec Data Loss Prevention은 기업내 중요 데이터가 어디에 저장되어 있는지 검색하고, 어떻게 사용되는지 모니터링하여 관리자에게 가시성을 제공합니다. 또한, 데이터가 유출될 수 있는 다양한 채널을 감시하여 유출되거나 도용 당하지 않도록 보호합니다. 클라우드로의 보호 영역 확장을 위해 Cloud DLP 서비스를 제공하며, 웹 게이트웨이, CASB와 연계하여 보다 강력한 데이터 보호를 실현합니다.

비즈니스 요구사항

- 개인정보보호법 및 각종 사내/외 컴플라이언스 준수를 위한 필요
- 개인정보 및 중요정보가 악의적 목적이나 실수로 외부로 유출되지 않도록 통제
- 가시성 확보 및 효과적 정책 수립을 위한 리포트 제공
- 클라우드로의 보호 영역 확장 필요

시만텍 솔루션

- 정책 정의를 위한 템플릿을 제공하고, 다양한 대응 규칙 적용을 통해 정보유출에 대한 통합 보안대책을 마련하는 기반을 제공
- 300여종 이상의 파일인식 지원, 세계 각국의 개인정보 탐지 지원, AND / OR 조건을 통한 유연한 정책 적용 지원
- 현재 사용중인 어플리케이션 뿐만 아니라 추가 도입되는 어플리케이션에 대한 보호조치까지 지원
- Cloud DLP 서비스를 제공하여 클라우드 상의 데이터 보호
- 글로벌 DLP 마켓 리더로 Fortune 500 기업의 절반 이상이 사용

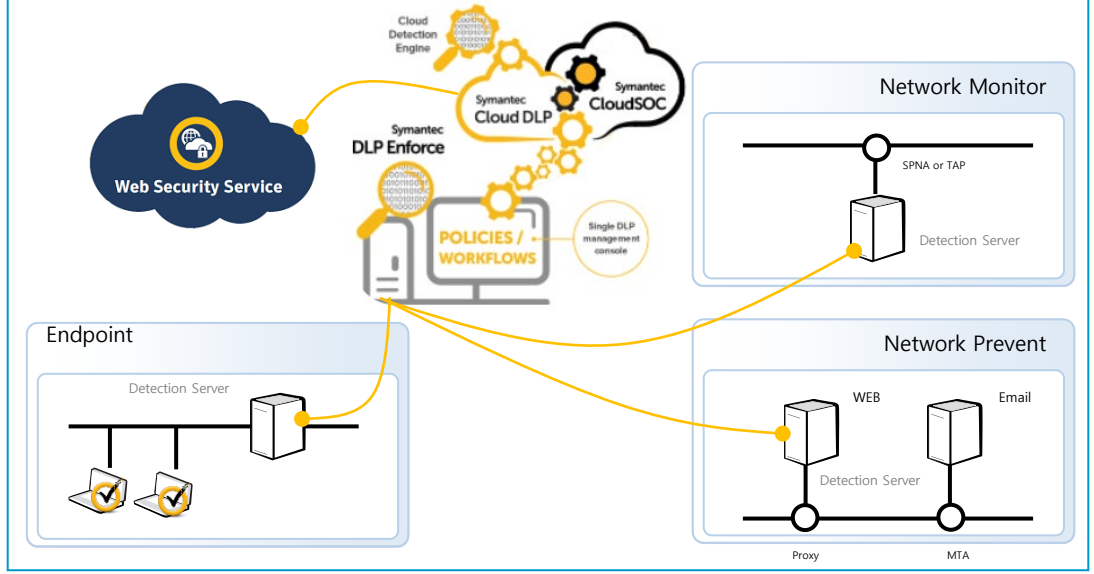
도입 기대 효과

- 컨텐트 기반의 실시간 정보유출 모니터링 및 차단
- 언제, 누가, 무엇을, 어떻게, 어디로 전송했는지에 대한 정확한 정보 제공을 통한 가시성 확보
- 클라우드 웹 보안 게이트웨이 및 CASB와 연동을 통한 기업 보호 영역의 확장
- 사용자 알림을 통한 임직원의 보안 인식 변화

시만텍 솔루션의 차별화 요소

- 엔드포인트 DLP의 광범위한 탐지 채널(Https, Smart Phone, 어플리케이션 등)
- 엔드포인트, 네트웍, 스토리지, 클라우드 등 가장 광범위한 보호 제공
- 키워드 뿐만 아니라 DB, 비정형데이타, 각종 양식에 대한 보호 제공
- 특허받은 머신러닝 기술을 통해 사용자와 자산 행위 기반의 Baseline 적용

솔루션 아키텍처



BROADCOM SOFTWARE

4. 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

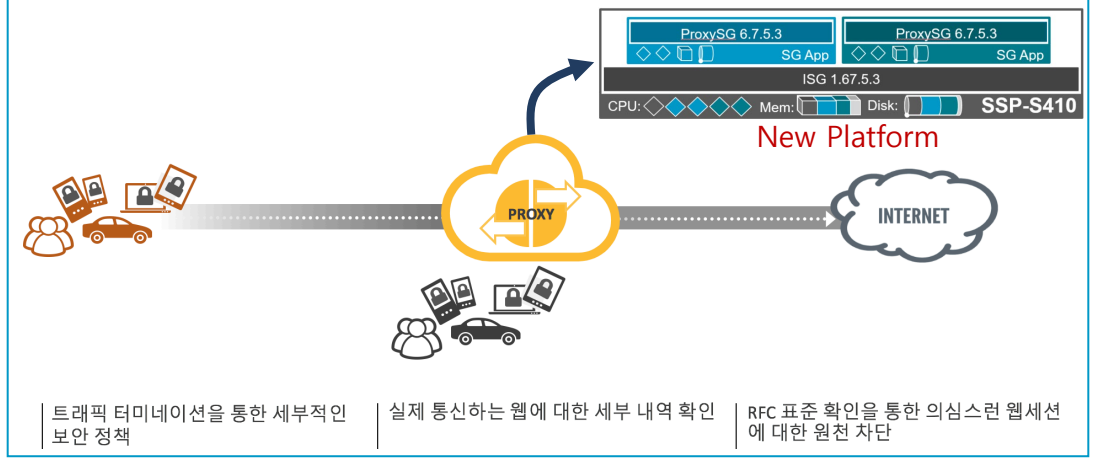
Host OS 기반의 High Performance 전용 플랫폼

- 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

감사합니다

BROADCOM SOFTWARE