엔드포인트 통합 보안 패키지 – SES (Symantec Endpoint Security)

최신 보안 위협으로부터 모든 유형의 단말을 보호하기 위한 엔드포인트 보안 통합 솔루션

- Symantec Endpoint Security는 사이버 공격의 주요 대상이 되는 다양한 엔드포인트 디바이스(데스크탑, 모바일, 서버, 클라우드 워크로드)를 보호하고, 단말의 보안을 강화하며, 악성코드 탐지, 위협에 대한 대응을 할 수 있도록 하는 토탈 보안 솔루션 패키지 입니다.

비즈니스 요구사항

- 고도화 된 위협을 방어하기 위해 여러 보안 제품들과의 협업 필요
- 여러 종류의 에이전트를 배포하고 관리하기 위한 업무 복잡성
- 보안 강화를 목적으로 도입된 여러 보안 솔루션들을 운영하기 위한 인력 부족
- 이러한 기업들의 노력에도 불구하고, 여러 보안 제품들 간의 연동 문제는 완전히 해결되지 못함 (설정 및 정책 오류, 보안 Gap, 운영 리스크 등)

시만텍 솔루션

	SEP	SES ENTERPRISE	SES COMPLETE
ATTACK PREVENTION			
INDUSTRYBEST ATTACK PREVENTION	✓	✓	✓
MOBILE THREAT DEFENSE		✓	✓
SECURE NETWORK CONNECTION		✓	✓
ATTACK SURFACE REDUCTION			
BREACH ASSESSMENT			✓
APPLICATION CONTROL			✓
DEVICE CONTROL	✓	✓	✓
BREACH PREVENTION			
INTRUSION PREVENTION	✓	✓	✓
FIREWALL	✓	✓	✓
DECEPTION	✓	✓	✓

	SEP	SES ENTERPRISE	SES COMPLETE
BREACH PREVENTION			
ACTIVE DIRECTORY SECURITY			✓
RESPONSE AND REMEDIATION			
ENDPOINT DETECTION AND RESPONSE			✓
TARGETED ATTACK CLOUD ANALYTICS			✓
BEHAVIORAL FORENSICS			✓
THREAT HUNTER			✓
THREAT INTELLIGENCE			✓
RAPID RESPONSE			✓
IT OPERATIONS			
DISCOVER & DEPLOY	✓	✓	✓
HOST INTEGRITY CHECKS	✓	✓	✓

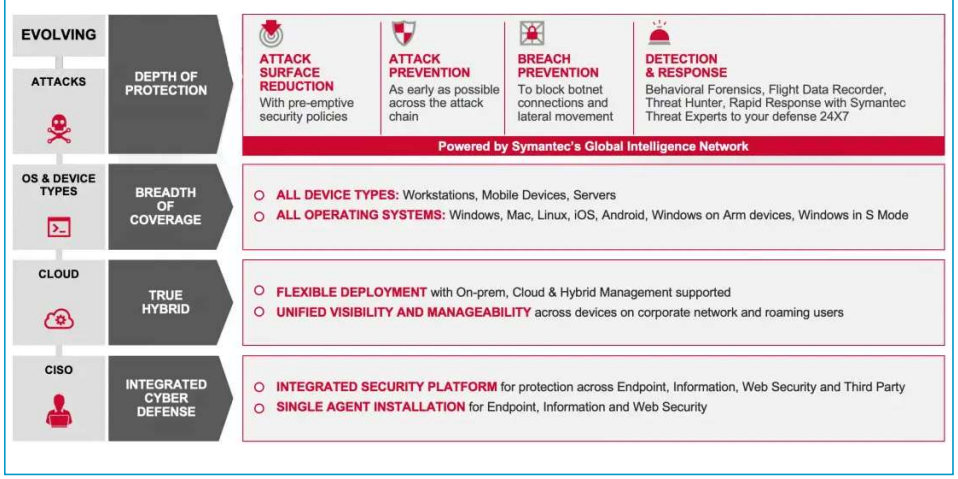
도입 기대 효과

- 단일 솔루션 패키지를 통한 기업 보안 경쟁력 극대화 및 관리 리소스 감소
- 여러 보안 솔루션들을 통합하기 위한 노력 최소화
- 사용자 단말 뿐만 아니라 서버, Active Directory 등 모든 유형의 자산 보호

시만텍 솔루션의 차별화 요소

- 모든 유형의 엔드포인트 보안 제공
- 단일 에이전트를 통한 엔드포인트 보안 & EDR 기능 제공
- 실시간 위협 가시성 확보를 위한 단일 콘솔
- 유연한 배포 방식(On-premise, 클라우드, 하이브리드)

솔루션 아키텍처



BROADCOM SOFTWARE

✓ On-premise
✓ Part of SES

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

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

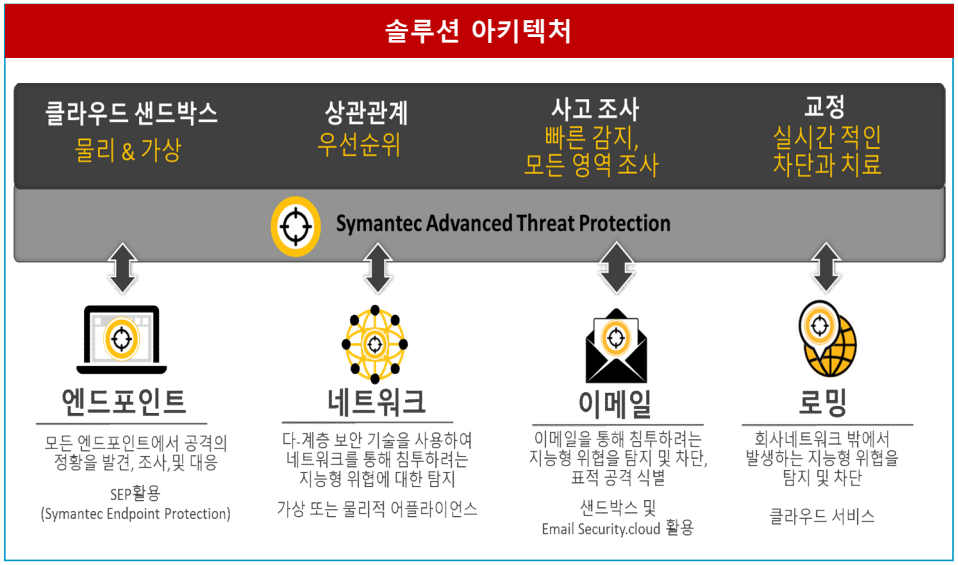
- SEP와 통합된 EDR솔루션으로 성능 저하 없이 엔드포인트 상의 위협 제거
- 인시던트 관리: 공격을 가시적으로 표현하여 공격을 직관적으로 이해 및 즉시 조치
- 우선순위 제공: 조치가 필요한 중요 인시던트를 먼저 표시하여 관리자가 피해를 최소화 하여 빠른 시간에 조치가 가능하게 함
- 통합 ATP 솔루션
  - ATP Endpoint(EDR): SEP클라이언트를 이용하여 엔드포인트 내의 의심스러운 악성코드를 판별, IOC 검색 , 조치 지원 (EDR기술)
  - ATP Email: Email Security.cloud 연동 모듈로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

✓ Part of SES-C

Active Directory 보안 – TDAD (Threat Defense for AD)

공격자의 내부 침투 후 확산을 위해 활용되는 AD 리소스 조회 및 공격 탐지를 위한 AD 보안 솔루션

- 대부분의 기업에서 내부 리소스(서버, 단말, 어플리케이션, 사용자 등)를 관리하기 위해 Microsoft 사의 Active Directory를 사용하고 있습니다. AD는 도메인에 연결된 모든 사용자에게 Open 되어있고, 이 것은 사용자에게 기업 내부의 Identity나 리소스 들이 노출될 수 있음을 의미합니다. 따라서, 많은 공격자들이 공격의 첫번째 목표로 AD를 지목하고 있습니다.

비즈니스 요구사항

- 도메인에 Join 된 Compromised User에 의해 내부 리소스 정보 노출
- 대부분의 공격자들은 AD를 Target 하여 공격을 시도함
- 지속적인 AD Assessment로 Attack Surface 노출 최소화

시만텍 솔루션

- SES Complete에 포함되어 APT 공격에 대한 강력한 방어 기능 수행
- Obfuscation(정보 교란)을 통한 AD 공격 무효화
- 잘못 설정된 AD configuration에 대한 지속적인 평가
- GPO, endpoints, domain controllers, Kerberos 등 모든 AD 구성 요소에 대한 Misconfiguration & backdoor 리스크 평가

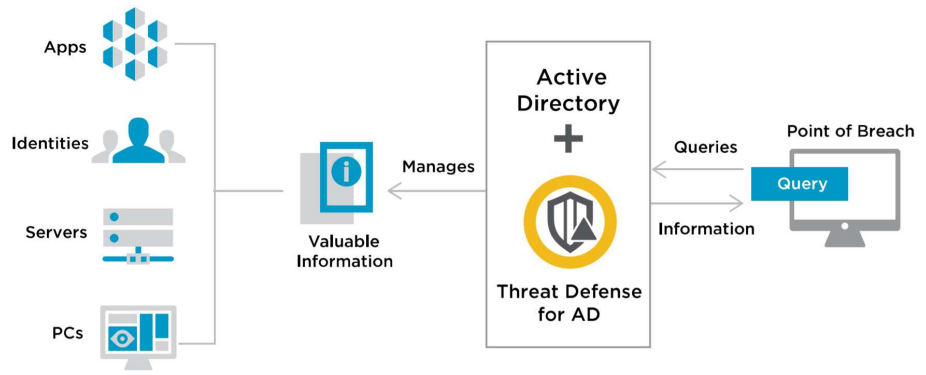
도입 기대 효과

- Compromised 된 User의 위협으로부터 내부 리소스 보호
- AD defense를 통한 AD Hardening

시만텍 솔루션의 차별화 요소

- SES complete 패키지를 통해 단일 Agent로 All-in-one 보안 기능 제공
- Attack simulation을 통한 자동화 된 Self assessment

솔루션 아키텍처



BROADCOM SOFTWARE