

SEP (Symantec Endpoint Protection) 엔드포인트 통합보안 솔루션

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 타겟공격 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 보장
- 방화벽: 업계 최고의 Endpoint 방화벽 기술 적용
- 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 SW설치 등 내부 보안정책 강제화 통제
- 랜섬웨어를 차단 위한 새로운 엔진 : 첨단 머신 러닝, 애플레이터, 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

