Deep Discovery

ZERO DAY INITIATIVE,NSS LABS에서 인정한 APT 대응 솔루션

지능형 지속위협(APT) 공격의 가장 핵심인 메일기반의 스피어 피싱을 포함해
실시간으로 변경되는 명령제어(C&C)서버와 악성URL에 대한 대응이 가능한 솔루션

제조사 : ㈜트렌드마이크로

30페이지를 참고해주세요!

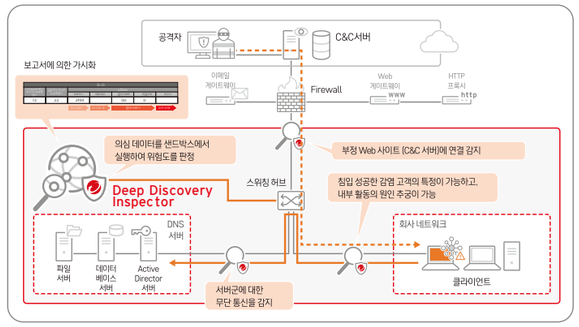
DEEP DISCOVERY와 **국내 1위 TST 기반 고성능 SSL 복호화 솔루션** ePrismSSL을 결합하면 **암호화된 악성코드 위협을 완벽하게 대응**할 수 있습니다.

Deep Discovery Inspector

Network APT 탐지

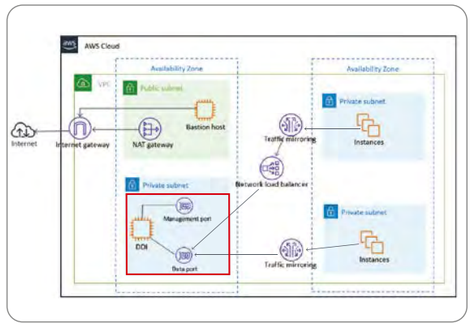
표적형 공격과 제로 데이 공격을 네트워크의 행동에서 찾아 조기에 대처하고 심각한 피해를 사전에 방어하기 위한 제품.
불법적인 파일 및 통신을 탐지하는 것 외에도 공격 초기 단계부터 내부 확산 및 외부와의 통신까지 다양한 공격 단계에서 관리 도구를 악용하는 공격을 발견함.

On-Prem구성



인터넷/내부트래픽검사 (업계최다 100+프로코콜/내부전파탐지)

AWS구성



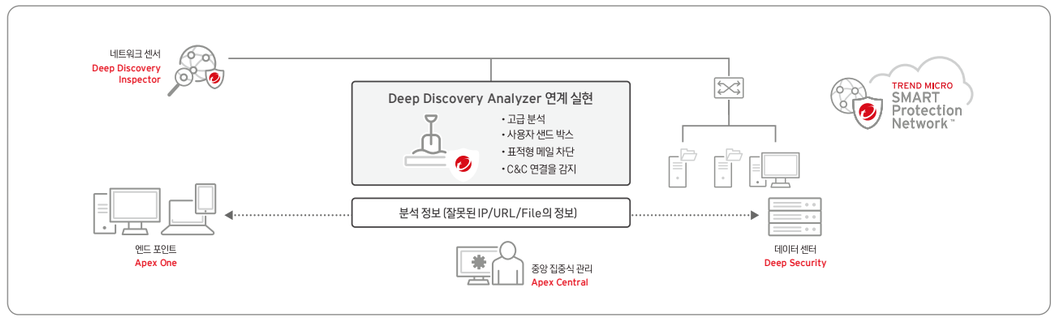
클라우드 VPC 트래픽검사 (다양한 VPC 구성 지원)

Deep Discovery Analyzer

Network APT 분석

Deep Discovery Analyzer는 Trend Micro의 웹, 이메일, 엔드포인트 및 서버 보호 제품과 함께 샌드박스 분석 기능 추가 가능.
표적형 공격, 제로 데이 공격 및 신,변종 랜섬웨어 공격에 대한 대응책으로 운영 환경의 큰 변경 없이도 Trend Micro 제품을 통해 보안을 강화할 수 있음. Deep Discovery Analyzer는 분석 기능 외에도 다른 Trend Micro 제품에 사용할 수 있는 시그니처를 자동으로 생성 및 공유. 수동 분석 기능이 있어 고객이 직접 수집한 위협의심 정보를 분석하는데 사용이 가능

시스템 구성도



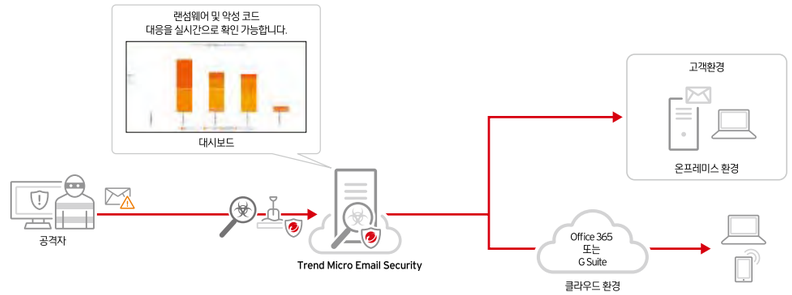
Email Security

이메일 및 파일 공유 위협에 대한 보안 솔루션

표적형 메일 공격과 기업이나 조직을 노리는 공격이 고도화·다양화되고 있으며 새로운 위협에 대응할 수 있는 솔루션이 필요함에 따라 기존의 '이메일 바이러스·스팸 메일 대응'에서 '표적형 메일 공격 대응'에 클라우드 이메일 보안이 가능한 솔루션

제조사 : ㈜트렌드마이크로

구성도



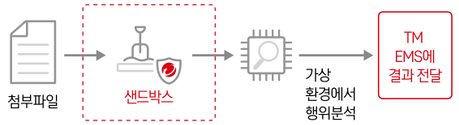
특장점 및 기능

고급 표적형 메일 공격에 의한 침입을 방지

- APT 공격에 최초로 이용되는 표적형 메일 공격에 대해 "클라우드 샌드 박스"를 사용한 동적 분석을 통해 알려지지 않은 위협 탐지
- 본문, 첨부문서 내의 악성 프로그램을 다운로드할 위험성이 있는 의심 URL차단
- 유연한 설정이 가능하며 관리가 쉬운 스팸 메일 대책
- 판정이 어려운 스팸 방어 뿐만 아니라 오탐이 적고 다층 검사를 실시하여 최종 사용자가 격리 정책에 대한 유연성 제공
- Office365, Google Workspace(G Suite) 환경 지원

클라우드 샌드박스

- 트렌드마이크로 "클라우드 샌드박스"는 소프트웨어 등의 실행 환경을 클라우드에서 에뮬레이션 (가상 실행)하여 지금까지 감지 할 수 없었던 알려지지 않은 위협을 탐지·차단



비즈니스 이메일 사기(BEC) 대응

- 기업 내부 임직원 행세를 이용하는 BEC 대응
- 머신러닝기반 BEC 탐지

요약	상세기능
바이러스·스팸·피싱 메일차단	바이러스 검색 등 규칙을 조합 보내는 메일 수신 메일에 대한 보안 위험을 탐지/처리의 설정 가능
그레이(Gray)메일 대응	이메일 마케팅 등 기업의 정책에 의해 결정이 갈라지는 그레이 구간의 메일을 대응
고급 위협 검색	패턴기반의 검색 및 추론검색을 결합하여 표적형 메일공격에 사용되는 문서의 공격코드 및 기타위협을 감지하고 필요에 따라 클라우드 샌드박스에 전달
클라우드 샌드박스	ATSE에서 감지 의심스러운 이메일 첨부 파일과 URL을 필요에 따라 트렌드마이크로가 관리하는 클라우드 샌드박스에서 실행하고 행동을 분석할 수 있는 동적 분석 기능을 제공하며 표적형 메일 공격에 대한 대응을 보다 고도화 할 수 있음
소셜 엔지니어링 공격대책	소셜엔지니어링 공격 방지를 실행하면 스팸 검색엔진에 의해 메일이 송수신 될 때마다 메일 각 부분(메일 헤더, 제목, 본문, 첨부 파일 및 SMTP 프로토콜 정보 등)에서 의심스러운 활동이 검색됨
콘텐츠 필터링	사전에 설정된 규칙이 준비되어 있으며, 키워드, 용어, 첨부파일의 특성 및 기타 필터 규칙에 따라 이메일 메시지와 첨부파일을 필터링 할 수 있음. 관리자는 기본 규칙 수정 및 새 규칙 생성이 가능
최종 사용자 격리	최종 사용자 격리 콘솔을 이용하여 각 최종 사용자는 격리된 스팸 메일 처리(재전송/삭제) 및 개별 승인 된 발신자 목록에 추가 실시 가능