N1000 네트워크 보안 어플라이언스

전자 메일, 웹 및 파일 전송에 대한 멀웨어 및 알려지지 않은 위협 가시성 제공

N1000은 이메일, 웹 및 파일 전송 등 네트워크 트래픽 내 파일을 포괄적으로 검사하고 분류합니다. 거의 실시간으로 파일에 대한 정보를 추출 및 저장하고, 알려지지 않거나 악성인 전송 데이터 분석을 통해 침해 대응속도를 가속화할 뿐만 아니라, 네트워크 콘텍스트로부터 가시성을 제공합니다. 또한 신규 위협 인텔리전스를 기반으로 새로운 위협을 식별할 수 있는 사용자 지정 탐지 규칙을 정의 및 디플로이하여 피해가 발생하기 전에 멀웨어 공격에 대한 선제 대응이 가능합니다.

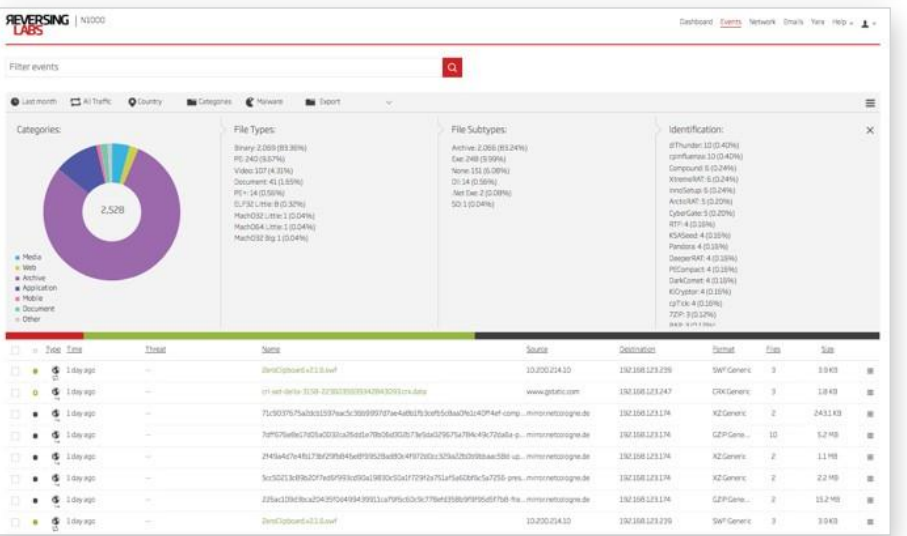
주요 장점

- **탁월한 규모와 커버리지** - 밀리세컨드 단위 속도의 빠른 파일분석
- **알려지지 않은 위협에 대한 가시성 제공** - HTTP, SMTP 및 FTP 트래픽의 파일 확인을 통한 가시성 확보
- **3,500개 이상의 파일형식 식별** - 파일이 실행되기 전에 "in flight"으로 분류
- **"레트로 탐지" 가능** - 기존 파일 현황에 대한 지속적인 모니터링 및 상태 변경 시 알람 제공
- **YARA 규칙을 통한 헌팅** - 리버싱랩스 제공 및 사용지 지정의 YARA 규칙을 통한 멀웨어 헌팅
- **SIEM 및 분석 플랫폼과 연동** - 다양한 파일 분석과 리포트 제공
- **대용량 및 심층 분석에 대한 확장성** - 대용량 분석을 위한 TitaniumScale, 멀웨어의 심층적인 분석 및 헌팅을 위한 A1000 및 온-프레미스를 위한 파일 평판 어플라이언스 T1000 제공

N1000은 ReversingLabs의 고유한 파일 디콤포지션 기술을 활용해 내부 상세 인디케이터를 도출합니다. 파일 디콤포지션은 샌드박스 제품보다 훨씬 빠른 속도로 심층적인 파일 검사를 수행하여 N1000이 네트워크 스트림에서 모든 주요 파일형식을 실시간으로 추출 및 분류할 수 있도록 합니다. 파일 분류는 업계 최고의 파일 평판 서비스의 최신 인텔리전스 및 강력한 규칙 엔진을 함께 활용해 위협 수준, 이름 및 형식을 할당합니다. 통합 GUI, 고객 SIEM, Splunk, Elasticsearch 등의 다양한 분석 플랫폼을 통해 결과에 대한 추가 작업을 수행할 수 있습니다.

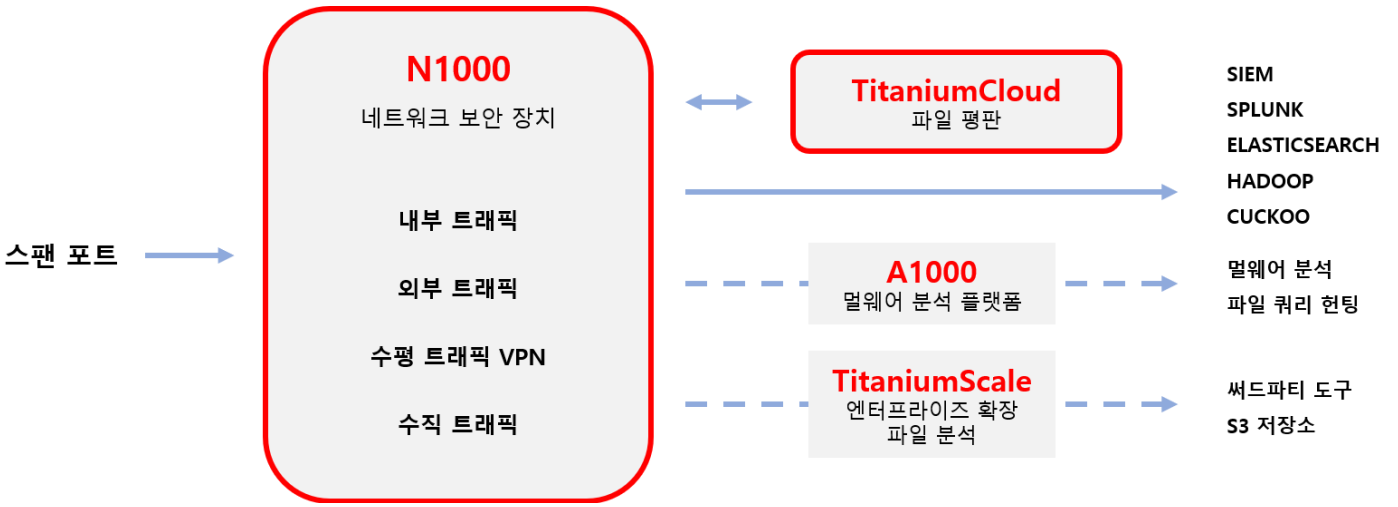
N1000 네트워크 위협 가시화

N1000을 통해 파일 이벤트 확인, 파일 요약 및 세부 정보 액세스, 파일 네트워크 콘텍스트(예: 송신지, 수신지) 확인, 파일 속성 별 검색 및 사용자 지정 YARA 규칙으로 위협 탐지를 커스터마이제이션 할 수 있습니다.



N1000
네트워크 위협 탐지, 분류 및 헌팅

N1000은 네트워크 트래픽의 파일을 실시간으로 분류하고 분석합니다. TitaniumScale을 추가하면 보다 높은 처리량의 애플리케이션에 대해서도 N1000의 환경설정을 할 수 있습니다. N1000에서 전달되는 관심대상의 파일정보는 SIEM 및 분석 플랫폼에서 보고서를 생성하거나 심층적인 분석을 위한 A1000 멀웨어 분석 플랫폼에서 사용됩니다.



N1000 주요 기능

네트워크 파일 평판 및 분석

- SPAN 포트에 연결하여 네트워크를 통과하는 모든 파일 모니터링
- HTTP, FTP 및 SMTP 트래픽의 실시간 파일 분석
- 최대 400MB의 파일 처리(기본값)
- 커버리지 및 볼륨면에서 모두 샌드박스 파일 처리 능력 초월

추출된 파일의 위협 분류

- 고유한 파일 디콤포지션 기술로 실시간 액세스 및 파일분류 가능
- Windows, Linux, Mac OS, Android, iOS, 문서 및 미디어 파일을 비롯한 플랫폼 전반에서 350개 이상의 파일형식 검사
- 송신지, 수신지 또는 또는 파일형식 별 파일 활동 리포팅
- TitaniumCloud 파일 평판 서비스의 화이트리스트 및 블랙리스트 콘텐츠 확인

서비스 배포 형태

- 가상머신 또는 하드웨어 기반

제로데이 / 어드밴스드 위협 식별

- 알려진 멀웨어의 기능적 유사성 식별을 통한 다변형 공격 인식
- 위협 수치화를 위해 모든 파일에 사용자 지정 YARA 규칙 적용

엔터프라이즈 데이터 통합

- 파일 분석 로그 및 위협 탐지를 SIEM 및 빅데이터 솔루션과 연동
- TitaniumScale 및 T1000을 통해 관심대상의 파일 저장
- 모니터링, 환경설정 및 리포팅을 위한 웹 GUI 포함

ReversingLabs 솔루션 연동

- 대용량 애플리케이션을 위한 TitaniumScale 연동
- 심층적인 분석 및 헌팅을 위해, A1000 멀웨어 분석 플랫폼에 인풋 제공
- 개인정보보호 및 망분리 환경을 위한 T1000 파일 평판 어플라이언스 연결

REVERSINGLABS

Korea Sales: 02.538.9225
briankim@reversinglabs.co.kr