Entobil Soft.

NetExtractor Platform

Entobil Soft.

파일 송·수신 가시성 제공 플랫폼

NetExtractor

NetExtractor 파일 송·수신 가시성 제공 플랫폼 개요

파일 송·수신에 대한 가시성 제공

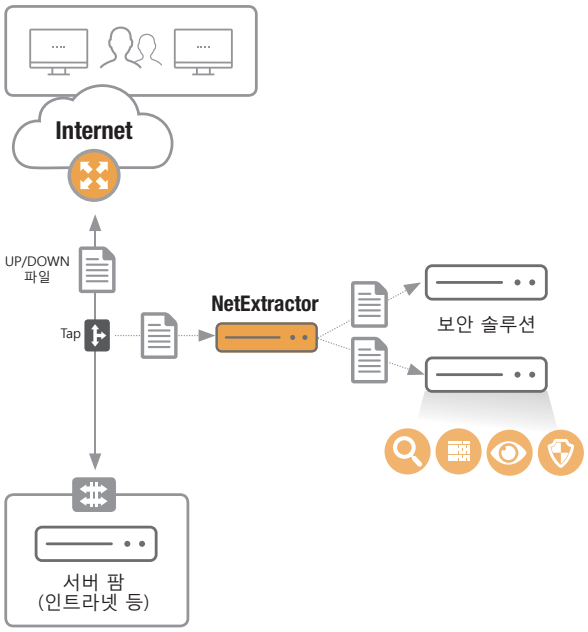
- 네트워크 기반의 간단한 설치 및 구성 (Tap/Mirror 방식)
- 최대 20Gbps 트래픽 처리
- HTTP/FTP/SMTP/POP/IMAP/SMB 프로토콜 지원
- 파일 송·수신에 대한 중복 제거를 통한 분석 효율성 제공
- 사건, 사고 발생 시, 파일 및 이메일 송·수신자 추적 관리
- 3rd 보안 솔루션 연계를 통한 보안성 향상
- 블랙/화이트 리스트 기반의 예외 처리 (UP/URI) 설정 제공

모니터링 및 리포트

- 프로토콜별 파일 송·수신 통계 정보
- 문서 유형별 송·수신 통계 정보
- 악성 파일 통계 및 Top 10 정보
- 파일 송·수신에 대한 로그 정보 관리 등

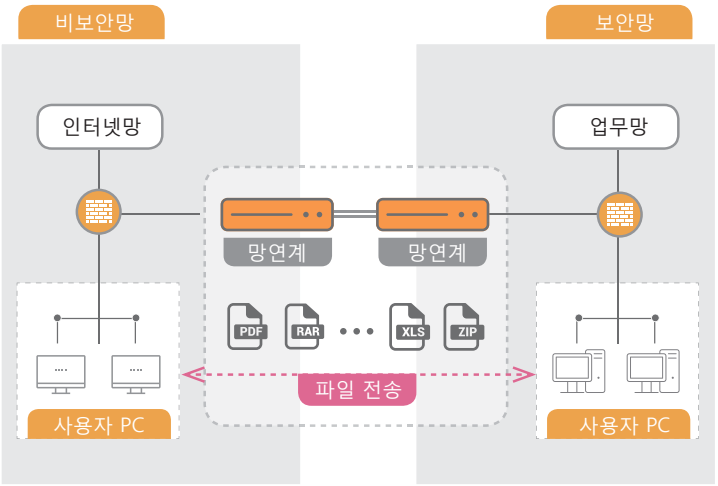
- 최대 10Gbps 성능 처리
  (HTTP/FTP/SMTP/POP3 프로토콜 기반)
- RAM 디스크 처리
- 파일 확장자, 크기 등 선택적 추출
- 중복 제거 기술
- 3rd 보안 솔루션 연동
  (APT/방화벽/IDS 등)
- 파일 전송 프로토콜 커스터마이징 지원
- 사용자 파일 접근 로그 생성

보안 솔루션 연동 방식



제안사례

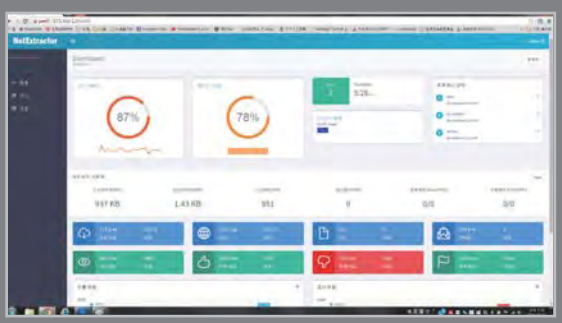
· 외부/내부망 간의 파일 송·수신 가시성 확보
· Tap 또는 Mirror 방식에 의한 파일 추출
  - 파일 공유 시스템의 직접적인 접근 권한 부여 불필요
· 보안사고 발생 시 파일 송·수신자 추적 용이

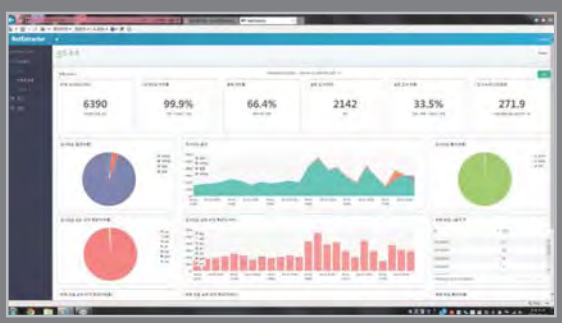


파일 추출 현황 및 로그 정보

추출된 파일을 저장 공간에 저장하면 생성
[로그 형식]
<time> <file-hash> <src-ip:port> <dst-ip:port> <file-type> <extension-type> <file-size> <origin-filename> <uri> <write-filename>
2014/10/26-17:35:19 8d026d6ae5587fd949c5286a0276900a 172.30.0.51:57247 61.247.193.201:80 7 0 5624568 “picpick_inst_kr.exe”

항목	내용	형식	예
time	저장 시간	yyyy/MM/dd-hh:mm:ss	2014/10/26-15:59:46
file-hash	파일 해시		8d026d6ae5587fd949c5286a0276900a
src-ip:port	근원지 IP 주소:포트 번호	ip-addr:port	172.30.0.51:57247
dst-ip:port	목적지 IP 주소:포트 번호	ip-addr:port	61.247.193.201:80
file-type	파일 추출 타입	0-7	7
extension-type	확장자 타입	0-2	0
file-size	파일 크기		5624568
origin-filename	Http 헤더에서 추출한 파일명		"picpick_inst_kr.exe"
uri	파일을 추출한 URI		"http://up.cafe.naver.com/AttachFile.nhn"
write-filename	NE 에서 저장한 파일명		"/mnt/log/net_extractor/http_knowns/20141026_083517_00000003_picpick_inst_kr.exe"





도입에 따른 기대효과

악성 코드 및 유해 파일 UP/DOWNLOAD 차단

내부 정보 유출 차단

파일 전송 모니터링 분석 및 관리

파일 송·수신에 대한 보안성 강화

제품 라인 업