전문 트래픽 분석·제어 및 가시성 제공 플랫폼/엔토빌소프트 솔루션

EntobilSoft

Internet Traffic Visibility,
Analysis, Protection
& Management

Entobil Soft.

https://www.entobilsoft.com

Entobil Soft.

Table of Contents

4 / About EntobilSoft

Organization ㈜엔토빌소프트 조직도
History ㈜엔토빌소프트 연혁
Products Overview ㈜엔토빌소프트 제품군

8 / NetShield Platform

고성능 통합 전문 차단 플랫폼 NetShield

12 / NetExtractor Platform

파일 송·수신 가시성 제공 플랫폼 NetExtractor

16 / NetCrypto Platform

SSL/TLS 암호화 가시성 제공 플랫폼 NetCrypto

20 / NetFreezer Platform

실시간 전체 패킷 수집, 추출, 분석 및 관리
플랫폼 NetFreezer

Internet Traffic Visibility, Analysis, Protection & Management

전문 트래픽 분석·제어 및 가시성 제공 플랫폼/엔토빌소프트 솔루션

Entobil Soft.

About EntobilSoft

Internet Traffic Visibility, Analysis, Protection & Management

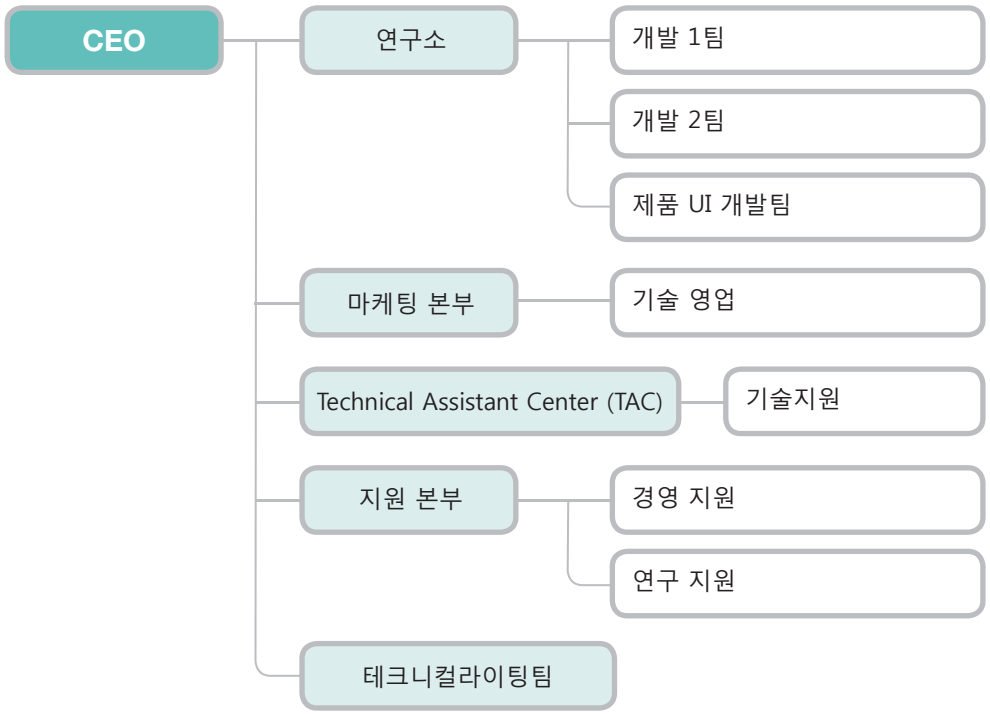
전문 트래픽 분석·제어 및 가시성 제공 플랫폼/ 엔토빌소프트 솔루션

㈜엔토빌소프트는 축적된 경험과 자체 연구 개발을 통해 통신 사업자급의 고성능 트래픽 분석 엔진을 탑재한 독자 플랫폼을 개발하였습니다.

이를 통해 우리는 보다 향상되고 특화된 트래픽 분석, 제어 및 차단 솔루션을 기업 및 서비스 사업자에게 제공합니다.

이제 ㈜엔토빌소프트의 플랫폼을 통해 차별화된 보안 정책을 수립하고, 안정되고 신뢰성 높은 보안 인프라를 구축해 보십시오.

Organization



Entobil Soft.

About EntobilSoft

History

2017	01	뉴엔네트웍스와 국내 총판 계약 체결
2016	12	국내 발전소에 NetCrypto 공급
	02	KT에 NetShield 공급
2015	11	대전정부통합전산센터에 NetFreezer 공급
	04	APT 전문솔루션기업 Fire-Eye 사와 기술 파트너쉽 체결
	03	악성코드 전문솔루션기업 ㈜엔피코어사와 기술 MOU 체결
	02	NetShield 출시 (전문 차단 플랫폼)
2014	12	NetProxy 출시 (Https Proxy 솔루션)
	11	NetSide 출시 (BitTorrent 트래픽 제어 솔루션)
	10	NetExtractor 출시 (네트워크 전송 파일 추출 솔루션)
	06	서울시에 NetShield 공급 (APT 대응시스템 구축 사업)
	05	SK Telecom과 P2P 트래픽 지역화 연구개발 계약
2013	12	SK Telecom과 Contents Router (지능형 CDN 솔루션) 계약
	10	삼성그룹사에 NetShield 공급 (10G 급 APT 대응 서비스)
2012	12	대전/서울 정부통합전산센터에 NetEDS 시스템 공급
	09	NetEDS 시스템 출시
	05	㈜엔토빌소프트 창립
2011	12	10G급 패킷분석시스템 출시 (대전/광주 정부통합전산센터 공급)

Products Overview

NetShield 고성능 전문 차단 플랫폼

· 최대 40Gbps 처리

· NetShield-ST (표준 TCP/IP v4/6 및 Full URI 기반의 전문 차단 플랫폼)

· NetShield-AT (APT 솔루션 연동 기반의 전문 차단 플랫폼)

NetExtractor 파일 송·수신 가시성 제공 플랫폼

· 최대 20Gbps 처리

· 기업 내 파일 송·수신에 대한 가시성 제공

· HTTP, E-mail (SMTP/POP/IMAP), FTP 파일 전송 기반 등

NetCrypto SSL/TLS 암호화 트래픽에 대한 가시성 제공 플랫폼

· Full Transparent 패킷 처리 구조

· 암복호화 정책, 화이트/블랙 리스트 정책 지원

· 자동 바이패스 기능 (비표준 암호화 트래픽 등 대응)

Entobil Soft.

NetShield Platform

Entobil Soft.

고성능 통합 전문 차단 플랫폼

NetShield

NetShield 전문 차단 플랫폼 개요

고성능 전문 차단 플랫폼

· Layer-7 DPI 엔진 기반으로 최대 40Gbps 트래픽 처리
· TCP/IPv4/6, HTTP Full URI 기반 정책 차단
  - 그룹별, 차단 정책별 우선순위 적용
  - 차단 정책별 차단 페이지 전송
  - 차단 정책 적용 기간 지원 등
· 3rd 보안 솔루션 연동
  - APT 솔루션별 차단 DB 별도 수집 및 차단 정책 적용
· HTTPS 트래픽 암/복호화 및 복제 (미러링) 지원 (별도 라이선스)
· 차단 DB IP/URI별 각 500만개 이상 지원
· 차단 정책 500만개 이상 지원
· NetShield-ST (표준 모델) 및 NetShield-AT
(APT 솔루션 연동) 모델 제공

모니터링 및 리포트

· 트래픽 (프로토콜 및 어플리케이션 등) IN/OUT BPS/PPS
통계 (5분/일/주/월/년간)
· 차단 통계 (3rd 보안 솔루션 통계 별도 제공)
  - 차단 대상별, 사용자별 차단 통계
  - 차단 로그 다운로드
· 상세 차단 정보 제공 및 검색 지원
· 차단 시점 이전의 과거 해당 사이트 접근 사용자 추출

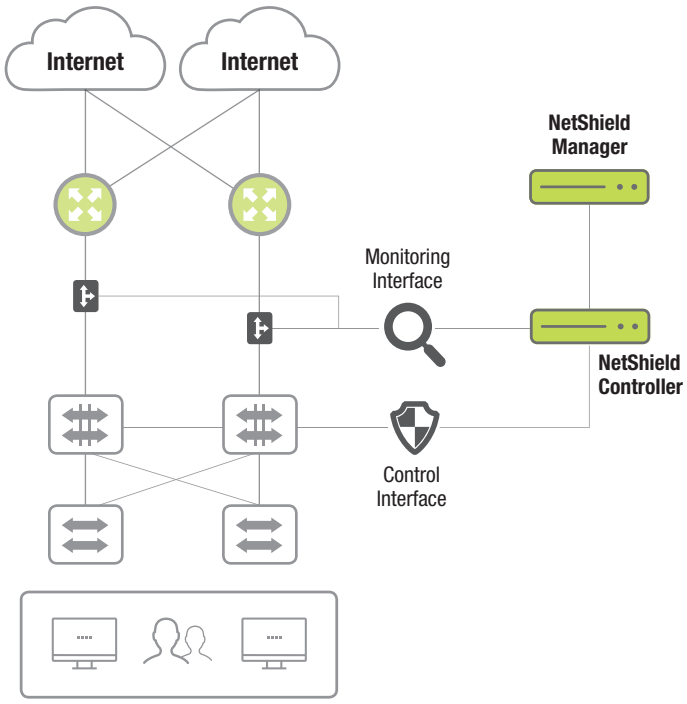
NetShield 플랫폼 구성

NetShield Manager
통합 관리 시스템
통계, 로그 및 시스템 설정 등

NetShield Controller
차단(제어) 시스템

Tap/Mirroring
스위치 미러링 또는
Fiber/Copper Tap

Interface
Monitoring: 1G/10GbE
Control: 1GbE (차단 신호 전송)



전문 차단 플랫폼의 필요성

견고한 차단 정책 수립
- TCP/IP, HTTP/HTTPS 프로토콜 지원
- 사용자 정의 기반의 정교한 차단 정책 제공
- 특정 악성 및 유해 사이트 자동/수동 차단 기능
- 목적지 국가별 선별적 차단 기능
- 안정적인 실시간 차단율 제공

통합 차단 플랫폼
- 기업 내 차단 기능의 단일화 (운영/관리 효율성)
- 다양한 3rd 보안 솔루션의 이벤트 정보 연계

보안 관제 플랫폼 연계
- 오탐 차단에 의한 서비스 장애 유발 방지
- 차단 DB 및 차단 정책 자동화 제어

도입에 따른 기대효과

APT 솔루션 연계를 통한 최적의 악성 트래픽 대응 체계 구축

실시간 악성 코드 배포 사이트 및 C&C 접속 차단 / 피싱, 파밍 및 유해 사이트 등 차단

APT 솔루션
보안 솔루션 (방화벽/IDS 등)
유해 사이트 URL DB 솔루션

· 악성 코드 및 C&C 접속 탐지 전송
· 비정상 행위 탐지 및 차단 DB 전송

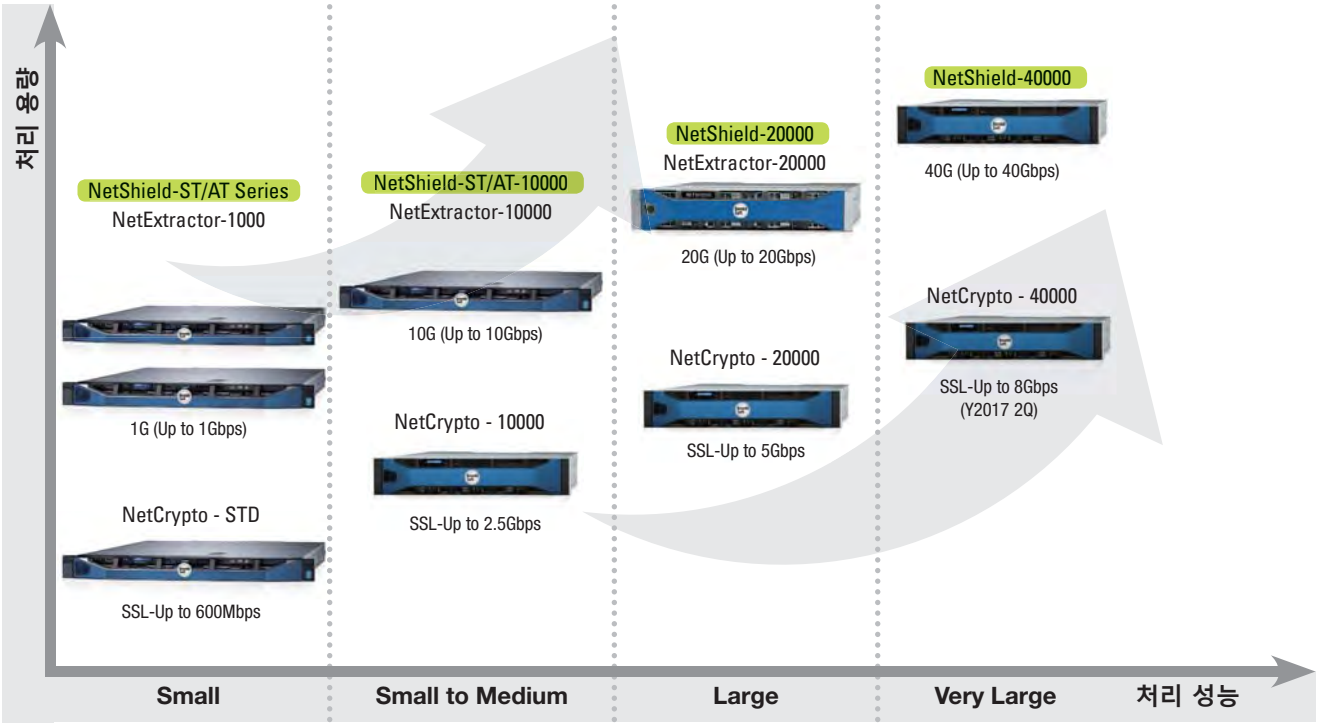
NetShield

· 악성 코드 배포 사이트 차단
· C&C 접속 차단
· 피싱 및 파밍 사이트 차단
· 유해 사이트 차단
· 비업무용 서비스 차단

기대 효과

· 투자 효율성 증가
· 효율적인 방어 시스템 구축
· 다양한 차단 정책 수립
· 기 사용 중인 보안 시스템 연계
· 보안 솔루션 간 상호 보완 효과

제품 라인 업



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

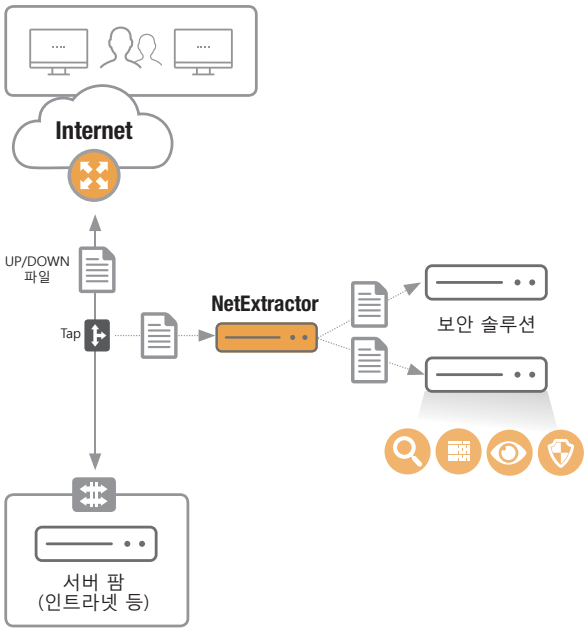
- 네트워크 기반의 간단한 설치 및 구성 (Tap/Mirror 방식)
- 최대 20Gbps 트래픽 처리
- HTTP/FTP/SMTP/POP/IMAP/SMB 프로토콜 지원
- 파일 송·수신에 대한 중복 제거를 통한 분석 효율성 제공
- 사건, 사고 발생 시, 파일 및 이메일 송·수신자 추적 관리
- 3rd 보안 솔루션 연계를 통한 보안성 향상
- 블랙/화이트 리스트 기반의 예외 처리 (UP/URI) 설정 제공

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

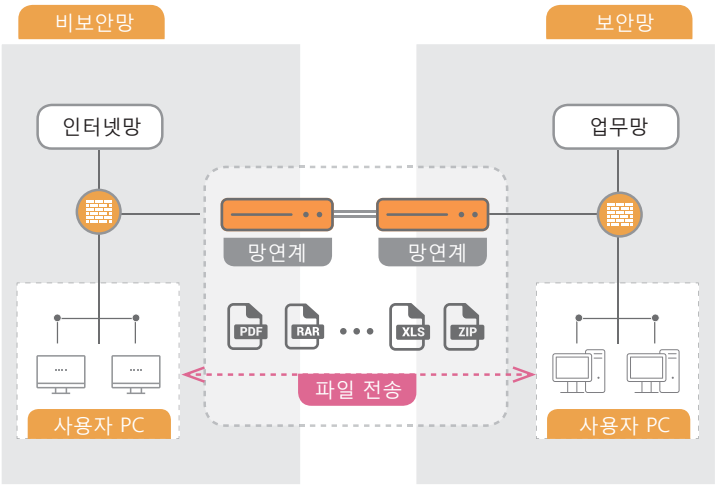
- 최대 10Gbps 성능 처리
  (HTTP/FTP/SMTP/POP3 프로토콜 기반)
- RAM 디스크 처리
- 파일 확장자, 크기 등 선택적 추출
- 중복 제거 기술
- 3rd 보안 솔루션 연동
  (APT/방화벽/IDS 등)
- 파일 전송 프로토콜 커스터마이징 지원
- 사용자 파일 접근 로그 생성

보안 솔루션 연동 방식



제안사례

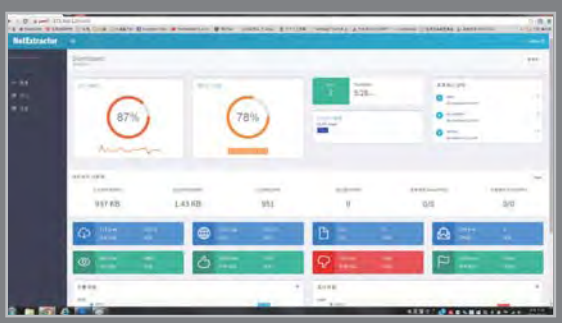
· 외부/내부망 간의 파일 송·수신 가시성 확보
· Tap 또는 Mirror 방식에 의한 파일 추출
  - 파일 공유 시스템의 직접적인 접근 권한 부여 불필요
· 보안사고 발생 시 파일 송·수신자 추적 용이

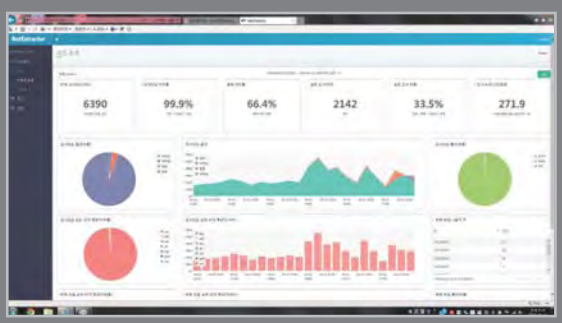


파일 추출 현황 및 로그 정보

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

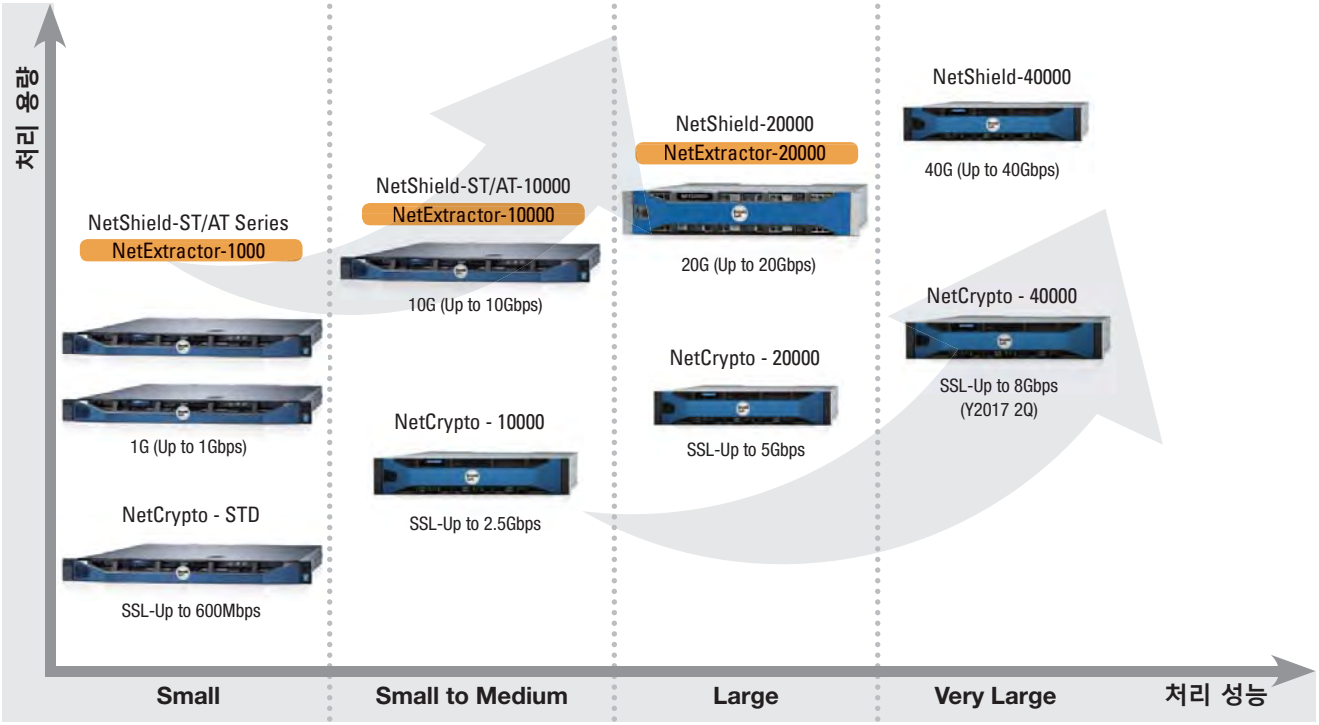
악성 코드 및 유해 파일 UP/DOWNLOAD 차단

내부 정보 유출 차단

파일 전송 모니터링 분석 및 관리

파일 송·수신에 대한 보안성 강화

제품 라인 업



Entobil Soft.

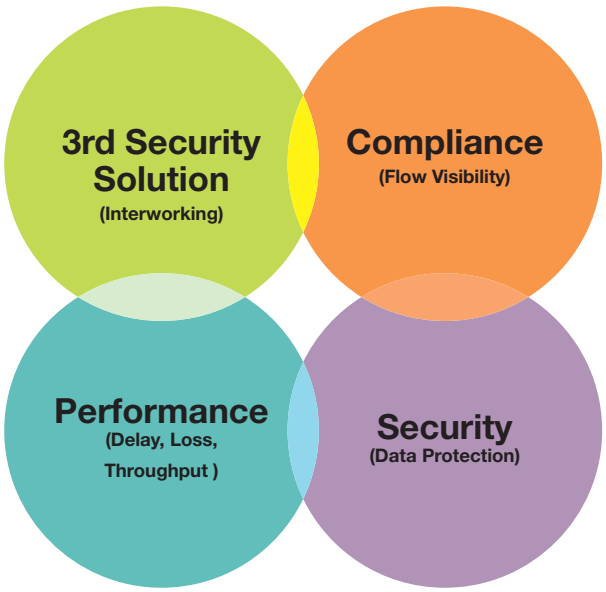
NetCrypto Platform

Entobil Soft.

SSL/TLS 암호화 가시성 제공 플랫폼

NetCrypto

NetCrypto SSL/TLS 가시성 제공 플랫폼 개요



Full Transparent 구조

- 네트워크 구성 변경 불필요
- End to End 세션 (5 Tuple) 투명성 보장
- SSL/TLS 트래픽 자동 인지
- In-Line/Mirror 모드 지원

SSL/TLS 암복호화 정책

- 정책 기반의 선별적 암·복호화 처리
- 비표준 또는 SSL/TLS 보안협상 오류 시, 자동 바이패스 지원
- 화이트/블랙 리스트 정책 지원
- POP3S/SMTPS/FTPS/HTTP2 등 다양한 암호화 프로토콜 지원
- Extended Master Secret Extension 대응
- 다양한 키 알고리즘 지원 (DHE/RSA8192)

3rd 보안 솔루션 연동 지원

- FW / IPS / APT 등 다양한 보안 솔루션 연동
- Active / Passive 디바이스 지원

다양한 바이패스 지원

- 하드웨어 / 소프트웨어
- 옵션 제어

고성능 처리

- 최대 20G 트래픽
- SSL 트래픽 5G 처리

Full Transparent 구조
(Reverse/Forward 모드, 암호화된 None-443 처리, 네트워크 구성 미변경)

다양한 보안 솔루션 연동
(IDS/IPS/FW/WAF/APT 등)

SSL 암복호화 정책 적용
(인증서 유효성 검증, 특정 사이트 예외 처리 등)

고성능 처리
(최대 20G 트래픽, SSL 트래픽 5G 처리)

모니터링 및 리포트

· IN/OUT 전체 트래픽 및 TLS, None-TLS 통계 (15분/일/주/년간/사용자 지정)
· SSL/TLS 세션 정보 제공 (송·수신자, 암호화 방식 등)
· 자동 바이패스 정보 및 포트별 처리량 통계 정보 제공

3rd 파티 연동 개요

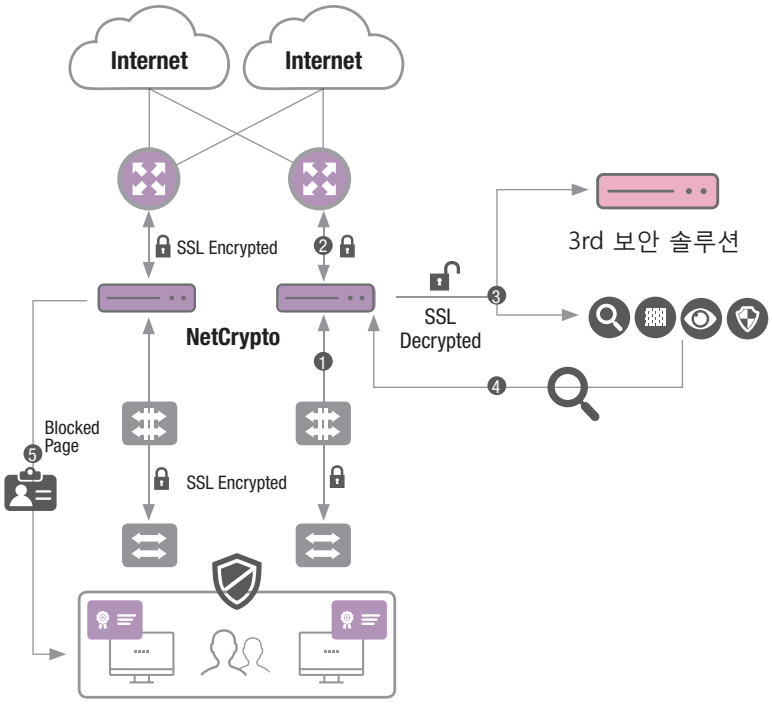
1. SSL 접속 시도 (2048/4096 bit key)

2. SSL Intercept 및 Session Key 정보 획득

3. SSL 트래픽 복호화 및 3rd 보안 솔루션으로 트래픽 복제

4. 트래픽 분석 및 탐지 결과 전송
· Syslog 메시지로 전송

5. 차단 DB 자동 생성 및 차단 시행
· 화이트/블랙 리스트 생성
· 차단 페이지 전송
· 차단 시점 이전의 해당 사이트로 접근 호스트 정보 추출



NetCrypto주요 기능

항 목	지원 여부	비고
Extended Master Secret Extension 대응	O	TLS 프로토콜의 Extended Master Secret 확장 옵션을 지원하여 보안 강화
ALPN(HTTP/2) 프로토콜 지원	O	TLS 프로토콜의 ALPN 확장 옵션을 지원하여 HTTP/2 프로토콜 암·복호화
443포트 외의 포트를 사용하는 SSL 트래픽 복호화 지원	O	SSL/TLS 트래픽을 자동으로 인지
HTTPS 프로토콜 외 암·복호화 지원	O	POP3s, SMTPs, FTPs 등 지원 가능
다양한 Bypass 기능 지원	O	H/W, S/W, Option
선별적 복호화 설정 기능 지원	O	White / Black List 기반 대상 사용자 / 서버
실시간 패킷 추출 기능	O	암호화, 복호화 트래픽 추출 가능
비표준 또는 자체 암호화 방식[응용프로그램]에 대한 Auto-Bypass 지원	O	특정 시간 임시 허용 가능
QUIC 차단 기능	O	크롬 브라우저의 UDP 암호화 전송 프로토콜
이중화 구성 시, 비대칭 트래픽 처리	O	패킷 포워딩 기능
자체 인증서 배포 지원	O	디지털 서명을 통한 안전한 배포 파일
URL 카테고리 DB 제공 (암·복호화 정책 적용)	O	기본 제공

주요 특장점

암복호화 처리 외

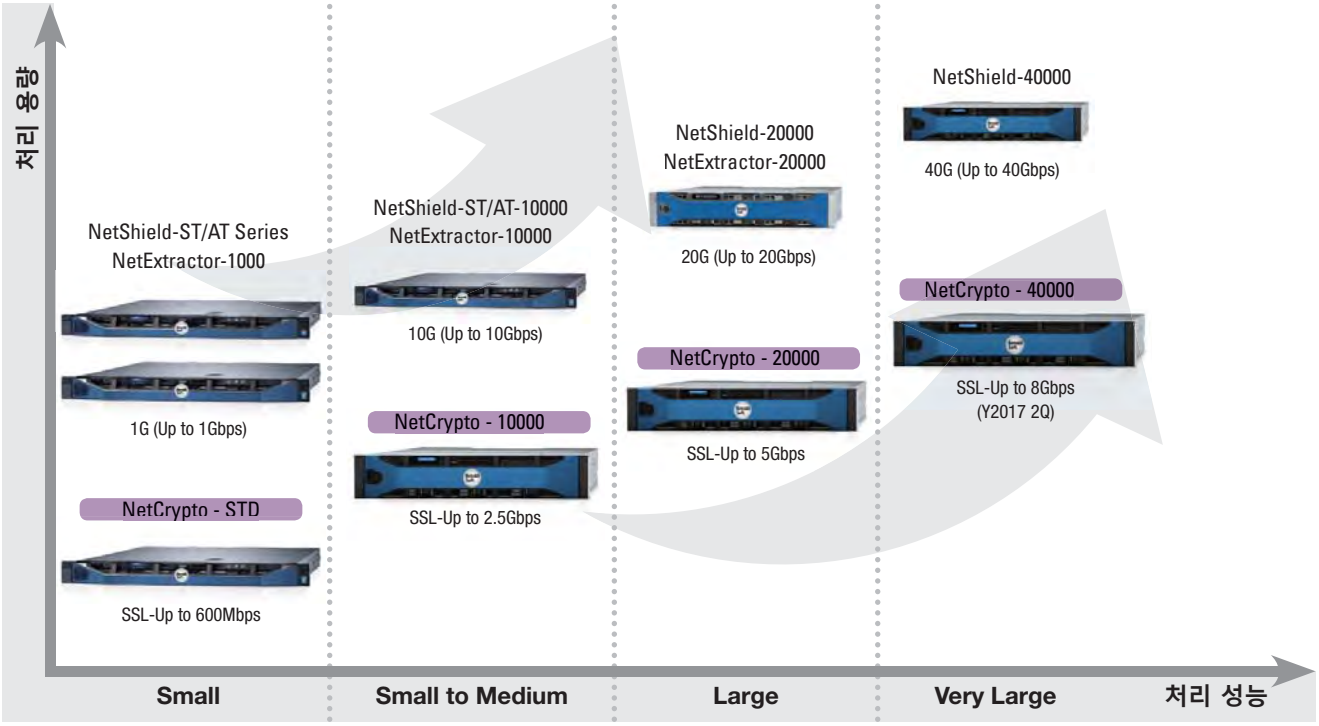
전문 차단 기능 제공
(정교한 차단 정책 수행 가능)

송·수신 파일 추출 기능 제공
(파일 보안성 강화)

Raw 패킷 저장/ 분석 등 제공
(침해 사고 분석 가능)

보안 솔루션 연동 시 유연한 커스터마이징 제공

제품 라인 업



Entobil Soft.

NetFreezer Platform

Entobil Soft.

실시간 전체 패킷 수집, 추출, 분석 및 관리 플랫폼

NetFreezer

Real-Time Traffic Analysis
- 1G/10G급 트래픽 양방향 패킷 수집, 저장 및 분석
- Connection, Protocol, IP, Port 상세 분석
- Top N, Bottom M 통계분석

Suspicion Monitoring
- 악성코드 발생 트래픽
- 내부 정보유출 정황
- 기타 유해 트래픽

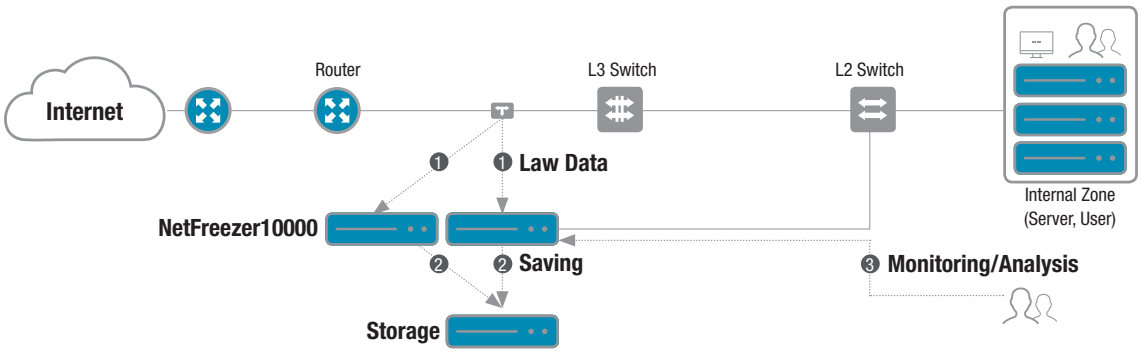
Logging & Analysis
- 전체 트래픽 전송 로그 저장
- 전체 패킷 단기저장
- 의심 패킷 단기 및 장기 저장
- HTTP, FTP, SMTP 등 프로토콜별 저장

NetFreezer 플랫폼 구성

NetFreezer 수집 시스템
- 패킷 수집, 추출, 관리 및 분석
- 저장 성능 7Gbps 보장 (최대 10Gbps 처리)
- Monitoring : 10GbE, Mgmt:1GbE
- 최대 20TB의 추출 결과 저장 공간 지원
- GUI

NetFreezer 저장 장치
- Storage (Option): DAS 방식, 최대 240TB 지원

이중화 구성
- 듀얼 포트 Tap으로 동시 저장

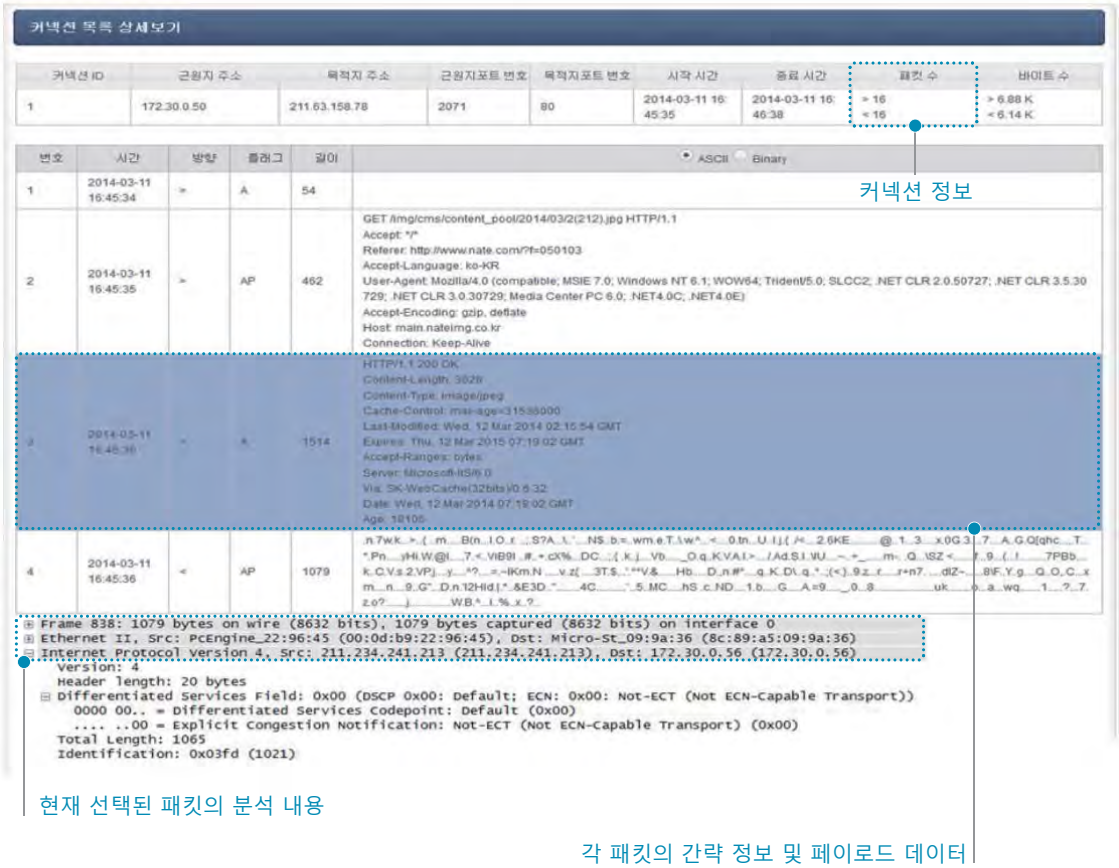


- 추출 결과 저장 공간 : NetFreezer에 추출 결과 파일을 저장하기 위해 할당된 공간, 20TB
- 전체 패킷 저장 공간 : NetFreezer Storage에 패킷을 저장하기 위해 할당된 공간, 192TB

실시간 패킷 분석 절차

단계	기능	설명
1단계	저장	· 전체 패킷 저장 공간[180TB]에 실시간 저장
2단계	1차 추출	· 다양한 검색 조건을 이용한 패킷 추출 · 추출 결과는 '추출 결과 저장 공간' (20TB)에 자동 보관 · 검색 조건: 기간, IP 주소, 포트 번호, 프로토콜, 최대 추출 파일 사이즈 · 추출 결과는 수십 MB ~ 수 GB 파일 사이즈 예상
3단계	커넥션 검색	· 1차 추출된 결과를 커넥션 단위로 조회 · 특정 시그너쳐를 포함한 커넥션 검색 기능을 이용하여 상세 분석 대상 커넥션 선택 · 시그너쳐 : PCRE 정규식, ASCII 문자열, 헥사 문자열 등
4단계	커넥션 분석	· 선택된 커넥션의 패킷을 상세하게 분석 · 페이로드 데이터를 ASCII 혹은 바이너리 형태로 표시 · Wireshark의 분석 기능 대응
5단계	pcap 파일 추출	· 상세한 커넥션 검색을 통해 선택된 커넥션만 pcap 파일로 추출해 저장 · 추출 결과는 수십KB ~ 수십MB 파일 사이즈 예상
6단계	PC로 다운로드 및 분석	· 저장된 pcap 파일을 다운로드 후 Wireshark 등을 통해 패킷 단위 분석

저장 패킷 추출 및 분석 화면



도입 및 기대 효과

· 실시간 전체 패킷 저장, 추출, 분석 및 모니터링 가능
· 보안 및 침해 사고 발생 시, 정밀한 세부 분석을 통한 빠른 사후 대처 가능
· 3rd 보안 솔루션 연계로 지능적이고 능동적인 대응 (APT 솔루션 등)

상세 스펙

구성 옵션	NetFreezer 수집 장치
CPU	Single Intel Xeon 60 Core 3.50GHz 25MB
RAM	96GB
HDD	4TB 7.2K RPM SATA HDD 3.5" * 8
Management Port	100/1000M Ethernet * 4
Capture Port	10GbE SFP+ * 4
RAID 컨트롤러	내부 컨트롤러 외부 컨트롤러 (6Gbps SAS * 2)
전원 공급 장치	듀얼, 핫플러그, 예비 전원 공급 장치 750W
Dim (WxDxH mm)	482.6 * 756.92 * 86.36
폼 팩터	Rack Type (2U size)
작동 온도	10℃~35℃
구성 옵션	**NetFreezer 저장 장치**
디스크	4TB 7.2K RPM SATA HDD 3.5” *60
디스크 확장	최대 4TB 3.5" * 180
RAID Controller Module	Two Hot-swappable Modules
모듈 인터페이스	SAS IN Port * 8
Management port	100/1000M Ethernet * 1
Dim (WxDxH mm)	482.6 * 825.5 * 177.8
폼 팩터	Rack Type (4U Size)
작동 온도	10℃~35℃

EntobilSoft

Internet Traffic Visibility, Analysis,
Protection & Management

Entobil
Soft.