Trellix

컴플라이언스 준수를 위한 Trellix DLP 활용 사례

㈜ 동훈아이텍

Sept 2022

Case#1. A 고객사 내부파일 외부 반출 시스템

고객사 요구사항

[기존 현황]

- 기존에 파일명 검사만 진행 후 외부 반출

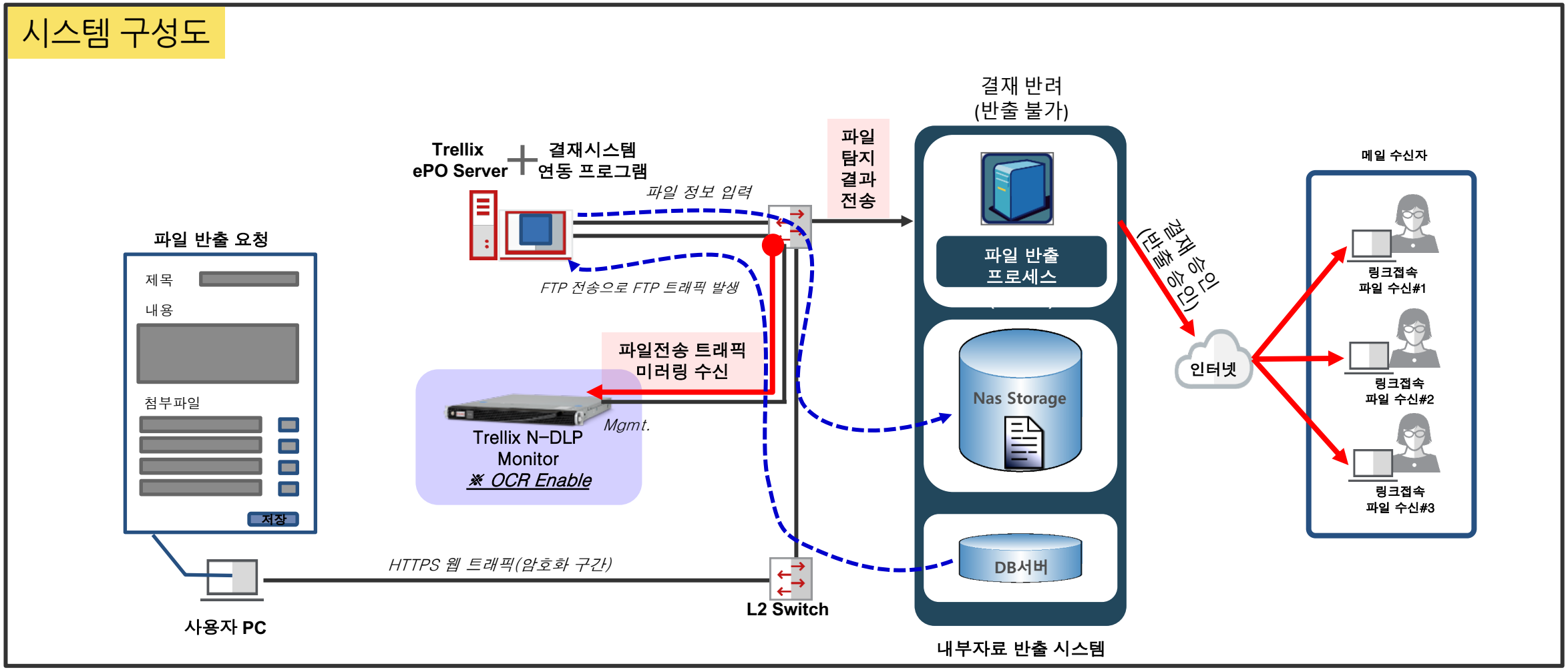
[개선요구사항]

- 장비에서 생성된 Log 파일(대용량) 검사 후 외부 반출
- 다수의 키워드(500개 이상) 탐지/차단 정책의 적용 필요성
- PDF 파일 외부 반출(이미지 타입의 텍스트는?)
- **외부반출 비 인가된 도면내용이 포함된 이미지 반출 차단(별도의 솔루션 없이)**
- **파일 외부 반출 승인 프로세스 연동(고객사 자체 반출 승인 프로세스)**

DONGHOON 동훈아이텍

Trellix

Case#1. A 고객사 내부파일 외부 반출 시스템



DONGHOON 동훈아이텍

Trellix

Case#1. A 고객사 내부파일 외부 반출 시스템

고객사 개선사항

- N-DLP 파일 검사를 통해 대용량 파일의 검사 속도 개선
  - 최대 2GB 파일의 검사 속도는 3분 내외
  - 최대 압축 100번의 파일검사는 1~2분내 검사 완료
- 약 400~600여개의 키워드 Policy 를 적용하여 파일 검사
- PDF, JPG 등의 이미지 파일에서 텍스트를 인지 하여 탐지 차단
  - 개인정보 및 도면의 일련번호 및 키워드에 대해서 이미지 탐지
- **※ OCR 기능 적용으로 이미지 파일에서 텍스트 인식기능 적용**
- **외부반출 요청 시 DLP 솔루션 탐지 결과를 외부반출시스템 DB에 업데이트**
  - **승인권자는 외부반출시스템에서 쉽게 DLP 탐지결과를 확인하여 승인/반려 조치**
- **파일 반출 시스템의 결재 연동으로 승인/반려 프로세스에 파일 탐지의 정확성과 업무에 소요되는 시간을 현저하게 절약**

DONGHOON 동훈아이텍

Trellix

Case#2. S 고객사 인터넷 개인정보 탐지 시스템

고객사 요구사항

[기존 현황]

- 웹프록시+NX를 활용하여 인터넷 악성코드 검사 활용

[개선요구사항]

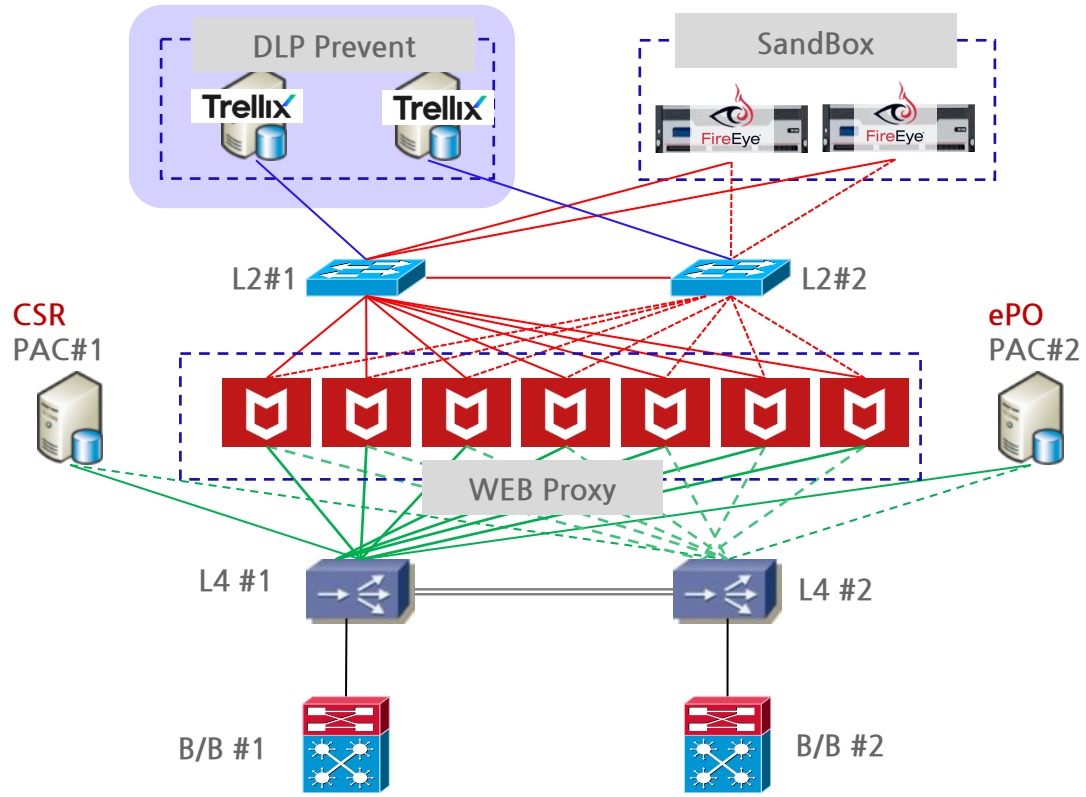
- **EndPoint DLP Agent를 적용하지 않고** 인터넷 사용시 개인정보 파일의 외부 전송을 **실시간 차단하는 방안**
- 그룹별 정책(허용 수량) 탐지/차단 차등적용
- **네트워크 구성의 변경 최소화**
- Incident 발생 시 SIEM 솔루션을 통한 즉시 확인

DONGHOON 동훈아이텍

Trellix

Case#2. S 고객사 인터넷 개인정보 탐지 시스템

시스템 구성도



개인정보 탐지

- PUT/POST 메소드 탐지
- ICAP 프로토콜 연동
- Decrypt 트래픽의 상세 검사
- 사용자/그룹 별 탐지 정책
- 탐지 뿐만 아닌 실시간 차단
- 기 사용중인 L2 스위치 연결구성

악성코드 탐지

- 다운로드 데이터 악성코드 검사
- ICAP 프로토콜 연동
- Decrypt 트래픽의 상세 검사
- 탐지 뿐만 아닌 웹프록시와 연계한 실시간 차단

DONGHOON 동훈아이텍
Trellix

Case#2. S 고객사 인터넷 개인정보 탐지 시스템

고객사 개선사항

- End-Point DLP Agent 미사용으로 사용자PC 부하를 최소화
- 실시간 차단을 위하여 기 사용중인 **웹프록시와 ICAP 프로토콜 연동**
- 임직원 인터넷 사용시 개인정보 뿐만 아니라 키워드를 적용한 내부 규정 준수
- 비밀번호로 압축된 파일의 경우 탐지 불가로 인한 차단 정책 사용
- **별도의 네트워크 구성 변경 없이 단순히 L2 스위치에 솔루션 연결만으로 구성 완료**
- 기존에 사용하던 임직원의 차단 페이지를 그대로 반영하여 업무의 혼선 최소화
- 사용자 인증정보를 연동하여 사용자/그룹별 정책 차등 적용
- **Fail-over 가능한 이중화 구성으로 안정적인 운영**
- 정책에 위반된 Incident 발생시 Syslog 연동으로 SIEM 솔루션에 즉각적인 모니터링

Case#3. End-Point DLP 활용한 Device 보호

고객사 요구사항

[기존 현황]

- 임직원 PC 에서 중요정보 유출 사례 적발
- 단말 Device 에서 외부(USB 메모리, 출력물, 등)로 유출 사례 발생

[개선요구사항]

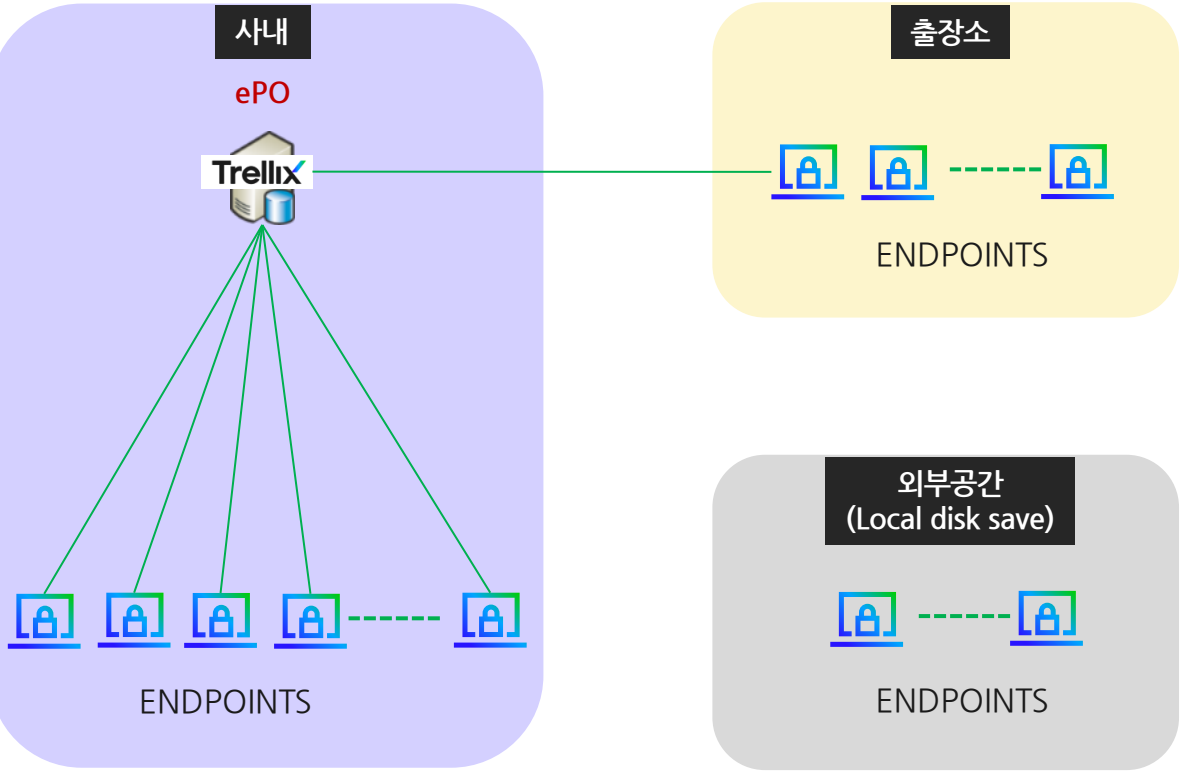
- 임직원 PC 사용시 개인정보 파일 및 중요 파일의 외부 유출 차단
- 사내/사외에서 PC Device 에서 파일의 유출 경로 탐지 및 차단 요청
- **압축파일의 경우도 전수 조사(비밀번호 압축치 차단)**
- Incident 발생 시 SIEM 솔루션을 통한 즉시 확인

DONGHOON 동훈아이텍

Trellix

Case#3. End-Point DLP 활용한 Device 보호

시스템 구성도



End-Point DLP

- 전사 PC E-DLP Agent 배포/설치
- ePO 통신 가능 구간의 경우 실시간 Incident 확인 (PC 차단은 ePo 통신 상관 없음)
- 단일화된 정책 배포
- 출장소의 경우 소단위 임직원에게 Agent 배포를 통해 손쉽게 관리
- 외부(출장 및 재택 근무 등)에서 PC 사용시 지속적인 탐지/차단
- ePO 통신 불가 지역의 경우 발생된 Incident 를 PC에 저장 후 ePO 통신 재개 시 정보 동기화

DONGHOON 동훈아이텍
Trellix

Case#3. End-Point DLP 활용한 Device 보호

고객사 개선사항

- End-Point DLP Agent 사용으로 사용자PC 에서 유출되는 Data 보호
- **중요 파일의 경우 USB 메모리, Print 출력, 등 탐지 차단**
- **PC Device 에서 사용하는 다양한 Application 을 통한 Data Loss 탐지/차단**
- 본사 및 출장소, 공장 등 다양한 공간에 쉽게 배포하여 구축
- 사용자 인증정보를 연동하여 사용자/그룹별 정책 차등 적용
- **특정사용자/그룹 에 우려되는 정책을 적용하여 사전에 데이터 유출 예방 (ex. 콜센터 및 퇴직 예정자)**
- Syslog 연동으로 SIEM 솔루션에 즉각적인 모니터링

Thank you