문서중앙화/VDI, DRM, DLP 솔루션 비교

DLP 솔루션을 검색하다 보면 함께 언급되는 다른 솔루션이 몇개 보인다. DRM과 문서중앙화 솔루션이다. 세 솔루션의 차이가 무엇인지, 자사에는 무엇을 도입해야 효율적일지, 아니면 셋 다 도입해야하는지 고민하는 게시글도 종종 볼 수 있다.

<문서중앙화/VDI>

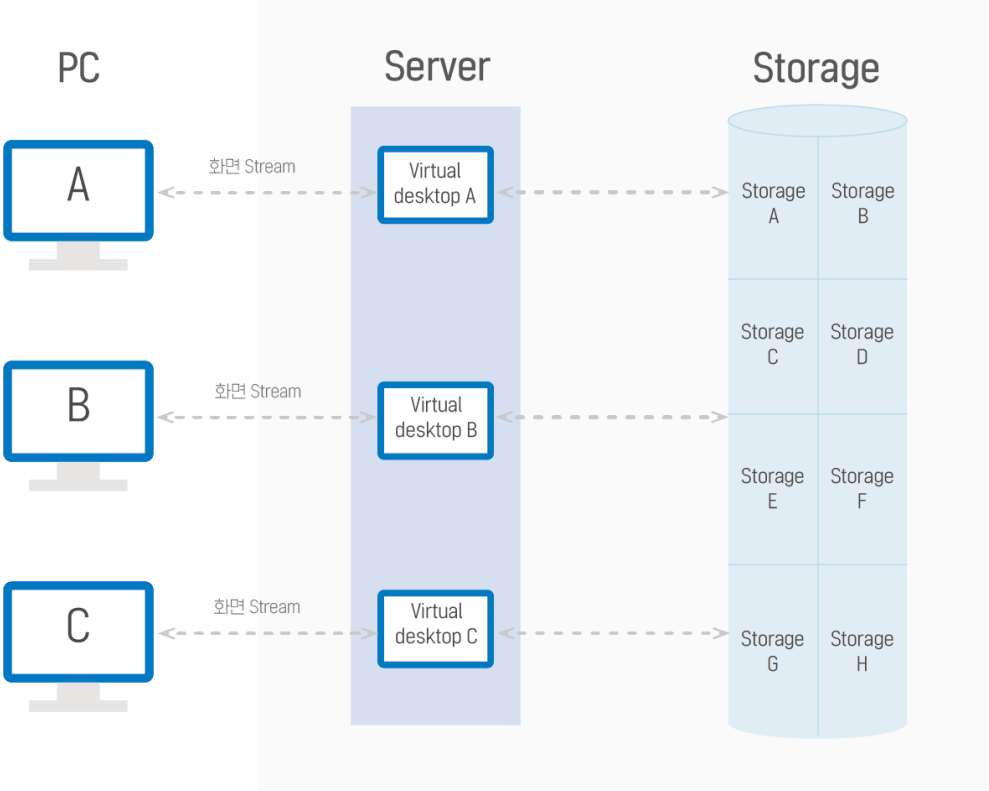
초기에는 사내 문서공유목적으로 개발된 솔루션이다. 로컬 PC가 아닌 중앙 스토리지에 일괄적으로 문서를 모아 관리한다. 사용자는 터미널 서비스처럼 중앙스토리지를 관리하는 서버에 접속하여 업무를 수행한다. 서버에는 수백수천대의 가상PC환경이 구축되어 있어서 사용자는 마치 자신의 데스크탑처럼 동일하게 작업할 수 있다. 문서중앙화의 경우 파일이 모두 중앙 스토리지에 저장되어 있고 컴퓨팅도 중앙서버에서 이루어진다. 사용자에게는 오직 윈도우 화면정보만 전송된다. 보안담당자는 중앙에서 관리만 하면 되기 때문에 자산관리가 용이하다. 정보보안 관점에서는 개인정보/기밀정보가 포함된 문서가 PC, USB, 외장하드 등에 저장/복사되는 것을 원천적으로 차단하여 정보유출을 막아주는 역할을 한다.

다만 모든 문서가 중앙 스토리지에 저장되어 있기 때문에 업무상 단점도 존재한다.

서버 안에 수백, 수천개 PC가 붙어있기 때문에 서버와 PC 사이에 전송되는 데이터, 트래픽 또한 만만치 않다. CAD, 영상편집, 일러스트레이터 등 디자인/이미지 제작이 주업무인 직군에서는 이 단점이 두드러진다. 중앙 스토리지에 접속해 문서에 접근하여 제작을 해야 하는데, 해상도가 떨어지고 색감에 차이가 발생하고 지연시간이 발생하는 문제가 발생할 수 있다. 서버에 부담이 되기 때문에 초당 60프레임까지 올라가는 4K 고화질 영상은 문서중앙화 환경에서는 지원되지 않기도 한다.

문서중앙화는 USB, 외장하드 등 매체통제 부분에서만 통제가 된다. 출력물, 인터넷 전송을 통한 유출은 '문서중앙화'로는 막을 수 없다. 해커는 네트워크를 통해 정보를 유출하는데 문서중앙화는 해당 부분에 대해 통제하는 기능이 없다.

'문서를 중앙에서 관리'한다고 해서 보안상 위험을 완전히 차단한 것은 아니다. 해커가 중앙 스토리지를 노려 공격할 때는 위험에 고스란히 노출된다. 모든 문서가 중앙 스토리지에 저장되어 있기 때문에 해킹된다면 사내 모든 문서가 랜섬웨어에 걸리는 최악의 사태까지 일어날 수 있다.



<DRM>

디지털 저작권 관리(Digital Rights Management)의 약자인 DRM은 본래 음원서비스의 무분별한 복제와 저작권 침해를 막기 위해 개발된 기술인데, 기업의 데이터보안으로 범위가 확장되었다.

DRM은 파일에 암호를 걸어 허가된 사용자에게만 열람을 허용한다. 또는 계정별로 접근권한에 차등을 두어 열람만 가능하고 편집은 불가능하도록 설정할 수 있다. DRM은 해커가 파일을 탈취해도 복호화할 수 없기 때문에 원천적으로 안전하다고 어필해왔다.

하지만 DRM 솔루션이 구축되지 않은 거래처에 파일을 전달해야 하는 경우 등 복호화가 반드시 필요한 경우가 발생한다. 업무관련 사유로 인한 DRM 암호화 해제는 대기업에서 한달에 수천 건씩 발생한다. 문제는 여기서 발생한다. 암호화 해제 이후부터는 추적이 되지 않는다. USB, 출력, 인터넷 전송시 통제도 되지 않고 감사증거도 남지 않는다. 또 문서 열람 권한이 있는 사람이 문서를 열람하고 정보를 유출할 경우에는 통제/대응이 어렵다.

이러한 약점을 보완하기 위해서 DRM은 USB통제, 출력물 통제 등 DLP 기본기능을 추가해서 보완하고 있다. "요즈음은 DLP와 DRM의 경계가 모호해졌다"라는 말이 나오는 이유이다.

DRM은 오피스과 같은 애플리케이션에서 시스템 후킹을 통해 문서 암복호화를 수행한다. 이때 시스템 간에 충돌이 일어나 장애가 발생하기도 한다. 또 애플리케이션이 신규버전을 출시할 경우 DRM도 업데이트가 필요하나 이에 시일이 소요된다. OS(운영체제)가 업그레이드될 때도 동일하게 DRM에 대대적인 업데이트가 필요하다. 심지어 이는 윈도우 OS에만 국한된 문제이다. Mac OS, Linux OS 기반 DRM 솔루션은 존재하지 않기 때문이다.

<엔터프라이즈 DLP>

DLP는 Data Loss Prevention의 약자로 정보유출방지 솔루션이다.

핵심기능은 검출(Discover)과 차단(Prevent), 기록(Audit)으로 설명할 수 있다.

<검출(Discover)>기능에서는 데이터가 개인정보인지, 기밀정보인지, 아니면 직원의 개인적인 정보인지 파악하는 역할을 한다. 주민등록번호, 카드번호, 핸드폰 번호 등 정보패턴에 따라 사전에 파일을 분류한 후 삭제, 암호화하여 PC 내 저장된 불필요한 개인정보를 정리해준다.

<차단(Prevent)>은 정책 이상의 정보가 외부로 반출될 경우 나가기 전에 사전에 통제하는 행위를 뜻한다. DLP는 DRM, 문서중앙화 솔루션과 다르게 정보의 유출차단 중심으로 운영된다. 정보유출은 대표적으로 USB나 외장하드를 통한 파일복사, 출력, 인터넷 파일전송을 통해 발생한다. 엔드포인트 단에서도 네트워크를 통한 파일전송을 차단할 수 있지만, 사내 정보자산을 일괄적으로 관리하기 위해 네트워크에 DLP를 구축해 전송을 통제하기도 한다.

DLP는 직원 PC내에서는 문서작성, 열람이 자유롭고 외부반출시에만 통제하는 것이 특징이다. 정책이상의 기밀/개인정보가 포함된 파일을 외부로 반출해야 할 경우에는 결재승인 후 반출 가능하다.

또는 결재승인은 생략하되 반출기록을 모두 기록하여 임직원 스스로 보안수칙을 지킬 수 있도록 유도한다. <기록(Audit)>기능이다. 외부로 나간 것은 모두 기록한다. 기록된 정보는 감사자료로 활용될 수 있으며, 무엇이 외부로 반출되었는지 기록하는 것만으로도 유출시도자는 위축되어 정보유출 확률을 효과적으로 낮출 수 있다. 사실, 앞서 언급한 결재승인 절차는 업무효율성을 중시하는 일반 기업에서는 선호하지 않는 방식이다. 되려 통제로 인하여 내부 불만이 쌓일 수도 있으며, 내부 직원들이 우회경로를 찾는데 촉매제가 될 수 있다. 기록(Audit)은 내부임직원의 업무 효율성

을 배려한 기능이다.

세가지 솔루션은 모두 정보유출차단을 목적으로 개발됐다. 다만 구현하는 방식에 차이가 있을 뿐이다. 정보유출을 막기 위해 한 솔루션은 데이터의 흐름을 모두 기록하고 (DLP), 다른 솔루션은 관리하기 쉽게 한 장소에서 일괄적으로 통제하고 (문서중앙화),나머지 한 솔루션은 권한이 있는 사용자에게만 문서를 오픈한다 (DRM).

구분	DLP	DRM	문서중앙화
개인정보 주요파일 검색/암호화/삭제	○	△	X
오피스문서 자동 암복호화	X	○	X
출력물 통제	◎	○	X
USB,외장하드 매체통제	◎	○	◎
인터넷 전송 통제	◎	△	X
스마트폰으로의 파일전송 통제	◎	△	X
Mac, Linux 플랫폼 지원	○	X	X
노트북 디바이스 반출시 통제	△	△	○

구분	DLP	DRM	문서중앙화
개인정보 주요파일 검색/암호화/삭제	○	△	X
오피스문서 자동 암복호화	X	○	X
출력물 통제	◎	○	X
USB,외장하드 매체통제	◎	○	◎
인터넷 전송 통제	◎	△	X
스마트폰으로의 파일전송 통제	◎	△	X
Mac, Linux 플랫폼 지원	○	X	X
노트북 디바이스 반출시 통제	△	△	○

정보보안 기업들은 단점을 극복하기 위해 에이전트 내 추가기능을 개발, 탑재하며 완성도를 높였다. 다른 솔루션이 가진 강점을 자사 제품에 적용하기도 했다. 이제 DLP, DRM, 문서중앙화 솔루션은 각 기술의 이름으로 불리기 보다는 기능을 통합해가며 '정보보호 솔루션'으로 정체성을 굳혀가고 있다.

정보유출과 정보위변조를 동시에 보안해야할 때

과거에는 내부직원 또는 해커의 정보유출행위를 차단하는데 중점을 두고 해당 솔루션을 도입했다. 그러나 최근에는 악성코드, 랜섬웨어를 통한 피해사례가 증가함에 따라 현재는 유출차단과 동시에 정보의 위변조를 막는 것에도 집중하고 있다.

정보자산을 보호하지 못할 경우 그 후폭풍은 거세다. 해커와의 협상을 통해 어떻게 해서든 암호화된 정보를 복호화하기 위해 노력함과 동시에 연일 오르내리는 여론을 감내해야 한다. 해킹사고로 피해를 입은 고객들, 거래처와도 피해복구를 위해 끊임없이 연락해야 하며, 한국인터넷진흥원의 사고조사에도 착실히 협조해야 한다. 온전한 협의가 이루어지지 않았을 경우 소송으로 돌입하기도 하며, 조사 중 우리회사의 과실이 발견되면 형사처벌도 면할 수 없을 것이다.

소만사는 자사 엔드포인트 DLP(내부정보 유출방지) 솔루션 'Privacy-i'에 EDR 기능을 탑재해 'Privacy-i EDR'을 출시했다. 이를 통해 도입기관은 데이터의 유출과 위변조로부터 정보자산을 안전하게 보호할 수 있게 되었다. 특징은 다음과 같다.

첫번째, 데이터의 중요도에 따라서 보호수준을 다르게 적용하여 관리할 수 있다. 회사등산대회 단체사진과 고객신용정보 파일 중 유출 또는 변조될 경우 회사에 치명적인 결과를 가져다줄 파일은 무엇일까? 'Privacy-i EDR'은 엔드포인트 안에 보관된 주요 기밀, 개인정보를 주기적으로 식별해 현황을 파악한다. 악성행위 등 보안위협 감지될 경우 엔드포인트에 설치된 탐지엔진이 사전에 식별, 분류한 기밀정보/개인정보 등 중요정보부터 우선 보호한다. 데이터 유출위험이 발생할 경우에는 DLP에서 웹메일, 웹하드, 메신저, 클라우드를 통한 정보유출을 차단한다.

두번째, DLP와 EDR 뿐만 아니라 개인정보파일검출, 매체제어, 출력물보안 기능이 탑재되어 에이전트 설치 하나만으로도 보안위협을 일괄적으로 통제할 수 있다. 개발사에서 기획부터 일체화하여 안전성, 정합성을 확보했다. 성능부하가 적다.

세번째, 이미 'Privacy-i'를 사용하고 있는 기업/기관은 에이전트 별도 설치없이 기존 'Privacy-i' 에이전트에 EDR 기능을 추가 적용할 수 있다. 에이전트 업그레이드 하나만으로 악성코드 차단부터 유출통제까지 전 구간의 데이터보호를 수행할 수 있게 된다. 기존 설치된 에이전트에 EDR을 추가하기 때문에 프로젝트 기간도 단축시킬 수 있다.

마지막, 통합 사이버 킬체인 보고서인 'MITRE ATT&CK' 프레임을 반영했다. 악성행위의 탐지방법, 피해경감기법까지 적용해 고도화했다. 최근의 추세는 'EDR 솔루션'에 'MITRE ATT&CK'을 얼마나 많이 적용하였는지에 따라 '솔루션의 성능'이 평가되고 있다.

'Privacy-i'는 삼성그룹, LG그룹, 대검찰청, 금융감독원, KB은행 등 500여곳에서 사용 중인 솔루션이다. 소만사는 'Privacy-i' 도입고객을 대상으로 2022년 말까지 EDR로의 전환을 완료할 계획이다.

Privacy-i EDR: https://www.somansa.com/solution/control/pc-endpoint-dlp-privacy-i-edr/

Privacy-i : https://www.somansa.com/solution/control/pc-endpoint-dlp-privacy-i/