테크놀로지 리더를 위한
Media & IT(Information Technology)

#3. 보안과 미디어

강자원
컴퓨터시스템응용기술사
/ KBS MNC(Media Network Center)팀

최근 보안 시장에서는 개인정보 보호를 위한 DB 암호화 솔루션과 콘텐츠 유출 방지를 위한 DRM 솔루션 시장이 두각을 나타낸 것으로 드러났다. 기술적 측면으로는 네트워크 DLP 등 콘텐츠 보안 솔루션 시장에서 인공지능(AI) 기술이 접목되는 양상을 보였다. 지난 COVID-19로 인해 VoD 시장과 e-learning, 화상회의 등의 스트리밍 미디어 콘텐츠 산업의 폭발적인 수요와 성장으로 새롭고 다양한 보안위협이 발생하고 있다.
이번 호에서는 미디어 콘텐츠와 관련된 보안 이야기를 해보고자 한다.

'STRIDE 위협 모델링 기법'을 통한 보안위협 요소 식별 및 대응 분석

보안위협을 진단하기 위해 필자는 MS(Microsoft)사의 STRIDE 모델링 기법을 기준으로 설명하고자 한다. 이는 가장 널리 알려진 위협 모델링 방법으로, 다음의 머리글자만 딴 약어이며 다음 6가지의 위협을 측정한다.

	위협분류	보안속성	설명 및 대처 방안
S	Spoofing 신원도용	인증	타인의 계정을 이용하여 시스템 권한 획득 대처방안 : 인증, 전자서명 등
T	Tempering 변조	무결성	디스크, 네트워크, 메모리의 데이터등을 변조 대처방안 : 해쉬, 전자서명 등
R	Reputation 부인	부인방지	작업수행에 대한 부인 대처방안 : 전자서명, 감시로그 등
I	Information Disclosure 정보유출	기밀성	권한이 없는 사용자에게 정보 제공 대처방안 : 보안 강화 프로토콜, 암호화 등
D	Denial of Service 서비스 거부	가용성	서비스 거부 또는 정상적인 서비스 제공 방해 대처방안 : 필터링, 공격 모니터링, 포트스캔 차단
E	Elevation of Privilege 권한 상승	권한 부여	권한이 없는 자가 권한을 부여 받아 서비스 수행 대처방안 : 전자서명, 권한 인증 등

그림 1. STRIDE 보안위협 모델링 기법

콘텐츠가 네트워크 기반에서 전송 및 공유되는 환경에 따라 STRIDE 모델링 기법과 같은 보안 위협이 존재할 수밖에 없고, 위협 유형별로 존재하는 보안에 대해 대응방안을 마련해야 한다. 위협 중 인증, 무결성, 부인방지, 권한 부여에 대한 부분은 포렌식 워터마킹과 DRM 기술로 대응 가능하며, 가용성과 기밀성에 관련된 부분은 DLP(Data Loss Prevention) 및 방화벽 등과 같은 보안기술로 대응할 수 있다.

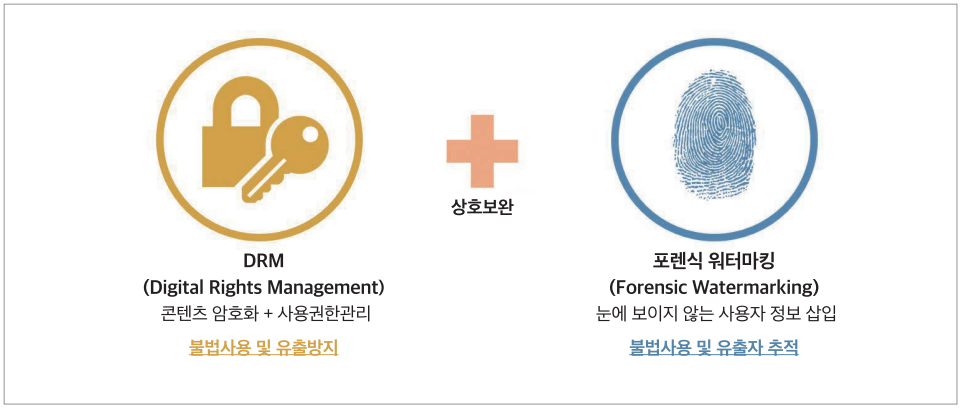


그림 2. 콘텐츠 보안을 위한 기술

CDN 환경에서의 콘텐츠 보안, DRM

콘텐츠 전송 네트워크(Contents Delivery Network, CDN)는 지리적 제약 없이 사용자에게 빠르고 안전하게 콘텐츠(웹 페이지, 동영상, 이미지 등)를 전송할 수 있는 콘텐츠 전송기술을 의미한다. 쉽게 설명하면 마치 은행의 ATM기라 생각해도 좋다. 여러 곳에 ATM을 설치해 놓으면 사용자가 빠르고 효율적으로 현금을 찾을 수 있기 때문에 은행에서 긴 줄을 서서 기다릴 필요 없이 가까운 곳에 있는 ATM을 이용하면 된다. 인터넷 환경에서 대용량의 미디어 콘텐츠를 전송하면 트래픽이 폭주할 때처럼 네트워크 혼잡 문제가 발생할 수 있다. CDN 서비스는 이러한 문제를 해결하기 위해 개발되었다. 그리고 대부분의 미디어 콘텐츠를 서비스하는 업체(Netflix, Youtube, Disney 등)들은 CDN을 사용해 고객 경험(QoE)을 개선한다. 이러한 IP 네트워크 기반 서비스 구조에서 콘텐츠의 보안은 어떻게 이루어지는지 알아보자.

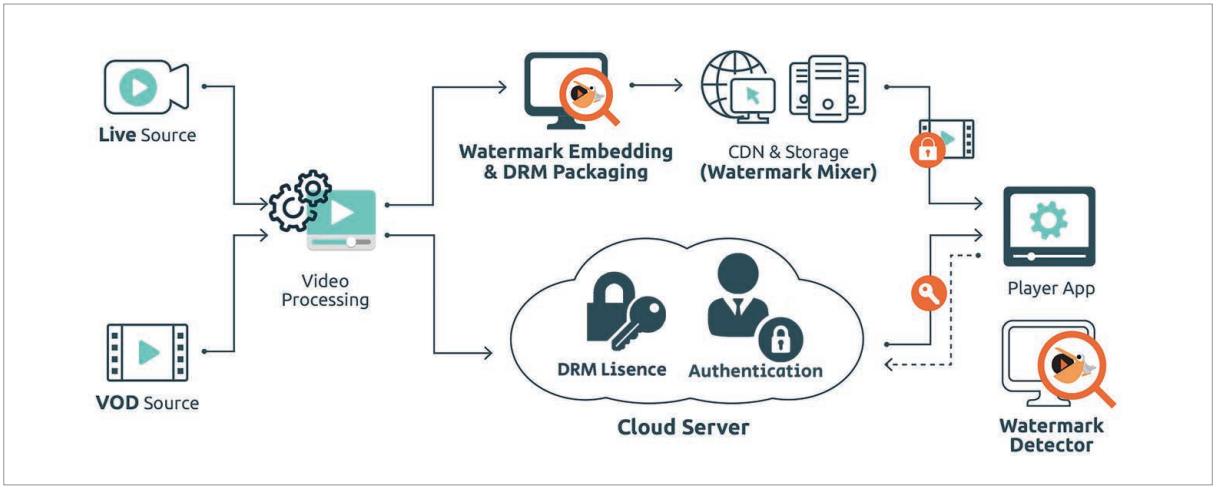


그림 3. 스트리밍 서비스를 위한 CDN 서비스 환경의 DRM 인증방식

먼저, DRM(Digital rights management)이란, 출판자 또는 저작권자가 그들이 배포한 디지털 자료나 하드웨어의 사용을 제어하고 이를 의도한 용도로만 사용하도록 제한하는 데 사용되는 모든 기술을 지칭하는 용어를 말한다. 즉, 정당한 금액을 지불하지 않는 불법적인 사용을 차단하기 위하여 인증된 사용자가 인증된 기간에만 사용할 수 있도록 통제함으로써 불법적인 사용을 제한하고 있는데 이때 많이 사용되는 기술이다.

CDN 환경에서 DRM 기술은 콘텐츠 패키징 과정에서 불법복사 차단, 암호화 불법 유통 및 복제경로 감지 등을 위해 콘텐츠 최초 소유자의 정보를 콘텐츠에 삽입하는 워크마크 기술이 적용되며, 저작권자가 정의한 콘텐츠 사용규칙(라이선스 정보) 등이 라이선스 서버에 기록된다. 사용자는 사용 단말기(Player App)에 DRM 복호화 모듈을 설치하게 되고 서버로부터 사용자 인증과 라이선스 정보를 발급받아 콘텐츠를 복호화하는 구조가 된다.

포렌식 워터마킹 (Forensic Watermarking)

암호화된 DRM 콘텐츠도 권한이 있는 사용자의 기기에서 최종적으로 재생되기 위해서는 복호화 과정을 통해 원본 형태로 전환되어야 하는데, 이 재생 과정에서 여러 가지 기술적인 한계로 인해 콘텐츠가 유출될 가능성이 있다. 이렇게 만에 하나 콘텐츠가 유출되는 상황에서 해당 유출자가 누구인지 추적해 더 이상의 콘텐츠 유출을 방지할 수 있는 기술이 '포렌식 워터마킹'이다.

"DRM으로 불법 사용을 막을 수 있다면 왜 포렌식 워터마킹이 필요하지?"

포렌식 워터마킹의 필요성에 대해 이런 의문을 가질 수도 있겠다. 그러나, '안전하지 않은 구간'에 암호화되지 않은 상태의 콘텐츠가 노출되는 것을 보완하기 위해 '하드웨어 기반 DRM', 'Trusted Execution Environment(TEE)', 'High-bandwidth Digital Content Protection (HDCP)' 등 여러 가지 기술들이 추가로 적용되고 있지만, 이러한 기술들만으로는 콘텐츠 유출을 막을 수 없는 경우들이 있다.

1) 캠코더를 이용한 화면 녹화
2) 스크린 레코더를 통한 영상 캡처

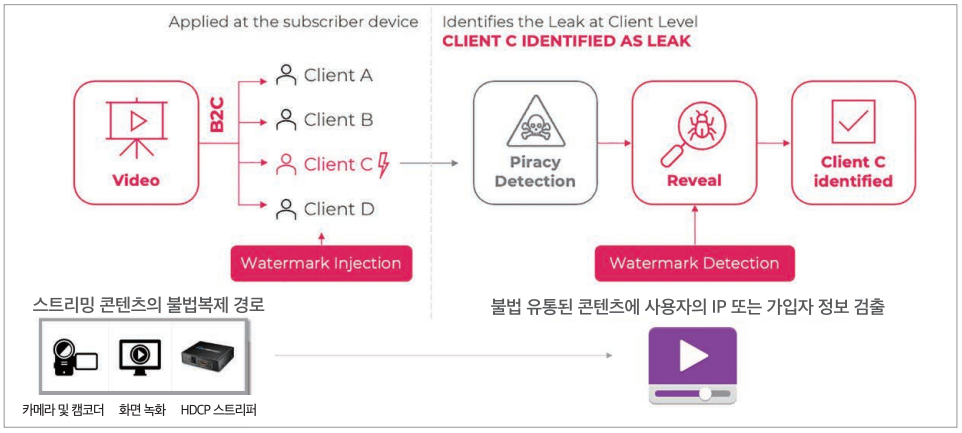
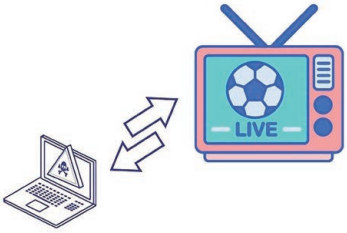


그림 4. 포렌식 워터마킹의 검출 방식

할리우드 스튜디오의 경우 콘텐츠 불법 유출로 인한 저작권자의 피해를 방지하기 위해, MovieLabs에서 발표한 'MovieLabs Specifications for Enhanced Content Protection' 규격에서는 UHD 해상도의 최신 영화와 같은 고부가가치 영상 콘텐츠에 대해서 하드웨어 기반의 DRM과 포렌식 워터마킹 기술을 필수적으로 적용하도록 제안하고 있다.

라이브 스트리밍 콘텐츠 보호 방안



스포츠 및 이벤트와 같은 라이브 방송은 방송 산업의 핵심이며, 이에 대한 중계권 확보에 막대한 비용을 사용하고 있다. 하지만 라이브 스트리밍 콘텐츠의 인기로 인해 불법 복제의 주요 표적이 되고 있으며 화면 녹화와 같은 방식으로 꾸준히 유출되고 있다. 프리미엄 라이브 콘텐츠의 방송권을 위해 매년 수십억 달러를 지출하고 있고, 이는 TV 서비스가 시청자와 구독자를 놓고 경쟁하면서 TV 서비스 비용이 비싸지는 원인이 되기도 한다.

흔히 우리가 많이 들어본 인스타그램의 라방(라이브 방송)이나, 페이스북 또는 유튜브를 통한 생중계, 각종 포탈을 통해 시청하는 스포츠 생중계 서비스 등의 경우가 HTML5를 이용한 스트리밍 콘텐츠라 볼 수 있겠다. HTML5 라이브 스트리밍은 플러그인이나 외부 플레이어 없이도 브라우저에서 비디오 파일을 재생할 수 있는 HTML5 비디오 요소를 기반으로 한다. HTML5 라이브 스트리밍은 HLS 또는 DASH와 같은 적응형 비트 전송률 스트리밍(ABR) 프로토콜을 사용하여 시청자의 네트워크 상태 및 장치 기능에 따라 다양한 해상도와 비트 전송률로 비디오 세그먼트를 제공한다. ABR 프로토콜은 M3U8 또는 MPD와 같은 매니페스트 파일을 사용하여 사용 가능한 비디오 세그먼트 및 해당 위치에 대한 정보를 제공한다.

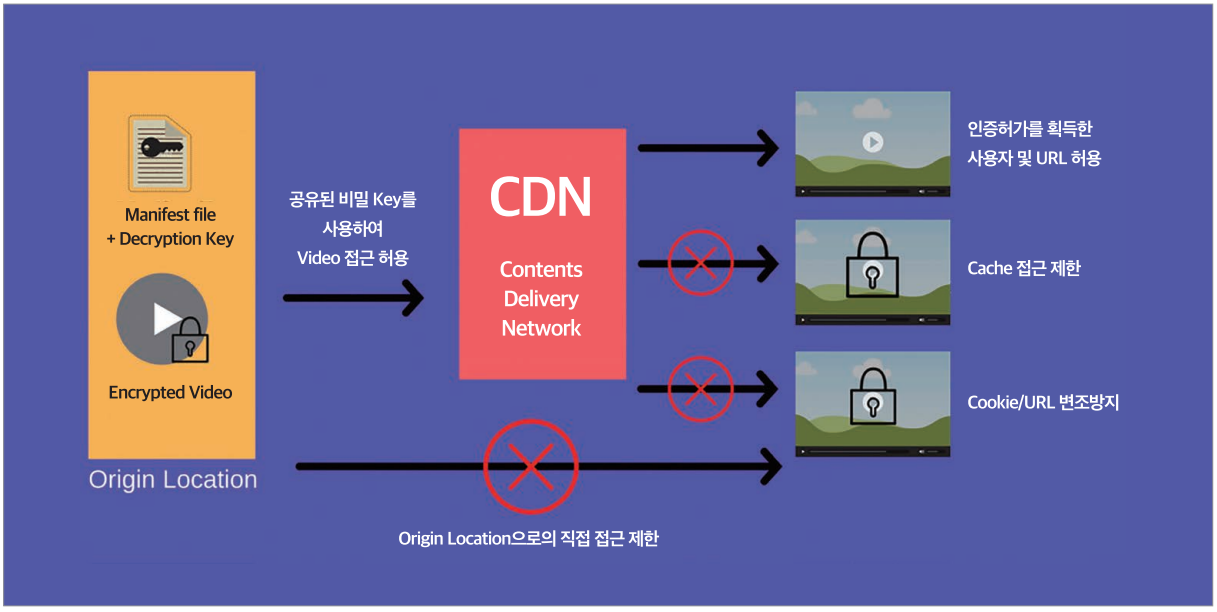


그림 5. 쿠키와 승인된 URL의 스트리밍 프로토콜 인증

HTML5 라이브 스트리밍 보안은 원본 서버 또는 비디오 세그먼트 및 매니페스트 파일을 생성하는 인코더인 비디오 소스를 보호하는 것으로 시작된다. 이를 위해 HTTPS를 사용하여 비디오 소스와 CDN 또는 뷰어 간의 통신을 암호화하고, 토큰 또는 쿠키와 같은 인증 및 승인 메커니즘을 사용하여 신원 및 액세스 권한을 확인하며, 디지털 서명 또는 체크섬을 사용하여 비디오 세그먼트 및 매니페스트 파일의 무결성을 검증할 수 있게 된다. 지리적 차단 또는 IP 필터링을 통해 위치 또는 IP 주소를 기반으로 액세스를 제한하기도 한다.

HTML5 라이브 스트리밍을 보호하는 두 번째 단계는 시청자에게 전달되는 실제 비디오 파일인 비디오 세그먼트를 암호화하는 것이다. 이를 위해 AES-128 또는 AES-256 암호화, Widevine, FairPlay 또는 PlayReady와 같은 DRM 시스템, EME(Encrypted Media Extensions) API와 같은 여러 방법을 사용할 수 있다. 이러한 암호화 알고리즘 및 시스템은 다양한 장치 및 플랫폼에 대해 서로 다른 키 및 정책으로 비디오 세그먼트를 보호할 수 있다.

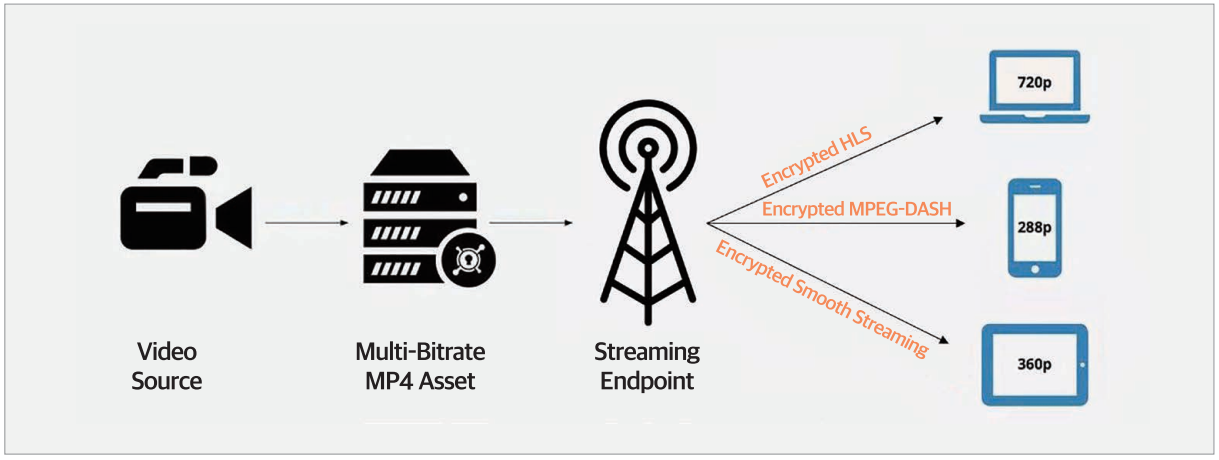


그림 6. 스트리밍 프로토콜의 암호화 구간

지금까지 스트리밍 콘텐츠의 보안과 관련된 기술에 대해 알아보았다. STRIDE 보안위협 모델 중에서도 가용성과 기밀성에 해당하는 보안기술을 마지막으로 DLP(Data Loss Prevention)를 예로 들어 설명하려 한다.

데이터 유출방지를 위한 솔루션, DLP(Data Loss Prevention)

DRM의 경우 이미지, 영상, 문서 등을 만들고 저장할 때마다 실시간으로 '잠금' 설정이 되어서 그 콘텐츠 자체를 암호화하는 보안 솔루션이지만, DLP(Data Loss Prevention) 솔루션 같은 경우, 그 데이터 정보가 오고 가는 흐름을 추적하여 기록하고 차단하는 것을 말한다. 데이터의 흐름 즉, 데이터 이동 경로를 감시하여 기업 내부의 중요 정보와 데이터 유출을 감시하고 기록한다. 그리고 데이터 이동 경로 감시 중 유출이 감지되었을 땐 이를 경고 혹은 차단하면서 데이터를 보호하는 기능을 한다.

DLP를 통해 3가지 상태의 데이터를 보호할 수 있다.

01 **저장 데이터**(Data at rest)는 아카이브되어 있거나 자주 접근 또는 수정하지 않는 데스크톱, 노트북, 서버 또는 클라우드에 저장된 정적 데이터다.
ex) 아카이브에 저장된 미디어 콘텐츠

02 **사용 데이터**(Data in use)는 네트워크 내에서 여러 사용자가 자주 업데이트하는 활성 상태의 데이터다.
ex) 현재 다양한 포맷으로 변환 중인 미디어 콘텐츠

03 **이동 데이터**(Data in motion)는 예를 들어 데스크톱에서 클라우드, 휴대용 저장 장치 또는 다른 엔드포인트로 이동되는 네트워크 외부로 전송되는 디지털 정보다.
ex) 웹하드 등으로 이동되는 촬영 원본 및 편집 완본

DLP를 활용하면 다음과 같은 구성을 통해 내부와 외부의 콘텐츠 유출을 탐지하고 방지할 수 있게 구성할 수 있을 것이다.

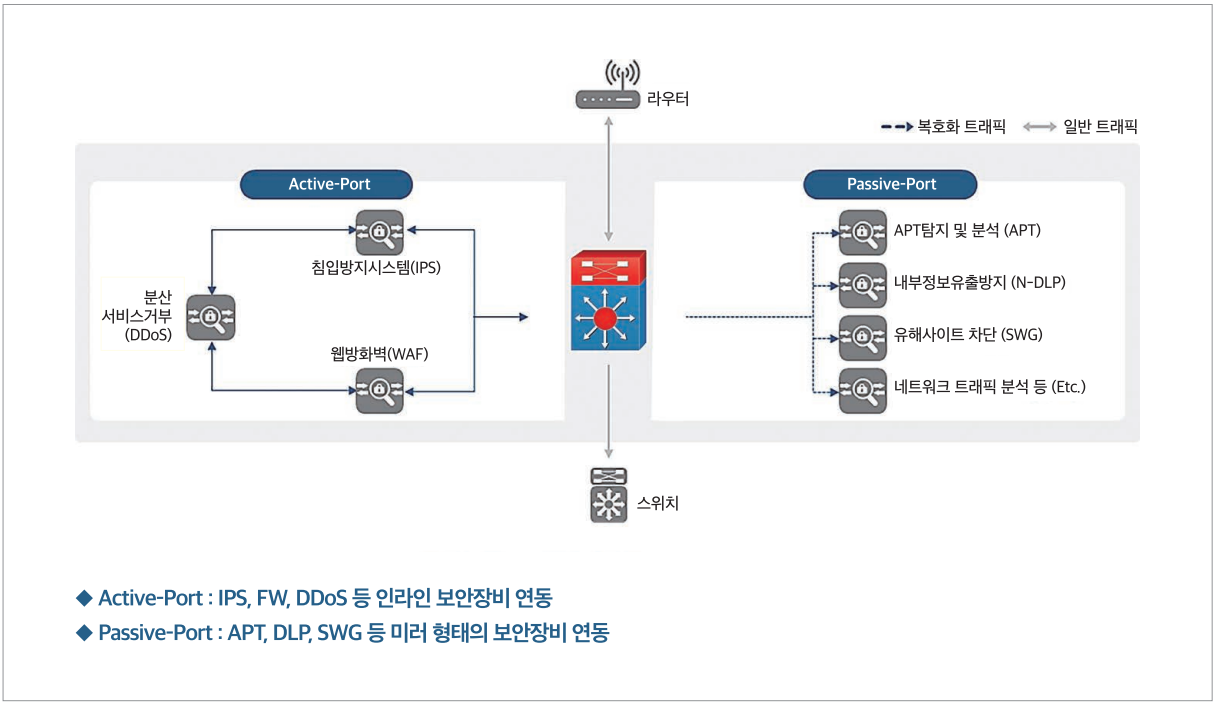


그림 7. DLP를 사용한 네트워크 구성 예시

필자는 단순히 콘텐츠와 관련된 보안기술만 소개했지만, 사실 보안의 영역은 스펙트럼이 매우 넓고 각각의 포인트별로 레벨별로 취약점이 존재하기 때문에 위협에 대응하고 해결하기 위해서는 구조적인 접근과 영역별 대응방안이 필요하다. 영역별 보안이란 콘텐츠를 제작하는 환경, 제작을 위한 솔루션의 시큐어코딩, 시스템 보안, 접근권한 제어, DB 암호화, 네트워크 접근제한 등이 있을 수 있겠다. 이를 위해서는 전사적인 보안 거버넌스를 구축하고 컴플라이언스에 따른 거시적이고 체계적인 접근이 이루어져야 한다.