Drive your digital transformation with LS ITC

Cloud 보안 관리 플랫폼 “LS First Security”

2023.04

CONTENT

목차

I 클라우드 보안 위협

- 클라우드 서비스 증가에 따른 보안사고 증가
- 클라우드 보안 영역 구분 – 책임 공유 모델
- 클라우드 보안 사고 주요 원인
- 클라우드 보안 설정 오류 예
- 클라우드 설정 오류 사고 대표 사례

클라우드 서비스 증가에 따른 보안 사고 증가

클라우드 공격 630% 증가, 클라우드 앱 노린 사이버 공격 6배⬆

코로나19 확산으로 클라우드 기반 서비스 이용이 높아지면서 이를 노린 사이버 공격이 6배 이상 증가한 것으로 조사됐다.

미국 지디넷은 최근 사이버보안 업체 맥아피의 클라우드 기반 서비스 사이버 보안 관련 리포트를 인용해 보도했다. 해당 보고서에 따르면 지난 1월부터 4월까지 클라우드 기반 서비스를 타깃으로 한 원격 공격은 630% 증가했다.
이 보고서는 맥아피 이용자 3천만명에 대한 데이터를 기반으로 조사됐다.

출처: 지디넷

IBM “한국기업 데이터 유출 피해, 1곳당 41억… 4년간 늘어

IBM시큐리티와 포네몬연구소는 작년 5월부터 올해 3월까지 세계 500개 기업이 1000~10만건 규모의 실제 디이터 유출을 경험한 사어버침해사고 조사 내용을 분석한 결과를 발표했다. 한국기업 1곳당 41억 이상의 데이터 유출

한국IBM은 "조사 대상 한국 기업들의 손실 규모는 4년간 꾸준히 증가하는 추세"라면서 "인공지능(AI)과 하이브리드클라우드, 제로트러스트 접근방식을 통해 데이터유출 비용을 절감할 수 있다"라고 밝혔다.

출처: 아주경제

보안침해사고 수치

630%
클라우드 보안 공격 증가

2020년 1월부터 4월까지 클라우드 서비스에 대한 공격이 기존보다 무려 630%나 증가(MxAfee)

38억
데이터 침해 비용 평균

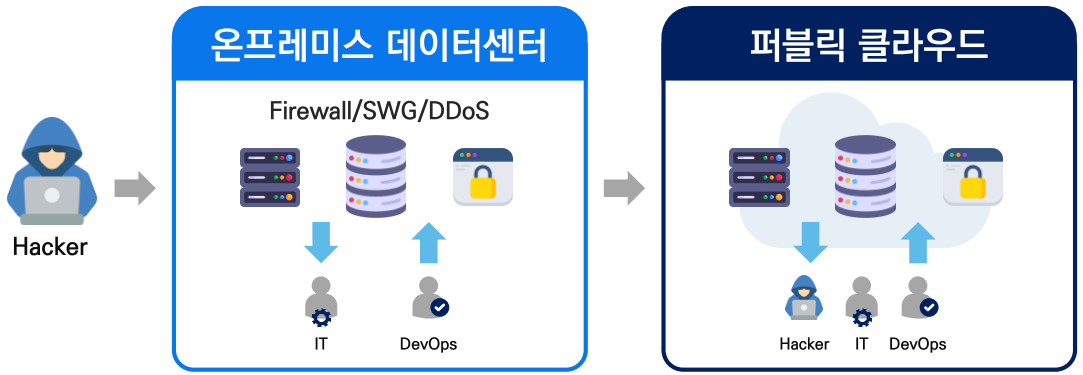
2020년 국내 24개 대기업 데이터 침해 비용으로 평균 38억 소요(IBM)

99%
사용자 실수에 의한 클라우드 침해 사고

클라우드 침해의 99%는 사용자 실수에 의해 발생(Gartner)

클라우드 환경에 대한 이해와 새로운 보안 필요

기존 레거시 보안은 벽을 만들어 외부 침입을 통제하지만 클라우드는 벽을 세울 수 없기에 사람에 대한 인증 권한 그리고 추적 등의 보안 기술이 중요합니다.

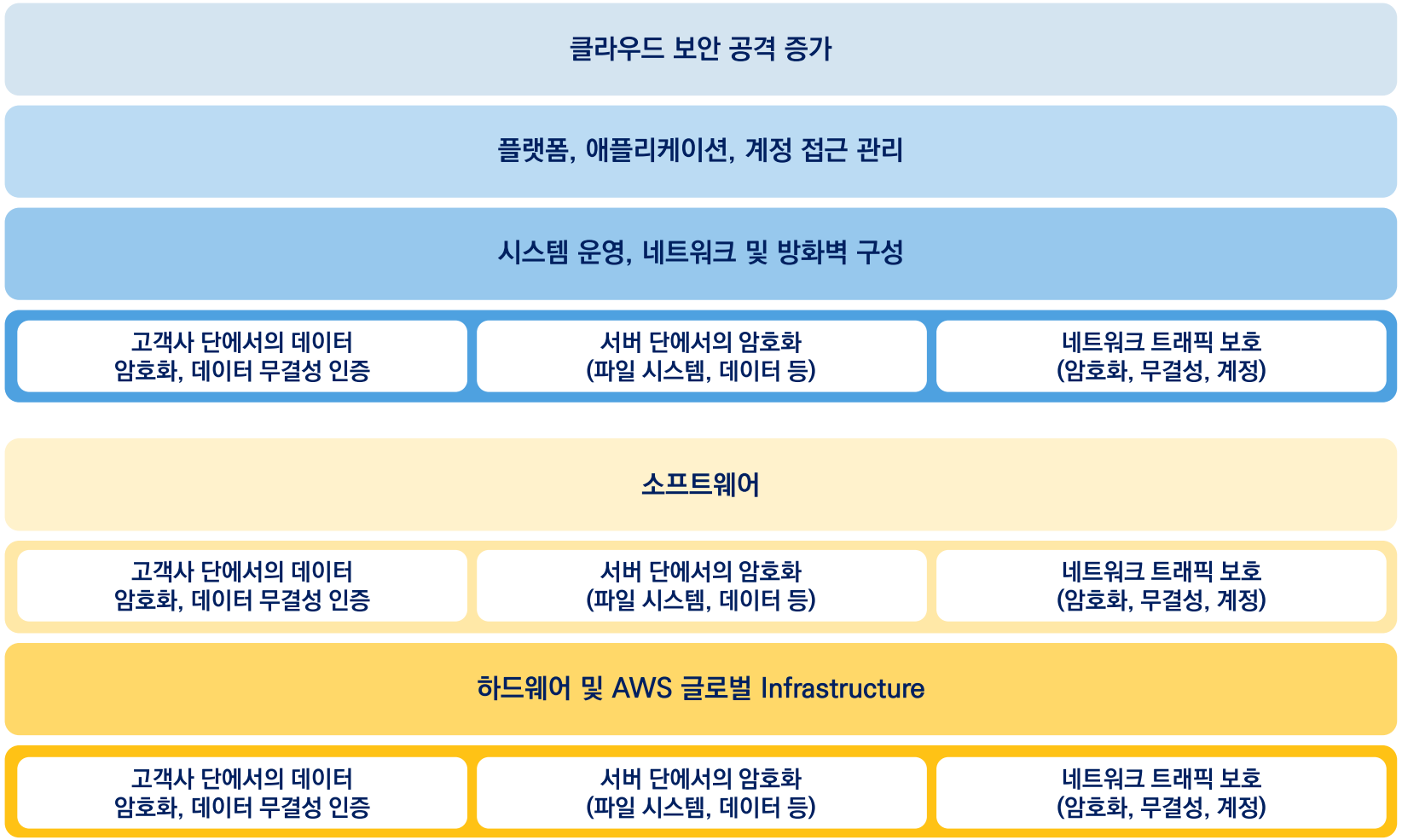


구분	레거시 환경 및 보안	클라우드 환경 및 보안
보안 방식	계층 방어 형태	사용자 인증 및 권한 제어
기술 적용 방식	개별 솔루션 기반 사일로화된 보안 기술 적용	통합된 보안 기술 적용
통제 대상	사람	기능, 권한
자동화 여부	X	O
책임 모델	데이터센터 전체 책임	책임 공유 모델(보안 구성 관리는 고객 책임)
인프라 복잡성	상대적으로 단순함	상대적으로 복잡함
자원 형태	물리적, 정적 자원	가상화 기반 동적 자원(자원 생성/삭제 등 변화 빠름)
자원 접점	단일 접점	다중 접점(공격 포인트가 많음)
권한 수준(사용자 자원 통제)	제한적	전체
추가 보안	없음	PaaS(람다, 컨테이너 등), SaaS형(풀 매니지드 서비스)

“클라우드에 맞는 특화된 보안 정책과 기술이 중요함”

클라우드 보안은 책임 공유 모델

클라우드 서비스 제공업체와 고객이 보호 해야할 영역을 인지 하고 보안 정책을 수립해야 합니다.



고객 보호 영역

- 권한 및 인증
- 데이터 보안
- 애플리케이션
- 클라우드 자원에 대한 보안

클라우드 서비스 제공업체 보호 영역

- 클라우드 서비스를 제공하는 인프라

AWS '책임 공유 모델(Shared Responsibility Model)'

클라우드 보안 사고 주요 원인

클라우드 보안 사고는 99%가 **고객보호영역(사용자 책임)**으로, 특히 **설정 오류**가 가장 큰 원인입니다.

Speciality

클라우드 보안에 대한 이해 부족

기업 보안 담당자가 클라우드 인프라, 기술, 관련 법규 등 클라우드 전반에 대한 이해와 책임 공유 모델에 이해가 부족한 경우

Compliance

클라우드 보안 정책 부족

클라우드에 대한 보안 컴플라이언스가 반영된 주기적 점검 기준, 보안성 심의 등을 위한 회사의 보안 정책, 가이드, 체크리스트가 아직 마련되지 않은 경우

Gartner "2025년까지 최소99%의 클라우드 보안 사고는 **사용자** 책임"

*책임 공유 모델 기반

Solution

클라우드 환경에서의 기술적 보안방안 부재

클라우드 환경에서의 보안 위협과 필요 보안 기능을 인지하고 이에 대응할 최적의 보안 솔루션 및 서비스에 대한 준비가 마련되지 않은 경우

Technology

새로운 클라우드 기술에 대한 보안방안 부재

매년 수백 개 이상의 클라우드 기술의 등장으로 이에 맞는 새로운 보안 기술들이 부재할 경우

클라우드 보안 설정오류 주요 예

설정 오류란 리소스의 잘못된 보안 설정으로, 설정 오류로 인한 보안사고는 사용자의 책임입니다.

잘못된 IAM 정책 설정

- 모든 사용자에게 Administrator 권한 부여
- 지정된 사용자에게 필요 이상의 권한 부여

잘못된 보안 그룹 정책 설정

- 모든 포트를 All Open(0.0.0.0/0)
- 실제 사용자 IP 또는 IP 대역 미설정

전송 중 암호화 미적용

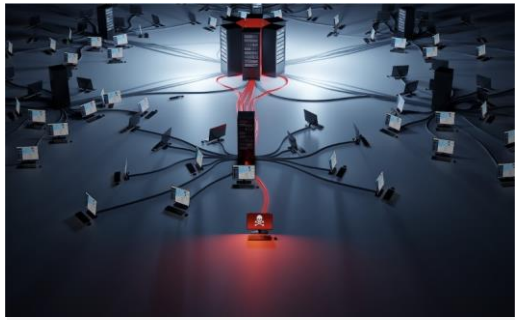
- Object Storage(S3, Storage Account)의 기본 암호화 미사용

클라우드 보안 사고 발생

Ransomware

Crypto Mining

Data Extortion



Attack Servers

클라우드 설정 오류 사고의 대표 사례

보안이 최우선인 기업조차도 **설정 오류로 인한 대규모 데이터 유출사고**로 막대한 피해 비용을 지출하고 있습니다.

	2021년	2022년
사례	**트위치 "서버 구성 오류로 정보 유출"** 크리에이터 정산 보고서 등 포함…"방송 암호 키 재설정" 컴퓨팅 | 입력 :2021/10/08 09:11 인터넷 방송 플랫폼 '트위치'에서 크리에이터의 수입 규모 정보를 포함한 내부 데이터가 유출된 것에 대해, 서버 구성 변경 상의 오류가 원인이라고 밝혔다. 이에 7일(현지시간) 방송 암호 키를 모두 재설정했으며, 이용자 대시보드를 통해 확인할 수 있다고 안내했다. 이는 지난 6일 트위치 내부 데이터 125GB 가량이 웹사이트 '포챈'에 등록된 것에 대한 자체 조사 결과다. 유출 데이터 게시자에 따르면 해당 데이터에는 2019년부터 현재까지 크리에이터들에 대한 정산 보고서와 트위치에서 사용되는 소프트웨어개발키트(SDK) 및 아마존웹서비스(AWS) 서비스, 모바일·데스크톱·비디오게임 콘솔용 트위치 클라이언트의 소스코드, 내부 정보보안 팀이 사용하는 도구 정보 등이 포함됐다.	**또 클라우드 설정 오류 사건! 이번엔 4개 공항 3TB 데이터 유출돼** 아마존 버킷 하나가 잘못 설정됐다. 그 바람에 남아메리카 공항 4군데와 관련된 데이터 3TB가 외부로 새나간 것으로 보인다. 직원들의 개인 신상 및 식별 정보이기 때문에 공항을 노리는 부류들에게 있어 매우 유용할 수 있다고 한다. [보안뉴스 문가용 기자] 아마존 S3 버킷의 설정 오류 때문에 3TB의 공항 관련 데이터가 외부로 노출되는 일이 발생했다. 무려 150만 개 이상의 파일들이라고 한다. 문제의 데이터베이스는 보안 업체 스카이하이 시큐리티(Skyhigh Security)가 발견했으며, 콜롬비아와 페루의 공항 4군데의 민감 정보로 구성되어 있는 것으로 분석됐다. 직원들의 개인 식별 정보도 포함되어 있다고 한다. 개인 식별 정보에는 항공사 직원들의 사진과 주민 등록 번호 카드들도 포함되어 있어 공항 쪽을 노리는 테러리스트들에게는 매우 유용하게 활용될 수 있다는 경고도 나왔다. 현재 문제의 버킷은 비밀번호로 잠긴 상태다. 잠기기 전까지 조사한 바에 따르면 해당 버킷에는 2018년부터 데이터가 저장되어 온 것으로 보이며, 사건 보고와 데이터 처리에 사용됐던 안드로이드 모바일 앱들도 있었다고 한다.
원인	• 서버 설정 오류 • Apache Airflow 내 Instance 설정 오류	• AWS S3 Bucket 설정 오류 • 접근제어 미설정
피해 유형	• **기업 내부 주요 정보 유출 (125GB)** – 트위치 스트리머 및 사용자 개인 정보 – 트위치 소스 코드, 내부 보안 툴 등	• **콜롬비아/페루 4개 공항 민감정보 유출 (3TB)** – 항공사 직원 개인 식별 정보 등 포함 • **테러리스트에게 유출 시 국가 안보 위협**

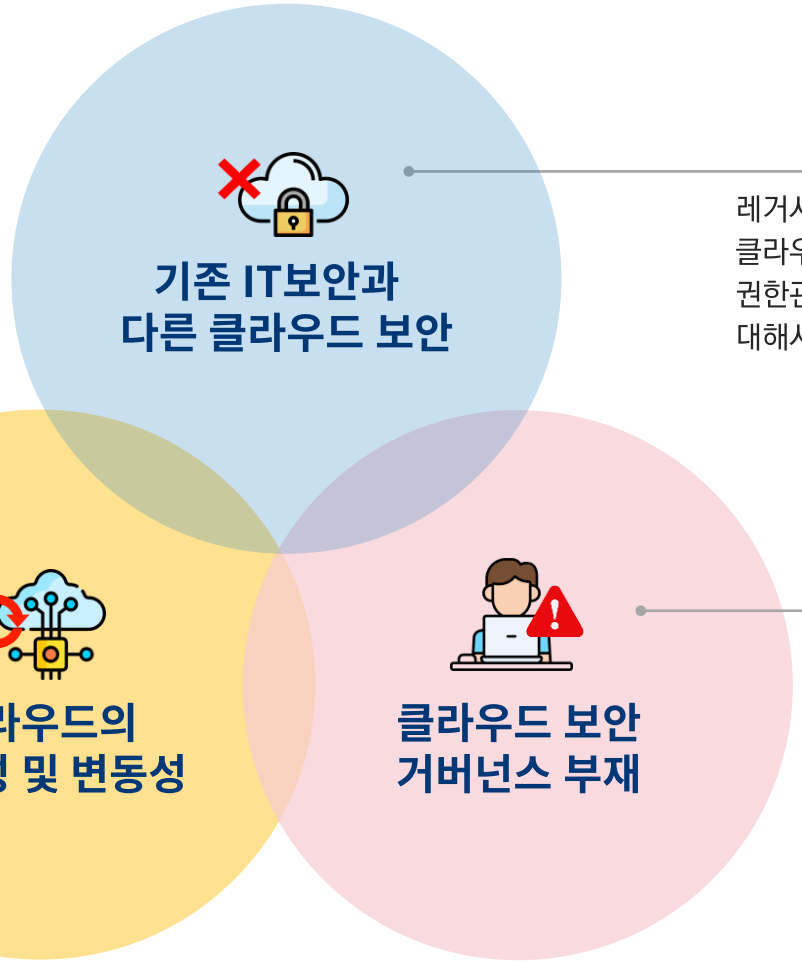
"사용자로 인한 설정 오류를 바로 잡는다면 많은 클라우드 보안 사고를 예방할 수 있음"

II 클라우드 보안 관리 플랫폼

- 클라우드 보안 설정 준비의 어려움
- 클라우드 보안 관리 플랫폼의 필요성

클라우드 보안 설정의 어려움

IT 운영자들은 기존 IT와 달리 클라우드 특성에 맞는 많은 보안 설정을 준비해야 합니다.



레거시는 사람만 통제 했다면 클라우드에서는 클라우드 자원과 API를 통제해야 한다.
권한관리도 사람 뿐만 아니라 클라우드 자원에 대해서도 모두 설정해야 한다.

멀티/하이브리드 클라우드 구성,
빠르게 출시되는 서비스,
CI/CD 환경에 대응하는 보안
관리 어려움

조직의 보안 목표 설정 관리,
보안 감사, 위협에 대한
개선안 마련 등 어려움

클라우드 보안 관리 플랫폼 필요

클라우드 보안설정의 어려움을 해소 할 방안으로 클라우드 보안 가시성 기반 보안플랫폼이 필요 합니다.

클라우드 보안 가시성 확보

보안 상태 관리(CSPM) 같은 가시화 도구를 통한 지속적인 모니터링으로 보안 사고 방지 가능

- 권한 및 클라우드 자원에 대한 직접적인 관리와 설정 제공
- 미흡한 설정으로 인한 구성 문제 해결

“보안플랫폼을 통한 해소”

새로운 기술에 대응

Full-managed 서비스에 대한 보안관리가 가능한 클라우드 워크로드 보호 플랫폼(CWPP)으로 새로운 자원에 대응 가능

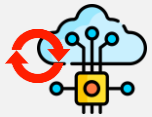
- 매년 수많은 신규 클라우드 기술과 서비스 출시
- 새로운 자원에 맞는 보안 고려 필요

Ⅲ LS First Security (LS FS)

- LS ITC 보안 플랫폼 ‘LS FS’
- LS FS 주요 구성
- LS FS 주요 기능
  - Ⅰ. 클라우드 보안정책 제공
  - Ⅱ. 클라우드 보안 현상 가시화 및 모니터링
  - Ⅲ. 클라우드 보안 운영 업무 지원

LS ITC 보안 플랫폼 'LS FS'

LS FS 솔루션과 보안 MSP를 통해 지속적으로 클라우드 보안 모니터링 하며, 보안 경고를 통해 인시던트 처리 등 보안 업무를 운영합니다.

클라우드 보안 사고 원인		☑ Solution : LS FS
 기존 IT와 다른 클라우드 보안	"클라우드 환경에 적용할 수 있는 보안 정책이 마련되어 있지 않아요"	LS ITC First Security  클라우드 보안 정책 제공
 클라우드의 복잡성 및 변동성	"클라우드 인프라가 복잡해서 보안 문제를 확인하기 어려워요" "새로운 클라우드 기능이 나올때마다 보안 요소를 일일이 확인하기 어려워요"	 클라우드 보안 형상 가시화 및 지속적 모니터링
 담당 운영자들의 클라우드 이해도 부족	"조직 보안 목표와 수준을 어떻게 정하죠?" "클라우드 보안 문제를 어떻게 대응하면 좋을 지 모르겠어요"	 클라우드 보안 운영 업무 지원 (보안 MSP)

LS FS 주요 구성

LS FS는 상태 관리(CSPM)와 워크로드 보호(CWPP) 서비스로 구성되어 있습니다.

	클라우드 보안 사고 원인	워크로드 보호(CWPP)
정의	클라우드 기반 시스템 및 인프라에서 위험과 잘못된 구성을 지속적으로 모니터링 하는 “클라우드 보안 상태 관리”	서버, 컨테이너, 스토리지, DB 및 기타 워크로드에 대한 특정 보호를 사용하는 “클라우드 워크로드 보호 플랫폼”
운영 프로세스	 ※ CSPM의 Native Cloud 지원 여부 상이하며 LS ITC는 보안 MSP를 통해 지원	
역할	• 내부 정책 및 컴플라이언스 기반 자산설정 모니터링 • 보안 취약점 점검, 개선안 제공 • 워크로드 / 서버 / 스토리지 리소스 / DB / 컨테이너 보호 • 보안 경고 / 보안 인시던트	• 서버 영역에서 위협 탐지 후 보안 경고 생성 • 클라우드 보안 태세 관리 / 지속적 보안 평가 • 보안 권장 사항 및 점수 확인 / 거버넌스와 규정 준수

LS FS 주요 기능

LS FS의 주요 기능은 보안정책, 보안형상 가시화 및 모니터링, 보안운영 업무지원 입니다.

클라우드 보안 정책 제공

- LS First Security
- 정책 커스터마이징

클라우드 보안 형상 가시화 지속적 모니터링

- 보안 점수화
- 취약점 진단
- 개선안 제공

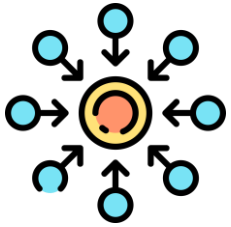
클라우드 보안 운영 업무 지원

- 클라우드 보안 경고 알림 및 조치
- 서버 상태 및 보안 모니터링 (secure OS 설정 및 보안 Agent)
- 개선사항 알림 및 월간 리포트 제공

LS FS 주요 기능_클라우드 보안 정책 제공

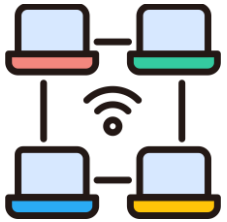
LS FS의 클라우드 보안정책을 통해 리소스 설정 상태를 지속적으로 모니터링 하여 보안 설정 오류를 예방 합니다.

중앙 집중식 정책 관리



- 환경 전체에서 유지 및 관리 보안 조건 정의
- 보안 정책 위반 리소스 식별 후 권장 사항으로 변환

다중 클라우드 적용 범위



- CSPM 인사이트 및 CWP 보호
- 에이전트 없는 method를 사용하여 다중 클라우드 환경에 연결

클라우드 보안 탐색기

- 클라우드 환경에서 보안 위험을 찾기 위한 쿼리 빌드

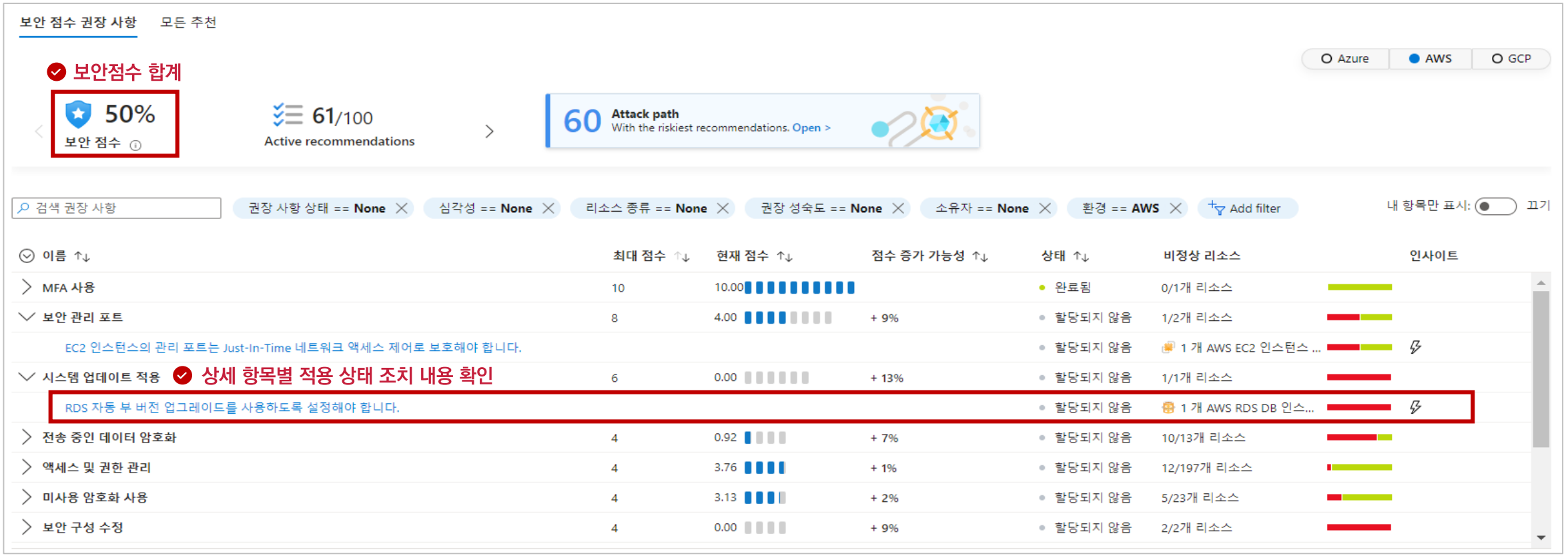
보안 거버넌스

- 리소스 소유자에게 작업 할당
- 보안 상태를 정책에 맞도록 진행 상황 추적
- 조직을 통해 보안 향상 추진

LS FS 주요 기능_클라우드 보안 형상 가시화 및 모니터링

LS ITC

LS FS의 CSPM 솔루션을 통해 리소스에 대한 보안 점수를 가시화하고 부족한 점수를 보충할 수 있도록 모니터링 합니다.



“Defender for Cloud는 리소스, 구독 및 조직의 보안 문제를 지속적으로 평가하여 현재 보안 상황을 한눈에 파악할 수 있도록 모든 결과를 단일 점수에 집계합니다.즉, 점수가 높을수록 식별된 위험 수준은 낮습니다.”

LS FS 주요 기능_클라우드 보안 운영 업무 지원

LS FS는 클라우드 보안 운영 업무에 도움을 드리기 위해 다음과 같은 서비스를 제공 하고 있습니다.

월간보고서

Power-BI 형태로 제공

- 권장사항, 경고, 조치사항 등에 대한 월간 레포팅

서버 Dashboard

Grafana

- 서버에 대한 퍼포먼스 및 Agent 대시보드
- Defender ATP에서 제공하는 Secure OS 룰 적용 현황 제공

LS FS 주요 기능_클라우드 보안 운영 업무 지원

LS FS는 클라우드 보안 운영 업무에 도움을 드리기 위해 다음과 같은 서비스를 제공 하고 있습니다.

보안 경고 알림

권장사항 알림

e-mail로 발송

- 보안경고 및 권장사항의 상세 내용 및 조치 사항에 대한 Alert 제공
- 관련 항목에 대한 Potal URL에서 디테일 항목 확인 가능

클라우드 보안의 시작 “LS FS”

LS ITC Cloud Center
T: 1688-6321
M: Cloud_msp@lsitc.com

별첨. Defender for Cloud

Defender for Cloud는 다양한 사이버 위협 및 취약성 으로부터 클라우드 기반 애플리케이션을 보호하도록 설계된 일련의 보안 조치 및 사례를 갖춘 CNAPP(클라우드 네이티브 애플리케이션 보호 플랫폼)입니다.

별첨. Defender for Cloud Architecture