국내 최초 Cloud SIEM

로그프레소 클라우드

LOGPRESSO

레거시 보안 솔루션은 클라우드와 SaaS 환경을 제대로 보호할 수 없습니다.

자산 및 취약점 현황 파악의 어려움

- 스마트폰 이용 증가, 컴퓨팅 리소스 동적 할당으로 어려워진 자산 및 취약점 현황 파악
- 업무 환경의 변화로 클라우드 및 SaaS의 감사 로그, NAC, 방화벽 정책을 실시간으로 통합하여 위협 현황 파악이 필요함

전사적으로 통합된 가시성의 부재

- 기존 온프레미스 보안 장비부터 SaaS, 클라우드 인프라 로그까지 모두 수집하는 것이 쉽지 않음
- 온프레미스, 클라우드, SaaS 전 영역에 걸쳐 데이터를 수집하여 전사적인 차원에서 위협을 탐지하고 대응해야함

부담스러운 시스템 구축, 유지 및 관리 비용

- 온프레미스 SIEM은 하드웨어를 포함한 억대의 예산과 시스템을 운영, 관리하는 전문 인력이 필요함
- 소규모 조직은 보안 모니터링 시스템 구축에 소극적

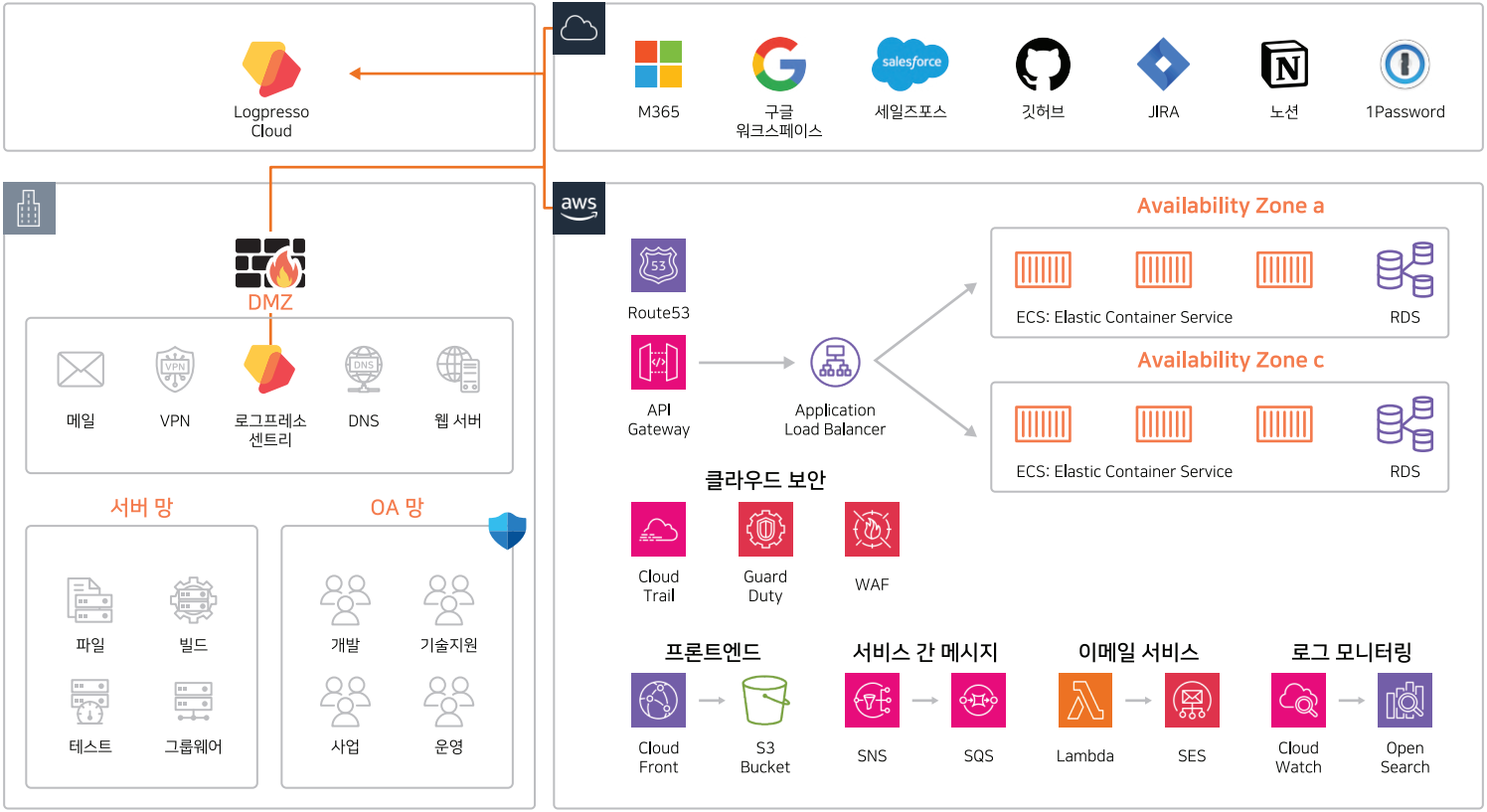
클라우드와 SaaS의 취약점을 이용한 대형 보안 사고의 발생 가능성

LAPSUS$ 공격 사례

다크웹, 텔레그램 등		VPN 사용		협업툴, 깃허브 등 SaaS, 클라우드 내 정보 활용
크리덴셜 구매	→	내부 시스템 접속	→	기밀정보 접근 및 탈취

하이브리드 업무 환경에는 클라우드 SIEM이 필요합니다.

컴플라이언스를 위한 온프레미스 방화벽·안티바이러스부터 업무에 활용하는 클라우드·SaaS까지 감사로그를 통합 모니터링할 수 있습니다.



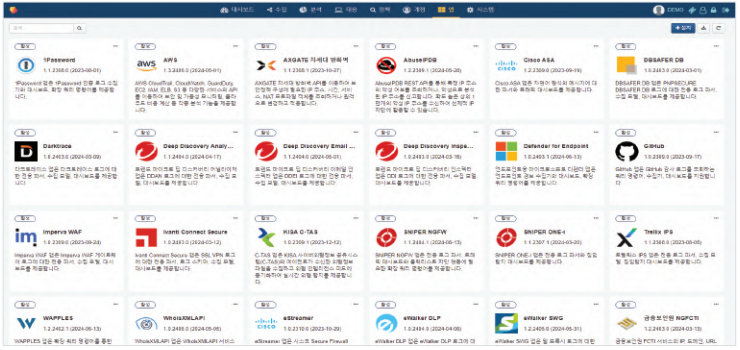
초기 스타트업이라도 서비스 운영에 필요한 성능 지표 및 애플리케이션 로그 모니터링과 함께 온프레미스 방화벽, 안티바이러스, AWS 보안로그, SaaS 감사로그 관제가 필수입니다.

로그프레소 클라우드는 국내 벤더 최초 클라우드 SIEM 입니다.

기업이 가장 많이 활용하는 Microsoft 365, Google Workspace, Microsoft Defender, GitHub, Notion, Microsoft Entra ID, 1Password 등 주요 SaaS와 AWS, Microsoft Azure, Naver Cloud 등 PaaS와 IaaS까지 통합 모니터링하고 위협 대응을 자동화할 수 있습니다.

앱 확장성

앱 설치만으로 써드 파티 서비스 및 장비의 데이터 통합과 연동이 가능합니다.



AWS WAF 자동 차단

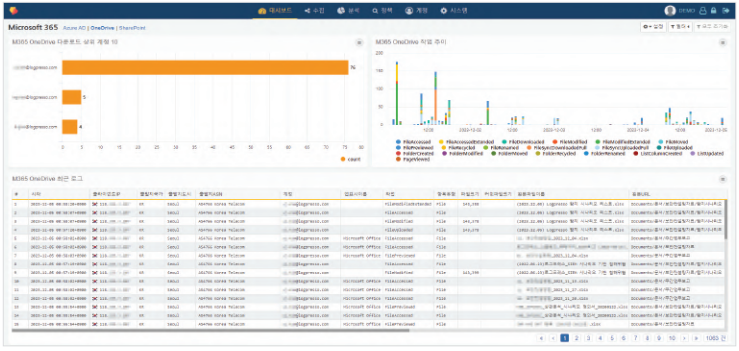
플레이북을 통해 위협 IP 평판 분석 후 자동으로 웹방화벽에서 차단합니다.

AWS 모니터링

CloudTrail, GuardDuty를 비롯한 RDS 감사로그, ELB, WAF 로그 모니터링이 가능합니다.

Microsoft 365 보안

OneDrive 파일에 대한 조회, 다운로드, 변경 등 이상징후를 모니터링합니다.



클라우드 환경에서의 ISMS 인증, 로그프레소 클라우드로 진행하세요.

정보보호 관리체계 인증을 위해 로그를 최소 6개월에서 1년 이상 장기간 보관해야 합니다. 로그프레소 클라우드 이용 시 글로벌 클라우드 SIEM 대비 비용을 50% 이상 절감할 수 있습니다.

ISMS

정보보호 관리체계 인증

ISMS-P

정보보호 및 개인정보보호 관리체계 인증

ISO27001

정보보호 관리체계 국제 표준

	로그프레소 클라우드	글로벌 D사
장기간 로그 보존	최대 2년 보관 지원(Basic 1년, Pro 2년)	최대 30일 보관 가능
장기 로그 분석	별도의 복원 작업 없이 과거 로그 즉각 분석 가능	S3 저장 로그 별도 rehydrate 작업 후 분석 가능
과금 형태	로그 장기 보관 시, 1GB당 1개월 저장 요금 100원 이하	30일 보관 시, 로그 100만 개당 USD 4.69
연동 가능 범위	클라우드, SaaS부터 온프레미스 솔루션까지 연동 가능	일부 클라우드, SaaS 서비스 한정
서비스 범위	LMS, SIEM, SOAR 및 디지털 포렌식	제한적 로그 저장 및 SIEM
보안 전문성	✓ LMS, SIEM, SOAR 전문 SecOps 기업	×
국내 리전 및 국내 CSP 지원	✓ 네이버 클라우드, 카카오 클라우드 지원 (AWS 지원 예정)	× (일본 리전)

로그프레소는 보안운영 (SecOps) 플랫폼 전문 기업입니다.

로그프레소는 빅데이터 원천 기술을 보유한 회사로, 통합로그관리(LMS), 통합보안관제(SIEM), 보안운영자동화(SOAR), 디지털 포렌식(DFIR) 솔루션, 위협 인텔리전스(CTI) 서비스를 제공합니다. 온프레미스부터 클라우드, SaaS 영역까지 완전하게 통합된 제품과 서비스를 제공하여 엔터프라이즈 환경에서 요구하는 높은 수준의 보안 운영을 지원합니다.

2013

- 2013. 03.14 이디엄 설립

2017

- BNK부산은행 통합로그 시스템 구축
- 기술혁신형 중소기업 인증 획득
- 특허 등록 (빅데이터 열 지향 처리 및 암호화)

2018

- 특허등록 (빅데이터 필드 인덱싱 방법)
- 조달청 나라장터 종합 쇼핑몰 등록
- KB국민은행 정보보호통합 플랫폼 구축
- LS전선 내부정보유출탐지 시스템 구축
- LG화학 인프라 장애 예측 시스템 구축

2019

- 시드 투자 유치 (우리은행)
- BNK부산은행 정보보호 통합 플랫폼 구축
- NH농협생명 통합정보보호 모니터링 시스템 구축
- NH농협손보 정보보호 통합 플랫폼 구축

2020

- 사명 변경 (주식회사 로그프레소)
- BNK시스템 그룹공동망 보안 관제 구축
- 특허 등록 (개인정보 유출 탐지 방법)

2021

- LG화학 AI기반 모니터링 시스템 구축
- BNK시스템 정보보호통합플랫폼 구축
- 삼성생명서비스 이상징후탐지시스템 구축
- 로그프레소 Log4j 취약점 스캐너 배포
- 로그프레소 미니 배포

2022

- 하나카드 정보보호모니터링 시스템 구축
- BNK캐피탈 SIEM 구축
- LG CNS 차세대 SIEM 구축
- 카카오 엔터프라이즈 SIEM 구축
- BNK경남은행 정보보호통합플랫폼 구축
- 한국재정정보원 차세대 보안관제 구축

2023

- 시리즈A 투자 유치 (KB 인베스트먼트, K2 인베스트먼트, CJ 인베스트먼트)
- 하나금융그룹 통합보안관제 구축
- LG CNS와 MDR 기술 및 사업협력 MOU 체결
- 로그프레소 소나 조달청 나라장터 등록
- 중소벤처기업부 스케일업 팁스 선정
- 로그프레소 클라우드 출시

2024

- 언어 모델을 활용한 보안관제시스템 운영 자동화 특허 등록
- 로그프레소 소나 4.0 GS인증 1등급 획득
- IITP 정보보호핵심원천기술개발사업 수주 (샌즈랩 컨소시엄)

로그프레소와 함께 더욱 정교해지는 위협으로부터 기업의 정보 자산을 지키세요.

로그프레소의 모든 제품은 서브스크립션을 통해 기능 확장이 가능합니다.

서비스

LOGPRESSO STORE　LOGPRESSO CTI　LOGPRESSO WATCH

SaaS

LOGPRESSO CLOUD

AWS 리전　네이버클라우드 리전　카카오클라우드 리전

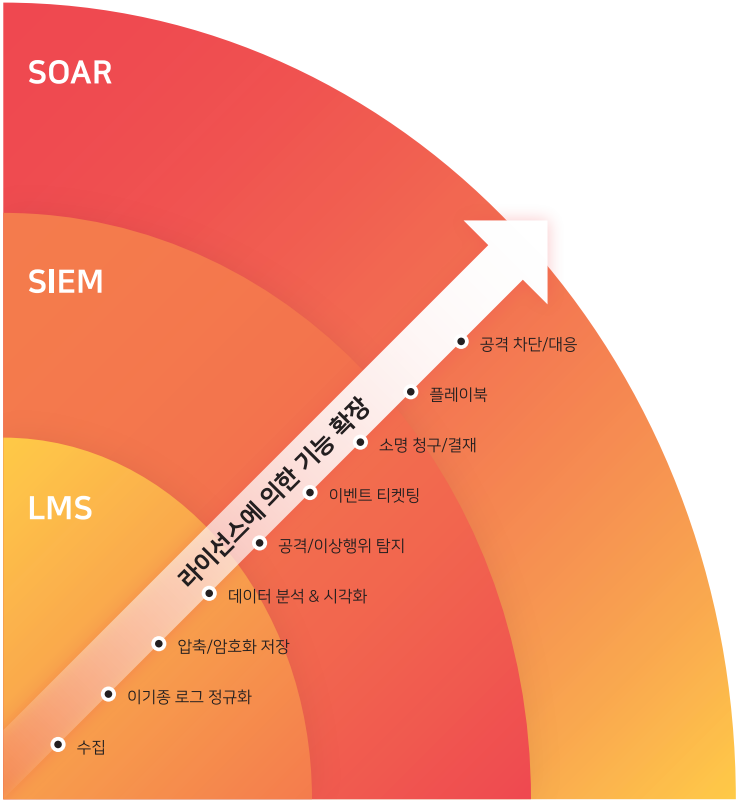
온프레미스

LOGPRESSO SONAR

통합로그관리 LMS　통합보안관제 SIEM　보안운영자동화 SOAR

디지털 포렌식

LOGPRESSO FORENSIC



200개 이상의 공공기관, 금융기관, 기업에서 로그프레소를 선택했습니다.

(주)로그프레소
서울특별시 마포구 새창로 7 9층