© 2020 SPLUNK INC.

Splunk Cloud

데이터를 위한 모든것 – Splunk Cloud Platform

박좌순 부장

Data Analytics Solution | 한컴MDS

2021.06

splunk> turn data into doing™

기억 하시나요?

100% 온-프레미스 IT

100% 영구 라이선스

100% 관리자 의존

클라우드 혁명을 목격합니다.

Splunk Cloud는 팀이 IT 관리에서 데이터를 가치로 전환하는 것에 이르기까지 보다 흥미로운 작업을 수행할 수 있도록 해줍니다.

splunk> turn data into doing™

© 2020 SPLUNK INC.

© 2020 SPLUNK INC.

멀티/하이브리드 클라우드 환경의 복잡성

Retain & Optimize

밀접하게 연결된 앱,
느린 배포 주기

Lift & Shift

대부분 Cloud IaaS

Re-Factor

더 많은 모듈,
종속 앱 구성 요소

Re-Architect / Cloud-Native

느슨하게 결합된 마이크로 서비스,
서버리스 기능

더 많은 모니터링 및 보안 서비스

확장된 공격 전반에 걸친 **더 많은** 데이터

더 많은 실패 지점과 예측 불가능

더 빈번한 릴리스 및 위험

© 2020 SPLUNK INC.

엔터프라이즈 SW를 사용하여 더 복잡하게 할 필요가 있을까요?

알맞은 Splunk 배포 옵션을 선택하여 시작하십시오.

Splunk Enterprise 플랫폼

온-프레미스 or Bring Your Own License (BYOL)

- 자체 퍼블릭 / 프라이빗 클라우드 또는 온 프레미스 인프라에서 Splunk 라이선스 실행
- Splunk 아키텍처 관리: 인프라, 검색 헤드, 인덱서 등
- 설치, 설정, 업데이트 및 업그레이드 담당

Splunk Cloud 플랫폼

Software as a Service (SaaS)

- 상시 가동되는 클라우드 지원 SaaS 제품 구독
- 4-6주마다 배포되는 새로운 기능
- Splunk가 아키텍처를 소유하고 관리하므로 Splunk를 사용하여 데이터 문제를 해결하기위한 더 많은 시간과 리소스
- 6년의 SaaS 전문 지식

활성 생산 환경	*총 클라우드 검색*	*가장 큰 테넌트*
>2500	**>1.45**	**>130**
SaaS Deployments	*Million per day*	*TB per day*

Splunk Cloud – 전세계 다양한 지역 지원

2020년 4월 서울 리전 정식 출시

splunk> turn data into doing™

Splunk Cloud Platform을 통한 비즈니스 성과 가속화

Reallocation
- 시간이 많이 걸리는 플랫폼 관리 작업 제거
- 가치가 높은 업무에 더 많은 시간 할당

Innovation
- 클라우드 네이티브 아키텍처 및 클라우드 지원 Apps'
- 배포 수일 vs. 수개월
- 가속화된 릴리즈

+

Security
- 엄격한 보안 및 컴플라이언스 표준 준수
- 2500+ 배포를 통해 획득된 지식 활용

Efficiency
- 최적화된 데이터 플랫폼
- 24x7 NOC & SOC
- 필요에 따라 100 TB+ 용량으로 확장

더 많은 다크데이터를 실제 실행 할 수 있도록 전환

재 할당된 시간과 내부 인력으로

클라우드상의 최대 속도와 규모로 실행

최신 Splunk 혁신 기술에 즉시 접근하여

더 빠른 위협 및 문제 해결 추진

최적화되고 상시 가동되는 데이터 플랫폼을 통하여

보안 침해에 대비

OOTB 보안 및 규정 준수를 통하여

© 2020 SPLUNK INC.

최소한의 리소스로 최대한의 효과

비즈니스 성과와 직접적으로 관련된 더 높은 가치의 작업에 집중

Customer Managed Splunk

35%

시간 단축
플랫폼 관리
(40% -> 5%)

시간 증가
고가치 사용 사례 작업
(20% -> 55%)

Splunk Cloud SaaS

- **High Value** use case delivery, adoption enablement, value realization
- Data and user onboarding
- Platform management

Note: metrics are based on 1000+ assessments with Splunk customers worldwide

© 2020 SPLUNK INC.

빠르고 유연한 서비스 – Cloud First !

추가 비용 없이 최신 Splunk 신기술 적용 가능

클라우드 데이터 스프롤 문제 해결, 대규모 데이터 라우팅, 스트림에서 ML 사용

새롭고 직관적인 인터페이스 통해 증가된 확장성, 가치 창출 시간 및 통찰력 경험

보안, IT 및 관찰 가능성을 위한 통합 클라우드 포트폴리오 통해 데이터 성숙도 경로 향상

SMLE 운영 인텔리전스 통한 휴먼 스케일 압도

Splunk Cloud 플랫폼에서 모든 데이터 비용 효율적으로 저장 및 유연한 탐색

스트림 처리

머신 러닝

경험 및 스케일

플렉스 인덱스 데이터 레이크

통합 보안, IT 및 관찰 가능성

클라우드에서만 제공되는 최신 Splunk 혁신

© 2020 SPLUNK INC.

업계 최고 수준의 보안 서비스 제공

엄격한 보안 및 규정 준수, 국제 표준 유지, 재해 복구 및 최신 보안 패치가 모두 처리

FedRAMP

HIPAA COMPLIANT

PCI

AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports

Information Security Management ISO 27001 Certified

© 2020 SPLUNK INC.

Splunk Cloud를 통한 효율적인 운용

splunk> turn data into doing™

© 2019 SPLUNK INC.

Splunk as a Service

세 단계로 끝!

1. 데이터 수집
2. 유저 등록
3. 데이터 → 인사이트 !

© 2019 SPLUNK INC.

Splunk Cloud Service Offering

- 초기 아키텍처 설정
- 커스텀 App
- 시스템 관리
- Splunk 업그레이드
- 아키텍처 업그레이드
- 모니터링
- 운영 관점의 보안
- 보안 인증
- Audit
- CMDB
- 설정 관리
- Git Repo
- 자동화
- SRE Administrators
- 변경 관리
- 다이나믹 아키텍처

© 2020 SPLUNK INC.

Splunk Cloud를 통한 관리 비용 절감

	Responsibility	On-Premises	BYOL	Splunk Cloud
Admin tasks: 일회성 설정 작업	HW 구매/대여	고객	고객	Splunk
	HW 장비 셋업(Rack, stack, cable, network 등)	고객	IaaS	Splunk
	Splunk 설치	고객	고객	Splunk
	OS 설치	고객	IaaS	Splunk
	Splunk 설정(사용자 생성, 앱 설치 등)	고객	고객	Splunk
	인덱서 설정	고객	고객	Splunk
	HA/클러스터링 설정	고객	고객	Splunk
	Disaster / recovery 설정	고객	고객	Splunk
	포워더 설정	고객	고객	Joint
	데이터 온보딩	고객	고객	Joint
	LDAP/AD 연동	고객	고객	Joint
Admin tasks: 지속적인 작업	HW 스케일업	고객	고객	Splunk
	Splunk 패치 / 업그레이드	고객	고객	Splunk
	OS 패치 / 업그레이드	고객	고객	Splunk
	배포 모니터링, health checks	고객	고객	Splunk
	포워더 관리	고객	고객	고객
	Users / roles 생성	고객	고객	고객
	인덱서 관리	고객	고객	고객
	추가 데이터 온보딩	고객	고객	고객
	서치헤더에 앱 설치	고객	고객	Splunk
	앱, 애드온 설치	고객	고객	Splunk
	프리미엄 앱 설치	고객	고객	Splunk
	데이터 Export	고객	고객	Splunk
User tasks	검색, 경고, 보고서, 대시보드	고객	고객	고객

75%이상의 인프라 관리/어드민 작업을 스플렁크가 대신 수행

고객은 보다 의미있는 데이터 인사이트 확보에 집중!

splunk> turn data into doing™

© 2019 SPLUNK INC.

Example of Value

여유 인원 활용을 통해 더 높은 가치의 업무에 집중

일반적인 **1TB** 온-프레미스 배포가 Splunk Cloud로 마이그레이션 되는 경우

2.5 온-프레미스 관리자

35% 시간 재할당

1820 시간 단축/연간

85 시간 작업/사용 사례

22 새로운 사용 사례/연간

$50K 가치/사용 사례 [1]

$1.1M
추가 비즈니스 가치 /연간

시간 단축

2.5 x 2080 hrs x 35% = 1820 hrs

재할당 리소스

1820 hrs / 85 hrs per use case = 22

비즈니스 가치 가속화

22 use cases x $50K per use case

[1] 전 세계 Splunk 고객과의 1000 개 이상의 평가 및 사용 사례 참여 기반

© 2019 SPLUNK INC.

EQUNIX

Technology - Security

- 데이터센터 사업 분야 세계 1위 선도 회사로, 전세계 211개 데이터 센서 보유
- 온-프레미스 기반 레거시 SIEM을 Splunk Cloud + Enterprise Security로 대체하여 50% TCO 절약
- 보안 인시던스에 30% 더 빠르게 대응
- 전체 인프라에 대한 운영 관점의 가시성 확보

© 2019 SPLUNK INC.

RAYMOND JAMES

On-prem to Cloud

- 금융 서비스를 제공하는 미국 투자은행
- 일주일만에 Splunk Cloud 배포 완료
- 검색 시간 98% 감소
- 보안, IT, DevOps 등 조직 전반에 Splunk 기반 분석 확대
- 직원들을 인프라와 툴 관리 대신 비지니스 관점으로 필요한 업무에 집중하도록 함으로써 효율성 증대 및 시간 절약

splunk>cloud

Splunk as a Service

최소한의 리소스로 최대한의 효과

"백엔드부터 구축하지 마세요."
이미 준비되어 있습니다.

빠르고 유연한 서비스

"단 2일만에 Go Live!"
빠른 확장이 가능합니다.

업계 최고 수준의 서비스 공급

"100% 업타임 보장"
업계 가장 엄격한 보안 준수

© 2019 SPLUNK INC.

한컴MDS & Splunk

Splunk 공인 교육

- 국내 유일 Splunk 공인 교육센터 & Splunk 총판
- Splunk 본사 공식 인증된 강사가 한국어로 교육 진행

Splunk 무료 교육

- 격월로 진행 (6월, 8월, 10월, 12월)
- 기존 고객은 담당 파트너에게 문의, 신규 고객은 아래 대표 메일로 신청

Splunk 관련 문의

- 홈페이지 : https://www.hancommds.com/splunk
- 대표 메일 : splunk@hancommds.com

Splunk 무료 다운로드

- 하루 500MB까지 무료 사용가능(60일), Splunk Cloud Platform (14일) (https://www.splunk.com/)

© 2019 SPLUNK INC.

Thank You

splunk> turn data into doing™