Splunk를 사용해 보안 운영을 개선하고 실용적인 통찰력을 얻는 Lenovo China

개요

고객과 파트너들은 신뢰할 수 있는 사용자 중심적인 기술과 탁월한 전문 서비스를 제공하는 Lenovo에 35년 넘게 의지해 왔습니다. 2018년 한 해에만 3422억 RMB(미화 510억 달러)라는 인상적인 수익을 창출한 이 글로벌 컴퓨터 대기업은 Fortune지 선정 2019년 글로벌 500 기업 명단에 22위로 등재되었고, 15개의 연구개발 센터와 180개 시장에서 일하는 57,000명이 넘는 직원을 고용하고 있습니다. Lenovo는 회사가 계속 확장됨에 따라 데이터 증가를 관리하고 회사 운영을 안전하게 보호할 효과적인 분석 도구가 필요했습니다. Splunk Enterprise 배포 후 Lenovo는 다음을 실현했습니다.

- 실시간 로그 관리로 비즈니스 민첩성 극대화
- 보안 모니터링을 개선하여 사고 대응 속도 향상
- 운영 효율 제고

대규모 보안

인프라 로그, 보안 소프트웨어 로그 및 애플리케이션 로그에서 데이터 스트림을 계속 수집하는 Lenovo China에서는 매일 2테라바이트의 데이터가 생성됩니다. 이처럼 분산된 데이터의 양이 끊임없이 증가하자 Lenovo는 팀이 보안 사고를 확인하고 사고에 대응하는 속도를 높이기 위해 믿고 사용할 수 있는 사전 모니터링 및 인텔리전트 분석 솔루션이 필요했습니다.

Splunk를 사용하기 전에 Lenovo의 보안 엔지니어들은 여러 시스템 로그에서 정보를 검색 및 상관한 후 결과를 통합하고 시각적인 형식으로 표시해야 했습니다. 노동력이 많이 필요한 이 프로세스에 엔지니어들은 많은 시간을 소모해야 했고, 그래서 문제 해결은 느리고 복잡했습니다. 예를 들어 바이러스 감염이 발생하면 엔지니어들은 여러 상이한 터미널 보안 플랫폼을 샅샅이 뒤져서 관련 세부 정보를 찾은 후 모든 데이터의 상관 관계를 수동으로 분석해야 했습니다.

확장이 용이한 로그 관리 및 보안 분석 플랫폼을 찾아 나선 Lenovo는 Splunk의 효율성과 경제성을 평가한 후 안정성 및 성능과 시스템 개발을 간소화할 수 있는 능력 때문에 Splunk Enterprise를 최종적으로 선택했습니다.

Lenovo 联想

산업

- 기술

Splunk 이용 사례

- 로그 관리
- 보안 & 사기탐지

도전과제

- 유연하지 않고 수작업 로그 분석으로 초래된 낮은 데이터 가용성
- 효과적이지 않은 데이터 모니터링 및 사고 대응
- 보안 운영을 지원하기 위한 시스템 간 데이터 상관 부재
- 분산된 IT 데이터의 비효율적인 관리 및 검색

비즈니스에 미치는 영향

- 실시간 자동 로그 관리로 보안 운영 개선
- 더 빠른 위협 예측과 시의적절한 사고 대응으로 신뢰성 제고
- 애플리케이션 개발 속도를 높이고 직원들의 시간을 더 효과적으로 사용하여 효율성 증대

데이터 소스

- 인프라 로그
- 보안 장비 로그
- 보안 소프트웨어 로그

Splunk 제품

- Splunk Enterprise

풍부한 시각화를 사용한 실시간 분석으로 의사 결정 개선

Splunk 덕에 Lenovo China는 광범위한 그룹의 워크플로를 간소화하고 생산성을 높였으며, 애플리케이션 및 보안 같은 팀은 더 민첩하고 효율적으로 일할 수 있게 되었습니다. Lenovo China는 Splunk를 사용하여 데이터 검색, 보고, 이상 경고 및 보안 모니터링을 개선할 뿐만 아니라 다양한 데이터 원본을 완벽하게 통합하여 정확한 실시간 데이터 검색과 중앙통제식 모니터링 및 분석에 사용할 수도 있습니다.

팀은 Splunk의 이해하기 쉬운 데이터 시각화를 사용하여 복잡한 데이터 집합을 실용적인 실시간 통찰력으로 효율적으로 변환할 수 있습니다. 이런 인텔리전트 분석을 통해 Lenovo는 데이터의 힘을 십분 활용하여 조직 전체에 걸쳐 실적을 높이고 데이터에 입각한 결정을 내릴 수 있게 되었습니다.

통합 데이터 상관으로 효율 제고 및 리소스 최적화

일상 업무의 효율을 높이고 보안을 강화하는 등, Splunk는 Lenovo China 전체의 IT 운영을 개선하는 데 중요한 역할을 했습니다. 전에 회사에서 오픈 소스 IT 모니터링 플랫폼을 사용했을 때는 작업을 개발하고 통합하는 데 기술 직원이 2명 이상 필요했기 때문에 상당한 시간과 공동 작업과 부서 간 커뮤니케이션이 요구되었습니다. Splunk는 로그를 하나의 플랫폼에 취합하고 상관 및 분석하여 이런 지루한 작업을 없앴고, 그러자 직원들은 보다 전략적인 목표에 시간을 할애하면서 비용을 절약하고 내외부의 잠재적인 위협으로부터 회사를 더 효과적으로 보호할 수 있게 되었습니다.

> "스마트하고 성능이 안정적인 **Splunk** 솔루션을 사용하면 원시 데이터에서 바로 상세 분석과 효과적인 보안 관제에 적용할 수 있는 데이터를 추출하여실시간 운영 통찰력을 얻을 수 있습니다. **Splunk**를 선택해서 만족스럽고, 앞으로 **Splunk**와 파트너 관계를 더 발전시킬 수 있기를 기대합니다."
>
> — Yu Sheng Li, IT 보안 이사, Lenovo China

클라우드 여정을 선도하는 Splunk

Lenovo는 클라우드 마이그레이션 여정에서 Splunk를 사용해 한 차원 더 높은 성공을 거둘 수 있었습니다. Lenovo는 과거에 데이터와 애플리케이션을 공용 클라우드 컴퓨팅 환경으로 옮길 때 배포 문제를 해결할 수 없었습니다. 이제 Lenovo는 Splunk의 신뢰할 수 있는 기술과 실시간 분석을 사용하여 발생하는 배포 문제를 빨리 해결하면서 공용 클라우드 로그를 수집하고 애플리케이션 보안 로그 작성을 간소화하는 일도 쉽게 처리할 수 있습니다.

Lenovo China는 Splunk에서 얻는 가치 있는 통찰력을 이용해 인텔리전트한 의사 결정을 비즈니스의 모든 부분으로 확장하여 경쟁 우위를 지속적으로 강화함으로써 미래 혁신을 실현할 것입니다.

Splunk를 무료로 다운로드 하거나 **무료 클라우드 평가판**으로 시작하십시오. Splunk 배포 모델은 클라우드, 사내 환경, 대규모 또는 소규모 팀 등 모든 환경의 요구사항을 충족합니다.

splunk>

자세히 알아보기: https://www.splunk.com/ko_kr/talk-to-sales

https://www.splunk.com/ko_kr

20-15687-SPLK-LenovoChinaImprovesSecurityOperations-103-CS