ATLASSIAN

지원 종료 소프트웨어 사용에 따른 보안 리스크 Top 5

결과 계산하기 – 데이터 침해에 따른 비용

지원 종료 소프트웨어를 사용할 경우, 그에 따른 위험 부담이 매우 크며 그 결과 사이버 공격과 잠재적 데이터 침해에 취약해진다는 것은 잘 알려진 사실입니다.또한 지원 종료 소프트웨어를 사용할 경우 회사 사용자들의 데이터와 개인정보에 보안 위협을 초래할 뿐 아니라 기업 실적에까지도 영향을 미칠 수 있습니다.다운타임에 따른 비용, 매출 손실, 복구에 들어가는 노력, 법적 비용 등은 사업에 장기적인 영향을 미칠 수 있습니다.실제로, 2022년에 IBM이 발간한 보고서에 따르면 데이터 침해에 따른 평균 비용은 무려 435만 달러에 달합니다.

서버 지원 종료 후 비즈니스를 안전하게 지키는 방법

Atlassian이 서버 제품에 대해 지원을 종료할 예정이라는 얘기는 들어 보셨을 겁니다.2024년 2월 15일 이후, Atlassian과 Marketplace 파트너들은 더 이상 서버 제품이나 앱에 대한 기술 지원이나 보안 업데이트, 또는 취약점에 대한 버그 픽스를 제공하지 않습니다.귀사의 비즈니스를 안전하게 지키려면 Atlassian 클라우드로 마이그레이션할 것을 강력히 권장합니다.

클라우드로 이동하는 것은 철저한 리서치와 리소스, 팀 내 정렬을 요하는 중대한 결정입니다.그리고 계획을 세우다 보면 지원 종료 서버 제품을 그냥 계속 사용하는 게 낫지 않을까 하는 유혹이 생길 수도 있겠지만 그것은 회사를 위험에 노출시킬 수 있는 선택입니다.CISA(Cybersecurity & Infrastructure Security Agency, 사이버보안 및 인프라 보안국)는 지원 종료 소프트웨어의 사용을 기업들이 어떠한 경우에도 반드시 피해야 하는 나쁜 보안 관행 1위로 꼽고 있습니다.

지원 종료 서버 제품 사용에 따른 보안 리스크 Top 5

빠르게 변화하는 오늘날의 디지털 환경에서 회사의 데이터 보안을 유지하는 것은 분명 가장 핵심적인 과제 중 하나일 것입니다.기술이 급속하게 진화하면서 악의적인 행위자들도 기업 소프트웨어의 취약성을 악용하기 위해 끊임없이 그에 맞게 전술을 바꾸고 있습니다.2022년에 발표된 Forrester 보고서에 따르면 이는 외부 사이버 공격의 주요 원인입니다.지원이 종료된 서버 제품과 앱에 의존할 경우 다음과 같이 불필요하고 예방 가능한 리스크에 노출되는 결과를 가져오게 됩니다.

#1: 취약점에 패치를 적용하지 않을 경우 기업이 보안 위협에 노출됩니다 – 2월 15일 이후부터는 서버 제품에 대해 더 이상 보안 패치와 업데이트가 제공되지 않으며 그에 따라 회사가 잠재적 보안 리스크에 노출되게 됩니다.패치나 업데이트가 없으면 취약점에 대한 대응이 이루어지지 않기 때문에, 악의적인 행위자들의 표적이 되기 쉽고, 이들이 회사 데이터와 시스템에 쉽게 무단 액세스할 수 있습니다.지원 종료 소프트웨어를 사용할 경우 리스크만 높아지는 것이 아니라 IT 팀에 추가적인 부담을 안겨주게 됩니다.Atlassian의 지원이 없으면 회사의 성장과 성공을 추진할 수 있는 전략적 이니셔티브에 투입해야 할 시간과 노력을 제품을 관리하고, 문제를 해결하고, 보안을 유지하는 데 할애해야 할 수 있습니다.

비즈니스를 안전하게 지키기 위해 할 수 있는 일

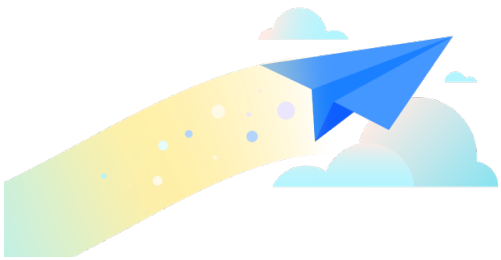
저희는 귀사 조직을 안전하게 지키는 것이 얼마나 중요한지 잘 알고 있습니다.비즈니스를 안전하게 보호하려면 클라우드 플랫폼 기반 자체에 데이터 보호 기능이 내재되어 있는 Atlassian 클라우드로 마이그레이션하는 것을 강력히 권장합니다.그렇게 하면 Atlassian의 전문과들과 책임을 공유할 수 있기 때문에 귀사 직원들은 Atlassian Cloud 네이티브 기능을 활용해 데이터를 안전하게 지키는 것을 포함해 보안 이니셔티브 중 보다 전략적인 측면에 안심하고 시간을 투자할 수 있을 것입니다.

지원 종료의 의미

당사는 세계적 수준의 클라우드 플랫폼을 구축하기 위한 노력의 일환으로 서버 제품에 대한 지원을 중단하기로 결정했습니다.당사는 이러한 결정을 2020년에 발표했으며, 그 이후 새로운 기능 개발 및 서버 라이선스 판매 중단을 포함해 점차적인 지원 종료를 위한 수순을 계속해서 밟아오고 있습니다.저희는 2월 15일이라는 최종 기한이 다가오는 상황에서 이러한 최종 단계가 부담스럽게 느껴질 수 있다는 것을 이해합니다.좋은 소식은 아직 시간 여유가 충분히 있고, 마이그레이션에 도움이 되는 지원과 리소스도 제공해 드리고 있다는 점입니다.

서버 지원 종료에 대해 자세히 알아보기

지금 바로 Atlassian 팀에 연락 클라우드 여정을 시작해 보세요.귀사의 앱 포트폴리오를 검토하고, 비즈니스 케이스를 구축하고, 마이그레이션 계획을 수립할 수 있도록 도와드리도록 하겠습니다. 추가적인 전문성과 실무적 지원이 필요하신 경우 당사 네트워크 소속의 솔루션 파트너에게 문의하시기 바랍니다.또한 Atlassian 마이그레이션 프로그램 커뮤니티 그룹에 가입하시면 피어 및 전문가들로부터 조언을 받으실 수 있습니다.



#2: 개인정보 보호 및 컴플라이언스 요건의 위반 – 지원 종료 서버 제품을 사용할 경우 개인정보 보호와 컴플라이언스 요건 측면에서 심각한 결과를 초래할 수 있으며, 특히 의료서비스나 금융 등 규제가 엄격한 업종의 경우 더 큰 문제로 이어질 수 있습니다.이런 업종의 경우 민감한 데이터 보호와 고객 개인정보 보호를 위해 엄격한 장치를 마련해 두고 있습니다.지원 종료 소프트웨어를 사용할 경우 취약점 악용 리스크가 커지며, 그에 따라 규정 위반 상황이 발생할 가능성이 높아지고, 이는 법적인 문제와 금전적 불이익을 초래할 수 있습니다.

#3: 다운타임 및 잠재적 데이터 손실 – 또 하나의 잠재적 문제는 막대한 다운타임입니다.지원 종료 소프트웨어 사용 시 좋은 의도를 가진 개인과 악의적인 행위자가 모두 리스크를 초래할 수 있습니다.전자는 의도치 않게, 후자는 의도적으로 회사의 시스템에 지장을 초래함으로써 데이터 손실이나 조작을 일으킬 수 있으며, 심지어 시스템을 완전히 오프라인 상태로 만드는 상황에까지 이를 수 있습니다.그 결과 이러한 다운타임은 회사의 운영 효율성에 영향을 미칠 뿐 아니라 원활한 고객 지원을 제공하는 능력에도 지장을 줄 수 있습니다.

#4: 노후한 보안 기술 – 기술 지원과 보안 업데이트만 못 받게 되는 것이 아니라, 보안 기술 분야에서 첨단 기술도 놓치게 됩니다.이러한 기술 혁신을 이용하지 못할 경우 회사 시스템이 진화하는 사이버 위협에 점차 더 취약해지게 됩니다.

#5: 지원 종료 Marketplace 앱에서 오는 리스크 – 더 이상 기존 서버 라이선스로 새로운 앱을 구입할 수 없게 됩니다.앞서 언급했다시피, Marketplace 파트너들도 더 이상 기술 지원이나 보안 업데이트, 취약점에 대한 버그 픽스를 제공해 드릴 수 없기 때문에 보안 위협에 대한 취약성이 배가되는 결과로 이어집니다.