RSA ARCHER® THIRD PARTY SECURITY RISK MONITORING

타사 거버넌스 활용 사례

당면 과제

조직에서 디지털 혁신을 진행하는 동안 강력한 정보 보안을 필요로 하는 제품, 서비스 및 비즈니스 프로세스의 신속한 혁신을 촉진함에 있어 타사에 대한 의존도는 점차 증가합니다. 이러한 타사 중 상당수는 보안 의무가 포함된 정식 계약 관계에 있지만 그렇지 않은 타사도 있습니다. 또한 타사는 자신의 타사(추가 관련자라고도 함)에 의존합니다.

비즈니스 활동을 타사에 아웃소싱할 수 있지만 타사 관계에서 발생하는 위험은 조직의 몫으로 남습니다. 허용 가능한 범위 내에서 위험을 관리하려면 이러한 위험 및 타사 공급업체가 갖추고 있는 제어 수단을 파악하는 것이 중요합니다.

개요

RSA Archer® Third Party Security Risk Monitoring은 투명한 보안 측정, 분석 및 분석가 수준의 통찰력을 제공하여 타사 정보 보안 위험 관리 프로그램의 성능을 대폭 향상시킵니다. 또한 조직에게 가시성, 통찰력 및 타사 및 추가 관련자의 IT 위험 환경에서 실행할 수 있는 인텔리전스를 제공합니다. 조직에서는 독립 실행형 기능을 사용하여 각 타사의 보안 제어 수단의 효율성을 신속하게 진단하거나 질의 응답서 기반의 제어 진단을 보완하는 수단으로 활용할 수 있습니다.

RSA Archer Third Party Security Risk Monitoring 활용 사례는 각 타사의 IT 환경을 파악 및 분석합니다. 알고리듬은 AI(Artificial Intelligence)를 사용하여 다양한 타사 IT 자산에 대한 위험 대비 태세를 자동으로 진단하여 해당 타사가 정보 보안을 얼마나 잘 관리하는지 파악합니다. Third Party Security Risk Monitoring을 타사 위험을 모니터링하기 위한 독립 실행형 솔루션으로 활용할 수 있으며 보완적 RSA Archer 활용 사례와 함께 배포된 경우에는 보다 폭넓은 IT 및 타사 위험 관리 프로그램의 실행을 위한 기초로 활용할 수 있습니다.

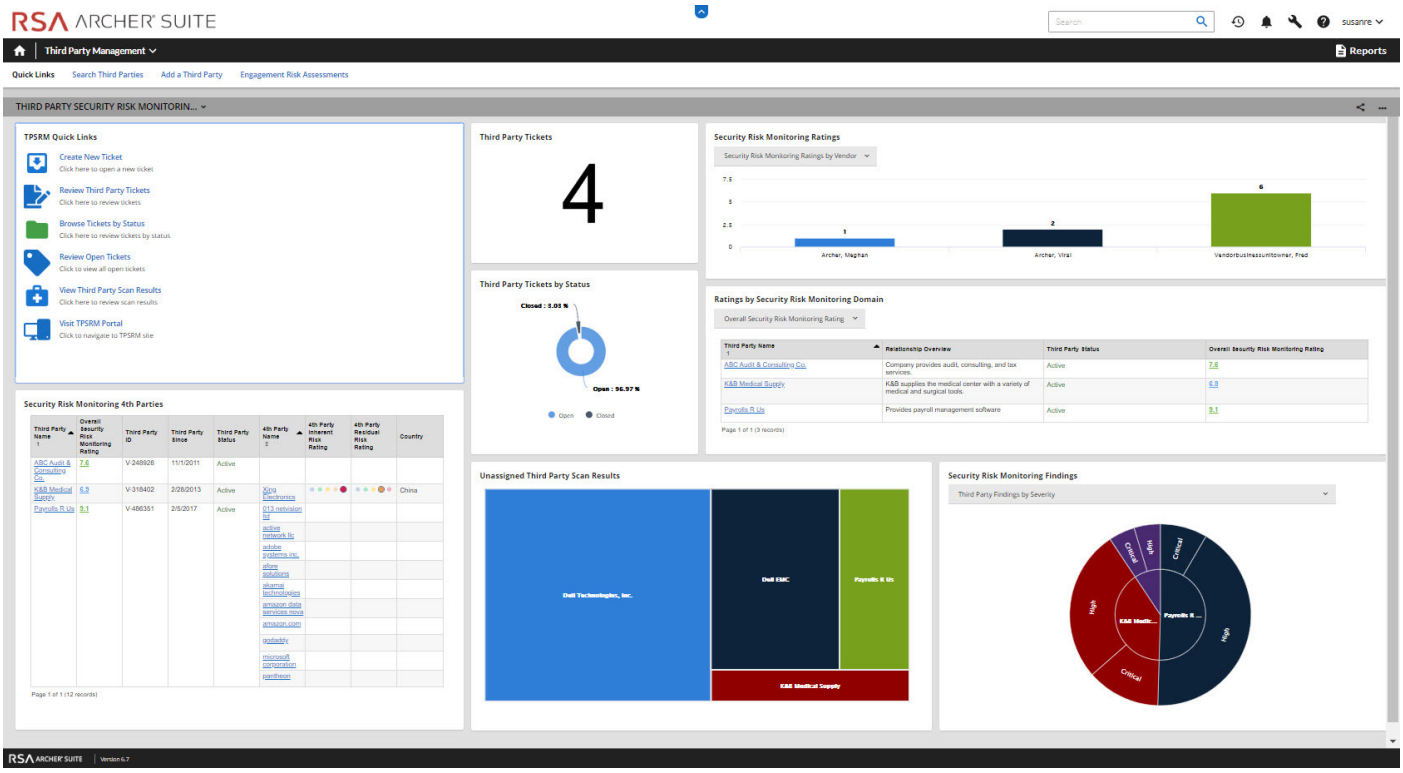
주요 특징

- 각 공급업체에 대해 실행 가능한 보안 문제 보기 제공
- 40개 이상의 보안 기준에 대한 잠재적 문제점 및 근본 원인 정확히 파악
- 필요 시 언제든지 조직의 보안 방식에 대한 진단 실행
- 규제 기관 및 표준 기관에게 높은 수준의 위험 제어 수단을 갖추고 있음을 입증
- 공급업체 포트폴리오 전체에 공통적으로 존재하는 문제점을 사전 예방적으로 파악

주요 이점

RSA Archer Third Party Security Risk Monitoring은 다음과 같은 이점을 제공합니다.

- 성능이 저하되어 정보 보안 침해로 이어질 수 있는 타사 제어 수단에 보다 신속하게 대응
- 타사의 보안 성능 및 IT 환경에 대한 객관적인 분석 정보 취득
- 위험도가 높은 타사에 대한 가시성을 향상하여 제한된 위험 관리 리소스를 할당
- 정확하고 실행 가능한 보안 성능에 대해 공급업체에게 알리고 개선 조치를 요구
- 공급업체의 보안 능력을 지속적으로 모니터링
- 분석 전문가의 업무 시간 및 외부 감사 리소스의 활용을 최적화



RSA 소개

RSA Archer® Suite는 조직이 광범위한 비즈니스 위험을 관리하면서 안심하고 디지털 기회를 추구하도록 지원합니다. 이 제품군은 비즈니스 중심의 보안 솔루션으로 구성된 RSA 포트폴리오의 일부로서 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 제공합니다. RSA는 전 세계 수백만 명의 사용자를 보호하고 있으며, Fortune지 선정 500대 기업의 90% 이상이 성공을 거두고 정보 변화에 지속적으로 적응할 수 있도록 지원하고 있습니다. 자세한 내용은 rsa.com/ko-kr을 참조하시기 바랍니다.