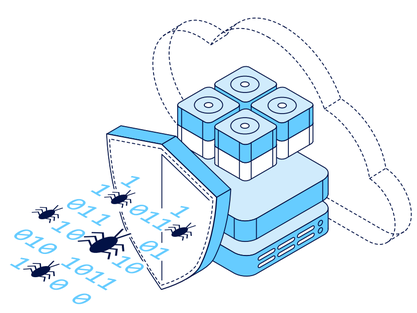
APJ 에디션

2022 랜섬웨어 트렌드 보고서

2022년 1월, 한 독립 조사 회사에서 **1,000**명의 편향되지 않은 IT 리더를 대상으로 환경 내에 랜섬웨어가 미친 영향과 완화 방법 및 미래 전략에 관한 설문조사를 실시했습니다. 응답자는 CISO, 보안 전문가, 백업 관리자 및 IT 운영이라는 4가지 집단 중 하나에 속합니다. 이러한 집단은 APJ, EMEA 및 아메리카 대륙의 16개 국가에 있는 모든 규모의 조직을 대변하며, 이 가운데 APJ 참가자는 **200**명입니다.

만연하게 퍼져 있는 랜섬웨어



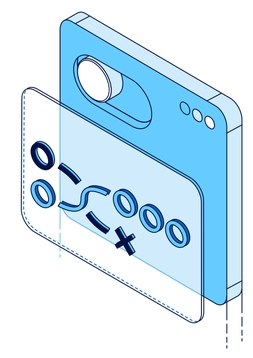
97%

백업 리포지토리 감염을 위한 랜섬웨어 공격이 시도되었고, 이 가운데 **73%**는 성공했음

52%

프로덕션 데이터가 암호화되었으며, 이 가운데 **68%**만이 복구가 가능했음

몸값 ≠ 완화



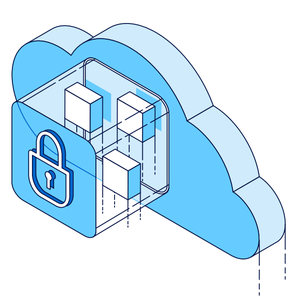
18%

조직이 몸값을 지불하기 않고 복구에 성공할 수 있었음

36%

조직이 몸값을 지불했지만 데이터를 복구할 수 없었음

생존을 위한 기술



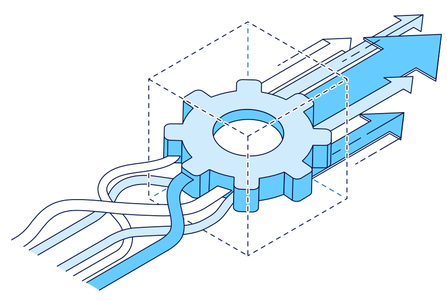
84%

복구 가능성 보장을 위해 백업 로그 또는 미디어 읽기 가능성에 의존하는 조직, **16%**만이 기능 복원 및 테스트를 통해 정기적으로 테스트

41%

랜섬웨어 공격 이후 데이터를 복구하기 전에 격리된 샌드박스로 처음 복원

조직적 연계



55%

백업과 사이버 보안 사이의 상당한 또는 전체적인 점검이 필요하다고 생각

29%

사이버 팀의 랜섬웨어 플레이북에 확인 또는 보장된 청결성 의무가 포함

안전한 백업은 최후의 방어선

랜섬웨어는 사고당 약 200만 달러의 비용을 발생시키는 재난입니다. Veeam®은 안전한 백업이 랜섬웨어에 대한 최후의 방어선이라고 생각합니다. Veeam의 소프트웨어는 안전을 염두에 두고 설계되어 독점 하드웨어에 대한 종속 없이 온프레미스와 클라우드 모두를 포함한 기존 아키텍처에서 사용할 수 있습니다. 안정적인 백업은 가동 중단 시간, 데이터 손실, 그리고 막대한 몸값 지불로부터 벗어날 수 있는 기회가 되기 때문입니다.

자세히 알아보기: **www.veeam.com**

여기에서 전체 조사 보고서 다운로드