APAC 에디션

THALES
Building a future we can all trust

2021 탈레스 데이터 위협 보고서

클라우드 전환 및 원격 근무가
가속화되는 시대의 데이터 보안

01

코로나19로인한 보안에 대한 새로운 문제점 대두

코로나19

코로나19의 여파로 원격 근무가 증가하면서 보안에 대한 요구가 높아지고 전략적 보안 지출에 대한 부분이 필요하게 되었습니다.

20%

의 응답자가 팬데믹 사태로 인한 보안 위험에 대해 준비되어 있다고 답했습니다.

83%

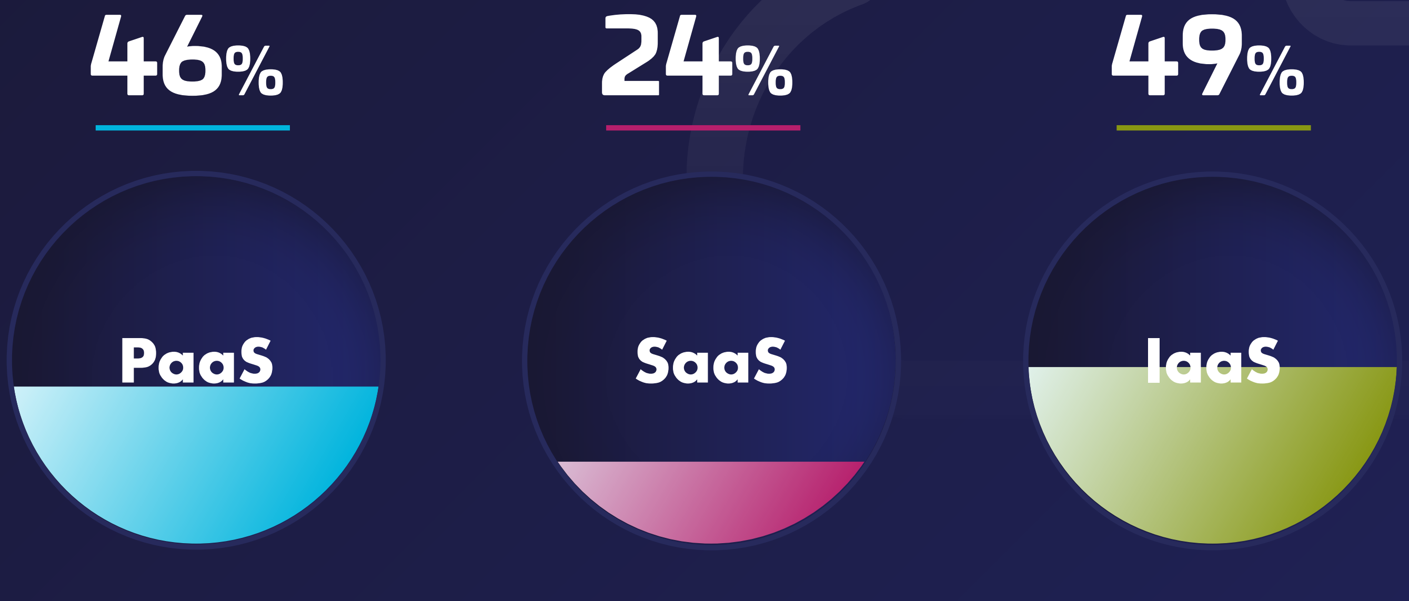
는 원격 근무로 인한 보안 위험/위협에 대해 우려하고 있다고 답했습니다.

44%

는 팬데믹 기간 동안 개인정보보호 및 보안이 가장 중요한 1순위 투자 대상이라고 답했습니다.

02

멀티클라우드 모멘텀이 기회를 창출하지만 또한 위험도 증대시키고 있습니다.



46% 의 응답자가 2개의 PaaS 제공업체를 이용하고 있습니다.

24% 의 응답자가 50개 이상의 SaaS 앱을 사용하고 있습니다.

49% 의 응답자가 2개의 IaaS 제공업체를 이용하고 있습니다.

56%

의 응답자가 데이터의 40% 이상을 퍼블릭 클라우드에 저장하고 있습니다.

50%

의 응답자가 외부에 저장한 데이터 40% 이상의 데이터가 매우 민감한 데이터라고 답했습니다.

48%

의 응답자가 클라우드에 저장된 거의 60% 이상의 민감 데이터가 암호화되지 않았다고 답했습니다.

83%

의 응답자가 클라우드에 저장된 50% 이상의 민감 데이터가 암호화되지 않았다고 답했습니다.

25%

응답자의 25%가 데이터가 저장된 장소를 정확하게 알고 있다고 응답

03

데이터 유출 및 보안 위협의 복잡성 증대

83%

의 응답자가 보안 위반에 대해 경험이 있다고 답했습니다.

45%

의 응답자가 지난 12개월동안 사이버 공격 증가를 목격했다고 보고했습니다.

57%

의 응답자가 멀웨어 공격 증가를 보았습니다.

48%

의 응답자가 랜섬웨어 공격 증가를 보았습니다.

04

점차 대두되는 Zero Trust 전략

34%

의 응답자가 공식 전략을 가지고 있고 적극적으로 Zero Trust 전략을 도입했다고 답했습니다.

65%

의 응답자가 Zero Trust 전략에 의지해서 클라우드 보안 전략을 수립하고 있습니다.

05

호라이즌 기반 위협: 퀀텀 컴퓨팅

50%

의 APAC 응답자가 퀀텀 컴퓨팅 보안 위협에 대해 큰 우려를 느끼고 있습니다.

이 정도의 인지 수준이면 포스트 퀀텀 암호 기술에 관심을 가지고 빠르게 암호화를 도입해야 합니다.

06

Zero Trust 세상을 위한 최신 데이터 보안

- 김감 데이터 검출
- 민감 데이터 암호화
- 암호키 관리
- 사용자 액세스 제어

후원사

SENETAS
versasec
KEYFACTOR
Canon
Canon Marketing Japan Inc.
NTT DATA
NTTデータ先端技術株式会社

451 Research 추천을 포함해서 전체 리포트를 다운로드하려면 cpl.thalesgroup.com/data-threat-report를 방문해 주십시오.

451 Research
S&P Global
Market Intelligence

출처: S&P Global Market Intelligence 소속 451 Research가 탈레스의 의뢰를 받고 실시한 2021 데이터 위협 보고서