

아시아 태평양 지역 보충 자료

2023 데이터 위협 보고서

디지털 주권 및 트랜스포메이션에
대한 관점과 경로

주요 연구 결과

이 보고서에서는 아시아 태평양(APAC) 지역에 초점을 맞춘 글로벌 데이터 위협 보고서(DTR) 연구의 주요 결과를 공유하고, 디지털 주권의 기회와 과제, 그리고 미래에 고려해야 할 사항에 대해 간략히 살펴봅니다. APAC 지역에서 나온 다수의 DTR 결과는 예상대로 글로벌 응답 결과와 매우 근접했지만, 중요한 차이점도 있었습니다.



우리는 그저 한낱 인간일 뿐이고,
클라우드 데이터
유출의 주된
요인은 바로 인적
오류라는 것입니다.

62%



이에 대응해 기업들은 오류를 방지하기 위한 사용자의 역량을 강화하고 있습니다. APAC 지역에서 MFA(Multi-Factor Authentication) 도입률이 전년 대비 6% 상승하여 62%로 증가했고, 응답자의 32%가 사이버 공격으로부터 중요 데이터를 보호하는 데 가장 효과적인 최고의 보안 기술로 ID 및 액세스 관리를 지목한 것에서 알 수 있듯이, 아시아 태평양 지역 내에서 인적 오류 방지에 대한 관심이 계속 높아지고 있습니다.

멀티 클라우드는 클라우드 성숙도에 관계없이 현실이 되었습니다.

APAC 지역 응답 기업 중 3/4 이상(80%)이 한 개 이상의 퍼블릭 클라우드에서 프로덕션 워크로드를 실행하고 있으며 조직마다 평균 2.3개의 클라우드 공급업체를 이용하고 있는 것으로 나타났는데, 이는 글로벌 응답 결과와 일치합니다.



내부 보안 태세가 개선되고 있음에도 보안 성과는 계속 뒤처지고 있습니다.

APAC 지역 응답자의 3/4 이상(80%)이 아직도 자사의 시스템으로 개인 데이터를 보호할 수 있다고 확신하고 있었는데, 이는 글로벌 응답에 비해 다소 낮은 수치입니다.



하지만 34%는 지난 12개월 동안 데이터 유출이 있었다고 답했습니다.

디지털 주권은 새롭게 떠오르고 있는 전략적 이니셔티브입니다.

96%

응답자의 96%가 다양한 수준의 디지털 주권을 달성하기 위해 데이터의 위치/관할 구역을 지정 또는 변경하거나 전체 데이터를 암호화하는 방법을 도입할 의향이 있다고 답했습니다

58%

또한, APAC 지역 조직의 58%는 최소 5개의 엔터프라이즈 키 관리 시스템을 보유하고 있어 복잡성이 가중되고 있다고 답했는데, 이는 글로벌 응답(62%)에 비해 약간 낮은 수치입니다.



클라우드에 내제된 위험에 대한 인식이 클라우드 도입률을 따라잡고 있습니다.

76%

APAC 지역 응답자의 76%가 5G 보안을 우려하고 있고, 대다수는 5G 네트워크에 연결되어 있는 사용자와 장치의 ID를 보호하는 것이 가장 큰 관심사라고 답했는데, 이는 글로벌 응답과 비슷한 결과입니다.



글로벌 응답자들은 사이버 공격의 표적 1, 2위로 클라우드 제공 SaaS와 클라우드 기반 스토리지를 각각 지목했습니다(각각 38%, 36%). APAC 지역 응답자 역시 응답 비율은 달랐지만(각각 43% 및 37%) 마찬가지로 두 표적을 지목했습니다.

랜섬웨어 대응과 관련해서는 엇갈린 결과가 나왔습니다.

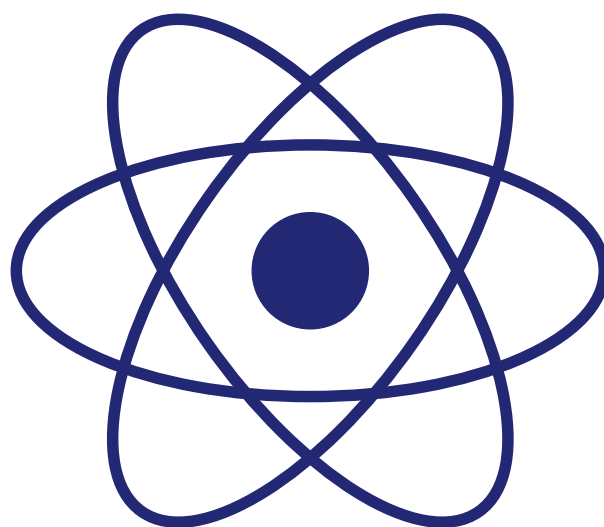


50%

APAC 지역 조직의 50%가 공식적인 랜섬웨어 대응 계획을 가지고 있다고 답했는데, 이는 첫 설문조사 결과였던 2022년의 47%에 비해 다소 증가한 수치입니다. APAC 지역 응답자의 약 1/4(23%)이 랜섬웨어 공격을 경험했다고 밝혔는데, 이는 글로벌 평균보다는 약간 높고 2022년보다는 약간 감소한 수치입니다. 흥미롭게도 공격의 양은 크게 줄었지만 랜섬웨어 공격의 막대한 영향력을 언급한 응답은 APAC 지역과 글로벌 지역 모두 다소 증가했습니다.



23%



학계에서나 거론되던 양자 내성 암호(PQC) 기술이 현실 세계에 실현되고 있습니다.

60%

APAC 지역 응답자의 60%가 네트워크 암호 해독을 양자 컴퓨팅 보안의 최대 위협 요소로 지목했습니다.

변화하는 규정과 외부 사건으로 인해 데이터 보안 대응력이 필요해질 것입니다.

82%

APAC 지역 응답자의 82%는 데이터 주권 및 개인 정보 보호 규정이 자사의 클라우드 배포 계획에 영향을 미칠까 봐 매우 우려하거나 다소 우려하고 있는 것으로 나타났습니다. 절반 이상(58%)이 개인 정보 보호 및 데이터 보호 규정을 클라우드 환경에서 관리하는 것이 온프레미스 네트워크에서 하는 것보다 더 복잡하다는 데 동의했는데, 이는 글로벌 응답 비율보다 약간 높은 수치입니다.

디지털 주권에 대한 기대

디지털 주권에 기업들의 관심이 집중되고 있습니다. 디지털 주권이 있어야만 제품과 서비스에 사용되는 데이터와 하드웨어 및 소프트웨어에 더 많은 자율성을 확보할 수 있기 때문입니다. 이를 통해 기업은 개인 정보 보호법을 현지 사정에 맞게 적용함으로써 공개적으로 식별 가능한 중요 정보를 안전하게 보호하기 위한 거버넌스를 유지하여 전 세계의 다양한 개인 정보 보호, 데이터 보안 및 탄력성 규정을 준수할 수 있습니다. 또한, 디지털 주권은 기업에게 이해 관계자와 시민에게 더 나은 서비스를 제공하면서도 시스템과 아키텍처를 최적화할 수 있는 중요한 기회를 제공합니다.

APAC 지역 응답자의 3/4 이상(82%)이 데이터 주권, 그리고 클라우드 배포 계획에 영향을 미치는 개인 정보 보호에 대해 다소 또는 매우 우려하고 있는 것으로 나타났습니다.

따라서 기업들은 멀티 클라우드 데이터 보안 전략을 이해하고 절차를 간소화해야 합니다. APAC 지역 응답자의 82%는 다소 또는 매우 우려한다고 답했는데, 이는 글로벌 결과(83%)와 비슷한 수치입니다. 거의 모든 응답자(96%)가 클라우드/디지털 주권의 다양한 요구 사항을 충족하기 위해 데이터의 위치/관할 구역을 지정하거나 전체 데이터를 암호화하는 방법을 도입할 의향이 있다고 답했습니다.

82%

APAC 지역 응답자의 82%가 데이터 주권, 그리고 클라우드 배포 계획에 영향을 미치는 개인 정보 보호 규정에 대해 다소 또는 매우 우려하고 있는 것으로 나타났습니다.

57%

APAC 지역 응답자의 57%가 클라우드 공급자의 키 관리 도구와 암호 키를 사용하면서 자사의 데이터 주권을 제어하기 보다는 공급자에게 전적으로 의존하고 있는 상태라고 답했습니다.

APAC 지역 응답자의 절반이 넘는 57%가 클라우드 공급자의 키 관리 도구와 암호 키를 사용하면서 자사의 데이터 주권을 제어하기 보다는 공급자에게 전적으로 의존하고 있는 상태라고 답했습니다

서로 다른 운영/데이터 주권 요구 사항을 충족하기 위해서는 프로세스를 간소화하고 다양한 암호화 체계를 유연하게 적용할 수 있어야 합니다. 응답 기업의 절반이 넘는 57%가 암호 키 제어의 전체 또는 대부분을 클라우드 서비스 공급자에게 위임한 것으로 나타났는데, 이는 2022년의 59%보다 약간 감소한 수치입니다.

54%

간소화가 관건입니다. APAC 지역 응답자의 절반이 넘는 54%가 주요 관리자를 5~10명 두고 있어서 여러 클라우드에서 데이터를 일관성 있게 관리하기가 어렵고 비용도 많이 든다고 답했는데, 이는 2022년보다 9% 증가한 수치입니다.

기본에 충실할 것.

소비자, 파트너, 고객, 규제 기관 같은 다른 이해 관계자들과 협력하면 데이터 보안에 대한 동의를 보다 쉽게 이끌어 낼 수 있습니다. 데이터 보안 이니셔티브는 파격적인 방식으로 시작될 수 있기 때문에 새로운 협업 패턴이 필요합니다. 기업은 데이터 보호에 모든 이해 관계자를 참여시킴으로써 동적인 변화를 거듭하는 시장에서 보다 강력하고 유연한 제어 기준을 마련할 수 있습니다.

간소화가 관건입니다. APAC 지역 응답자의 절반이 넘는 54%가 주요 관리자를 5~10명 두고 있어서 여러 클라우드에서 데이터를 일관성 있게 관리하기가 어렵고 비용도 많이 든다고 답했는데, 이는 2022년보다 9% 증가한 수치입니다. 이는 APAC 지역 조직의 절반 이상이 클라우드에서 제공되는 키 관리 도구를 선택하면서 멀티 클라우드 조직의 수가 증가한 것이 원인일 수 있습니다.

디지털 주권은 기업에게 장/단기적인 기회를 제공합니다. 변화하는 데이터 규정으로 인해 보다 즉각적인 대응이 요구되고 있는 가운데, 데이터와 운영 및 소프트웨어 측면에서 단일 클라우드 공급자에 대한 의존성을 탈피한다면 새로운 클라우드 기술을 수용할 수 있는 기반을 마련하여 전략적으로 성장을 도모할 수 있습니다. 단일 클라우드 공급자로부터 탈피하여 더 많은 데이터 보안 제어권을 유지하는 기업은 보안 전략의 실행 가치를 극대화하면서 보안 환경을 보다 안정적으로 제어할 수 있습니다.

연구 소개

본 연구는 각 국가별 보안 및 IT 관리 전문가 2,889명을 대상으로 2022년 11월과 12월에 실시한 웹 글로벌 설문 조사를 기반으로 합니다. 설문 조사의 일반적 주제에 대한 지식 수준과 관련된 기준 외에도, 선별 기준을 통해 연간 수익이 미화 1억 달러 미만인 조직(일부 국가의 경우 수익이 미화 1억 ~ 2억 5천만 달러인 조직)과 제휴를 맺고 있는 응답자는 제외했습니다. 본 연구는 관찰 연구로 수행되었으며 인과 관계를 주장하지 않습니다. 7개 주요 아시아 태평양 시장(호주, 홍콩, 인도, 일본, 뉴질랜드, 싱가포르, 한국)의 888명 응답자에 초점을 맞춰 글로벌 연구 데이터를 추출했습니다.

S&P Global
Market Intelligence

출처: 탈레스의 의뢰로 S&P 글로벌 마켓 인텔리전스가 실시한
맞춤형 설문 조사 결과를 토대로 작성된 2023 데이터 위협 보고서

후원사



THALES
Building a future we can all trust

모든 사무실 위치 및 연락처 정보는
cpl.thalesgroup.com/contact-us를 참조하십시오.

cpl.thalesgroup.com/data-threat-report

