APAC 에디션

THALES
Building a future we can all trust

2022 탈레스 데이터 위협 보고서

하이브리드 근무, 랜섬웨어 및 클라우드 전환 가속화 시대의 데이터 보안 현황

#2022DataThreatReport

cpl.thalesgroup.com

서론

2년이 지난 지금에도 여전히 코로나 19 팬데믹은 전 세계 IT 팀에 계속해서 막대한 영향을 미치고 있습니다. 2022 탈레스 데이터 위협 보고서는 랜섬웨어, 제로 트러스트 보안 전략 및 클라우드 데이터 보안 트렌드 같은 주제와 관련된 인사이트를 바탕으로 이러한 영향을 여러 측면에서 살펴봤습니다. 이 보고서는 호주, 홍콩, 인도, 일본, 뉴질랜드, 싱가포르, 한국 등 APAC 지역 국가의 응답자들을 대상으로 합니다. 공공 및 민간 부문의 다양한 업종에 종사하는 중소기업 및 대기업 소속 응답자 876명의 답변 내용을 분석했습니다. 달리 명시되지 않는 한, 이 보고서의 '응답자'는 APAC 지역 응답자를 나타냅니다.

451 Research

S&P Global
Market Intelligence

출처: 2022 데이터 위협 맞춤 설문 조사(S&P Global Market Intelligence 내 리서치 그룹인 451 Research가 탈레스의 의뢰로 실시)

45%

APAC 응답자의 45%가 공격 횟수가 증가했다고 보고

77%

APAC 응답자의 77%가 조직을 믿고 자신의 개인 정보를 맡기겠다고 보고

목차

데이터 유출 사고율이 여전히 엄청나게 높은 상태

해마다 사이버 보안에 상당한 비용이 지출되고 있음에도 불구하고 데이터 유출 사고율은 여전히 엄청나게 높게 보고되고 있습니다. 2022년 보고서에서는 응답자의 절반(50%)이 보안 침해를 경험한 적이 있다고 보고했고, 이들 중 32%는 지난 12개월 동안 데이터 유출 사고를 경험했다고 답했습니다.

데이터 유출 사고율이 여전히 높은 한 가지 이유는 데이터의 위치 및 분류에 대한 정보가 부족하기 때문입니다. 2022년 설문 조사에서 데이터가 저장된 위치를 명확하게 알고 있다고 답한 응답자는 16%에 불과했고, 데이터를 완벽하게 분류할 수 있다고 답한 응답자도 23%에 불과했습니다. 데이터 유출 통지 프로세스가 세이프 하버(safe harbor) 역할을 하는지도 애매한 상태입니다. 데이터 유출 사고를 당한 사람의 62%가 도움을 얻을 수 없었다고 답했습니다. 마찬가지로 전체 미국 응답자의 61%가 암호화나 토큰화를 통해 세이프 하버를 얻을 수 없었다고 답했습니다.

APAC 응답자들이 보고한 데이터 유출

Q: 조직에서 데이터 유출이 발생한 적이 있습니까?

대상: APAC 응답자(n=876)

출처: 451 Research의 2022 데이터 위협 맞춤 설문 조사

32%

APAC 응답자의 32%가 지난 12개월 동안 보안 침해를 경험했다고 보고

16%

APAC 응답자의 16%만이 데이터가 저장되는 위치를 정확하게 알고 있다고 보고

"

APAC 응답자의 23%만이 데이터를 완벽하게 분류할 수 있다고 답했습니다.

보안 위협

응답자의 45%가 공격 횟수가 증가했다고 보고했습니다. 공격 증가를 경험한 응답자 가운데 58%는 랜섬웨어 공격이, 57%는 맬웨어 공격이, 45%는 DoS(Denial-of-Service) 공격이 증가했다고 답했습니다. 작년에는 응답자의 57%가 보안 공격 증가의 주요 원인 1위로 맬웨어를 꼽았고, 랜섬웨어는 47%로 2위를 차지했습니다. 랜섬웨어 공격이 빠르게 증가하고 있고 경제적 피해도 커지면서 조직이 데이터 유출을 감지하고 대응하는 방식 역시 계속 바뀔 것입니다.

공격이 증가하고 있음에도 불구하고 조직들은 여전히 보안 관련 신뢰를 유지하고 있었습니다. 응답자의 77%가 조직을 믿고 자신의 개인 정보를 맡기겠다고 답했습니다. 전 세계 모든 응답자의 경우, 그들이 속한 조직에 대한 신뢰도가 79%로 전반적으로 높게 나타났습니다.

위협 행위자의 순위를 매기는 투표에서 APAC 응답자의 75%가 내부의 우발적 오류를 가장 먼저 꼽았고, 그 뒤를 이어 73%가 자신의 이념을 전파하기 위해 공격을 감행하는 "해킹활동가"를 꼽았습니다. 국가 소속 해커와 같이 지정학적 목적을 가진 외부의 적이 69%로 3위를 차지했습니다. 또 다른 순위 투표에서 응답자의 34%가 최대 공격 대상으로 클라우드 스토리지를 꼽았습니다. 응답자의 31%와 28%는 각각 클라우드 데이터베이스와 온프레미스 웹 애플리케이션을 꼽았습니다.

랜섬웨어 계획 및 대응

2022년 설문 조사에서는 랜섬웨어 계획 및 대응에 새롭게 초점을 맞췄습니다. 대부분의 맬웨어에서 이뤄지는 "로우 앤 슬로우(low and slow)" 방식의 데이터 유출 공격과 비교해, 랜섬웨어는 공격의 속도와 심각도가 높아서 데이터 기밀성과 가용성 모두에 악영향을 미칩니다. APAC 응답자의 24%가 랜섬웨어 공격을 경험했다고 보고했습니다. 공격을 받은 사람 중 82%는 내부적/외부적 영향을 다소 받았다고 답했고, 24%는 상당한 내부적/외부적 영향을 받았다고 답했습니다. 응답자의 21%는 복구하기 위해 돈을 지불했거나 지불할 의사가 있다고 답했습니다. 더 우려되는 것은, 공식적인 랜섬웨어 대응 계획을 갖추고 있다고 답한 응답자가 47%에 불과하다는 사실입니다. 랜섬웨어 공격의 심각도와 속도를 감안할 때, 보안 운영 팀, 법무 팀, 고위 경영진 팀 등 다양한 이해 관계자들을 하나로 묶는 중앙 집중식 공식 계획을 최우선으로 해서 일관된 대응 전략을 마련해야 합니다.

불과

47%

응답자의 47%만이 공식적인 랜섬웨어 대응 계획을 갖추고 있다고 보고

계속되는 원격 근무 시대

많은 조직에서 작년에 직원을 대상으로 원격 근무를 확장했습니다. 원격 근무 직원의 보안 위험에 대한 우려는 2022년에도 계속되었는데, 33%가 "매우 우려됨", 47%가 "다소 우려됨"이라고 답했습니다. 전 세계적으로도 마찬가지 결과가 나왔습니다. 전 세계 응답자의 31%가 "매우 우려됨", 48%가 "다소 우려됨"이라고 답했습니다. 한편 직원의 안전한 근무를 효과적으로 지원하는 현재의 원격 액세스 보안 솔루션에 대한 태도는 개선되었습니다. 그들의 원격 액세스 보안 솔루션에 대해 응답자의 24%가 "매우 신뢰함", 34%가 "상당히 신뢰함", 26%가 "약간 신뢰함", 16%가 "전혀 신뢰하지 않음"이라고 답했습니다.

애플리케이션에 대한 원격 액세스와 관련된 질문에 APAC 응답자의 59%가 가상 데스크톱 인프라(VDI)를 사용하고 있다고 답했습니다. VPN 및 클라우드 기반 SSO(싱글 사인온)가 53%로 공동 2위를, 제로 트러스트 네트워크 액세스(ZTNA)가 38%로 3위를 차지했습니다. 이에 비해 전 세계 응답자의 경우 59%가 VPN을, 55%가 VDI를, 51%가 클라우드 기반 SSO를, 36%가 ZTNA를 꼽았습니다.

2022년에는 APAC 응답자의 80%가 원격 근무 직원의 보안 위험에 대해 "매우 우려됨" 또는 "다소 우려됨"이라고 답했습니다.

추진력을 얻고 있는 제로 트러스트 전략

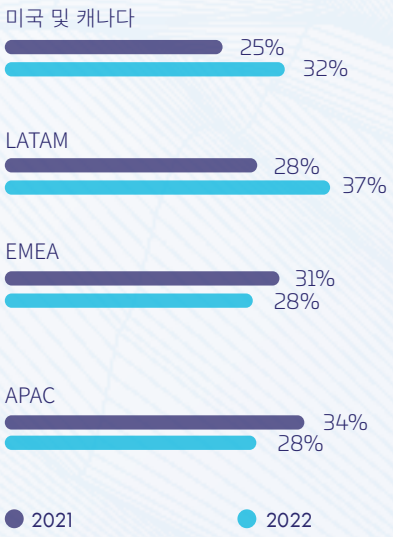
제로 트러스트의 원칙은 ID, 네트워크, 장치, 애플리케이션 및 데이터가 기존의 기업 네트워크 내에 더 이상 국한되지 않는다는 인식을 기반으로 합니다. 일반적으로 제로 트러스트 원칙에 따르면 ID, 네트워크 또는 데이터 세트 간에 암시적 수준이나 가정된 수준의 신뢰가 존재하지 않습니다. 따라서 경계 기반의 보안 접근 방식은 대체로 물리적 위치(예: 네트워크 데이터가 존재하는 위치)에 근거를 둔 시대에 뒤떨어진 '신뢰'라는 개념에 의존한다는 점에서 효과가 떨어집니다. 이와 달리, 제로 트러스트 접근 방식은 리소스에 대한 액세스 권한을 부여하는 핵심 수단으로 주로 ID를 활용합니다.

공식적인 제로 트러스트 전략을 갖추고 있다고 답한 응답자가 적은 것은 제로 트러스트 보안 전략이 너무 많은 분야를 포괄하기 때문일 수 있습니다. 2021년에는 응답자의 34%가 공식 전략을 갖고 있다고 보고한 반면, 2022년 응답자의 경우 공식 전략을 채택하고 있다고 답한 비율이 28%에 불과했습니다. 2022년 설문 조사 당시, 또다른 28%의 응답자는 아직 연구 단계에 있으며 공식적인 제로 트러스트 보안 전략을 개발할 계획이라고 답했습니다.

응답자의 48%는 전반적인 클라우드 보안 전략을 구축하기 위해 제로 트러스트의 "일부 개념"을 활용했다고 답했고, 또다른 30%는 제로 트러스트가 클라우드 보안 전략을 구축하는 데 "상당 부분" 영향을 미쳤다고 답했습니다. 이는 전 세계 결과보다 약간 낮은 수치입니다. 전 세계 응답자 중 47%가 제로 트러스트의 "일부 개념"을 활용하고 있다고 답했고, 34%가 제로 트러스트가 클라우드 보안 전략을 구축하는 데 "상당 부분" 영향을 미쳤다고 답했습니다.

공식적인 제로 트러스트 전략/정책을 갖추고 있다고 답한 응답자 비율

제로 트러스트 여정에서 어떤 단계에 있습니까?



대상: 전체 응답자(2,800명, "실행: 공식적인 전략을 갖추고 있으며 제로 트러스트 정책을 적극적으로 수용"을 선택한 비율 표시)

출처: 451 Research의 2021 및 2022 데이터 위협 맞춤 설문 조사

2022년에는 공식적인 제로 트러스트 보안 전략을 갖추고 있다고 답한 APAC 응답자가2021년에 비해 6%나 감소했습니다.

클라우드 모멘텀, 클라우드 적용 범위의 격차

전 세계 조직들이 점차 더 많은 양의 데이터를 클라우드에 저장하고 있으며, APAC 조직들도 예외는 아닙니다. 2021년 설문 조사에서는 응답자의 31%가 데이터의 41~50%를 외부 클라우드에 저장하고 있다고 답했고, 25%는 데이터를 50% 넘게 외부 클라우드에 저장하고 있다고 답했습니다. 2022년 설문 조사에서는 응답자의 51%가 데이터의 최소 40%를 외부 클라우드에 저장하고 있다고 답했고, 19%는 데이터를 60% 넘게 클라우드에 저장하고 있다고 답했습니다. 전 세계적으로는 응답자의 55%가 데이터의 최소 40%를 클라우드에 저장하고 있다고 보고했고, 23%가 데이터의 최소 60%를 클라우드에 저장하고 있다고 답했습니다.

보호 측면에서 격차는 점차 줄어들고 있습니다. 2021년 설문 조사에서는 응답자의 30%만이 클라우드에 저장된 민감한 데이터 중 41~50%가 암호화되었다고 답했고, 민감한 클라우드 데이터를 50% 넘게 암호화했다고 답한 응답자는 17%에 불과했습니다. 2022년에는 응답자의 48%가 민감한 클라우드 데이터의 최소 40%를 암호화했다고 답했고, 민감한 클라우드 데이터의 최소 60%를 암호화했다고 답한 응답자도 21%로 증가했습니다. 데이터 유출 사고율은 최근에도 여전히 높은 상태지만, 조금씩 개선되고 있습니다. 2021년 설문 조사에서는 응답자의 37%가 지난 12개월 동안 클라우드 데이터 및 애플리케이션과 관련해 데이터 유출을 경험했거나 감사에 실패했다고 답했습니다. 2022년에는 이 응답 비율이 33%로 다소 개선되었습니다.

클라우드 및 클라우드 퍼스트 전략의 성장에도 불구하고, 작년에는 응답자의 46%가 조직 내 온프레미스 네트워크와 비교해 클라우드 환경에서 개인 정보 보호 및 데이터 보호 규정을 관리하는 것이 더 복잡해졌다는 데 "동의" 또는 "매우 동의"한다고 답했습니다. 2022년에는 응답자의 51%가 온프레미스 환경보다 클라우드 환경의 개인 정보 보호 및 데이터 보호 규정이 관리하기 더 복잡하다는 데 "동의" 또는 "매우 동의"한다고 답했습니다. 또한, 2022년 전 세계 응답자 역시도 51%가 "동의" 또는 "매우 동의"한다고 답했습니다. 이러한 복잡성 문제 외에도 서로 다른 직책의 사람들이 클라우드 보안 전략을 시행한다는 문제가 있습니다. 2022년 설문 조사에서 APAC 응답자의 47%가 보안 팀이 중앙에서 정책을 정의하지만, 기술 표준을 정의하고 이를 시행하는 것은 개별 개발자나 애플리케이션 소유자의 몫이라고 답했습니다. 보안 팀이 중앙에서 정책과 표준을 정의하고 시행한다고 답한 응답자는 38%였습니다.

정책 정의 및 이행 이해 관계자

클라우드 보안을 위한 정책을 어떻게 결정 및 시행하고 있습니까?

- 중앙 보안 팀에서 정책을 정의하고 시행 — 38%
- 보안 팀에서 정책을 정의하고 클라우드 제공 팀에서 이행 — 47%
- 클라우드 제공 팀에서 정책을 정의하고 시행 — 15%

대상: APAC 응답자(n=876)

출처: 451 Research의 2022 데이터 위협 맞춤 설문 조사

33%

APAC 응답자의 33%가 지난 12개월 동안 클라우드 데이터 및 애플리케이션과 관련해 데이터 유출을 경험했거나 감사에 실패했다고 보고

대부분의 기업이 멀티클라우드 전략을 사용 중

설문 조사에 응한 조직의 대다수가 IaaS, PaaS, SaaS 등 모든 “유형”의 클라우드에서 여러 클라우드 제공업체를 이용하고 있는 것으로 보고하는 등 클라우드의 암호화 상태는 훨씬 복잡해졌습니다. 2022년 설문 조사 결과, APAC 응답자 가운데 AWS를 사용하는 비율과 Azure를 사용하는 비율이 거의 동일한 수준으로 나타났습니다. 생산 워크로드에서 응답자의 49%가 AWS를 사용하고 있다고 답했고, 43%가 Azure를 사용하고 있다고 답했습니다. 이는 2021년과 비교해 상당한 변화라 할 수 있습니다. 2021년에는 응답자의 53%가 AWS를 사용한다고 답했고, 46%만이 Microsoft Azure를 사용한다고 답했기 때문입니다. 예상대로 클라우드 사용 사례가 가장 다양한 분야는 SaaS였습니다. APAC 응답자 중 가장 큰 비율인 31%가 50개가 넘는 SaaS 애플리케이션을 사용한다고 답했고, 16%는 100개가 넘는 SaaS 앱을 사용한다고 답했습니다. 응답자 중 소수는 (3%) 500개가 넘는 SaaS 앱을 사용한다고 답했습니다. 더 많은 SaaS가 API 형식으로 제공되면서 클라우드의 사용 사례가 다양화될 것으로 예측됩니다. 이에 따라 여러 제공업체의 암호화 키 및 ID를 관리하는 것과 관련해 우려의 목소리가 높아지고 있고 문제도 발생하고 있습니다.

여러 클라우드 및 키 관리 옵션으로 인해 복잡성 증가

IaaS 및 SaaS의 다양성과 기존 온프레미스 인프라, 조직 전반에서의 일관된 제어를 요구하는 보안 규정을 감안할 때, 조직들이 암호화 솔루션과 키 관리 솔루션을 혼용하는 것이 놀랄 일도 아닙니다. 2022년 설문 조사 결과, APAC 지역 조직 가운데 5~7개의 개별 키 관리 제품을 사용한다고 답한 응답자 비율이 39%로 가장 많았습니다. 11%는 8~10개의 키 관리 제품을 사용한다고 답했습니다. 키 관리 소프트웨어, 하드웨어 보안 모듈, 자체 개발 솔루션, 스프레드시트 또는 플랫 파일을 보통 혼용하고 있었습니다.

조직들은 다양한 클라우드 제공업체 및 키 관리 기술을 이용하고 있을 뿐 아니라, 클라우드 제공업체의 암호화 및 키 관리 솔루션에 대한 제어 유형도 한 가지가 아니었습니다. 예를 들어 응답자의 절반 이상(59%)이 클라우드 제공업체가 암호화 키의 대부분 또는 전체를 제어하고 있다고 답했고, 34%는 조직이 클라우드 데이터용으로 배포된 암호화 키의 대부분 또는 전체를 제어하고 있다고 답했습니다. 2022년 APAC 응답자의 7%만이 기업이 키 생성 자료를 제어하고 클라우드 제공업체가 키 제어를 제공하는 '공유' 키 생성/키 제어 방식을 채택하고 있다고 보고했습니다.

클라우드 암호화의 동인

Q: 클라우드에서 암호화를 사용하는 위치와 방법을 결정하는 주요 요인은 무엇입니까?

- 내부 보안 아키텍처 결정(n=46) 46%
- 규정 준수 요구 사항(n=335) 38%
- 고객 또는 파트너 요구 사항 (n=104) 12%
- 기타 요구 사항 (n=31) 4%

대상: APAC 응답자(n=876)

출처: 451 Research의 2022 데이터 위협 맞춤 설문 조사

많은 클라우드 서비스 및 플랫폼의 경우, 데이터 암호화를 하나의 기능으로 제공할 수는 있지만, 근본적인 키 관리에 대한 강조 또는 이해가 부족하여 클라우드 데이터 보호가 한층 복잡해질 수 있습니다. 클라우드의 민감한 데이터를 최우선으로 생각하는 보안 기술이 무엇인지를 묻는 질문에 응답자의 61%가 저장 데이터 암호화를 선택했고, 53%는 다중 인증(MFA)을 선택했습니다. 키 관리는 51%로 3위를 차지했습니다. 조직들은 수많은 암호화 및 키 관리 솔루션을 총체적으로 파악하여 이행 및 안전의 격차를 파악할 때 더 좋은 결과를 얻을 것입니다.

39%

APAC 지역 조직의 39%가 5~7개의 서로 다른 키 관리 제품을 사용하고 있다고 보고

향후 전망

이번 설문 조사 결과는 APAC 지역 조직이 보안 여정에서 따라야 할 경로를 보여주는 지표 역할을 할 수 있습니다. 코로나 19 팬데믹을 통해 배운 중요한 교훈 중 하나는 보안 전략은 급변하는 세상에 대처할 수 있을 정도로 민첩해야 한다는 것, 또한 재택 근무와 클라우드가 모두 보안 환경에서 영구적인 고정 요소가 되어감에 따라 서로 다른 특성의 인프라, 애플리케이션, 데이터 및 사용자를 처리할 수 있을 정도로 유연성을 갖춰야 한다는 것입니다. 바로 이런 지점에서 제로 트러스트 접근 방식이 도움이 될 수 있으며, APAC 응답자들에겐 제로 트러스트를 보다 적극적으로 활용할 기회가 있습니다.

클라우드 컴퓨팅과 하이브리드 환경은 모든 이점에도 불구하고 상당한 복잡성을 기반으로 합니다. 이러한 복잡성은 보안의 적이 됩니다. 따라서 보안 제어와 보안 관리 모두를 클라우드로까지 확장하여 각각의 클라우드 환경이 고립된 채 운영되는 일이 없게 하고, 서비스 기반 제품군과 자동화 기술을 활용해 수동 작업의 부담을 줄여야 합니다.

클라우드 컴퓨팅과 하이브리드 환경은 상당한 복잡성을 기반으로 하며 복잡성은 철통보안의 적이나 다름없습니다.

설문 조사 소개

코로나 19 팬데믹은 전 세계 IT 팀에 즉각적이고 극적인 영향을 미쳤으며, 그 장기적 여파가 여전히 계속되고 있습니다. 2022 탈레스 데이터 위협 보고서 APAC 에디션은 코로나 19와 재택 근무 전략부터 양자 컴퓨팅에 이르기까지 다양한 이슈와 관련해 보안 전문가와 경영진을 대상으로 실시한 광범위한 설문 조사를 실시하여 코로나 19의 영향을 다양한 측면에서 살펴보았습니다. 2022 탈레스 데이터 위협 보고서는 APAC 지역의 응답자 876명을 포함해 약 2,800명의 보안 전문가와 경영진을 대상으로 한 설문 조사 결과를 바탕으로 작성되었습니다.

산업 부문

제조	157명
소매	154명
기술	127명
금융 서비스	120명
의료	115명
공공 부문	109명
소비재	107명
컴퓨터/전자/소프트웨어	106명
엔지니어링	104명
연방 정부	103명

산업 부문

1억 ~ 2억 4,990만 달러	162명
2억 5,000만 ~ 4억 9,990만 달러	802명
5억 ~ 7억 4,990만 달러	865명
7억 5,000만 ~ 9억 9,990만 달러	458명
10억 ~ 14억 9,000만 달러	254명
15억 ~ 19억 9,000만 달러	58명
20억 달러 이상	168명

THALES
Building a future we can all trust

연락처

모든 사무소 위치와 연락 정보는
cpl.thalesgroup.com/contact-us를 참조하세요.

cpl.thalesgroup.com/data-threat-report