CPL.thalesgroup.com #2020DataThreat

THALES

요약본
2020 탈레스 데이터 위협 보고서
아태지역판

서론

오늘날 기업들은 시장과 공급망의 붕괴로 이전에는 경험하지 못했던 새로운 문제들에 봉착해 있습니다. 기업들은 비즈니스 방식을 전면적으로 재검토하고 조정하며, 지금까지와는 완전히 다른 새로운 길을 모색해야 할 수도 있습니다. 비즈니스의 성공 여부는 클라우드, 모바일, 인공지능(AI), 머신러닝(ML) 및 사물인터넷(IoT)과 같은 디지털 트랜스포메이션(DX) 기술의 도입에 달려 있습니다. 디지털 트랜스포메이션은 기업들이 계속해서 진화하는 뉴 노멀(new normal) 시대에 적응하고, 포스트 코로나 시대를 대비하는 데 중요한 역할을 합니다. 2020년 6월 실시된 IDC COVID 기술 지수 조사에 따르면 보안, IoT 및 5G 기술 구입에 대한 관심은 높아지고, 기존 IT에 대한 지출 지수는 하향세로 나타났습니다.

> "응답 기업의 45%가 2020년도 보안 예산을 초과하여 지출할 것이라고 예상했습니다."

아태 지역은 다른 지역에 비해 디지털 트랜스포메이션에 아직까지는 뒤쳐져 있는 상황입니다. 하지만 다소 불리해 보이는 지금 상황은 오히려 아태 지역 기업들에게는 디지털 트랜스포메이션 전환을 가속화하여 비즈니스 혁신을 꾀함으로써 다른 지역을 뛰어 넘을 수 있는 전화위복의 기회가 될 수도 있을 것입니다. 실제로 IDC 조사 결과에 따르면 아태 지역의 일부 기업들은 이미 디지털 트랜스포메이션을 가속화하고 있습니다. 설문에 응한 아태 지역 기업의 1/4 이상(26%)이 시장을 공격적으로 혁신하고 있거나, 기업 민첩성을 높이기 위해 디지털화를 진행 중이라고 응답했습니다.

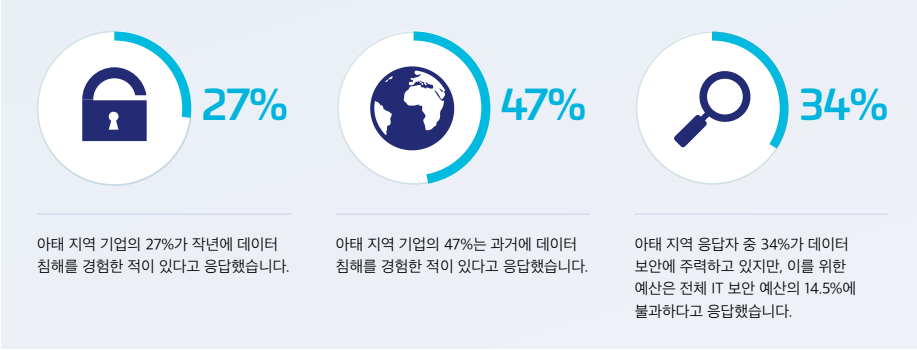
디지털 트랜스포메이션은 엄청난 혁신을 가져올 수 있으나, 한편으로는 데이터 보안을 위협하기도 합니다. 게다가 COVID-19로 인한 대대적인 재택 근무로의 전환으로 인해 보안의 어려움은 점차 가중되고 있습니다. 오늘날 비즈니스 혁신을 위한 디지털 트랜스포메이션 채택이 가속화되고, 팬데믹 이후 데이터 위협이 날로 증가되고 있습니다.기업의 보안팀은 전례없는 위협에 노출되고 있는 비즈니스 및 IT를 보호하기 위해 최대한의 노력을 기울여야 합니다. 재택 근무와 같은 트렌드에 발맞춰 기업들은 점차 방대한 양의 데이터를 클라우드에 저장하고 있습니다. 이러한 요인들로 인해 오늘날 데이터 보안 위협은 점점 높아지고 있으며, 아태 지역 기업들은 데이터 보안 구현에 있어 인력, 체계, 예산과 같은 기업의 리소스 부족이 상황을 더욱 악화시키고 있다고 응답했습니다.

한편, 아태 지역 기업들은 데이터 보안과 관련하여 현실을 제대로 파악하지는 못하고 있는 듯 보입니다. 응답 기업의 52%는 자신들이 보안 측면에서 매우 안전하다고 생각했지만, 실제로는 증가하는 데이터 위협에 대한 보안에 필요한 기술에 투자를 하는 등의 노력은 하고 있지 않습니다. 응답자의 절반 이상은 보안 침해를 겪었거나 보안 감사를 위반했다고 응답했습니다. 또한 클라우드 데이터 보안에 있어 대부분 기업들은 책임 공유 모델에서 클라우드 공급업체가 기업이 책임져야 할 부분까지 책임진다고 여기는 것으로 나타났습니다.

COVID-19 사태로 인해 아태 지역의 응답 기업들에게 있어 보안은 더욱 중요한 부분이 되었습니다. IDC의 "COVID-19가 IT 지출에 미치는 영향" 조사(2020년 6월 4일부터 15일까지 실시된 설문 조사)에서 응답 기업의 45%가 2020년도 보안 예산을 초과했을 것이라고 응답했고, 20%는 보안 예산에는 변화가 없을 것이라고 답했습니다. 확실한 것은 재택 근무로의 전환이 보안 지출에 실질적인 영향을 미쳤다는 사실입니다. 조사 대상인 아태 지역 국가 중 호주와 중국은 2020년도 보안 예산을 각각 50%와 47% 초과하였다고 보고했으며, 이는 아태 지역에서 가장 높은 수치를 기록하였습니다. 반면 뉴질랜드와 인도는 가장 낮은 수치를 기록하였습니다.

COVID-19 팬데믹은 보안 제품 뿐만 아니라 보안 구현에 필요한 인력에도 영향을 미쳤습니다. "1차 경제 회복기에 기업이 구축/재구축/채택해야 하는 가장 중요한 IT 기술은 무엇이 될 것 같습니까?"라는 IDC의 질문에 아태 지역의 응답 기업들은 공통적으로 사이버 보안을 꼽았습니다. 특히 호주와 인도네시아는 사이버 보안에 가장 주안점을 두었습니다.

데이터 위협의 확산



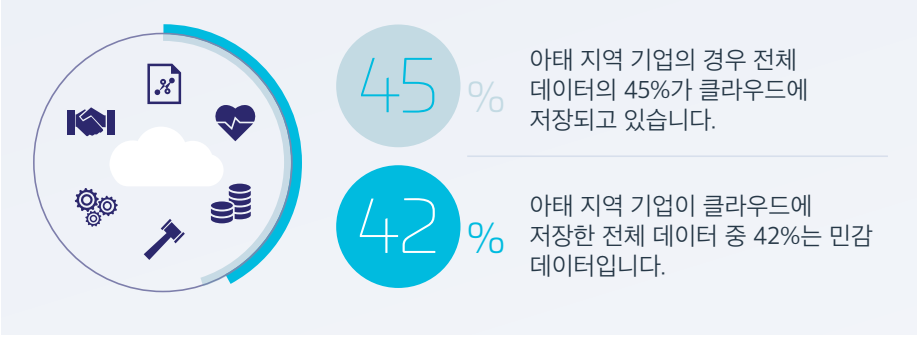
> "아태 지역 응답자의 27%가 작년에 보안 침해를 겪었다고 보고했고, 47%는 과거에 보안 침해를 경험했다고 답했습니다."

그림 1 - 데이터 위협의 확산

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

안타깝게도 어떠한 기업도 데이터 보안 위협으로부터 안전을 보장받을 수 없습니다. 특히나 COVID-19 팬데믹이 시작된 이후로 전 세계에서 보고되는 보안 침해 사례는 증가하고 있습니다. 조사 당시는 COVID-19가 발생하기 직전임에도 불구하고 아태 지역 응답자의 27%가 작년에 보안 침해를 경험했다고 보고했으며, 47%는 과거에 보안 침해를 경험했다고 답했습니다. 게다가 기업은 여전히 네트워크 보안 투자에 더욱 집중하고 있으며, 아태 지역 기업의 34%만이 데이터 보안을 위한 투자에 주력하고 있었습니다. 또한 데이터 보안이 전체 IT 보안 예산에서 차지하는 비중은 14.5%에 불과합니다(전 세계적으로 데이터 보안이 전체 IT 보안 예산에서 차지하는 비중은 15.7%).

클라우드에 저장된 민감 데이터 증가



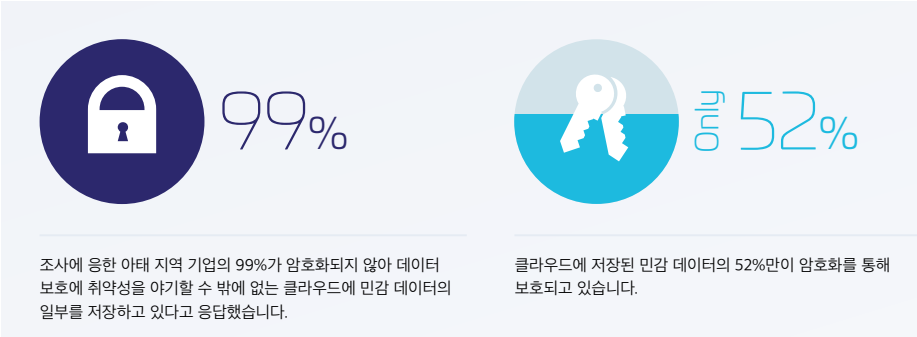
> "데이터의 45%가 클라우드에 저장되고 있으며, 클라우드 데이터의 42%는 민감 데이터입니다."

그림 2 - 클라우드에 저장된 민감 데이터 증가

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

조사에 응한 아태 지역 기업들은 클라우드에 민감 데이터의 일부를 저장하고 있었습니다. 응답 기업들은 데이터의 45%를 클라우드에 저장하고 있으며, 현 보안환경은 변곡점을 맞이하고 있다고 응답하였습니다. 이는 글로벌 수치인 50%보다는 낮은 수치입니다. 보다 중요한 것은 아태 지역 기업들이 클라우드에 저장하고 있는 데이터의 42%가 민감 데이터라는 사실입니다.

현재의 클라우드 보안 실태



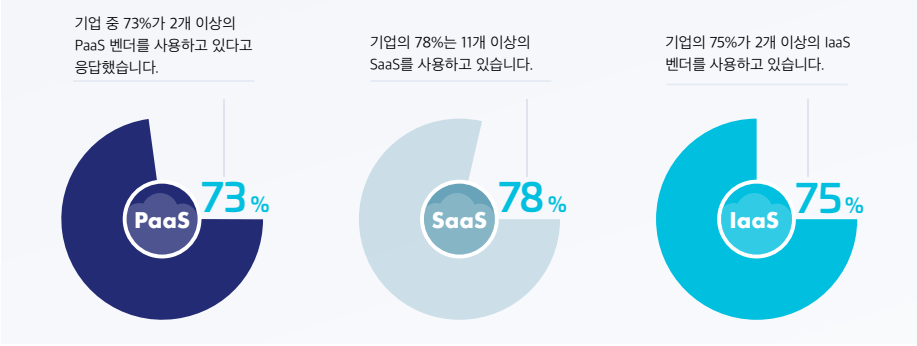
> "클라우드에 저장된 민감 데이터의 52%만이 암호화를 통해 보호되고 있습니다."

그림 3 - 현재의 클라우드 보안 실태

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

클라우드에 민감 데이터를 저장할수록 데이터 보안 위험은 증가합니다. 이렇듯 민감 데이터의 유출 위협이 심각함에도 불구하고 데이터 암호화 및 토큰화 비율은 여전히 낮습니다. 실제로 조사에 응한 아태 지역 기업의 99%는 암호화 없이 클라우드에 일부 민감 데이터를 저장하고 있다고 답했습니다. 클라우드에 저장된 민감 데이터의 52%만이 암호화를 통해 보호되고 있습니다.

멀티클라우드 시대



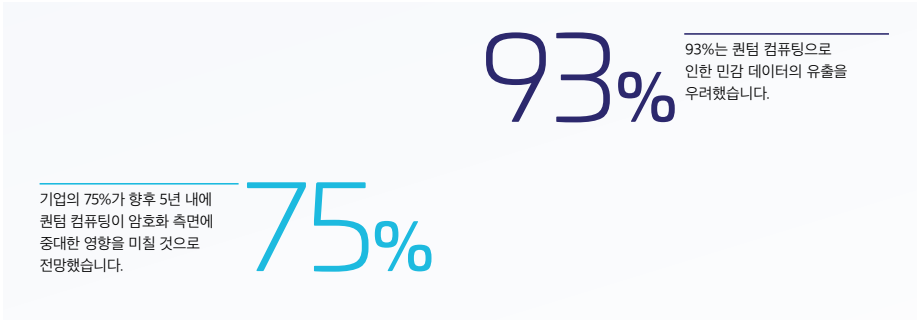
> "아태 지역 기업의 78%가 11개 이상의 SaaS를 사용하고 있습니다."

그림 4 - 멀티클라우드 시대의 도래

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

클라우드로 이전되는 데이터가 증가함에 따라 데이터 보안의 복잡성 역시 더욱 증가합니다. 이러한 복잡성은 멀티클라우드 보편화에 따른 IT팀의 주의 분산과 통합되지 않은 암호키 관리가 불러온 당연한 결과입니다. 아태 지역 기업의 73%가 2개 이상의 PaaS를, 78%가 11개 이상의 SaaS를, 75%가 2개 이상의 IaaS를 사용하고 있습니다.

퀀텀 컴퓨팅에 대한 대비



> "아태 지역 기업의 93%가 퀀텀 컴퓨팅으로 인한 민감 데이터 유출을 우려하고 있습니다."

그림 5 – 퀀텀 컴퓨팅에 대한 대비

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

퀀텀 컴퓨팅은 새로운 보안 위협이 되고 있으며, 데이터 보안의 책무를 더욱 가중시킬 것입니다. 퀀텀 컴퓨팅이 온라인화 되면 암호화 요구사항도 근본적으로 변화할 것입니다. 응답 기업의 75%가 향후 5년 내에 퀀텀 컴퓨팅이 암호화 측면에 영향을 미칠 것으로 전망했고, 93%는 퀀텀 컴퓨팅으로 인한 민감 데이터의 유출을 우려했습니다.

데이터 보호를 위한 제로 트러스트 도입

그림 6 - 데이터 보호를 위한 제로 트러스트 도입

출처: 2020 탈레스 데이터 위협 보고서, IDC 조사, 2019년 11월

더욱 방대하고 복잡해진 데이터 보안이라는 과제에 직면함에 따라 기업들은 보다 효과적인 전략으로 데이터 보안에 접근해야 할 필요가 있습니다. 아태 지역의 기업들은 클라우드 책임 공유 모델을 도입하고, 애플리케이션 및 네트워크에 접속하는 사용자 및 기기를 인증 및 검증하기 위하여 제로 트러스트 모델을 채택하는 한편, 강력한 데이터 검출 및 강화, 데이터 손실 방지 및 암호화 솔루션을 통해 데이터 보안에 대한 다양한 접근 방식을 취해야 합니다. 중요한 것은 데이터 보안이 유연한 프레임워크를 적용한 트러스트 모델 도입을 통하여 디지털 트랜스포메이션을 시도하려는 기업의 노력을 저해시켜서는 안 된다는 것입니다.

IDC 지침

- COVID-19 이후의 데이터 위험에 대비하기 위해서는 데이터 보안 솔루션, 특히 암호화 솔루션은 매우 중요합니다. 재택 근무로 인해 사무실 출근이 줄어들고 있는 현 상황에서는 더욱 그렇습니다. 회사에 출근할 때는 직원들이 자신의 기기를 가져와(Bring Your Own Devices) 업무를 수행하는 동안 방대한 양의 회사 데이터를 액세스 및 수정할 수 있었습니다.
- 회사 내부에서 클라우드로, 그리고 다시 회사 내부로 데이터가 이동하고 있고, 직원들이 사무실로 복귀할 수 있을지 여부가 불투명한 상황에서 COVID-19 이후의 IT환경 보안을 위해서는 새로운 데이터 보안 방법이 절실합니다.
- 또한 일반적으로 데이터 보안 및 사이버 보안이 기업의 운영과 비즈니스 성과에 영향을 미친다는 사실에 대한 명확한 이해가 필요합니다.
- 디지털 트랜스포메이션은 사이버 위협에 대해 탄력적으로 대처하는 것은 물론이고, 보안 사고가 발생했을 때 민첩하게 대응할 수 있어야 합니다.
- 책임 공유 모델 실현을 위한 최신 하이브리드 및 멀티클라우드 기반의 데이터 보안 툴에 투자하십시오.
- 데이터와 데이터에 액세스하는 사용자를 모두 보호할 수 있는 최소 권한 모델을 고려해 보십시오.
- 그리고 데이터 검출 솔루션과 중앙집중식 키 관리를 통해 데이터 보안을 강화하십시오.
- 규정을 준수할 수 있도록 엄격한 분류를 통한 검출 기능을 보강하십시오.
- 퀀텀 컴퓨팅이 암호화에 미치는 영향에 대해서도 대비하십시오.
- 통제 가능한 위협 벡터에 집중하십시오.
- SaaS 비즈니스 애플리케이션에서 데이터 보안 기능을 강화하십시오.

보고서 소개

이 보고서는 전 세계의 총 1,723명의 경영자가 조사에 참여했으며, 그 중 호주, 인도, 인도네시아, 일본, 말레이시아, 뉴질랜드, 싱가포르 및 대한민국을 포함한 아태 지역의 IT 및 데이터 보안 담당 경영자 500명 이상을 대상으로 실시한 조사 결과를 정리한 것입니다. 설문 조사, 보고 및 분석은 탈레스의 의뢰를 받아 IDC가 작성하였습니다.

보고서 전문은 cpl.thalesgroup.com/APAC-DTR 에서 다운로드 가능합니다.

탈레스 소개

개인 정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련하여 결정적인 순간에 직면하곤 합니다. 탈레스를 사용하면 결정적인 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 끊임없는 디지털 혁신이 가능합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.

후원사 여러분께 감사드립니다.

SENETAS

KEYFACTOR

PURESTORAGE

CSA cloud security alliance SM

OASIS Open standards. Open source.

Canon Canon Marketing Japan Inc.

netpoleon Network • Security

uniPoint

FIRST TECH

TI Safe

THALES

문의

모든 사무실 위치 및 연락처 정보는
cpl.thalesgroup.com/contact-us 를
참조하시기 바랍니다.

> cpl.thalesgroup.com <

cpl.thalesgroup.com/apac-data-threat-report

#2020DataThreat