cpl.thalesgroup.com

THALES
Building a future we can all trust

당신의 데이터, 남의 클라우드

클라우드의 이점을 누리면서 데이터 직접 제어하기

백서

목차

요약

오늘날 조직들에게 디지털 트랜스포메이션은 필수 과제가 되었습니다. 클라우드 서비스는 디지털 경제에서 성공을 거두기 위해 수행하는 조직의 포지셔닝 변경 속도를 높일 수 있는 입증된 경로를 제공합니다. 조직이 디지털 트랜스포메이션을 성공적으로 수행하기 위해서는 보안, 개인정보보호 및 규정 준수 목표를 달성해야 합니다. 이 백서에서는 클라우드 서비스 사용의 확대를 촉진하는 요소들과 조직이 충족해야 하는 중요한 보안, 개인정보보호 및 규정 준수 목표, 클라우드를 직접 제어하는데 필요한 핵심적인 보안 기능들에 대해 살펴보겠습니다.

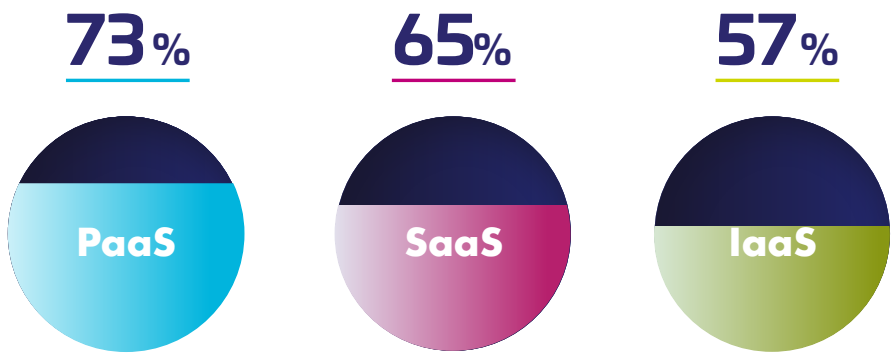
디지털 트랜스포메이션 목표를 달성하기 위해 클라우드 서비스의 확대가 반드시 필요

예나 지금이나 기업은 최적화된 고객 경험(CX)을 제공해야 합니다. CX의 최적화란 고품질의 디지털 경험을 일관되게 제공하여 사용자 기반을 만족시키는 것을 의미합니다. 기대치가 높은 고객들은 기대가 충족되지 않을 때 빠르게 이탈하기 때문입니다.

클라우드 서비스는 성공적인 디지털 트랜스포메이션의 기본 토대입니다. 그 어떤 접근 방식 또는 기술도 클라우드 서비스를 뛰어넘을 수 없습니다. 클라우드 서비스에는 퍼블릭, 프라이빗 및 하이브리드 형태의 IaaS(Infrastructure-as-a-Service, PaaS(Platform-as-a-Service), SaaS(Software-as-a-Service) 등이 모두 포함됩니다.

탈레스의 의뢰로 451 Research가 작성한 2021년 데이터 위협 보고서에 따르면, 전 세계 응답자의 73%가 PaaS 공급업체를 2개 이상 이용하고 있고 57%는 IaaS 공급업체를 2개 이상 이용하고 있으며, 65%는 SaaS 애플리케이션을 26개 이상 보유하고 있는 것으로 나타났습니다.[1]

1 2021년 탈레스 데이터 위협 보고서 https://cpl.thalesgroup.com/data-threat-report



PaaS 공급업체를 2개 이상 이용하는 전 세계 응답자 비율

26개가 넘는 SaaS 애플리케이션을 이용하는 전 세계 응답자 비율

IaaS 공급업체를 2개 이상 이용하는 전 세계 응답자 비율

클라우드 환경에서 중요한 보안 요구 사항

여러 형태의 클라우드 서비스가 대규모로 채택되면서 보안 임원이 복잡한 하이브리드 IT 환경을 관리해야 하는 문제가 발생하고 사이버 보안 및 규정 준수 요건의 충족이 까다로워졌습니다. 규정 준수를 보장하고, 사이버 위협을 퇴치하며, 특권 사용자가 야기한 위험으로부터 환경을 보호하는 것도 디지털 트랜스포메이션만큼 중요합니다.

규정 준수

최근 몇 년 동안 다양한 산업 분야의 조직들에 대한 규제 요건의 수가 늘어나고 범위가 넓어지고 있습니다. 대표 규제인 EU의 GDPR(European Union General Data Protection Regulation)에 이어 CCPA(California Consumer Privacy Act)와 브라질의 LGPD(General Data Protection Law)가 등장했습니다. 이러한 규제들은 시작에 불과합니다. 여러 국가의 입법부와 실무 그룹들이 개인정보보호를 보장하는 법안과 명령 제정의 최종 단계를 거치고 있기 때문입니다.

(클라우드에 보관되어 있더라도 데이터를 주권 경계 내에 유지한다는) 데이터 주권 규칙으로 인해 복잡성이 더욱 심화되고 있습니다. 2020년의 Schrems II 판결은 미국과 EU 간의 개인 데이터 전송을 규제하는 EU-미국 프라이버시 실드(Privacy Shield)를 무효화했습니다. 현재 전 세계 다국적 기업들은 규제 대상인 데이터의 반출을 허용하지 않도록 각별히 주의를 기울여야 하지만, 이것이 말처럼 쉽지 않습니다. Schrems II에 따르면 미국에 거주하는 직원이 유럽 시민과 관련된 민감 데이터에 액세스하는 경우, 이를 "반출"로 간주하기 때문입니다.

게다가 금융 서비스 기관들은 PCI DSS(Payment Card Industry Data Security Standard) 같은 글로벌 지침이나 퍼블릭 클라우드에서의 사이버 보안 위험에 대한 MAS(Monetary Authority of Singapore) 자문 같은 지역 지침을 포함해 여러 규칙들을 준수해야 합니다. 정부 기관은 FISMA(Federal Information Security Management Act) 같은 국가 규정을 준수해야 하고, 의료 기관들은 HIPAA(Health Insurance Portability and Accountability Act)를 준수해야 합니다.

사이버 공격으로부터 보호

갈수록 교묘해지고 집요해지는 사이버 공격자와 계속해서 증가하는 대규모 데이터 유출로 인해 클라우드로 서비스를 마이그레이션한 이후에도 계속해서 데이터 유출을 막아야 하는 상황이 되었습니다.

클라우드 인프라 보안은 CSP(Cloud Service Provider)가 주목하고 있는 영역이지만, 사이버 보안은 이들의 주된 사업 분야가 아닙니다. CSP를 위한 보안 제어 기능은 찾아보기 어렵기 때문에 간과하기 쉽습니다.[2] 클라우드 인프라는 크고 작은 조직들에게 갈수록 위협이 되고 있는 랜섬웨어 공격에 취약할 수 있습니다.

> "암호화를 통해 클라우드의 민감 데이터 대부분을 보호해왔다고 답한 기업은 17%에 불과했습니다."

IDC에서 발표한 보고서에 따르면, 응답 기업의 80%가 지난 18개월 동안 클라우드 데이터 유출을 한 번 이상 경험했다고 답했고, 10번 이상 경험했다고 답한 기업이 거의 절반(43%)에 달했습니다.[3]

클라우드 사용량이 계속해서 증가하고 있음에도 클라우드의 보안 수준은 나아지지 않았다는 것이 클라우드 데이터 유출의 주요 원인 중 하나입니다. 퍼블릭 클라우드의 사용량 증가에 발맞춰 로그인 액세스 지점에서 애플리케이션을 보호하고 암호화 같은 메커니즘을 통해 데이터를 보호하는 방법이 확대 적용되고 있지 않는 것으로 보입니다. 2021년 탈레스 데이터 위협 보고서에 따르면, 암호화를 통해 클라우드의 민감 데이터 대부분을 보호해왔다고 답한 기업은 17%에 불과했고, 어떤 형태로든 MFA를 구현했다고 답한 기업은 55%에 불과했습니다.

경쟁이 치열한 시장에서 데이터 유출이 발생할 경우, 조직은 벌금, 평판 하락, 고객 손실 같은 심각한 불이익을 받을 수 있습니다. 게다가, 이러한 데이터 유출로 인한 직접적인 비용 손실이 계속 늘어나고 있습니다. 한 글로벌 연구 조사에 따르면 데이터 유출로 인한 평균 비용 손실은 현재 424만 달러에 달하는데, 이는 전년도에 비해 10% 증가한 수치입니다.[4]

2 Wall Street Journal, "사람의 실수가 클라우드 데이터 유출의 주범"
3 Security Magazine, "기업의 약 80%가 지난 18개월 동안 클라우드 데이터 유출을 경험"
4 IBM, "Ponemon의 2021년 데이터 유출 비용 연구"

특권 사용자의 남용으로부터 보호

외부 사이버 공격으로부터 데이터를 보호하는 것은 필수 과제가 분명하지만, 이 외에도 해결해야 할 위험 요소들이 있습니다. 한 명의 불성실한 관리자로 인해 기업과 기업의 데이터가 심각한 위험에 노출될 수 있는 것이 현실입니다. 2021년 Verizon 데이터 유출 보고서에 따르면, "특권 사용자의 남용"이 지금까지 전 세계적으로 가장 흔한 사이버 공격 벡터인 것으로 나타났습니다.[5]

> "특권 사용자를 인증하기 위해 MFA(Multi- Factor Authentication)를 사용하는 기업은 48%에 불과했습니다."

특권 사용자는 조직의 가장 민감한 계정에 액세스를 할 수 있다는 점에서 가장 큰 위험 요소라고 할 수 있습니다.

게다가 실수로 포트를 열어두거나 방화벽이 제대로 구성되어 있지 않기만 해도 조직이 중대한 데이터 유출을 경험할 수 있습니다. 한 분석 업체는 향후 몇 년 동안 클라우드 보안 실패의 최소 95%가 고객의 잘못 때문에 발생할 것으로 추정했습니다.[6]

이러한 명백한 위험에도 불구하고 특권 사용자를 인증하기 위해 MFA(Multi- Factor Authentication)를 사용하는 기업은 48%에 불과했습니다. 설상가상으로 기업의 39%는 정책 기반 액세스, 클라우드 SSO(Single Sign-On) 인증을 제공하는 통합 시스템을 배포조차 하지 않았다고 답했습니다.[7]

우발적인 데이터 유출 방지

IT 인프라의 주요 부분을 CSP든 누구든 한 업체에게 아웃소싱하면 모든 데이터를 하나의 바구니에 담게 되어 보안에 위험이 발생할 수 있습니다. 때로는 바구니에 구멍이 나 있기도 합니다. 악성 공격자의 적극적인 해킹으로 인해 발생하는 데이터 유출 외에도, 구성 오류, 사용자의 오해, 운영 절차상의 황당한 공백으로 인해 수 많은 클라우드 보안 사고가 발생하고 있습니다. 안타깝게도 추상화 및 가상화 계층에 복잡성이 숨겨져 있기 때문에 이러한 문제가 클라우드와 관련해 심심치 않게 발생하고 있습니다. 단일 구성을 손쉽게 변경해서 보이지 않는 곳에서 액세스 권한을 탈취하는 경우도 있습니다. 운영이나 IT 보안에 경험이 없는 사용자가 클라우드를 배포하는 경우가 증가하면서 이러한 문제는 더욱 심각해지고 있습니다.

클라우드 보안의 장애물

이전 섹션에서 설명한 바와 같이, 규정을 준수하고 외부 사이버 공격, 내부 실수 및 남용을 방지하기 위해서는 클라우드 환경에 강력한 보안 통제를 구현해야 합니다. 클라우드 환경의 요구를 해결하는 과정에서 다음과 같은 문제가 발생할 수 있습니다.

1. 민감 데이터와 애플리케이션이 기업의 경계 밖에 상주하게 되면서 경계를 기반으로 하는 기존의 보안 접근 방식과 기술이 더 이상 적용되지 않습니다.
2. 오늘날의 하이브리드 환경은 복잡성을 가중시킵니다. 보안 팀이 기존의 온프레미스 환경과 증가하는 하이브리드 및 클라우드 서비스 어레이 문제를 동시에 해결해야 하기 때문입니다. 빠르게 변화하는 요구로 인해 조직들은 보안 포인트 제품을 "볼트온(bolt-on)"하거나, 클라우드 네이티브 보안을 사용해 특정한 보안/규정 준수 요건을 충족하게 되었습니다. 이는 곧 액세스 보안 및 인증을 더 이상 소유하지 않게 되었다는 의미입니다. 결과적으로 IT는 점차 사일로화되는 데이터 보안 솔루션을 관리하여 다양한 플랫폼과 다양한 환경을 보호해야 하는 상황이 되었습니다.
3. 클라우드 제공업체가 보안 기능을 제공할 수도 있지만, 이는 온프레미스 및 멀티 클라우드에 배포된 애플리케이션에 대한 보안 및 통제를 유지 관리하기에 완벽한 솔루션은 아닙니다. 한 CSP의 기능이 다른 클라우드 공급업체의 환경이나 온프레미스 애플리케이션에 반드시 적용되는 것은 아니기 때문입니다. 게다가 클라우드 모델마다 서로 다른 수준의 제어를 제공합니다. 예를 들어, IaaS 환경에서 작동하는 제어 기능이 SaaS 애플리케이션에서 반드시 실용적인 것은 아닙니다. 여러 클라우드에서 앱을 사용하고 하이브리드 환경에서 보안을 관리하는 경우에는 보안 공백의 문제가 더 심각해집니다.

궁극적으로 보안 팀은 고립되고 단편적인 방식으로 보안 제어를 구현하게 되어 비효율성, 불일치, 높은 관리 오버헤드, 과도한 비용, 보안 공백, 제어권 상실 등의 문제와 씨름하게 됩니다.

5 2021년 Verizon 데이터 유출 보고서
6 Gartner, "클라우드는 안전합니까?" 2018년 3월 27일, Kasey Panetta,
7 2021년 탈레스 IAM(Identity and Access Management) 인덱스

CSP 책임 공유 모델

책임 공유 모델에서는 클라우드 고객이 책임질 부분과 CSP가 책임질 부분을 명시합니다. CSP는 물리적 시설, 유틸리티, 케이블, 하드웨어 등 클라우드 "자체"의 보안을 책임집니다. 고객은 네트워크 제어, ID 및 액세스 관리, 애플리케이션 구성, 특히 데이터 보안 같이 클라우드 "내의" 보안을 책임집니다.

		온프레미스	IaaS	PaaS
애플리케이션 요소는 고객의 비즈니스에 따라 다르기 때문에 고객에게 책임 부과	애플리케이션 사용자 액세스 관리	✔	✔	✔
	애플리케이션별 데이터 자산	✔	✔	✔
	애플리케이션별 로직 및 코드	✔	✔	✔
IaaS 모델이냐 PaaS 모델(PaaS는 종종 "서버리스"라고 지칭)이냐에 따라 워크로드에 대한 책임 부과 대상 결정	애플리케이션/플랫폼 소프트웨어	✔	✔	✔
	운영 체제 및 로컬 네트워킹	✔	✔	✔
	가상 머신/서버 인스턴스	✔	✔	✔
하위 수준 인프라는 보다 일반적이고 상품화되어 있기 때문에 제공업체에게 책임 부과	가상화 플랫폼	✔	✔	✔
	물리적 호스트/서버/컴퓨팅	✔	✔	✔
	물리적/경계 네트워크	✔	✔	✔
	물리적 데이터 센터 환경	✔	✔	✔

✔ 고객 ✔ 제공업체

출처: Cloud Security Alliance 웹사이트: 책임 공유 모델 설명

위의 그림에서 알 수 있듯이, 조직이 사용하는 클라우드 서비스 모델에 관계 없이 앱과 데이터에 대한 액세스 권한을 소유하고 있고 권한을 부여하는 조직이 궁극적으로 앱과 데이터의 보안을 책임집니다. 내부 조직에서 저장 또는 관리하지 않는 데이터에 대해 규정 준수를 보장하고 이를 문서화하여 입증하려면 보안 통제를 적용해야 합니다. 업무 분장, 액세스 제어, MFA, 보증 수준이 높은 키 제어 등이 여기에 포함됩니다.

클라우드 보안 핵심 요구 사항

보안 팀은 클라우드 환경에서 워크로드, 앱 및 데이터 세트를 보호하는 임무를 맡고 있다는 점에서 몇 가지 구체적인 목표를 해결해야 합니다. 온프레미스 또는 클라우드에 저장되어 있거나 전송 중인 경우를 포함해 민감 데이터의 기밀성과 보안성을 항상 유지해야 합니다. 그러기 위해서는 하드웨어나 가상 리소스가 폐기된 이후나 CSP가 소환된 경우에도 자산을 계속해서 보호할 수 있는 통제 기능이 필요합니다.

기업 또는 CSP 관리자가 악의적으로, 또는 실수로 민감한 자산을 노출시키는 일이 없도록 방지하는 통제 기능이 구현되어 있어야 합니다. 또한 보안 팀은 멀티 테넌트 클라우드 환경 내에서 다른 테넌트가 데이터에 액세스할 수 없도록 해야 합니다.

실용적인 솔루션이 되기 위해서는 다음과 같은 특성을 갖춰야 합니다.

- **포괄적이고 통합된 적용 범위.** 보안 팀은 액세스 제어, 암호화 및 키 관리에 대한 정책을 효율적이고 일관성 있게 적용할 수 있도록 중앙 집중식 통제를 구현할 수 있어야 합니다. 또한, 온프레미스 및 멀티 클라우드 제공업체를 포함해 복잡하고 분산된 환경을 중앙에서 편리하게 제어할 수 있는 통합 플랫폼이 필요합니다.
- **데이터 중심 보안.** 오늘날에는 데이터가 조직의 가장 귀중한 자산이라는 것과 데이터가 기하급수적으로 증가하고 있음을 잘 알고 있는 데이터 보안 솔루션이 요구되고 있습니다. 데이터 중심 보안은 데이터를 사용 중인 애플리케이션이나 데이터가 상주하는 환경, 데이터가 이동하는 네트워크에 관계없이 데이터 자체를 보호합니다.
- **높은 보증 수준.** 최고 수준의 가용성 및 성능을 비롯해 인증되고 입증된 보안을 제공하는 암호화 및 키 관리 시스템을 선택해야 합니다. 액세스 관리를 위해서는 특권 계정에는 인증된 관리자만 액세스할 수 있도록 허용하고 덜 민감한 애플리케이션과 일반 사용자에게는 덜 엄격한 액세스 제어를 적용하는 등 모든 액세스 지점에서 액세스 제어를 적용해야 합니다.

배포 접근 방식

최소한의 기능에 의존해서 핵심 보안 기능만 적용하는 것으로는 충분하지 않습니다. 실제 요구와 위협을 고려해 제품 및 서비스를 평가해야 합니다.

분산된 모든 환경에서 포괄적이고 통합된 보안 접근 방식을 구축하고 싶은 보안 팀이라면 각각의 기본 보안 영역 내에서 다음과 같이 중요한 질문들을 던져봐야 합니다.

- 데이터 암호화 조직, CSP 또는 MSSP(Managed Security Service Provider) 중 누가 보호 기능을 제공합니까? 보호 메커니즘이 애플리케이션 수준에서 사용됩니까, 아니면 인프라 수준에서 사용됩니까? 클라우드 환경의 업스트림 및 다운스트림에서 암호화를 지원하는 방법은 무엇입니까?
- 키 관리. 키가 어디에 저장되어 있습니까? CSP의 키 볼트(key vault)에 저장되어 있습니까, 아니면 고객이 제어하는 중앙 집중식 엔터프라이즈 키 관리 시스템(온프레미스 또는 MSSP의 클라우드 기반)에 저장되어 있습니까? 키 저장 플랫폼은 얼마나 안전합니까?
- 액세스 제어. 고객 또는 CSP가 액세스 제어 정책을 정의하고 적용합니까? CSP의 ID가 사용됩니까, 아니면 고객의 SSO가 사용됩니까? MFA는 어떤 조건 하에서 사용되고 있습니까? 컨텍스트 기반의 적응형 액세스 정책이 위험 조건을 지속적으로 평가하여 필요한 경우 인증을 적용하고 있습니까?

어떤 접근 방식을 채택할 것인지 결정하려는 의사 결정권자는 반드시 이러한 질문들을 던져봐야 합니다. 아래에는 채택할 수 있는 6가지 배포 접근 방식이 간략하게 설명되어 있습니다.

접근 방식 1: 고객이 데이터 보호 관리

IaaS 환경에서 고객은 기반이 되는 인프라에 대해 높은 수준의 제어를 구현할 수 있습니다. 현재 출시되어 있는 솔루션들은 온프레미스, 프라이빗 클라우드, MSSP 같이 신뢰할 수 있는 외부 서비스 제공업체의 시설, 암호화 공급업체의 환경 등을 포함해 키 관리 기능과 액세스 보안 및 인증 기능이 실행되는 위치와 관련해 고객들에게 다양한 옵션을 제공하고 있습니다. 보안 팀은 IaaS 환경에서 워크로드를 실행할 때 키 관리를 유지하고 애플리케이션을 호스팅하는 클라우드 환경 외부에서 보안 및 인증 기능에 액세스할 수 있습니다.

이점

보안 팀은 클라우드 및 기타 서비스 제공업체 모델의 이점을 활용하는 동시에, 지금까지 수행해 온 온프레미스 환경 관리와 관련된 모든 작업을 수행할 수 있습니다. 이 접근 방식에서는 액세스 제어, 암호화, 키 및 키 관리에 대한 정책을 고객이 통제합니다. 따라서 보안 팀이 보다 엄격한 인증을 적용하여 CSP의 환경에서 관리자와 특권 사용자로 인해 야기되는 위험으로부터 데이터를 보호하도록 지원합니다. 또한 이 접근 방식은 적용될 수 있는 모든 데이터 레지던시 요구 사항을 포함해 조직의 규정 준수 의무를 충족할 수 있는 방법을 제공합니다. 암호화된 데이터는 여러 환경과 지리적 위치로 이동이 가능하지만, 데이터를 암호화하고 해독하는 데 사용되는 키는 항상 조직의 통제 하에 있는 중앙 지역에 보관할 수 있습니다.

접근 방식 1 개요

클라우드 환경: IaaS

접근 방식:

- 고객이 키 관리 및 RoT(Root of Trust)에 대한 제어권을 가집니다.
- 관리자에 대한 로그인 지점에서의 액세스 보안 및 인증은 고객의 통제 하에 이루어집니다.

접근 방식 2: CSP 제공 암호화

IaaS 환경에 비해 PaaS 환경에서는 고객이 보안 제어를 구현할 수 있는 옵션이 더 적어집니다. 이러한 경우에 고객은 PaaS 공급업체가 제공하는 암호화 메커니즘을 사용하는 동시에 키에 대한 몇 가지 통제 수준을 설정할 수 있습니다. 이러한 고차원적 접근 방식에서는 보안 팀이 다음 중에서 선택할 수 있습니다.

- BYOK(Bring Your Own Key). 고객이 암호 키를 생성해서 CSP에게 제공하고, CSP가 키 볼트를 이용해 키를 관리합니다.
- HYOK(Hold Your Own Key). 고객이 클라우드 데이터에 대한 암호 키를 생성하고 보유합니다. 조직은 클라우드 서비스를 활용하면서도 암호 키에 대한 완전한 소유권과 단독 통제 권한을 갖습니다.
- 자체 액세스 보안 및 인증을 제어. CSP에 의존하는 대신 고객이 IAM을 소유하고 제어합니다. 조직은 IAM에 대한 완전한 소유권과 단독 통제 권한을 갖습니다.

이점

이러한 키 관리 접근 방식에서는 고객이 CSP가 제공하는 키 관리 및 암호화 기능을 활용하는 동시에, 마스터 키와 관련 키 관리 및 암호화 정책을 정의해서 업로드할 수 있습니다. 한편, 보안 팀은 여러 클라우드에서 일관된 제어를 구현할 수 있습니다. 또한 키 교체 및 만료와 관련된 정책을 설정해 적용함으로써 보안을 강화할 수 있습니다.

고객은 이러한 책임 공유 모델을 통해 공격 표면을 줄이고, “위협 상속”을 방지하며, 제3자에 의한 데이터 액세스 위험을 줄이고, 디렉토리 유연성을 보장하는 등 IAM을 제어할 수 있습니다. 또한 보안 팀은 고객과 관리자에게 일관된 로그인 환경을 제공하고 필요에 따라 보다 엄격한 인증을 적용하여 여러 클라우드에서 일관성 있는 통제를 구현할 수 있습니다.

접근 방식 2 개요

클라우드 환경: PaaS

접근 방식:

- 고객이 키를 생성하고, CSP가 키와 암호화를 관리합니다.
- 관리자 및 사용자에 대한 로그인 지점에서 액세스 보안 및 인증은 고객이 수행합니다.

접근 방식 3: 키 브로커 서비스

현재, 많은 SaaS 공급업체들과 독립 브로커들이 키 관리 및 중개 옵션이 포함된 클라우드 액세스 보안 서비스를 제공하고 있습니다. 조직들은 이러한 서비스를 사용하면서도 자체적인 중앙 키 관리 플랫폼에서 키를 관리할 수 있습니다.

이점

이 접근 방식에서는 고객이 SaaS 제품의 모든 이점을 활용하는 동시에, 이러한 환경에 보관되어 있는 데이터에 액세스할 수 있는 사람을 통제할 수 있습니다. 고객은 키 관리 수명 주기 전반에 걸쳐 키 관리 정책을 설정하고 적용할 수 있습니다. 이 접근 방식은 다양한 보호 기능을 제공합니다. 예를 들어 SaaS 제공업체가 소환되더라도 데이터 공개 여부에 대한 통제권은 고객이 계속 갖게 됩니다.

접근 방식 3 개요

클라우드 환경: SaaS

접근 방식:

고객이 MSSP 또는 SaaS 공급업체 같은 외부 공급업체에서 제공하는 키 브로커 서비스를 사용합니다.

접근 방식 4: 이중 키 암호화

CSP는 외부 보안 공급업체와 협력하여 조직이 암호 키에 대한 완전한 제어권을 유지하면서도 가장 민감한 데이터를 보호할 수 있도록 지원합니다. 이 접근 방식에서는 두 개의 키를 사용해 데이터를 보호합니다. 첫 번째 키는 인증된 RoT에서 고객이 통제하고, 두 번째 키는 CSP에 안전하게 저장됩니다.

이점

보호 대상 데이터에 액세스하기 위해서는 두 키가 모두 필요하기 때문에 CSP와 그 외의 제3자가 보호 대상 데이터에 자체적으로 액세스할 수 없습니다. 금융 서비스 기관, 정부 및 의료 기관 같이 규제가 엄격한 산업 분야의 조직들은 GDPR, HIPAA, Schrems II 같은 규정을 준수할 수 있습니다.

접근 방식 4 개요

클라우드 환경: 모든 환경

접근 방식:

고객은 보호 대상 데이터를 해독하기 위해 키에 액세스할 수 있는 권한을 가진 사람을 단독적으로 통제할 수 있습니다.

고객이 보유한 키는 CSP와는 별도로 고객 환경에서 유지 관리됩니다.

접근 방식 5: 어디서든 인증

CSP 및 외부 보안 공급업체는 조직이 가장 민감한 데이터를 보호할 수 있도록 서비스를 제공합니다. 보안 환경을 이해하고, 모든 인증 공백을 메우며, 인증을 통해 모든 앱을 보호하는 것은 고객의 책임입니다.

이점

어디서든 인증을 수행하는 접근 방식은 모든 유형의 클라우드 환경에 적용이 가능하고, 모든 앱에 일관된 보호 및 사용자 경험을 제공하며, 필요에 따라 기존의 온프레미스 솔루션을 활용하고, 전면 교체가 필요하지 않습니다.

고객은 이러한 책임 공유 모델을 통해 공격 표면을 줄이고, “위협 상속”을 방지하며, 제3자에 의한 데이터 액세스 위험을 줄이고, 디렉토리 유연성을 보장하는 등 IAM을 제어할 수 있습니다. 또한 보안 팀은 고객과 관리자에게 일관된 로그인 환경을 제공하고 필요에 따라 보다 엄격한 인증을 적용하여 여러 클라우드에서 일관성 있는 통제를 구현할 수 있습니다.

접근 방식 5 개요

클라우드 환경: 모든 환경

접근 방식:

고객은 모든 인증 공백을 메우고, 배포된 IDP 및 SSO 솔루션에 관계 없이 인증을 통해 모든 앱을 보호합니다.

접근 방식 6: 위의 모든 접근 방식 사용

이러한 접근 방식을 사용하면 중앙 집중식 키 및 액세스 보안 관리를 구현해서 배포된 모든 하이브리드 클라우드에서 데이터, 액세스 및 인증을 통제할 수 있습니다.

이점

이 접근 방식을 통해 조직은 액세스 제어, 암호화 및 키 관리에 대한 정책을 중앙에서 일관되게 정의해 적용하고, 수명 주기 전반에서 키를 안전하게 관리하는 등 중앙 집중식 통제의 이점을 실현할 수 있습니다. 동시에, 다양한 클라우드 공급업체 및 모델에서 제공하는 특정 옵션과 이점을 최대한 활용할 수 있도록 접근 방식을 조정할 수 있습니다.

고객은 이러한 책임 공유 모델을 통해 공격 표면을 줄이고, “위협 상속”을 방지하며, 제3자에 의한 데이터 액세스 위험을 줄이고, 디렉토리 유연성을 보장하는 등 IAM을 제어할 수 있습니다. 또한 보안 팀은 고객과 관리자에게 일관된 로그인 환경을 제공하고 필요에 따라 보다 엄격한 인증을 적용하여 여러 클라우드에서 일관성 있는 통제를 구현할 수 있습니다.

클라우드 서비스는 디지털 트랜스포메이션을 추구하는 조직에게 강력한 이점을 제공하지만, 보안 및 규정 준수 측면에서 전례 없는 문제들을 야기하기도 합니다. 위에서 설명한 접근 방식들을 사용하면 다양한 클라우드 서비스 및 모델의 이점을 극대화하는 동시에 중요한 규정 준수 의무 및 보안 목표를 이행하는데 필요한 기능들을 구현할 수 있습니다.

접근 방식 6 개요

클라우드 환경: 모든 환경

접근 방식:

고객은 중앙 집중식 키 및 액세스 보안 관리를 구현하여 모든 클라우드 모델과 공급업체에서 데이터, 액세스 및 인증을 통제하는 데 사용합니다.

클라우드 보안 방법론

클라우드 보안 전략을 수립하는 IT 및 보안 팀은 다음과 같은 단계를 거쳐야 합니다.

1. 민감 데이터 및 애플리케이션과 상주 위치 파악

직원 및 고객의 개인 기록, 지적 재산, 재무 기록, 계정 정보 등을 포함해 기업의 모든 민감 자산을 실시간으로 완벽하게 파악해야 합니다. 또한 물리적 위치 및 환경 유형을 포함해 이러한 자산이 상주하는 위치를 정확히 확인해야 합니다.

2. 위험 요소 확인

민감 자산의 범주 및 위치에 따라 노출될 수 있는 특정 위험 요소를 파악해야 합니다. 외부의 사이버 공격자를 비롯해 특권 사용자에 대한 취약성은 물론이고 규정 준수 위험도 확인해야 합니다.

3. 배포 유형별 데이터 제어 수준 이해

배포 환경 및 모델 고유의 특성에 맞는 접근 방식을 채택해야 합니다. 예를 들어, PaaS 환경에서 HYOK(Host Your Own Key) 접근 방식을 추구하는 경우에는 PaaS 공급업체에 제공되는 키에 연결할 수 있는 키 관리 정책의 유형을 지정합니다.

4. 전반적인 클라우드 전략 정의

조직이 클라우드 퍼스트 전략을 채택하고 있든, 온프레미스 환경을 주로 사용하고 있든, 하이브리드 환경을 사용 중이든 관계 없이, 모든 환경과 플랫폼을 관통하는 전반적인 보안 전략을 정의하는 것이 중요합니다. 일단 전략이 수립되면 민감도, 개인정보보호, 위험 등에 따라 자산을 평가하고 각자에게 맞는 적정 수준의 보안 솔루션을 배포해야 합니다.

5. 키, 액세스 및 정책을 중앙 집중식으로 관리하기 위한 접근 방식 마련

조직의 기존 IT 환경을 비롯해 보안 및 비즈니스 목표에 따라 보안 태세의 세부적인 내용이 다를 수 있습니다. 그러나 조직에게 가장 바람직한 방법은 동적인 사이버 보안 위협을 예측, 예방 및 대응하는 데 도움이 되는 중앙 집중식 키 관리 및 액세스 관리 솔루션을 구축하는 것입니다. 온프레미스 솔루션이든, 클라우드 솔루션이든, 하이브리드 솔루션이든 조직의 요구에 가장 부합하는 형태로 구축할 수 있습니다. 솔루션이 중앙 집중화되어 있으면 조직 전반에 걸쳐 연속성과 일관성을 보장할 수 있습니다.

6. 사용 가능한 최상의 통제 기능 배포

IT 및 보안 팀은 현재 환경을 기반으로 최적화된 보안 및 운영 효율성을 달성할 수 있도록 통제 기능을 혼합해야 합니다. 위에서 설명한 것처럼 앞으로는 점차 중앙 집중식의 통합된 방식으로 암호화, 키 관리 및 액세스 통제 기능을 관리해야 합니다.

7. 클라우드 기능의 진화 모니터링

클라우드 서비스 시장의 혁신이 빠른 속도로 이루어지면서 공급업체와 제품의 수가 계속해서 증가하고 있습니다. 클라우드 서비스 사용 및 보안 통제에 대한 최적의 접근 방식을 구축했다면, 이제 중요한 것은 시장 발전에 뒤처지지 않는 것입니다. 이를 위해서는 기존 공급업체에 대한 정기적인 모니터링을 통해 의사 결정권자에게 새롭게 출시된 기능과 제품군을 알려야 합니다. 또한 경영진은 보다 일반적인 관점에서 시장을 모니터링하여 보안, 효율성 또는 비용 절감 측면에서 강력한 이점을 제공할 수 있는 새로운 공급업체와 제품군을 식별해야 합니다.

탈레스 솔루션의 이점

탈레스는 포괄적인 통합 솔루션 세트를 통해 온프레미스, 멀티 클라우드 및 전체 하이브리드 IT 환경을 포함한 모든 환경에서 앱과 데이터를 보호할 수 있도록 중앙 집중식의 효율적인 통합 기능을 제공하고 있습니다. 조직은 탈레스 솔루션을 통해 민감한 디지털 자산의 가용성, 무결성 및 기밀성을 최적화하는 세분화된 정보 보안 통제를 구현할 수 있습니다.

1. 모든 민감 데이터 검출

일반적으로 데이터 보안 전략의 첫 단계는 민감 데이터나 규제 대상 데이터를 찾는 것입니다. 데이터가 여러 플랫폼에 분산되어 있는 멀티 클라우드 환경에서는 이 작업이 특히 어려울 수 있습니다. CipherTrust Data Security Platform의 구성 요소 중 하나인 CipherTrust Data Discovery and Classification은 온프레미스 및 클라우드에서 정형 데이터와 비정형 데이터를 모두 찾아서 분류합니다. 클라우드에 저장된 민감 데이터의 종류와 저장 방법, 저장 이유를 알지 못하면 데이터 보호를 위해 효과적인 키 관리, 암호화 정책 및 통제를 적용할 수가 없습니다.

2. 데이터 및 액세스 보호

저장 중인 데이터 보호

CipherTrust Data Security Platform은 다양한 데이터 저장소, 플랫폼 및 IT 환경 전반에서 업계 최고의 데이터 보호 솔루션들을 하나로 통합합니다. 덕분에 보안 팀은 거의 모든 상황에서 민감한 데이터에 대해 적정 수준의 보안 통제를 적용할 수 있습니다.

- **투명 암호화**
  특히 IaaS 시스템의 경우, CipherTrust Transparent Encryption은 저장 중인 데이터를 암호화하기 위해 특권 사용자의 액세스를 제어하는 기능과 업계 최고의 강력한 암호화 기능, 데이터 액세스에 대한 상세한 감사 로깅을 포함한 고급 기능 및 확장 기능을 제공합니다. 투명 암호화는 파일, 데이터베이스 볼륨 및 기타 리포지토리의 데이터를 보호하고, 특허 받은 실시간 데이터 변환 기술을 통해 암호화 및 키 교체(rekeying) 중에도 데이터를 사용할 수 있도록 지원합니다.

- **토큰화**
  CipherTrust Tokenization은 민감 데이터를 대표 토큰으로 대체하여 데이터베이스 관리자와 권한이 없는 사용자가 원래의 기밀 데이터에 액세스할 수 없도록 합니다. 토큰화는 클라우드에서 PaaS 서비스를 사용할 때 데이터베이스 필드 수준에서 향상된 보안을 구현하기에 적합한 방법입니다. 또한 CipherTrust Tokenization은 REST를 기반으로 하기 때문에 애플리케이션 및 클라우드 오케스트레이션에 손쉽게 통합됩니다.

- **애플리케이션 데이터 보호**
  CipherTrust Data Security Platform은 데이터에 대한 추가 제어를 지원합니다. CipherTrust Application Data Protection은 키 관리, 서명, 해싱, API를 통한 암호화 서비스 같은 암호화 기능을 제공하기 때문에 개발자는 특히 PaaS 수준에서 이러한 복잡한 작업들을 클라우드 또는 온프레미스에서 실행 중인 애플리케이션에 손쉽게 통합할 수 있습니다.

- **데이터베이스 보호**
  CipherTrust Database Protection은 코드나 애플리케이션을 변경할 필요 없이 데이터베이스에 컬럼 단위의 데이터 암호화를 제공합니다. 솔루션들이 사전 통합되어 있어 고객들은 Oracle, Microsoft SQL Server, IBM DB2 및 Teradata에서 암호화 및 키 관리를 제공하기 위해 소요되는 시간과 노력을 줄일 수 있습니다.

SureDrop은 안전한 파일 공유 협업을 위한 엔터프라이즈급의 클라우드 기반 또는 온프레미스 솔루션입니다. 보안 내재화 전략을 채택한 SureDrop은 파일 스토리지와 관련해 엄격한 보안 정책을 가지고 있지만, 여전히 완전한 기능을 갖춘 파일 공유 솔루션의 생산성 이점을 필요로 하는 조직들을 위해 개발되었습니다.

전송 중인 데이터 보호

Thales HSE(High-Speed Encryptors)는 네트워크와 독립적으로 전송 중인 데이터를 암호화(Layer 2, 3, 4)하여 데이터가 사이트 간을 이동할 때나 온프레미스와 클라우드 간을 이동할 때 데이터를 안전하게 보호합니다. 탈레스의 네트워크 암호화 솔루션을 사용하면 성능 저하 없이 저렴한 비용으로 도청, 감시, 노골적 가로채기 및 은밀한 가로채기로부터 데이터, 비디오, 음성 및 메타데이터를 보다 안전하게 보호할 수 있습니다. Thales HSE는 물리적 어플라언스 형태 및 가상 어플리언스 형태 모두를 지원하며, 단일 포트 어플라이언스부터 다중 포트 어플라이언스에 이르는 다양한 플랫폼에서 10Mbps ~ 100Gbps의 광범위한 네트워크 속도를 지원합니다.

암호 키 보호

보증 수준이 높은 FIPS 140-2 레벨 3 인증을 획득한 Thales Luna HSM을 사용해 중요한 환경을 확실하게 보호함으로써 규정 준수를 달성하고 중요한 사용 사례로까지 이점을 확장할 수 있습니다. Luna HSM는 저장 중인 데이터와 전송 중인 데이터의 키를 보호하는 것은 물론 데이터, 디지털 ID 및 트랜잭션을 암호화하는 마스터 키를 보호하는 트러스트 앵커 역할을 합니다. 탈레스는 아래와 같이 다양한 업계 최고의 HSM을 제공하고 있습니다.

- **범용 HSM**
  Thales Luna 범용 HSM은 장치, ID 및 트랜잭션을 포함해 조직의 전체 디지털 보안 에코시스템에서 신뢰의 토대가 됩니다. 네트워크 연결 어플라이언스, 내장형 PCIe 카드, 휴대용 USB 어플라이언스, Cloud HSM 서비스 등 다양한 폼 팩터 내에서 암호화 키와 기능을 보호하여 무결성을 보장합니다. 다양한 API, 뛰어난 성능, 즉시 사용이 가능한 수 백 개의 기술 파트너 애플리케이션을 토대로 통합 및 개발 작업을 간소화하여 암호 키의 수명 주기와 운영을 보호할 수 있습니다.

- **클라우드 기반 HSM**
  Thales DPoD(Data Protection on Demand)는 단순한 온라인 마켓플레이스를 통해 Luna Cloud HSM, CipherTrust Key Management(키 브로커) 및 payShield Cloud(P2PE) 서비스를 제공하는 클라우드 기반 플랫폼입니다. 따라서 하드웨어를 구매, 배포 및 유지 관리할 필요가 없기 때문에 보다 간단하고 비용 효율적으로 데이터 보안을 관리할 수 있습니다. 클릭만 하면 필요한 보호 기능을 배포하고, 서비스를 프로비저닝하며, 보안 정책을 추가하고, 몇 분 내에 사용 보고서를 받아볼 수 있습니다.

앱 및 특권 계정에 대한 액세스 제어

Thales SafeNet Trusted Access는 퍼블릭 및 프라이빗 클라우드에서 신뢰할 수 있는 ID 제공자 역할을 하는 클라우드 기반의 IAM(Identity and Access Management) 서비스입니다. 또한, 다양한 클라우드를 포함해 조직 환경 전반에 IAM 솔루션을 안전하게 배포할 수 있는 기능을 제공합니다.

SafeNet Trusted Access는 인증 및 조건부 액세스를 사용하고 사용자가 앱에 로그인할 때마다 정책 기반 액세스 제어를 적용하는 방법으로 로그인 지점에서 클라우드 리소스를 보호합니다.

- **클라우드 플랫폼에 대한 정책 기반 액세스 관리**
  외부 IAM 솔루션을 사용해 액세스 보안 및 인증을 보호하면 클라우드에서 위협이 상속되는 일을 방지할 수 있습니다. 즉, 클라우드의 백엔드에서 보안 침해가 발생하더라도 통제를 유지할 수 있습니다. 외부 IAM 서비스를 사용할 경우, 보안을 분리시켜 여러 클라우드를 지원하는 솔루션을 선택할 수 있다는 추가적 이점이 있습니다. 따라서 비즈니스 요구에 따라 여러 클라우드를 지원해야 할 때 단일 클라우드 공급업체에게 고착되는 일이 발생하지 않습니다.

- **2FA 규정 준수**
  다양한 규정 준수 법규에서 클라우드 리소스 관리를 위해 2FA(Two-Factor Authentication)를 요구하고 있습니다. SafeNet Trusted Access는 조직이 사용자 경험을 최적의 상태로 유지하면서 적정 수준의 인증을 제공할 수 있도록 컨텍스트 기반의 MFA를 광범위하게 지원합니다.

- **관리자 및 고객을 위한 Cloud SSO 및 MFA**
  SafeNet Trusted Access는 규정 준수를 보장하는 외에도 퍼블릭 및 프라이빗 클라우드에서 클라우드 SSO 및 MFA를 지원하여 사용자가 상주 위치에 관계 없이 어디서든 원격으로 인증 및 액세스 제어를 프로비저닝할 수 있도록 지원함으로써 IT 관리자와 고객의 생산성을 향상합니다.

3. 데이터 및 액세스 통제

중앙 집중식 키 관리

CipherTrust Manager

CipherTrust Manager는 CipherTrust Data Security Platform의 중앙 관리 지점으로, 키의 생성, 교체, 폐기, 가져오기 및 내보내기를 포함한 주요 수명 주기 작업을 관리하고, 키 및 키 관리 정책에 대한 역할 기반 액세스 제어를 제공하며, 강력한 감사 및 보고 기능을 지원합니다. 이 솔루션은 AWS, Microsoft Azure, Google Cloud, VMware, Microsoft HyperV 등에서 네이티브 가상 머신 형태로 실행할 수 있습니다. 또한 CipherTrust Manager에서는 CipherTrust Cloud Key Manager가 기본 지원되기 때문에 여러 클라우드 인프라와 SaaS 애플리케이션에서 키 관리를 간소화할 수 있습니다.

고객이 자신의 키를 스스로 통제해야 한다는 사실을 인식한 많은 클라우드 제공업체들에 대해 BYOK(Bring Your Own Key) 옵션을 지원하고 있습니다. BYOK는 고객이 클라우드에서 자신의 키를 더 잘 제어할 수 있도록 지원하지만, API와 방법이 다양하므로 멀티 클라우드 전략에 있어 문제가 되고 있습니다. 보안 팀은 CipherTrust Cloud Key Manager를 사용해 단일 창을 통해 클라우드 환경 전반에서 BYOK를 관리할 수 있습니다.

서비스 형태의 키 관리

Thales DPoD(Data Protection on Demand) 플랫폼을 기반으로 하는 CipherTrust Key Management Service는 BYOK 기능을 클라우드 기반 서비스 형태로 제공합니다. DPoD를 사용하면 CSP, IaaS 및 PaaS 환경, SaaS 공급업체 내에서 키와 암호화 관련 보안 정책을 손쉽고 안전하게 제어할 수 있습니다.

이러한 키 브로커는 키에 대한 통제를 유지하고 여러 환경에서 키 관리 정책을 조정할 수 있도록 지원합니다. 키 관리자 역할을 수행하는 키 브로커는 모든 키를 관리, 검색 및 감사할 수 있는 통합 키 관리 디렉토리를 제공합니다. 이러한 키 브로커를 사용해 키 관리 정책을 설계하고 적용하면 규정을 준수하는 데 도움이 됩니다.

앱 및 계정에 대한 액세스 제어

탈레스는 Thales SafeNet Trusted Access라는 정책 기반 IAM과 함께 탈레스 인증자 앱, 소프트웨어 인증자 또는 하드웨어 인증자를 사용해 2FA 또는 MFA를 수행하여 액세스를 제어할 것을 권장하고 있습니다.

클라우드 기반의 액세스 관리 솔루션인 SafeNet Trusted Access IDaaS(Identity-as-a-Service)를 통해 SSO(Single Sign-On), 다단계 인증 및 시나리오 기반의 액세스 정책을 하나로 결합한 통합 플랫폼을 이용해 클라우드 서비스와 엔터프라이즈 애플리케이션 모두에 대한 액세스를 손쉽게 관리할 수 있습니다. SafeNet Trusted Access는 앱 자산 전반에서 액세스 이벤트를 파악할 수 있는 단일 창을 제공하여 적정 권한을 가진 사용자가 적정 신뢰 수준에서 적정 애플리케이션에 액세스할 수 있도록 보장합니다.

탈레스 소개

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

결단이 필요한 순간을 위한 결정적인 솔루션

THALES

Building a future we can all trust

문의

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

> cpl.thalesgroup.com <