Vol.1

플래티어 IDT부문
김 대 웅 책임

2022 플래티어 인사이트 리포트

디지털 전환 시대, 보안 패러다임의 변화와 대응

PLATEER

디지털 전환 시대,
보안 패러다임의 변화와 대응

디지털 전환 시대,
보안 패러다임의 변화와 대응

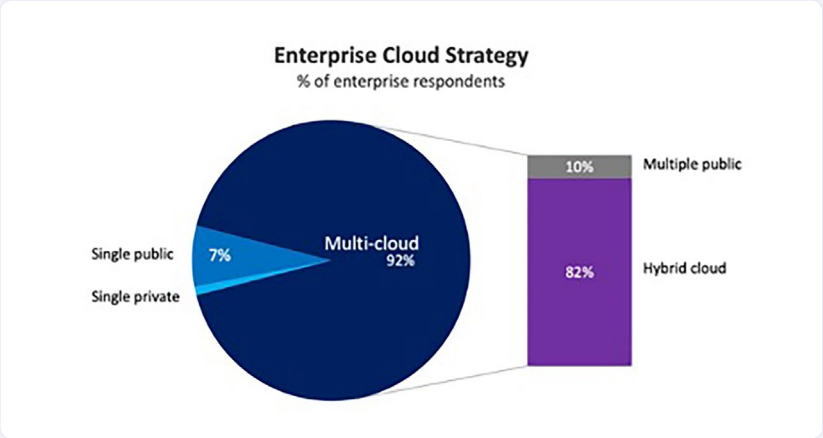
김 대 웅 | 플래티어 IDT부문 | 책임

들어가며

대부분의 기업에서 '디지털 전환'은 새로운 비즈니스 및 고객 가치를 사회 전반에 보다 빠르고 대규모로 제공하는 것을 의미하며, 이에 따라 비용 최적화보다는 속도 최적화를 지향하고 있다. 그런 의미에서 '클라우드'는 무한 확장으로 온디맨드 On-Demand 서비스를 신속하게 구축할 수 있는 기회를 제공하기 때문에 대부분의 기업들이 필수적으로 고려하게 되었다. 더불어 회사 내 여러 조직이 퍼블릭 클라우드를 통해 독자적인 IT 인프라를 구축할 수 있게 되면서 IT 부서에서 독점하던 인프라 운영은 개별 현업 부서로 넘어가고 있고, 부서별로 서로 다른 클라우드를 사용하거나 조직의 M&A 등으로 인해 많은 기업들이 여러 클라우드 제공자를 혼용하는 '멀티 클라우드' 상태에 놓이게 되었다.

실제로 소프트웨어 기업 플렉세라 Flexera의 2021년 클라우드 현황 보고서 Flexera 2021 State of the Cloud Report에 따르면, 임직원 1,000명 이상의 기업 750여 곳 중 92% 가 멀티 클라우드 Multi cloud전략을 채택했으며, 이중 82%는 프라이빗 클라우드 Private cloud와 퍼블릭 클라우드 Public cloud를 혼용하는 하이브리드 클라우드 Hybrid cloud 형태의 환경을 사용하고 있는 것으로 나타났다. (Flexera, 2021)

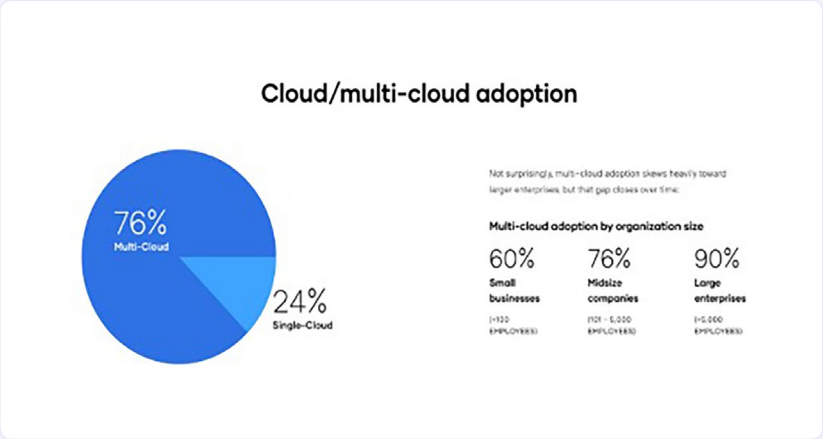
<그림1> 2021 기업들의 클라우드 전략 (※ 임직원 수 1,000명 이상 규모)



출처 : Flexera 2021 State of the Cloud Report (2021)

마찬가지로 인프라 자동화 소프트웨어 업체 하시코프 HashiCorp는 대기업의 90% 이상, 중견 기업의 76% 이상이 이미 멀티 클라우드를 도입하여 비즈니스 가치 제고에 나섰다고 밝혔다. (HashiCorp, 2021)

<그림2> 2021 기업들의 단일 클라우드/멀티 클라우드 채택 현황

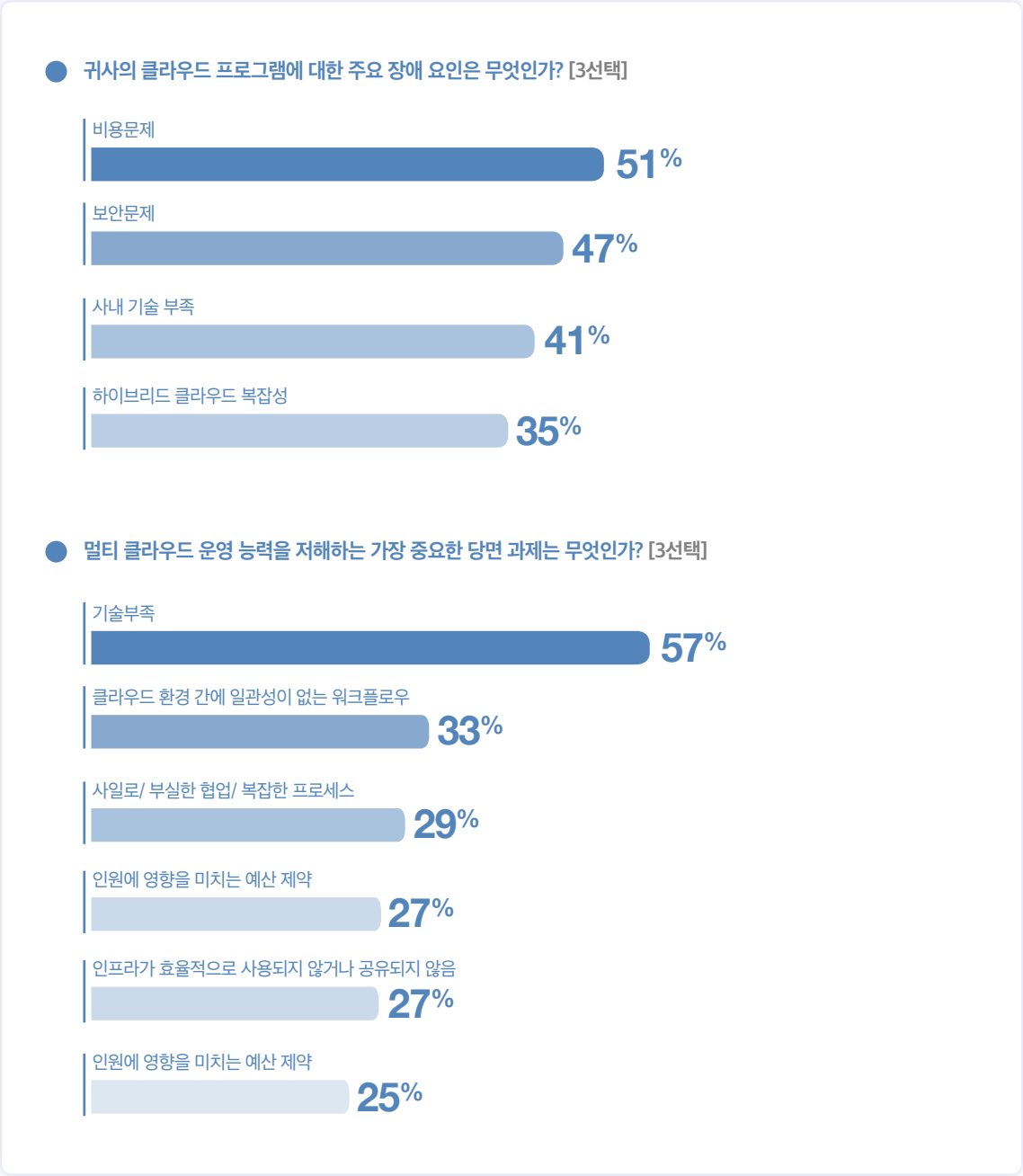


출처 : HashiCorp State of Cloud Strategy Survey (2021)

또한, 클라우드 환경, 특히 멀티 클라우드 환경에서는 비즈니스 목표 달성을 위해 여러 부문에서 여전히 해결해야 할 과제들이 존재하는 것으로 나타났다.

먼저 멀티 클라우드 환경 운영에 대한 주요 장애 요인으로 ▲비용(51%), ▲보안(47%), ▲사내 기술 부족(41%), ▲하이브리드 클라우드의 복잡성(35%) 등이 꼽혔다. 이와 함께 기업들이 선정한 멀티 클라우드 운영을 저해하는 주요 당면 과제로 ▲기술 부족(57%), ▲클라우드 환경 간에 일관성 없는 워크 플로우(33%), ▲복잡한 프로세스(29%), ▲인프라의 효율적인 관리 문제(27%), ▲보안 및 거버넌스 관리의 어려움(25%) 등이 제기되었다. (HashiCorp, 2021)

<그림3> 2021 클라우드 마이그레이션 주요 장애 요인(上) 및 운영 능력을 저해하는 당면 과제(下)

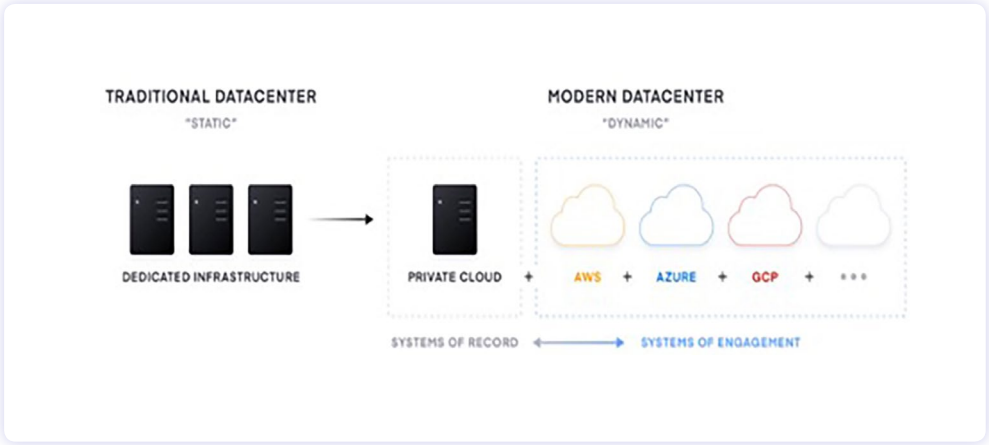


출처 : HashiCorp State of Cloud Strategy Survey (2021)

본고에서는 위에서 언급한 여러 당면 과제들 중 멀티 클라우드 환경에서의 보안 및 거버넌스 관리를 위해 어떤 것들이 필요하고, 어떻게 관리할 수 있는지 그 방안에 대해 논의하고자 한다.

1. 멀티 클라우드 환경에서의 보안문제

<그림4> 클라우드 운영 모델의 변화



출처 : HashiCorp

클라우드 이전에 정적인 인프라를 사용할 때에는 네트워크를 외부와 단절시킴으로써 외부 위협에 대한 경계선 방어를 할 수 있었다. 하지만 클라우드를 사용하게 되면서 명확하게 정의된 네트워크 경계가 사라졌다. 그리고 클라우드 인프라의 접속은 원격 형태이기 때문에 온프레미스 On-premise[1] 환경에 비해 공격 경로가 다양하여 악성코드 전파가 쉽고, 내부자나 관리자 실수에 의한 정보 유출이나 손실이 발생할 위험이 크다.

또한 멀티 클라우드 환경에서는 모든 인프라가 하나 이상의 클라우드 제공자를 통해 매우 다양하게 분산되므로, 보안팀에서 각 조직의 가상 인프라 환경에 맞는 데이터 암호화, 사용자 인증 및 접근 제어 등의 보안 정책을 적용하고 관리하기 힘든 환경으로 변모했다.

결국 이러한 운영 모델의 변화는 신뢰를 전제로 한 격리된 네트워크 환경에서 로우 트러스트 Low Trust 혹은 제로 트러스트 Zero Trust[2] 네트워크 환경으로의 이동을 의미하며, 이런 환경에 배포되는 응용 프로그램은 사용하는 인프라 환경이 어떻게 변화하더라도 그 자체로써 보안 구현을 제공해야 하는 상태에 이르렀다.

1. 소프트웨어를 서버에 직접 설치해 쓰는 방식이다.
2. IT 보안 접근 방식을 의미하며, 신뢰할 수 있는 네트워크 경계는 존재하지 않고 모든 네트워크 트랜잭션이 이뤄지려면 먼저 인증을 받아야 한다고 가정한다.

이와 관련하여 미국의 클라우드 보안 연합 Cloud Security Alliance, CSA 은 클라우드 상의 보안을 위해 공통적으로 필요한 사항을 정리하여 서비스로서의 보안 Security as a Service, SECaaS[3] 형태로 해결할 것을 권고하고 있으며, 12가지 주요 기준을 제시했다.

- **ID 기반의 액세스 관리** Identity and Access Management, IAM
  - ID 기반의 신원보증, 정보접근, 권한 부여

- **데이터 유출/손실 방지** Data Loss Prevention
  - 사용 중인 데이터의 보안 및 모니터링 보안 검증

- **웹 보안** Web Security
  - 웹 트래픽을 프록시 처리하여 웹 응용 프로그램 실시간 보호

- **이메일 보안** Email Security
  - 피싱 및 스팸으로부터 조직 보호

- **보안 감사** Security Assessments
  - 클라우드 서비스에 대한 감사

- **침입 관리** Intrusion Management
  - 패턴 인식으로 이벤트 감지 및 탐지

- **보안 정보 및 이벤트 관리** Security Information and Event Management
  - 보안 로그 및 이벤트 정보에 대한 실시간 분석

- **암호화** Encryption
  - 해독할 수 없도록 데이터를 암호문으로 변환

- **서비스 연속성과 재난 복구** Business Continuity Disaster Recovery·재난 복구 서비스 Disaster Recovery as a Service
  - 서비스 중단 시 운영의 탄력성을 보장하도록 설계

- **네트워크 보안** Network Security
  - 네트워크 액세스를 할당하고 네트워크 서비스를 배포/모니터링/보호

- **취약점 검사** Vulnerability Scanning
  - 대상 인프라와 시스템의 취약점 검사

- **지속적인 모니터링** Continuous Monitoring
  - 현재 보안 상태에 대해 지속적인 위험 모니터링

3. 클라우드에서는 보안을 서비스의 관점으로 바라보고 있으며, CSA는 클라우드 보안 서비스 모델을 제시했다.

이후 이를 기반으로 국제 표준 지침이 정립되었으며, ISO/IEC 27017 은 클라우드의 정보 보안 지침을, ISO/IEC 27018은 클라우드의 개인정보보호에 대한 지침을 제공하고 있고 AWS, Azure, GCP는 ISO/IEC 27017, ISO/IEC 27018 인증을 받아 관련 서비스를 제공 중이다.

이때 각각의 보안 서비스를 그룹화하거나 연결하는 방식은 클라우드 제공자 별로 조금씩 다르지만 유사하며, AWS의 경우 미국 국립표준기술연구소NIST의 사이버 보안 프레임워크에 따라 서비스를 분류 및 연결하고 있다.

이 프레임워크의 핵심은 앞서 언급한 표준 지침들을 ▲ 식별 Identify[4] , ▲ 보호 Protect[5] , ▲ 탐지 Detect[6] , ▲ 대응 Respond[7] , ▲ 복구 Recovery[8] 그룹으로 구분하고 각 활동을 정의한 것으로, 실제AWS의 보안 서비스를 확인해 보면 아래 그림과 같이 구분하고 있다.

<그림5> AWS의 시큐리티 서비스 구성

출처 : AllCloud 블로그

결국 클라우드에서 운영되는 응용 프로그램이라면 위의 보안 기준에 맞게 식별, 보호, 탐지, 대응, 복구가 가능하도록 설계되어야 함을 의미하고 구체적으로는 아래와 같은 사항을 만족해야 한다.

1. 식별 - 응용 프로그램이 보호가 필요한 자산을 식별
2. 보호 - 자산에 대한 데이터 보호 수행
3. 탐지, 대응 - 보안 문제에 대한 탐지 와 대응을 위한 감사 Audit
4. 복구 - 복구 프로세스

따라서 본고에서는 이러한 부분들을 어떻게 응용 프로그램에 반영할 수 있는지 하나씩 짚어보도록 하겠다.

---

4. 식별은 사이버보안 위험을 관리하기 위한 조직의 시스템, 자산, 데이터, 역량 등에 관한 이해를 의미하며, Asset Management, Risk Assessment 등의 활동을 포함한다.
5. 보호는 주요기반시설의 서비스 제공을 보장하기 위해 필요한 보호 수단을 개발하는 것으로, Access Control, Awareness and Training, Data Security 활동을 포함한다.
6. 탐지는 사이버보안 사고 발생을 감지할 수 있는 행위 뜻하며, 지속적인 보안 모니터링을 통해 구현된다.
7. 대응은 탐지된 사이버보안 사고에 대한 조치를 취하기 위해 필요한 행위들을 의미하며, 보안위협의 분석Analysis 및 완화Mitigation 등이 포함된다.
8. 복구는 사이버보안 사고로 손상된 기능과 주요 기반 시설 서비스를 복구하기 위한 활동으로서 Recovery Planning 등이 해당된다.

2. ID 기반의 접근관리

먼저 사용자 클라우드에서 운영되는 응용 프로그램에 대한 '식별' 과 '보호' 부분에 대해 살펴보자.

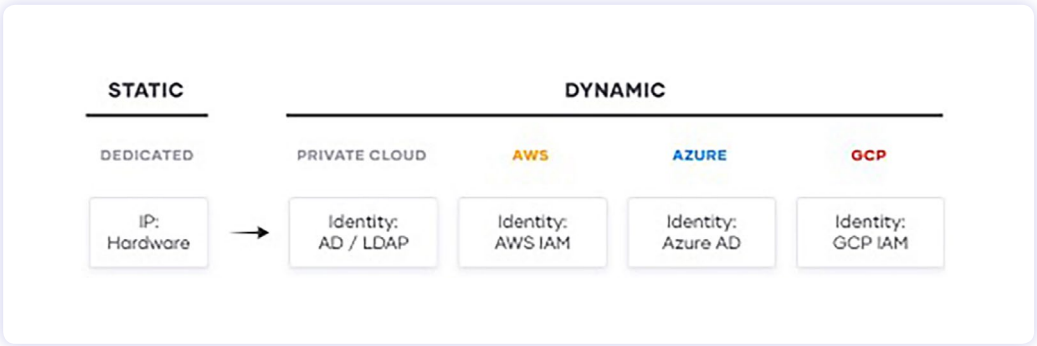
먼저 식별이 필요한 자산은 보통 응용 프로그램에서 사용되는 보호가 필요한 모든 정보에 해당하며 이런 정보들을 보호하기 위해서 사용자별 접근 제어를 제공해야 한다.

그리고 그것은 보안의 기준을 네트워크가 아닌 'ID'에 두는 것에서 시작한다. 왜냐하면 복잡한 방화벽 규칙과 빈번한 업데이트가 필요한 IP 주소와 달리 'ID'는 응용 프로그램에 연결된 사람이나 시스템에 매겨지는 고유성과 독립성을 띄기 때문이다.

이를 확인할 수 있는 좋은 예는 클라우드 제공자의 ID 기반 보안관리 서비스이다. 예를 들어 AWS 에서는 클라우드에 접속을 시도하는 ID 가 정상적인 사용자인지 확인하기 위해 ID 및 비밀번호 외에 추가인증을 요구하는 MFA[9] 인증방식을 수행하며, 사용자는 로그인 후에 ID에 부여된 정책에 따라 특정 인프라와 기능에만 접근할 수 있다. 이것이 바로 접근관리 Access Management, AM 솔루션이며, 이는 우리가 익히 알고 있는 서비스인 'IAM (ID+AM)' 이다.

이런 서비스는 대표적으로 AWS IAM, Azure AD, GCP IAM 등이 있으며, 프라이빗 클라우드를 운영하는 경우는 Active Directory나 LDAP Lightweight Directory Access Protocol 와 연계하여 사용자 ID 인증에 대한 부분을 수행하고 있다.

<그림6> 클라우드에서 사용하는 주요 IAM 서비스



출처 : HashiCorp

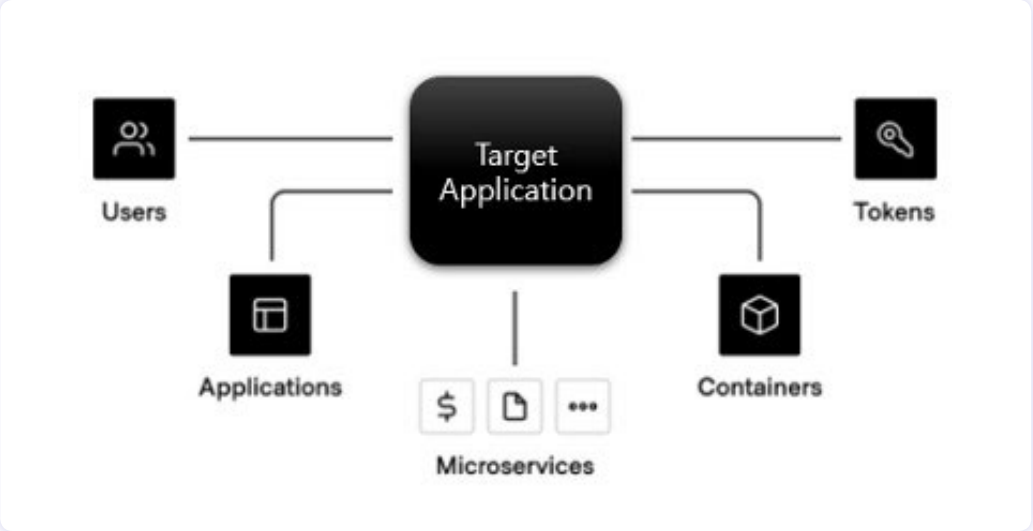
9. MFA(Multi Factor Authentication)는 로그인 프로세스에 보호 계층을 추가하여 계정이나 앱에 액세스할 때 사용자가 지문 스캔, 전화로 받은 코드 입력 등과 같은 추가 ID 확인을 수행하는 다단계 인증 방식이다.

이와 마찬가지로 클라우드 환경에서 사용되는 응용 프로그램은 먼저 보호가 필요한 정보를 구분하고 저장해야 하며, 클라우드에서 제공하는 IAM 시스템과 연계하여 이를 기준으로 해당 정보에 대한 접근 권한을 줄 수 있어야 한다.

그리고 응용 프로그램에 대한 효율적인 접근 권한 관리를 위해서 두 가지 사항을 고려하면 좋은데, 그 첫 번째는 접근 주체를 잘 파악하는 것이다.

접근 주체가 '사람'일 경우, 일반적으로 자격증명이 오래 지속되고 보관된다. 하지만 접근 주체가 '시스템(서버·애플리케이션· 마이크로서비스·스크립트 등)'인 경우, 접근 방식에 따라 굉장히 많은 ID가 생성될 수 있으므로, 동적으로 임시 자격증명에 해당하는 ID를 만들어 필요한 최소한의 권한만 부여하고, 작업이 끝나거나 TTL Time to Live 설정이 만료되면 사용한 ID를 삭제하는 프로세스가 필요하다.

<그림7> 응용 프로그램에 접근 가능한 다양한 클라이언트



출처 : HashiCorp (플래티어 재구성)

두 번째 고려사항은 사용자별 ID 관리 체계와 보호가 필요한 데이터 관리 체계의 통합이다.

단일 클라우드 환경에서 멀티 클라우드 혹은 하이브리드 클라우드 환경으로 바뀌거나, 사용하는 클라우드 제공자가 변경되더라도 사용자는 기존에 액세스가 가능했던 정보에 그대로 액세스할 수 있어야 한다.

이와 같은 고려사항들을 응용 프로그램 내에서 모두 수행하는 것은 상당한 노력이 필요하다. 이에 응용 프로그램은 보안이 필요한 정보를 보관할 수 있고, 멀티 클라우드 환경에서의 통합된 자격증명을 지원하는 도구와 연계하는 것이 효율적일 수 있다.

예를 들어 하시코프의 Vault는 멀티 클라우드 환경에서 응용 프로그램의 ID 기반 자격증명 관리를 위해 사용할 수 있는 대표적인 솔루션이다. Vault는 LDAP, AD 혹은 클라우드 제공자의 IAM 제품 자격증명과 연동하여 임시 자격 증명을 발급해주거나, 애플리케이션에 대한 액세스를 제어할 수 있다.

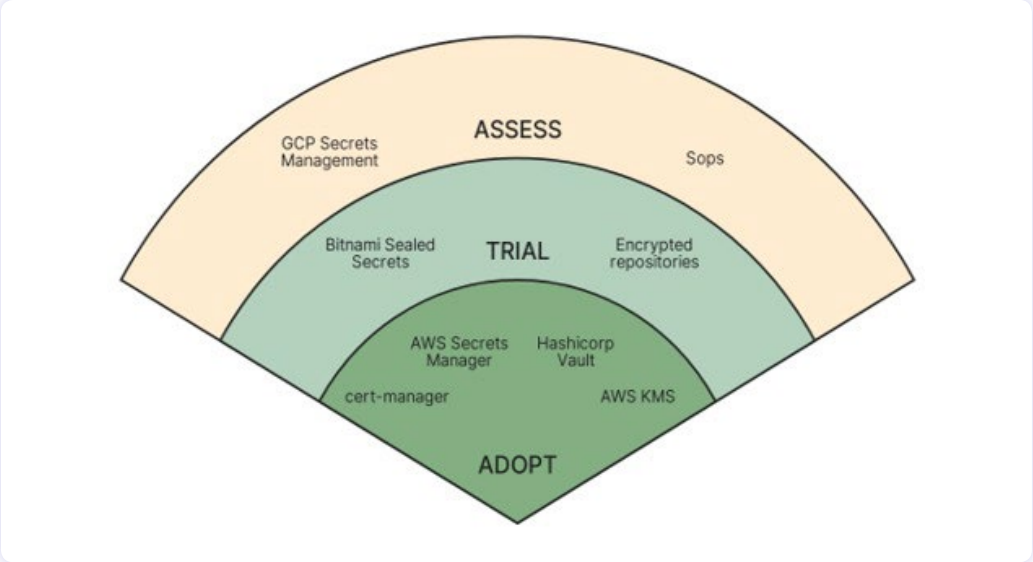
3. 시크릿 관리

이와 같이 멀티 클라우드 환경에서 통합된 정보 관리 체계 및 ID 기반의 자격증명 체계가 마련되었다면, 자산으로 식별된 ▲ 기존에 보안 처리가 되지 않은 액세스 자격 증명, ▲ 하드 코딩 된 호스트명이나 방화벽 규칙, ▲ 스크립트·구성파일·소스코드에 포함된 암호화되지 않은 사용자 이름/암호/API 키, ▲ 파일 시스템에 저장된 인증서/암호화 키와 같이 보안이 필요한 정보 보호를 고려해야 한다.

이러한 정보를 보통 '시크릿'이라 하는데, 시크릿은 운영, 테스트, 배포, 외부 프로그램 등을 사용할 때 지속적으로 발생하게 되므로 클라우드의 암호화 서비스 혹은 외부 도구를 통해 정보를 암호화하여 저장되어야 한다.

이러한 클라우드 암호화 서비스로는 아마존의 AWS Secret Manager 와 KMS, 구글 클라우드의 Cloud HSM 및 EKM, 애저의 Key Vault가 있으며, 암호화 외부 서비스로는 하시코프의 Vault 같은 제품이 있다. 이런 서비스와 제품은 암호화 키 배포와 관리 메커니즘을 API 기반으로 제공하고 있어 응용 프로그램과의 연계가 어렵지 않다.

<그림8> 대표적인 시크릿 관리 도구

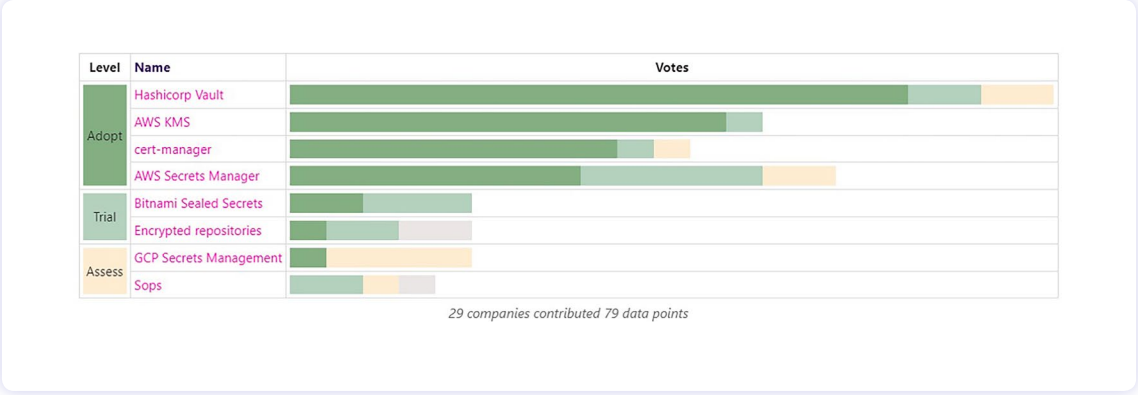


출처: CNCF (2021)

CNCF[10] 리포트에 따르면, 많은 기업들이 사내 솔루션을 만들고 유지하는 것보다 시크릿 관리를 아웃소싱하는 방식을 선호하고 있다. 이들은 현재 시크릿 관리를 위해 하시코프Vault를 가장 많이 사용 중이며, Vault를 도입하는 주된 이유는 클라우드에 종속되지 않는 방식으로 시크릿 관리를 다룰 수 있기 때문인 것으로 드러났다. (CNCF, 2021)

10. Cloud Native Computing Foundation(CNCF) : 컨테이너 기술을 발전시키고 기술 산업을 진화에 맞춰 조정할 수 있도록 지원하기 위해 2015년에 설립된 Linux Foundation 단체이다.

<그림9> 대표적인 시크릿 관리 도구 (상세)



출처 : CNCF

이러한 시크릿 관리에 대한 영역은 여러 부분이 있는데 이중 몇 가지 중요한 사항을 기술하면 아래와 같다.

1. 암호화 키 관리
2. 세분화된 정책을 통한 시크릿 접근제어
3. 다양한 타입의 시크릿을 관리
4. 시크릿을 중앙 집중식으로 관리
5. EaaS를 통한 암호화 관리

1) 암호화 키 관리

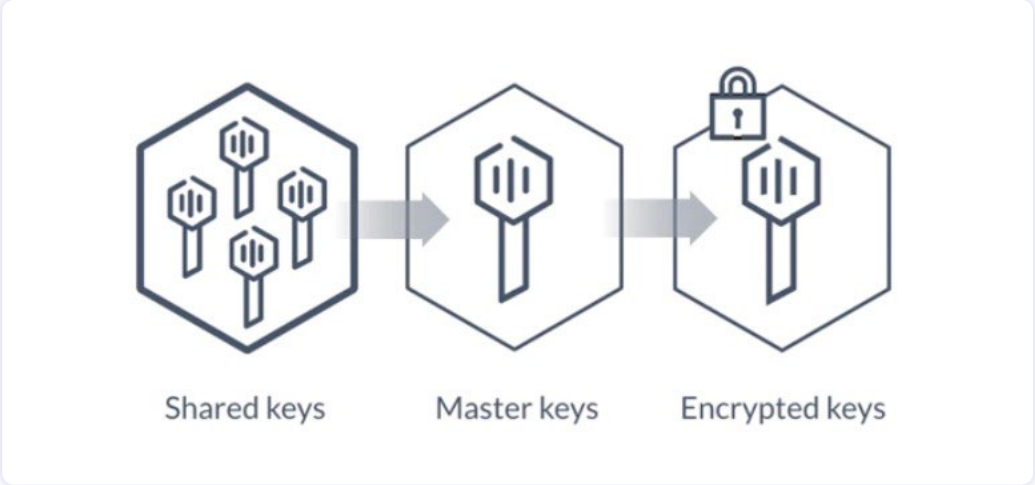
보안이 필수인 정보들은 반드시 암호화한 다음 저장해야 스토리지 해킹을 당하더라도 키, 암호, 인증서 및 암호화 키에 대한 액세스를 엄격하게 제어함으로써 시크릿 정보를 읽을 수 없도록 방지할 수 있다.

이런 암호화 키를 관리하기 위한 전통적인 HSM Hardware Security Module 장비는 온프레미스 환경에는 적합할 수 있지만 하이브리드, 멀티 클라우드 확장에는 유연하게 대응하기 어려우며 멀티 클라우드를 고려한다면 클라우드 기반 키 관리 방안을 찾아야 한다.

예를 들어 하시코프 Vault는 시크릿이 스토리지에 저장되기 전에 암호화 키를 통해 자동으로 암호화하는데, 이 암호화된 키를 보호하기 위한 수단으로 마스터 키를 사용하여 이중 잠금을 한다. 마스터 키는 봉인 해제 unseal 과정을 거쳐야 생성할 수 있는데 Vault를 설정 없이 디폴트로 사용하는 경우, 샤미르 공유 알고리즘 Shamir's Secret Sharing[11] 을 적용하여 마스터 키를 공유 수로 분해하고, 여러 사용자가 초기화 한계 threshold 수 이상을 입력하면 마스터 키가 생성되도록 하여 마스터 키를 보호하고 있다.

11. Shamir's Secret Sharing (SSS)는 분산적인 방법으로 시크릿을 보호하기 위해 사용되며, 시크릿을 공유 수로 분해하고 이 공유들은 원래의 시크릿을 재구성하는데 사용된다. 다른 암호화 키를 보호하기 위해 가장 많이 활용된다.

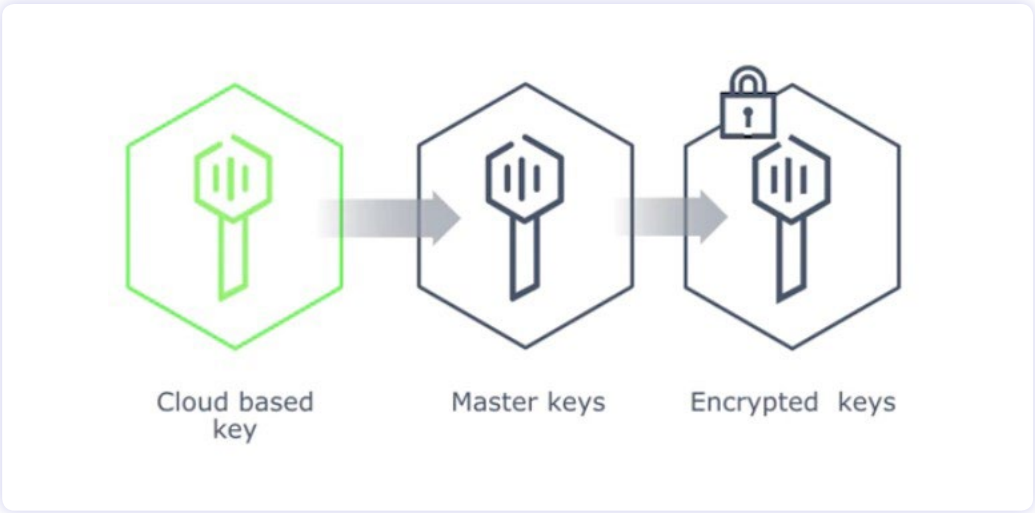
<그림10> Vault의 암호화 키 관리 (Manual Unseal)



출처 : HashiCorp

다만 샤미르 키 공유 방식은 관리자가 부재중일 때에는 사용하기 어려울 수 있으므로 Vault에서는 클라우드 자동 봉인해제 Cloud Auth Unseal 기능을 제공하고 있다. 이 방식은 아래 그림과 같이 마스터키를 공유수로 분해하지 않고 생성한 다음, 클라우드의 KMS 서비스에서 생성한 키로 암호화한 후, Vault에 연결된 스토리지에 마스터키를 저장하여 사용하는 구조다.

<그림11> Vault의 암호화 키 관리 (Cloud Auth Unseal)



출처 : HashiCorp

이렇게 활성화된 마스터 키로 시크릿 액세스용 암호화 키를 복호화 할 수 있게 되며, 이때 Vault는 얻어낸 암호화 키를 스토리지에 저장하지 않고 휘발성인 메모리에 저장하여 사용하기 때문에 해커는 이 암호화 키를 탈취하여 사용할 수 없게 된다.

2) 세분화된 정책을 통한 시크릿 접근제어

저장된 시크릿 정보는 사용 권한이 있는 사용자에게만 액세스 가능해야 하며, 항상 최소 권한의 원칙을 지켜 권한을 부여할 수 있도록 세분화된 정책을 제공해야 한다.

예를 들어 Vault는 사용자 인증 후 토큰을 발행하는데, 발행된 토큰은 일종의 쿠키라고 볼 수 있다. 사용자가 발행된 토큰으로 Vault에 액세스 하면, 인증 메서드가 토큰의 액세스 정책을 반환하며 토큰은 반환된 정책을 기준으로 시크릿에 대한 액세스를 제어한다. Vault의 디폴트 정책은 '거부' deny by defaul[12] 로 설정되어 있기 때문에 관리자가 정책을 바탕으로 적절한 권한을 부여하지 않는다면, 어떠한 시크릿에도 액세스가 불가능하다.

또한 토큰과 정책의 연계는 토큰 발행 시간에 이뤄지기 때문에 로그인 이후 정책을 수정하더라도 이미 발급된 토큰에는 정책 권한이 부여되지 않고 이전에 발행된 권한만 가진다. 기존 토큰의 권한을 업데이트하려면, 업데이트 API를 통해 토큰에 정책 권한을 업데이트 해야 하는 등 굉장히 엄격한 관리 체계를 가지고 있다. Vault에서 제공하는 정책은 아래와 같이 시크릿이 저장된 경로를 기반으로 설정되고 최소 권한을 경로별로 설정할 수 있다.

<그림12> Vault의 시크릿 정책 설정

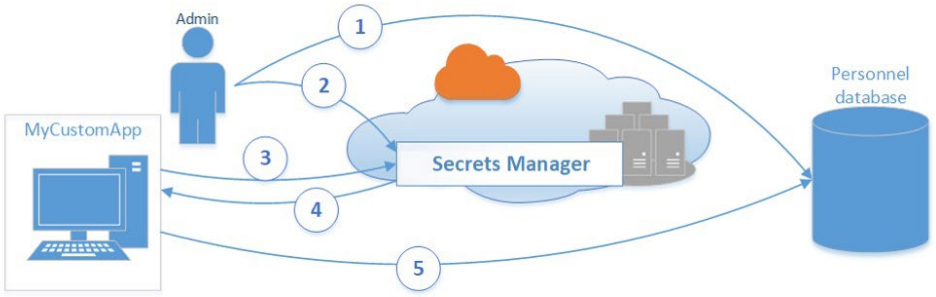
출처 : HashiCorp

12. Deny by default는 일종의 화이트리스트로, 명시적으로 허용되지 않는 모든 규칙을 거부하는 최소 권한의 원칙을 위한 기본 조건이다.

이와 유사하게AWS Secrets Manager[13] 에서는 세분화된 IAM 정책 및 리소스 기반 정책을 토대로 보안 정보에 대한 액세스를 관리할 수 있다. 또한, AWS의 여러 서비스와 통합하여 사용 가능하다.

아래 예시를 통해 AWS Secret Manger에 데이터베이스 자격 증명을 저장한 후, 해당 데이터베이스에 액세스하기 위해 응용 프로그램에서 자격 증명을 사용하는 방식을 확인해볼 수 있다.

<그림13> AWS Secret Manager의 기본 시나리오



출처 : HashiCorp

AWS Secret Manager 사용 설명서

1. 관리자가 MyCustomApp을 통해 DB에 접근 시, 사용할 수 있는 자격증명을 구성한다.
2. 관리자가 Secret Manager를 사용하여 1에서 구성한 자격증명을 암호화하여 보안 암호 텍스트로 저장한다.
3. MyCustomApp에서 DB에 액세스할 때, MyCustomApp은 API를 통해 Secret Manager에 보안 암호 텍스트를 쿼리한다.
4. Secret Manager는 쿼리를 수행하여 보안 암호 텍스트의 암호를 해독한 후, 보안 채널을 통해 클라이언트 앱에 보안 암호를 전달한다.
5. 클라이언트 애플리케이션은 응답에서 자격 증명, 연결 문자열 및 기타 필요한 정보를 구문 분석한 다음, 해당 정보를 활용해 DB서버에 액세스한다.

출처 : AWS Secret Manager 사용 설명서

13. AWS Secrets Manager는 AWS Key Management Service(AWS KMS)를 사용하여 보안 암호의 보호되는 텍스트를 암호화한다. 여러 AWS 서비스에서 키 저장 및 암호화에 AWS KMS를 사용하며 AWS KMS는 유휴 시 보안 암호의 보안 암호화를 지원한다.

3) 다양한 타입의 시크릿 관리

보안이 필요한 모든 데이터를 시크릿이라고 할 수 있다. 데이터는 키와 값만 가지는 단순한 정보일 수도 있지만, SSH 혹은 AWS IAM 사용자와 같은 임시 자격 증명이거나 TLS 인증서, 대용량 파일일 경우도 있어 시크릿의 특성에 맞는 관리가 필요하다.

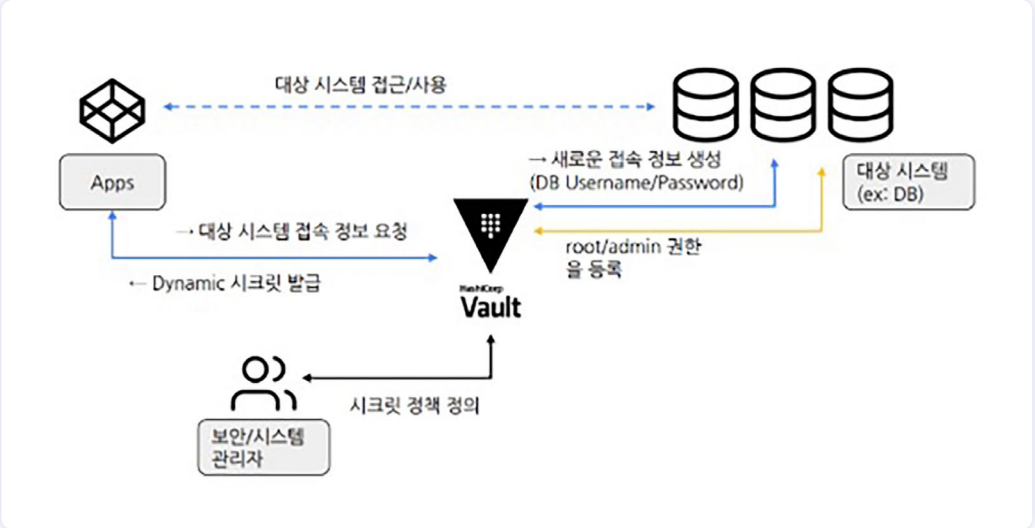
예를 들어 키-값 시크릿은 단순히 스토리지에 저장 후 사용이 끝나더라도 값을 바꿔 계속해서 갱신하여 사용하는 경우가 대부분이지만 TLS 인증서, SSH 임시 자격증명, 시스템이 사용하는 IAM User나 IAM Role 과 같은 자격증명들도 클라우드 환경에서 관리되어야 하는 시크릿의 한 종류로 생각할 수 있다.

특히 이러한 자격증명 시크릿을 시스템에서 사용하는 경우라면, 외부 시스템이 응용 프로그램에 접속을 시도할 때 보안/시스템 관리자가 미리 설정해 놓은 권한을 부여한 임시 자격 증명을 자동으로 발급해주고, 설정된 TTL 시간이 지나거나 관리자가 지정한 오퍼레이션 수를 넘어가면 명시적으로 자격증명을 갱신하지 않는 이상 삭제할 수 있도록 하는 것이 좋다.

Vault에서는 이렇듯 TTL 이 필요한 시크릿을 '동적 시크릿'으로 구분하고 있으며, 동적 시크릿을 발급하는 엔진 중 하나로 데이터베이스 시크릿 엔진이 있다. 이 엔진은 외부 응용 프로그램이 데이터 베이스에 접속을 시도하면 보안/시스템 관리자가 미리 설정해 놓은 권한을 부여한 임시 자격 증명을 발급해준다.

이때 발급된 임시 자격증명은 설정된 TTL 시간이 지나거나 관리자가 지정한 오퍼레이션 수를 넘어가면 명시적으로 자격증명을 갱신(Renew) 하지 않는 이상 삭제되므로, 관리자가 신경 쓰지 않아도 되기 때문에 동적 시크릿을 효율적으로 관리할 수 있게 한다.

<그림14> DB 시크릿 엔진의 데이터베이스 동적 자격증명 생성 프로세스



출처 : HashiCorp

4) 시크릿을 중앙 집중형으로 관리

시크릿 관리 도구를 중앙 집중형으로 사용하기 위해서는 반드시 앞서 언급한 1,2,3 번 조건을 만족해야 한다. 추가로 시크릿 관리 도구는 굉장히 많은 클라이언트의 요청을 처리해야 하거나 관리해야 할 시크릿의 양이 드라마틱하게 많아질 수 있기 때문에 반드시 고가용성 및 멀티 리전에서의 다중 클러스터 운영 및 재해복구 능력을 보유해야 한다.

5) EaaS를 통한 암호화 관리

암호화가 필요한 데이터의 사이즈가 큰 경우 (전체 디스크 암호화, 데이터베이스 암호화 또는 파일 암호화 등), 암호화된 정보를 운영중인 시크릿 관리 도구가 아닌 시스템에 저장하고, 필요시 복호화 하는 것이 더 합당하다. 아울러 이 경우에는 아래와 같이 응용 프로그램 내부에 암호화 키를 관리하여 데이터를 암호화 및 복호화 하는데 사용할 수 있다.

EaaS Encryption as a Service는 단순히 암호화 및 복호화 기능을 서비스로써 제공받아 응용 프로그램에서 직접 암호화를 수행하지 않고도 암호화 기능을 활용할 수 있도록 도와준다. 이 접근 방식은 암호화를 자체적으로 관리할 리소스가 부족한 고객에게 멀티 클라우드 환경에서 데이터를 보호할 수 있는 방법을 알려준다. 보통 이런 서비스를 제공하는 도구는 암호화 키 로테이션 기능이나 여러 암호화 방식을 지원하기 때문에 레거시 응용 프로그램에 대해 보다 용이하게 효율적인 암호화 적용을 할 수 있다.

뿐만 아니라, 단순히 키를 통한 암호화 및 복호화 기능을 수행해주기 때문에 Vault는 스토리지에 어떤 데이터도 저장하지 않게 되며 아래의 워크플로우를 가지게 된다.

암호화

1. 외부 프로그램이 암호화 서비스에 API를 통해 암호화가 필요한 데이터를 전달
2. 암호화 서비스가 해당 정보를 암호화
3. 암호화 서비스가 암호화된 정보를 외부 프로그램에 전달
4. 외부 프로그램이 암호화된 정보를 DB에 저장

복호화

1. 외부 프로그램 DB에서 암호화된 데이터를 쿼리
2. 암호화된 데이터를 API를 통해 암호화 서비스에 전송
3. 암호화 서비스는 관리 중인 키를 사용하여 데이터를 복호화 한 후 외부 프로그램에 전송

이와 같이 외부 프로그램은 암호화 키에 직접 액세스 할 수 없으며, 단순히 암호화 서비스에 암호화 및 복호화 요청만 수행하게 된다.

4. 감사 로깅(Audit Logging)

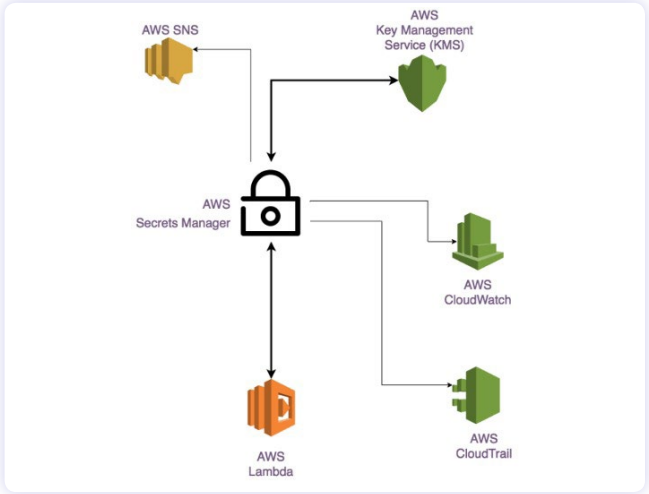
응용 프로그램 접근 관련 보안 문제를 탐지하고 대응하기 위한 '감사' 부분도 이어서 살펴보도록 하자.

멀티 클라우드 환경은 다수의 클라우드 사용자들에게 자원을 제공하기 위해 물리적인 자원을 논리적으로 분할하고 격리하는 멀티테넌시 multitenancy[14] 환경으로, 공유 문제 발생 가능성이 크고 자원의 공유를 위해 여러 사용자가 쉽게 접근 가능하므로 이용 중인 시크릿에 대한 액세스 정보를 기록하고 추적해야 한다. 이를 잘 활용하면 액세스 로그들을 분석하여 위협을 사전에 예측하거나 감사 로깅을 통해 허가되지 않은 활동을 감지할 뿐만 아니라, 보안 조치를 자동화하여 지속적으로 활용할 수 있다.

클라우드 제공자는 보통 이런 기능을 위해 여러 가지 서비스를 제공해주는데, 대표적으로 AWS CloudTrail[15]은 AWS API 요청의 처리내역을 로깅할 수 있으며, 이때 AWS Secret Manager 와 KMS 서비스에 대한 액세스 로깅을 필터링하여 사용할 수 있고, Amazon Detective 서비스는 보안사고 원인을 분석 및 조사 규명하는 서비스로 이용되고 있다.

또한 Amazon GuardDuty[16]는 관리형 위협 탐지 및 통지 서비스로, AWS CloudTrail 로그에 대해 에이전트 없이 머신 러닝을 기반으로 이상행동을 탐지할 수 있다.

<그림15> AWS CloudTrail 과 AWS Secret Manager의 연계



출처 : AWS

또 다른 예로 Vault에 발생한 모든 요청 및 응답에 대한 자세한 로그를 보관하는 감사 로깅 기능을 사용하면, 오류를 포함하여 인증 방식, 인증된 사용자가 한 요청, 그리고 요청을 어떻게 처리했는지에 대한 정보를 저장하고 이 중 민감한 정보는 암호화하여 저장된다.

---

14. Multitenancy는 그 용어에서 유추할 수 있듯 여러 테넌트(Tenant, 사용자)를 가진 아키텍처라는 의미로, 단일 소프트웨어 인스턴스로 서로 다른 여러 사용자 그룹에 서비스를 제공할 수 있는 소프트웨어 아키텍처를 말한다.
15. AWS CloudTrail은 AWS 계정의 거버넌스, 규정 준수, 운영 및 감사가 가능하도록 지원하는 AWS 서비스이다.
16. Amazon GuardDuty는 AWS 계정 및 워크로드를 지속적으로 모니터링하여 악의적인 활동을 모니터링하고 자세한 정보를 제공하는 위협 탐지 서비스이다.

<그림 16> Vault의 감사 로깅

출처 : HashiCorp

결국 클라우드 상에서 운영되는 응용 프로그램은 위와 같은 서비스나 도구를 API로 연계하여 사용함으로써 민감한 정보에 대한 접근을 지속적으로 기록하고, 모니터링 시스템과 연계하여 문제가 발생하면 이를 자동으로 감지한 후 해결할 수 있도록 설계해야 한다.

마치며

클라우드 인프라는 여러 클라우드에 걸쳐 신뢰도가 낮고 네트워크 경계선이 명확하지 않은 환경에서 정적으로 정의된 기존 호스트 기반 ID가 애플리케이션 기반 ID로 전환되는 것을 의미한다. 전통적인 보안 세계에서 우리는 네트워크가 본질적으로 높은 신뢰라고 가정했고, 외부 방어를 최대한 수행하고 내부에서는 보안에 많은 신경을 쓰지 않아도 되었다. 이런 상황이 클라우드 시대가 본격화되면서 '제로 트러스트' 네트워크 접근법으로 바뀌었고 이제 우리는 내부에서도 보안을 구축해야 하는 시대가 되었다.

이와 관련하여 미국 클라우드 보안 연합은 클라우드 상의 보안을 위해 공통적으로 필요한 사항을 정리하여 '서비스로서의 보안' 형태로 해결할 것을 권고하고 있으며, 관련하여 보안 서비스 모델을 제공하고 있다. 이에 따라 클라우드에서 운영되는 응용 프로그램은 이 보안 서비스 표준에 위배되지 않도록 설계되어야 한다.

이를 위해 클라우드 환경에서 운영되는 응용프로그램은 최소한 '자산 식별'과 '사용자별 접근 제어', '시크릿에 대한 데이터 보호' 및 '보안 감사' 부분을 고려하여 설계되어야 하며, 이는 응용 프로그램 내에서 사용자를 인증하고 적절한 권한을 부여하며 철저한 감사를 받는 동시에, 발생하는 각종 민감한 데이터를 보호해야 함을 의미한다.

결국 이런 과제들로 인해 조직이 클라우드로 전환하는 과정에서 마이그레이션 진행에 상당한 진통을 겪을 것으로 예상된다. 클라우드 보안은 클라우드 컴퓨팅 서비스 채택의 주요 저해 요소로 남아 있지만, 반드시 표준 준수를 통해 응용 프로그램에 대한 보안 이슈를 해결해야 하며, 클라우드 보안 서비스 혹은 시크릿 관리 도구와의 연계를 통해 처리하는 것을 권장한다.

[참고자료]

책/논문/보고서

- Hashicorp(2021) Vault Security Whitepaper vault-com-security-whitepaper-v2-digital.pdf
- 김병섭 외 8인 (2019), 멀티 클라우드 기술 개요 및 연구 동향
  https://ettrends.etri.re.kr/ettrends/183/0905183004/35-3_45-54.pdf
- 멀티 클라우드 서비스 공통 프레임워크(Cloud-Barista) 시스템 설계서 Ver. 0.5, 2019
  https://github.com/cloud-barista/docs/blob/master/design/(Cloud-Barista)시스템설계서(v0.5)-2019-10-06.pdf
- 클라우드 보안 기술 및 표준 동향
  https://itfind.or.kr/WZIN/jugidong/1977/file87971870746955102 74-197701.pdf
- 최근 클라우드 보안버시브(SECaaS) 주요 동향 분석
  http://www.kisa.or.kr/uploadfile/201812/201812201702401993.pdf

기사/컬럼/웹사이트

- HashiCorp(2021), Unlocking the Cloud Operating Model
  https://www.hashicorp.com/cloud-operating-model
- HashiCorp(2021), Unlocking the Cloud Operating Model: Security in Multi-Cloud
  https://www.hashicorp.com/resources/unlocking-the-cloud-operating-model-security-in-multi-cloud
- HashiCorp(2021), Why We Need Dynamic Secrets
  https://www.hashicorp.com/blog/why-we-need-dynamic-secrets
- HashiCorp(2021), 5 best practices for secrets management
  https://www.hashicorp.com/resources/5-best-practices-for-secrets-management
- HashiCorp(2021), HashiCorp Vault Secrets Management: 18 Biggest Pros and Cons
  https://www.contino.io/insights/hashicorp-vault
- HashiCorp(2017-06-01), Webinar: Build a Secure Cloud with AWS and HashiCorp Vault
  https://www.youtube.com/watch?v=8kafXiaCdRw
- HashiCorp(2021), HashiCorp State of Cloud Strategy Survey
  https://www.hashicorp.com/blog/hashicorp-state-of-cloud-strategy-survey-welcome-to-the-multi-cloud-era
- HashiCorp(2021), Vault Auth Method
  https://www.vaultproject.io/docs/auth
- HashiCorp(2021), Vault Secrets Engines
  https://www.vaultproject.io/docs/secrets
- HashiCorp(2021), Vault Concepts
  https://www.vaultproject.io/docs/concepts
- HashiCorp(2021), Vault Audit Device
  https://www.vaultproject.io/docs/audit

- HashiCorp(2021), Vault Disaster Recovery
  https://learn.hashicorp.com/tutorials/vault/disaster-recovery
- Vault Auto-unseal using AWS Key Management Service
  https://www.hashicorp.com/resources/vault-auto-unseal-using-aws-key-management-service
- 김선애(2020.09.08), [비대면 업무 보안②] 'ID'로 내려온 보안 경계
  https://www.datanet.co.kr/news/articleView.html?idxno=150415
- 윤대균(2021-04-29), 데브섹옵스(DevSecOps), 왜 중요한가?
  https://slownews.kr/80565
- ChiefExecutive Vol.227(2021-10), 디지털 전환시대 멀티 클라우드의 부상
- Gabia(2021), 왜 멀티 클라우드가 필요한가요?
  https://library.gabia.com/contents/infrahosting/7349/
- RedHat(2018-03-07), 멀티클라우드란 무엇일까요?
  https://www.redhat.com/ko/topics/cloud-computing/what-is-multicloud
- 위키피디아 (2021), Multicloud
  https://en.wikipedia.org/wiki/Multicloud
- 도리(2020-03-23) 멀티 클라우드
  http://blog.skby.net/%EB%A9%80%ED%8B%B0-%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C-multi-cloud/
- 김동진(2020-11-25) 멀티 클라우드 복잡성으로 발생하는 '보안 취약점' 대비해야
  http://it.chosun.com/site/data/html_dir/2020/11/25/2020112500325.html
- Mary K.Pratt (2018-10-24) 멀티 클라우드 보안 과제 3가지와 대응 전략 수립방법
  https://www.itworld.co.kr/news/111217
- 테크비전(2021-07-19) "고민되는 하이브리드 멀티 클라우드 보안
- AWS Secret Manager user Guide
  https://docs.aws.amazon.com/ko_kr/secretsmanager/latest/userguide/intro.html
- CNCF Secret management (2021)
  https://radar.cncf.io/2021-02-secrets-management
- Hasan Tayyar Besik(2018-04-30) Simplified AWS Secrets Manager Flow
  https://htayyar.medium.com/simplified-aws-secrets-manager-flow-127ea697ecac
- AWS Cloud Trail
  https://aws.amazon.com/cloudtrail/
- AWS Guardduty
  https://aws.amazon.com/guardduty/
- Security as a Service
  https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/

플래티어 추천 콘텐츠 목록

인사이트 리포트 Vol.4 - Agile에 대한 허상과 진실

애자일을 적용하는 데 있어 문제점과 실패하는 이유를 살펴보고, 애자일을 잘 적용하기 위한 방법 소개

인사이트 리포트 Vol.4 다운로드

인사이트 리포트 Vol.3 - 메타버스 시대, 실감기술(XR)을 활용한 패션 비즈니스 흐름과 전망

'실감기술'을 활용한 사례 분석을 통해 메타버스 시대를 준비하는 패션 시장의 비즈니스 흐름과 전망을 조명

인사이트 리포트 Vol.3 다운로드

인사이트 리포트 Vol.2 - 두려움 없는 조직문화 만들기

조직 구성원과의 원활한 소통 및 기업 문화·환경 개선을 위한 구체적인 방법 소개

인사이트 리포트 Vol.2 다운로드

인사이트 리포트 Vol.1 - 검색에서 검색 추천으로, 검색 패러다임의 확장

이커머스 업계의 새로운 화두이자 구매 행동과 연관성 높은 '검색'에 대해 집중 분석

인사이트 리포트 Vol.1 다운로드

IT/TECH 리포트 Vol.3 - 이커머스 산업의 AI 기술 동향

이커머스 고객에게 차별화된 쇼핑 경험 및 서비스 제공을 위한 다양한 AI 기술 사례 조명

IT/TECH 리포트 Vol.3 다운로드

IT/TECH 리포트 Vol.2 - 포스트 코로나 시대를 이끌 8가지 IT 기술 동향

포스트 코로나 시대를 이끌고 비즈니스 패러다임의 변화를 가져올 IT 기술 동향 분석

IT/TECH 리포트 Vol.2 다운로드

IT/TECH 리포트 Vol.1 - 이커머스를 위한 인공지능(AI) 개인화 상품 추천 백서

개인화 상품 추천 기술은 어디까지 왔을까? 최신 인공지능 추천 알고리즘 철저히 해부

IT/TECH 리포트 Vol.1 다운로드

★ **트렌드 리포트 Vol.3 - 자사몰을 통한 'D2C' 열풍, 그 이유와 성공을 위한 준비 전략은?**

이커머스 업계에서 D2C가 주목받게 된 이유와 D2C 시장으로의 성공적인 진입을 위해 필요한 전략 분석

👉 트렌드 리포트 Vol.3 다운로드

★ **트렌드 리포트 Vol.2 - 온라인과 오프라인 연결에서 통합으로, OMO 시대의 전환**

국내 커머스 업계의 주목을 받고 있는 OMO(Online Merge with Offline) 소개와 기존 O2O(Online to Offline) 서비스의 한계 분석

👉 트렌드 리포트 Vol.2 다운로드

★ **트렌드 리포트 Vol.1 - 라이브 커머스 흐름과 동향**

최근 이커머스 업계의 화두인 '라이브 커머스'의 동향과 사례 집중 분석

👉 트렌드 리포트 Vol.1 다운로드

★ **마케팅 리포트 Vol.1 - 개인화된 온라인 쇼핑 트렌드와 마케팅 사례**

이커머스 고객의 니즈와 요구를 충족시키기 위한 마케팅 전략인 '개인화'와 관련 마케팅 사례 집중 분석

👉 마케팅 리포트 Vol.1 다운로드

★ **플래티어 온라인 채널**

👉 플래티어 홈페이지

👉 플래티어 페이스북

👉 플래티어 브런치

PLATEER

플랫폼, 그 이상의 가치를 만들어내는 기업, 그리고 사람들

이커머스
e-Commerce

축적된 경험과 솔루션을 토대로 고객의 가치와 함께 성장하는 최고의 e-Commerce 플랫폼 제공

90여 개 기업에서 안정성과 성능이 검증된 솔루션
중대형 프로젝트 경험이 축적된 최고의 전문가 그룹
대한민국 최고 수준의 구축, 개발운영, 컨설팅 제공

데브옵스/협업
DevOps / Collaboration

고객의 환경과 특성에 맞는 지속적이고 통합적인 관리 프로세스, 글로벌 글로벌 툴 체인(Tool Chain) 솔루션 및 서비스 제공

'데브옵스(DevOps)플랫폼' 비즈니스와 '협업(Collaboration) 플랫폼'에 기반한 컨설팅

검증된 글로벌 툴 체인(Tool Chain) 솔루션 제공
체계적 교육과 세미나 수행을 통한 고객사 지원

마테크
Martech

빅데이터, 인공지능(AI) 기술 기반의 실시간 개인화 마케팅, 마케팅 자동화 솔루션 및 컨설팅 제공

빅데이터 처리 AI 기술 기반한 알고리즘 최적화
구매 전환율과 객단가 향상에 집중한 On-Site 마케팅
4천만 명의 고객 데이터로 검증된 마케팅 솔루션

2022 인사이트 리포트

2022.2

디지털 전환 시대,
보안 패러다임의 변화와 대응

2022 인사이트 리포트 Vol.1 | 플래티어

2022년 02월 22일 발행일

(주)플래티어 전략기획실 마케팅팀 발행인

PLATEER