백서 • 2017년 5월

하이브리드 아키텍처를 위한 하이브리드 특권 액세스 관리: 클라우드 전환에 따른 위험에 대한 전략적 접근법

목차

개요

과제

위험을 파악, 관리 및 억제하는 작업은 많은 조직이 하이브리드 아키텍처 전략을 세울 때 고려하는 매우 중요한 요소가 되었습니다. 조직이 비용 효율성과 민첩성 개선을 위해 클라우드 서비스를 전술적으로 사용하는 것 이상을 고려할 때, 점점 증가하는 특권 ID의 액세스는 큰 위험 문제로 다가오게 됩니다. 정적 인프라를 위해 개발된 기존 접근법은 초기 위험 문제를 해결할 수는 있겠지만 동적인 분산 인프라에 대한 지속적 가시성과 일관된 정책 적용을 제공하기에는 역부족입니다.

기회

기업이 얼마나 효과적으로 자동화를 채택하고 혁신 성숙도를 높일 수 있느냐에는 여러 요소가 영향을 미칩니다. 그러나 성숙도 모델 여정의 각 단계에서 주요 액세스 위험을 관리하기 위한 체계적이고 신중한 접근법을 실현하는 데는 보안 도구가 핵심적입니다. 적합한 특권 액세스 플랫폼과 도구를 갖춘 기업은 액세스 관리를 순차적으로 자동화 및 확장하여 위험 완화 작업을 비즈니스 니즈에 맞춰 조율할 수 있습니다.

이점

하이브리드 클라우드 아키텍처와 각각의 특정 액세스 설계를 위해 고안된 특권 액세스 관리는 여러 환경을 잇는 연결 고리인 동시에 모든 특권 작업을 위한 세부적 권한 부여 정책의 동적 적용 지점으로서 유연성을 개선하고, 공급업체 종속 현상을 제한하며, 특권 자격 증명을 이용한 공격에 대한 사전 감지를 지원할 수 있습니다. 클라우드 전환에 맞춰 위험 관리를 조율할 수 있는지 여부는 모든 중요 작업에 대한 액세스를 이용할 수 있는 관리 프로세스에 달려 있습니다.

섹션 1

새로운 아키텍처로 인한 새로운 위험 관리 요구: 하이브리드 아키텍처의 일관성, 가시성 및 자동화

하이브리드 아키텍처와 클라우드 기반 서비스에 대한 특권 액세스를 관리하는 데 이용되는 현재 접근법 중 상당수는 한 가지 패턴을 따릅니다. 바로 기존 암호 보관 기능을 새로운 자격 증명 범주(AWS(Amazon Web Services) 관리 콘솔 키, 퍼블릭 클라우드 서비스에서 애플리케이션을 배포하는 개발자를 위한 SSH 키 또는 자격 증명을 통합하는 AWS EC2 인스턴스를 위한 자동화 프로비저닝 스크립트 등)로 확장하는 것입니다. 분명 기업은 이러한 접근법을 통해 특권 액세스 제어에 대한 기존 투자를 활용함으로써 신규 사용 사례의 기본 보안 및 규정 준수를 달성할 수 있습니다.

하지만 문제는 하이브리드 아키텍처와 클라우드 기반 서비스의 영향력이 훨씬 크다는 점입니다. 따라서 이러한 사용 사례는 IT가 제공되고 작동하는 방법을 혁신해야 하는 필요를 보여주는 선도적 역할을 수행합니다. 물론 하이브리드 클라우드 아키텍처에는 기업이 소유하진 않지만 관리하는 인프라와 기업이 소유하고 관리하는 인프라를 연결하는 일도 수반됩니다. 상당수의 규정 준수 요구 사항과 마찬가지로, 가장 시급한 위험 관리 요구 사항은 여러 환경의 특권 ID에 대한 액세스 및 권한 부여 정책의 일관성과 기업이 관리하는 모든 환경에서 발생하는 사항에 관한 통합적 가시성을 확보하는 것입니다.

작업 수행을 위해 누가 또는 무엇이 특권 자격 증명에 액세스하는지 파악하는 것이 이 요구 사항을 해결하는 시작점이지만, 완전한 솔루션이 될 수 없는 이유는 채택 성숙도로 인해 복잡성이 늘어나는 데다 상당한 수준의 자동화가 필요해지기 때문입니다. 또한 많은 기업이 멀티 클라우드 배포를 촉진하고 공급업체에 대한 장기적 종속을 방지하기 위해 고심하는 것을 고려할 때 이들에게 필요한 것은 여러 환경에서 확장할 수 있고 감독 관리 부족이나 프로비저닝 스크립트에서 자격 증명을 추출하는 맬웨어로 인해 손상될 수 있는 특권 액세스 보안에 대한 위협을 효과적으로 감지할 수 있는 모델입니다.

혁신을 위한 지속 가능한 위험 완화의 또 다른 측면은 바로 특권 액세스 보안이 독립적으로 해결될 수는 없다는 점입니다.

후속 수정 없이 처음부터 목적에 맞게 설계

대체로 클라우드 아키텍처를 채택하기 위한 비즈니스의 추진력은 애플리케이션과 서비스의 딜리버리를 가속화하고 민첩성을 촉진하며 규모의 경제와 운영 비용 절감의 이점을 활용하는 데서 발생합니다. 이러한 비즈니스 니즈의 기술적 영향으로는 현재 범위에 포함되어 있으며 점점 다양해지고 있는 특권 ID(개발자, API, 컨테이너 형태의 코드, 사물 인터넷 게이트웨이 포함)와 이점을 완전히 제공하기 위해 자동화를 활용하는 소프트웨어 딜리버리 프로세스(대체로 DevOps라고 불림)가 있습니다.

따라서 효과적인 특권 액세스 위험 관리를 위해서는 클라우드 리소스 액세스 및 작업에 대한 권한 부여를 어떻게 자동화된 워크플로우와 프로세스에 통합할지에 관한 답을 얻어야 합니다. 최소 특권 액세스 및 역할 기반 액세스에 쉽게 이해할 수 있는 원칙을 적용하면 거버넌스의 토대가 될 수 있지만, 이는 정책 적용 자체가 동적 분산 인프라에서 쉽게 통합 및 인스턴스화된 경우에만 가능합니다.

클라우드 서비스 검색과의 통합은 어떤 계정과 자격 증명을 관리 대상에 포함해야 하는지를 결정하는 데 유용한 단계입니다. 그러나 근본적인 문제는 새로운 자격 증명 세트를 관리 범위에 포함하는 것만이 아니라 다음을 목적으로 어떻게 특권 액세스를 자동화할 수 있느냐입니다.

- 특권 자격 증명을 이용하는 작업을 특정 ID에 다시 연결
- 특정 개별 작업을 실시간으로 역할 기반 액세스 정책과 대조하여 평가
- 분석을 통한 모니터링, 보고 및 사전 감지를 위해 멀티 클라우드 환경에서 모든 작업 통합

유일한 적용 지점이 클라우드 엔드포인트가 아닌 자격 증명 액세스를 제한할 경우 위험 관리는 인프라가 동적이고 클라우드 엔드포인트 자체가 임시적일 때에도 특권 ID의 작업과 변경 사항이 아닌 프론트 도어에 상응하는 정도로만 확장됩니다. 클라우드 엔드포인트(AWS EC2 인스턴스 등)에서의 작업이 아닌 프론트 도어에만 집중하면 역설적이고 역효과적이게도 관리 감독이 거의 이뤄지지 않은 상태에서 권한이 과도하게 부여된 사용자 클래스가 생성될 수 있습니다. 물리적 서버의 공유 계정 관리를 위해 설계된 접근법을 후속 수정하는 것으로는 기본 요구 사항은 해결할 수는 있지만 클라우드 전환 성숙도 모델을 지원하기 위한 기반이 될 수 없습니다.

섹션 2

하이브리드 클라우드 특권 사용자 관리의 과제: 암호 관리에서의 탈피

ID 및 액세스 관리 영역에서는 사용자에게 액세스 권한을 제공하는 경우 위험도 당연히 발생합니다. 하이브리드 아키텍처와 클라우드 기반 서비스의 환경에서는 관리자나 특권 엔터티에 리소스를 프로비저닝할 수 있는 능력이 부여될 때 위험이 더욱 심화됩니다. 상당한 권한이 주어지는 단일 하이퍼바이저 또는 클라우드 서비스 관리 콘솔 계정에 피해가 발생하면 개별 서버 인스턴스뿐 아니라 전체 클라우드 데이터 센터에 영향을 미칠 수 있습니다.

물리적 데이터 센터에서는 여러 체크 포인트로 리소스를 프로비저닝하는 일이 수동 프로세스로 이뤄지는 반면, 클라우드 관리자는 리소스와 서비스를 훨씬 더 넓은 범위로 프로비저닝하고, 실행한 다음 다시 프로비저닝 해제할 수 있습니다. 예를 들어 Amazon Web Services가 자사 발행 문건에서 지적한 바와 같이, 보안 그룹 액세스 정책으로 특별히 제한 및 관리하지 않는 보안 자격 증명은 사용자에게 "AWS 리소스를 무한대로 사용할 수 있는 권한을 부여"합니다. 마찬가지로, AWS Management Console에 대한 자격 증명이 있는 사용자는 "기업이 권한을 부여하는 수준까지" AWS 리소스에 액세스할 수 있습니다.

그러나 고객은 이러한 액세스 권한 부여의 정책 로직이 최소 특권 액세스 원칙에 비춰볼 때 적절한지, 규정 준수나 직무 분리와 같은 내부 요구 사항과 일관되는지 확인해야 할 부담을 안게 됩니다. SSH 키(자동 등록으로 애플리케이션 개발자 및 서비스에서 널리 이용됨)와 같은 기존 특권 계정 및 자격 증명에 대한 검색을 통합하면 거버넌스와 모니터링 프레임워크의 범위를 벗어나거나 특권 자격 증명이 노출된 계정이 초래할 위험을 완화할 수 있습니다.

인증 그 이상의 기능을 수행하는 액세스 제어

클라우드 및 애플리케이션 특권 자격 증명을 암호 저장소에 등록하면 공유 암호에 대한 액세스 권한을 가진 사용자뿐 아니라 특권 계정에 대한 액세스 권한이 있는 사용자 역시 편리하게 관리할 수 있습니다. 그러나 더 시급한 문제는 특권 자격 증명이 어떻게 사용될지, 이러한 자격 증명이 인증하는 리소스 액세스 수준은 무엇인지, 클라우드 엔드포인트에서의 작업이 정책에 의해 어떻게 제어 및 관리될지에 관한 것인데, 특히 컨테이너 채택으로 인해 클라우드 인스턴스의 평균 수명이 몇 주가 아닌 며칠로 줄어들고 있어 해결이 시급합니다. 2017년 4월 연구 결과에 따르면 "Docker 채택 기업에서 컨테이너의 평균 수명은 2.5일인 반면 모든 기업에 존재하는 기존의 클라우드 기반 VM은 평균 수명이 23일입니다."[1]

역할 기반 액세스 정책을 적용하여 어느 특권 ID로든 액세스할 수 있는 자격 증명 클래스를 제한하는 것은 첫 단계로서 합리적이지만, 아래와 같은 여러 질문이 체계적으로 해결되지 않으면 많은 위험이 여전히 존재하게 됩니다.

- 사용자 또는 서비스가 자격 증명 액세스 권한을 가지면 수행할 수 있는 특정한 개별 작업은 무엇인가?
- 어떤 역할이 어떤 특권 자격 증명에 적합하며, 해당 자격 증명 액세스 권한을 가진 사용자에게도 적합한가?
- 신뢰할 수 있는 역할 기반 액세스 정책의 소스는 무엇인가?

- 이러한 정책이 여러 환경, 특히 멀티클라우드 배포에서 업데이트되고 조정되는가?
- 플랫폼 운영자는 언제 특권 액세스 권한을 얻는가? 이들에게 어느 수준의 권한 부여가 적절한가?
- 관리자 액세스는 어떻게 관리되는가? 권한 부여를 위해 SSH 키를 이용하는 기존 개발 프로세스가 어떻게 특권 액세스 관리 거버넌스에 통합될 수 있는가?

점점 더 많은 조직이 정책을 온프레미스, 가상화 및 여러 클라우드 서비스 환경과 같은 자사 하이브리드 아키텍처의 모든 요소에 걸쳐 일관적으로 적용하고 이러한 정책으로 인해 정책 로직 사일로가 생성되지 않도록 하는 데 어려움을 겪고 있습니다. 많은 기업에서 이미 특권이 점점 증가하는 현상을 겪고 있는데, 이러한 상황에서 관리자는 합법적인 운영상의 이유로 제어를 완화하거나 역할을 광범위하게 정의하게 됩니다. 여기서 문제는 취약한 액세스 정책이 위험을 키울 뿐 아니라 이러한 작업 방식 때문에 보안 인식 프로그램 및 분석을 통해 유의미하고 세분화된 인텔리전스를 생성하여 사전 대응적인 감지를 수행하기가 더욱 어려워진다는 점입니다.

섹션 3

특권 관리에 대한 현대적 접근법: 아는 데 그치지 않고 실천할 수 있는 해법

하이브리드 아키텍처의 위험을 완화하기 위해서는 특권 자격 증명에 인증을 적용하는 것이 필수 요소임에 유의해야 합니다. 관리자가 AWS Admin Console에 액세스하든, 개발자가 CI/CD 환경의 프로세스에 SSH 키를 활용하든, API가 자격 증명에 액세스하여 스크립트를 실행하든, 엔터티가 규정 준수 요건은 물론 로깅, 감사 및 보고에 대한 액세스 권한을 받을지 설정하려면 특권 자격 증명을 릴리스하기 전에 인증을 요청하는 것이 중요합니다. 엔터티가 자격 증명에 액세스할 권한을 부여받았는지 확인하려면 신뢰할 만한 저장소에 대한 인증 시도 검증이 제일 먼저 수행되어야 합니다. 그러나 인증이 위험 완화와 더불어 클라우드 전환 여정과 액세스 보안의 효과적인 통합 모두에 핵심적인 여러 질문에 대한 해답이 될 수는 없습니다.

기본 인증에서 클라우드 환경에 맞춰 조율되고 일관적인 직무 분리 정책 적용과 더불어 더 높은 수준의 자동화를 지원하는 권한 부여로 효과적으로 전환하려면 몇 가지 요소를 추가로 마련해야 합니다.

아키텍처 측면에서 특권 액세스 관리 적용은 쉽게 인스턴스화되고 동적 환경에서 운영 가능하며, API를 통해 통신하는 서비스 기반 환경에 정책을 적용할 수 있도록 설계되어야 합니다. 결과적으로 이러한 정책은 네이티브 플랫폼 도구에서 쉽게 추출할 수 있는 최소 특권 액세스 원칙과 역할을 기반으로 액세스를 정의하는 신뢰할 수 있는 소스에 따라 결정되어야 합니다.

이러한 아키텍처가 마련되면 자동화된 검색을 통해 적용이 이뤄지고 이러한 적용으로 정책이 특정 환경 및 기본 운영 요소(AWS ID 관리 규칙 및 EC2 인스턴스 등)로 변환되어야 합니다. 신뢰할 수 있는 데이터 소스를 유지 관리하고 정책을 특정 환경에 연결하면 특권이 증가할 가능성을 제한하고 멀티클라우드 배포에서 정책 로직의 사일로가 생성되는 것을 억제할 수 있습니다. 또한 이러한 접근법은 특정 ID(사람 또는 서비스)의 활동에 대한 통합적 가시성을 높이고 여러 환경에서의 페더레이션을 지원합니다.

클라우드 전환에 맞춰 위험 관리를 성공적으로 조율하려면 하이퍼바이저 등을 통해 수행되거나 API를 통해 호출되는 실제 작업을 관리하고, 그 결과로 특권 자격 증명(특권 액세스 자격 증명을 이용하는 사람에 국한되지 않음)을 사용해야 합니다.

하이브리드 아키텍처를 위한 특권 액세스 관리 재구상

- 동적 분산 환경 내에서 종속성 없이 동작할 기능을 생성하고 AMI 또는 가상 이미지로서 실행되며 효과적으로 확장할 수 있는 탄력성 보장
- API를 활용하여 가상화된 리소스 및 클라우드 리소스를 자동으로 검색한 후 적절한 자격 증명 및 액세스 관리 정책을 프로비저닝(또는 프로비저닝 해제)
- API를 API 호출을 가로채 세부적 권한 부여 정책의 적용 지점으로 활용할 뿐 아니라 대상 환경에 대한 통합 수단으로 활용
- 최소 권한 액세스와 직무 분리에 대한 분석 기반 평가, 정책 테스트 및 특권 ID 수명 주기 관리를 통합
- 고속 임시 인프라를 처리할 때에도 통합된 로깅, 기록 및 모니터링을 통해 사전 대응적 감지를 지원
- 기업 자격 증명을 기반으로 SSO와 페더레이션을 지원하여 거버넌스를 중앙 집중화하고 모든 특권 ID의 이벤트 데이터와 로그의 통합된 단일 소스를 확보

섹션 4

AWS 특권 ID에 대한 거버넌스: 권한 부여 및 정책 적용 자동화 대 액세스 제어

정적 인프라를 위해 설계된 방법을 이용하여 클라우드 서비스 콘솔에 대한 관리 액세스를 보호하는 작업과 하이브리드 아키텍처에 대한 보안을 혼동하는 경향이 있는 접근법과 달리, CA 테크놀로지스의 접근법은 고객이 서비스와 리소스에 대한 특권 액세스를 관리 및 모니터링하는 데 더욱 효과적이고 지속 가능한 접근법을 구현할 수 있도록 지원합니다. CA는 AWS에 대한 액세스 제어의 중앙 집중식 지점을 단순히 제공하는 대신 기업이 동적 분산 환경 내의 특권 자격 증명과 관련 있는 모든 상호 작용, 조치 및 작업에 대해 세분화되고 감사된 권한 부여 정책을 적용하도록 지원합니다.

CA PAM(CA Privileged Access Manager)은 하이브리드 클라우드 아키텍처, 특히 Amazon Web Services와 가상화된 데이터 센터를 위해 주요 보안 및 거버넌스 연결 기능을 제공합니다. 이에 더해 CA 제품의 아키텍처를 사용하면 클라우드 서비스 환경 내의 자동화와 유연성을 높일 수 있으므로, 기업은 프록시를 여러 클라우드 데이터 센터에서 인스턴스화하고 확장할 수 있습니다.

권한이 부여된 특권 ID만 AWS Admin Console, 작업, 리소스 및 API에 액세스하고, 모든 액세스와 활동이 관리자, 플랫폼 운영자, 개발자 또는 서비스 등 기업에서 발급한 특정 ID로 역추적될 수 있도록 하는 것은 초기에 해결할 중요 요구 사항입니다. 그러나 CA PAM은 특권 액세스 거버넌스를 규모에 따라 효과적으로 제공하고 AWS 운영 자동화를 촉진하기 위해 액세스 및 권한 부여 정책을 중앙 집중식으로 정의하고 이러한 정책을 로컬로 적용할 수 있는 기능을 기반으로 구축되었습니다. 액세스 및 권한 부여 정책을 로컬로 또는 상황별로 적용하는 데는 2가지 주요 차원이 있습니다.

정책 자동화 및 전파

CA PAM은 종속성 없이 동적 임시 환경에서 원활하게 운영되므로 EC2 인스턴스와 프로비저닝 이벤트 같은 리소스 검색 프로세스의 결과가 정책에 자동으로 연결될 수 있습니다. CA PAM은 계정이 검색된 후에 등록되는 2단계 프로세스를 이용하는 대신 지속적인 권한 부여 정책 적용 모델을 촉진합니다.

따라서 정책은 신뢰할 만한 소스에 따라 결정되며, 클라우드 IAM 서브시스템은 중앙 집중식 정책을 사용하게 됩니다. 이러한 접근법은 일관성을 보장하고 특권 증가에 따른 문제를 억제할 뿐 아니라 프로세스가 하이브리드 환경에서 실행될 때 정책이 확장되도록 지원하고 공급업체에 종속될 가능성을 줄이기도 합니다. AWS를 전략적 실행 환경으로 간주하는 기업의 경우에도 공급업체에 대한 종속 문제는 가장 시급하고 핵심적인 사안입니다.

세부적인 실시간 적용

CA PAM은 프론트 도어에 대한 액세스 권한을 가진 사용자를 관리할 뿐 아니라 권한 부여 적용의 더 심층적인 계층을 제공하여 클라우드 엔드포인트(이 경우 EC2 인스턴스)까지 확장하며, 클라우드 관리 콘솔이나 AWS 관리 API를 통해 호출되는 정책에 대한 호출을 가로채고 평가하여 작업을 실시간으로 제한할 기능도 제공합니다. AWS API 프록시는 AWS 클라우드 내에서 분산된 고가용성 리소스로서 실행되며, 세션을 위해 동적으로 생성된 브로커로서 역할을 수행하여 대상 리소스와의 모든 상호 작용을 관리함으로써 일관된 제어력과 가시성을 보장합니다.

오늘의 니즈를 해결하고 내일의 위험에 대비

AWS Admin Console 액세스의 기능과 인프라 및 클라우드 엔드포인트의 동적 특성 때문에, 역할과 최소 권한 액세스 기반의 권한 부여 결정에 대한 실시간 평가는 위험 관리와 운영 성숙도 조율의 주요 구성 요소가 되었습니다. 또한 기업이 공급업체에 대한 종속 문제를 경계하는 동시에 플랫폼별 규칙 및 그룹에서 일정 수준의 추상화를 요구하므로, 대상 환경의 구조와 자동으로 통합할 수 있는 능력을 확보하고 중앙 집중화된 정책 로직을 재사용해야 하는 니즈가 생겼습니다.

CA PAM은 AWS API 호출 및 대응을 평가하여 사전 정의되고 감사된 정책을 기반으로 관리자, 개발자 또는 운영자나 특권 애플리케이션이 취할 수 있는 조치를 명령 수준에 이르기까지 제한할 수 있는 능력과 프록시 기반 아키텍처를 제공하여 다른 동종 기술보다 앞선 서비스를 제공합니다. CA AWS API 프록시는 프로그래밍 방식으로 호출되는 운영 및 작업까지 이러한 제어력을 확장하여 제공합니다.

CA의 접근법은 위협 감지에 대한 데이터 기반 접근법에 추가적인 이점을 제공하는데, 바로 분산 인프라 전반의 활동 로그가 중앙 집중식으로 수집되고 시스템이 높은 충실도를 달성하는 것입니다.

섹션 5

결론

클라우드 기반 서비스가 더욱 전략적으로 채택되고 하이브리드 아키텍처 성숙도에 더 많은 초점이 맞춰지면 여러 새로운 환경의 특권 액세스 관리와 관련된 기존 문제가 다시 반복되는 것으로 그치지 않습니다. 대신 기업이 혁신과 자동화를 추진하려면 특권 ID와 자격 증명의 관리 및 보호 방법을 재구상해야 하며, 이를 통해 특권 ID와 자격 증명이 공격에 악용되지 않도록 방지할 뿐 아니라 위험 관리를 새로운 프로세스와 동적 인프라에 통합해야 합니다.

API가 통합과 경계 정의 모두를 위한 수단으로써 사용되는 이러한 새로운 환경에서 특권 액세스 관리는 이제 글로벌 액세스 및 권한 부여 정책을 적용하는 동시에 동적으로 기능할 수 있어야 합니다. 그러나 중요 리소스에 대한 역할 기반 액세스를 보장하고, 이후 프로세스에서 세분화된 권한 부여 정책을 적용하며, 규정 준수와 손상 또는 유출의 사전 대응적 감지를 위해 가시성을 유지 관리 하는 등 핵심 요구 사항이 남아 있습니다.

자세한 내용은 **ca.com/pam**을 참조하십시오.

CA 테크놀로지스에 연결

CA 테크놀로지스(NASDAQ: CA)는 회사가 혁신을 통해 애플리케이션 경제에서 기회를 잡을 수 있도록 하는 소프트웨어를 만듭니다. 소프트웨어는 모든 업계에서 모든 기업의 핵심 요소입니다. CA는 계획부터 개발, 관리 및 보안에 이르기까지 전 세계 기업들과 협력하여 모바일, 프라이빗 및 퍼블릭 클라우드, 분산 및 메인프레임 환경에서 업무, 거래, 소통의 방식을 바꾸고 있습니다.
자세한 내용은 **ca.com/kr**을 참조하십시오.

1 Datadog, "8 Surprising Facts About Real Docker Adoption," 2017년 4월.

CS200-270961_0517