IBM **Cloud**

클라우드 플랫폼 보호 가이드

목차

IBM

주요 시사점

1 이상적인 경우, 클라우드 공급자는 귀사의 ID 관리 시스템을 자체 플랫폼에 통합할 수 있어야 하며, 필요 시 사용할 수 있는 신뢰성이 있는 ID 관리 솔루션을 반드시 제공해야 합니다.

2 신뢰 구축의 일환으로, 클라우드 플랫폼이 워크로드 및 신뢰할 수 있는 컴퓨팅 호스트를 기반으로 하여 마이크로 세분화를 위한 잘 통합된 방화벽, 보안 그룹 및 옵션을 제공하는지 확인하십시오.

3 클라우드 공급자는 귀사가 모든 데이터 저장소 및 서비스에서 키를 독점적으로 관리할 수 있도록 BYOK 솔루션을 제공할 수 있어야 합니다.

4 컨테이너에 대한 최고의 보안 모범 사례는 배포 이전 및 실행 도중에 취약점을 검사하는 것입니다.

5 클라우드 플랫폼 보안은 효과적으로 액세스를 제어하고, 작업 부하 수준에서 작동하며, 세부적인 활동을 추적하고, 온 프레미스 시스템에 통합되어야 합니다.

클라우드 기반 애플리케이션의 보안을 다시 생각하기

앱 개발 및 작업 부하 관리를 위해 클라우드 고유 모델로 이동하는 조직이 늘어남에 따라 클라우드 컴퓨팅 플랫폼은 기존의 경계 기반 보안 모델의 효율성을 급속하게 제한하고 있습니다 effectiveness of the traditional perimeter-based security 경계 보안은 여전히 필요하지만 그 자체로는 충분하지 않습니다. 클라우드의 데이터 및 애플리케이션은 과거의 엔터프라이즈 경계 외부에 있으므로, 새로운 방식으로 보호해야 합니다.

클라우드 기본 모델로 전환하거나 하이브리드 클라우드 앱을 배포하려고 계획하는 조직은 클라우드 기반 작업 부하를 보호하는 기술로 기존의 경계 기반 네트워크 보안을 보완해야 합니다. 기업은 클라우드 서비스 공급자가 인프라에서 스택을 보호하는 방법에 대해 확신을 가져야 합니다. 플랫폼 보안에 대한 신뢰를 확립하는 것이 공급자 선택의 기본입니다.

클라우드 보안의 동력

데이터 보호 및 규정 준수는 클라우드 보안의 주요 동력 중 하나이며, 동시에 클라우드의 채택을 방해하고 있습니다. 이러한 우려 사항을 해결하려면 개발 및 운영의 모든 측면을 고려해야 합니다. 클라우드 고유 애플리케이션을 사용하는 경우에는 데이터가 개체 저장소, 데이터 서비스 및 클라우드에 분산될 수 있으므로 잠재적인 공격에 대해 다양한 전선이 구성됩니다. 그리고, 공격은 정교한 사이버 범죄집단과 외부 소스에서 오는 것이 아닙니다. 최근의 조사에 따르면 응답자의 53%가 지난 12개월 동안 내부의 공격을 확인했습니다.[1]

클라우드 보안의 5개 기본 요소

조직이 클라우드 플랫폼을 사용할 때 특별한 보안 요구 사항을 해결하려면, 공급자는 신뢰할 수 있는 기술 파트너가 되어야 하며 그렇게 예상합니다. 실제로 조직은 조직의 고유한 요구 사항과 관련된 보안의 5개 측면을 기반으로 클라우드 공급자를 평가해야 합니다.

1. **ID 및 액세스 관리:** 인증, ID 및 액세스 제어
2. **네트워크 보안:** 보호, 격리 및 세분화
3. **데이터 보호:** 데이터 암호화 및 키 관리
4. **애플리케이션 보안 및 DevSecOps:** 보안 테스트 및 컨테이너 보안 포함
5. **가시성 및 인텔리전스:** 패턴의 로그, 플로우 및 이벤트에 대한 모니터링 및 분석

클라우드 플랫폼에서 ID 확인 및 관리 액세스

클라우드 플랫폼의 모든 상호 작용은 신원 확인부터 시작하여 관리자, 사용자 또는 서비스와 같은 상호 작용을 수행하는 대상 또는 작동을 확인합니다. API가 작동하는 경우, 서비스는 자체 ID를 사용하기 때문에, 클라우드 고유 앱을 성공적으로 실행하려면 이 ID를 기반으로 서비스에 API 호출을 정확하고 안전하게 수행하는 기능이 필수적입니다.

API 액세스 및 서비스 호출에 대해 ID를 인증하는 일관된 방법을 제공하는 공급자를 찾아야 합니다. 또한, 클라우드에 호스팅된 애플리케이션에 액세스하는 최종 사용자를 식별하고 인증하는 방법이 필요합니다. 예를 들어, IBM® Cloud는 개발자가 모바일 및 웹 앱에 인증을 통합할 수 있는 방법으로 App ID를 사용합니다 App ID as a way for developers to integrate authentication into their mobile and web apps.

강력한 인증은 허가를 받지 않은 사용자의 클라우드 시스템 액세스를 차단합니다. 플랫폼 ID 및 액세스 관리(IAM)가 매우 중요하기 때문에, 기존 시스템을 보유한 조직은 클라우드 공급자가 회사의 ID 관리 시스템을 통합하도록 요구해야 합니다. 이것은 종종 개인 ID와 속성을 여러 시스템에 연결하는 ID 연합 기술을 통해 지원됩니다.

서비스 호출을 인증하는 이유는 무엇입니까?

마이크로 서비스 기반 아키텍처의 경우 API를 사용하면 애플리케이션에서 통신을 하고 데이터를 공유할 수 있습니다. 애플리케이션이 실행되면, API를 사용하여 다양한 작업을 완료하는 데 필요한 서비스를 호출합니다. 예를 들어, 애플리케이션이 데이터에 대해 개체 저장소 서비스를 호출할 수 있습니다. 요청 이행 과정의 일부로서 개체 저장소 서비스 자체가 키 관리 서비스를 호출하여 데이터 해독에 필요한 암호화 키를 얻을 수 있습니다. 그리고 사용자 경험 제공의 일부로서, 앱이 API를 사용하여 사용자 신원 정보에 액세스하고 앱 사이에서 콘텐츠를 게시하고(예를 들어, 앱의 콘텐츠를 Twitter에 게시) 위치별 정보를 제공할 사용자의 위치를 결정할 수 있습니다. **이러한 모든 작업은 보안 문제가 발생한다는 것을 의미합니다.**

클라우드 공급자는 API 또는 서비스에 액세스해야 하는 사용자 또는 서비스의 ID를 인증하는 일관된 방법을 가져야 합니다. 물론, 인증의 일부로서 감사의 목적으로 모든 액세스 요청 세션과 트랜잭션을 기록해야 합니다. **API와 서비스는 귀중한 지적 재산을 보유하고 있을 가능성이 높습니다. 단지 사용하려고만 하는 사람은 필요하지 않습니다.**

협업할 클라우드 공급자에게 IAM 아키텍처와 시스템이 모든 기반을 제공한다는 점을 입증하게 하십시오. 예를 들어, IBM Cloud의 경우 ID 및 액세스 관리는 다음과 같은 몇 가지 주요 기능을 기반으로 합니다(그림 1):

ID

- 각 사용자는 고유한 식별자를 지닙니다
- 서비스 및 애플리케이션은 서비스 ID로 식별합니다
- 리소스는 클라우드 리소스 이름(CRN)으로 식별하고 접근합니다
- 사용자와 서비스는 ID를 통해 인증 및 발급되는 토큰입니다

액세스 관리

- 사용자와 서비스가 리소스에 액세스를 시도하면, IAM 시스템이 액세스 및 작업의 허용 또는 거부 여부를 결정합니다
- 서비스가 동작, 리소스 및 역할을 정의합니다
- 관리자는 다양한 리소스에 대해 사용자 역할 및 사용 권한을 할당하는 정책을 정의합니다
- 클라우드에서 호스팅하는 API, 클라우드 기능 및 백엔드 리소스까지 보호가 확장됩니다

클라우드 공급자의 보안을 평가하는 경우, 사용자를 특정 리소스뿐만 아니라 해당 리소스의 특정 작업으로 제한할 수 있는 공용 리소스 이름과 함께 액세스 제어 목록을 찾아야 합니다. 이러한 기능을 통하여 권한이 없는 외부 및 내부 액세스에 대해서 데이터를 보호할 수 있습니다.

자체의 엔터프라이즈 ID 공급자(Enterprise IdP)를 클라우드로 확장하는 경우, Enterprise IdP를 사용하는 기존 엔터프라이즈 애플리케이션뿐만 아니라 클라우드 고유 앱을 빌드할 때 특히 유용합니다. 사용자는 여러 개의 시스템이나 ID를 사용하지 않아도 클라우드 고유 응용 프로그램 및 기본 애플리케이션에 원활하게 로그인할 수 있습니다. 복잡성을 줄이는 것은 언제나 소중한 목표입니다.

주요 시사점

이상적인 경우, 클라우드 공급자는 귀사의 ID 관리 시스템을 자체 플랫폼에 통합할 수 있어야 하며, 필요 시 사용할 수 있는 신뢰성이 있는 ID 관리 솔루션을 반드시 제공해야 합니다.

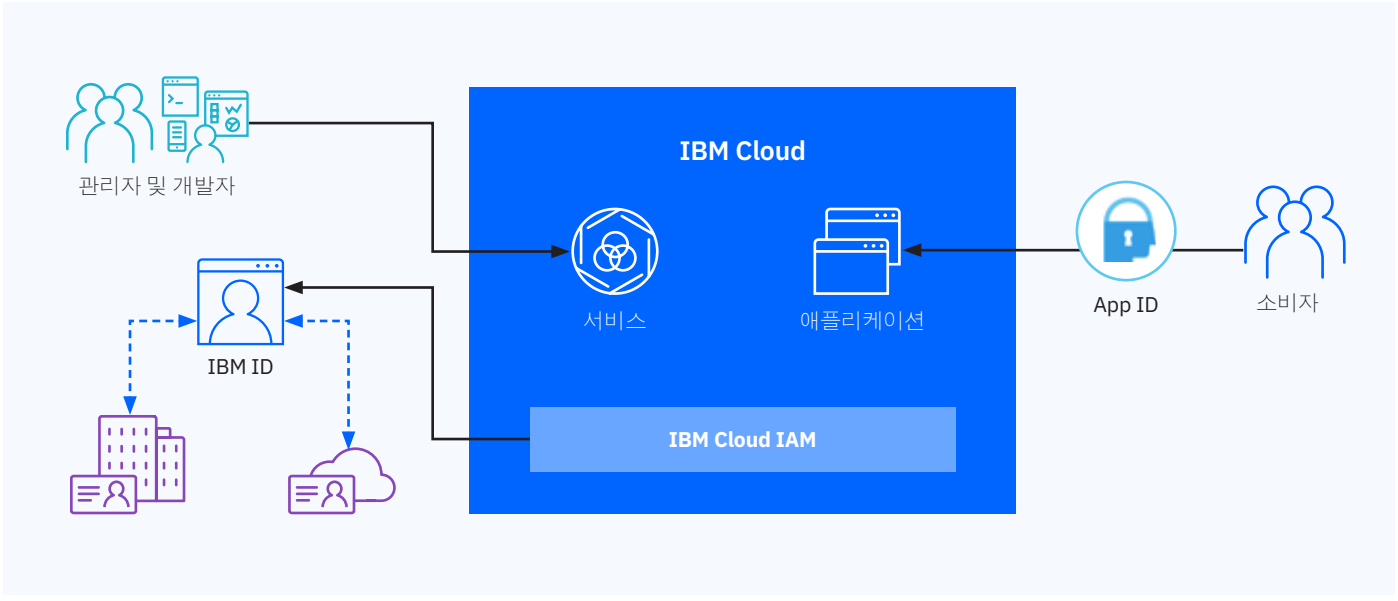

그림 1. 공급자가 관리하는 클러스터 요소와 고객이 관리하는 클러스터 요소를 분리합니다.

네트워크 격리 및 보호 다시 정의하기

많은 클라우드 공급자는 네트워크 세분화를 사용하여 동일한 네트워크에 있는 장치 및 서버에 대한 액세스를 제한합니다. 또한, 공급자는 물리적 인프라 위에 가상 격리 네트워크를 만들고 사용자 또는 서비스를 특정 격리 네트워크로 자동 제한합니다. 이것 및 다른 기본 네트워크 보안 기술은 클라우드 플랫폼에 대한 신뢰 구축에 필요한 기본 사항입니다.

클라우드 공급자는 웹 애플리케이션 방화벽부터 가상 사설 네트워크 및 서비스 거부 공격 완화책과 같은 보호 기술까지 소프트웨어 정의 네트워크 보안 및 사용당 요금 부과 서비스로 제공합니다. 다음의 기술을 클라우드 컴퓨팅 시대의 중요한 네트워크 보안책으로 고려하십시오.

보안 그룹 및 방화벽

클라우드 고객은 경계 보호(가상 사설 클라우드/서브넷 수준 네트워크 액세스)를 위해 네트워크 방화벽을 삽입하고, 인스턴스 수준 액세스를 위해 네트워크 보안 그룹을 생성하는 경우가 있습니다. 보안 그룹은 클라우드 리소스에 대한 액세스를 할당하기 좋은 첫 번째 방어선입니다. 이 그룹을 사용하여 인스턴스 수준의 네트워크 보안을 손쉽게 추가하여 공용 및 사설 네트워크에서 출입하는 트래픽을 관리할 수 있습니다.

많은 고객의 경우 경계 네트워크 및 서브넷을 보호하기 위해 경계 제어가 필요하며, 가상 방화벽은 이러한 필요를 충족시키기 위해 쉽게 배포할 수 있는 방법입니다. 방화벽은 원하지 않는 트래픽이 서버에 영향을 주는 것을 방지하고, 공격 표면을 줄이기 위해 디자인되었습니다. 클라우드 공급자는 가상 네트워크와 하드웨어 방화벽을 모두 제공하여 전체 네트워크 또는 서브넷에 대한 사용 권한 기반 규칙을 구성할 수 있어야 합니다.

VPN 역시 온 프레미스 리소스에 대한 클라우드의 안전한 연결을 제공합니다. 하이브리드 클라우드 환경을 실행하는 경우에는 반드시 사용해야 하는 사항입니다.

마이크로 세분화

여러 가지 소규모 서비스를 위해 클라우드 전용의 애플리케이션을 개발하면 네트워크 세분화를 사용하여 격리가 가능한 보안상의 장점이 있습니다. 네트워크 구성 및 네트워크 프로비저닝 자동화를 통해 마이크로 세분화를 구현하는 클라우드 플랫폼을 찾으십시오. **마이크로 서비스 모델을 기반으로 설계된 컨테이너형 애플리케이션은 확장성이 있는 작업 부하 격리를 지원하는 표준이 되고 있습니다.**

주요 시사점

신뢰 구축의 일환으로, 클라우드 플랫폼이 작업 부하 및 신뢰할 수 있는 컴퓨팅 호스트를 기반으로 하여 마이크로 세분화를 위한 잘 통합된 방화벽, 보안 그룹 및 옵션을 제공하는지 확인하십시오.

암호화와 키 관리로 데이터 보호

데이터를 안전하게 보호하는 것은 디지털 비즈니스, 특히 금융 서비스 및 의료와 같이 규제가 엄격한 업계의 보안 기본 사항입니다.

클라우드 고유 애플리케이션과 관련된 데이터는 개체 저장소, 데이터 서비스 및 클라우드 전반으로 확산될 수 있습니다. 전통적인 애플리케이션은 전용 데이터베이스, 전용 VM을 지니고 중요한 데이터는 파일에 보관합니다. 이러한 경우, 저장 및 전송 상태 모두에 대해 중요한 데이터를 반드시 암호화해야 합니다.

기업은 클라우드 운영자 또는 권한이 없는 다른 사용자가 적합한 인식을 갖지 않고 데이터에 액세스하는 것에 대해 우려해야 하며 데이터 액세스에 대해 완전한 가시성을 기대해야 합니다. **암호화를 사용하여 데이터에 대한 액세스를 제어하고, 암호화 키에 대한 액세스를 제어하는 것이 안전 장치가 됩니다.** 그 결과, BYOK(Bring-your-own-keys) 모델이 이제 클라우드 보안 요구 사항으로 되었습니다. 이를 사용하면 중앙에서 암호화 키를 관리할 수 있으므로, 루트 키가 키 관리 시스템의 경계를 벗어나지 않는 것을 확인하고 모든 키 관리 수명 주기를 감사할 수 있습니다(그림 2).

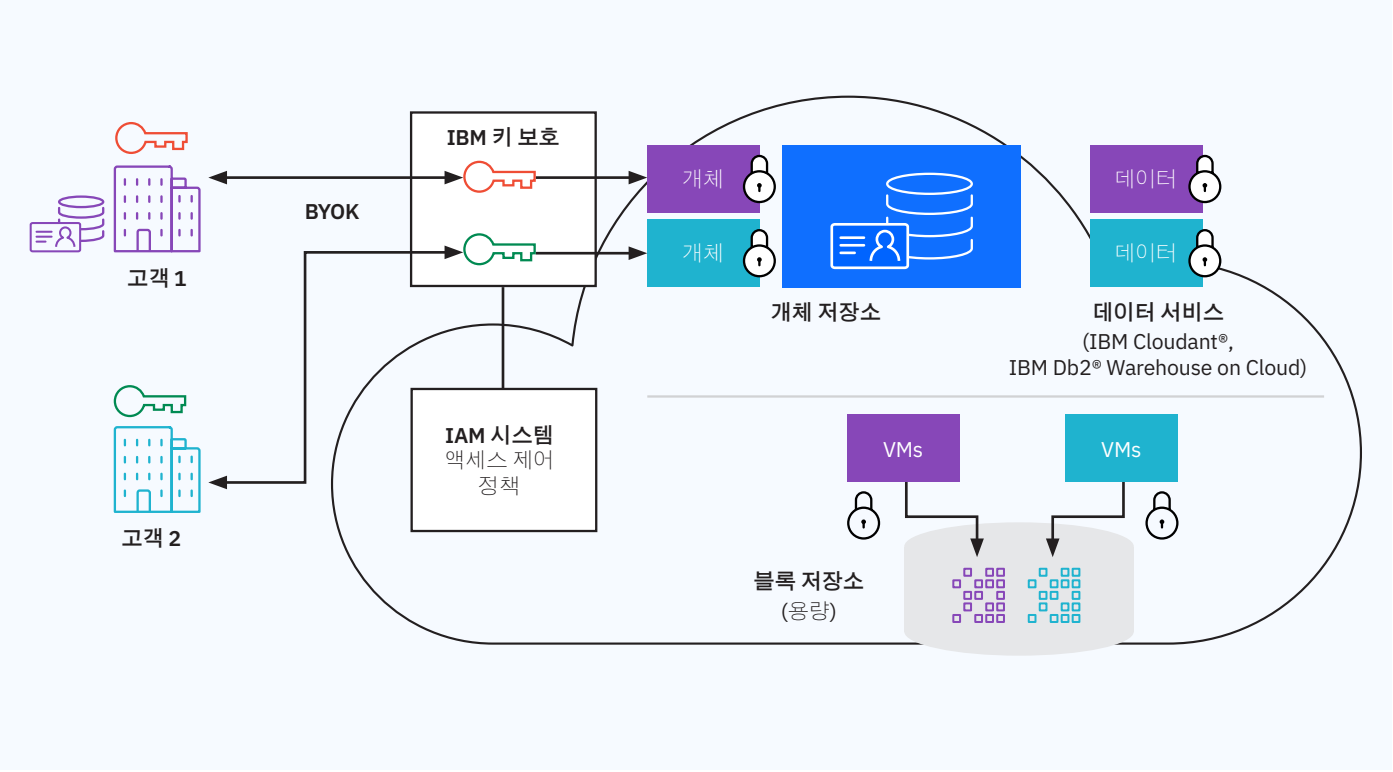

그림 2. BYOK 솔루션의 아키텍처.

신뢰할 수 있는 컴퓨팅 호스트

결론은 하드웨어입니다. 신뢰할 수 없는 호스트에 중요한 데이터와 애플리케이션을 배포하려는 사람은 없습니다. 측정-검증-실행 프로토콜을 갖춘 하드웨어를 제공하는 클라우드 플랫폼 공급자는 컨테이너 오케스트레이션 시스템 내에 배포된 애플리케이션에 대해 매우 안전한 호스트를 제공합니다.

Intel TXT(Trusted Execution Technology) 및 TPM(Trusted Platform Module)은 클라우드 플랫폼에 대한 신뢰를 보여주는 호스트 수준 기술의 사례입니다. Intel TXT는 시스템 또는 BIOS 코드를 손상시키거나 플랫폼 구성을 변조하여 중요한 정보를 도용하려는 소프트웨어 기반 공격에 대해 보호를 제공합니다. Intel TPM은 운영 체제에 대한 시스템 제어를 해제하기 전에 무단 변경을 방지하여 시스템 시작 프로세스를 보호하는 데 도움이 되는 하드웨어 기반 보안 장치입니다.

저장 및 전송 상태에서 데이터 보호

BYOK를 이용하는 내장형 암호화를 사용하여 온 프레미스 또는 클라우드 기반 데이터에 대한 관리를 유지할 수 있습니다. 이는 클라우드 고유 애플리케이션 배포에서 데이터에 대한 액세스를 제어하는 훌륭한 방법입니다. 이 접근법에서 고객의 키 관리 시스템은 온 프레미스에서 키를 생성하여 공급자의 키 관리 서비스에 전달합니다. 이 접근법에는 블록, 개체 및 데이터 서비스와 같은 스토리지 형식 전체에 대해 저장된 데이터 암호화가 포함됩니다.

전송 중인 데이터의 경우, 보안 통신 및 전송은 TLS/SSL(Transport Layer Security/Secure Sockets Layer)을 통해 이루어집니다. 또한, TLS/SSL 암호화를 사용하는 경우 암호화 시스템이나 인프라를 관리할 필요 없이 규정 준수, 보안 및 거버넌스를 입증할 수 있습니다. 클라우드 플랫폼에 대한 신뢰성에는 SSL 인증서를 관리하는 능력이 있어야 합니다.

감사 및 규정 준수 요구 충족

자체 암호화 키를 제공하고 서비스 공급자가 액세스하지 못하는 클라우드에 보관하는 경우, CISO 준수 감사에 필요한 정보를 가시화하고 제어할 수 있습니다.

주요 시사점

클라우드 공급자는 귀사가 모든 데이터 저장소 및 서비스에서 키를 관리할 수 있도록 BYOK 솔루션을 제공할 수 있어야 합니다.

DevOps의 보안 자동화

DevOps 팀은 클라우드 고유의 서비스를 만들고 컨테이너 기술을 사용하기 때문에 자동화 파이프라인 내에 보안 검사를 통합하는 방법이 더욱 더 필요합니다. Docker Hub와 같은 사이트는 공개 교환을 촉진하므로, 개발자는 필요한 것을 다운로드하여 이미지 준비 시간을 쉽게 단축할 수 있습니다. 그러나, 이러한 유연성 덕분에 배포에 앞서 레지스트리에 있는 모든 컨테이너 이미지를 정기적으로 검사해야만 합니다.

자동 검색 시스템은 이미지를 실행하기 전에 이미지의 잠재적 취약성을 검색하므로 신뢰를 확보하는 데 도움이 됩니다. 귀사가 DevOps 파이프라인 보안의 일부로서 정책을 만들도록 허용하는지(예: "취약한 이미지를 배포하지 마십시오" 또는 "이러한 이미지를 제품화 배포하기 전에 경고합니다") 플랫폼 공급자에게 문의하십시오.

예를 들어, IBM Cloud Container Service는 VA(Vulnerability Advisor) 시스템을 제공하여 정적 및 동적 컨테이너 검색을 제공합니다. VA는 클라우드 고객의 사설 레지스트리에 있는 모든 이미지의 모든 레이어를 검사하여 이미지 배포 전에 취약성이나 맬웨어를 탐지합니다. 레지스트리 이미지를 단순히 검사만 하면 정적 이미지에서 배포된 컨테이너로 이동하는 등의 문제를 놓치기 때문에, VA는 실행 중인 컨테이너에서 비정상 상태를 검색합니다. 또한, 계층화된 알림 형식으로 권장 사항을 제공합니다.

주요 시사점

컨테이너에 대한 최고의 보안 모범 사례는 배포 이전 및 실행 도중에 취약점을 검사하는 것입니다.

DevOps 파이프라인에서 보안 자동화에 도움이 되는 다른 VA 기능은 다음과 같습니다.

- **정책 위반 설정:** VA를 사용하여 관리자는 세 가지 유형의 이미지 오류 상황을 기반으로 이미지 배포 정책을 설정할 수 있습니다. 즉, 알려진 취약성이 있는 패키지 설치, 원격 로그인 사용 그리고 암호를 쉽게 추측한 일부 사용자의 원격 로그인 가능성입니다.
- **모범 사례:** 현재, VA는 암호 최소 기간 및 최소 암호 길이와 같은 설정을 포함하여 ISO 27000을 기준으로 26개의 규칙을 확인합니다.
- **보안 구성 오류 감지:** VA는 각 구성 오류를 문제를 표시하고, 이에 대한 설명을 제공하며, 수정에 필요한 조치 과정을 권장합니다.
- **IBM X-Force®와 통합:** VA는 5개의 타사 소스에서 보안 인텔리전스를 가져오고 공격 벡터, 복잡성 및 알려진 방법의 가용성과 같은 기준을 사용하여 각 취약점을 평가합니다. 평가 시스템(중요, 높음, 보통 또는 낮음)은 관리자가 취약성의 심각도를 신속하게 파악하고 수정 우선 순위를 정하는 데 도움이 됩니다.

수정 단계에서 VA는 패치 적용을 위해 실행 중인 이미지를 방해하지 않습니다. 이를 대신하여 IBM은 레지스트리에서 "황금" 이미지를 수정하고 컨테이너에 새 이미지를 배포합니다. 이 접근법으로 해당 이미지의 모든 향후 인스턴스화는 동일한 수정을 갖게 됩니다. VM은 엔드포인트 보안 서비스를 사용하여 VM을 패치하고 Linux 보안 취약점을 수정하는 전통적인 처리가 가능합니다.

Kubernetes 관련 사항

DevOps 팀이 인기있는 Kubernetes 컨테이너 오케스트레이션 소프트웨어를 사용하는 경우에는 원하는 도구를 계속해서 사용할 수 있는지 확인하십시오. Kubernetes container orchestration software 또한, 플랫폼이 새로운 기능 제공 및 기존의 Kubernetes 클러스터를 얼마나 쉽게 관리하는지 평가하십시오.

클라우드 플랫폼 공급자가 자사의 Kubernetes 시스템으로 Calico 및 Istio를 지원하는지 문의하십시오. Calico와 Istio는 애플리케이션과 작업 부하 보안을 지원하는 Kubernetes 의 두 가지 중요한 구성 요소입니다. Calico 는 컴퓨팅 노드에서 작업 부하에 할당된 IP 주소 관리를 단순화하고, 각 컴퓨팅 노드의 제어 목록에 액세스하여 보안 정책을 시행하도록 프로그램합니다 Istio는 구성 레이블을 통해 설정 및 시행되는 정책 정의를 사용하여 Kubernetes 포드 또는 클러스터 내의 마이크로 서비스 간 통신에 인증서 기반 제어를 제공합니다. Istio provides certificate-based control of communication among microservices within a Kubernetes pod or cluster.

지능형 모니터링을 통한 보안 면역 시스템 구축

클라우드로 이동할 때 CISO는 가시성이 낮고 제어가 손실되는 것을 자주 염려합니다. 특정 키가 삭제되거나, 구성이 우발적으로 바뀌어 서버가 온 프레미스 혹은 엔터프라이즈 보안 운영 센터(SOC)에 다시 연결되면 회사 조직의 전체 클라우드가 다운될 수 있는데, 운영 엔지니어는 클라우드 기반 작업 부하, API, 마이크로서비스 등의 모든 것에 완전한 가시성을 기대하면 안 됩니까?

내역 및 감사 로그에 대한 액세스

클라우드 공급자 또는 귀사이건 무관하게 모든 사용자 및 관리 액세스는 자동으로 기록되어야 합니다. 내장 클라우드 활동 추적기는 API, 웹 및 모바일 액세스를 포함하여 플랫폼 및 서비스에 대한 모든 액세스 내역을 만들 수 있습니다. 귀사는 이러한 로그를 사용하여 엔터프라이즈 SOC에 통합시킬 수 있어야 합니다.

기업 보안 인텔리전스

모든 로그 및 이벤트를 온 프레미스 보안 정보 및 이벤트 관리(SIEM) 시스템에 통합할 수 있는 옵션이 있는지 확인하십시오(그림 3). 일부 클라우드 서비스 공급자는 발생문제 관리와 보고, 보안 경고 실시간 분석 그리고 하이브리드 배포 전반에 대한 통합 보기가 가능한 보안 모니터링을 제공합니다.

예를 들어, IBM QRadar®는 조직의 필요에 따라 확장 가능한 일련의 보안 인텔리전스 솔루션을 제공하는 포괄적인 SIEM 솔루션입니다. 이 솔루션의 머신 러닝 기능은 예측 가능한 보안 면역 시스템을 구축하는 방식으로 위협 패턴을 학습합니다.

전문 지식을 갖춘 보안 관리

조직 내에 중요한 보안 전문 지식이 없는 경우에는 보안을 관리할 수 있는 공급자를 찾아보십시오. 일부 공급자는 보안 사고를 모니터링하고 다양한 업계의 위협 정보를 적용하며, 이 정보를 상호 연관시켜 조치를 취할 수 있습니다. 사내 보안 및 관리 보안 서비스를 통합하는 단일 창을 제공할 수 있는지 물어보십시오.

주요 시사점

클라우드 플랫폼 보안은 효과적으로 액세스를 제어하고, 작업 부하 수준에서 작동하며, 세부적인 활동을 추적하고, 온 프레미스 시스템에 통합되어야 합니다.

그림 3. 기업 SIEM / SOC에 클라우드 가시성 통합.

비즈니스 성공을 촉진하는 보안

클라우드 기술이 디지털 비즈니스를 운영하는 데 있어 점점 더 중요해지고 있기 때문에 고객이 직접 사용하는 애플리케이션이 의존하는 데이터, 애플리케이션 및 클라우드 인프라를 보호하기 위한 올바른 기능의 조합과 제어를 제공하는 클라우드 공급자를 잘 선택해야 합니다. 플랫폼 보안 솔루션은 ID 및 액세스, 네트워크 보안, 데이터 보호, 애플리케이션 보안, 가시성과 인텔리전스 등의 5가지 주요 클라우드 보안 집중 영역을 담당해야만 합니다. 목표는 기술에 대한 걱정을 줄이고, 핵심 비즈니스에 더욱 집중하는 것입니다.

잘 확립된 클라우드는 다음과 같이 중요한 비즈니스 및 IT 장점을 제공합니다:

- **가치 창출 시간 단축:** 보안이 이미 설치 및 구성되어 있으므로, 팀은 자원을 쉽게 프로비저닝하고 신속하게 사용자 경험을 프로토타입화하고 결과를 평가하며 필요에 따라 반복할 수 있습니다.
- **자본 지출 감소:** 클라우드에서 보안 서비스를 사용하게 되면 서버, 소프트웨어 라이센스 및 장치를 포함하여 상당한 선행 비용을 감축할 수 있습니다.
- **관리 부담 감소:** 클라우드 플랫폼에 대한 신뢰를 성공적으로 수립하고 유지하여 올바른 보안 서비스를 제공하는 공급자는 관리 부담을 가장 많이 담당하므로, 보고 및 자원 관리 비용을 절감합니다.

자세한 정보

IBM의 클라우드 보안 및 관련 기술 및 서비스의 5가지 주요 영역에 대한 자세한 내용은 다음 사이트를 참조하십시오: ibm.com/cloud/security

커넥티드를 유지하십시오

IBM Cloud 블로그

팔로우 하십시오

@IBMcloud
페이스북

연락처

링크드인
유튜브

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

2018년 1월 미국에서 제작

[1] 2017년 11월 발간된 내부자 위협 2018 보고서,
http://crowdresearchpartners.com/portfolio/insider-threat-report