AWS 보안 다시보기

aws 파트너 네트워크

고급
기술 파트너

SaaS 파트너

이상적인 IT 보안 환경 제공

많은 기업들은 그 규모와 상관없이 자본 효율성, 민첩성, 확장성에 대한 요구가 더욱 커짐에 따라 전례 없는 규모의 IT 리소스를 AWS(Amazon Web Services)로 이동시키고 있습니다. AWS 같은 새로운 동적 환경의 경우, 정보 보안 문제에 민감한 조직에서는 신중하게 접근해야 합니다.

그러나 AWS는 AWS보다 작은 조직이 이용할 수 있는 대부분의 대체 서비스보다 질적으로 우수한 IT 보안 환경을 제공하는 것으로 볼 수 있습니다. AWS에서 기본 제공되는 가시성, ID 및 정책 시행을 통해 문제를 즉시 탐지할 수 있기 때문에 알려진 문제를 예방할 수 있습니다. AWS의 기능과 AWS 리소스의 행동에서 알려지지 않은 위협을 탐지할 수 있는 Cisco® Stealthwatch Cloud를 결합하면 AWS 고객에게 민첩성, 확장성, 비용 효율성을 갖춘 보안 솔루션을 제공할 수 있습니다.

AWS가 보안에 이상적인 환경으로 손꼽히는 이유는 무엇일까요? 모든 보안 전문가들이 동의할 수 있도록 단기적 측면에서 보자면, 대규모 기업에서 겪고 있는 까다로운 기존 정보 보안 문제 대부분이 AWS를 구축한 첫날에 해결되기 때문입니다. 이에 대한 심층적인 답변은 궁극적으로 데이터 분석 및 컴퓨팅 접근 방식이 클라우드 네이티브 형태인 오늘날의 기업에게 미래 지향적이고 안정적인 보안을 성공적으로 제공하기 때문이지만, 우선 단기적 측면의 답변에 대해 살펴보도록 하겠습니다.

목차

AWS 보안으로 해결된 문제

기존 온프레미스 환경의 문제로는 가시성, ID 및 액세스 관리, 정책 선언 및 시행이 있습니다. 이러한 문제는 AWS에서 모두 해결됩니다.

사용 중인 온프레미스 네트워크를 생각해 보십시오. 다음과 같은 경우에 사용할 수 있는 체계적인 감사 추적이 있다고 가정해 보십시오.

- 네트워크에 새 디바이스가 들어오거나 나가는 경우
- 사용자가 특정 디바이스에서 인증하는 경우
- 사용자가 정보 서비스를 사용하는 경우
- 누군가 라우팅 테이블 또는 방화벽 규칙 같은 인프라 요소를 변경하는 경우
- 누군가 사용자 또는 디바이스의 보안 권한 또는 조직 역할 수정
- IT 자산에 네트워크 상호 작용이 있는 경우

한 단계 더 나아가, 이러한 정보가 유연하게 프로그래밍 방식으로 제공된다고 가정해 보십시오. 또한, 모니터링하려는 다른 애플리케이션 레벨 로그를 제공받고 사용자, 애플리케이션 및 IT 리소스의 활동을 추적해 주는 맞춤형 메트릭도 캡처할 수 있다면 어떨까요? 이러한 가시성은 AWS에서 즉시 이용할 수 있는 기능입니다. AWS에서 가시성과 계측은 해결된 문제입니다.

이 가시성 및 계측을 지원하기 위해 AWS는 SOA(Service-Oriented Architecture)로 운영됩니다. AWS 공간에서의 모든 작업은 웹 서비스 엔드포인트에 대한 인증받은 API 호출로 시작됩니다. 즉, 특정 API 호출은 새로운 사용자 어카운트를 생성하고, 방화벽 규칙을 변경하고, 서버를 인스턴스화할 때 인증된 사용자 크리덴셜을 사용하여 이루어집니다.

AWS 리소스에 대한 모든 변경은 인증된 API 호출을 통해 이루어지며, 이러한 모든 호출은 기록되어 어카운트 소유자가 사용할 수 있게 됩니다. 이러한 감사 추적은 AWS의 피상적인 기능이 아니라, 사용자에게 사용한 만큼의 비용을 청구할 수 있게 해 주는 AWS의 본질적인 기능입니다. 따라서 이 기능이 머지않아 사라질까 봐 걱정할 필요가 없습니다. 이러한 API 가시성은 이론상으로만 가능한 것이 아닙니다. AWS에서 가시성은 AWS CloudTrail이라는 서비스에 의해 제공됩니다. 이 서비스는 AWS 공간에 대한 모든 액세스 또는 수정 요청에 대해 구조화된 피드를 제공합니다.

다음 두 가지 AWS 서비스도 중요한 가시성 기능을 기본으로 제공합니다. 첫째, Amazon CloudWatch는 AWS 리소스와 애플리케이션에 대한 모니터링 서비스입니다. Amazon Elastic Compute Cloud(서버), Amazon Relational Database Service(데이터베이스), Amazon Elastic MapReduce(데이터 분석) 등 AWS의 모든 기본 제공 서비스는 Amazon CloudWatch를 사용하여 사용량 및 상태를 보고합니다. 개발자는 Amazon CloudWatch의 오픈 API를 사용하여 맞춤형 애플리케이션 및 서비스에 로그 및 메트릭 모니터링을 추가할 수 있습니다.

또한, Amazon CloudWatch는 문제 상태를 탐지하고 자동 작업을 작동하는 알람 및 맞춤형 이벤트를 지원합니다. 예를 들어, Amazon CloudWatch 알람을 사용하여 자동 확장 그룹을 관리할 수 있으므로, 유지 관리하는 사용률 메트릭에 대응하여 AWS 공간에서 사용되는 서버의 수를 동적으로 확장하거나 축소할 수 있습니다. Amazon CloudWatch를 통해 특정 애플리케이션 및 서비스의 작업과 활동에 대한 가시성을 얻을 수 있습니다.

둘째, VPC 플로우 로그 서비스는 AWS 서버가 보내거나 받는 네트워크 트래픽에 대한 가시성을 제공합니다. AWS VPC 리소스에 네트워크 상호 작용이 있는 경우 VPC 플로우 로그는 네트워크 대화의 세부 사항, 즉 소스 및 대상 네트워크 인터페이스와 IP 주소, 포트, 프로토콜, 바이트 수 및 패킷수 등을 기록합니다. 온프레미스 네트워크 보안 사용 경험이 있는 경우 이것이 엔터프라이즈급 스위치, 라우터 및 방화벽에서 생성할 수 있는 NetFlow 로그와 비슷하다고 생각하실 것입니다. 이러한 로그는 AWS VPC(Virtual Private Cloud) 공간 내 모든 네트워크 상호 작용에 대한 감사 가능 기록을 나타내므로 매우 중요합니다.

따라서 이 세 가지 AWS 서비스(AWS CloudTrail, Amazon CloudWatch, VPC 플로우 로그)는 모두 AWS 공간에 대한 종합적인 가시성을 제공합니다. 이러한 서비스를 통해 어카운트 사용, 사용자 행동, 인프라 관리, 애플리케이션 및 서비스 활동, 네트워크 활동에 대한 가시성을 즉각적으로 확보할 수 있습니다. 중요한 것은, AWS 사용자가 이러한 서비스를 제공하는 데 필요한 유지 관리 또는 자본 비용의 부담 없이 이러한 서비스의 이점을 누릴 수 있다는 점입니다.

가시성에 대한 이러한 논의는 IAM(Identity and Access Management)의 중요성 또한 보여줍니다. 사실, 구조적이고 감사를 받는 IAM 크리덴셜이 없으면 AWS를 사용할 수 없습니다. AWS에는 AWS 서비스 상호 작용의 모든 측면에 대해 크리덴셜을 제공하는 완전 통합 IAM 서비스가 기본적으로 제공됩니다. 이 서비스는 어떤 사용자 ID가 있고 이들이 어떤 권한을 소유하고 있는지 보여주므로 AWS 공간을 관찰하고 조작할 수 있습니다. AWS의 네이티브 IAM 서비스를 사용하여 전체 ID를 관리하고 관리 워크플로에 액세스할 수 있으며 IAM을 서드파티 서비스와 통합할 수도 있습니다. IAM 서비스를 통하지 않고는 어떤 경우에도 AWS 리소스(서버, 데이터베이스, 스토리지, 로그, 정책 개체 등)를 보거나 조작할 수 없습니다. AWS는 가시성과 마찬가지로 ID 및 액세스 관리 문제도 해결하였습니다.

마지막으로, AWS에는 종합적인 정책 선언 및 시행을 위한 기본 제공 서비스인 AWS Config가 있습니다. 이 서비스는 AWS 리소스 및 그 내부 컨피그레이션에 대해 임시 및 지속적 감사를 모두 제공합니다.

간단한 예로, 모든 서버에서 사용자 비밀번호가 비활성화되어 AWS 공간에서 키 기반 액세스만 가능하도록 원하는 경우를 가정해 보겠습니다. AWS Config는 모든 서버에 대한 감사 보고서를 쉽게 실행하게 해 줍니다. 조금 더 복잡한 예로, "모든 서버에서 포트 22를 사용할 수 없음", "관리자만 방화벽 규칙을 변경할 수 있음", 또는 "사용자 Betsy만 새 사용자 어카운트를 생성할 수 있으며, 이러한 작업은 화요일에만 가능함" 과 같은 경우를 가정해 보도록 하겠습니다. AWS Config에서 이것이 모두 가능한데, 그 이유는 다음과 같습니다.

- AWS 리소스의 모든 변경 내용은 AWS 엔드포인트에 대한 인증된 호출을 통해 관리됩니다.
- AWS 리소스 및 해당 리소스의 사용을 관리하는 모든 정책이 코드에 표시되고 시행됩니다.

2016년 여름에 AWS Config Rules 서비스가 완전히 릴리스되어 정책 위반의 탐지가 자동화되었습니다. AWS Config Rules는 사실상 위반 시 이벤트 알림을 생성하는 지속적 컨피그레이션 쿼리입니다. 예를 들어, 모든 서버 디스크가 암호화되었는지 확인하기 위해 정기적으로 AWS Config 쿼리를 실행하는 대신, AWS Config Rules를 사용하여 이 조건에 대해 지속적으로 서버 디스크를 면밀히 검토할 수 있습니다. 이 방법을 사용하면 모든 AWS 자산의 구성된 상태를 정확하게 보여주는 컴플라이언스 보고서를 지속적으로 자동 생성할 수 있습니다.

AWS가 모든 보안 문제를 해결합니까?

AWS에서 가시성, ID 및 액세스 관리, 정책 시행 문제가 해결된다면, 모든 보안 문제가 해결된다는 의미일까요? 물론 아닙니다.

AWS 보안의 공동 책임 모델이 이를 설명해 줍니다. AWS는 컴퓨팅을 지원하는 유연한 플랫폼이며 오류를 허용하는 충분한 유연성을 제공합니다. AWS 환경에서는 알려진 취약점이 있는 소프트웨어의 사용을 피하는 것에서부터 적절한 사용자 크리덴셜을 유지 관리하는 것에 이르기까지 사용자가 자신의 공간에서 실행하는 리소스를 보호하기 위해 반드시 주의를 기울이도록 요구합니다.

그리고, AWS에서는 일반적으로 다른 곳에는 존재하지 않는 보안에 대한 문제가 발생합니다. 흥미롭게도, 이러한 새로운 문제는 "하드웨어를 소유하지 않으므로 물리적으로 보안을 유지할 수 없습니다."와 같은 우려와는 아무런 관련이 없습니다. 그보다는 기술과 규모에 대한 변화 속도, 소프트웨어의 개발 및 유지 관리와 관련한 본질적인 변화와 관계가 있습니다. 이러한 문제에 대해서는 나중에 살펴보겠습니다.

AWS의 보안에 대한 간단한 사고방식

AWS 공간을 확보할 때 던지는 두 가지 중요한 질문이 있습니다. 바로, "AWS는 어떻게 구성되는가?"와 "AWS는 무슨 일을 하는가?"입니다. 이러한 질문에 명확하게 답변할 수 있다면, AWS에서 보안에 대한 공동 책임을 다하고 있다고 믿을 수 있습니다.

어떻게 구성되는가? 모든 AWS 리소스의 컨피그레이션 상태를 아는 것이 중요합니다. 모든 서비스, 디바이스, 사용자 및 정책 개체의 컨피그레이션 상태를 알고 있는 경우, 그것이 기대 수준 및 모범 사례와 일치하는지, 알려진 문제 및 취약점과 관련이 있는지 확인할 수 있습니다. 컨피그레이션 상태를 이해하고 비판적으로 검토하며 정책을 준수하고 있음을 보여주는 것은 보안 및 위험 관리를 위한 대부분의 규정 준수 형식을 구성하는 핵심 지식입니다.

앞에서 설명했듯이, AWS Config에서는 자산 생성, 액세스, 사용을 관리하는 정책의 준수를 사용자가 주석을 다는 방식으로 쉽게 표현하고 시행할 수 있습니다. Amazon Inspector 등 다른 서비스를 사용하면 각 AWS 서버에 에이전트를 설치할 수 있으므로 서버에서 다음 사항을 정기적으로 확인할 수 있습니다.

- 모범 사례와 일치하는 내부 서버 컨피그레이션이 있음
- 알려진 취약점을 보여주는 소프트웨어를 포함하지 않음(CVE 아카이브에서 설명)

AWS Config 및 Amazon Inspector의 평가 기능이 AWS 리소스의 컨피그레이션 상태를 효과적으로 자동 추적합니다. 사람이 직접 개입하지 않고도 소프트웨어 패치, 크리덴셜 갱신, 잘못된 컨피그레이션 수정 등의 시정 조치를 취할 수 있습니다. 요약하자면, AWS 리소스의 컨피그레이션을 추적하면 알려진 문제를 식별하고 수정할 수 있으며 이로 인한 보안 문제를 방지할 수 있습니다.

무슨 일을 하는가? 모든 문제가 사전에 알려져 있지는 않습니다. 컨피그레이션 관리 및 평가를 통해 탐지할 수 없는 상황으로는 알려지지 않은 소프트웨어 취약점, 도난된 크리덴셜, 사용자 실수, 의도하지 않은 정책 선택의 결과가 있습니다. 리소스에서 허용되는 동작과 리소스에서 나타나는 동작 사이에 중요한 차이가 있습니다. 대부분의 보안 문제를 추적하면 컨피그레이션에서는 허용되었지만 여전히 보안을 침해하는 것으로 확인된 리소스 동작으로 거슬러 올라갑니다.

AWS 리소스 동작은 AWS 환경의 우수한 계측 및 가시성을 통해 관찰 가능합니다. 그러한 IT 가시성의 가치는 대부분 어떻게 문제를 탐지하느냐와 결부되어 있습니다. 그러나, AWS 가시성은 분명히 수많은 유용한 정보를 제공하며, 문제를 식별하는 것은 가시성 정보를 소비하는 사람에게 달려 있습니다. 이 점에서 바로 Cisco Stealthwatch Cloud가 두각을 나타냅니다.

Stealthwatch Cloud는 엔티티 모델링을 제공합니다. 우리의 엔티티 모델링 솔루션은 각 AWS 리소스의 소프트웨어 모델(즉, 거의 실시간 시뮬레이션)을 유지합니다. 여기에는 서버와 사용자는 물론, 보안 그룹 및 자동 확장 그룹 같은 AWS에 특정된 리소스 유형도 포함될 수 있습니다. 이러한 모델에는 VPC 플로우 로그, AWS CloudTrail, Amazon CloudWatch, AWS Config 및 Amazon Inspector 등 AWS 서비스에서 제공하는 구조화된 데이터 피드를 입력할 수 있습니다. 엔티티 모델링은 AWS 리소스의 역할 및 동작을 자동으로 발견합니다. 그런 다음 해당 동작을 지속적으로 추적하여 위험하거나 위협하는 동작이 발생하는 시기를 탐지합니다.

예를 들어, 정책 의도에 따라 VPC 내의 서버 인스턴스는 원격 로그인의 대상이 될 수 없다고 가정하고, 방화벽 규칙 정책을 실수로 변경하여 해당 컴퓨터에서 원격 로그인이 발생하였다고 가정합시다. 엔티티 모델링은 이 활동("비정상 원격 액세스")을 거의 실시간으로 발견하고 보고하며, 방화벽 규칙의 변화를 가져온 특정 AWS CloudTrail API 호출(사용자 이름, 날짜, 시간, 기타 세부 사항 포함)을 알려줍니다.

고려 사항: 소프트웨어, 정책 및 컨피그레이션 상태에 오류나 의도하지 않은 결과가 없음을 얼마나 확신합니까? 실수와 자잘한 사고를 신경 쓰지 않아도 된다고 확신할 수 있습니까? 안전한 시스템을 구축하는 것 자체로 보안이 유지되면 좋겠지만 현실은 오류, 오해, 오용이 보안 사고의 가장 일반적인 원인입니다. IT 환경을 운영하기 위해서는 위협 동작을 모니터링 할 수밖에 없습니다.

엔티티 모델링은 다음과 같은 몇 가지 중요한 등급의 보안 문제를 자동으로 탐지할 수 있습니다. 누군가 우리가 사용하는 소프트웨어 패키지의 백 도어를 발견했는가? 우리 공간에 설치되어 있는 서드파티 소프트웨어 또는 어플라이언스가 홈에 전화를 거는가? 권한 있는 사용자가 권한을 남용하는가? 컨피그레이션 실수로 인해 원격 액세스가 가능하거나 리소스를 의도와 다르게 사용되었는가? 엔티티 모델링은 사람, 프로세스 또는 기술에 대해 이전에 알려지지 않은 문제를 발견할 수 있는 고유한 형태의 보안 자동화 기능입니다.

심층 답변

가시성, ID 관리 및 정책 시행은 종합적으로 첫 날부터 제공되므로 AWS는 효과적인 보안을 유지할 수 있습니다. Stealthwatch Cloud의 엔티티 모델링 같은 기술을 사용하면 알려진 문제와 알려지지 않은 문제를 모두 신속하게 찾을 수 있고 효과적인 보안 성과를 얻을 수 있습니다. 이것이 처음 질문에 대한 간단한 답변입니다.

궁극적인 답변은 클라우드 컴퓨팅 자체의 특성에서 찾을 수 있습니다. 클라우드로의 전환은 단순히 "다른 사람의 환경으로 서버를 이동"하는 것이 아닙니다. 새로운 소프트웨어 아키텍처, 그리고 소프트웨어 개발자의 활동을 조직하기 위한 새로운 습관과 프로세스는 IT 운영 방식의 실질적인 변화를 만들어 가고 있습니다.

근본적인 예로서, 소위 DevOps 추세는 기존 방식의 개발, Q&A 및 운영 업무 분담이 단일 개발자 조직으로 축소되었음을 의미합니다. 이는 일시적인 추세가 아닙니다. 업무의 통합은 더욱 지속 가능하고 생산적인 인센티브를 통해 이루어집니다. 이제 소프트웨어 개발자는 스스로 테스트 및 QA 문제를 처리합니다. 이들은 프로덕션 운영 문제를 분류하는 것을 교대로 담당하고 디버깅 및 버그 수정을 최초의 코드 개발자에게 다시 되돌립니다. 프로세스의 모든 단계에서 피할 수 있는 곳이 없으므로, 향후에 당황스러운 일이나 더 큰 스트레스가 생기지 않도록 프로세스의 각 단계에서 모두가 최선을 다합니다. 그 결과, 클라우드 기반 개발 팀 및 IT 팀은 더 신속하게 기능을 제공하게 되고 운영 문제도 감소했습니다.

이러한 차이는 그저 피상적인 것이 아닙니다. AWS 자체가 그렇게 급성장하고 있는 이유가 무엇인지 생각해 보십시오. AWS를 도입한 기업들이 폭발적인 성장을 보였기 때문에 AWS도 덩달아 급속히 성장하고 있는 것입니다. AWS는 효율성, 확장성, 서비스와 기능의 민첩성을 위해 AWS만의 서비스를 사용하려는 기업에 적합합니다. AWS 고객은 대부분 의도적으로 3가지를 모두 추구합니다. 이러한 회사는 효율성, 확장성 및 기능 민첩성을 효과적으로 달성하기 때문에 번성한다고 생각해도 무방합니다.

이렇게 최신 AWS를 기반으로 하는 민첩한 기업은 시장에서 승리합니다. 이제 AWS에서 질적으로 우수한 보안을 제공하기 위한 더 심층적인 동기는 분명합니다. AWS 보안은 모든 측면에서 효율성, 확장성, 민첩성을 염두에 두고 설계해야 하기 때문입니다. AWS 기반 회사는 이 점을 요구합니다. 사실, 대부분의 AWS 기반 DevOps 조직에서 보안 및 사고 대응 활동은 운영 문제로 지원됩니다. 알림은 보안, 운영 또는 소프트웨어 정확성 문제 등 어떤 문제이든 일반적으로 최종 리소스 변경을 담당하는 DevOps 엔지니어에게 다시 배정됩니다. 정보 보안 문제와 관련하여 특히 대규모 조직에서는 전문가에게 문제가 배정될 수 있도록 하는 노력이 이루어지고 있습니다. 전문가들은 무엇보다 침입 또는 위반의 결과를 처리하고, 보고를 위해 사건을 문서화하며, 정책 변경 내용을 관리하고 학습한 내용에 따라 처리합니다.

하지만 중요한 것은 보안 사고 대응이 QA 및 독립형 작업에 일어났던 것과 유사한 방식으로, 그리고 거의 같은 이유로 점차 DevOps로 통합되고 있다는 점입니다. 기능을 제어하는 개발자보다 보안 문제를 더 잘 이해하고, 진단하고, 수정할 수 있는 사람은 없습니다.

결론

요약하자면, AWS 네이티브 서비스 및 Cisco Stealthwatch Cloud의 엔티티 모델링을 사용하는 AWS 환경은 알려진 보안 위협과 알려지지 않은 보안 위협을 확장 가능하고 비용 효율적인 방식으로 방지할 수 있습니다.

엔티티 모델링이 AWS 공간에 적합하다고 생각하거나 궁금한 사항이 있다면 www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html에서 무약정 무료 평가판을 시작해 보십시오.

C11-739663-00 09/17