에서 반도체 개발 환경을 보호하기 위한 전략 AWS

AWS 권장 가이드

AWS 권장 가이드: 에서 반도체 개발 환경을 보호하기 위한 전략 AWS

Table of Contents

에서 반도체 개발 환경을 보호하기 위한 전략 AWS

Mike Virgilio, Allan Carter, Nikhil Marrapu, Amazon Web Services(AWS)

2023년 6월(문서 기록)

이 문서는 AWS 클라우드에서 작동하는 반도체 워크로드의 규정 준수 요구 사항을 보호하고 충족하는 데 도움이 되는 전략적 지침을 제공합니다. 여기에는 이 지침을 구현하고 보안 위험으로부터 민감한 데이터를 보호하는 데 사용할 수 있는 AWS 서비스 및 기능에 대한 아키텍처 샘플과 개요가 포함되어 있습니다.

반도체 산업 개요

반도체 산업 협회에 따르면 반도체 비즈니스는 5,734억 4,000만 USD 규모의 글로벌 산업입니다. 지적 재산(IP)을 보호하기 위해 보안은 업계의 최고 우선순위입니다. 반도체 회사에는 엔지니어가 칩, 전자 시스템, 회로 기판 및 기타 제품을 설계할 수 있도록 개발 환경이 필요합니다. 보안 개발 환경은 IP에 액세스할 수 있는 사용자를 엄격하게 제어해야 합니다.

기업은 자체 IP를 개발하지만 일반적으로 프로세서 코어, 표준 인터페이스, 반도체 파운드리의 프로세스 설계 키트(PDK) 및 전자 설계 자동화(EDA) 회사의 라이선스 도구와 같은 서드 파티 벤더의 IP도 사용합니다. 협업 수준이 매우 높은 개발 프로세스의 특성으로 인해 내부 엔지니어와 서드 파티 회사의 엔지니어가 모두 개발 환경에 액세스해야 합니다. 중요한 보안 요구 사항은 보안 개발 환경에서 무단 데이터 유출을 방지하는 것입니다.

반도체 회사에는 최신 기술 기능이 필요합니다.

반도체 기업은 빠른 시장 출시 및 혁신이 성공에 필수적인 경쟁 업계 환경에서 운영됩니다. 칩 설계 및 제작 요구 사항이 점점 더 복잡해짐에 따라, 반도체 회사는 업계의 수요를 충족하고 능가하기 위해 최신 기술에 액세스해야 합니다. 컴퓨팅 및 스토리지 요구 사항의 기하급수적인 증가는 AWS 클라우드의 확장성과 용량으로 충족될 수 있습니다. 포괄적인 인프라와 강력한 컴퓨팅, 네트워크 및 스토리지 솔루션 세트를 통해 AWS 는 반도체 기업이 기계 학습, 고성능 컴퓨팅 및 자동화와 같은 최첨단 기술을 활용할 수 있도록 지원합니다. 이러한 기술을 사용하면 연구 및 개발 노력을 가속화하고, 제조 프로세스를 최적화하며, 최신 기술에 액세스할 수 있습니다. 소중한 IP는 정교한 공격의 매력적인 대상이므로 보안이 안전한 개발 환경의 최고 우선순위입니다.

규모, 탄력성 및 자동화의 경제 사용

AWS 는 기업에 성공에 필수적인 규모, 리소스 탄력성 및 자동화 기능의 경제성을 제공합니다. AWS 는 수십만 개의 기업과 파트너 관계를 맺고 있기 때문에 대규모 규모의 경제를 달성할 수 있으며, 이로 인해 모든 기업의 비용이 절감됩니다. AWS 인프라 탄력성을 통해 기업은 가장 까다로운 워크로드를 충족하기 위해 쉽게 확장한 다음 비용을 최적화하기 위해 축소할 수 있습니다. 또한 AWS 자동화 기능은 기업이 차별화되지 않은 수동 작업을 최소화하는 반복 가능한 프로세스를 생성하는 데 도움이 됩니다. 는 광범위한 보안 서비스 및 기능을 AWS 제공하여 네트워크 세분화, 데이터 암호화 및 규정 준수를 비롯한 강력한 보안 제어를 통해 반도체 기업이 워크로드를 보호할 수 있도록 지원합니다. 를 구축하면 AWS 클라우드반도체 기업은 혁신과 성장에 집중할 수 있을 뿐만 아니라 데이터와 운영이 잠재적 보안 위험으로부터 복원력을 유지할 수 있습니다.

에서 반도체 개발 환경의 보안 및 규정 준수 달성 AWS

AWS 는 보안 제어를 구현하기 위한 모범 사례 지침을 개발하고 반도체 산업 요구 사항을 해결하기 위해 참조 아키텍처를 게시했습니다. 이 섹션에서는 AWS 권장 설계 및 참조 아키텍처를 사용하여 미션 크리티컬 워크로드의 보안 및 규정 준수를 달성하는 방법을 설명합니다 AWS.

를 사용하여 규정 준수 작업 감소 AWS

AWS 공동 책임 모델은 AWS 와 고객 간에 보안 및 규정 준수에 대한 책임을 공유하는 방법을 설명합니다. AWS 는 클라우드의 보안을 담당하고 고객은 클라우드의 보안을 담당합니다. 이를 통해 기업은 클라우드 인프라에 대한 책임을 AWS에 넘겨 기업 및 규제 요구 사항을 준수하는 데 필요한 노력을 줄일 수 있습니다.

다음은 반도체 회사가 기업 및 규제 요구 사항 준수를 입증하는 데 도움이 될 AWS 서비스 수 있습니다.

- AWS Artifact에서는 국제 표준화 기구(ISO), 국립 표준 기술 연구소(NIST), 연방정부의 위험 및 인증 관리 프로그램(FedRAMP)을 비롯한 다양한 규정 준수 프레임워크에 대한 다운로드 가능한 규정 준수 보고서를 제공합니다. AWS Artifact 보고서를 클라우드 리소스에 대한 기업 평가와 결합하여 감사자에게 규정 준수를 입증하고 미국 국제 무기 거래 규정(ITAR)과 같은 규정을 준수하는 데 필요한 시간과 노력을 줄일 수 있습니다.
- AWS Audit Manager는 사전 구축된 사용자 지정 프레임워크와 자동 증거 수집을 사용하여 규정 준수 요구 사항을 AWS 사용 데이터에 매핑할 수 있습니다.

회사는 이러한 서비스와 기능을 사용하여 기업 및 규제 요구 사항을 보다 효율적이고 효과적으로 준수할 수 있습니다. AWS 서비스 가 AWS 보증 프로그램의 범위에 속하는지 여부에 대한 자세한 내용은 AWS 서비스 규정 준수 프로그램별 범위 내 섹션을 참조하세요.

제공된 참조 아키텍처 사용

AWS 는 다양한 산업에 걸쳐 수천 개의 배포를 기반으로 규범적 지침과 모범 사례를 개발합니다. 이러한 권장 사항은 AWS Well-Architected Framework, AWS Cloud Adoption Framework(AWS CAF) 및 AWS Security Reference Architecture(AWS SRA)에 포함되어 있습니다.

보안 개발 환경을 설계하고 설계할 때는 앞서 언급한 프레임워크를 기반으로 하는 반도체 및 전자 참조 아키텍처를 AWS 제공합니다. 이러한 참조 아키텍처는 데이터와 워크로드를 보호하도록 설계되었습니다.

AWS 보안 성숙도 모델을 사용하여 단계별 접근 방식으로 보안 제어 백로그를 안내할 수 있습니다.

이러한 프레임워크, 모델 및 참조 아키텍처를 활용하여 클라우드에서 강력한 보안 태세를 구축하고 중요한 자산을 보호할 수 있습니다.

에서 반도체 데이터 보호 AWS

를 사용하면 데이터의 프라이버시 제어를 AWS관리하고 데이터가 사용되는 방식, 데이터에 액세스할 수 있는 사람, 데이터가 암호화되는 방식을 제어할 수 있습니다. 이러한 역량은 유연한 보안 클라우드 컴퓨팅 환경에서 보강됩니다. 이 섹션에서는 반도체 회사가 데이터 액세스 제어를 구현하고 데이터 레지던시 요구 사항을 해결하는 데 도움이 되는 AWS 기능을 검토합니다.

이 섹션은 다음 주제를 포함합니다:

- 무단 액세스 및 데이터 유출 방지
- 에서 데이터 레지던시 요구 사항 충족 AWS

무단 액세스 및 데이터 유출 방지

2022 Cost of a Data Breach Report(Ponemon Institute 보고서)에 따르면 2022년 데이터 침해로 인해 발생한 평균 비용은 430만 USD였습니다. 반도체 회사의 경우 지적 재산(IP)을 보호하는 것이 중요합니다. 무단 액세스로 인해 IP가 손실되면 재정적 손실, 평판 손상 또는 규제 결과가 발생할 수 있습니다. 이러한 잠재적 결과로 인해 잘 설계된 설계의 중요한 데이터 측면과 데이터에 대한 액세스를 제어할 수 있습니다.

데이터 보안을 위한 주요 고려 사항은 다음과 같습니다.

- 보안 개발 환경에 액세스하기 위한 사용자 인증
- 보안 개발 환경 내부의 데이터에 액세스하기 위한 사용자 권한 부여
- 보안 개발 환경 내부 및 외부로 모든 전송 로깅
- 여러 환경 사이에서 보안 데이터 흐름 설계
- 저장 데이터 및 전송 중 데이터 암호화
- 아웃바운드 네트워크 트래픽 제한 및 로깅

권한 구성

AWS Identity and Access Management (IAM)는 AWS 리소스에 대한 액세스를 인증하고 사용할 수 있는 권한을 부여받은 사용자를 제어하여 리소스에 대한 액세스를 안전하게 관리하는 데 도움이 됩니다. 기본적으로 AWS 의 모든 작업은 명시적으로 허용되지 않는 한 묵시적으로 거부됩니다. 정책을 생성하여 AWS 에서 액세스를 관리합니다. 정책을 사용하여 세분화된 수준에서 사용자가 액세스할 수 있는

리소스와 해당 리소스에 대해 수행할 수 있는 작업을 정의할 수 있습니다. AWS 가장 좋은 방법은 최소 권한 권한을 적용하는 것입니다. 즉, 사용자에게 작업을 수행하는 데 필요한 권한만 부여하는 것입니다. 자세한 내용은 IAM 설명서에서 다음을 참조하세요.

- IAM의 정책 및 권한
- 정책 평가 로직
- IAM의 보안 모범 사례

사용자 인증

인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 에 액세스하도록 요구하는 것이 AWS 모범 사례입니다. 사용자 인력 액세스를 중앙 집중화하는 데 권장되는 서비스는 AWS IAM Identity Center입니다. 이 서비스를 사용하면 직원 자격 증명을 안전하게 생성 또는 연결하고 AWS 계정 및 애플리케이션에서 액세스를 중앙에서 관리할 수 있습니다. IAM Identity Center는 원활한 통합 및 사용자 관리를 제공하기 위해 SAML 2.0, Open ID Connect(OIDC) 또는 OAuth 2.0을 사용하여 외부 ID 제공업체(idP)와 페더레이션할 수 있습니다. 자세한 내용은 (AWS 마케팅)의 자격 증명 페더레이션 AWS 및 자격 증명 공급자 및 페더레이션(IAM 설명서)을 참조하세요.

AWS Directory Service를 사용하여 Active Directory와 같은 디렉터리에 정의된 사용자 및 그룹을 관리해 사용자를 인증하고 권한을 부여할 수도 있습니다. 보안 개발 환경 내에서 Linux 파일 권한을 사용하여 가상 프라이빗 클라우드(VPC) 내의 데이터 액세스를 승인하고 제한할 수 있습니다. VPC 엔드포인트를 사용하여 퍼블릭 인터넷을 통과 AWS 서비스 하지 않고에 대한 액세스를 제공합니다. 엔드포인트 정책을 사용하여 엔드포인트를 사용할 수 있는 보안 AWS 주체를 제한하고 자격 증명 기반 정책을 사용하여 액세스를 제한합니다 AWS 서비스.

데이터 전송

AWS 는 온프레미스 데이터를 클라우드로 마이그레이션하는 몇 가지 방법을 제공합니다. 처음에는 Amazon Simple Storage Service(Amazon S3)에 데이터를 저장하는 것이 일반적입니다. Amazon S3는 원하는 양의 데이터를 저장, 보호 및 검색하는 데 도움이 되는 클라우드 기반 객체 스토리지 서비스입니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 데이터를 송수신하는 경우 최대 25Gbps의 대역폭을 제공합니다. 또한 교차 리전 데이터 복제 및 데이터 계층화를 제공합니다. Amazon S3에 저장된 데이터는 복제 소스 역할을 할 수 있습니다. 이를 사용하여 새 파일 시스템을 생성하거나 EC2 인스턴스로 데이터를 전송할 수 있습니다. Amazon S3를 반도체 도구 및 흐름을 위한 AWS 관리형 포터블 운영 체제 인터페이스(POSIX) 호환 파일 시스템의 백엔드로 사용할 수 있습니다.

또 다른 AWS 스토리지 서비스는 업계 표준 연결 프로토콜을 지원하고에서 고가용성 및 복제를 제공하는 파일 시스템을 제공하는 Amazon FSx입니다 AWS 리전. 반도체 산업의 일반적인 선택 사항으로,

Amazon FSx for NetApp ONTAP, Amazon FSx for Lustre, Amazon FSx for OpenZFS가 포함됩니다. Amazon FSx의 확장 가능한 고성능 파일 시스템은 보안 개발 환경 내부에 로컬로 데이터를 저장하는 데 매우 적합합니다.

AWS 에서는 먼저에서 AWS 반도체 워크로드의 스토리지 요구 사항을 정의한 다음를 AWS 사용하여 온프레미스에서 로 데이터를 전송하는 적절한 데이터 전송 메커니즘AWS DataSync을 식별할 것을 권장합니다 AWS. DataSync는 파일 또는 객체 데이터를 AWS 스토리지 서비스 간에 또는 해당 서비스에서 송수신하는 데 도움이 되는 온라인 데이터 전송 및 검색 서비스입니다. 자체 관리형 스토리지 시스템을 사용하는지 또는 NetApp과 같은 스토리지 공급자를 사용하는지에 따라 인터넷을 통해 또는 AWS Direct Connect를 통해 안전한 개발 환경으로 데이터를 빠르게 이동하고 복제하도록 DataSync를 구성할 수 있습니다. DataSync는 소유권, 타임스탬프, 액세스 권한과 같은 파일 시스템 데이터 및 메타데이터를 전송할 수 있습니다. FSx for ONTAP과 NetApp ONTAP 간에 파일을 전송하는 경우 NetApp SnapMirror를 사용하는 것이 AWS 좋습니다. Amazon FSx는 저장 및 전송 중 암호화를 지원합니다. AWS CloudTrail 및 기타 서비스별 로깅 기능을 사용하여 모든 API 직접 호출 및 관련 데이터 전송을 로깅합니다. 전용 계정의 로그를 중앙 집중화하고 변경 불가능한 기록에 대해 세분화된 액세스 정책을 적용합니다.

AWS 는 , AWS Network Firewall Amazon Route 53 Resolver DNS 방화벽, 및 웹 프록시AWS WAF와 같은 애플리케이션 인식 네트워크 방화벽을 포함하여 데이터 흐름을 제어하는 데 도움이 되는 추가 서비스를 제공합니다. Amazon Virtual Private Cloud(Amazon VPC)의 보안 그룹, 네트워크 액세스 제어 목록 및 Amazon Virtual Private Cloud(Amazon VPC)의 VPC 엔드포인트, 네트워크 방화벽, 전송 게이트웨이 라우팅 테이블 및 AWS Organizations의 서비스 제어 정책(SCP을 사용해 네트워크 세분화를 적용하여 환경 내에서 데이터 흐름을 제어합니다. VPC 흐름 로그와 VPC 흐름 로그 버전 2~5의 사용 가능한 필드를 사용하여 모든 네트워크 트래픽을 중앙에서 로깅합니다.

데이터 암호화

AWS Key Management Service (AWS KMS) 고객 관리형 키 또는 AWS CloudHSM을 사용하여 저장된 모든 데이터를 암호화합니다. 세분화된 키 리소스 정책을 생성하고 유지 관리합니다. 자세한 내용은 Creating an enterprise encryption strategy for data at rest를 참조하세요.

업계 표준 256비트 고급 암호화 표준(AES-256) 암호로 최소 TLS 1.2를 적용하여 전송 중 데이터를 암호화합니다.

아웃바운드 네트워크 트래픽 관리

보안 개발 환경에 인터넷 액세스가 필요한 경우 모든 아웃바운드 인터넷 트래픽은 오픈 소스 프록시인 Network Firewall 또는 Squid와 같은 네트워크 수준 적용 지점을 통해 로깅되고 제한되어야 합니다.

VPC 엔드포인트와 인터넷 프록시는 사용자의 무단 데이터 유출을 방지하는 데 도움이 됩니다. 이는 보안 개발 환경 내에서 그리고 VPC 내에서만 데이터에 대한 액세스를 허용하는 데 중요합니다.

마지막으로 Amazon VPC의 기능인 Network Access Analyzer를 사용하여 네트워크 세분화 검증을 수행하고 지정된 요구 사항을 충족하지 않는 잠재적 네트워크 경로를 식별할 수 있습니다.

보안 제어를 계층화하면 강력한 데이터 경계를 설정하고 적용할 수 있습니다. 자세한 내용은 데이터 경계 구축을 참조하세요 AWS.

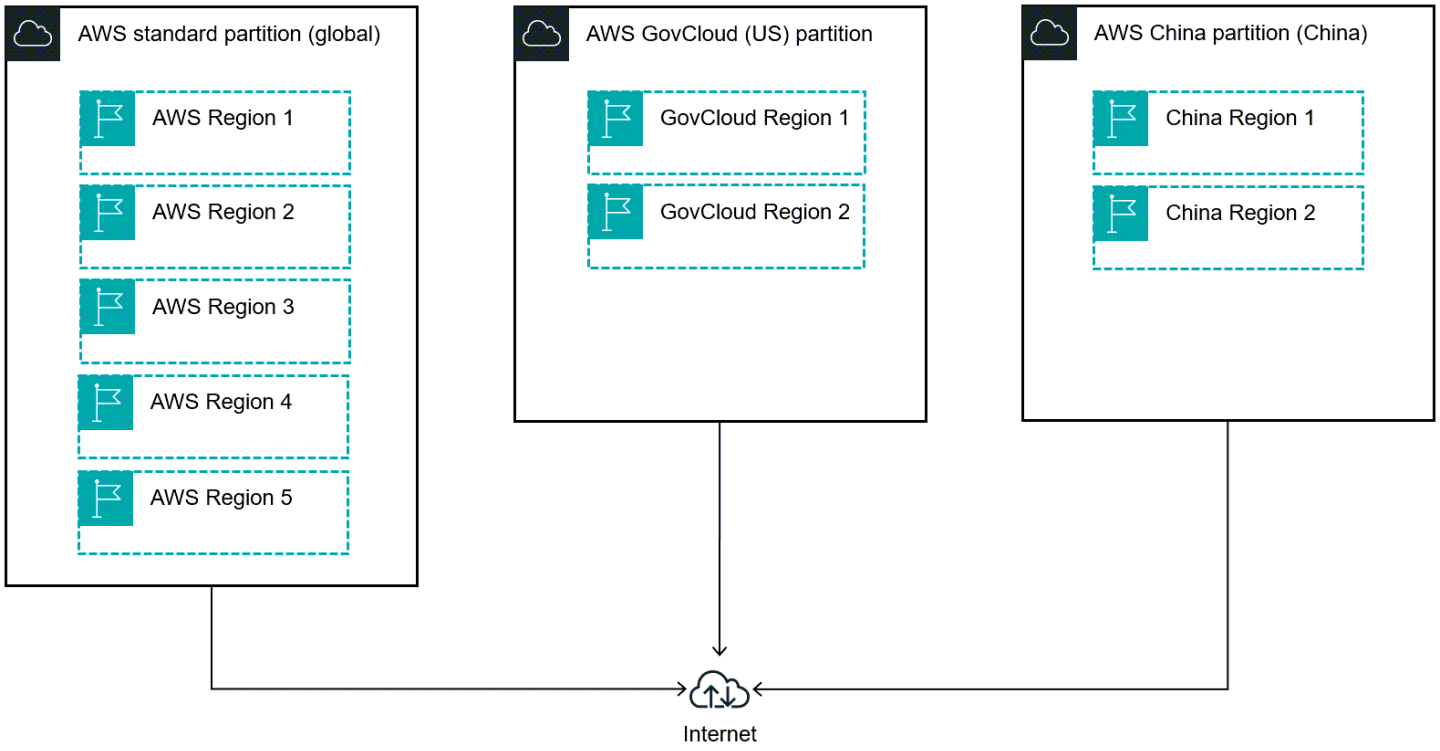
에서 데이터 레지던시 요구 사항 충족 AWS

사용 가능한 파티션, AWS 리전가용 영역 및 로컬 영역을 통해 기업은 고유한 요구 사항에 따라 데이터 및 워크로드에 가장 적합한 위치를 선택할 수 있습니다.

- 파티션은의 논리적 그룹입니다 AWS 리전. AWS 상용 리전은 `aws` 파티션에 있고, 중국 리전은 `aws-cn` 파티션에 있으며, `aws-us-gov` 파티션에 AWS GovCloud (US) Regions 있습니다.
- AWS 리전는가 데이터 센터를 AWS 클러스터링하는 별도의 지리적 영역입니다.
- 각 AWS 리전 에는 가용 영역이라고 하는 격리된 위치가 여러 개 있습니다.
- 로컬 영역은 사용자와 지리적으로 가까운 리전의 확장입니다.

현재 사용 가능한 리전, 가용 영역 및 로컬 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

파티션은 다른 파티션의 리전에서 데이터, 네트워크 및 시스템 격리를 제공합니다. AWS 파티션은 서로 다른 파티션의 리전 간에 별도의 보안 인증 액세스로 논리적 네트워크 격리를 생성합니다. 파티션에는 하나 이상의 리전이 포함되지만는 하나의 파티션 내에만 AWS 리전 존재하며는 두 파티션의 일부가 될 수 AWS 리전 없습니다.



미국 정부 보안 분류가 필요한지에 따라 파티션 중에서 선택할 수 있습니다. 미분류 또는 공식 데이터를 처리하는 워크로드는 AWS GovCloud (US) 또는 표준 파티션을 모두 사용할 수 있습니다. AWS 또한는 비밀 및 미국 일급 보안 분류 수준에서 워크로드를 운영할 수 있도록 인증된 추가 파티션을 제공하지만이 설명서의 범위를 벗어납니다. 이러한 분류 수준에서 워크로드를 운영하는 방법에 대한 자세한 내용은 Cloud Computing for US Defense 및 Cloud Computing for the US Intelligence Community를 참조하세요.

규정 준수, 운영 및 기술적 문제를 줄이려면 단일 파티션 내에 다중 리전 워크로드를 배포하는 것이 좋습니다. 그러나 AWS Direct Connect 또는 Amazon CloudFront에서와 같이 제한된 사용 사례가 있습니다. 이 경우 특정 목표를 달성하기 위해 여러 위치에서 서비스를 통합할 수 있습니다. 자세한 내용은 AWS 솔루션 아키텍트에 문의하십시오.

엔지니어에게 안전한 원격 경험 제공

원격 시각화는 반도체 설계의 핵심 구성 요소입니다. 도구 엔지니어는 원격 확인을 사용하고 칩 디자이너는 이를 사용하여 작업을 제출하고 상태를 확인합니다. 이 섹션에서는 다양한 네트워크 조건에서 뛰어난 성능을 발휘할 수 있는 강력한 솔루션을 제공합니다. 클라우드 네이티브로 설계되어 AWS 보안 서비스와 원활하게 통합할 수 있습니다.

이 섹션은 다음 주제를 포함합니다:

- 원격 데스크톱 경험 최적화
- 서드 파티와의 엔지니어링 협업 보안

원격 데스크톱 경험 최적화

디자이너는 일반적으로 터미널 기반 SSH 세션 또는 그래픽 원격 데스크톱을 사용하여 워크플로를 제출하고 시각화합니다. 원격 데스크톱은 도구 엔지니어와 칩 디자이너가 작업을 제출할 수 있도록 GUI 기반 대화형 도구(예: 레이아웃, 장소 및 경로)를 제공합니다. AWS 는 엔지니어링 및 물리적 설계 팀을 위한 강력한 사용자 인터페이스를 제공하는 고성능 원격 디스플레이 프로토콜인 Amazon DCV를 제공합니다. Amazon DCV는 다양한 네트워크 조건에서 뛰어난 성능을 발휘합니다.

Amazon DCV는 데이터 개인 정보 보호를 보호하기 위해 지오메트리가 아닌 픽셀을 스트리밍합니다. 또한 Amazon DCV는 TLS를 사용하여 픽셀 및 최종 사용자 입력을 보호합니다.

연결 파일을 사용하여 사용자는 Amazon DCV 세션에 즉시 연결할 수 있습니다. 그러나 연결 파일 파라미터는 암호화 없이 `password` 및 `proxypassword` 필드를 사용합니다. 자세한 내용은 Using a connection file을 참조하세요. Amazon DCV는 서버와 클라이언트 간에 TLS 연결을 설정합니다. 연결 파일의 검증 정책은 인증서를 신뢰할 수 있는 것으로 확인할 수 없을 때 클라이언트가 응답하는 방식을 결정합니다. 자세한 내용은 Set certificate validation policy를 참조하세요.

원격 데스크톱 기능을 제공하는 다른 온프레미스 상용 솔루션으로, NoMachine 또는 OpenText Exceed TurboX가 포함됩니다.

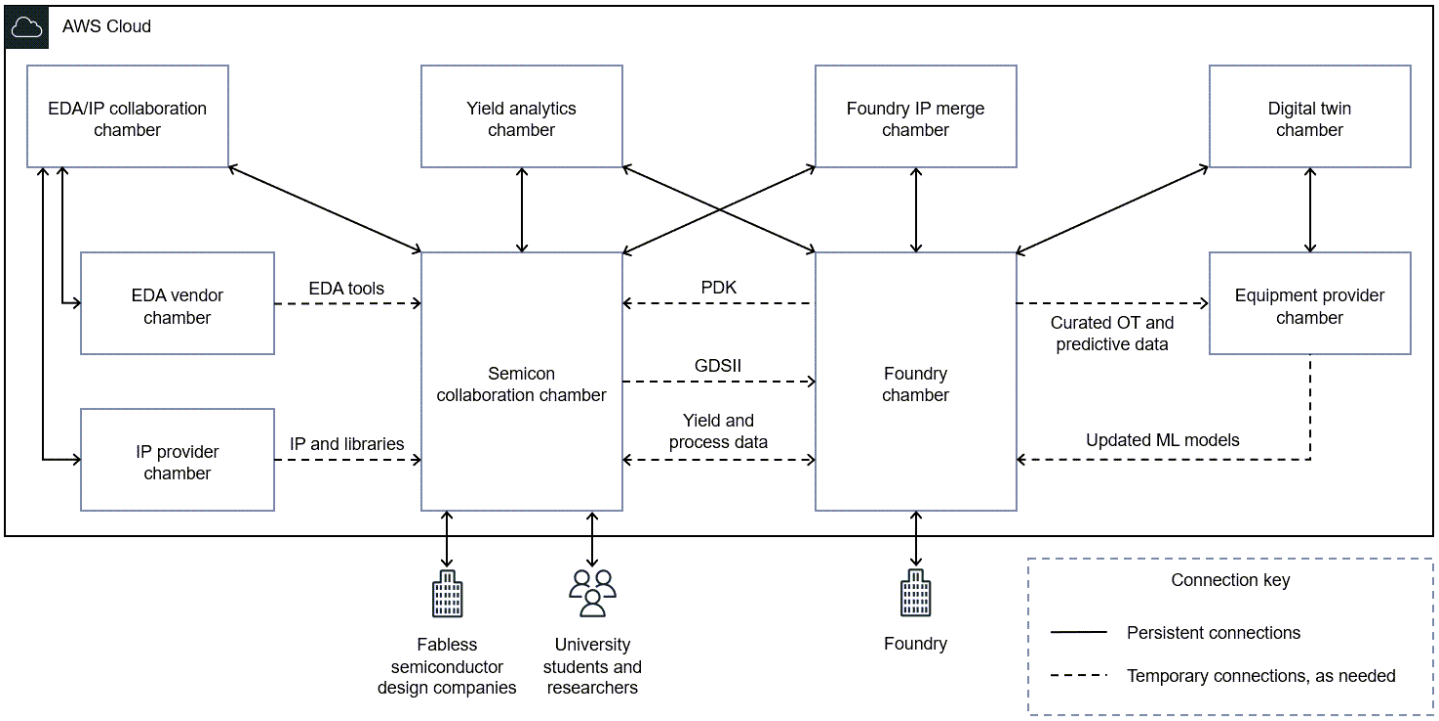
원격 데스크톱 솔루션에서 기본 인프라는 Amazon Elastic Compute Cloud(Amazon EC2)로 구동됩니다. 공동 책임 모델에 따르면 사용자의 책임에 원격 데스크톱 인스턴스를 보호하는 데 도움이 되도록 다음 영역이 포함됩니다.

- VPC 및 보안 그룹을 구성하는 등의 작업을 통해 인스턴스에 대한 네트워크 액세스 제어. 자세한 내용은 네트워크 트래픽 제어를 참조하세요.

- 인스턴스 연결에 사용되는 자격 증명을 관리합니다.
- 업데이트 및 보안 패치를 포함하여 게스트 운영 체제에 배포된 게스트 운영 체제 및 소프트웨어를 관리합니다. 자세한 내용은 Amazon EC2 업데이트 관리를 참조하세요.
- 인스턴스에 연결된 IAM 역할 및 해당 역할과 연결된 권한을 구성합니다. 자세한 내용은 Amazon EC2의 IAM 역할을 참조하세요.

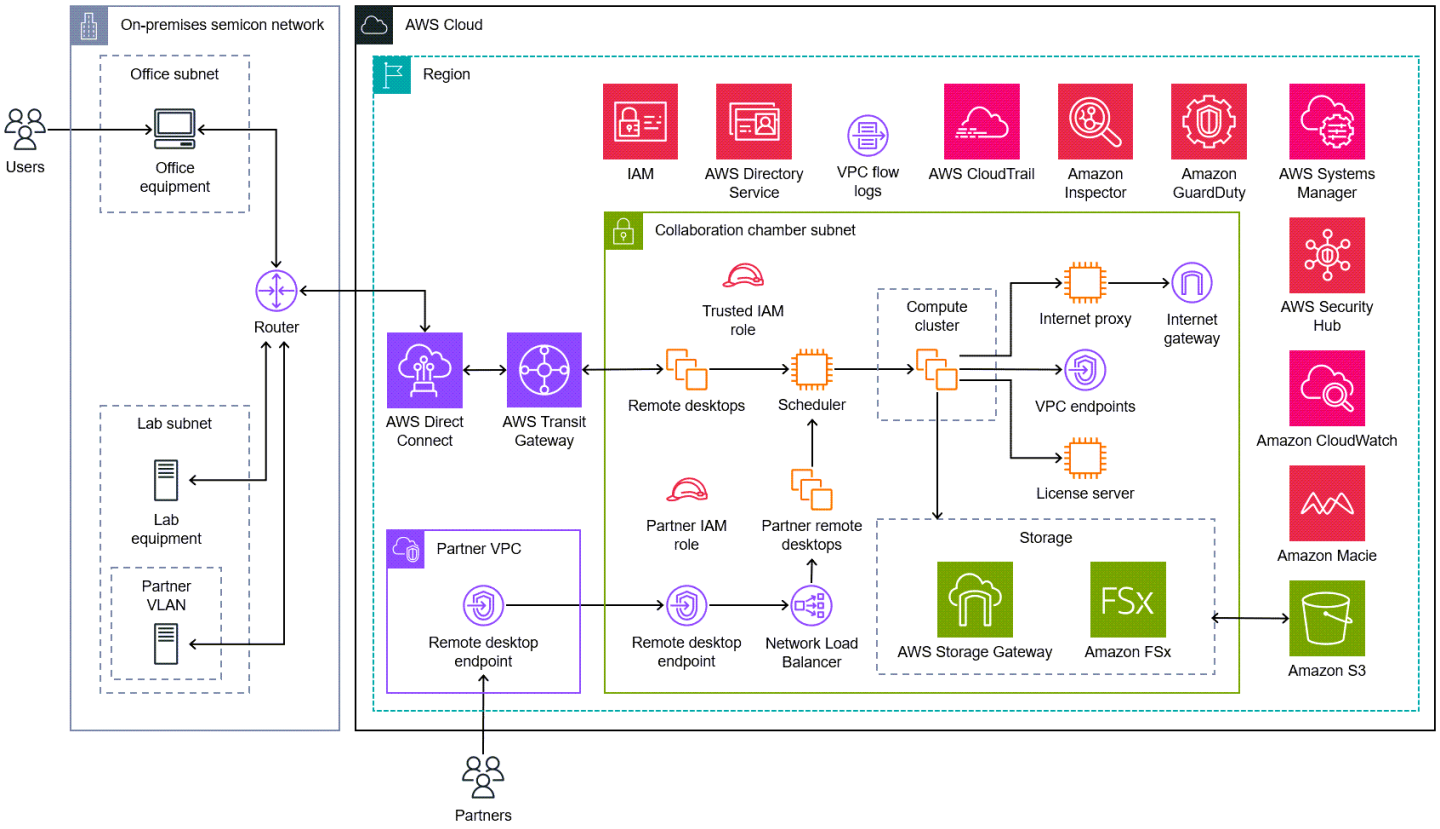
서드 파티와의 엔지니어링 협업 보안

도구 문제를 디버깅하고, 설계를 위한 IP 통합에 대한 도움을 받으며, 전문 기술을 갖춘 외부 계약업체를 도입하려면 개발 중에 서드 파티와의 협업이 필수적입니다. 온프레미스 인프라에서 서드 파티에 보안 액세스를 제공하는 것은 어려울 수 있습니다. 코드형 AWS 인프라(IaC)를 사용하면 공동 작업실이라는 기본 보안 개발 환경의 사본을 생성할 수 있습니다. 데이터 유출을 방지하려면 인터넷에 액세스할 수 없도록 하여 협업 챔버의 보안 태세를 강화합니다. 협업 챔버에는 협업자를 위한 계정이 있으며, 협업에 필요한 것만 포함하도록 챔버의 데이터, 도구 및 인프라를 선별할 수 있습니다. 협업이 완료되면 협업 챔버를 삭제하여 비용을 절감하고 데이터에 대한 잠재적 액세스를 제거합니다. 다음 다이어그램에서는 설계 및 제조 프로세스의 여러 참가자가 다양한 유형의 협업 챔버를 사용하는 방법을 보여줍니다.



다음 이미지는 협업 챔버의 참조 아키텍처입니다. 이 아키텍처는 AWS에서 협업 챔버를 설계하고 구축할 때 참조로 사용할 수 있습니다. 다이어그램의 AWS 보안, 거버넌스 및 모니터링 서비스는 IP를 보호

하기 위해 체임버를 보호하는 데 도움이 됩니다. 이 서비스에 대한 자세한 내용은 이 가이드의 AWS 반도체 개발 환경을 위한 보안 서비스 섹션을 참조하세요.



AWS 반도체 개발 환경을 위한 보안 서비스

AWS 는에서 워크로드와 애플리케이션을 보호하도록 설계된 보안 서비스를 개발했습니다 AWS 클라우드. 이러한 서비스는 반도체 워크로드뿐만 아니라 클라우드에서 작동하는 모든 유형의 워크로드를 보호하는 데 도움이 될 수 있습니다. 이를 통해 AWS 서비스기업은 강력한 예방 및 탐지 제어를 설정하고, 보안 태세를 거의 실시간으로 모니터링하고, 보안 위험 및 인시던트가 발생할 때 신속하게 해결할 수 있습니다. 이러한 서비스는 적용 범위와 설정된 보안 태세를 유지 관리하기 위해 환경에 따라 자동으로 규모를 조정할 수 있습니다. 또한 이러한 서비스는 특정 기능에 초점을 맞출 수 있지만 Amazon EventBridge라는 공통 메시징 버스를 지원하므로 서비스를 통합하고 보안 위험에 자동으로 대응할 수 있습니다.

다음 AWS 서비스 및 기능은 액세스 및 정책을 관리하고, 보안 위험 및 이벤트를 감지 및 대응하고, 환경에서 모니터링 및 로깅을 구현하는 데 도움이 될 수 있습니다 AWS .

- AWS CloudTrail은 AWS 계정의 거버넌스, 규정 준수, 운영 및 위험을 감사하는 데 도움이 됩니다.
- Amazon GuardDuty는 AWS 환경에서 예상치 못한 활동, 잠재적으로 승인되지 않은 활동 또는 악의적 활동을 식별할 수 있도록 지원하는 보안 모니터링 서비스입니다.
- Amazon Inspector는 소프트웨어 취약성 및 의도하지 않은 네트워크 노출이 AWS 있는지 워크로드를 지속적으로 스캔하는 취약성 관리 서비스입니다.
- AWS Security Hub CSPM는의 보안 상태에 대한 포괄적인 보기를 제공합니다 AWS. 또한 보안 업계 표준 및 모범 사례를 기준으로 AWS 환경을 확인하는 데 도움이 됩니다.
- Amazon Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화합니다 AWS 계정. 이 보안 데이터를 쿼리하고 분석하여 추세와 이상을 검색할 수 있습니다.
- 서비스 제어 정책(SCPs)은 AWS 서비스 여러 계정에서 사용을 중앙에서 관리하는 데 도움이 AWS Organizations 되는의 정책 유형입니다.
- VPC 흐름 로그는 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처하는 데 사용할 수 있는 Amazon Virtual Private Cloud(Amazon VPC)의 기능입니다. 이 데이터를 사용하여 문제를 해결하고 인시던트에 대응할 수 있습니다.

랜섬웨어로부터 반도체 워크로드 및 데이터 보안

랜섬웨어는 결제가 완료될 때까지 컴퓨터 시스템이나 데이터에 대한 액세스를 차단하도록 설계된 악성 소프트웨어입니다. 안타깝게도 이러한 유형의 공격은 인터넷에서 널리 발생하며 모든 규모의 기업에 영향을 미칠 수 있습니다. 재정적 손실 및 평판 손상 외에도, 중단으로 인해 비즈니스 에코시스템 전반에 걸쳐 대규모의 계단식 공급망이 영향을 받을 수 있으므로 반도체 회사는 운영 중단을 방지해야 합니다. 또한 중요한 지적 재산이 손실될 수 있습니다.

랜섬웨어로부터 보호하기 위해 반도체 회사는 온프레미스 및 클라우드 환경의 모든 측면, 특히 데이터를 저장, 처리 또는 전송하는 시스템을 보호하기 위해 주의해야 합니다.는 이러한 유형의 인시던트로부터 보호하는 데 도움이 되는 많은 아키텍처 설계 및 제어를 AWS 제공합니다. 이 가이드에서 언급한 제어 외에도 랜섬웨어로부터 클라우드 워크로드를 보호하는 방법에 대한 다음 AWS 리소스를 참조하세요.

- AWS 클라우드 보안 - 랜섬웨어로부터 보호(AWS 클라우드 보안)
- AWS 랜섬웨어 방어를 위한 블루프린트(AWS 보안 블로그 게시물)
- 랜섬웨어로부터 AWS 환경 보호(AWS 웨비나)
- eBook: 랜섬웨어로부터 AWS 환경 보호(AWS eBook)
- The anatomy of ransomware event targeting data residing in Amazon S3(AWS 보안 블로그 게시물)
- NIST 사이버 보안 프레임워크(CSF) AWS 사용에 대한 랜섬웨어 위험 관리(AWS 백서)

반도체 산업의 AWS 클라우드 차별화 요소

온프레미스 환경에서 로 마이그레이션하는 비즈니스 사례는 반도체 기업에 매우 매력적일 AWS 수 있습니다. 온프레미스 인프라는 관리하는 데 비용이 많이 들고, 상당한 선결제 투자가 필요하며, 최신 기술을 유지하고 최신 상태를 유지하기 위해 상당한 노력이 필요하고, 광범위한 독립 벤더로부터 보안 도구를 소싱해야 합니다. AWS를 사용하면 사용하는 리소스에 대해서만 비용을 지불하므로 워크로드 비용을 최적화하는 데 도움이 될 수 있습니다. AWS 또한는 최신 고성능 컴퓨팅(HPC)과 클라우드 스토리지 서비스 및 기능에 대한 즉각적인 액세스를 제공합니다. 예를 들어 Amazon FSx for NetApp ONTAP은 일반적으로 사용되는 스토리지 서비스입니다. 이를 사용하여 온프레미스 NetApp 스토리지에서 로 데이터를 원활하게 마이그레이션할 수 있으며, 네트워크 격리 AWS 클라우드, 리소스 수준 권한, 자격 증명 기반 인증, 암호화, 로깅 및 감사를 제공합니다.

AWS 또한는 반도체 회사의 보안 솔루션을 프로비저닝하고 관리하는 효율성을 개선할 수 있습니다. 의 고급 보안 기능 및 서비스를 사용하면 보안 위험으로부터 데이터와 워크로드를 보호하는 데 도움이 되는 강력한 보안 태세를 구현 AWS할 수 있습니다. AWS Organizations 및 통합 보안 서비스를 사용하면 조직 내 모든 AWS 계정 에 보안 제어를 자동으로 배포할 수 있습니다. 자동화 기능을 사용하면 위험에 자동으로 대응하고 보안 운영을 간소화하여 포괄적인 보안 아키텍처를 관리하는 데 필요한 시간과 리소스를 줄일 수 있습니다. 예를 들어는 전체 환경에서 자동화된 보안 관리, 지속적인 규정 준수 모니터링, 위험 감지 및 대응을 위한 도구와 서비스를 AWS 제공합니다. 이러한 솔루션을 사용하여 반도체 회사는 비용을 절감하고 효율성을 높이는 동시에 보안 태세를 개선할 수 있습니다. 전반적으로 로 마이그레이션하면 반도체 기업이 확장성, 유연성 및 보안 측면에서 상당한 이점을 실현하는 데 도움이 될 AWS 수 있습니다.

결론

AWS는 반도체 회사의 요구 사항을 지원하는 광범위하고 안전한 플랫폼을 제공합니다. 최신 기술을 사용하고 규모 조정의 경제성, 탄력적 규모 조정 역량 및 다양한 보안 서비스를 활용하면 반도체 회사는 AWS 클라우드에서 비즈니스를 혁신할 수 있습니다. AWS 클라우드의 이러한 이점은 혁신과 지속적인 성장을 위해 최적화하면서 복잡한 문제를 해결합니다. AWS 글로벌 인프라는 데이터 레지던시 및 보안 분류 요구 사항과 같은 가장 정교한 요구 사항을 지원할 준비가 되어 있습니다. AWS는 비용을 절감하고, 민첩성을 개선하며, 더 빠르게 혁신하고, 클라우드에서 지적 재산을 보호하는 데 도움이 될 수 있습니다. AWS 클라우드에서 반도체 개발 환경을 구성하는 데 도움이 필요하면 AWS 계정 팀에 문의하거나 AWS 문의 양식을 사용하세요. 반도체 산업에 대한 추가 AWS 정보 및 리소스는 Semiconductor & Hi-Tech Electronics를 참조하세요.

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
최초 게시	—	2023년 6월 20일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.